Detection of Denial-of-Service Attacks Based on Computer Vision Techniques

A Thesis Submitted for the Degree of
Doctor of Philosophy

By

Zhiyuan Tan

in

Faculty of Engineering and Information Technology
UNIVERSITY OF TECHNOLOGY, SYDNEY
AUSTRALIA
19TH DECEMBER 2013

CERTIFICATE

Date: **19th December 2013**

Author: **Zhiyuan Tan**

Title: **Detection of Denial-of-Service Attacks Based on Computer Vision Techniques**

Degree: **Ph.D.**

I certify that this thesis has not already been submitted for any degree and is not being submitted as part of candidature for any other degree.

I also certify that the thesis has been written by me and that any help that I have received in preparing this thesis, and all sources used, have been acknowledged in this thesis.

Signature of Author

Acknowledgements

I am greatly indebted to my supervisor, Xiangjian He for his continuous encourgement, advice, help and invaluable suggestions. He is such a nice, generous, helpful and kindhearted person. I feel really happy, comfortable and unconstrained with him during my PhD study. I owe my research achievements to his experienced supervision. Many thanks are also due to my co-supervisors, Priyadarsi Nanda and Ren Ping Liu for their valued suggestions and constant support, and for the numerous conversations with them. I gratefully acknowledge the useful discussions with Aruna Jamdagni and Qiang Wu. I appreciate the travel support for attending the international conferences which I received from the Faculty of Engineering and IT and the Vice-Chancellor's Conference Fund. I wish to thank my fellow research students and the staff of the school, especially those people listed below for providing various assistance for the completion of this research work.

- Wenjing Jia, Min Xu, Yida Xu, Massimo Piccardi, Doan B. Hoang, Mao Lin Huang, Valerie Gay, Jinjun Chen, Karla Felix Navarro, Ruo Du, Cao Zeng, Sheng Wang, Muhammad Abul Hasan, Man To Wang, Mohammed Ambu Saidi, Ava Bargi, Thawatchai Chomsiri, Mian Ahmad Jan, Yi Wan and Minqi Li.

I would like to thank my wife, Shanshan, for her understanding and assistance. I also thank my parents for the freedom to study for the long time necessary to complete postgraduate studies. This thesis could not have been completed without the support and encouragement of my mother-in-law. My special thanks go to my best friends, Ming Deng and Susan Lai for their continuous care and wishes.

Last but not least, the financial assistance of a University of Technology Sydney International Research Scholarship and a CSIRO ICT Centre Top-up Scholarship is gratefully appreciated.

To My Family

Table of Contents

List of Tables

List of Figures

Abbreviation

Abbreviations	**Descriptions**
ABC	Association Based Classification
ANN	Artificial Neural Networks
AR	Auto-regression
BF	Basic Feasible
bPDM	bivariate Parametric Detection Mechanism
CAT	Change Aggregation Trees
CIDS	Collaborative Intrusion Detection System
CPM	Change-Point Monitoring
CUSUM	Cumulative Sum
DEMD	Differential Earth Mover's Distance
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
DR	Detection Rate
EDM	Euclidean Distance Map
EMD	Earth Mover's Distance
EMD-L_1	EMD with L_1 distance
FPR	False Positive Rate
FNR	False Negative Rate
FN	False Negative
FP	False Positive
GDI	Global Defence Infrastructure

Abbreviations	**Descriptions**
GSAD	Geometrical Structure Anomaly Model
ISP	Internet Service Provider
LDA	Linear Discriminant Analysis
LDSes	Local Detection Systems
LP	Linear Programming
MARS	Multivariate Adaptive Regression Splines
MCA	Multivariate Correlation Analysis
MD	Mahalanobis Distance
MDM	Mahalanobis Distance Map
MIB	Management Information Based
PCA	Principal Component Analysis
PoD	Ping of Death
RBFNN	Radial Basis Function Neural Networks
RePIDS	Real-time Payload-based IDS
ROC	Receiver Operating Characteristic
TAM	Triangle Area Map
TCB	Transmission Control Block
TCP	Transmission Control Protocol
TNR	True Negative Rate
TN	True Negative
TP	True Positive
SIP	Secure Infrastructure Protocol
SNMP	Simple Network Management Protocol
SPRT	Sequential Probability Ratio Test
SVM	Support Vector Machine
UDP	User Diagram Protocol
ICMP	Inter Control Message Protocol

Abstract

A Denial-of-Service (DoS) attack is an intrusive attempt, which aims to force a designated resource (e.g., network bandwidth, processor time or memory) to be unavailable to its intended users. This attack is launched either by deliberately exploiting system vulnerabilities of a victim (e.g., a host, a router, or an entire network) or by flooding a victim with large volume of useless network traffic. Since 1990s, DoS attacks have emerged as a type of the most severe network intrusive behaviours and have posed serious threats to the infrastructures of computer networks and various network-based services.

This thesis aims to provide an intelligent and effective solution for DoS attack detection. Unlike the related works based on machine learning and statistical analysis, this thesis suggests to treat network traffic records as images and to redefine the DoS attack detection problem as a computer vision task.

To achieve the aforementioned objectives, this thesis first conducts a detailed literature review on the state of the art in DoS attack detection. Then, it analyses and chooses the most appropriate mechanisms for DoS attack detection. Afterwards, it designs a general system framework for DoS attack detection with respect to the chosen mechanisms. Furthermore, two Multivariate Correlation Analysis (MCA) approaches are proposed based on two techniques, namely Euclidean distance and triangle area.

These two proposed MCA approaches provide accurate description for network traffic records and facilitate conversion of network traffic into the respective images.

In addition, this thesis proposes a DoS attack detection system, in which the images of network traffic are served as the observed objects and the task of DoS attack detection is reformulated as a computer vision problem, namely image retrieval. This proposed DoS attack detection system applies a widely used dissimilarity measure, namely the Earth Mover's Distance (EMD), to object classification. The EMD takes cross-bin matching into account and provides a more accurate evaluation on the dissimilarity between distributions than some other well-known dissimilarity measures, such as Minkowski-form distance L_p and X^2 statistics. The merits of the EMD facilitate the capability of our proposed system with effective detection.

Last but not least, our intelligent and effective solutions, including the two proposed MCA approaches and the EMD-based DoS attack detection system, are evaluated using the KDD Cup 99 dataset. The evaluation results illustrate that our proposed MCA approaches provide accurate characterisation for network traffic, and the proposed detection system can detect unknown DoS attacks and outperforms two state-of-the-art approaches.

Papers from the Thesis

Papers Appearing in LNCS Series

[1] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, Multivariate Correlation Analysis Technique Based on Euclidean Distance Map for Network Traffic Characterization, Information and Communications Security, LNCS, Vol.

7043/2011, pp.388-398. Springer Berlin Heidelberg New York. ISBN: 978-3-642-25242-6.

[2] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis. Neural Information Processing, LNCS, Part 3, Vol. 7064/2011, pp.756-765. Springer Berlin Heidelberg New York. ISBN: 978-3-642-24964-8.

[3] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, W. Jia, W. Yeh, A Two-tier System for Web Attack Detection Using Linear Discriminant Method, Information and Communications Security, LNCS, Vol. 6476/2010, pp.459-471. Springer Berlin Heidelberg New York. ISBN: 978-3-642-17649-4.

Refereed Journal Articles

[4] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, Detection of Denial-of-Service Attacks Based on Computer Vision Techniques, IEEE/ACM Transactions on Networking (IEEE/ACM ToN), Submitted for review on 25th May 2013.

[5] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis, IEEE Transactions on Parallel and Distributed Systems (IEEE TPDS), Available online, 03/05/2013. DOI: 10.1109/TPDS.2013.146.

[6] A. Jamdagni, Zhiyuan Tan, P. Nanda, X. He, R. Liu, RePIDS: A Multi Tier Real-Time Payload-Based Intrusion Detection System, Computer Networks, 57(3) 2013, pp. 811-824. ISSN: 1389-1286. DOI: 10.1016/j.comnet.2012.10.002.

[7] A. Jamdagni, Zhiyuan Tan, P. Nanda, X. He, R. Liu, Mahalanobis Distance Map Approach for Anomaly Detection of Web-based Attacks, Journal of Network Forensics, Volume 2 Issue 2, 2010, pp.25-39.

Refereed Conference Papers

[8] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, Evaluation on Multivariate Correlation Analysis Based Denial-of-Service Attack Detection System, 1st International Conference on Security of Internet of Things (SecurIT 2012), Kerala, India, 17-19 August, 2012.

[9] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, Triangle-Area-Based Multivariate Correlation Analysis for Effective Denial-of-Service Attack Detection, 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2012), Liverpool, UK, 25-27 June 2012.

[10] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, Network Intrusion Detection Based on LDA for Payload Feature Selection, IEEE Globecom 2010 Workshop on Web and Pervasive Security (WPS 2010), Miami, USA, December 6 - 10, 2010, pp.1590-1594. IEEE Communication Society.

[11] A. Jamdagni, Zhiyuan Tan, P. Nanda, X. He, R. Liu, Mahalanobis Distance Map Approach for Anomaly Detection of Web-based Attacks, The 8th Australian Information Security Management Conference, Perth, Australia, November 30 - December 2, 2010, pp.8-17.

[12] A. Jamdagni, Zhiyuan Tan, R. Liu; P. Nanda, X. He, Pattern Recognition Approach for Anomaly Detection of Web-based Attacks, The proceedings of

the seventh annual CSIRO ICT Centre Science and Engineering Conference, CSIRO, Australia, November, 2010.

[13] A. Jamdagni, Zhiyuan Tan, P. Nanda, X. He, R. Liu, Intrusion Detection Using GSAD Model for HTTP Traffic on Web Services, 6th International Wireless Communications and Mobile Computing Conference (IWCMC 2010), Caen, France, June 28 July 2, 2010, pp. 1193-1197. ACM.

[14] A. Jamdagni, Zhiyuan Tan, P. Nanda, X. He, R. Liu, Intrusion Detection Using Geometrical Structures, 4th International Conference on Frontier of Computer Science and Technology (FCST 2009), Shanghai, China, December 17-19, 2009, pp. 327 - 333. IEEE Computer Society.

[15] A. Jamdagni, Zhiyuan Tan, R. Liu; P. Nanda, X. He, A Frame Work for Geometrical Structure Anomaly Detection Model, The proceedings of the sixth annual CSIRO ICT Centre Science and Engineering Conference, CSIRO, Australia, November 11, 2009.

Other Publications

[16] Zhiyuan Tan, Linear Discriminant Analysis Based Feature Selection for Network Intrusion Detection, UTS: FEIT Research Showcase 2010, University of Technology Sydney, Australia, June 2, 2010

Chapter 1

Introduction

This thesis considers the application of statistical and computer vision techniques to DoS attack detection, and attempts to reformulate the task of DoS attack detection as a computer vision problem. Section 1.1 outlines the background and motivation for the work presented in this thesis. The research objectives are discussed in Section 1.2. The contributions and novelty of the work are discussed in Section 1.3, followed by an outline of the structure of the remainder of the thesis in Section 1.4.

1.1 Background and Motivation

Computer networks have become a key component of the infrastructure of today's human society. They support our daily life in different aspects from governing, personal social networking to business. According to the recent statistics from Australian Bureau of Statistics, 13.3 million people in Australia were reported accessing the Internet at home in the period between 2010 and 2011 [70]. The top three activities of Internet users were (1) emailing, (2) research, news and general browsing, and (3) paying bills online or online banking. The Internet users performing these activities accounted for 91%, 87% and 64% of the population respectively. Additionally, online shopping expenditure in Australia reached \$13.6 billion in 2011, and it is predicted to be worth \$26.9 billion by 2016 [3].

Thus, as a growing popular communication platform, computer networks have been targeted by cyber criminals, whose attacks to online business and transaction systems are becoming widespread and more sophisticated. As such, network security is becoming increasingly critical. DoS attacks have emerged as one of the most severe network intrusive behaviours and have posed serious threats to the infrastructures of computer networks and various network-based services. DoS was first documented in [68] in 1986 as causing a series of congestion collapses on the Internet. Billions of dollars loss was imputed to DoS attacks over the past few years [36].

1.1.1 Denial-of-Service Attack Mechanisms

DoS attacks can be launched by deliberately exploiting system vulnerabilities of a victim (e.g., a host, a router or an entire network) or flooding a victim with a large volume of useless network traffic to occupy the designated resources (e.g., network bandwidth, processor time or memory).

DoS attacks result in a serious interruption to a victim. They not only violate the availability of systems, but also have close relationships with the breaches of confidentiality and integrity [106]. For example, some DoS attacks are launched from compromised machines (breach of confidentiality) [19], and some use spoofed (forged) source addresses (breach of integrity) [6].

Exploitation of System Vulnerability

System vulnerability has been a common problem in computer software development, since computer systems evolved to be more complex and required to deal with complicated tasks. The collaboration between different components within an operating system or between an application and an operating system needs thoughtful coordination. This causes serious challenges to the implementation of operating systems, applications and protocols. For instance, system vulnerability (bugs) which is unintentionally introduced into computer systems due to the carelessness in design. These bugs leave loopholes that could be exploited to either compromise or deny service to a computer system.

The defects in the implementation of the TCP/IP protocol suit have claimed as the victims of many DoS attacks. The summarisation of some of the notorious instances of such attacks are given as follows.

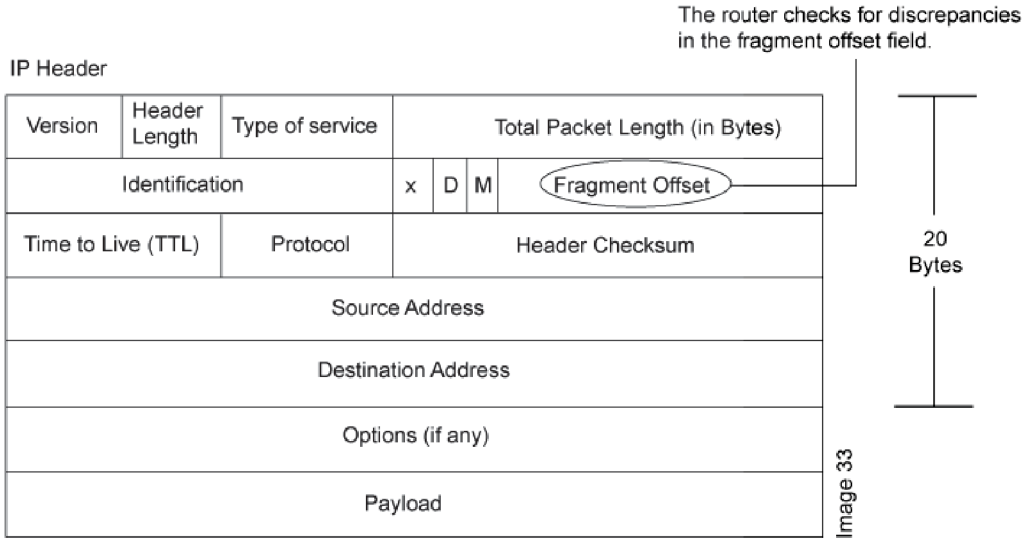


Figure 1.1: IP fragment structure [50]

Teardrop is a DoS attack exploiting the vulnerability in IP fragmentation reassembly [15], which often can be found on older operating systems such as Windows 3.1x, Windows 95, Windows NT and versions of the Linux kernel prior to 2.1.63. Overlapping IP fragments are sent by an attacker to a target machine connecting to the Internet or a network. As shown in Fig. 1.1, the fragment offset field in the header of each IP fragment indicates the relative starting position of its data in the data carried by the original unfragmented packet.

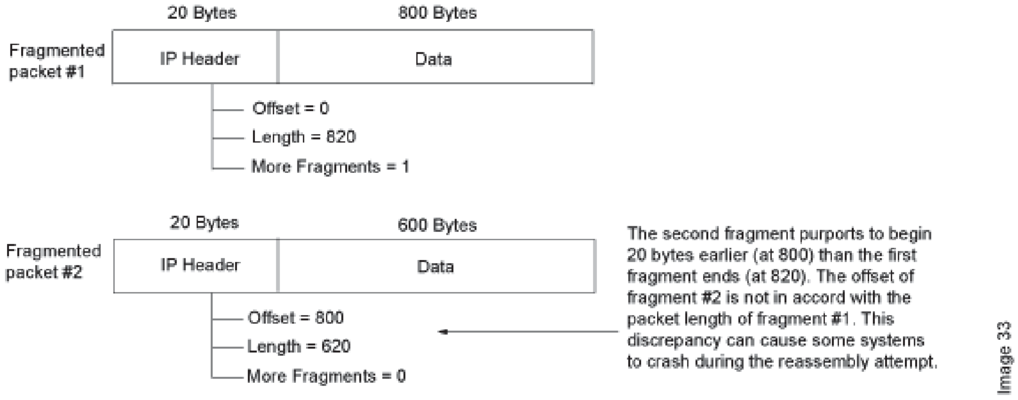

20 Bytes
800 Bytes
Fragmented packet #1
IP Header
Data
Offset = 0
Length = 820
More Fragments = 1
20 Bytes
600 Bytes
Fragmented packet #2
IP Header
Data
Offset = 800
Length = 620
More Fragments = 0
The second fragment purports to begin 20 bytes earlier (at 800) than the first fragment ends (at 820). The offset of fragment #2 is not in accord with the packet length of fragment #1. This discrepancy can cause some systems to crash during the reassembly attempt.
Image 33

Figure 1.2: An example of overlapping IP fragments [50]

The overlapping IP fragments appear discrepancies in the field of fragment offset, in which the sum of the offset and the length of an IP fragment is found different from the offset of the next IP fragment as shown in Fig. 1.2. Due to the incapability in properly reassembling the overlapping IP fragments, the target machine is trapped into malfunction and required a simple reboot to restore itself to normal. This results in a service denial.

Land attack [15] intends to cause denial-of-service on a target machine through the exploitation of another vulnerability in the faulty implementations of TCP/IP protocol suit on some operating systems, such as Windows 95/NT and various flavors of UNIX. This bug makes the target machine vulnerable to a crafted anomaly TCP SYN packet, where the source IP address and the source port number are intentionally set as identical to the destination IP address and the port number. Sending this crafted anomaly TCP SYN packet could bring down the victim.

Ping of Death (PoD) is another DoS attack, which also takes advantage of the careless implementation of IP fragmentation reassembly [14]. An oversize IP packet with data larger than 65,535 bytes is sent to the target machine. The fragments of this oversize IP packet reach the victim machine over networks and need reassembling. However, the vulnerable machine cannot reassemble the packet and suffers from an unwanted crash or reboot. The PoD attack can be easily achieved using the ping application bundled with any operating system, such as ICMP ECHO request.

Although more new vulnerabilities have been discovered in software applications, system level vulnerabilities are still the favours of the cyber attackers. They are keen to gain privilege access to sensitive information, or to take control over the victims by exploiting these system level vulnerabilities.

Network Flooding to Connected Systems

In comparison with exploitation of vulnerability which can be prevented by patching the system vulnerability, flooding-based DoS attacks are difficult to be handled. This issue is caused by the underlying mechanisms of computer networks, which specify that connected devices need to process any network traffic addressed to them. These underlying mechanisms assure the functionality of computer networks but simultaneously expose the devices to flooding-based DoS attacks. Moreover, in today's

Internet, attack toolkits are readily available and easy to use. Any Internet user can use these toolkits to launch attacks with minimum efforts. Sometimes, the users of the attack toolkits may not even have any knowledge about network security. Some of the common flooding-based DoS attacks are briefly introduced below.

UDP flood is a simple DoS attack, which needs not exploit any vulnerability on a target machine and is achieved by purely sending a overwhelming number of UDP packets with spoofed source IP addresses to random ports on the victim [12]. This, however, does not bring down the target machine straightforward but keeps it busy with the following routine instead. This routine first checks for the application listening at the port to which the UDP request addressed. If the port is not being listened by any application, a reply with an ICMP Destination Unreachable packet will be sent. The UDP flood ensures that the victim is fully occupied by the excessive spoofed UDP requests and not reachable to other legitimate network participants.

ICMP flood adopts a similar attack mechanism and presents alike behaviour to the UDP flood [49]. Basically, a flood of ICMP ECHO packets is generated and destined to a victim machine. The amount of the ICMP ECHO packets significantly exceed the resources (e.g., CPU and network resources) of the victim available to make full responses. Smurf attack is one of the notorious instances of ICMP flood [16].

TCP flood is a kind of DoS attacks taking advantage of the imperfect implementation of TCP protocol. A famous instance of TCP flood, which is also known as TCP SYN flood, exploits the vulnerability in the three-way handshake process [13]. To understand the TCP SYN flood, it is necessary to be clear about the normal three-way handshake process. The process of the three-way handshake during the initialisation of a TCP connection is detailed below.

1) The client needs to send a TCP SYN packet to the server for requesting some service.

2) Upon the receipt of the SYN packet, the server allocates a Transmission Control Block (TCB) to hold all the information about this connection and acknowledges the client with a SYN-ACK packet.

3) Then, the client finishes the establishment of the connection with a ACK packet sent to the server and meanwhile a TCB is allocated to contain the information of the connection.

Upon completion, the connection is fully open. The service-specific data can be exchanged between the client and the server.

However, this process is vulnerable. It could be exploited by attackers to create half-open connections, which refer to a state after a SYN-ACK packet has been sent by the server but the ACK packet is not yet received, so that the allocated buffer is on hold until one of the following conditions is satisfied.

1) The client sends a ACK packet;

2) Closing the connection by sending a RST packet;

3) A timeout occurs and the server automatically closes the connection.

To cause denial of service on the server by exploiting this vulnerability, an attacker force a server to generate an excessive number of half-open connections, which results in no more resource available for other legitimate TCP connection requests. Neptune attack is one of well-known TCP SYN flood attacks [20]. Similarly, TCP RST attack and TCP ACK attack [2] are feasible and are easy to perpetrate as a UDP flooding attack.

1.1.2 Denial-of-Service Attack Framework

Generally, any intrusive activities that cause denial of access by legitimate users to shared services or resources can be defined as DoS attacks [34]. Frameworks used to launch these attacks are categorised into single source DoS attack framework and Distributed DoS (DDoS) attack framework in accordance with the number of attack sources involved in a single attempt.

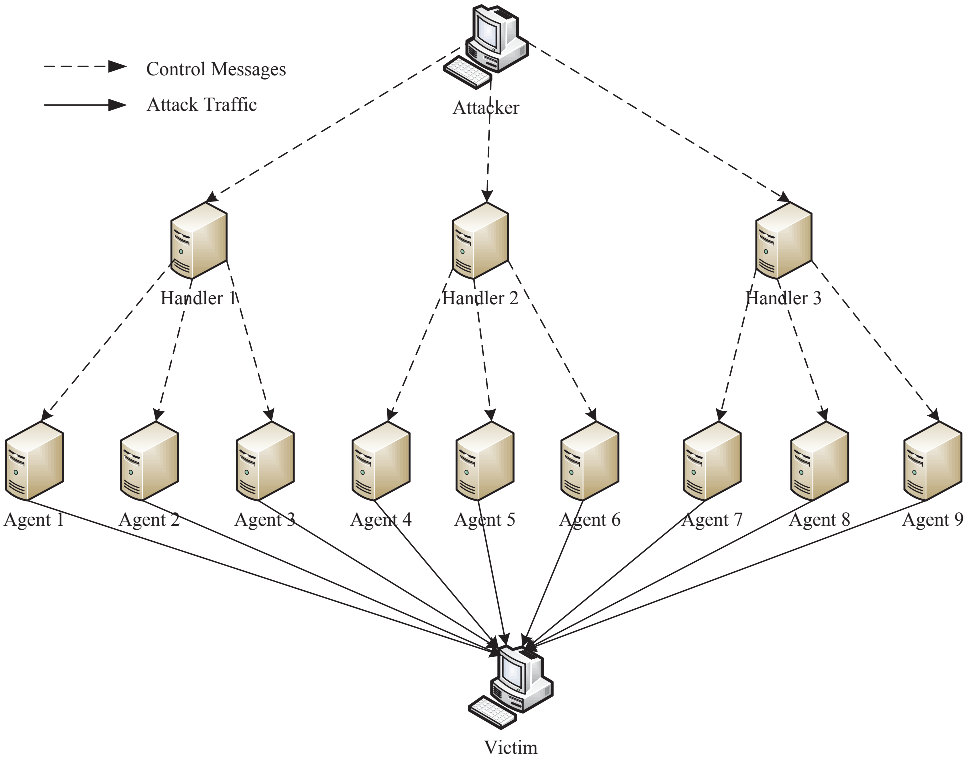


Figure 1.3: Typical architecture of a DDoS attack

An attack based on the former framework has all traffic generated from one single source. To ensure the success of this attack, the volume of attack traffic generated by the source must exceed the range that a victim is capable of processing, especially in the case of flooding-based DoS attacks.

The DDoS attack framework, by contrast, suggests a more sophisticated means to amplify the impact of an attack on a victim. Instead of requiring a single high-end machine, a collaborative attack network is recruited and used by an intruder to launch an attack. In this scenario, the attack traffic coming from multiple sources is directed to the same victim. This sophisticated attack scheme helps the real attacker hide from being traced and makes defence become more complicated.

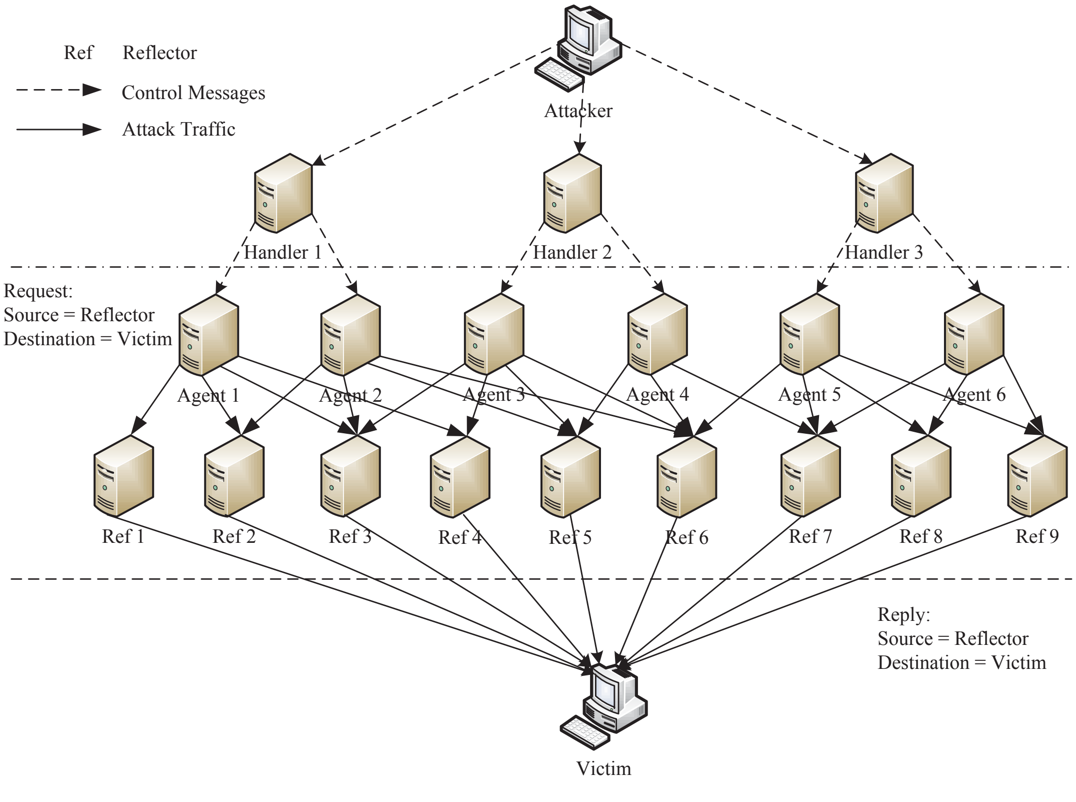


Figure 1.4: Architecture of a DDoS attack using reflectors

DDoS attacks can be coordinated in two different distributed fashions. The architecture shown in Fig. 1.3 illustrates the first method, where the attacker sends control messages through handlers to instruct the previously compromised agents to generate and send attack traffic to the victim [26]. The second architecture shown in Fig. 1.4 presents a more sophisticated method, namely a reflective DDoS attack. Similar to a typical DDoS attack, a reflective DDoS attack also requires the involvement of a number of handlers and agents. However, the agents in this architecture do not send attack traffic to the victim directly. The agents are commanded to issue spoofing requests to a number of reflectors instead. These requests fools the reflectors to believe they were from the victim. The reflectors are some normal hosts on the Internet and reply the victim with legitimate responses. The victim is then overwhelmed by this flood of requests. The attack sources can even hide themselves better by using this method because reflectors are in use [73].

1.1.3 Schemes of Defence

In recent years, a significant number of works have concentrated on building systems for defending DoS attacks. However, there are obvious imperfections within the traditional network security paradigms, which rely on simple packet filtering or alerting the system while the program is in execution [85]. Many new defence mechanisms have been proposed, such as detection, prevention, mitigation and response [25]. Within the realm of a set of network security schemes, detection is playing an increasingly important role and is the very first step to protect against DoS attacks among the aforementioned defence mechanisms. Detection systems are required to provide prompt reaction and high detection accuracy.

In general, detection mechanisms can be divided into two major categories, namely misuse-based detection and anomaly-based detection. Misuse-based detection mechanism employs signature or rule matching in its recognition of intrusive behaviours. Misuse-based detection systems [4][9][47][72][76] can achieve high detection rates in known attacks. However, they are incapable of detecting any unknown malicious behaviours or even variants of existing attacks. Furthermore, generating signatures for previously unseen attacks is an expensive and complicated labour intensive task, which heavily involves network security expertise.

Research community, therefore, started to explore a way to achieve novelty-tolerant detection systems and developed a more advanced concept, namely anomaly-based detection. Anomaly-based detection uses a different detection methodology that monitors and labels any network activities presenting significant deviation from the respective legitimate traffic profiles as suspicious objects. Since these profiles are built based on the knowledge of normal network behaviours, anomaly-based detection systems are able to identify zero-day intrusions that exploit previously unknown system vulnerabilities [21]. Moreover, it is not constrained by the expertise in network security, due to the fact that the profiles of legitimate behaviours are developed using techniques, such as machine learning [42][55][86][107] and statistical analysis [17][96].

Over the recent two decades, a variety of anomaly-based detection systems have been proposed to defence DoS attacks. A significant number of anomaly-based detection systems have adopted the network-based detection mechanisms, which advocate monitoring of network traffic transmitting over the protected networks. These mechanisms release the protected online servers from monitoring attacks and ensure that the servers can dedicate themselves to provide quality services with minimum delay in response. Moreover, network-based detection systems are loosely coupled with operating systems running on the host machines which they are protecting. As a result, the configurations of network-based detection systems are less complicated than those of host-based detection systems.

However, the existing systems [71] are usually ineffective in prompt detection because of the nature of computationally expensive underlying techniques and the overhead of data pre-processing. In addition, these systems also commonly suffer from high false positive rates. This is partly because most of these systems only use several simple network features of incoming traffic (e.g., IP header fields) in their detection, and ignore the correlations between the network features [80].

Although there is a current research trend to make use of the correlations between the features in intrusion detection, most of the proposed systems [48][97][98][108] are based on traditional statistical correlation analysis techniques, such as covariance coefficient and covariance matrix, which are only capable of studying the correlations between the features (variables) in a given sample set. The properties inherited from these traditional statistical correlation analysis techniques make these anomaly-based detection systems incapable of recognising individual attack records hidden in a sample set. Thus, to develop anomaly-based attack detection systems, which overcome the aforementioned problems and withstand the previously discussed issues, is one of the current research focuses.

1.2 Objectives

This thesis focuses on the research of network traffic characterisation and classification, and aims to provide an innovative scheme for securing computer networks. The detailed objectives are shown as follows.

1) Propose approaches that contribute effective and accurate analysis to various types of network traffic;

2) Provide means, which are independent to prior knowledge, to extract highly discriminative features for network traffic classification;

3) Develop methods that can identify individual attack records in a set of mixed network traffic;

4) Design a network intrusion detection system that achieves high detection accuracy and withstands zero-day attacks.

5) Suggest an innovative fusion between intrusion detection and computer vision techniques

1.3 Contribution and Novelty

A more sophisticated security scheme for protecting computer networks from being compromised by DoS attacks is proposed in this thesis. The proposed security scheme is designed from the perspective of computer vision. The contributions and novelty of the proposed scheme are given as follows.

1) This thesis propose two unique MCA approaches to effectively extract the correlations between features within network traffic records with the following properties:

- The proposed MCA approaches withstand the problem that features are changed linearly,
- They do not require any prior knowledge of network traffic in the process of analysis, and
- They supply with accurate characterisation to network traffic.

2) Individual attack records hidden in the crowd can be easily recognised by our system. This is owing to one of the merits (i.e., the capability of analysing correlation between features within individual records) of our MCA approaches which equips the analysis of correlation being conducted on individual network traffic records.

3) The task of DoS attack detection is innovatively reformulated as a computer vision problem, such as image retrieval or object shape recognition. This is motivated by the commonalities shared between the two problems. The reformulation provides us a perceptual solution to achieve accurate detection on DoS attacks.

4) The EMD [61] (a robust distance metric supporting full and partial matchings) is used as a dissimilarity measure for intrusion detection. This may be the first attempt to apply EMD in field of network DoS attack detection.

1.4 Structure

The rest of this thesis is organised as follows. A review of prior research works on anomaly-based detection and EMD is conducted in **Chapter 2**. **Chapter 3** proposes a general system framework for DoS attack detection, and a mathematical derivation is conducted in this chapter to prove that sample-by-sample detection mechanism is advanced over group-based detection mechanism in terms of detection accuracy. **Chapter 4** proposes a novel MCA approach based on Euclidean Distance Map (EDM) technique, and a network intrusion detection system is proposed using the proposed EDM-based MCA approach. In **Chapter 5**, a different MCA approach is suggested based on Triangle Area Map (TAM) technique, and it helps extract multivariate correlations from a perspective that is different than the EDM. Then, a network intrusion detection system based on the TAM-based MCA approach is proposed in **Chapter 5** as well. **Chapter 6** presents an innovative DoS attack detection system based on computer vision techniques, where the EMD is used for measuring the dissimilarity between legitimate network traffic and DoS attack traffic. Finally, summary and future work are drawn together with the thesis conclusion in **Chapter 7**.

Chapter 2

Related Works

A literature review is conducted in this chapter to give an overview of the state-of-the-art algorithms for DoS attack detection. Section 2.1 summarises the general detection mechanisms for DoS attacks. The major related works on network anomaly-based DoS attack detection are recapped in Section 2.2. Finally, EMD and its applications in network security research area are introduced in Section 2.3.

2.1 DoS Attack Detection

This section aims to deliver an overview of the security schemes those are designed for the detection of DoS attacks. These security schemes can be categorised in accordance with the detection method used in a security scheme and the location of audit source, as suggested by the taxonomy introduced in [54]. The characteristics of different detection schemes with respective to the detection method, the location of audit source and the defence framework are discussed in Section 2.1.1 Section 2.1.2 and Section 2.1.3 respectively.

2.1.1 Detection Method

Detection methods adopted in DoS attack detection systems are commonly classified as misuse-based detection and anomaly-based detection [56][60].

Misuse-based Detection

Misuse-based detection attempts to detect attacks by monitoring network activities and looking for matches with the existing attack signatures or rules [4][9][44][47][72]. According to Gollman [35], the applications of misuse-based detection in commercial intrusion detection systems have received much success. In spite of having high detection rates to known attacks and low false positive rates, systems using misuse-based detection methods are easily evaded by any new attacks and even variants of the existing attacks. Furthermore, it is a complicated and labour intensive task to keep signature database updated because signature generation is a manual process and heavily involves network security expertise.

Anomaly-based Detection

Anomaly-based detection, in contrast, attempts to study the feature patterns of normal behaviours, It monitors and flags observed events, whose feature patterns presenting significant deviation from the learnt profiles of normal behaviours, as suspicious objects. Anomaly-based detection shows more promising performance in detecting zero-day intrusions that exploit previous unknown system vulnerabilities [21]. Moreover, it is not constrained by the expertise in network security, due to the fact that the profiles of legitimate behaviours are developed based on techniques, such as machine learning [42][55][86][107] and statistical analysis [17][96]. However, these proposed systems are prone to issue false positives [54]. This defect is primarily caused by the problem that all previously unseen behaviours including legitimate behaviours are considered to be anomalies.

Despite these methods show limitations in different aspects, anomaly-based detection is more encouraging for the evolving network environment. This is because the profiles equipped in an anomaly-based detection system are built on the knowledge of normal behaviours, which facilitates the detection of previously unknown attacks. This, in turn, helps reduce the costs of generating signatures for new emerging attacks or variants.

2.1.2 Audit Source Location

Regardless of the use of detection method in an attack detection system, it can operate either on host level or on network level [1].

Host-based Attack Detection Systems

A host-based attack detection approach monitors various system level behaviours on a host machine. It investigates the system status and system logs to determine occurrence of violations or unauthorised access to system files [1]. However, host-based detection is not suitable for monitoring network activities that may be part of an attack process on the host machine, and has to take different operating systems into account.

Network-based Attack Detection Systems

In terms of network-based detection, network traffic instead of system status and logs are analysed during detection. Network-based detection has been a trend over the recent decade [51], and releases the protected online servers from monitoring attacks and ensures that the servers can dedicate themselves to provide quality services with minimum delay in response. Moreover, network-based detection is loosely coupled with operating systems running on the host machines which they are protecting. As a result, the configurations of network-based detection systems are less complicated than those of host-based detection systems.

Thus, network-based detection is a better choice than host-based scheme for the task of DoS attack detection.

2.1.3 Detection Framework

A detection framework defines the deployment of a DoS attack detection system in a network. In general, DoS detection frameworks can be divided into three categories, namely source-end detection framework, victim-end detection framework and distributed detection framework. The characteristics of these frameworks and some instances are introduced in the subsequent sections.

Source-end Detection

The source-end detection framework attempts to facilitate early response to attacks before they cause interruptions to victims. This is achieved by deliberately deploying detection units as close to the attack sources as possible. In the meanwhile, this detection mechanism brings a few benefits to network Quality-of-Service (QoS) control [65], such as enabling more effective congestion control and multiple-level detection strategies.

D-WARD [65] is a typical source-end Distributed DoS (DDoS) defence system. It handles DDoS attacks using TCP, UDP or ICMP protocol. D-WARD determines the occurrence of attacks by comparing the statistics (gathered at the aggregate flow and connection granularity within each observation interval) against the corresponding legitimate traffic model (i.e., TCP, UDP or ICMP model) at source end. However, UDP protocol provides best effort delivery, where no acknowledgement of receipt is required. As a result, no response packet from the victim is available for D-WARD to build an accurate UDP model.

Kim and Reddy [52] suggested a statistical-based approach to detect anomalies at an egress router. This approach conducts time series analysis on various packet header data in real-time and applies a discrete wavelet-based method to transform address correlation data (i.e., the correlation of destination IP addresses, port numbers and the number of flows). The evaluation results [52] show that it achieves higher efficiency in detecting DDoS attacks than those schemes based on the analysis of traffic volume. Although wavelet-based methods enable detection decisions to be made in relatively short time, larger computational resources are needed to achieve this.

By way of conclusion, the source-end detection framework has made a good attempt to provide quick responses to DoS attacks. However, it is not the most effective means in comparison with the victim-end framework because more comprehensive information of attack traffic is available at the victim end [62].

Victim-end Detection

As a conventional framework, the victim-end detection has been embraced in most existing detection systems because more accurate attack information is available at the victim end, and a victim receives more direct benefits from having a detection system installed in comparison with a source [30][103]. However, under extremely aggressive DDoS attacks, victim-end detection systems can hardly help administrators make effective responses in time because the attacks have already been at doorstep.

Traffic Rate Analysis (TRA) system [69] is a typical victim-end DoS detection system. In [69], three machine learning techniques, namely C4.5, CN2 and a Bayesian classifier, were used by TRA to analyse network traffic. The relative occurrence rates of various types of flags (i.e., SYN, FIN, RST, ACK, PSH and URG flags) in TCP packet headers and the relative occurrence rates of different protocols (i.e., TCP, UDP or ICMP) were computed for a given sampling period and studied to differentiate legitimate network traffic from DoS attack traffic. The experimental results shown in [69] illustrate that the combination of the SYN and ACK flag rates for inbound traffic and the Bayesian Classifier provides the best performance for detecting SYN flooding attacks.

Li [59] proposed a detection scheme based on the autocorrelation function of inbound network traffic. In this scheme, network traffic is modelled using Fractional Gaussian Noise (FGN), which provides approximation for autocorrelation functions of various types of traffic. The distance between an estimated autocorrelation function and the template autocorrelation function is used to determine whether or not the victim is under a DoS attack. However, existing research has cast doubt on FGN in modelling traffic in real-time traffic [99].

The schemes having been discussed above attempt to protect the victims against intrusions by running detection on incoming traffic. The detection performance could be further improved by introducing distributed or collaborative detection framework.

Distributed Detection

The distributed detection framework is discussed in this section. This framework allows individual detection systems/sensors to collaborate together and attempts to achieve better detection efficiency and accuracy.

A Global Defence Infrastructure (GDI) was proposed in [100]. Local Detection Systems (LDSes) were deployed at intermediate network devices, where most cross-domain traffic would transmit through. Packet counts of different types of traffic (i.e., TCP data, UDP data, ICMP data, TCP SYN segments and TCP RST segments) for a given attack detection interval on a LDS were used to signal DoS attacks. An alert would be raised in the LDS if the current packet count of a certain type of traffic for an address slot (to which might have more than one destination IP address assigned) was significantly greater than the all-time maximum packet count excluding the current one. The suspicious traffic would be confirmed as a DoS attack only if same alerts from other remote LDSes were received by the current LDS. However, the overhead of attack detection at intermediate network devices reduce the throughput of legitimate traffic. Furthermore, additional memory is needed at a LDS-enabled intermediate device to store relevant data structures.

Chen et al. [18] proposed a distributed DDoS attack detection system at traffic-flow level to detect abrupt traffic changes across multiple ISP domains. Internet routers or the gateways of edge networks were recruited to contribute to this distributed detection system. Each Internet Service Provider (ISP) domain had a Change Aggregation Trees (CAT) server deployed and to be responsible for aggregating the flooding alerts reported by the participant routers. These CAT servers in different ISP domains collaborated together to draw a complete picture of the protected portion of the Internet. The final detection decision was made based on this aggregated information. To secure the communication channels between participants and to establish mutual trust, a Secure Infrastructure Protocol (SIP) was proposed in [18]. The success of this distributed DDoS attack detection system is based on the collaboration among the different ISPs. However, this involves privacy issues and business interests of different ISPs.

Although the afore-discussed schemes have demonstrated the possibility of employing the distributed detection framework in DoS attack detection, many practical issues (e.g., communication overhead and data privacy) need to be taken into serious consideration.

2.2 Network Anomaly-based Detection

Anomaly-based detection shows promising results in detecting zero-day attacks [58] that exploit previously unknown system vulnerability, and it has less dependency on domain knowledge. Due to these unique merits, anomaly-based mechanism has been widely adopted in recent work on DoS attack detection. Techniques commonly used in these systems are machine learning and statistical analysis. To demonstrate how these techniques have been applied in network anomaly-based DoS attack detection, we conduct a review on some typical detection systems in this section.

Machine Learning

Machine Learning (ML) techniques help in classification of observed objects using known properties learnt from training data. Some exiting ML-based detection schemes are discussed in this section.

Clustering is one type of well-known ML techniques and features a unique capability of handling unlabelled data. Natural patterns in the data can be extracted using clustering techniques. This property makes them become one of the favourite types of techniques used in anomaly-based intrusion detection [28][38][75][83]. The work presented in [55] demonstrates a typical application of clustering techniques in DDoS attack detection. The authors proposed a detection approach based on hierarchical clustering method. The approach can detect different phases of a DDoS attack instance. However, the final detection accuracy of the approach is not revealed. Moreover, it is not clear how to correlate the clusters with the specific phases.

Fuzzy rules allow us to quantify the probabilities of the data belonging to various categories. Thus, IDS's reasoning is based on the degree of belonging instead of a crisp decision boundary [22][23]. Inspired by this merit, Tajbakhsh et al. [86] proposed two classification approaches, called Association Based Classification (ABC) and ABC extension. Models of different classes were described using fuzzy association rules. The ABC and the ABC extension were applied for misuse-based detection and anomaly-based detection respectively. Although results on known attacks are encouraging, they do not perform well in detecting unseen attacks.

Support Vector Machines (SVMs) [10] are supervised learning algorithms. They show promising in learning high-dimensional data [8]. Schölkopf et al. [81] proposed an unsupervised one-class SVM, which facilitates the application of SVM in anomaly-based intrusion detection. In 2008, Yu et al. [107] suggested a two-tier hierarchical detection system using SVM. The hierarchical structure and one-class SVM (i.e., Support Vector Data Description) equip it with the advantage in classifying various flooding-based attacks into their appropriate classes. Whereas, its detection accuracy can be improved if the correlation of the selected Simple Network Management Protocol (SNMP) Management Information Based (MIB) variables are taken into account.

Naïve Bayes (NB) is a simplified version of Bayesian networks. NB has been successfully applied to network based intrusion detection, such as the work presented in [74]. The authors of [74] conducted a study on Naïve Bayes with Kernel Estimation (NBKE). In comparison with the basic NB algorithm, NBKE has a better performance on the detection of flooding attacks and port scans. With a further improvement using the Hurst exponent [43] to measure traffic rate and port dispersion, a gentle rise in detection accuracy on UDP flooding attacks is shown.

Apart from those popular ML techniques we have discussed by far, other ML techniques have also been successfully applied to network intrusion detection. For example, a DoS attack detection approach proposed in [33] adopts a Radial Basis Function Neural Networks (RBFNN) detector in network traffic classification. The evaluation results suggest that the choice of sampling interval, input features, the number of hidden neurons and training data have a considerable impact on this approach. To ensure this detection approach can achieve a consistent performance, a feature selection method was proposed in [24]. The most appropriate features were chosen from the 44 initial statistical features using a genetic algorithm. It has been proven that the number of hidden neurons and the selection and mutation probabilities are the critical factors needed to be taken into consideration in the process of selection. Moreover, Mukkamala et al. [67] proposed an ensemble design of intrusion detection system, where Artificial Neural Networks (ANN), Support Vector Machines (SVM) and Multivariate Adaptive Regression Splines (MARS) techniques were used. The experimental results show that this system outperforms any of the individual techniques. However, the ensemble detection system involves time-consuming computation and cannot work in real-time. In addition, Hu et al. [42] proposed to use the AdaBoost algorithm [31] to build a strong classifier for network intrusion detection. The AdaBoost-based detection approach is proven to be of light weight in terms of computational complexity and to have low error rates.

However, the knowledge of normal traffic behaviour and the knowledge of attack traffic behaviour are essential in the construction of a strong classifier.

Statistical Analysis

Statistical analysis techniques have been employed to conduct investigation into attributes of network traffic packets and to determine a rationale threshold for discriminating attacks from the legitimate traffic.

In [29], Feinstein et al. proposed a DoS attack detection system, in which activity level and source address distribution were analysed at the victim end. This system grouped all inbound traffic flows into six clusters according to the destination addresses. Chi-square statistic was used to measure the dissimilarity between the activity level of each cluster and the expectation (i.e., a normal profile). A significant deviation from the expectation indicated the appearance of an intrusion.

Wang et al. [101] proposed a sequential Change-Point Monitoring (CPM) approach for the detection of DoS attacks. CPM monitors the change of ratio between the number of SYN packets and the number of SYN/ACK packets at the first-mile, and the change of ratio between the number of SYN packets and the number of FIN packets at the last-mile. A non-parametric Cumulative Sum (CUSUM) algorithm was used in the CPM to evaluate the significance of the changes of traffic patterns and to determine the appearance of DoS attacks. The CPM is more suitable for analysing a complex network environment. Whereas in [101], CPM was only tested using SYN flooding attacks. Moreover, its performance is possibly affected by network indiscipline.

Thatte et al. [96] developed a bivariate Parametric Detection Mechanism (bPDM) operating on aggregate traffic. bPDM applies the Sequential Probability Ratio Test (SPRT) on two aggregate traffic statistics (i.e., packet rate and packet size), and it alleges an anomaly only when a rise in the traffic volume is associated with a change in the distribution of packet-size. Whereas, bPDM may not capture smart attacks, which manage to vary both bit-rate and packet-size distribution.

Although the afore-discussed systems and approaches show innovative and promising in different aspects of attack detection, they still suffer from relatively high false positive rates. This is partly because they either neglect the dependency and correlation between features/attributes or do not manage to fully exploit the correlation [80]. Some recent studies attempt to cope with this problem by taking full advantage of the correlation in their designs.

Thottan and Ji [97] developed an abrupt change detection approach which employs statistical signal processing technique based on the Auto-Regression (AR) process. An operation matrix (A), which retains “the ensemble average of the two point spatial cross-correlation of the abnormality vectors estimated over a time interval T” [97], participated in the computation of the value of abnormality indicator. Although this detection approach has shown to be effective in detecting several network anomalies, it has significant delay in detection. In addition, it is still an open topic on how to manage features with various time granularities.

Jin et al. [48] proposed a statistical detection approach using covariance matrix to represent the multivariate correlation for sequential samples. Although the approach achieves good detection rates, it is vulnerable to attacks that linearly change all monitored features. Moreover, it can only label a group of observed samples as legitimate or attack traffic without distinguishing individual attack traffic records from the crowd.

Tsai and Lin [98] designed a new detection approach based on the nearest neighbours technique. The approach applied a triangle area based method to discover the correlation between observed objects and the cluster centroids pre-identified using the K-means algorithm. The extracted correlation was then used in the nearest neighbours algorithm for classification. Although this detection approach was carefully designed to be immune to the problem of linear changing features, the dependency on prior knowledge of anomalous behaviours dilutes its accuracy and reliability on correlation discovery.

In our previous works [45][90][93], mechanisms to overcome the above weaknesses were studied and the corresponding solutions were proposed. A multi-tier Real-time

Payload-based IDS (RePIDS) was proposed in [45], where a novel geometrical structure based analysis technique was deliberately designed for feature correlation extraction. Mahalanobis Distance Map (MDM) was used to reveal the correlation between packet payload features. In [90] and [93], we attempted to further extend RePIDS to be suitable for non-payload-based attacks and eliminate the restriction of the use of IDS on encrypted network traffic. Two MCA approaches proposed in [90] and [93] embrace two techniques (i.e., spatial Euclidean distance and triangle area respectively) in estimating the correlation between features. These two MCA approaches equip our proposed DoS attack detection systems with encouraging detection accuracy and higher efficiency.

Chapters 4 and 5 of this thesis are developed based on the works published in [90] and [93] respectively. However, the DoS attack detection systems proposed in these two works are based on Mahalanobis distance, which does not support partial matching. A more sophisticated distance metric, such as EMD, can enhance the performance of detection.

2.3 Earth Mover's Distance

EMD was originally proposed by Rubner et al. [77] as a cross-bin dissimilarity measure to evaluate the perceptual difference between two distributions. It was defined as the minimal cost of the transformation from one distribution to another. EMD supports partial matching and outperforms bin-by-bin distances in matching perceptual dissimilarity. This benefits from the extension of the concept of a distance from between corresponding elements to between the entire distributions, in which the ground distance reflects the notion of nearness between the elements in the distributions. Quantisation and other binning problems of histograms can be further avoided by taking the above ideas.

2.3.1 Earth Mover's Distance Approaches

A considerable amount of research interest on EMD has been raised by the early work [77][78] from Rubner et al., who adopted transportation problem [40] in modelling distribution comparison and suggested to compare the signatures of distributions rather than histograms. Due to the fact that signatures are usually compressed (clustered) versions of histograms, the computation time of the EMD can be reduced.

However, simplex algorithm [39], applied to solve the EMD, has a supercubic empirical time complexity in $\Omega(N^3) \cap O(N^4)$ for a signature with N elements, which mostly limits the applications of EMD to non-time-sensitive tasks. Grauman and Darrell [37] proposed a fast contour matching algorithm using an approximate EMD, which utilised embedding technique to accelerate the computational speed. Thus, the EMD between two sets of descriptive local features can be quickly computed in the complexity of $O(Nd \log(\triangle))$, where N is the number of features, d is their dimension, and $\triangle$ is the diameter of the feature space.

Moreover, Ling and Okada [61] suggested an alternative and fast version for the EMD in which L_1 distance was used as ground distance to compute the dissimilarity between histograms. An efficient tree-based algorithm was developed replacing the original simplex algorithm to solve the proposed EMD-L_1 in a more efficient fashion. It is shown in [61] that the EMD-L_1 has an average empirical complexity of $O(N^2)$ that is much less expensive in computation than the original EMD. The EMD-L_1 was applied to shape recognition and interest point matching.

Based on the same motivation that was to speed up the original EMD, the Differential Earth Mover's Distance (DEMD) was recently presented in [109]. The authors proposed to apply sensitivity analysis of the simplex algorithm to solve the EMD. The signatures of distributions were used to represent the interested objects in visual tracking.

Considering the efficiency and the scenarios for which the above approaches were proposed, the EMD-L_1 is believed to be the best candidate for our task.

2.3.2 Applications of Earth Mover's Distance in Network Security

EMD has been widely used to solve many problems in computer vision, such as image retrieval [77][78], contour matching [37], object shape recognition [61], interest point matching [61] and visual tracking [109] etc. It is still a new technique to computer and network security, and only a small amount of work based on EMD has been found in the literature.

In this part, some of the most closely related works on intrusive behaviour detection are introduced. For instance, an approach for phishing web page detection was presented in [32], where web pages were first converted into normalised images and then were described using signatures (i.e., features consisting of dominant colour category and the respective centroid coordinates). Visual similarities between a test web page and protected web pages were assessed using the EMD [78] between their image signatures. If the similarity between the tested web page and a particular protected web page exceeds the pre-defined threshold, the tested page is deemed as a phishing web page.

In [104], Yen and Reiter developed a test method to differentiate between Plotters (i.e., bots) and Traders (i.e., normal peers) on a Peer-to-Peer (P2P) network. The EMD [78] helped evaluate the similarity between the per-destination interstitial time distributions of hosts. Plotters normally showed similar patterns in distribution, but those of Traders tended to be far apart from each other. The hosts were then grouped into the clusters with respect to the similarity of their timing patterns.

Micarelli and Sansonetti proposed a case-based anomaly intrusion detection approach in [64]. This approach monitored the output parameters and the arguments of system calls (i.e., execve(), chmod(), chown(), exit(), open() and setuid()) revoked by instances of applications on a host. A signature (consisting of the centroids of the clusters of system calls and the corresponding weights) was used to represent an instance of an application. Then, the signature was compared with the case (represented by the signature of the generic instance of the same application) stored in the profile database using the EMD [78]. Behaviours of the system call sequences performing significantly non-compliant with the corresponding profiles inferred that attacks were underway.

Although the above studies have made contributions to the integration of the EMD and the respective detection approaches, none of the approaches has been designed particularly for DoS attack detection. Additionally, these studies employ the original EMD rather than any other enhanced versions. Thus, heavy computational complexity of the original EMD prevents them from being applied to prompt detection tasks.

Therefore, we innovatively employed the EMD in our work [89] submitted to

IEEE/ACM Transactions on Networking and provided a reliable solution for DoS attack detection. This solution takes the advantages of the EMD and reformulates the task of DoS attack detection as an image retrieval problem. Chapter 6 of this thesis is developed based on the work in [89].

2.4 Summary

This chapter has summarised the general detection mechanisms for DoS attacks, and has recapped the major related works on network anomaly-based DoS attack detection. EMD and its applications in network security tasks have been introduced in this chapter as well.

This chapter has also pointed out that network anomaly-based detection shows unique merits as follows.

- The protected online servers can be free from monitoring attacks and dedicate themselves to provide quality services with minimum delay in response.
- Network-based scheme is loosely coupled with operating systems running on the host machines which they are protecting, and
- Anomaly-based detection mechanism enables any detection system recognise previously unseen intrusions.

There merits make network anomaly-based detection and more suitable to be employed in future solutions for DoS attack detection. The review of EMD has revealed that the advanced version EMD (i.e., EMD-L_1) is the best candidate among the other variants of EMD introduced in Section 2.3.1 to be used for our task.

Chapter 3

A System Framework for Denial-of-Service Attack Detection

A general system framework for DoS attack detection is proposed and discussed in this chapter. This general system framework is developed based on one of our works published in [93]. This framework intends to address the problems and to achieve the objectives highlighted in Chapter 1 by employing various mechanisms to the design. These mechanisms are introduced in Section 3.1, and the general system framework is proposed in Section 3.2.

3.1 Detection Mechanisms

This section introduces the detection mechanisms (i.e., network traffic monitoring at destination network, attack detection based on individual traffic records, multivariate correlation analysis, anomaly-based intrusion detection and traffic classification based on computer vision techniques) involved in our proposed general system framework. The motivations and contributions of using these mechanisms in this general system framework are also highlighted.

3.1.1 Network Traffic Monitoring at Destination Network

Any detection systems based on our proposed framework are positioned at the peripheral of the networks where the protected servers reside. Moreover, these systems monitor ingress traffic to the network. This allows the detection systems to concentrate on relevant inbound traffic only and helps reduce data processing overheads. Monitoring and analysing ingress traffic at the destination networks also enable detectors to provide protection which is the best fit for the target networks because legitimate traffic profiles used by the detectors are developed for a smaller number of network services.

3.1.2 Attack Detection Based on Individual Traffic Records

The literature review shows that the sample-by-sample detection and the group-based detection are two common mechanisms used in intrusion detection systems. These two detection mechanisms conduct investigation for individual traffic records and for individual groups of the records respectively. Given an assumption that the samples in a test set are all from the same distribution (class), the group-based detection mechanism maintains a higher probability in classifying a set of sequential traffic records than the sample-by-sample detection mechanism [48]. However, this assumption does not hold in general scenarios, where attacks occur unpredictably and sequential samples hardly come from the same distributions.

Thus, the group-based detection mechanism is merely suitable to apply to limited scenarios. Comparatively, the sample-by-sample detection mechanism is believed to be advantageous over the group-based detection mechanism in general scenarios, because it is not bonded with the above assumption. To demonstrate the advantage of the sample-by-sample detection mechanism, mathematical analysis is conducted on both of these two detection mechanisms and a comparison between the expected detection precisions of the two mechanisms is made in the following sections.

Sample-by-sample Detection

The sample-by-sample detection suggests performing investigation on each single traffic record. This equips an attack detector with the capability of flagging attack traffic records individually. The precision of classification achieved by the sample-by-sample detection mechanism is analysed systematically in this section. The analysis is in compliance with a known assumption that traffic samples are independent and identically distributed [11, 48, 66].

Given legitimate traffic and illegitimate traffic are normally distributed, they follow distributions $X_1 \sim N(\mu_1, \sigma_1^2)$ and $X_2 \sim N(\mu_2, \sigma_2^2)$ respectively. The distributions of legitimate traffic and illegitimate traffic are depicted statistically using the probability density functions (3.1.1) and (3.1.2) respectively.

$$\begin{cases} f(x;\mu_1,\sigma_1^2) = (1/(\sigma_1\sqrt{2\pi}))e^{-(x-\mu_1)^2/2\sigma_1^2}, & (3.1.1) \\ f(x;\mu_2,\sigma_2^2) = (1/(\sigma_2\sqrt{2\pi}))e^{-(x-\mu_2)^2/2\sigma_2^2}, & (3.1.2) \end{cases}$$

where $x \in (-\infty, +\infty)$. Then, assume that there is a group of k independent samples $\{x_1, x_2, \cdots, x_k\}$, the probabilities of correctly classifying a sample into its distribution using the sample-by-sample detection mechanism are defined as the cumulative distribution functions shown in (3.1.3) and (3.1.4) respectively.

$$\begin{cases} P_1 = \displaystyle\int_{-\infty}^{\overline{\mu}} \frac{1}{\sigma_1\sqrt{2\pi}} e^{-(x-\mu_1)^2/2\sigma_1^2} dx, & (3.1.3) \\ P_2 = \displaystyle\int_{\overline{\mu}}^{+\infty} \frac{1}{\sigma_2\sqrt{2\pi}} e^{-(x-\mu_2)^2/2\sigma_2^2} dx, & (3.1.4) \end{cases}$$

where

$$\overline{\mu} = \mu_1 \times \frac{\sigma_2}{\sigma_1 + \sigma_2} + \mu_2 \times \frac{\sigma_1}{\sigma_1 + \sigma_2} \tag{3.1.5}$$

is the threshold to determine which distribution (i.e., $N(\mu_1, \sigma_1^2)$ or $N(\mu_2, \sigma_2^2)$) that a sample should be classified into. Correspondingly, the probability that a sample coming from the distribution $N(\mu_1, \sigma_1^2)$ is not correctly classified into X_1 is denoted by (3.1.6)

$$P_1' = 1 - P_1, \tag{3.1.6}$$

and the probability that a sample coming from the distribution $N(\mu_2, \sigma_2^2)$ is not correctly classified into X_2 is defined by (3.1.7)

$$P_2' = 1 - P_2. \tag{3.1.7}$$

As shown in (3.1.5), $\overline{\mu}$ is the weighted/normalised mean of the two normal distributions $N(\mu_1, \sigma_1^2)$ and $N(\mu_2, \sigma_2^2)$. Thus, the proportional distances between the means (i.e., μ_1 and μ_2) of the distributions and the weighted/normalised mean $\overline{\mu}$ of the two normal distributions are equal. This results in the equivalent of the two probabilities P_1 and P_2. For the clarity of presentation, we define a common notation P to denote the probabilities P_1 and P_2. They maintain a correlation as presented in (3.1.8).

$$\begin{cases} P_1 & = P_2 = P \\ P_1' & = P_2' = 1 - P \end{cases}. \tag{3.1.8}$$

Moreover, due to these samples distributed independently and the results of classification following the binomial distribution, the probability of correctly classifying j samples is defined by (3.1.9)

$$Pr(j) = C_k^j P^j (1 - P)^{k-j}, \tag{3.1.9}$$

where $j = 1, 2, \cdots, k$. Thus, the probability of correctly classifying all k samples is shown in (3.1.10).

$$Pr(k) = P^k. \tag{3.1.10}$$

Group-based Detection

In comparison with the sample-by-sample detection mechanism, the group-based detection mechanism monitors traffic records as groups such that any attack detectors designed based on this mechanism can only label the traffic records within a group as attack records or normal traffic records entirely.

To classify the same group of independent samples $\{x_1, x_2, \cdots, x_k\}$ using the group-based detection mechanism, a new random variable z, which is the mean of k random samples from the distribution $N(\mu_l, \sigma_l^2)$, is defined as shown in (3.1.11).

$$z = \frac{1}{k}\sum_{t=1}^{k} x_t, \tag{3.1.11}$$

where $x_t \in X_l$ and $l = 1, 2$. Clearly, the new random variable z follows the distribution $Z_l \sim N(\mu_l, \frac{1}{k}\sigma_l^2)$ in which $l = 1, 2$. The threshold to determine which distribution (i.e., $N(\mu_1, \sigma_1^2)$ or $N(\mu_2\sigma_2^2)$) a group of samples should be classified into is defined by (3.1.12).

$$\overline{u} = \mu_1 \times \frac{\sigma_2}{\sigma_1 + \sigma_2} + \mu_2 \times \frac{\sigma_1}{\sigma_1 + \sigma_2}. \tag{3.1.12}$$

Since the random variable z is generated using k random samples x_t from the distribution $N(\mu_l, \sigma_l^2)$, the detection precision rate of assigning the z correctly into the respective distribution $N(\mu_1, \sigma_1^2)$ or $N(\mu_2, \sigma_2^2)$ is thus as given in (3.1.13) and

(3.1.14) respectively.

$$\begin{cases} q_1 = \displaystyle\int_{-\infty}^{\overline{u}} (1/(\frac{1}{\sqrt{k}}\sigma_1\sqrt{2\pi}))e^{-(z-\mu_1)^2/\frac{2}{k}\sigma_1^2}dz, & (3.1.13) \\ q_2 = \displaystyle\int_{\overline{u}}^{+\infty} (1/(\frac{1}{\sqrt{k}}\sigma_2\sqrt{2\pi}))e^{-(z-\mu_2)^2/\frac{2}{k}\sigma_2^2}dz. & (3.1.14) \end{cases}$$

Given the elaboration presented in Section 3.1.2, the two probabilities q_1 and q_2 show the following correlation

$$\begin{cases} q_1 = q_2 = q, & (3.1.15) \\ q_1' = q_2' = 1 - q. & (3.1.16) \end{cases}$$

The z defined in (3.1.11) represents a group of samples completely coming from the same distribution $N(\mu_1, \sigma_1^2)$ or $N(\mu_2, \sigma_2^2)$. However, in practice, samples may come from either distribution independently so that the probability of having a group of samples which come only from a single distribution $N(\mu_1, \sigma_1^2)$ or $N(\mu_2, \sigma_2^2)$ is $1/2^k$. Thus, the probability of correctly classifying all k samples by using the group-based detection mechanism is

$$\begin{cases} k & = 1, Q(k) = q_1 = q_2 \\ k & > 1, Q(k) = \frac{1}{2^k}q_1 = \frac{1}{2^k}q_2 \end{cases} . \qquad (3.1.17)$$

Comparison

The detailed comparison between the sample-by-sample detection mechanism and the detection precision of the group-detection mechanism is given in this section. The analytical results in the section of sample-by-sample detection and the section of group-based detection show clearly that the sample-by-sample detection mechanism and the group-based detection mechanism perform differently in detection precision. The relationship between the detection probabilities of the two detection mechanisms can be found by analysing (3.1.10) and (3.1.17).

As shown in (3.1.18) and (3.1.19), when k equals to 1, the probability of correctly classifying all k samples using the sample-by-sample detection mechanism is same as the one achieved using the group-based detection mechanism. If k is greater than 1, both the probabilities $Pr(k)$ and $Q(k)$ decrease gradually, but the one of the group-based detection mechanism drops faster in comparison with that of the sample-by-sample detection mechanism, namely,

$$\begin{cases} k = 1, Pr(k) = Q(k), & (3.1.18) \\ k > 1, Pr(k) > Q(k). & (3.1.19) \end{cases}$$

Apparently, the sample-by-sample detection mechanism always achieves equal or better detection probability than the group-based detection mechanism.

Given an example that there are two normally distributed populations $X_1^{ex} \sim N(0, 12^2)$ and $X_2^{ex} \sim N(10, 18^2)$, the thresholds $\overline{\mu} = 4$ and $\overline{u} = 4$ are computed according to (3.1.5) and (3.1.12). On one hand, the detection precision of the sample-by-sample detection mechanism on a single sample is computed using (3.1.3) and (3.1.4), and whose value is $P_1 = P_2 = P = 0.63$. Thus, if the number of samples is set to $k = 16$, the overall detection precision of the sample-by-sample detection mechanism is $Pr(k) = 0.63^{16} =$ **6.1581e–04** in accordance with (3.1.10). On the other hand, the detection precision of the group-based detection mechanism is obtained for a group of 16 samples using (3.1.17), in which q_1 and q_2 are computed using (3.1.13) and (3.1.14). Due to $q_1 = q_2 = 0.90824$, the detection precision of the group-based detection mechanism for 16 samples is $Q(16) = \frac{1}{2^{16}} q_1 = \frac{1}{2^{16}} q_2 = \frac{1}{2^{16}} \times 0.90824 =$ **1.3859e–05**. It is clear that the sample-by-sample detection mechanism achieves higher detection precision than the group-based detection mechanism in the above example.

The afore-analysis shows that the sample-by-sample detection mechanism performs better than the group-based detection mechanism in detection precision. Moreover, the sample-by-sample detection mechanism offers benefits that are not found in the group-based detection mechanism. For example, intrusive traffic samples can be labelled individually, and the probability of correctly classifying a sample into its population is higher than the one achieved using the group-based detection mechanism in a general network scenario. Therefore, we decide to employ the sample-by-sample detection mechanism in this study.

3.1.3 Multivariate Correlation Analysis

The multivariate correlation analysis is motivated by the fact that the occurrence of network intrusions causes changes of these correlations. The correlations between the features of an attack traffic record appear different in quantity in comparison with the ones of the legitimate network traffic. Raw network traffic features, such as the ones in KDD Cup 99 dataset [84], maintain plain or hidden correlations among themselves. However, these correlations are often ignored in the decision making methods that relies only on the plain information coming from the raw features. This leads to a disadvantage in detection accuracy. Thus, it is suggested to use the changes as indicators to reveal any intrusive activities. The correlations between any two distinct features within each single network traffic record are extracted through this analysis.

3.1.4 Anomaly-based Intrusion Detection

Anomaly-based detection mechanism [21] facilitates the detection of zero-day DoS attacks. Furthermore, the labour-intensive attack analysis and the frequent update of the attack signature database in the case of misuse-based detection are avoided. Meanwhile, the mechanism enhances the robustness of the proposed detection systems and makes them harder to be evaded because attackers need to generate attacks that match the normal traffic profiles built by a specific detection algorithm. This is, however, a labour-intensive task and requires expertise in the target detection algorithm. Thus, the defence can hardly be penetrated.

3.1.5 Traffic Classification Based on Computer Vision Techniques

Anomaly-based network intrusion detection approaches have been proven to be promising in detecting zero-day attacks. They, however, commonly suffer from high false positive rates, which results in an unacceptable number of false alerts to be generated. An administrator of a production network that employed this type of detection approaches would be seriously confused by the overwhelming inaccurate information. This hampers anomaly-based network intrusion detection approaches from being applied in commercial detection systems.

To solve the aforementioned problem, more sophisticated modelling and classification techniques are desired. These techniques help develop accurate representations for legitimate network behaviours and provide precise classification for legitimate and attack traffic. The commonalities shared between the DoS attack detection task and computer vision tasks (e.g., image retrieval and object shape recognition) motivate us to adopt the techniques used in computer vision into this mission.

According to the principal assumption of anomaly-based intrusion detection, cyber attack traffic behaves significantly different from legitimate network traffic. Thus, we can consider each network traffic record as an image in a data warehouse. Legitimate network traffic records are the ones showing a particular theme. Whereas, attack traffic records are those depicting themes other than that described in the legitimate network traffic records. A profile representing legitimate network traffic behaviours is taken as a query to an image retrieval system, which retrieves the matched images (i.e., the legitimate network traffic records) from the data warehouse. Such that the legitimate traffic records and attack traffic records are differentiated. If there are more than one category of themes, each category will be stored in a distinct section of a data warehouse. Retrieval is proceeded to a particular section of the data warehouse according to the category to which a query belongs.

Given that three categories of network traffic themes are studied in this thesis, namely TCP, UDP and ICMP traffic. These three categories of network traffic carrying data from different user applications. Network traffic records belonging to different categories are stored in the respective sections of a data warehouse. Given a query about legitimate TCP traffic, the retrieval system proceeds the query to the section of TCP traffic and retrieves the relevant records from there. Those unmatched traffic records in the same section are determined as attacks.

Through the aforementioned reformulation, an intrusion detection task is converted into a computer vision problem. Any appropriate techniques successfully used in computer vision tasks are able to be applied to this intrusion detection task.

Among a variety of state-of-the-art techniques, EMD [77] is a well-suited candidate. EMD supplies effective measures to differentiate observed objects by taking cross-bin correlation and partial matching into account. The detailed discussion on the merits of EMD and its application in DoS attack detection will be presented in Chapter 6.

3.2 Detection System Framework

In this section, the general system framework for DoS attach detection is presented and shown in Fig. 3.1. The framework consists of three major steps, namely **basic feature generation**, **multivariate correlation analysis** and **decision marking**. The attack detection mechanism based on individual traffic records, discussed in Section 3.1.2 is involved in the whole detection phase (i.e., Steps 1, 2 and 3). The detailed discussion of each step is given below.

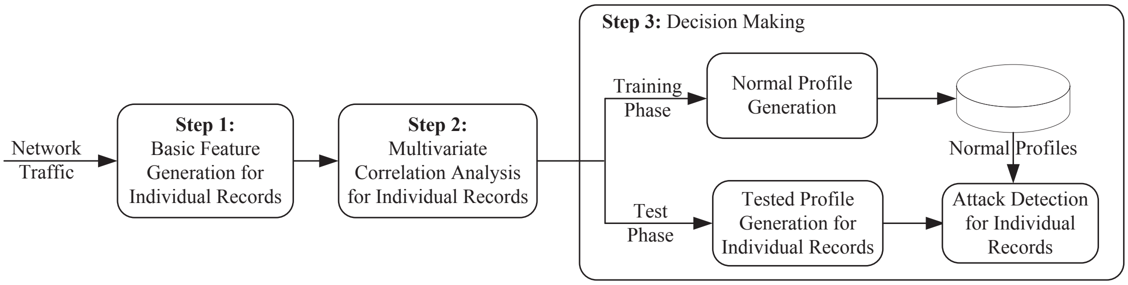

Network Traffic
Step 1: Basic Feature Generation for Individual Records
Step 2: Multivariate Correlation Analysis for Individual Records
Step 3: Decision Making
Training Phase
Normal Profile Generation
Normal Profiles
Test Phase
Tested Profile Generation for Individual Records
Attack Detection for Individual Records

Figure 3.1: A general system framework for denial-of-service attack detection

Step 1: Basic Feature Generation for Individual Records

The detection mechanism discussed in Section 3.1.1 is adopted in Step 1 of the framework to monitor only the ingress network traffic to the target network. This enables our detectors to provide the best-fit protection because legitimate traffic profiles used by the detectors are developed for a smaller number of network services. The monitored and collected ingress network traffic is characterised in the current step and used to generate basic features of traffic records for a well-defined time interval. The detailed process can be found in [84]. The generated basic features are then handed over the next step of the framework for further process.

Step 2: Multivariate Correlation Analysis

In Step 2 of the system framework, the multivariate correlation analysis mechanism introduced in Section 3.1.3 is conducted on individual records from Step 1. All of the extracted correlations are later applied to replace the original basic features of the observed network traffic records and to represent the traffic records. To meet the requirement of Step 2 that is to extract high discriminative information (i.e., correlations between features) from network traffic records, two multivariate correlation analysis approaches are proposed and discussed in Chapters 4 and 5.

Step 3: Decision Marking

In Step 3, the anomaly-based detection mechanism discussed in Section 3.1.4 is employed in the Decision Making. Specifically, two phases are involved in the Decision Marking, namely the Training Phase and the Test Phase. In the *Training Phase*, the Normal Profile Generation module is operated to generate profiles for various types of legitimate traffic records. The generated normal profiles are stored in a database for future detection. In the *Test Phase*, the Tested Profile Generation module is used to build profiles for individual observed traffic records. Then, the tested profiles are handed over to the Attack Detection module, which compares the individual tested profiles with the respective stored normal profiles. A threshold-based classifier, which is based on computer vision techniques as suggested in Section 3.1.5, is employed in the Attack Detection module to distinguish DoS attacks from legitimate traffic.

3.3 Summary

The general system framework for DoS attack detection has been proposed in this chapter. It employs various detection mechanisms, including network traffic monitoring at destination network, attack detection based on individual traffic records, multivariate correlation analysis, anomaly-based intrusion detection and traffic classification based on computer vision techniques. These relevant detection mechanisms equip the proposed system framework with the following desirable properties.

1. It facilitates detection systems to provide best-fit protections to the targeted networks,

2. Detection can achieve a higher probability of correctly classifying a sample in a prompt manner into its population than the one achieved using the group-based detection mechanism in a general network scenario, and

3. It enables detection systems with the capability of labelling intrusive network traffic samples individually.

Therefore, the proposed general detection system framework will be applied into the following chapters.

Chapter 4

Multivariate Correlation Analysis Based on Euclidean Distance Map

Multivariate correlation coefficient is a statistic estimating the relationship between two random variables. It is playing an increasingly important role in network intrusion detection, especially DoS attack detection. The correlations extracted from the features of the given network traffic data provide critical discriminative power for accurate classification. The changes of these correlations are effective indicators of the variance of network traffic pattern. Any significant deviation from the patterns of the correlations extracted from the features of legitimate network traffic infers the appearance of abnormal traffic, such as DoS traffic.

The most recent studies on IDSs have employed the principle of MCA. For example, the detection systems, proposed in [48], [95] and [105], employed covariance matrix technique to analyse the multivariate correlations between the features from network packet header fields. A geometrical correlation extraction approach based on Mahalanobis Distance (MD) [46] and its enhancement [45] were proposed by Jamdagni et al. to measure the weighted distance between each pair of features. In addition, a MCA approach based on the estimation of triangle areas among an observed data sample and any pairs of distinct centroids of the clusters (i.e., different types of network traffic) was suggested in [98].

Although these MCA approaches adopted the key idea of applying multivariate correlation analysis in discriminative feature extraction, the imperfection of these techniques restricts their applications in limited scenarios. These detection systems in [48], [95] and [105] can be evaded by any attacks managing to make all monitored features change linearly and are vulnerable to mix-traffic containing both normal and attack traffic. The two approaches presented in [45] and [46] withstand the above problem, but they were typically designed for network traffic packet payload. Although the approach proposed in [98] is deemed to be the most general among the discussed MCA approaches, it has a strong dependency on the knowledge of historic network traffic.

To address the aforementioned problems, a novel MCA approach based on EDM is proposed in this chapter to analyse the basic features and to extract the multivariate correlations. This MCA approach is designed based on our works published in [90], [91] and [92]. Owing to the computational simplicity of Euclidean distance and the valuable discriminative information extracted from the basic features, our MCA equips IDSs with the capability of effective detection. Moreover, our MCA conducts analysis on individual network traffic records, avoiding the dependency on prior knowledge of network traffic.

The rest of this chapter is organised as follows. The novel MCA based on Euclidean distance map is proposed in Section 4.1. Section 4.2 proposes a DoS attack detection system using MCA based on Euclidean distance map. The evaluation on the proposed MCA approach is presented in Section 4.3, and the evaluation of the proposed DoS attack detection system is given in Section 4.3.4. Section 4.5 draws a summary to the chapter.

4.1 Multivariate Correlation Analysis Approach

A novel MCA approach is proposed in this section to analyse the correlations within network traffic data. The statistical properties (e.g., the number of data bytes from source to destination, the length of a connection and the number of connections to the same host in the past two seconds etc.), providing rough descriptions to the network traffic flows, are studied using the proposed MCA approach to discover their relations.

The feature vectors, formed using the extracted correlations, supply with accurate depictions to the patterns of network traffic behaviours. An abrupt change would appear on the pattern of the network traffic behaviour when network intrusions were being launched, especially DoS attacks. This is due to the fact that DoS attacks attempt to degrade the availability of a victim, such as host, router or even entire network, by imposing floods with a huge amount of useless packets. This makes the flooding network traffic behave differently from the legitimate network traffic.

The proposed MCA approach employs Euclidean distance in the extraction of correlative information from the basic feature space of network traffic data. The details are shown in the following section.

4.1.1 Multivariate Correlation Extraction

Given an arbitrary dataset $X = [x_1\, x_2\, \cdots\, x_n]$, where

$$x_i = \begin{bmatrix} f_1^i \\ f_2^i \\ \vdots \\ f_m^i \end{bmatrix}$$

represents the i^{th} m-dimensional traffic record, and i is ranged from 1 to n. By substituting x_i into the X, the dataset can be represented in detail as (4.1.1).

$$X = \begin{bmatrix} f_1^1 & f_1^2 & \cdots & f_1^n \\ f_2^1 & f_2^2 & \cdots & f_2^n \\ \vdots & \vdots & \ddots & \vdots \\ f_m^1 & f_m^2 & \cdots & f_m^n \end{bmatrix}, \qquad (4.1.1)$$

where f_l^i is the value of the l^{th} feature in the i^{th} traffic record, and l and i are varying from 1 to m and from 1 to n respectively.

In order to explore the correlations reserved in the i^{th} traffic record on a multi-dimensional space, the record x_i is transformed into a new m-by-m feature matrix x_i'. The transformation is done by simply multiplying x_i^T (i.e., the transpose of x_i) with an m-by-m identity matrix I as shown in (4.1.2).

$$x_i' = x_i^T I = \begin{bmatrix} f_1^i & f_2^i & \cdots & f_m^i \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}_{m \times m} = \begin{bmatrix} f_1^i & 0 & \cdots & 0 \\ 0 & f_2^i & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & f_m^i \end{bmatrix}. \qquad (4.1.2)$$

The elements along the diagonal of the matrix x_i' are the features of the record x_i. Each single column of the matrix x_i' is defined as a new m-dimensional feature vector

F_j^i given in (4.1.3).

$$F_j^i = \begin{bmatrix} \eta_{j,1}^i \\ \eta_{j,2}^i \\ \vdots \\ \eta_{j,m}^i \end{bmatrix}, \tag{4.1.3}$$

where $\eta_{j,p}^i = 0$ if $j \neq p$ and $\eta_{j,p}^i = f_j^i$ if $j = p$. The superscript i and the subscripts j and p satisfy the constrains $1 \leq i \leq n$, $1 \leq j \leq m$ and $1 \leq p \leq m$ respectively. As such, the m-by-m feature matrix x_i' can be rewritten as (4.1.4).

$$x_i' = [F_1^i \; F_2^i \; \cdots \; F_m^i]. \tag{4.1.4}$$

Correlation analysis commences upon the completion of the above transformation. The correlation between the feature vectors j and k of the feature matrix x_i' is analysed and extracted using Euclidean distance, and it is defined in (4.1.5).

$$ED_{j,k}^i = \begin{cases} \sqrt{(F_j^i - F_k^i)^T (F_j^i - F_k^i)} & ,\text{if } j \neq k, \\ 0 & ,\text{if } j = k, \end{cases} \tag{4.1.5}$$

where $1 \leq i \leq n$, $1 \leq j \leq m$ and $1 \leq k \leq m$. In the case of $j = k$, F_j^i and F_k^i refer to the same feature vector in the feature matrix x_i' so that the correlation (i.e., the distance) between F_j^i and F_k^i is zero. The complete overview of the correlations reserved within the original traffic record x_i is denoted by a Euclidean Distance Map (EDM) and shown in (4.1.6).

$$EDM_{x_i} = \begin{bmatrix} ED_{1,1}^i & ED_{1,2}^i & \cdots & ED_{1,m}^i \\ ED_{2,1}^i & ED_{2,2}^i & \cdots & ED_{2,m}^i \\ \vdots & \vdots & \ddots & \vdots \\ ED_{m,1}^i & ED_{m,2}^i & \cdots & ED_{m,m}^i \end{bmatrix}. \tag{4.1.6}$$

Since Euclidean distance is a direction insensitive distance measure and the distance between a node and itself is zero, a EDM, such as EDM_{x_i} shown in (4.1.6), is a symmetric matrix with elements of zeros along its diagonal.

Using the above proposed MCA approach, EDMs are generated for individual traffic records in the given arbitrary dataset X. The entire set of EDMs is given in (4.1.7) .

$$X_{EDM} = [EDM_{x_1}\ EDM_{x_2}\ \cdots\ EDM_{x_n}]_{m \times m \times n}. \tag{4.1.7}$$

4.1.2 Example and Discussion

To give some insights into the afore-discussed MCA, an example is presented in the section. Assume a three-dimensional data record $x_{example} = [1\ 2\ 4]^T$, its inner correlations are studied and extracted using (4.1.2) of the proposed analysis approach as shown in $x'_{example}$ below.

$$x'_{example} = x^T_{example} I = [1\ 2\ 4] \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{bmatrix}.$$

The columns (i.e., the feature vectors $F_1^{example}$, $F_2^{example}$ and $F_3^{example}$) of the 3-by-3 transformation matrix $x'_{example}$ are denoted by

$$F_1^{example} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad F_2^{example} = \begin{bmatrix} 0 \\ 2 \\ 0 \end{bmatrix}, \quad F_3^{example} = \begin{bmatrix} 0 \\ 0 \\ 4 \end{bmatrix}.$$

Then, the matrix $x'_{example}$ is redefined using (4.1.4) and the notions $F_1^{example}$, $F_2^{example}$ and $F_3^{example}$.

$$x'_{example} = [F_1^{example}\ F_2^{example}\ F_3^{example}].$$

The correlations between any two feature vectors (i.e., $ED_{1,1}^{example}$, $ED_{1,2}^{example}$, $ED_{1,3}^{example}$, $ED_{2,1}^{example}$, $ED_{2,2}^{example}$, $ED_{2,3}^{example}$, $ED_{3,1}^{example}$, $ED_{3,2}^{example}$ and $ED_{3,3}^{example}$) are computed using (4.1.5), and their respective values are shown as follows.

$$\begin{cases} ED_{1,1}^{example} = ED_{2,2}^{example} = ED_{3,3}^{example} = 0, \\ ED_{1,2}^{example} = ED_{2,1}^{example} = \sqrt{(F_1^{example} - F_2^{example})^T (F_1^{example} - F_2^{example})} = \sqrt{5}, \\ ED_{1,3}^{example} = ED_{3,1}^{example} = \sqrt{(F_1^{example} - F_3^{example})^T (F_1^{example} - F_3^{example})} = \sqrt{17}, \\ ED_{2,3}^{example} = ED_{3,2}^{example} = \sqrt{(F_2^{example} - F_3^{example})^T (F_2^{example} - F_3^{example})} = \sqrt{20}. \end{cases}$$

Finally, the complete multivariate correlations retained in the $x_{example}$ is presented using (4.1.6), and the Euclidean distance map (i.e., $EDM_{x_{example}}$) is determined by the above correlations and shown below.

$$EDM_{x_{example}} = \begin{bmatrix} ED_{1,1}^{example} & ED_{1,2}^{example} & ED_{1,3}^{example} \\ ED_{2,1}^{example} & ED_{2,2}^{example} & ED_{2,3}^{example} \\ ED_{3,1}^{example} & ED_{3,2}^{example} & ED_{3,3}^{example} \end{bmatrix} = \begin{bmatrix} 0 & \sqrt{5} & \sqrt{17} \\ \sqrt{5} & 0 & \sqrt{20} \\ \sqrt{17} & \sqrt{20} & 0 \end{bmatrix}.$$

The above example illustrates how the proposed MCA is applied to conduct analysis on a sample data record. It shows clearly that a Euclidean distance map is a symmetric matrix along its main diagonal.

Furthermore, the proposed MCA approach presents unique characteristics. The use of Euclidean distance on the original multi-dimensional distance helps eliminate the dilemmas of other multivariate correlation analysis approaches [45][46][48][95][98][105]. Firstly, our proposed MCA approach is only based on the current network traffic record. This releases the analysis of correlations from the dependency on prior knowledge of historic network traffic (neither legitimate traffic nor attack traffic). Secondly, our MCA approach solves the issue of linear change of all observed features.

Assume that an intruder launched an attack which managed to change all features of the previous example linearly and the attack is shown as $x_{attack} = [2\ 4\ 8]^T$. It contributes a different Euclidean distance map (i.e., EDM_{attack}) from $EDM_{example}$.

$$EDM_{x_{attack}} = \begin{bmatrix} 0 & \sqrt{20} & \sqrt{68} \\ \sqrt{20} & 0 & \sqrt{80} \\ \sqrt{68} & \sqrt{80} & 0 \end{bmatrix}.$$

Thus, the change can be revealed by using our proposed MCA approach. By making use of the multivariate correlations, various types of network traffic can be clearly characterised. This is evaluated in Section 4.3.

4.2 Network Intrusion Detection Using Multivariate Correlation Analysis Based on Euclidean Distance Map

To appropriately evaluate the effectiveness of the proposed EDM-based MCA approach, we decide to apply it to a real intrusion detection problem, namely DoS attack detection, which is one of the core objectives of this thesis. Following the system framework suggested in Chapter 3, the EDM-based MCA approach to be evaluated is plugged into Step 2 of Fig. 3.1.

4.2.1 Framework

A new system framework based on our MCA approach is presented in Fig. 4.1. This new system framework embraces the anomaly-based detection mechanism and the other mechanisms discussed in Sections 3.1.1-3.1.3. This enables IDSs based on this system framework to effectively recognise known and unknown network intrusions.

In the following of this section, we give an overview of how our proposed MCA approach is applied to a DoS attack detection system, which is designed based on

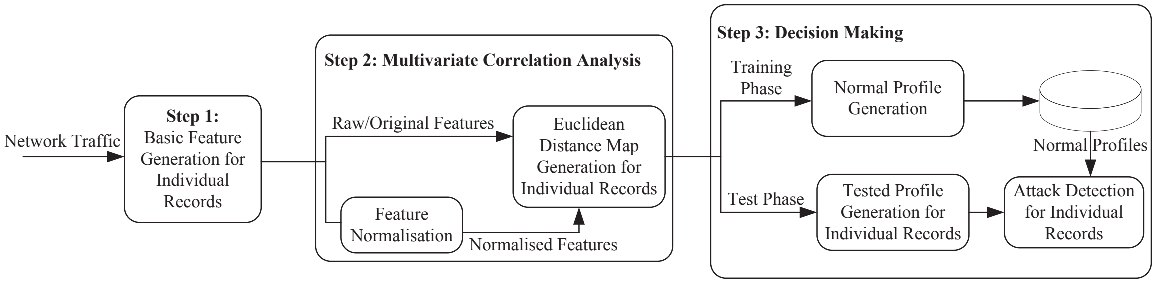

Network Traffic
Step 1:
Basic Feature Generation for Individual Records
Step 2: Multivariate Correlation Analysis
Raw/Original Features
Euclidean Distance Map Generation for Individual Records
Feature Normalisation
Normalised Features
Step 3: Decision Making
Training Phase
Normal Profile Generation
Normal Profiles
Test Phase
Tested Profile Generation for Individual Records
Attack Detection for Individual Records

Figure 4.1: A system framework for denial-of-service attack detection using multivariate correlation analysis based on Euclidean distance map

the system framework shown in Fig. 4.1. The Training Phase and the Test Phase are focused. The normal profiles of the IDSs are generated using only legitimate network traffic during the Training Phase in Step 3 of the framework, which provides the best fit solution for protecting the targeted networks.

Additionally, the Euclidean distance maps of network traffic records are eventually symmetric matrices. EDMs can be deemed as images that are symmetric along their main diagonals. Any differences, identified on the upper triangles of the images, can be found on their lower triangles as well. Therefore, to perform a quick comparison of the two EDMs, we can choose to investigate either the upper triangles or the lower triangles of the EDMs only. This produces the same result as comparing using the entire EDMs. The correlations residing in a traffic record can be represented effectively and correctly by the upper triangle or the lower triangle of the respective EDM. For consistency, we consider the lower triangles of EDMs when training and testing the proposed DoS attack detection system.

Now, assume that there is a set of g m-dimensional normal training network traffic records (i.e., $X^{normal} = [x_1^{normal}\ x_2^{normal}\ \cdots\ x_g^{normal}]$), which are denoted by the lower triangles of the EDMs extracted using our proposed EDM-based MCA approach, namely

$$X_{EDM}^{normal} = [EDM_{x_1^{normal}}^{lower} \; EDM_{x_2^{normal}}^{lower} \; \cdots \; EDM_{x_g^{normal}}^{lower}],$$

where

$$EDM_{x_i^{normal}}^{lower} = \begin{bmatrix} ED_{2,1}^{x_i^{normal}} \\ ED_{3,1}^{x_i^{normal}} \\ \vdots \\ ED_{m,m-1}^{x_i^{normal}} \end{bmatrix}_{\frac{m\times(m-1)}{2}}$$

and $1 \le i \le g$. An observed network traffic record (i.e., $x^{observed}$) is denoted by the lower triangle of its EDM extracted by the EDM-based MCA approach, namely

$$EDM_{x^{observed}}^{lower} = \begin{bmatrix} ED_{2,1}^{x^{observed}} \\ ED_{3,1}^{x^{observed}} \\ \vdots \\ ED_{m,m-1}^{x^{observed}} \end{bmatrix}_{\frac{m\times(m-1)}{2}} .$$

The training and the testing of the proposed DoS attack detection system are presented in Sections 4.2.2 and 4.2.3 based on the given training and test samples.

4.2.2 Training Phase

In the Training Phase, the main task is to build profiles for various types of legitimate network traffic. This is proposed to be done through the density estimation of the MDs between the given legitimate traffic records and the expectation of the legitimate traffic. The probability distribution of the MDs is described by two parameters, namely the mean $\overline{Dis}$ and the standard deviation Std of the distances.

The two parameters are determined using the algorithm proposed in Fig. 4.2, in which the training dataset X_{EDM}^{normal} is to be analysed. As shown in line 2 of the algorithm, the expectation (i.e., $\overline{EDM_{X^{normal}}^{lower}}$) of the data objects (e.g., $EDM_{x_i^{normal}}^{lower}$)

```
Require: A dataset $X_{EDM}^{normal}$ {It contains the lower triangles of the EDMs of the $g$ normal training records, and each of which has $\frac{m\times(m-1)}{2}$ features.}
Initialise $DIS$ {It is an array with $g$ elements denoted by $Dis_i(1 \leq i \leq g)$.}
$\overline{EDM_{X^{normal}}^{lower}} \leftarrow \frac{1}{g}\sum_{i=1}^{g} EDM_{x_i^{normal}}^{lower}$
Generate covariance matrix $Cov$ for $X_{EDM}^{normal}$ using (5.2.3)
for $i = 1$ to $g$ do
    $Dis_i \leftarrow MD(EDM_{x_i^{normal}}^{lower}, \overline{EDM_{X^{normal}}^{lower}})$ {Mahalanobis distance between $EDM_{x_i^{normal}}^{lower}$ and $\overline{EDM_{X^{normal}}^{lower}}$}
end for
$\overline{Dis} \leftarrow \frac{1}{g-1}\sum_{i=1}^{g} Dis_i$
$Std = \sqrt{\frac{1}{g}\sum_{i=1}^{g}(Dis_i - \overline{Dis})^2}$
$Pro \leftarrow (N(\overline{Dis}, Std^2), \overline{EDM_{X^{normal}}^{lower}}, Cov)$
return $Pro$
```

Figure 4.2: An algorithm for normal profile generation based on EDM-based MCA approach.

is computed over all the data objects within the dataset. Then, the Mahalanobis distances between the expectation and the individual data objects are measured using (4.2.1) over the whole dataset.

$$Dis_i = \sqrt{\frac{(EDM_{x_i^{normal}}^{lower} - \overline{EDM_{X^{normal}}^{lower}})^T (EDM_{x_i^{normal}}^{lower} - \overline{EDM_{X^{normal}}^{lower}})}{Cov}}, \tag{4.2.1}$$

where Cov is the covariance matrix of the given dataset X_{EDM}^{normal} and is denoted by (4.2.2).

$$Cov = \begin{bmatrix} \sigma_{ED_{2,1}^{X^{normal}} ED_{2,1}^{X^{normal}}} & \sigma_{ED_{2,1}^{X^{normal}} ED_{3,1}^{X^{normal}}} & \cdots & \sigma_{ED_{2,1}^{X^{normal}} ED_{m,m-1}^{X^{normal}}} \\ \sigma_{ED_{3,1}^{X^{normal}} ED_{2,1}^{X^{normal}}} & \sigma_{ED_{3,1}^{X^{normal}} ED_{3,1}^{X^{normal}}} & \cdots & \sigma_{ED_{3,1}^{X^{normal}} ED_{m,m-1}^{X^{normal}}} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{ED_{m,m-1}^{X^{normal}} ED_{2,1}^{X^{normal}}} & \sigma_{ED_{m,m-1}^{X^{normal}} ED_{3,1}^{X^{normal}}} & \cdots & \sigma_{ED_{m,m-1}^{X^{normal}} ED_{m,m-1}^{X^{normal}}} \end{bmatrix} \tag{4.2.2}$$

and the covariance/variance between $ED_{j,k}^{X^{normal}}$ and $ED_{l,v}^{X^{normal}}$ in the lower triangle of the normal EDM is defined by (4.2.3).

$$\begin{aligned}\sigma_{ED_{j,k}^{X^{normal}}\, ED_{l,v}^{X^{normal}}} = \frac{1}{g-1}\sum_{i=1}^{g}&(ED_{j,k}^{x_i^{normal}} - \mu_{ED_{j,k}^{X^{normal}}}) \\ &(ED_{l,v}^{x_i^{normal}} - \mu_{ED_{l,v}^{X^{normal}}})\ ,\end{aligned} \tag{4.2.3}$$

where j and k are ranged from 2 to m, and l and v are ranged from 1 to $m-1$. The $\mu_{ED_{j,k}^{X^{normal}}}$ and $\mu_{ED_{l,v}^{X^{normal}}}$ in (4.2.3) are computed using (4.2.4) and (4.2.5).

$$\mu_{ED_{j,k}^{X^{normal}}} = \frac{1}{g}\sum_{i=1}^{g} ED_{j,k}^{x_i^{normal}}, \tag{4.2.4}$$

and

$$\mu_{ED_{l,v}^{X^{normal}}} = \frac{1}{g}\sum_{i=1}^{g} ED_{l,v}^{x_i^{normal}}. \tag{4.2.5}$$

Afterwards, these obtained Mahalanobis distances are kept in the respective Dis_i, where i is varying from 1 to g, for normal profile generation at the later stage. Finally, the mean $\overline{Dis}$ and the standard deviation Std of the distances are computed as presented in lines 7 and 8 of Fig. 4.2. The obtained parameters (i.e., $\overline{Dis}$ and Std), the $\overline{EDM_{X^{normal}}^{lower}}$ and the Cov are stored in the normal profile Pro.

4.2.3 Test Phase

In the Test Phase, observed (tested) network traffic records are examined individually against the normal profiles that are generated in the training phase. According to the definition of normal distribution, roughly 99.7% of the values are within three standard deviations from the mean (i.e., $\overline{Dis}$) of the Mahalanobis distances. Therefore, the decision can be made by comparing the distance (i.e., $Dis_{observed}$) of an observed data object (i.e., $EDM_{x^{observed}}^{lower}$) to the expectation (i.e., $\overline{EDM_{X^{normal}}^{lower}}$) of the training data objects against the pre-defined thresholds (i.e., $(\overline{Dis} - \alpha \times Std)$ and $(\overline{Dis} + \alpha \times Std)$), where α is a parameter to determine the range of acceptance of an observed network traffic record to be normal traffic. The detailed procedure for the detection of DoS intrusions is defined in the algorithm shown in Fig. 4.3.

```
Require: The $EDM^{lower}_{x^{observed}}$ of a tested sample $x^{observed}$, normal traffic
    profile $Pro$ and parameter $\alpha$
1: $Dis_{observed} \leftarrow MD(EDM^{lower}_{x^{observed}}, \overline{EDM^{lower}_{X^{normal}}})$
2: if $(\overline{Dis} - \alpha \times Std) \leq Dis_{observed} \leq (\overline{Dis} + \alpha \times Std)$ then
3:     return Normal
4: else
5:     return Attack
6: end if
```

Figure 4.3: An algorithm for attack detection based on EDM-based MCA approach.

As shown between lines 2 and 6 in Fig. 4.3, if the distance (i.e, $Dis_{observed}$) exceeds the pre-defined thresholds (i.e., $(\overline{Dis} - \alpha \times Std)$ and $(\overline{Dis} + \alpha \times Std)$), the observed network traffic record is flagged as an attack otherwise it is normal. For a normal distribution, α is usually ranged from 1 to 3. This means that we would like to make a detection decision with a certain level of confidence varying from 68% to 99.7% in associate with the selection of different values of α.

4.3 Evaluation on the Multivariate Correlation Analysis Based on Euclidean Distance Map

The proposed Multivariate Correlation Analysis based on Euclidean Distance Map (EDM-based MCA) approach is evaluated for its accuracy on characterisation of network traffic and its contribution to the DoS attack detection system in this section.

The evaluation is carried out on both the original network traffic data and the normalised network traffic data. The final results are compared with two state-of-the-art approaches.

4.3.1 Evaluation Datasets

As a well-known benchmark, the KDD Cup 99 dataset [84] has contributed substantially to the evaluation of the advances in network intrusion detection and has remained active in many recent cutting-edge research [48][57][93][98]. In addition, this dataset has been recommended for evaluating the performance of an anomaly-based IDS in detecting new intrusions. Due to the reason that the primary concern to an anomaly-based IDS is its accuracy in modelling normal traffic behaviour of a network, the age of data does not prevent a fair evaluation on the system [27]. Moreover, testing our approach using KDD Cup 99 dataset contributes convincing evaluations and comparisons with other related state-of-the-art techniques [48][98].

However, the dataset has been criticised for redundant records that prevent algorithms from learning infrequent harmful records [94]. Thus, the selection of non-redundant data may apply to avoid this negative impact, but it is a labour-intensive task. Alternatively, algorithms innately withstand the problem are more desirable. As one of this kind, the underlying algorithms of our proposed DoS attack detection system are immune to the problem because its profiles are built purely based on legitimate network traffic. Therefore, the aforementioned problem introduced by the redundant data can be avoided in our evaluations.

Although some other evaluation datasets are available, these datasets all have some drawbacks. For example, CDX datasets [79] were poorly documented, and University of New Brunswick (UNB) ISCX Intrusion Detection Evaluation dataset [82] contains data collected from a simulation run in a control environment, in which computer programs simulated users' behaviours to generate network traffic. Therefore, these drawbacks prevent these datasets from being used in our evaluations.

4.3.2 Experimental Data for Evaluation

In this evaluation, the 10 percent labelled data of the KDD Cup 99 dataset are applied, which include five types of DoS attacks (i.e., Teardrop, Smurf, Pod, Neptune and Land attacks) and three types of legitimate network traffic (i.e., legitimate TCP, UDP and ICMP traffic).

The DoS attacks were launched using different types of network traffic, such as TCP, UDP and ICMP traffic. Among the aforementioned five types of attacks, Neptune and Land attacks were carried by TCP traffic, whereas, Teardrop was launched via UDP traffic. Finally, Smurf and Pod attacks were using ICMP packets.

4.3.3 Evaluation on Network Traffic Characterisation

An effective multivariate correlation analysis approach must provide accurate characterisation to various types of network traffic. Since DoS attack traffic behaves anomalously in comparison with legitimate network traffic, the EDMs of DoS attack records must be different from those of normal traffic records. If significant differences are identified from these maps (i.e., EDMs), the proposed EDM-based MCA approach can be demonstrated as promising in characterisation of network traffic and extraction of discriminative power from various types of network traffic.

To show how the correlations between the features of a network traffic record are presented in Euclidean distance map, the EDMs of normal traffic records and those of various types of attack traffic records are exhibited in this section. These EDMs are generated using 32 numerical features of the network traffic records available in the aforementioned 10 percent labelled data.

0	1448	4269	11	11	11	11	11	11	11	11	11	11	19	21	11	11	11	11	12	11	11	137	228	12	11	11	11	11	11	11	11
1448	0	5490	1439	1439	1439	1439	1439	1439	1439	1439	1439	1439	1440	1440	1439	1439	1439	1439	1439	1439	1439	1481	1531	1439	1439	1439	1439	1439	1439	1439	1439
4269	5490	0	4264	4264	4264	4264	4264	4264	4264	4264	4264	4264	4265	4265	4264	4264	4264	4264	4264	4264	4264	4289	4309	4264	4264	4264	4264	4264	4264	4264	4264
11	1439	4264	0	3.91 E-05	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	3.91 E-05	0	0	0	0	0	0	0	0	3.91 E-05	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	3.91 E-05	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
19	1440	4265	8	8	8	8	8	8	8	8	8	8	0	13	8	8	8	8	8	8	8	128	218	8	8	8	8	8	8	8	8
21	1440	4265	10	10	10	10	10	10	10	10	10	10	13	0	10	10	10	10	10	10	10	128	218	10	10	10	10	10	10	10	10
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
12	1439	4264	1	1	1	1	1	1	1	1	1	1	8	10	1	1	1	1	0	1	1	127	218	1	1	1	1	1	1	1	1
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
137	1481	4289	127	127	127	127	127	127	127	127	127	127	128	128	127	127	127	127	127	127	127	0	268	127	127	127	127	127	127	127	127
228	1531	4309	218	218	218	218	218	218	218	218	218	218	218	218	218	218	218	218	218	218	218	268	0	218	218	218	218	218	218	218	218
12	1439	4264	1	1	1	1	1	1	1	1	1	1	8	10	1	1	1	1	1	1	1	127	218	0	1	1	1	1	1	1	1
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0
11	1439	4264	0	0	0	0	0	0	0	0	0	0	8	10	0	0	0	0	1	0	0	127	218	1	0	0	0	0	0	0	0

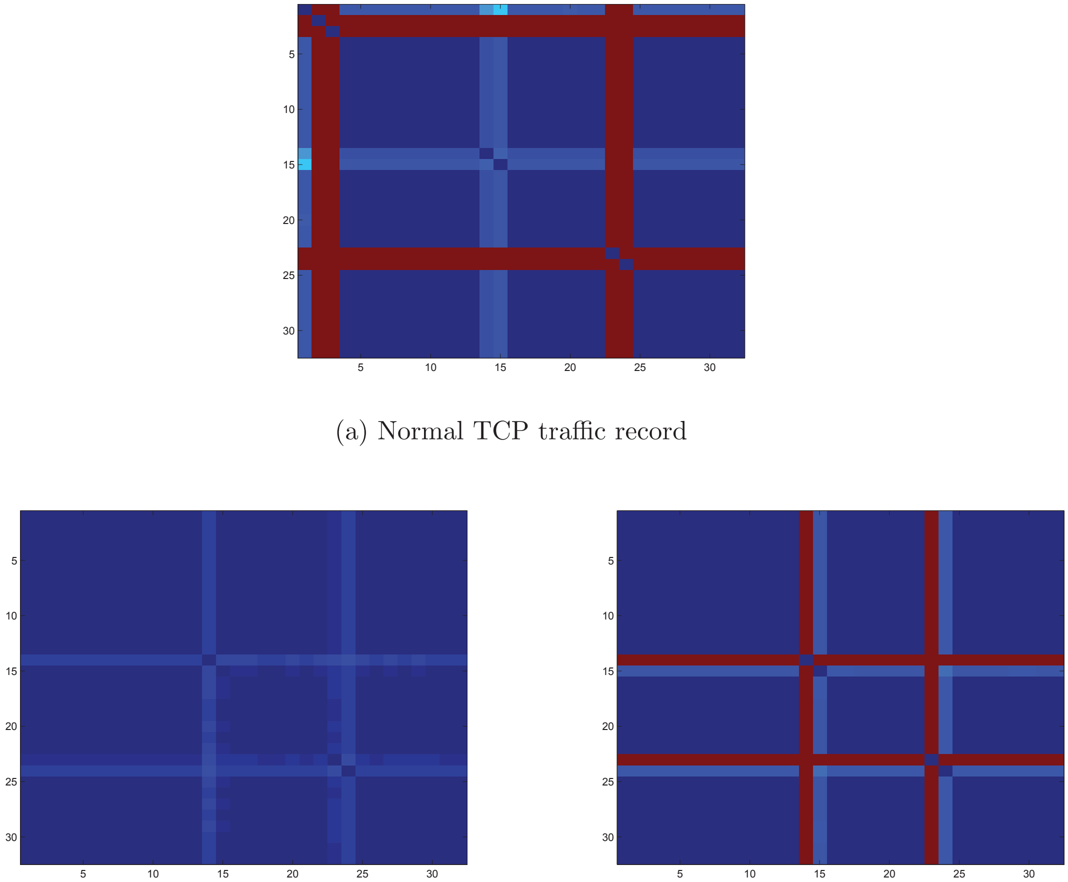
Figure 4.4: The EDM of a normal TCP traffic record.

As shown in Fig. 4.4, the EDM of normal TCP traffic record is a symmetric matrix and the values of the elements along its main diagonal from the top left hand side to the bottom right hand side are all zeros. This is because the Euclidean distance measure is insensitive to the orientation of a straight line formed by any two objects in the Cartesian coordinate system, and the distance between a feature vector (i.e., F_j^i) and itself is always zero. In other words, assume that there are two objects D and E. The distance from object D to object E is equivalent to the distance from object E to object D, and if object D and object E are the same object, then their distance is zero.

With the accurate characterisation of various types of network traffic, the differences between these types of network traffic could be recognised by investigating into and comparing their raw EDMs straight-away. However, this is a manual labour intensive task. In contrast, visual comparison might give a better solution in terms of efficiency. Therefore, we suggest to convert these EDMs into colour images. As such, the comparison can be made on the images of the EDMs rather than the raw EDMs.

The images of normal TCP traffic record, Neptune attack record and Land attack record are given in Fig. 4.5. The images of normal UDP traffic record and Teardrop attack record are shown in Fig. 4.6. Finally, Fig. 4.7 presents the images of normal ICMP traffic record and Smurf attack record and Pod attack record.

As can be seen from Fig. 4.5a, the image represents the visual pattern of the EDM of normal TCP traffic record. The colour of an image point stands for the value of an element on the EDM. The lighter and warmer the colour is, the greater value the element has. In other words, the darkest cold blue colour areas on the image are the lowest value areas on the EDM, and conversely the lightest warm red colour areas on the image are the highest value areas on the EDM. Figs. 4.5b and 4.5c visualise the EDMs of Land attack record and Neptune attack record in the same manner respectively.



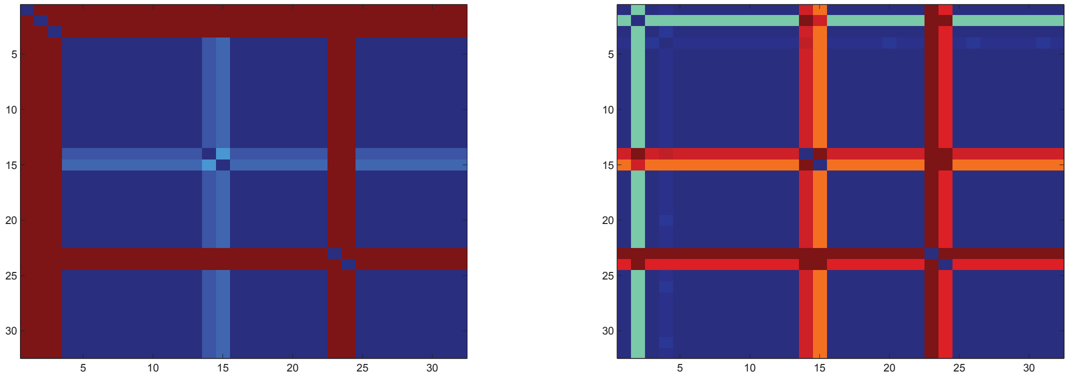
(a) Normal TCP traffic record

(b) Land attack traffic record

(c) Neptune attack traffic record

Figure 4.5: Images of the EDMs of normal TCP traffic record, Land attack record and Neptune attack record.

The images of the EDMs of the attacks show clear different visual patterns from that of the EDM of the normal TCP traffic record. Similarly, the images of the EDMs of the normal UDP traffic record and Teardrop attack record are exhibited in Fig. 4.6.



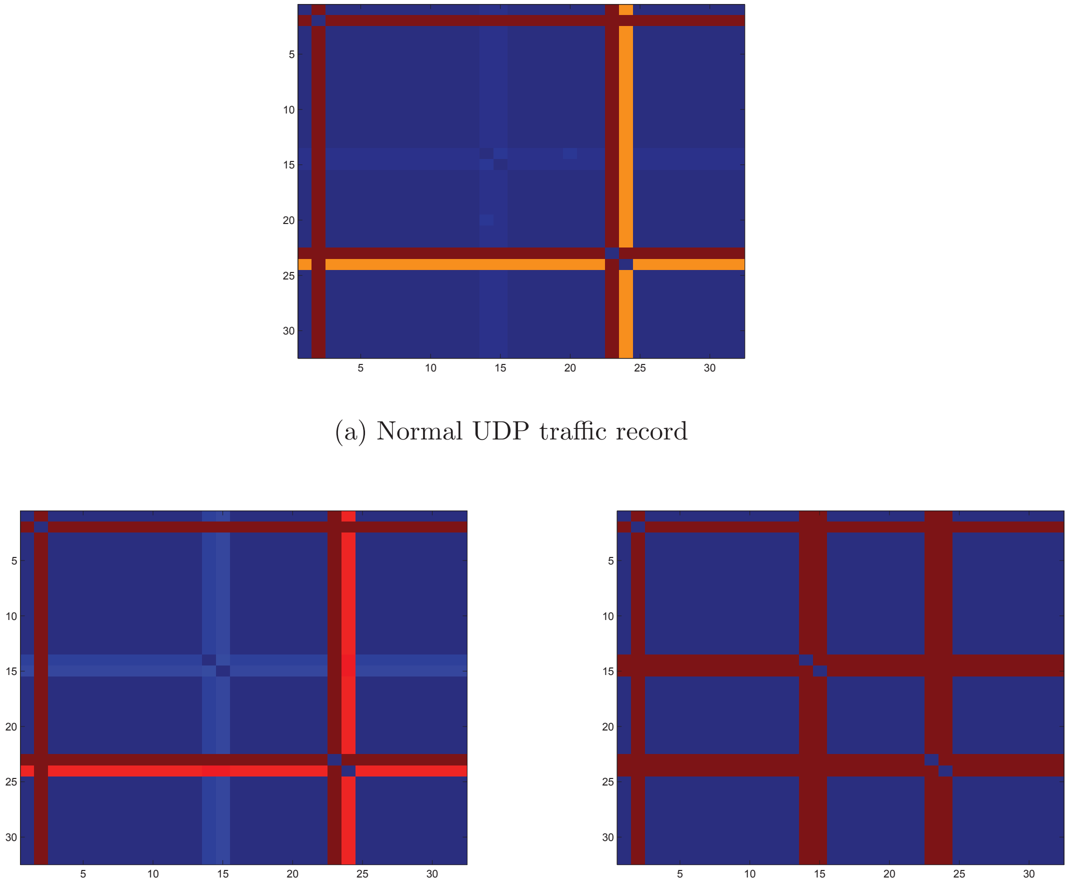
(a) Normal UDP traffic record

(b) Teardrop attack traffic record

Figure 4.6: Images of EDMs of UDP traffic record and Teardrop attack record.

The image of the EDM of the Teardrop attack record shows apparent dissimilarity to the image of the EDM of the normal UDP traffic. In addition, the images of the EDMs shown in Fig. 4.7 reveal that the behaviours of ICMP-based attacks, namely the Pod attack and the Smurf attack, are away from the normal ICMP traffic record as well.

The above evaluation results demonstrate that our proposed EDM-based MCA approach achieves promising performance in characterisation of various types of network traffic. Our results also suggest that, by taking advantage of the retained significant discriminative power, utilisation of the extracted multivariate correlations could improve the performance of DoS attack detection system. Moreover, by looking into the images, we can easily identify the visual patterns of the different traffic records.



(a) Normal UDP traffic record

(b) Pod attack traffic record

(c) Smurf attack traffic record

Figure 4.7: Images of EDMs of ICMP traffic record, Pod attack record and Smurf attack record.

Therefore, the proposed EDM-based MCA approach could be further applied to creating the statistical signatures of network intrusions. However, this is out of the scope of this thesis. To further inspect the above suggestions, we conduct evaluations on the detection of DoS attacks using the discriminative power provided by the EDM in Section 4.3.4.

4.3.4 Evaluation on DoS Attack Detection

In this section, 10 percent labelled data from the KDD Cup 99 dataset [84] is involved in the evaluation, in which three types of legitimate network traffic (i.e., TCP, UDP and ICMP traffic) and five types of DoS attack traffic (i.e., Teardrop, Smurf, Pod, Neptune and Land attacks) are chosen from the 10 percent labelled data. These selected data samples are then grouped into six different clusters with respect to their labels (i.e., Normal, Teardrop, Smurf, Pod, Neptune and Land). The detailed description of the clusters is found in Table 4.1.

Table 4.1: The Number of Records of Normal Traffic and Various of DoS Attack Traffic

Normal	Teardrop	Smurf	Pod	Neptune	Land
97,260	9,790	2,807,900	2,640	1,072,010	210

To give a comprehensive evaluation on the proposed DoS attack detection system based on the proposed EDM-based MCA approach, 10-fold cross-validations are conducted using both the original data and the data normalised using statistical normalisation technique [102]. This aims to investigate an assumption that classification is biased by the features with larger values in non-normalised data. Knowing the impact of the original data and the normalised data on the detection accuracy is critical to the proposed DoS attack detection system.

The results of the experimentations are shown and analysed in Section 4.3.4. The performance of the proposed detection system is compared with two state-of-the-art approaches to illustrate its effectiveness at the end of the section.

Evaluation Metrics

Five metrics are used to evaluate the proposed DoS attack detection system based on EDM-based MCA approach. They are True Negative Rate (TNR), Detection Rate (DR), False Positive Rate (FPR), False Negative Rate (FNR) and Accuracy. These metrics are defined as follows.

$$TNR = \frac{TN}{FP + TN}, \tag{4.3.1}$$

$$DR = \frac{TP}{TP + FN}, \tag{4.3.2}$$

$$FPR = 1 - TNR, \tag{4.3.3}$$

$$FNR = 1 - DR, \tag{4.3.4}$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \tag{4.3.5}$$

where TP, FP, TN and FN have the following meanings:

- True Positive (TP): the number of attacks correctly classified as attacks,
- False Positive (FP): the number of legitimate records incorrectly classified as attacks,
- True Negative (TN): the number of legitimate records correctly classified as legitimate records, and
- False Negative (FN): the number of attacks incorrectly classified as legitimate records.

A system which can achieve a high DR while retaining a low FPR is highly appreciated. In other words, a high detection accuracy rate is desired. To visually reveal the performance of our DoS attack detection system, Receiver Operating Characteristic (ROC) curve [63] is employed to show the relation between these two metrics, DR and FPR.

Process of Evaluation

In the evaluation, the 32 continuous features in each data record within the 10 percent labelled data coming form **Step 1** of the system framework shown in Fig. 4.1 are chosen. These features are analysed by the proposed EDM-based MCA approach in Step 2 of framework to extract the hidden correlations retaining in a data record and to provide high accurate characterisation for the respective network traffic.

Particularly, both the original data and the normalised data participate in **Step 2** during different sets of experimentations. The statistical technique [102] used in the normalisation of the original data takes both the mean scale of attribute values and their statistical distribution into account. It converts data derived from any normal distribution into standard normal distribution, in which 99.9% samples of the attribute are scaled into [-3, 3]. In addition, it has been proven that statistical normalisation improves detection performance of distance-based classifiers and outperforms other normalisation methods, such as mean range [0, 1], ordinal normalisation etc. [102]. The details of the statistical normalisation technique are shown as follows.

Considering the same arbitrary dataset $X = \{x_1, x_2, \cdots, x_n\}$ given in Section 4.1.1, the normalised value of feature f_j^i is given by (4.3.6).

$$\mathtt{f}_j^i = \frac{(f_j^i - \overline{f_j})}{\sigma_{f_j^i}}, \tag{4.3.6}$$

where

$$\bar{f_j} = \frac{1}{n}\sum_{i=1}^{n} f_j^i \tag{4.3.7}$$

is the mean of feature f_j^i, and

$$\sigma_{f_j^i} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(f_j^i - \bar{f}_j)^2} \tag{4.3.8}$$

is the standard deviation of feature f_j^i. The normalised traffic record x_i is represented by (4.3.9).

$$\begin{bmatrix} \mathtt{f}_1^i \\ \mathtt{f}_2^i \\ \vdots \\ \mathtt{f}_m^i \end{bmatrix}, \tag{4.3.9}$$

in which $1 \leq i \leq n$. In the following evaluation, the data is normalised in a batch manner. However, real-time normalisation can be achieved through the incremental learning [53] when our detection system is put on-line. The mean $\bar{f}_i$ can be updated as $\bar{f}_i = \bar{f}_i + \frac{x_{n+1}-\bar{f}_i}{n+1}$.

In **Step 3**, normal profiles are built with respect to the types of legitimate traffic (i.e., TCP, UDP and ICMP traffic) during the training phase. All the generated normal profiles are stored in the detection system for later use. During the test phase, the corresponding thresholds (i.e., $(\overline{Dis} - \alpha \times Std)$ and $(\overline{Dis} + \alpha \times Std)$) of the different normal profiles are determined by given the parameter α varying from 1 to 3 with an increment of 0.5. An observed sample is examined against the respective normal profile, which is built based on the normal traffic records transmitted using the same type of protocol. If the observed sample has a distance (i.e., $Dis_{observed}$) which exceeds the pre-determined thresholds, it is classified as a DoS attack. Otherwise, it is classified as normal traffic.

Results and Analysis

To illustrate the performance of our DoS attack detection system along with the change of the thresholds, the average TNRs for normal traffic records and the average DRs for individual types of DoS attack traffic records are shown in this section.

Results for Original Data The average detection performance of the proposed DoS attack detection system based on the EDM-based MCA approach on the original data against different thresholds is shown in Table 4.2.

Table 4.2: Average Detection Performance of the Proposed Attack Detection System on Original Data against Different Thresholds

Type of records	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
Normal	97.92%	98.47%	98.75%	98.99%	99.13%
Teardrop	100.00%	100.00%	100.00%	99.99%	99.98%
Smurf	100.00%	100.00%	100.00%	100.00%	100.00%
Pod	100.00%	100.00%	100.00%	100.00%	100.00%
Neptune	100.00%	100.00%	100.00%	99.99%	99.99%
Land	100.00%	100.00%	96.19%	87.62%	74.76%

The results in Table 4.2 demonstrate that our proposed attack detection system achieves encouraging performance in most of the cases throughout the experimentation. The rate of correct classification of Normal records rises from 97.92% to 99.13% along the increase of the threshold. Meanwhile, the Smurf attack records and the Pod attack records are completely detected without being affected by the change of the threshold. Moreover, the detection system achieves approximately 100% detection rate for the Teardrop attack records and the Neptune attack records in almost all cases. However, the detection system suffers serious degeneration in the Land attack when the threshold is set greater than 2σ, and the detection rate drops sharply down to 74.76% while the threshold is set equal to 3σ.

In Fig. 4.8, the relationship (i.e., the tradeoff) between the DRs and FPRs, achieved by our proposed attack detection system on original data, is revealed using ROC curves of various types of DoS attack traffic. The trends of the ROC curves of the attacks (i.e., Teardrop, Smurf, Pod and Neptune) are nearly flat and their ROC curves maintain a high level of DRs. However, the ROC curve of Land attack shows a sharp downslope.

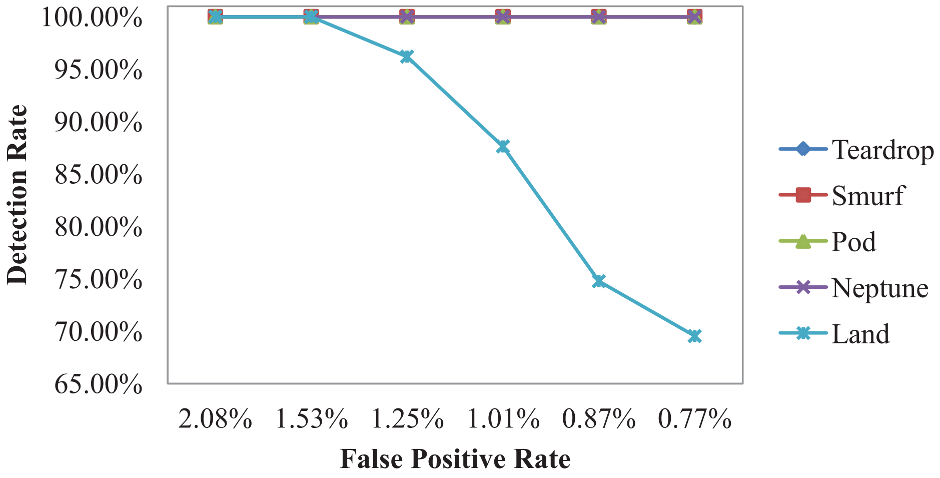


Figure 4.8: The ROC curves of various types of original DoS attack traffic data

To provide a better overview of the performance of our DoS attack detection system, the detection accuracy is highlighted in Table 4.3. It is clearly seen that the detection system achieves the highest accuracy (i.e., 99.91%) when the threshold is set to 1σ. Then, the accuracy rises gradually and slightly to 99.95% when the threshold increases to 3σ.

Table 4.3: Accuracy Achieved by the Proposed Detection System on Original Data against Different Thresholds

	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
Accuracy	99.91%	99.93%	99.94%	99.95%	99.95%

Results for Normalised Data Although the DoS attack detection system performs well on the original data as shown in Tables 4.2 and 4.3, the detection performance can be further improved by normalising the original data using the statistical normalisation technique presented in Section 4.3.4 before putting it into analysis and detection. The performance of the proposed DoS attack detection system achieving on the normalised data is shown in Table 4.4, and the detection accuracy is presented in Table 4.5.

As shown in Table 4.4, the proposed detection system can detect almost all attacks with 100% DRs. The detection rate of Land attack is also improved to 100% regardless of the change of the threshold. Although the detection system experiences a little degradation in detecting Pod attack, it is still able to achieve 98.11% DR in the worst case. In comparison with the TNR achieved on original data, the system gains a TNR (for legitimate traffic) that declined a bit to maximum 98.38% when the threshold is set to 3σ but it still manages to remain in the reasonable range.

Comparatively, the ROC curves of the attacks (such as Teardrop, Smurf, Pod, and Neptune) in Fig. 4.9 look closely similar to the ones shown in Fig. 4.8 except Land attack. Working with the normalised data enable our DoS attack detection system to reach a higher level of DR. The ROC curve of Land attack remains stable beyond the threshold of 2σ.

Table 4.4: Average Detection Performance of the Proposed Attack Detection System Based on Normalised Data against Different Thresholds

Type of records	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
Normal	96.49%	97.34%	97.82%	98.16%	98.38%
Teardrop	100.00%	100.00%	100.00%	100.00%	100.00%
Smurf	100.00%	100.00%	100.00%	100.00%	100.00%
Pod	99.77%	98.37%	98.30%	98.30%	98.11%
Neptune	100.00%	100.00%	100.00%	100.00%	100.00%
Land	100.00%	100.00%	100.00%	100.00%	100.00%

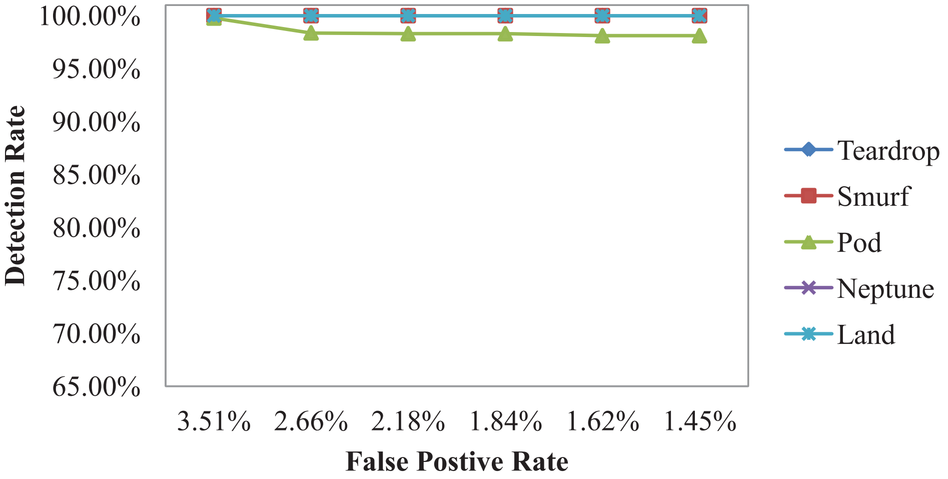


Figure 4.9: The ROC curves of various types of normalised DoS attack traffic data

Moreover, Table 4.5 shows that the normalised data boosts the accuracy of the proposed detection system slightly by 0.01% at the thresholds of 2σ and 3σ. In other words, the detection system achieves 99.95% accuracy in the case of 2σ threshold and 99.96% accuracy at threshold of 3σ when working with the normalised data.

Clearly, data do have positive influence on the proposed attack detection system, whose overall performance increases slightly when taking normalised data as the inputs. Although the results in Tables 4.4 and 4.5 show little improvements in

Table 4.5: Accuracy Achieved by the Proposed Detection System on Normalised Data against Different Thresholds

	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
Accuracy	99.91%	99.93%	99.95%	99.95%	99.96%

comparison with the ones (presented in Tables 4.2 and 4.3) achieved with the original data, the improvements are important to the proposed DoS attack detection system. Comparing Tables 4.2 and 4.4, our detection system achieves more promising DRs with the normalised data in Teardrop attack, Neptune attack and Land attack than the ones with the original data. Meanwhile, it underperforms in Normal traffic and Pod attack while working with the normalised data in comparison with the original data. However, the increase in the detection of Teardrop attack, Neptune attack and Land attack has a more significant impact on the detection accuracy than the decrease in the detection of Normal traffic and Pod attack. Especially, when the number of Land attack traffic increases, the detection accuracy decreases dramatically in the case of working with the original data. The difference between the detection accuracies using the two different data is 25.24% (= 100.00% - 74.76%).

Discussion and Comparison

Our analysis confirms that some original features with comparatively large values bias the detection system. This makes that the changes appearing in some other more important features with much smaller values can hardly take effect in distinguishing DoS attack traffic from legitimate traffic. This vitally degrades the discriminative power of the new feature set (i.e., $EDM^{lower}_{x_i^{normal}}$), which is not supposed to happen.

To illustrate the effectiveness of our proposed DoS attack detection system using

EDM-based MCA approach, comparisons are made against two state-of-the-art detection systems (i.e., the intrusion detection system based on covariance feature space [48] and the intrusion detection using nearest neighbour based on triangle area [98]). The best results of the individual detection systems are compared in this section. The results of the comparisons shown in Table 4.6 reveal that our system outperforms theses two state-of-the-art systems.

Table 4.6: Performance Comparisons with Different Detection Systems

	Threshold			
	Our detection system based on EDM-based MCA (with the original data and Threshold = 3σ)	Our detection system based on EDM-based MCA (with the normalised data and Threshold = 3σ)	The intrusion detection system based on covariance feature space (with 4D principle and Cov_len3_150) [48]	The intrusion detection using nearest neighbour based on triangle area [98]
DR	99.99%	100.00%	99.95%	99.53%
FPR	0.87%	1.62%	10.33%	2.99%

In terms of the performance of our proposed DoS attack detection system, it achieves around 99.99% DR when working with the original data and approximately 100.00% DR when working the normalised data. The FPR of our detection system with the original data is approximately 0.87%, and the one of our detection system with the normalised data is around 1.62%. On one hand, although it suffers a higher FPR with the normalised data, it provides better protection. Especially, when the number of Land attack traffic increases, the protection is more outstanding. On the other hand, the FPR can be reduced by using false positive reduction techniques [7].

4.4 Computational Complexity

In this section, we conduct an analysis on the computational complexity of our proposed DoS attack detection system using EDM-based MCA approach in two folds, namely the complexity of the proposed EDM-based MCA approach and the complexity of the detection process in our proposed attack detection system.

On one hand, as discussed in Section 4.1, Euclidean distances between any two distinct features in a traffic record need to be computed when processing our proposed EDM-based MCA approach. Since each traffic record has m features (or dimensions), $\frac{m(m-1)}{2}$ Euclidean distances are calculated and are used to construct a $EDM_{x_i}^{lower}$. Thus, the proposed MCA approach has a computational complexity of $O(m^2)$. **On the other hand**, as explained in Section 4.2, the MD between the observed feature vector (i.e., the $EDM_{x_i}^{lower}$) and the expectation (i.e., $\overline{EDM_{X^{normal}}^{lower}}$) of the respective normal profile needs to be computed in the detection process of our proposed detection system to evaluate the level of the dissimilarity between them. Thus, this computation incurs a complexity of $O(M^2)$, in which $M = \frac{m(m-1)}{2}$ is the dimensions of $EDM_{x_i}^{lower}$. $O(M^2)$ can be written as $O(m^4)$. By taking the computational complexities of the proposed MCA and the detection process of our proposed detection system into account, the overall computational complexity of the proposed detection system is $O(m^2) + O(m^4) = O(m^4)$. However, m is a fixed number which is 32 in our case, so that the overall computational complexity is indeed equal to $O(1)$.

The computational complexities of the other two state-of-the-art detection systems compared in Section 4.3.4 are analysed in the following. Network intrusion detection system based on covariance feature space [48] incurs a computational complexity of $O(2n \times \frac{m \times (m+1)}{2}) = O(nm^2)$ in data preprocessing, where n is the number of sequential samples in a group and m is the number of physical features of a sample. In attack detection, the observed covariance matrix of a group of sequential samples needs to be compared with all l known classes/clusters. Therefore, it has a computational complexity of $O(lm^2)$. The overall computational complexity of the network intrusion detection system based on covariance feature space is $O(nm^2) + O(lm^2) = O(lm^2)$.

The intrusion detection system using nearest neighbour based on triangle area [98] suffers a heavier overall computational complexity. In data processing and attack detection phases, the computational complexities are $O(ml^2)$ and $O(l^2n^2)$ respectively, where m is the number of features (or dimensions) in a traffic record, l is the number of clusters used in generating triangle areas and n is the number of training samples. The overall complexity is $O(ml^2) + O(l^2n^2) = O(l^2n^2)$. In real network environments, the types of attacks and the number of available training samples are often varying. Thus, the computational complexities of these two state-of-the-art detection systems cannot be constants.

In general, our proposed DoS detection system can achieve better computational complexity than the above two other systems. Table 4.7 is provided to summarize the computational complexities of the above discussed approaches.

Table 4.7: Computational Complexities of Different State-of-the-art Detection Approaches

The proposed attack detection system based on EDM-based MCA approach	Network intrusion detection system based on covariance feature space [48]	Intrusion detection system using nearest neighbour based on triangle area [98]
$O(1)$	$O(lm^2)$	$O(l^2n^2)$

4.5 Summary

This chapter has proposed a MCA approach based on EDM to extract the multivariate correlations between two distinct features of a network traffic record. This proposed MCA approach can better exhibit the network traffic behaviours. We have evaluated the effectiveness of the proposed MCA approach in network traffic characterisation on the records of Normal traffic and various types of DoS attack traffic from the KDD Cup 99 dataset. The results illustrate that the extracted information can clearly reveal the correlations between features and accurately characterise the various types of traffic, and the information can clearly reveal the changes of network behaviour caused by DoS attacks.

Moreover, this chapter has also proposed a DoS attack detection system using EDM-based MCA approach. We have evaluated the proposed attack detection system on the KDD Cup 99 dataset as well. The detection system has achieved encouraging detection accuracy on both the original data and the normalised data. It outperforms the other two state-of-the-art systems (i.e., the network intrusion detection system based on covariance feature space and the intrusion detection system using nearest neighbour based on triangle area) completely.

However, the false positive rate of our detection system needs to be further reduced in order to release network administrators from being disrupted by frequent shown false alarms. Thus, we will employ more sophisticated classification techniques in our future work to alleviate the false positive rate.

Chapter 5

Multivariate Correlation Analysis Based on Triangle Area Map

Multivariate correlation analysis has been a rising trend in the research areas of network intrusion detection. Recent studies on feature correlation analysis have gained progresses and helped improve the accuracy of attack detection. Various kinds of analysis techniques were introduced by these early research works to the task of multivariate correlation extraction. These analysis techniques are systematically classified into two different categories (i.e., the payload-based analysis techniques and the flow-based analysis techniques) with respective to the types of objects, which they are intended to study.

In terms of **payload-based analysis**, the analysis techniques, such as the Geometrical Structure Anomaly Model (GSAD) [46], feature correlation analysis approach based on Linear Discriminant Analysis (LDA) [87], RePIDS [45] and so on, were developed to study the multivariate correlations that reside in network traffic packet payloads. This type of MCA techniques/approaches enables the discovery of the patterns of the analysed network traffic packet payloads. However, these techniques are ineligible to extract the patterns of the flow-based information of network traffic.

In terms of **flow-based analysis**, the MCA techniques, such as the covariance-matrix-based approach [48], the triangle-area-based approach [98], correlation-coefficient-based approach [108] and so on, were proposed to analyse the multivariate correlations retained by network traffic flows. While these MCA techniques/approaches show encouraging performance in extracting the correlation between the features/statistics of network traffic flows during the experimentation, they have dependency on the prior knowledge of the behaviours of network traffic during the process of analysis.

Adopting this idea, we have proposed the EDM-based MCA approach in Chapter 4, which not only provides efficient and accurate characterisation to various types of network traffic, but also is free from the aforementioned problems. However, it would be even more appreciated if the computational cost of the process of multivariate correlation analysis could be further reduced. As such, in this chapter, we suggest another MCA approach that employs Triangle Area Map (TAM) in extracting multivariate correlations between the features. This new MCA approach is developed based on one of our works published in [88].

In order to evaluate the effectiveness of the TAM-based MCA approach on the detection of DoS attacks, we design an anomaly-based IDS using the proposed TAM-based MCA approach for the task. This anomaly-based IDS is designed based on one of our works published in [93]. Its performance is tested using the KDD 99 CUP dataset [84].

The rest of this chapter is organised as follows. Section 5.1 proposes a novel MCA approach in which TAM is used for multivariate correlation extraction. A DoS attack detection system based on the TAM-based MCA approach is proposed in Section 5.2. The evaluations on the efficiency of the proposed TAM-based MCA approach in characterising various types of network traffic and on the developed DoS attack detection system are presented in Section 5.3. The computational complexity and the time cost of the proposed DoS attack detection system are then evaluated and shown in Section 5.4. Finally, the summary is drawn in Section 5.5.

5.1 Multivariate Correlation Analysis Approach

A new approach is proposed in this section to enhance and speed up the multivariate correlation analysis approach proposed in Chapter 4. This new MCA approach is developed based on triangle area map technique, which is used to present the correlations within network traffic data. The occurrence of DoS attacks causes the change of the network traffic behaviour, which in turn affects the correlations. Thus, the correlations can help indicate the suspicious change of the network traffic behaviour.

These correlations are extracted from the basic statistical properties (e.g., the number of data bytes from source to destination, the length of a connection and the number of connections to the same host as the current connection in the past two seconds etc.) of the network traffic flows in a prompt fashion. The extracted correlations give accurate descriptions to the behaviours of various types of network traffic. The description vectors representing network traffic records are constructed using these newly extracted correlations of the respective traffic records. The details are shown in the following section.

5.1.1 Multivariate Correlation Extraction

Considering the same arbitrary dataset $X = [x_1\, x_2\, \cdots\, x_n]$ given in Chapter 4, where

$$x_i = \begin{bmatrix} f_1^i \\ f_2^i \\ \vdots \\ f_m^i \end{bmatrix}$$

represents the i^{th} m-dimensional traffic record, and i is ranged from 1 to n. The dataset X can now be represented explicitly in (5.1.7).

$$X = \begin{bmatrix} f_1^1 & f_1^2 & \cdots & f_1^n \\ f_2^1 & f_2^2 & \cdots & f_2^n \\ \vdots & \vdots & \ddots & \vdots \\ f_m^1 & f_m^2 & \cdots & f_m^n \end{bmatrix}, \tag{5.1.1}$$

where f_l^i is the value of the l^{th} feature in the i^{th} traffic record, and l and i are varying from 1 to m and from 1 to n respectively.

In this scheme, the concept of triangle area rather than Euclidean distance is applied to extract the geometrical correlation between the features f_j^i and f_k^i, where j and k are varying from 1 to m, in the vector x_i. In order to obtain the triangle formed by these two features (i.e., f_j^i and f_k^i), data transformation is involved, where the vector x_i is first projected onto the (j, k)-th two-dimensional Euclidean subspace as defined in (5.1.2).

$$y_{i,j,k} = [\varepsilon_j\ \varepsilon_k]^T x_i = \begin{bmatrix} f_j^i \\ f_k^i \end{bmatrix}, \tag{5.1.2}$$

where $j \neq k$, and the vectors ε_j and ε_k are two unit vectors given in (5.1.3) and

(5.1.4).

$$\varepsilon_j = \begin{bmatrix} e_{j,1} \\ e_{j,2} \\ \vdots \\ e_{j,m} \end{bmatrix}, \tag{5.1.3}$$

and

$$\varepsilon_k = \begin{bmatrix} e_{k,1} \\ e_{k,2} \\ \vdots \\ e_{k,m} \end{bmatrix}, \tag{5.1.4}$$

in which all the elements are with values of zero, except the (j, j)-th element and the (k, k)-th element whose values are ones in ε_j and ε_k respectively.

The $y_{i,j,k}$ shown in (5.1.2) can be interpreted as a two-dimensional column vector, which can also be defined as a point on the Cartesian coordinate system in the (j, k)-th two-dimensional Euclidean subspace with a coordinate $(f_j^i,\ f_k^i)$. Then, on the Cartesian coordinate system, a triangle $\Delta f_j^i O f_k^i$, formed by the origin (i.e., O) and the projected points of the coordinate $(f_j^i,\ f_k^i)$ on the j-axis and k-axis, is found. Its area $Tr_{j,k}^i$ is defined as (5.1.5).

$$Tr_{j,k}^i = (\parallel (f_j^i, 0) - (0, 0) \parallel \times \parallel (0, f_k^i) - (0, 0) \parallel)/2, \tag{5.1.5}$$

where $1 \leq i \leq n$, $1 \leq j \leq m$, $1 \leq k \leq m$ and $j \neq k$.

To make a complete analysis, all possible permutations of any two distinct features in the vector x_i are extracted, and the respective triangle areas are computed. A TAM is constructed and all the triangle areas are arranged on the map with respect to their indexes. For example, the $Tr_{j,k}^i$ is positioned on the j^{th} row and the k^{th} column of the map TAM_{x^i} given in (5.1.6).

$$TAM_{x_i} = \begin{bmatrix} 0 & Tr^i_{1,2} & \cdots & Tr^i_{1,m} \\ Tr^i_{2,1} & 0 & \cdots & Tr^i_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ Tr^i_{m,1} & Tr^i_{m,2} & \cdots & 0 \end{bmatrix}_{m\times m} . \tag{5.1.6}$$

The values of the elements on the diagonal of the map are set to zeros ($Tr^i_{j,k} = 0$, if $j = k$) because we only care about the correlation between each pair of distinct features. For the non-diagonal elements $Tr^i_{j,k}$ and $Tr^i_{k,j}$ where $j \neq k$, they indeed represent the areas of the same triangle. This infers that the values of $Tr^i_{j,k}$ and $Tr^i_{k,j}$ are actually equal. Hence, the TAM_{x^i} is a symmetric matrix having the elements with the values of zero on the main diagonal.

For the aforementioned arbitrary dataset X, its geometrical multivariate correlations can be extracted using the proposed TAM-based MCA approach and is represented by (5.1.7).

$$X_{TAM} = [TAM_{x_1}, TAM_{x_2}, \cdots, TAM_{x_n}]_{m\times m\times n}. \tag{5.1.7}$$

5.1.2 Example and Discussion

To provide a clear picture of how the proposed TAM-based MCA approach works, an example is used for illustration as follows. Given a feature vector

$$x_{ex} = \begin{bmatrix} 1 \\ 3 \\ 5 \end{bmatrix},$$

whose triangle area map TAM_{ex} is obtained by first placing the vector x_{ex} into a 3-Dimensional (3D) feature space formed by three orthogonal unit vectors ε_1, ε_2 and

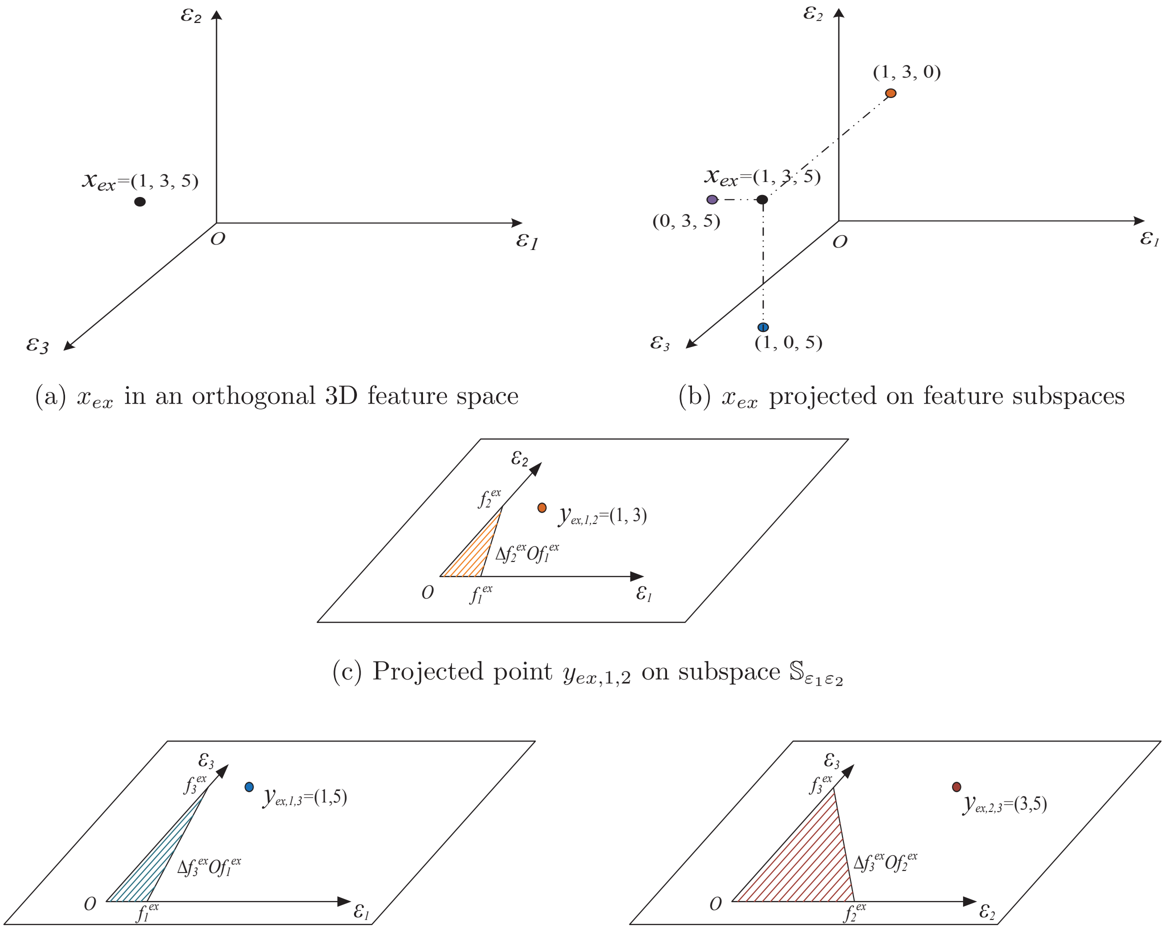
ε_3.

$$\begin{array}{c} \begin{matrix} \varepsilon_1 & \varepsilon_2 & \varepsilon_3 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array}$$

The x_{ex} is now a point in the 3D space as shown in Fig. 5.1a. The projected points on three distinct subspaces $\mathbb{S}_{\varepsilon_1\varepsilon_2}$, $\mathbb{S}_{\varepsilon_1\varepsilon_3}$ and $\mathbb{S}_{\varepsilon_2\varepsilon_3}$ within the 3D space are denoted as $A(1,3,0)$, $B(1,0,5)$ and $C(0.3.5)$ shown in Fig. 5.1b respectively.

When we analyse these projected points of x_{ex} in 2D spaces rather than a 3D space, the projected points on the subspaces $\mathbb{S}_{\varepsilon_1\varepsilon_2}$, $\mathbb{S}_{\varepsilon_1\varepsilon_3}$ and $\mathbb{S}_{\varepsilon_2\varepsilon_3}$ are then redefined as $y_{ex,1,2}$, $y_{ex,1,3}$ and $y_{ex,2,3}$ and shown in Figs. 5.1c, 5.1d and 5.1e respectively. The corresponding values of the projected points are $y_{ex,1,2} = [\varepsilon_1 \;\; \varepsilon_2]^T x_{ex} = [f_1^{ex} \;\; f_2^{ex}]^T = [1 \;\; 3]^T$, $y_{ex,1,3} = [\varepsilon_1 \;\; \varepsilon_3]^T x_{ex} = [f_1^{ex} \;\; f_3^{ex}]^T = [1 \;\; 5]^T$ and $y_{ex,2,3} = [\varepsilon_2 \;\; \varepsilon_3]^T x_{ex} = [f_2^{ex} \;\; f_3^{ex}]^T = [3 \;\; 5]^T$.

Then, the points $y_{ex,1,2}$, $y_{ex,1,3}$ and $y_{ex,2,3}$ are further projected on the axes of the respective subspaces. Triangles on the three subspaces $\mathbb{S}_{\varepsilon_1\varepsilon_2}$, $\mathbb{S}_{\varepsilon_1\varepsilon_3}$ and $\mathbb{S}_{\varepsilon_2\varepsilon_3}$ are constructed by connecting any two of the points (i.e., f_1^{ex}, f_2^{ex} and f_3^{ex}) and the origin O. These triangles are denoted by $\Delta f_2^{ex} O f_1^{ex}$, $\Delta f_3^{ex} O f_1^{ex}$ and $\Delta f_3^{ex} O f_2^{ex}$ and shown in Figs. 5.1c, 5.1d and 5.1e respectively. The areas (i.e., $Tr_{2,1}^{ex}$, $Tr_{3,1}^{ex}$ and $Tr_{3,2}^{ex}$) of the triangles (i.e., $\Delta f_2^{ex} O f_1^{ex}$, $\Delta f_3^{ex} O f_1^{ex}$ and $\Delta f_3^{ex} O f_2^{ex}$) are computed using (5.1.5), and the values are shown as follows.



(a) x_{ex} in an orthogonal 3D feature space

(b) x_{ex} projected on feature subspaces

(c) Projected point $y_{ex,1,2}$ on subspace $\mathbb{S}_{\varepsilon_1\varepsilon_2}$

(d) Projected point $y_{ex,1,3}$ on subspace $\mathbb{S}_{\varepsilon_1\varepsilon_3}$

(e) Projected point $y_{ex,2,3}$ on subspace $\mathbb{S}_{\varepsilon_2\varepsilon_3}$

Figure 5.1: Geometrical structure of features

$$\begin{cases} Tr^{ex}_{2,1} = (\parallel (3,0)-(0,0) \parallel \times \parallel (0,1)-(0,0) \parallel)/2 = 1.5, \\ Tr^{ex}_{3,1} = (\parallel (5,0)-(0,0) \parallel \times \parallel (0,1)-(0,0) \parallel)/2 = 2.5, \\ Tr^{ex}_{3,2} = (\parallel (5,0)-(0,0) \parallel \times \parallel (0,3)-(0,0) \parallel)/2 = 7.5. \end{cases}$$

Due to the fact that $Tr^{ex}_{j,k}$ and $Tr^{ex}_{k,j}$ refer to the area of the same triangle $\Delta f^{ex}_j O f^{ex}_k$, where $1 \leq j \leq 3$, $1 \leq k \leq 3$ and $j \neq k$, the corresponding triangle area map TAM_{ex}

is defined using the above triangle areas (i.e., $Tr^{ex}_{2,1}$, $Tr^{ex}_{3,1}$ and $Tr^{ex}_{3,2}$) and given as follows.

$$TAM_{ex} = \begin{bmatrix} 0 & Tr^{ex}_{1,2} & Tr^{ex}_{1,3} \\ Tr^{ex}_{2,1} & 0 & Tr^{ex}_{2,3} \\ Tr^{ex}_{3,1} & Tr^{ex}_{3,2} & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1.5 & 2.5 \\ 1.5 & 0 & 7.5 \\ 2.5 & 7.5 & 0 \end{bmatrix}.$$

It is worth notice that when our proposed TAM-based MCA approach is put into practice, the computation of the $Tr^{i}_{j,k}$ defined in (5.1.5) can be simplified as given in (5.1.8).

$$Tr^{i}_{j,k} = (|f^{i}_{j}| \times |f^{i}_{k}|)/2. \tag{5.1.8}$$

This is because the value of the $Tr^{i}_{j,k}$ is eventually equal to half of the product of the absolute values of the features f^{i}_{j} and f^{i}_{k}. Thus, the transformation shown in (5.1.2) can be eliminated and the process of multivariate correlation extraction can be speeded up by more than one-third.

Besides, this example also shows four unique merits of our TAM-based MCA approach in data analysis in comparison with other state-of-the-art MCA approaches, and the merits are shown as follows.

- First, it does not require the knowledge of historic traffic (i.e., both legitimate and illegitimate traffic) in performing analysis.

- Second, unlike the Covariance matrix approaches proposed in [48] which is vulnerable to linear change of all features, our proposed TAM-based MCA withstands the problem.

- Third, it provides accurate characterisation for individual network traffic records rather than model network traffic behaviour of a group of network traffic records.

This results in lower latency in decision making and enable sample-by-sample detection. Thus, prompt response to attacks can be taken.

- Fourth, the correlations between distinct pairs of features are revealed through the geometrical structure analysis. Changes of these structures may occur when anomaly behaviours appear in the network. This provides an important signal to trigger an alert.

5.2 Network Intrusion Detection Using Multivariate Correlation Analysis Based on Triangle Area Map

Similar to Section 4.2, the contributions of our TAM-based MCA approach to DoS attack detection are evaluated in this section. To do so, a new DoS attack detection system is designed based on the general system framework proposed in Chapter 3. The TAM-based MCA approach is applied in Step 2 of the architecture and plays a key role in the analysis of the correlations within network traffic records.

The overview of the proposed DoS attack detection system is given in Section 5.2.1. The details of the Training Phase and the Test Phase in Step 3 of the framework are given in Sections 5.2.2 and 5.2.3.

5.2.1 Framework

The framework of our proposed DoS attack detection system is presented in this section. This system framework coincides with the architecture of the general detection system framework shown in Fig. 3.1. The anomaly-based detection mechanism and

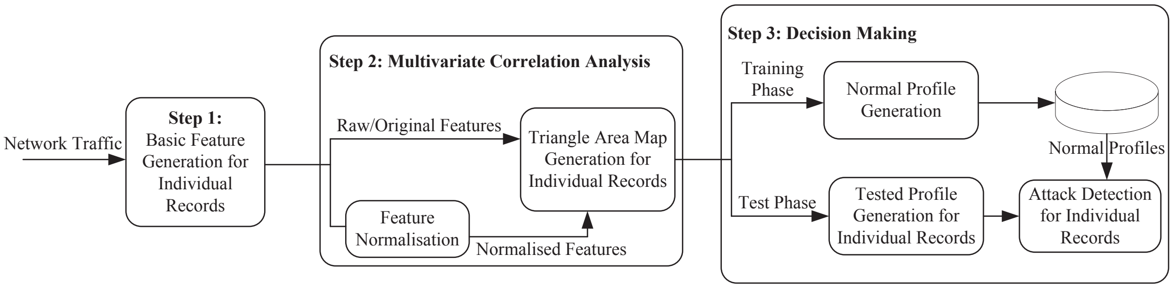

Network Traffic
Step 1:
Basic Feature Generation for Individual Records
Step 2: Multivariate Correlation Analysis
Raw/Original Features
Triangle Area Map Generation for Individual Records
Feature Normalisation
Normalised Features
Step 3: Decision Making
Training Phase
Normal Profile Generation
Normal Profiles
Test Phase
Tested Profile Generation for Individual Records
Attack Detection for Individual Records

Figure 5.2: A system framework for denial-of-service attack detection using multivariate correlation analysis based on triangle area map

the other mechanisms discussed in Sections 3.1.1-3.1.3 enable this newly proposed detection system to effectively recognise known and unknown network intrusions.

This system framework deviates from the reference detection system framework in Step 2, where the Triangle Area Map Generation module other than a general conceptual MCA module is introduced to function as an traffic analyser in this new detection system. Apart from that, the system framework shown in Fig. 5.2 includes a Feature Normalisation module in Step 2, where the same normalising technique [102] used in Chapter 4 is adopted.

The Triangle Area Map Generation module in Step 2 applies the TAM-based MCA approach to extract the correlations between two distinct features within each traffic record, which either comes from Step 1 or from the Feature Normalisation module in the same step (i.e., Step 2). The occurrence of network intrusions causes changes to these correlations so that the changes can be used as indicators to identify the intrusive activities. All the extracted correlations, namely triangle areas stored in TAMs, are then used to replace the original basic features or the normalised features to represent the traffic records. This provides higher discriminative information to differentiate between legitimate and illegitimate traffic records. These TAMs are then used in the Training Phase and the Test Phase in Step 3. The relevant algorithms are presented are detailed in Sections 5.2.2 and 5.2.3 respectively.

In order to maintain the efficiency of the system, we suggest to reduce the computation in the process of detection by examining only the upper triangle or the lower triangle of the TAM of a tested network traffic record. This suggestion is based on the fact that TAMs are symmetric matrices, in which any differences, identified on the upper triangles of the images, can be found on their lower triangles as well. Therefore, to perform a quick comparison of the two TAMs, we can choose to investigate either the upper triangles or the lower triangles of the TAMs only. This produces the same result as comparing using the entire TAMs. Therefore, the correlations residing in a traffic record x_i can be represented effectively and correctly by the upper triangle or the lower triangle of the respective TAM (i.e., TAM_{x_i}). For consistency, we consider the lower triangles of TAMs in the following sections. The lower triangle of the TAM_{x_i} is converted into a new correlation vector $TAM_{x_i}^{lower}$ as denoted in (5.2.1).

$$\begin{aligned} TAM_{x_i}^{lower} = [&Tr_{2,1}^{x_i}\ Tr_{3,1}^{x_i}\ \cdots\ Tr_{m,1}^{x_i}\ Tr_{3,2}^{x_i} \\ &Tr_{4,2}^{x_i}\ \cdots\ Tr_{m,2}^{x_i}\ \cdots\ Tr_{m,m-1}^{x_i}]_{\frac{m\times(m-1)}{2}}^{T}\ . \end{aligned} \tag{5.2.1}$$

Now, given the same set of g m-dimensional normal training network traffic records (i.e., $X^{normal} = [x_1^{normal}\ x_2^{normal}\ \cdots\ x_g^{normal}]$) considered in Section 4.2.1, these network traffic records are denoted by the lower triangles of the TAMs extracted using our proposed TAM-based MCA approach, namely

$$X_{TAM}^{normal} = [TAM_{x_1^{normal}}^{lower}\ TAM_{x_2^{normal}}^{lower}\ \cdots\ TAM_{x_g^{normal}}^{lower}],$$

where

$$TAM^{lower}_{x_i^{normal}} = \begin{bmatrix} Tr^{x_i^{normal}}_{2,1} \\ Tr^{x_i^{normal}}_{3,1} \\ \vdots \\ Tr^{x_i^{normal}}_{m,m-1} \end{bmatrix}_{\frac{m\times(m-1)}{2}}$$

and $1 \leq i \leq g$. Additionally, an observed network traffic record (i.e., $x^{observed}$) is denoted by the lower triangle of its TAM extracted using the TAM-based MCA approach, namely

$$TAM^{lower}_{x^{observed}} = \begin{bmatrix} Tr^{x^{observed}}_{2,1} \\ Tr^{x^{observed}}_{3,1} \\ \vdots \\ Tr^{x^{observed}}_{m,m-1} \end{bmatrix}_{\frac{m\times(m-1)}{2}} .$$

The training phase and the test phase of the proposed DoS attack detection system are presented in Sections 5.2.2 and 5.2.3 based on the above given training and test samples.

5.2.2 Training Phase

In this section, we provide a detailed discussion about the Training Phase and present the relevant algorithm in Fig. 5.3. As the main task in the Training Phase, building profiles for various types of legitimate network traffic is done through the density estimation of the similarities between the given normal traffic records and the expectation of the legitimate traffic.

MD is adopted to measure the similarity between network traffic records, due to the fact that MD has been successfully and widely used in cluster analysis, classification and multivariate outlier detection techniques. Moreover, unlike Euclidean distance and Manhattan distance, it evaluates distance between two multivariate data objects by taking the correlations between variables into account and removing the dependency on the scale of measurement during the calculation.

```
Require: A dataset $X_{TAM}^{normal}$ {It contains the lower triangles of the TAMs of the $g$
    normal training, and each of which has $\frac{m \times (m-1)}{2}$ features.}
 1: Initialise $DIS$ {It is an array with $g$ elements denoted by $Dis_i (1 \leq i \leq g)$.}
 2: $\overline{TAM_{X^{normal}}^{lower}} \leftarrow \frac{1}{g} \sum_{i=1}^{g} TAM_{x_i^{normal}}^{lower}$
 3: Generate covariance matrix $Cov$ for $X_{TAM}^{normal}$ using (5.2.3)
 4: for $i = 1$ to $g$ do
 5:     $Dis_i \leftarrow MD(TAM_{x_i^{normal}}^{lower}, \overline{TAM_{X^{normal}}^{lower}})$ {Mahalanobis distance between
        $TAM_{x_i^{normal}}^{lower}$ and $\overline{TAM_{X^{normal}}^{lower}}$ computed using (5.2.2)}
 6: end for
 7: $\overline{Dis} \leftarrow \frac{1}{g} \sum_{i=1}^{g} Dis_i$
 8: $Std \leftarrow \sqrt{\frac{1}{g-1} \sum_{i=1}^{g} (Dis_i - \overline{Dis})^2}$
 9: $Pro \leftarrow (N(\overline{Dis}, Std^2), \overline{TAM_{X^{normal}}^{lower}}, Cov)$
10: return $Pro$
```

Figure 5.3: An algorithm for normal profile generation based on TAM-based MCA approach.

During the estimation of the density of the MDs (e.g., Dis_i) between the given normal traffic records (e.g., $TAM_{x_i^{normal}}^{lower}$) and the expectation (i.e., $\overline{TAM_{X^{normal}}^{lower}}$) of the g legitimate training traffic records as shown between the lines 4 and 6 of Fig. 5.3. The probability distribution of the MDs is determined by two parameters (i.e., the mean $\overline{Dis}$ and the standard deviation Std of the distances) as described in the algorithm shown in lines 7 and 8 of Fig. 5.3. The MD (i.e., Dis_i) between the $TAM_{x_i^{normal}}^{lower}$ and the $\overline{TAM_{X^{normal}}^{lower}}$ is computed using (5.2.2), and the covariance matrix (i.e., Cov) involved in (5.2.2) can be obtained using (5.2.3).

$$Dis_i = \sqrt{\frac{(TAM_{x_i^{normal}}^{lower} - \overline{TAM_{X^{normal}}^{lower}})^T (TAM_{x_i^{normal}}^{lower} - \overline{TAM_{X^{normal}}^{lower}})}{Cov}}, \qquad (5.2.2)$$

and

$$Cov = \begin{bmatrix} \sigma_{Tr_{2,1}^{X^{normal}} Tr_{2,1}^{X^{normal}}} & \sigma_{Tr_{2,1}^{X^{normal}} Tr_{3,1}^{X^{normal}}} & \cdots & \sigma_{Tr_{2,1}^{X^{normal}} Tr_{m,m-1}^{X^{normal}}} \\ \sigma_{Tr_{3,1}^{X^{normal}} Tr_{2,1}^{X^{normal}}} & \sigma_{Tr_{3,1}^{X^{normal}} Tr_{3,1}^{X^{normal}}} & \cdots & \sigma_{Tr_{3,1}^{X^{normal}} Tr_{m,m-1}^{X^{normal}}} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{Tr_{m,m-1}^{X^{normal}} Tr_{2,1}^{X^{normal}}} & \sigma_{Tr_{m,m-1}^{X^{normal}} Tr_{3,1}^{X^{normal}}} & \cdots & \sigma_{Tr_{m,m-1}^{X^{normal}} Tr_{m,m-1}^{X^{normal}}} \end{bmatrix}. \tag{5.2.3}$$

The covariance (e.g., $\sigma_{Tr_{j,k}^{X^{normal}} Tr_{l,v}^{X^{normal}}}$) between two arbitrary elements (e.g., $Tr_{j,k}^{X^{normal}}$ and $Tr_{l,v}^{X^{normal}}$) in the lower triangle of the TAM of the i-th normal traffic record is defined in (5.2.4).

$$\begin{aligned} \sigma_{Tr_{j,k}^{X^{normal}} Tr_{l,v}^{X^{normal}}} = \frac{1}{g-1} \sum_{i=1}^{g} & (Tr_{j,k}^{x_i^{normal}} - \mu_{Tr_{j,k}^{X^{normal}}}) \\ & (Tr_{l,v}^{x_i^{normal}} - \mu_{Tr_{l,v}^{X^{normal}}}) \,, \end{aligned} \tag{5.2.4}$$

where $2 \leq j \leq m$, $2 \leq l \leq m$, $1 \leq k \leq (m-1)$ and $1 \leq v \leq (m-1)$. Moreover, the mean (i.e., $\mu_{Tr_{j,k}^{X^{normal}}}$) of the (j,k)-th elements and the mean (i.e., $\mu_{Tr_{l,v}^{X^{normal}}}$) of the (l,v)-th elements in the lower triangles of the TAMs over g legitimate training traffic records are defined in (5.2.5) and (5.2.6) respectively.

$$\mu_{Tr_{j,k}^{X^{normal}}} = \frac{1}{g} \sum_{i=1}^{g} Tr_{j,k}^{x_i^{normal}} \,, \tag{5.2.5}$$

and

$$\mu_{Tr_{l,v}^{X^{normal}}} = \frac{1}{g} \sum_{i=1}^{g} Tr_{l,v}^{x_i^{normal}} \,. \tag{5.2.6}$$

As shown in Fig. 5.3, the distribution of the MDs is described by the two parameters, namely the mean $\overline{Dis}$ and the standard deviation Std of the MDs. Finally, the obtained distribution $N(\overline{Dis}, Std^2)$ of the normal training traffic records, the $\overline{TAM_{X^{normal}}^{lower}}$ and the Cov are stored in the normal profile Pro, which is then kept in the database of normal profiles as shown in Fig. 5.2, for attack detection.

```
Require: The $TAM^{lower}_{x^{observed}}$ of a tested sample $x^{observed}$, normal traffic profile $Pro$ :
    $(N(\overline{Dis}, Std^2), \overline{TAM^{lower}_{X^{normal}}}, Cov)$ and parameter $\alpha$
1: $Dis_{observed} \leftarrow MD(TAM^{lower}_{x^{observed}}, \overline{TAM^{lower}_{X^{normal}}})$ {Mahalanobis distance between
    $TAM^{lower}_{x^{observed}}$ and $\overline{TAM^{lower}_{X^{normal}}}$ computed using (5.2.7)}
2: if $(\overline{Dis} - \alpha \times Std) \leq Dis_{observed} \leq (\overline{Dis} + \alpha \times Std)$ then
3:     return Normal
4: else
5:     return Attack
6: end if
```

Figure 5.4: An algorithm for attack detection based on TAM-based MCA approach.

5.2.3 Test Phase

In this section, an algorithm for attack detection is proposed to be used in the test phase of Step 3 in Fig. 5.2, and it is given in Fig. 5.4. Tested (or observed) network traffic records (e.g., $x^{observed}$) are examined individually against the respective normal profiles (e.g., $Pro : (N(\overline{Dis}, Std^2), \overline{TAM^{lower}_{X^{normal}}}, Cov))$, which are generated in the training phase discussed in Section 5.2.2. The descriptor $TAM^{lower}_{x^{observed}}$ of an observed network traffic $x^{observed}$, the respective normal profile Pro and the parameter α are the required inputs of the detection algorithm shown in Fig. 5.4. The similarity between the observed record $x^{observed}$ and the expectation $\overline{TAM^{lower}_{X^{normal}}}$ of the respective type of legitimate network traffic is evaluated as defined in line 1 of Fig. 5.4 using (5.2.7), namely the Mahalanobis distance.

$$Dis_{observed} = \sqrt{\frac{(TAM^{lower}_{x^{observed}} - \overline{TAM^{lower}_{X^{normal}}})^T (TAM^{lower}_{x^{observed}} - \overline{TAM^{lower}_{X^{normal}}})}{Cov}}. \tag{5.2.7}$$

Given a common assumption that legitimate network traffic follows the Gaussian distribution, the population of the Mahalanobis distances between individual legitimate network traffic records and the expectation of these instances also coincide with the normal distribution. Thus, approximately 99.7% of the legitimate network traffic have the similarities to the normal profile with the maximums of three standard deviations from the average distance (i.e., $\overline{Dis}$) to the expectation (i.e., $\overline{TAM^{lower}_{X^{normal}}}$) of legitimate traffic kept in the normal profile Pro. As such, the lower threshold (i.e., $\overline{Dis} - \alpha \times Std$) and the upper threshold (i.e., $\overline{Dis} + \alpha \times Std$) are given in line 2 of Fig. 5.4. The observed network traffic, whose $Dis_{observed}$ falls into the range between the lower threshold and the upper threshold, will be classified as a normal record, otherwise it will be determined as an attack.

The thresholds are essential to the detection accuracy of our DoS attack detection system, and three parameters in each threshold that need to be chosen with care to assure the effectiveness of the detection system. Since the $\overline{Dis}$ and the Std are determined in the training phase of Step 3, there is only one parameter remaining to be designed. For a normal distribution, α is usually ranged from 1 to 3. This means that detection decision can be made with a certain level of confidence varying from 68% to 99.7% in association with the selection of different values of α.

5.3 Evaluation on the Multivariate Correlation Analysis Based on Triangle Area Map

The MCA approach proposed in Section 5.1 is based on Triangle Area Map (TAM-based MCA) technique and aims to provide accurate characterisation for various types of network traffic. In order to evaluate the performance of TAM-based MCA approach, we conduct a series of experiments in this section, where its accuracy on characterisation of network traffic and its contribution to the DoS attack detection system are evaluated using the KDD Cup 99 dataset [84].

The experiments are carried out on both original network traffic data and normalised network traffic data. The final experimental results are presented in Sections 5.3.1 and compared with two state-of-the-art approaches.

5.3.1 Experimental Data for Evaluation

In the evaluation, the 10 percent of labelled data of the KDD Cup 99 dataset are applied, and they include five types of DoS attacks (i.e., Teardrop, Smurf, Pod, Neptune and Land attacks) and three types of legitimate network traffic (i.e., TCP, UPD and ICMP traffic).

All these traffic records are filtered and grouped into six clusters with respective to their labels before the commencement of the evaluation. The selected DoS attacks were carried using different transport layer protocols. For example, Neptune and Land attacks were carried by TCP traffic. Teardrop was launched via UDP traffic. Smurf and Pod attacks were using ICMP packets. The details of filtered traffic records are available from Table 4.1 in Section 4.3.4.

5.3.2 Process of Evaluation

The overall evaluation process is detailed in this section.

- First, the proposed TAM-based MCA approach is assessed for its capability of network traffic characterisation.

- Second, a 10-fold cross-validation is conducted to evaluate the detection performance of the proposed DoS attack detection system based on TAM-based MCA approach, and the entire filtered data subset is used in this task. During the 10-fold cross-validation, we employ only the Normal records in the training, and normal profiles are built with respect to the different types of legitimate traffic using the algorithm presented in Fig. 5.3. In the test phase, both the Normal records and the attack records are taken into account. The respective thresholds are determined as shown in line 2 of Fig. 5.4 given the parameter α varying from 1 to 3 with an increment of 0.5. Moreover, as given in Fig. 5.4, the observed samples are examined against the respective normal profiles which are built based on the legitimate traffic records carried using the same type of Transport layer protocol.

- Lastly, four metrics, namely TNR, DR, FPR and Accuracy (i.e. the proportion of the overall samples which are classified correctly), are used to evaluate the proposed DoS attack detection system. The definitions of these four metrics can be found in Section 4.3.4. To be a good candidate, our proposed detection system is required to achieve a high detection accuracy.

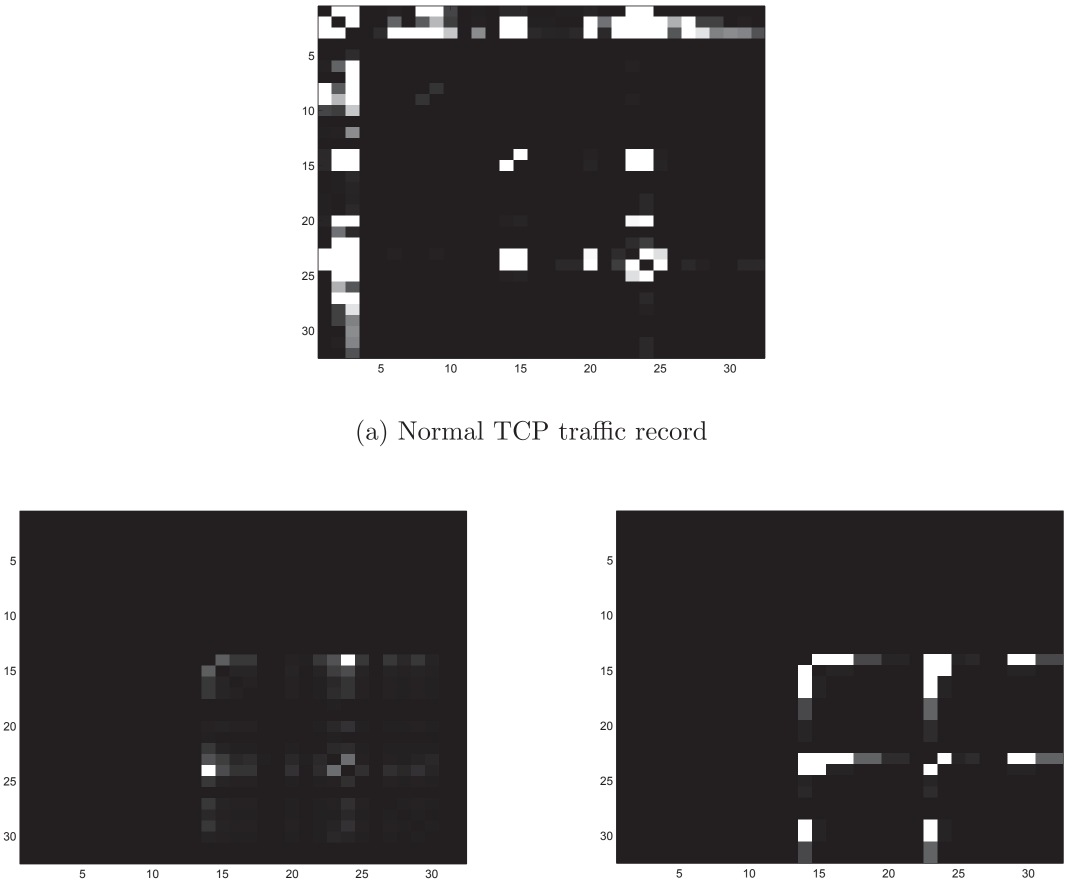
The evaluations conducted using the original data and the normalised data coincide with this process and the results are shown in Sections 5.3.3 and 5.3.4 respectively.

5.3.3 Evaluation Using the Original Data

In this evaluation, the TAMs of the different types of traffic are generated using the original network traffic records from the 10 percent labelled data, each of which contains 32 continuous features. The results of characterisation and the performance of the proposed DoS attack detection system are shown below.

Network Traffic Characterisation

The results of the network traffic characterisation using the TAM-based MCA approach on the original network traffic data is presented in this section. The images of the TAMs of the various types of filtered traffic are given in Figs. 5.5-5.7 respectively. The images demonstrate that TAM is a symmetric matrix, whose upper triangle and lower triangle are identical. The brightness of an element in an image represents its



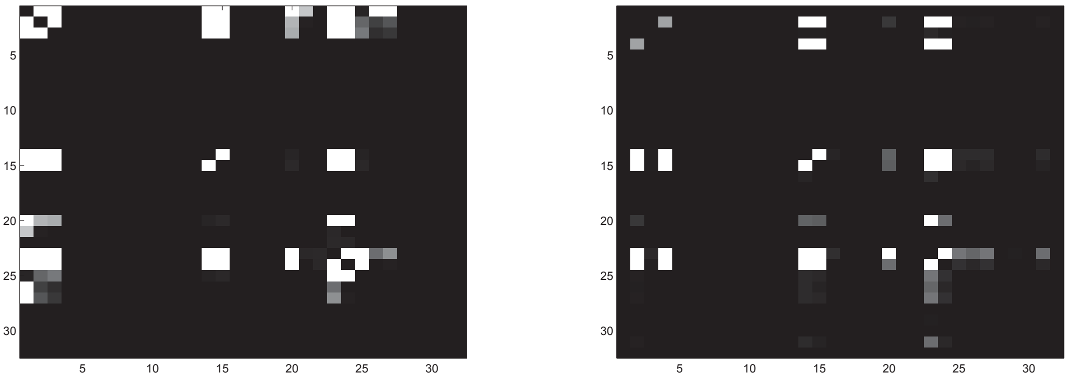
(a) Normal TCP traffic record

(b) Land attack traffic record

(c) Neptune attack traffic record

Figure 5.5: Images of the TAMs of normal TCP traffic record, Land attack record and Neptune attack record generated using original data.

value in the corresponding TAM. The greater the value is, the brighter the element is. As shown in Fig. 5.5, the images of the full TAMs of the Land attack record and the Neptune attack record exhibit clear deviation from the image of the TAM of normal TCP traffic record. The completely different patterns are also revealed in the TAMs of these two attack records.

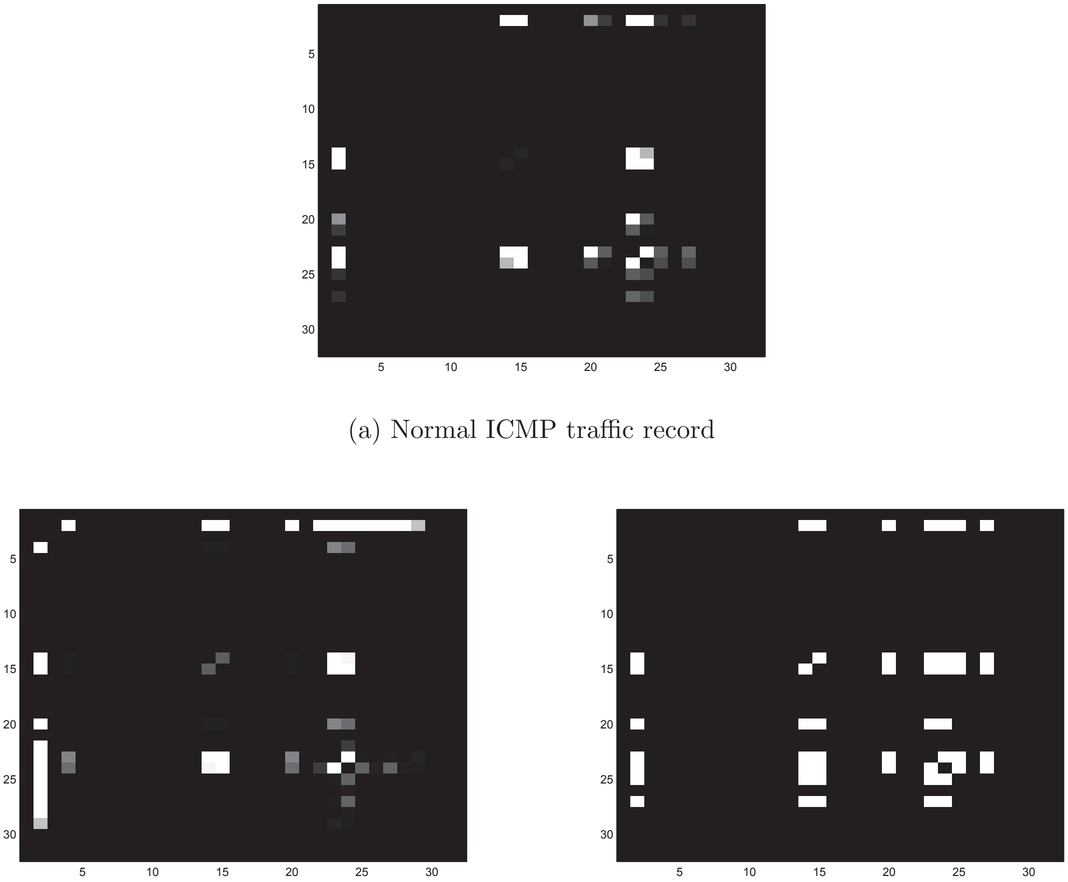


(a) Normal UDP traffic record

(b) Teardrop attack traffic record

Figure 5.6: Images of TAMs of UDP traffic record and Teardrop attack record generated using original data.

This phenomenon is found in other attacks as well. The images of the TAMs of the normal UDP traffic record and the Teardrop attack record are exhibited in Fig. 5.6. In comparison with the image of the normal UDP traffic TAM, the TAM of the Teardrop attack traffic demonstrates the distinct pattern of the multivariate correlations. In addition, the images of the TAMs shown in Fig. 5.7 reveal that the behaviours of ICMP-based attacks, namely the Pod attack and the Smurf attack, show apparent dissimilarity to the image of the TAM of the normal ICMP traffic.



(a) Normal ICMP traffic record

(b) Pod attack traffic record

(c) Smurf attack traffic record

Figure 5.7: Images of TAMs of ICMP traffic record, Pod attack record and Smurf attacks generated using original data

The above evaluation results demonstrate that our proposed TAM-based MCA approach achieves promising performance in characterisation of various types of network traffic. Utilising the extracted multivariate correlations could improve the performance of DoS attack detection system. Moreover, by looking into the images, we can easily identify the visual patterns of the different traffic records. However, the difference is not clear enough between some of images such as the images of the normal ICMP traffic record and the Pod attack traffic record and so on. This may dilute the accuracy of our detection system.

To further inspect the above suggestions, we conduct a 10-fold cross-validation in the following section to evaluate the performance of detecting DoS attacks using the discriminative power provided by the TAM.

Ten-fold Cross-validation

To evaluate the performance of our DoS attack detection system using TAM-based MCA approach along with the change of the threshold, the average TNRs for legitimate traffic and the average DRs for the individual types of DoS attacks are shown in Table 5.1.

Table 5.1: Average Detection Performance of the Proposed System on Original Data Against Different Thresholds

Type of records	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
Normal	98.74%	99.03%	99.23%	99.35%	99.47%
Teardrop	71.50%	63.92%	57.93%	52.81%	48.45%
Smurf	100.00%	100.00%	100.00%	100.00%	100.00%
Pod	100.00%	100.00%	100.00%	100.00%	100.00%
Neptune	82.44%	61.79%	57.00%	54.84%	52.96%
Land	0.00%	0.00%	0.00%	0.00%	0.00%

Throughout the evaluation, our proposed detection system achieves encouraging performance in most of the cases except Land attack. The rate of correct classification of the Normal records rises from 98.74% to 99.47% along with the increase of the threshold. Meanwhile, the Smurf and Pod attack records are completely detected without being influenced by the change of the threshold. However, the detection system suffers serious degeneration in the cases of the Teardrop and Neptune attacks when the threshold is greater than 1.5σ. The DRs for these two attacks drop sharply to 48.45% and 52.96% respectively while the threshold is set to 3σ.

Table 5.2: Detection Rate and False Positive Rates Achieved by the Proposed System on Original Data

	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
FPR	1.26%	0.97%	0.77%	0.65%	0.53%
DR	95.09%	89.38%	88.05%	87.44%	86.91%
Accuracy	95.17%	89.62%	88.32%	87.73%	87.22%

To have a better overview of the performance of our MCA-based detection system, the overall FPR and DR are highlighted in Table 5.2. The overall FPR and DR are computed over all traffic records regardless the types of attacks. When the threshold grows from 1σ to 3σ, the FPR drops quickly from 1.26% to 0.53%. Correspondingly, the DR also drops from 95.09% to 86.91% while the threshold rises. It shows clearly in the table that a larger number of legitimate traffic records are covered by a greater threshold, and more DoS attack records are incorrectly accepted as legitimate traffic in the meantime.

Problems with the Current System and Solution

Although the detection system achieves a moderate overall detection performance in the above evaluation, we want to explore the causes of degradation in detecting the Land, Teardrop and Neptune attacks.

Our analysis shows that the problems come from the data used in the evaluation, where the basic features in the non-normalised original data are in different scales. Therefore, even though our TAM-based MCA approach is promising in characterisation and clearly reveals the patterns of the various types of traffic records, our detector is still ineffective in some of the attacks. For instance, the Land, Teardrop and Neptune attacks whose patterns are different than the patterns of the legitimate traffic. However, the level of the dissimilarity between these attacks and the respective normal profiles are close to that between the legitimate traffic and the respective normal profiles. Moreover, the changes appearing in some other more important features with much smaller values can hardly take effect in distinguishing the DoS attack traffic from the legitimate traffic, because the overall dissimilarity is dominated by the features with large values. Nevertheless, the non-normalised original data contains zero values in some of the features (both the important and the less important features), and they confuse our MCA approach and make many new generated features (e.g., $Tr^i_{j,k}$) equal to zeros. This severely degrades the discriminative power of the new feature set (e.g., $TAM^{lower}_{x_i}$), which is not supposed to happen.

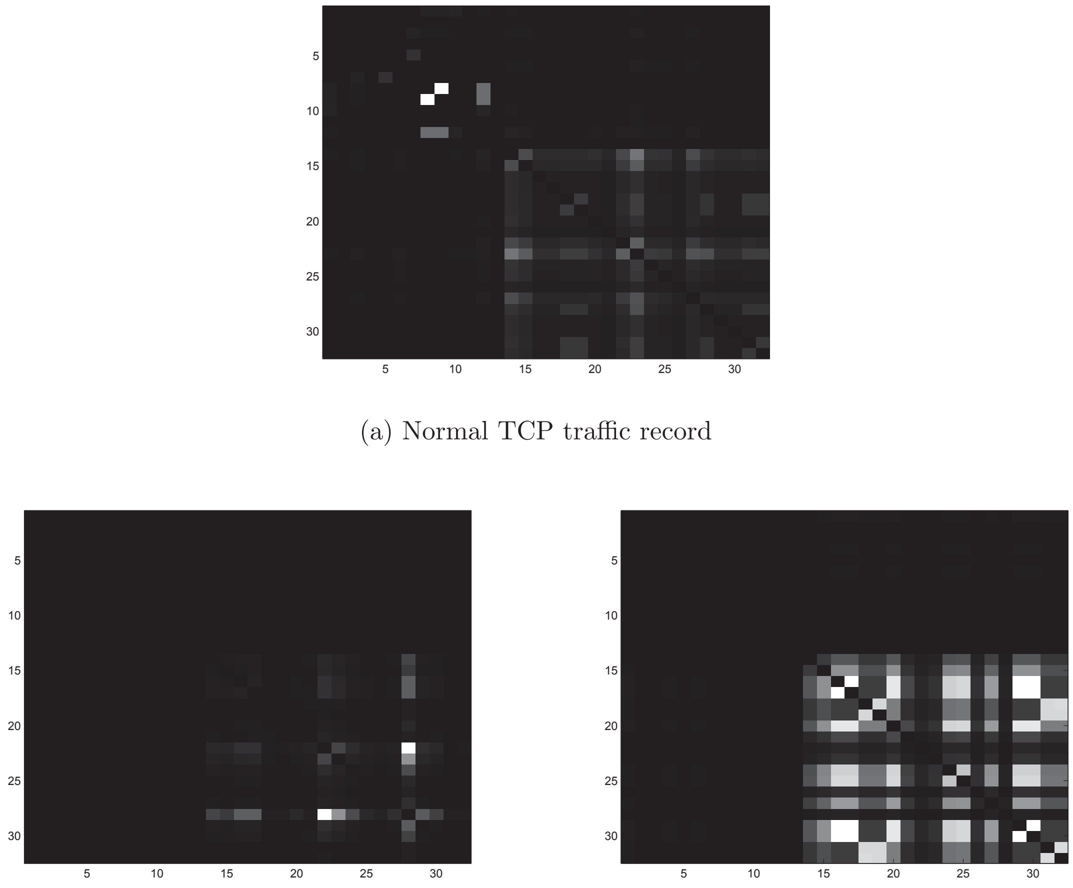
Apparently, an appropriate data normalisation technique should be employed to eliminate the bias. Therefore, we adopt the statistical normalisation technique [102] to this work. The statistical normalisation has been detailed in Section 4.3.4.

5.3.4 Evaluation Using the Normalised Data

Taking consideration of the afore-discussed solution, we conduct the same series of experiments in this section on the data normalised using the statistical normalisation technique.

Network Traffic Characterisation

In this section, the characterisation of network traffic is conducted on the data normalised using the statistical normalisation technique. The images of the respective TAMs are shown in Figs. 5.8-5.10. The images of the attack TAMs present completely different patterns to the respective normal TAMs. Moreover, the values of



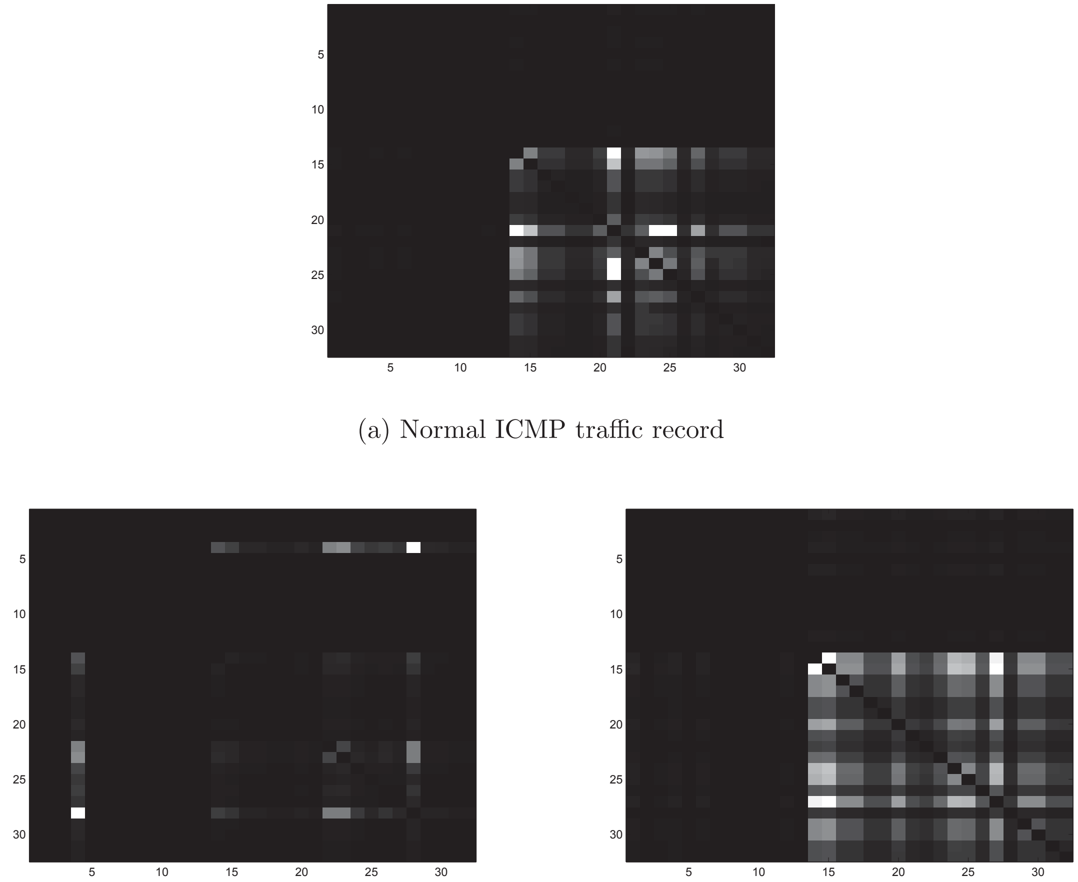
(a) Normal TCP traffic record

(b) Land attack traffic record

(c) Neptune attack traffic record

Figure 5.8: Images of TAMs of normal TCP traffic record, Land attack record and Neptune attack record generated using normalised data

elements of the TAMs are in the same scale, so that the TAMs generated by the proposed TAM-based MCA approach using normalised data provide a higher accurate characterisation to the corresponding network traffic.



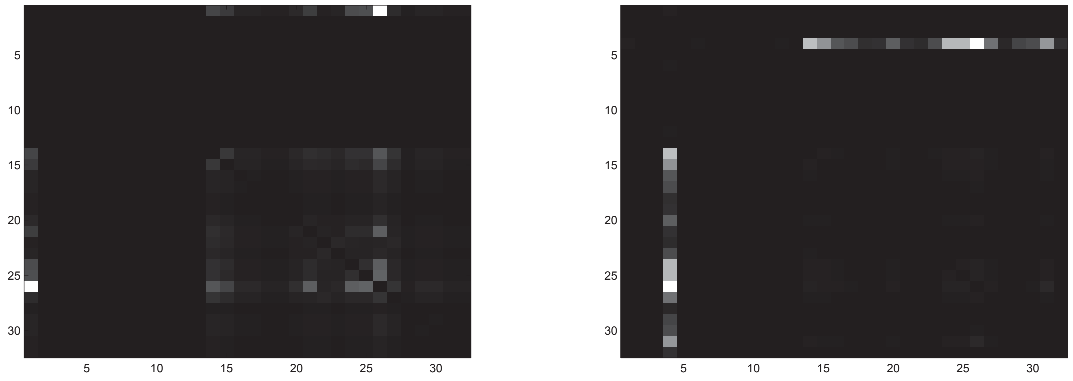
(a) Normal ICMP traffic record

(b) Pod attack traffic record

(c) Smurf attack traffic record

Figure 5.9: Images of TAMs of ICMP traffic, Pod attack record and Smurf attack record generated using normalised data

To verify our observation, a 10-fold cross-validation is conducted as done in Section 5.3.3 on the data normalised using the aforementioned statistical normalization technique. The results are given in Section 5.3.4.



(a) Normal UDP traffic record

(b) Teardrop attack traffic record

Figure 5.10: Images of TAMs of UDP traffic record and Teardrop attack record generated using normalised data

Ten-fold Cross-validation

The detection performance based on the normalized data is given in Table 5.3. The results reveal that the data do have significant influence on our detection system, whose overall performance increases dramatically when taking the normalized data as the inputs.

Table 5.3: Average Detection Performance of the Proposed System on Normalised Data Against Different Thresholds

Type of records	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
Normal	97.36%	97.97%	98.32%	98.56%	98.75%
Teardrop	100.00%	100.00%	100.00%	100.00%	100.00%
Smurf	100.00%	100.00%	100.00%	100.00%	100.00%
Pod	100.00%	100.00%	100.00%	100.00%	100.00%
Neptune	100.00%	100.00%	100.00%	100.00%	100.00%
Land	100.00%	100.00%	100.00%	100.00%	100.00%

The Teardrop, Neptune and Land attacks, which are mostly misclassified in the previous evaluation, can now be completely and correctly classified by the system along with the increase of the threshold. In comparison with the TNR of our detection system achieved on the non-normalised Normal records, the one achieved on the normalised Normal records decreases a bit to maximum 98.75% when the threshold is set to 3σ. However, it manages to remain in the reasonable range.

Then, similar to the previous evaluation, we show the overall FPR and DR in Table 5.4. The FPR shown in the table drops nearly 1% when the threshold increases from 1σ to 2σ. Finally it reaches to 1.25% while the threshold is staying at 3σ. The DR of the system remains constant at 100.00%. It is clearly seen that the proposed detection system achieves a better DR with the normalised data than with the original (non-normalised) data.

Table 5.4: Detection Rate and False Positive Rate Achieved by the Proposed System on Normalised Data

	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
FPR	2.64%	2.03%	1.68%	1.44%	1.25%
DR	100.00%	100.00%	100.00%	100.00%	100.00%
Accuracy	99.94%	99.95%	99.96%	99.96%	99.97%

5.3.5 Performance Comparisons

To make a complete comparison, the ROC curves of the previous two evaluations are shown in Figs. 5.11 and 5.12. The relationship between DR and FPR is clearly revealed in the ROC curves. The DR increases when larger numbers of false positive are tolerated.

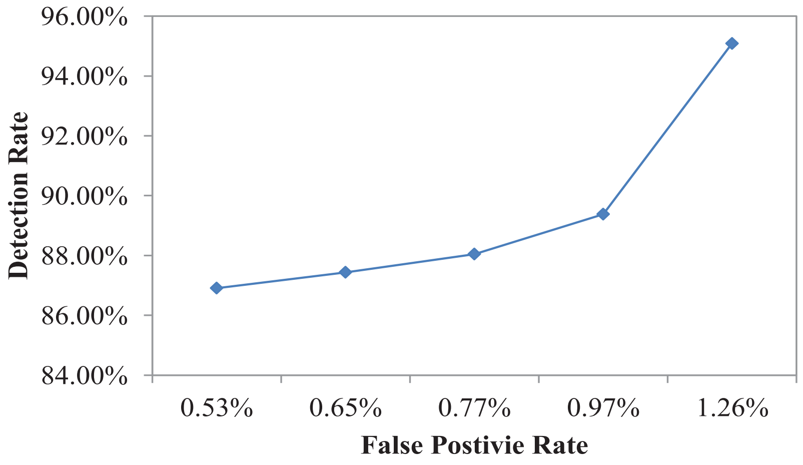


Figure 5.11: The ROC curve for analysing original data

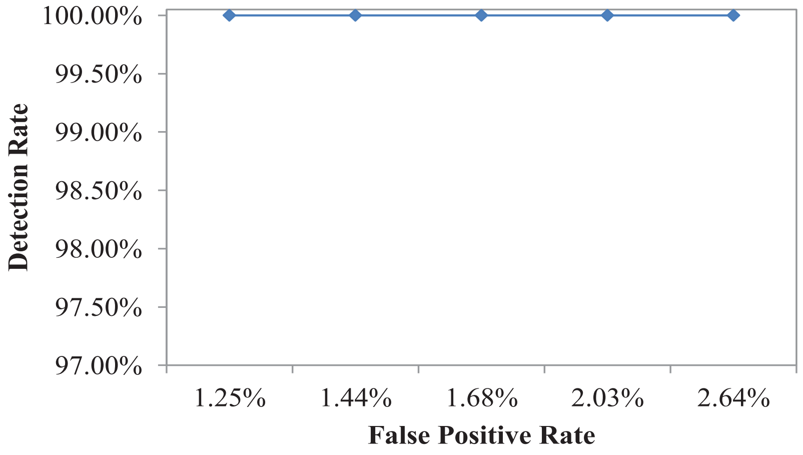


Figure 5.12: The ROC curve for analysing normalised data

In Fig. 5.11, the ROC curve for analysing the original data using our proposed detection system shows a rising trend. The curve climbs gradually from 86.91% DR to 89.38% DR, and finally reaches to 95.09% DR. Likewise, the ROC curve for analysing the normalised data remains a high level of DR at 100.00% constantly as shown in Fig. 5.12. It is clear that our DoS attack detection system always enjoys higher detection rates while working with the normalised data than with the original data in all cases.

Last but not least, three state-of-the-art detection approaches, namely network intrusion detection system based on covariance feature space [48], intrusion detection system using nearest neighbour based on triangle area [98], and the proposed attack detection system using EDM-based MCA approach proposed in Chapter 4 are selected to compare with our proposed detection system. The best accuracies on detecting DoS attacks achieved by the various approaches and systems are given in Table 6.5.

Although all approaches and systems highlighted in Table 6.5 have high accuracies on DoS attack detection, our proposed detection system using TAM-based MCA approach (95.17% for the original data and 99.97% for the normalised data) clearly outperforms the network intrusion detection system based on covariance feature space (97.89%) and intrusion detection system using nearest neighbour based on triangle area (92.15%). In addition, our proposed detection system cooperating with normalised data (99.97%) shows a marginal advantage over the DoS attack detection system using EDM-based MCA approach (99.96%). Although this is a narrow lead, our detection system is more promising especially when it is deployed on a production network with a throughput of 1 Gbps. Due to a significantly fewer number of false alarms generated per second, network administrators will be much less interrupted by the false information.

Table 5.5: Performance Comparisons with Different Detection Approaches

	The proposed detection system using TAM-based MCA approach (Original data, Threshold = 1σ)	The proposed detection system using TAM-based MCA approach (Normalised data, Threshold = 3σ)	Network intrusion detection system based on covariance feature space [48] (Threshold approach with 4D principle and Cov_len3_150)	Intrusion detection system using nearest neighbour based on triangle area [98]	The DoS attack detection system using EDM-based MCA approach proposed in Chapter 4 (Normalised data, Threshold = 3σ)
Accuracy	95.17%	99.97%	97.89%	92.15%	99.96%

5.4 Computational Complexity and Time Cost Analysis

In this section, we conduct an analysis on the computational complexity and the time cost of our proposed DoS attack detection system using the proposed TAM-based MCA approach.

The computational complexity of the proposed DoS attack detection system consists of two components, namely the complexity of the proposed TAM-based MCA approach and the complexity of the detection process in our proposed attack detection system.

On one hand, as discussed in Section 5.1.1, triangle areas of all possible combinations of any two distinct features in a traffic record need to be computed when processing our proposed MCA. Since each traffic record has m features (or dimensions), $\frac{m(m-1)}{2}$ triangle areas are generated and are used to construct a $TAM_{x_i}^{lower}$. Thus, the proposed MCA has a computational complexity of $O(m^2)$.

On the other hand, as explained in Section 5.2, the MD between the observed feature vector (i.e., the $TAM_{x_i}^{lower}$) and $\overline{TAM_{X^{normal}}^{lower}}$ of the respective normal profile needs to be computed in the detection process of our proposed detection system to evaluate the level of the dissimilarity between them. Thus, this computation incurs a complexity of $O(M^2)$, in which $M = \frac{m(m-1)}{2}$ is the dimensions of $TAM_{x_i}^{lower}$. $O(M^2)$ can be written as $O(m^4)$. By taking the computational complexities of the proposed MCA and the detection process of our proposed detection system into account, the overall computational complexity of the proposed detection system is $O(m^2) + O(m^4) = O(m^4)$. However, m is a fixed number which is 32 in our case, so that the overall computational complexity is indeed equal to $O(1)$.

Similarly, the DoS attack detection system using EDM-based MCA approach proposed in Chapter 4 achieves the same computational complexities of $O(m^2)$ and $O(m^4)$ in data processing and attack detection respectively. Moreover, the number of features (m) in use is identical to that used in our proposed detection system as well. Thus, the overall computational complexity of the DoS attack detection system using EDM-based MCA approach is $O(1)$.

The computational complexities of the other two state-of-the-art detection systems that have been compared in Section 5.3.5 has already been analysed in Section 4.4. The overall computational complexity of the network intrusion detection system based on covariance feature space [48] is $O(nm^2)+O(lm^2) = O(lm^2)$, where n is the number of sequential samples in a group, m is the number of physical features of a sample and l is the number of known classes/clusters needed to be compared with. Another state-of-the-art approach (i.e., intrusion detection system using nearest neighbour based on triangle area [98]) has an overall complexity of $O(ml^2) + O(l^2n^2) = O(l^2n^2)$, where m is the number of features (or dimensions) in a traffic record, l is the number of clusters used in generating triangle areas and n is the number of training samples. In real network environments, the types of attacks and the number of available training samples are often varying. Thus, the computational complexities of these two state-of-the-art detection systems cannot be constants.

In general, our proposed detection system can achieve equal or better computational complexity than the three other approaches. The computational complexities of the above discussed approaches are summarised in Table 5.6.

Table 5.6: Computational Complexities of Different State-of-the-art Detection Approaches

The proposed flooding DoS attack detection system using TAM-based MCA approach	The DoS attack detection system using EDM-based MCA approach proposed in Chapter 4	Network intrusion detection system based on covariance feature space [48] (Threshold approach with 4D principle and Cov_len3_150)	Intrusion detection system using nearest neighbour based on triangle area [98]
$O(1)$	$O(1)$	$O(lm^2)$	$O(l^2n^2)$

Moreover, time cost is discussed to show the contribution of our proposed TAM-based MCA approach in terms of acceleration of data processing. Our proposed TAM-based MCA approach can proceed approximately 23,092 traffic records per second. In contrast, the EDM-based MCA approach presented in Chapter 4 can achieve approximately 12,044 traffic records per second, which is nearly less than half of that achieved by our proposed TAM-based MCA approach. Due to the unavailability of the source code of triangle area based nearest neighbours approach [98], we cannot provide a comparison to it.

5.5 Summary

This chapter has proposed a TAM technique to enhance and to speed up the process of MCA. The evaluation shows that the new TAM-based MCA approach accurately characterises the various types of network traffic and reveals the correlations between features.

In addition, this chapter has also proposed a new DoS attack detection system based on the TAM-based MCA approach and the anomaly-based detection technique. The evaluations have been conducted using the KDD Cup 99 dataset to verify the effectiveness and the performance of the proposed DoS attack detection system. The influence of original (non-normalised) and normalised data has been studied in the paper. The results have revealed that when working with non-normalised data, our detection system achieves maximum 95.17% detection accuracy although it does not work well in identifying Land, Neptune and Teardrop attack records.

The problem, however, can be solved by utilising statistical normalisation technique to eliminate the bias from the data. The results of evaluating with the normalised data have shown a more encouraging detection accuracy of 99.97% and nearly 100.00% DRs for the various DoS attacks. Besides, the comparison result has proven that our detection system outperforms three state-of-the-art approaches in terms of detection accuracy.

Moreover, the computational complexity and the time cost of the proposed detection system have been analysed and shown in Section 5.4. The proposed system achieves equal or better performance in comparison with the three state-of-the-art approaches shown in [48], [98] and Chapter 4.

To be part of the future work, we will further employ more sophisticated classification techniques to further alleviate the false positive rate.

Chapter 6

Detection of Denial-of-Service Attacks Based on Computer Vision Techniques

DoS attacks have emerged as one of the most severe network intrusive behaviours and have posed serious threats to the infrastructures of computer networks and various network-based services.

Over the recent two decades, a variety of anomaly-based detection systems have been proposed. However, the existing systems [60][71] suffer from a common issue in achieving high accuracy in classifying both normal traffic and attack traffic. This is partly because most of these systems only use several simple network features of incoming traffic (e.g., IP header fields) in modelling normal network traffic, and ignore the correlations between the network features. Although there is a current research trend to make use of the correlations between the features in intrusion detection, most of the proposed systems [48][97][98] are based on traditional statistical correlation analysis techniques, which are only capable of studying the correlations between the features (variables) in a given sample set. The properties inherited from these traditional statistical correlation analysis techniques make these anomaly-based detection systems incapable of recognising individual attack records hiding in a sample set.

In addition, more sophisticated classifiers are demanded to help improve detection accuracy. The techniques used in computer vision tasks are the potential candidates. Due to some commonalities shared between DoS attack detection and computer vision tasks, such as image retrieval and object shape recognition. Normal traffic to DoS attack detection can be equivalent to queries to image retrieval tasks or object shape recognition tasks. DoS attacks to our detection task can be interpreted as the images or the object shapes that do not match the queries. Therefore, computer vision techniques can provide intuitive and effective solutions to the problem.

In this chapter, we propose a more sophisticated anomaly-based system for detecting DoS attacks. The proposed system is designed, based on our work [89] submitted to IEEE/ACM Transactions on Networking, to overcome all the aforementioned issues and solves the detection problem from the perspective of computer vision. Our system has three key features:

- First, the hidden correlations between the features of network traffic are extracted using the MCA techniques previously developed in Chapters 4 and 5 to provide accurate network traffic characterisation,

- Second, individual attack records hidden in the crowd can be easily recognised by our system. This is owing to one of the merits (i.e., the capability of analysing correlation between features within individual records) of our MCA techniques which equips the analysis of correlation being conducted on individual network traffic records, and

- Finally, to improve the detection accuracy, our proposed system adopts the principle of image retrieval in the design of attack detectors. To the best of our knowledge, it is the first time that the Earth Mover's Distance [61] (a robust distance metric) has ever been applied to field of network DoS attack detection.

The proposed anomaly-based DoS attack detection system is evaluated using the KDD Cup 99 dataset [84] on DoS attacks. The experimental results are compared against two state-of-the-art detection systems (i.e., the network intrusion detection system based on covariance feature space [48] and the intrusion detection system using nearest neighbour based on triangle area [98]). The computational complexity of our system is also discussed and compared with the two state-of-the-art detection systems. The overall evaluation shows that our detection system achieves 99.95% accuracy, outperforming previous systems by more than 2%.

The rest of this chapter is organised as follows. Section 6.1 introduces the relevant mathematical techniques for network traffic data analysis. Section 6.2 proposes a new DoS attack detection system based on computer vision techniques. Section 6.3 designs and discusses the relevant algorithms involved in the proposed DoS attack detection system. Section 6.4 illustrates performance evaluations of our proposed detection system on the KDD Cup 99 dataset. Finally, summary is drawn in Section 6.5.

6.1 Mathematical Techniques for Network Traffic Data Analysis

This section introduces the relevant mathematical techniques to be involved in network traffic data analysis. These techniques are principal component analysis (discussed in Section 6.1.1), multivariate correlation analysis (discussed in Section 6.1.2) and earth mover's distance (discussed in Section 6.1.3). They will be applied in dimensionality reduction, multivariate correlation analysis and attack recognition respectively.

6.1.1 Principal Component Analysis

As a linear mathematical system, the PCA helps eliminate distractive noise and seek the best lower dimensional representation for data with a high dimensionality. It is driven by the idea that greater contribution on data representation comes from the eigenvectors which conserve larger variations (i.e., eigenvalues). To reveal the importance of the eigenvectors in a data space to which the interested data belongs, a multivariate analysis is performed. The analysis involves a transformation converting the interested data into a new orthonormalised coordinate system, where the axes indicate the directions of the eigenvectors and the data is maximally linearly decorrelated. The detailed process of the PCA is shown as follows.

Given a dataset $X = [x_1\, x_2\, \cdots\, x_n]$, where

$$x_i = \begin{bmatrix} f_1^i \\ f_2^i \\ \vdots \\ f_m^i \end{bmatrix}$$

denotes the i^{th} observation with m features and i is ranged from 1 to n, zero-mean normalisation is first conducted on the dataset for all the observations to make the PCA work properly. The zero-mean dataset is represented by (6.1.1).

$$X_{zm} = [(x_1 - \bar{x})\ (x_2 - \bar{x})\ \cdots\ (x_n - \bar{x})], \tag{6.1.1}$$

in which

$$\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i. \tag{6.1.2}$$

Then, the principal components (i.e., eigenvectors) are obtained by performing eigen decomposition on the sample covariance matrix defined in (6.1.3).

$$C_X = \frac{1}{n-1} X_{zm} X_{zm}^T. \tag{6.1.3}$$

The C_X is then decomposed into a matrix W and a diagonal matrix Λ. The two matrices satisfy the condition given in (6.1.4).

$$\Lambda W = C_X W. \tag{6.1.4}$$

The columns of the matrix W stand for the eigenvectors (i.e., the principal components) of the covariance matrix C_X, and the elements along the diagonal of the matrix Λ are the ranked eigenvalues associated with the corresponding eigenvectors in the matrix W.

To determine the optimal number of principal components to be retained based on the analysis results from the PCA, a cumulative-variance-based selection criterion is applied. The selected k ($1 \leq k \leq m$) principal components, namely the eigenvectors in matrix W which are associated with the first k largest eigenvalues, provide the best presentation for the original dataset and reduce the dimensionality of the original data space from m to k. A new lower-dimensional representation, defined in (6.1.5), for the given dataset is obtained by projecting X onto the selected k-dimensional data subspace.

$$X_{Pr} = [x_{1_{Pr}} \; x_{2_{Pr}} \; \cdots \; x_{n_{Pr}}]. \tag{6.1.5}$$

The i^{th} observation is now represented as shown in (6.1.6).

$$x_{i_{Pr}} = \begin{bmatrix} f^i_{1_{Pr}} \\ f^i_{2_{Pr}} \\ \vdots \\ f^i_{k_{Pr}} \end{bmatrix}, (1 \leq i \leq n). \tag{6.1.6}$$

6.1.2 Multivariate Correlation Analysis

There are two distinct MCA approaches proposed in Chapters 4 and 5 for the extraction of hidden correlative information from the features of an observation. They are EDM-based MCA approach and TAM-based MCA approach respectively. In comparison with other approaches shown in [48] and [98], these two MCA approaches have been proven to be advanced in the following aspects. These approaches

- Require only the knowledge of current observation in performing analysis, and
- Withstand the problem that all features being changed linearly [48].

Given the dataset $X_{Pr} = [x_{1_{Pr}} \; x_{2_{Pr}} \; \cdots \; x_{n_{Pr}}]$ obtained using PCA, the correlative information residing in the i^{th} observation $x_{i_{Pr}} = [f^i_{1_{Pr}} \; f^i_{2_{Pr}} \; \cdots \; f^i_{k_{Pr}}]^T$, $(1 \leq i \leq n)$ is extracted using the EDM-based MCA approach and the TAM-based approach respectively as follows.

EDM-based MCA Approach

In the EDM-based MCA approach proposed in Chapter 4, a data transformation is first carried out on the i^{th} observation and is achieved by simply multiplying $x_{i_{Pr}}^T$ with a k-by-k identity matrix I. This results in a new k-by-k feature matrix $x'_{i_{Pr}}$ as shown in (6.1.9).

$$x'_{i_{Pr}} = x_{i_{Pr}}^T I = \begin{bmatrix} f_{1_{Pr}}^i & 0 & \cdots & 0 \\ 0 & f_{2_{Pr}}^i & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & f_{k_{Pr}}^i \end{bmatrix}_{k\times k} . \tag{6.1.7}$$

The elements on the diagonal of the matrix $x'_{i_{Pr}}$ are the features of the observation $x_{i_{Pr}}$. The j^{th} column of the matrix $x'_{i_{Pr}}$ is a k-dimensional column vector denoted by (6.1.8).

$$F_j^i = \begin{bmatrix} \eta_{j,1}^i \\ \eta_{j,2}^i \\ \vdots \\ \eta_{j,k}^i \end{bmatrix} , \tag{6.1.8}$$

where $\eta_{j,p}^i = 0$ if $j \neq p$, otherwise $\eta_{j,p}^i = f_{j_{Pr}}^i$. The superscript i stands for the index of an observation varying from 1 to n, and the subscripts j and p are both ranged from 1 to k. Then, the k-by-k feature matrix $x'_{i_{Pr}}$ can be rewritten as (6.1.9).

$$x'_{i_{Pr}} = [F_1^i \; F_2^i \; \cdots \; F_k^i]. \tag{6.1.9}$$

Once the transformation is finished, the Euclidean distance is applied to extract the correlation between the column vectors F_j^i and F_p^i in the matrix $x'_{i_{Pr}}$. The correlation is defined as $ED_{j,p}^i = \sqrt{(F_j^i - F_p^i)^T(F_j^i - F_p^i)}$, where $1 \leq i \leq n$, $1 \leq j \leq k$ and $1 \leq p \leq k$. Therefore, the correlations between features in the original traffic record

$x_{i_{Pr}}$ can be denoted using a k-by-k matrix (i.e., a Euclidean distance map) as shown in (6.1.10).

$$EDM_{x_{i_{Pr}}} = \left[ED^{i}_{j,p} \right]_{k \times k}, \tag{6.1.10}$$

where all the correlations are arranged on the map in accordance with their indices. For example, $ED^{i}_{j,p}$ is positioned on the j^{th} row and the p^{th} column of the map. Furthermore, $EDM_{x_{i_{Pr}}}$ is a symmetric matrix in which $ED^{i}_{j,p} = ED^{i}_{p,j}$. For the whole dataset, the hidden correlations are represented by the EDMs of individual feature vectors, namely $X_{EDM} = [EDM_{x_{1_{Pr}}} \; EDM_{x_{2_{Pr}}} \; \cdots \; EDM_{x_{n_{Pr}}}]_{k \times k \times n}$.

TAM-based MCA Approach

By contrast, the TAM-based MCA approach proposed in Chapter 5 attempts to accomplish the same task from a different perspective, in which the concept of triangle area is applied to extract the geometrical correlation between the j^{th} and p^{th} features in an observation $x_{i_{Pr}}$. To obtain the triangle formed involving the j^{th} and p^{th} features, a data transformation is engaged. The observation $x_{i_{Pr}}$ is first projected on the (j, p)-th two-dimensional Euclidean subspace as shown in (6.1.11).

$$y_{i,j,p} = [\varepsilon_j \; \varepsilon_p]^T x_{i_{Pr}} = \begin{bmatrix} f^{i}_{j_{Pr}} \\ f^{i}_{p_{Pr}} \end{bmatrix}, \tag{6.1.11}$$

where $1 \le i \le n,\ 1 \le j \le k,\ 1 \le p \le k$ and $j \ne p$. Moreover, $\varepsilon_j = [e_{j,1} \; e_{j,2} \; \cdots \; e_{j,k}]^T$ and $\varepsilon_p = [e_{p,1} \; e_{p,2} \; \cdots \; e_{p,k}]^T$. The elements in the vectors ε_j and ε_p are all zeros, except the (j, j)-th and the (p, p)-th elements whose values are ones in ε_j and ε_p respectively. The projected point, $y_{i,j,p}$, is located on the Cartesian coordinate system in the (j, p)-th two-dimensional Euclidean subspace with coordinate ($f^{i}_{j_{Pr}}$, $f^{i}_{p_{Pr}}$). Then, on the Cartesian coordinate system, a triangle (i.e., $\Delta f^{i}_{j_{Pr}} O f^{i}_{p_{Pr}}$) formed by the origin (i.e.,

O) and the projected points of the coordinate $(f^i_{j_{Pr}}, f^i_{p_{Pr}})$ on the j-axis and the p-axis is found, and whose area is defined as $Tr^i_{j,p} = (\parallel (f^i_{j_{Pr}}, 0) - (0,0) \parallel \times \parallel (0, f^i_{p_{Pr}}) - (0,0) \parallel)/2$, where $1 \leq i \leq n$, $1 \leq j \leq k$, $1 \leq p \leq k$ and $j \neq p$. In order to make a complete analysis, all possible permutations of any two distinct features in the observation $x_{i_{Pr}}$ are extracted and the corresponding triangle areas are computed. A k-by-k matrix (i.e., a Triangle area map) is constructed and represented in (6.1.12).

$$TAM_{x_{i_{Pr}}} = \left[Tr^i_{j,p} \right]_{k \times k}, \tag{6.1.12}$$

where all the triangle areas are arranged on the map in accordance with their indexes similar to Euclidean distance map in the EDM-based MCA approach. Additionally, the values of the elements on the diagonal of the map are set to zeros ($Tr^i_{j,p} = 0$, if $j = p$), because we only care about the correlation between each pair of distinct features. Furthermore, since $TAM_{x_{i_{Pr}}}$ is a symmetric matrix in which $Tr^i_{j,p} = Tr^i_{p,j}$. For the dataset X_{Pr}, its geometrical multivariate correlations can be represented as $X_{TAM} = [TAM_{x_{1_{Pr}}}\ TAM_{x_{2_{Pr}}}\ \cdots\ TAM_{x_{n_{Pr}}}]_{k \times k \times n}$.

6.1.3 EMD-L_1

The EMD [78] is a cross-bin function measuring the perceptual dissimilarity between two distributions. It is inspired by the intuition that looking for a solution with the minimum overhead on moving a mass of earth properly spreading in space to a collection of holes in the same space. The mass of earth and the collection of holes are taken as two distributions of signatures, which subsume histograms. The process of measuring the distance between two signatures is modelled as the transportation problem that is a special case of Linear Programming (LP) [5]. The cost of transporting a unit of earth from its origin to a hole is determined by the ground distance that the earth needs to travel until it reaches the hole.

Assume that there are two-dimensional histograms with m rows and n columns and $N = m \times n$ bins. The index set for bins is defined in (6.1.13).

$$\mathcal{I}' = \{(i, j) : 1 \le i \le m, 1 \le j \le n\}, \tag{6.1.13}$$

where (i, j) denotes the index of a bin or a node. The index set for flows is defined in (6.1.14).

$$\mathcal{J}' = \{(i, j, k, l) : (i, j) \in \mathcal{I}', (k, l) \in \mathcal{I}'\}, \tag{6.1.14}$$

where (i, j, k, l) denotes the flow from the bin (i, j) to the bin (k, l).

$$P = \{p_{ij} : (i, j) \in \mathcal{I}'\}, \tag{6.1.15}$$

and

$$Q = \{q_{ij} : (i, j) \in \mathcal{I}'\}, \tag{6.1.16}$$

are the two histograms to be compared. Histograms are normalised to a unit mass (i.e., $\sum_{i,j} p_{ij} = 1$ and $\sum_{i,j} q_{ij} = 1$). With these notations, the definition of EMD between two histograms P and Q is obtained as follows.

$$\mathrm{EMD}(P, Q) = \min_{F=\{f_{i,j;k,l}:(i,j,k,l)\in\mathcal{J}'\}} \sum_{\mathcal{J}'} f_{i,j;k,l} d_{i,j;k,l}, \tag{6.1.17}$$

$$s.t. \begin{cases} \sum_{(k,l)\in\mathcal{I}'} f_{i,j;k,l} = p_{ij} & \forall (i, j) \in \mathcal{I}' \\ \sum_{(i,j)\in\mathcal{I}'} f_{i,j;k,l} = q_{kl} & \forall (k, l) \in \mathcal{I}' \\ f_{i,j;k,l} \ge 0 & \forall (i, j, k, l) \in \mathcal{J}' \end{cases}, \tag{6.1.18}$$

where F is the set of $f_{i,j;k,l}$, which denotes the flow from the bin (i, j) of the histogram P to the bin (k, l) of the histogram Q. An F satisfying the restrictions given in (6.1.18) is called a feasible flow from the histogram P to the histogram Q. The ground distance $d_{i,j,k,l}$ between the bin (i, j) and the bin (k, l) is commonly defined by L_p distance

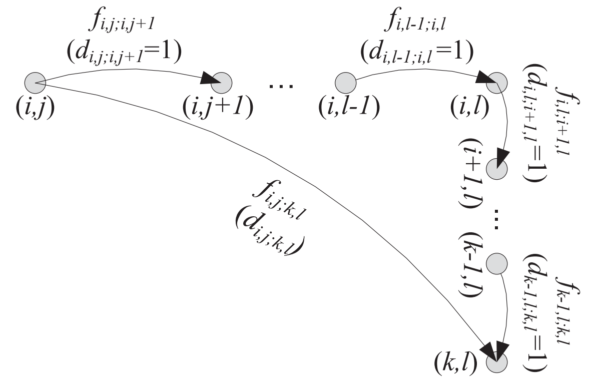
$$d_{i,j;k,l} = \| (i, j)^T - (k, l)^T \|_p = (| i - k |^p + | j - l |^p)^{1/p}. \tag{6.1.19}$$

New Formulation of EMD

Although the EMD has proven to be effective and to be perceptually consistent with human vision for comparing distributions, the expensive computation restricts the applications of the EMD mainly in offline tasks. Subsequent research on the EMD suggests various techniques to alleviate the overhead of computation. An equivalent simplification, the EMD-L_1 [61], introduces a new efficient formulation of the EMD between histograms (a special type of signatures with non-sparse structures). L_1 (i.e., Manhattan) distance is chosen as the ground distance in this new formulation, which redefines the computation of the EMD as a “network flow problem”.

With the new formulation, the computational complexity of the EMD can be reduced by one order of magnitude in comparison with the original formulation using transportation problem. This is owing to an important property of the L_1 distance that any shortest path between two points on a network can be decomposed into a collection of edges between neighbour nodes with a ground distance of one between them.

As shown in Fig. 6.1, the shortest path between the node (i, j) and the node (k, l), where $i < k$ and $j < l$, is decomposed into the collection of edges (including $f_{i,j;i,j+1}$, $f_{i,l-1;i,l}$, $f_{i,l;i+1,l}$, $f_{k-1,l;k,l}$ etc.) with ground distance of one, and its distance is defined as the summation of the distances of the edges (i.e., $d_{i,j;k,l} = d_{i,j;i,j+1} + \cdots + d_{i,l-1;i,l} + d_{i,l;i+1,l} + \cdots + d_{k-1,l;k,l}$).



Remark: $d_{i,j;k,l} = d_{i,j;i,j+1} + \ldots + d_{i,l-1;i,l} + d_{i,l;i+1,l} + \ldots + d_{k-1,l;k,l}$

Figure 6.1: Decompose a flow

Using the following notations, the new formulation of the EMD (i.e., the EMD-L_1) considering only the flows (edges) between neighbour bins (nodes) is defined. Without loss of generality, we assume that there are two-dimensional histograms with k rows and q columns and $N = k \times q$ bins.

$$\mathcal{I} = \{(j,p) : 1 \leq j \leq k, 1 \leq p \leq q\} \tag{6.1.20}$$

is the index set where (j,p) indicates the index of a bin (or node) within a histogram.

$$\mathcal{J} = \{(j,p,c,d) : (j,p) \in \mathcal{I}, (c,d) \in \mathcal{I}\} \tag{6.1.21}$$

is the index set where (j,p,c,d) is the index of a flow $f_{j,p;c,d}$ from the bin (j,p) to the bin (c,d).

$$\mathcal{J}_1 = \{(j,p,c,d) : (j,p,c,d) \in \mathcal{J}, d_{j,p;c,d} = 1\} \tag{6.1.22}$$

denotes the index set where (j,p,c,d) is the index of a flow $f_{j,p;c,d}$ from the bin (j,p) to the bin (c,d), and the bin (j,p) to the bin (c,d) are neighbour bins with a ground distance of one.

A histogram Y and a histogram Z are defined in (6.1.23) and (6.1.24) respectively.

$$Y = \{y_{jp} : (j,p) \in \mathcal{I}\}, \tag{6.1.23}$$

and

$$Z = \{z_{jp} : (j, p) \in \mathcal{I}\}, \tag{6.1.24}$$

where y_{jp} denotes the bin (j, p) of the histogram Y, and z_{jp} denotes the bin (j, p) of the histogram Z. To compare the two histograms using EMD-L_1, The histograms Y and Z are first normalised to two unit masses (i.e., $\sum_{j,p} p_{jp} = 1$ and $\sum_{j,p} q_{jp} = 1$, where p_{jp} and q_{jp} denote the normalised masses of the earth on the bin (j, p) of the histogram Y and the bin (j, p) of the histogram Z respectively). The EMD-L_1 is defined in (6.1.25).

$$\text{EMD-}\, L_1(Y, Z) = \min_{F=\{f_{j,p;c,d}:(j,p,c,d)\in\mathcal{J}_1\}} \sum_{\mathcal{J}_1} f_{j,p;c,d}, \tag{6.1.25}$$

$$s.t. \begin{cases} \displaystyle\sum_{c,d:(j,p,c,d)\in\mathcal{J}_1} (f_{j,p;c,d} - f_{c,d;j,p}) = b_{jp} & \forall (j, p) \in \mathcal{I} \\ f_{j,p;c,d} \geq 0 & \forall (j, p, c, d) \in \mathcal{J}_1 \end{cases}, \tag{6.1.26}$$

where b_{jp} is the difference between the two histograms Y and Z at the bin (j, p), and a flow F satisfying (6.1.26) is called a feasible flow which consists of a number of sub-flows $f_{j,p;c,d}$.

The EMD-L_1 can be interpreted as a network flow model, where each bin (j, p) is treated as a node with weight b_{jp} and has eight directed flows between itself and its four neighbours. The intuition of constraint (6.1.26) is that the difference between the total flow entering any node (j, p) on the network and the total flow leaving the node (j, p) must equal to b_{jp}. The total weight associated with all the nodes is 0 (i.e., $\sum_{(jp)\in\mathcal{I}} b_{jp} = 0$), since the two histograms Y and Z carry equal weights. Thus, the task of this network flow modelling of the EMD-L_1 is to make all nodes bear zero weights by redistributing the weights via the flows.

Owing to the new formulation, the EMD-L_1 has significantly simplified the original EMD from three aspects as follows.

- First, it reduces the number of variables from N^4 to $4N$ as shown in (6.1.25).
- Second, it decreases the number of equality constraints by fifty percent.
- Third, it converts all ground distances to ones, which it is essentially important due to the elimination of the expensive computation of ground distances.

Thus, each sub-flow $f_{j,p;c,d}$ is equivalent to the respective weighted sub-flow $f_{j,p;c,d} \times d_{j,p;c,d}$, since the respective ground distance $d_{j,p;c,d}$ is now set to one.

Moreover, a tree-based algorithm was designed in [61] as an efficient discrete optimization solver for EMD-L_1 to find a Basic Feasible (BF) solution (i.e., a spanning tree), which satisfies the constraint (6.1.26). The tree-based algorithm significantly boosts up the process of problem solving and achieves much higher efficiency than the original simplex algorithm. The underlying infrastructure to this improvement has been well illustrated in [61, pp.847-848].

6.2 DoS Attack Detection System

As the core components of comprehensive network security schemes, DoS attack detection systems defend internal networks under administrative control from being affected by the imposed malicious traffic. An overview of our proposed DoS attack detection system architecture, which complies with the detection mechanisms suggested in Chapter 3, is given in this section, in which general detection mechanism and system framework are discussed in Sections 6.2.1 and 6.2.2 .

6.2.1 General Detection Mechanisms

Four mechanisms (i.e., sample-by-sample detection, anomaly-based detectors, feature extraction based on multivariate correlation analysis and attack recognition based on computer vision techniques) are employed in the proposed DoS attack detection system to achieve the objectives of this research project. The merits of these detection mechanisms have been discussed in Chapter 3. Thus, in this section, we only attempt to answer why and how to apply computer vision techniques to attack recognition.

First, the commonalities shared between DoS attack detection and computer vision tasks (e.g., image retrieval and shape recognition) encourage us adopt the principals used in computer vision into the task of this paper. Normal traffic profiles to our DoS attack detection system are treated as queries to image retrieval tasks or shape recognition tasks. Instances of normal traffic, on one hand, are interpreted as the images or the shapes that match the queries. DoS attacks, on the other hand, are interpreted as the unmatched images or the unmatched shapes. The ideas and techniques used in computer vision tasks can be introduced to solve the problems of DoS attack detection.

Moreover, computer vision techniques, such as the EMD-L_1, make use of cross-bin correlation in assessing perceptional dissimilarity between two images, which contributes higher accuracy than other bin-to-bin dissimilarity measures (e.g., L_1, L_2 and X^2 distances) [61]. This coincides with one of the aims of our work that exploiting correlation of features in detection. In addition, partial matching, another merit supported by the EMD and its variants, helps further enhance the detection accuracy of the proposed detection system. This is because this merit allows our system to adjust its degree of tolerance to the variance of normal network traffic.

However, it is not an easy mission to formula a network intrusion detection problem as a computer vision task. The above idea cannot be applied to an existing detection system as simple as a plug-and-play component to a computer system. Since the fact that the EMD-L_1 was originally designed for shape recognition, we cannot straightly use it on either network traffic payloads or network flow statistics. To achieve the task, reformulation of the existing detection system needs to be performed to fill the gap between the EMD-L_1 and the ordinary detection. In this study, for instance, the ordinary network traffic records are converted into a kind of format that is used to represent images. Then, the EMD-L_1 can be applied to measure the dissimilarity between the transformed network traffic records.

The means that we suggest to convert network traffic records are the proposed MCA approaches discussed in Section 6.1.2. The approaches not only supply our detection system with high quality discriminative features but also facilitate the fusion of intrusion detection and computer vision. The two-dimensional EDM and TAM are taken as the images of the analysed network traffic records.

6.2.2 System Framework

In this section, we deliver the complete framework of the proposed DoS attack detection system. It elaborates the detailed processes of dimensionality reduction, normal profile generation and attack recognition. The integration of the aforementioned mechanisms and algorithms into the proposed system is also presented in the discussion below. Our proposed DoS attack detection system, shown in Fig. 6.2, is comprised of three major steps. They are Step 1: Basic Feature Generation, Step 2: Dimensionality Reduction Based on PCA and Step 3: Decision Making. Output from each step is passed down to and used as input in the next step.

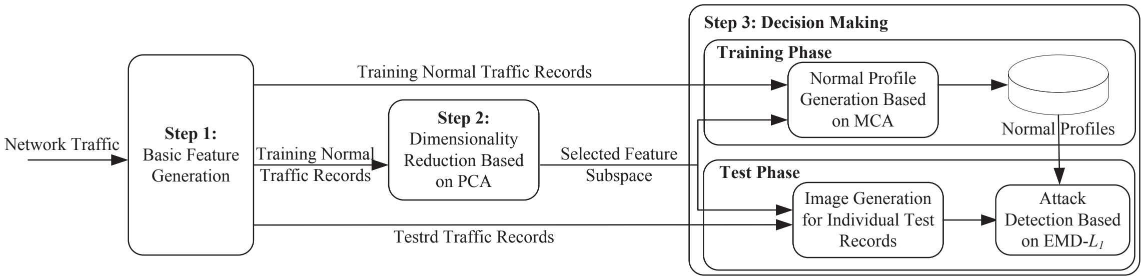

Step 3: Decision Making
Training Phase
Training Normal Traffic Records
Normal Profile Generation Based on MCA
Normal Profiles
Network Traffic
Step 1: Basic Feature Generation
Training Normal Traffic Records
Step 2: Dimensionality Reduction Based on PCA
Selected Feature Subspace
Test Phase
Image Generation for Individual Test Records
Attack Detection Based on EMD-L_1
Testrd Traffic Records

Figure 6.2: The framework for our proposed denial-of-service attack detection system

Basic Feature Generation

In this step, basic features are generated from network traffic packets captured at the destination network. Then, they are applied to construct records describing statistics for a well-defined time interval. The detailed process can be found in [84].

Dimensionality Reduction Based on PCA

This step performs dimensionality reduction using PCA for the training normal traffic records generated in Step 1. The detailed algorithm presented in Section 6.3.1 is engaged in this task. Standing out from the feature reduction techniques, our suggested dimensionality reduction algorithm does not cause loss of information due to the use of PCA which seeks the optimal subspace for the best representation of the data. The selected lower dimensional feature subspace obtained in the current step is then used in both of the Training Phase and the Test Phase in Step 3 (i.e., Decision Marking) to reduce the computational overhead.

Decision Making

This step consists of Training Phase and Test Phase. The anomaly-based detection mechanism is adopted in both of the phases. The detailed introduction to this step is given as follows.

In Training Phase, normal profiles are generated for various types of legitimate /normal traffic records (i.e., TCP, UDP and ICMP traffic) using the algorithm presented in Section 6.3.2. The normal traffic records used in this phase are identical to the set of records involved in Step 2. In the process of generation, normal profiles are built with the data projected onto the selected feature subspace recommended by Step 2. The generated normal profiles (Pro) are stored in the database and are to be used in attack detection.

In Test Phase, the sample-by-sample detection mechanism and the computer vision based attack recognition mechanism are adopted. Images of individual tested records are generated and compared against the respective normal profiles Pro from the Training Phase using the EMD-L_1. As shown in the algorithm proposed in Section 6.3.3, attack detection is modelled as a computer vision task, in which normal profiles are used as queries to retrieve the matched records (i.e., normal TCP, UDP and ICMP traffic records). Any unmatched images (records) are determined as attacks.

6.3 Relevant Algorithms

In this section, a series of algorithms are proposed to equip our system with the expected functionality. Detailed discussions are then presented to give insights into the ideas behind.

6.3.1 Algorithm for Dimensionality Reduction Based on PCA

Low dimensional feature space with an accurate representation for data makes significant contribution to accelerate the processing speed of the detection phase. Analysis that provides insight into the space where the given data reside and help determine the optimal subspace for data representation is desirable. Therefore, we suggest an algorithm shown in Fig. 6.3 for dimensionality reduction based on PCA.

```
Require: Dataset $X$ {$X$ contains $n$ instances, and each of which has $t$ features.}
Ensure: $1 \le k \le t$
$\bar{x} \leftarrow \frac{1}{n}\sum_{i=1}^{n} x_i$
$X_{zm} \leftarrow X - \bar{x}$ {Subtract $\bar{x}$ from each instance in $X$}
$C_X \leftarrow \frac{1}{n-1} X_{zm} X_{zm}^T$
Obtain $\Lambda$ and $W$, which are subject to $\Lambda W = C_X W$
for $i = 1$ to $n$ do
    $\sigma_i^2 \leftarrow \sum_{l=1}^{i} \lambda_l$
end for
Plot $\{\sigma_1^2, \sigma_2^2, \ldots, \sigma_n^2\}$
Locate the "elbow" on the scree plot and identify the index ($k$) of the "elbow" point
$W_k \leftarrow$ the selected first $k$ eigenvectors of $W$
return $W_k$
```

Figure 6.3: The algorithm for dimensionality reduction based on the PCA.

Different from the work which applied PCA to dimensionality reduction for network packet payloads [45], PCA is used in this work to determine the optimal feature subspace for a given set of network traffic records without containing packet payloads. In addition, we suggest using a cumulative-variance-based selection criterion in the feature subspace selection.

This algorithm is designed to analyse the feature space of a given dataset X, which contains n instances and each of which is comprised of t features. PCA is first conducted to investigate the contribution of the components as depicted from lines 1 to 4 in Fig. 6.3. Λ and W are sorted in descending order against the variance associated to each component. Then, cumulative variance σ_i^2 is computed with an increment of one as described in lines 5 to 7 and plotted on the screen. The "elbow" point on the up-slope plot is located to determine the first k most influential components. The motivation behind this assumption is that the cumulative variance increases rapidly until the "elbow" point, and the curve becomes flat beyond the point. This infers that the principal components beyond the "elbow" point retain very small variances and are not important to the representation of the data. An example will be given in Section 6.4.2 to demonstrate how cumulative variance plot works. Finally, once the value of k is settled, the optimal feature subspace will be obtained and denoted by W_k.

6.3.2 Algorithm for Normal Profile Generation Based on MCA

Profiles of legitimate network traffic behaviours are core components to an anomaly-based detection system. Accurate characterisation to network traffic behaviours is essential and affects the detection performance of our proposed system directly. The algorithm for normal profile generation is elaborated in Fig. 6.4. The EDM-based MCA approach and the TAM-based MCA approach are employed in the algorithm for charactering legitimate network traffic behaviours.

```
Require: Dataset $X$ and subspace $W_k$ {$X$ contains $n$ instances, and each of which has $t$ features. $W_k$ is the selected first $k$ eigenvectors of $W$.}
Initialise $DIS$ {It is an array with $n$ elements denoted by $Dis_i (1 \leq i \leq n)$.}
if using EDM-based MCA then
  Initialise $X_{EDM}$ with $n$ $k$-by-$k$ matrices denoted as $EDM_{x_i} (1 \leq i \leq n)$
else if using TAM-based MCA then
  Initialise $X_{TAM}$ with $n$ $k$-by-$k$ matrices denoted as $TAM_{x_i} (1 \leq i \leq n)$
end if
$X_{Pr} \leftarrow X \times W_k$ {$X_{Pr}$ contains $n$ instances, and each of which has $k$ features.}
if using EDM-based MCA then
  for $i = 1$ to $n$ do
    $EDM_{x_i} \leftarrow [ED^i_{j,p}]_{k \times k}$, where $1 \leq j, p \leq k$ {Euclidean distance between projected features $i$ and $j$ is computed and assigned to the $(i, j)$-th element in $EDM_{x_i}$.}
  end for
  $\overline{EDM} \leftarrow \frac{1}{n} \sum_{i=1}^{n} EDM_{x_i}$
  for $i = 1$ to $n$ do
    $Dis_i \leftarrow$ EMD- $L_1(EDM_{x_i}, \overline{EDM})$ {Earth mover's distance between $EDM_{x_i}$ and $\overline{EDM}$.}
  end for
else if using TAM-based MCA then
  for $i = 1$ to $n$ do
    $TAM_{x_i} \leftarrow [Tr^i_{j,p}]_{k \times k}$, where $1 \leq j, p \leq k$
  end for
  $\overline{TAM} \leftarrow \frac{1}{n} \sum_{i=1}^{n} TAM_{x_i}$
  for $i = 1$ to $n$ do
    $Dis_i \leftarrow$ EMD- $L_1(TAM_{x_i}, \overline{TAM})$
  end for
end if
$\overline{DIS} \leftarrow \frac{1}{n} \sum_{i=1}^{n} Dis_i$
$Std = \sqrt{\frac{1}{n} \sum_{i=1}^{n} (Dis_i - \overline{DIS})^2}$
if using EDM-based MCA then
  $Pro \leftarrow (\overline{EDM}, \overline{DIS}, Std)$
else if using TAM-based MCA then
  $Pro \leftarrow (\overline{TAM}, \overline{DIS}, Std)$
end if
return $Pro$
```

Figure 6.4: The algorithm for normal profile generation based on MCA.

A normal profile is generated based on a given training dataset X and a selected subspace W_k. The normal profile consists of three elements, namely an image ($\overline{EDM}$

or $\overline{TAM}$) of the mean of the given training samples, the mean ($\overline{DIS}$) and the standard deviation (Std) of the earth mover's distances (Dis_i) between individual training samples and the mean of the given training samples.

To develop the normal profile, an algorithm described in Fig. 6.4 is to be used. Two variables DIS and X_{EDM} (or X_{TAM}) are defined and initialised at the first place. DIS is a 1-by-n array to record the earth mover's distances between the given training samples and their mean. X_{EDM} and X_{TAM} are three-dimensional (k-by-k-by-n) matrices to store the EDM and the TAM generated for the given training samples respectively. However, only one of the two will be defined in accordance with the MCA approach chosen in the algorithm. The previously mentioned EDM and TAM are both k-by-k matrices and represent the images of the training samples.

The transformation of a training sample from a feature vector to an image is an important step in the process of normal profile generation. It builds a bridge between network traffic classification and computer vision. Since none of the computer vision techniques is initially designed for the task of network traffic classification, modification to the existing techniques or redefinition of the original problem is necessary. Thus, in this chapter we redefine our DoS attack detection problem as a computer vision problem, namely taking network traffic records as images and building up profile for these images. The details of the redefinition (transformation) are given below.

Dimensionality reduction is first conducted by projecting X onto the selected subspace W_k as shown in line 7 of Fig. 6.4 before the transformation of the given dataset X commences. Then, EDM_{x_i} or TAM_{x_i} is generated for each training sample using the corresponding MCA techniques discussed in Section 6.1.2. The mean ($\overline{EDM}$ or $\overline{TAM}$) of the image (EDM or TAM) is computed as shown in line 12 or line 20 after the transformation is completed. Afterwards, the earth mover's distance between the image of each training sample and the image of the mean of the given training samples is calculated using the EMD-L_1 and assigned to Dis_i. Upon the completion of measuring the earth mover's distances of individual training samples to the mean, the distribution of the earth mover's distances is then estimated. The mean ($\overline{DIS}$) and the standard deviation (Std) of the EMDs (Dis_i) are computed as given in lines 25 and 26 respectively. Finally, the **normal profile** is built corresponding to the chosen MCA approach as shown in line 28 (or line 29) of Fig. 6.4.

6.3.3 Algorithm for Attack Detection Based on EMD-L_1

The algorithm presented in Fig. 6.5 describes the procedure of attack recognition. To determine whether a tested sample x_{test} is legitimate or intrusive, the selected feature subspace W_k, the pre-generated normal profile Pro and parameter α are required.

```
Require: Tested sample $x_{test}$, subspace $W_k$, normal profile $Pro$ and parameter $\alpha$
$x_{test}^{Pr} \leftarrow x_{test} \times W_k$ {Project tested sample $x_{test}$ onto the subspace $W_k$.}
if using EDM-based MCA then
    $EDM_{x_{test}} \leftarrow [ED_{j,p}^{i}]_{k \times k}$, where $1 \leq j, p \leq k$
    $Dis_{test} \leftarrow$ EMD- $L_1(EDM_{x_{test}}, \overline{EDM})$
else if using TAM-based MCA then
    $TAM_{x_{test}} \leftarrow [Tr_{j,p}^{i}]_{k \times k}$, where $1 \leq j, p \leq k$
    $Dis_{test} \leftarrow$ EMD- $L_1(TAM_{x_{test}}, \overline{TAM})$
end if
if $(\overline{DIS} - \alpha \times Std) \leq Dis_{test} \leq (\overline{DIS} + \alpha \times Std)$ then
    return Normal
else
    return Attack
end if
```

Figure 6.5: The algorithm for attack detection based on the EMD-L_1.

Dimensionality reduction is performed on the tested sample x_{test} through projecting the sample onto the selected feature subspace W_k in order to enhance the detection speed and accuracy. Then, the transformation of the projected tested sample x_{test}^{Pr} to an image is conducted in accordance with the chosen MCA approach, namely the EDM-based MCA approach or the TAM-based MCA approach. The image is matched against the pre-determined query (i.e., the normal profile Pro). The similarity between the image ($EDM_{x_{test}}$ or $TAM_{x_{test}}$) of the tested sample and the mean image ($\overline{EDM}$ or $\overline{TAM}$) from the provided normal profile Pro is measured using the EMD-L_1 and assigned to Dis_{test}.

The tested sample is finally classified as an attack or a normal record using the criterion depicted in line 9 of Fig. 6.5. The lower threshold on the left most hand side and the upper threshold on the right most hand side are both determined by three parameters $\overline{DIS}$, Std and α. The parameters $\overline{DIS}$ and Std are suggested by the profile Pro developed in the phase of normal profile generation using the algorithm given in Fig. 6.4. The parameter α is ranged from 1 to 3, and it denotes the range where network traffic records are allowed to be accepted as legitimate ones in the estimated distribution of the EMDs learnt during normal profile generation.

6.4 System Evaluation

In this section, we conduct evaluations on our proposed DoS attack detection system using the KDD Cup 99 dataset [84]. During the evaluations, the 10 percent labelled data subset of the KDD Cup 99 dataset is used, where five different types of DoS attacks (Teardrop, Smurf, Pod, Neptune and Land attacks) and three types of legitimate traffic (TCP, UDP and ICMP traffic) are available. All records of the above mentioned network traffic from the 10 percent labelled data subset are first extracted. Then, they are further categorised into six groups according to their labels. The specific numbers of the filtered records can be found in Table 4.1.

6.4.1 Evaluation Metrics

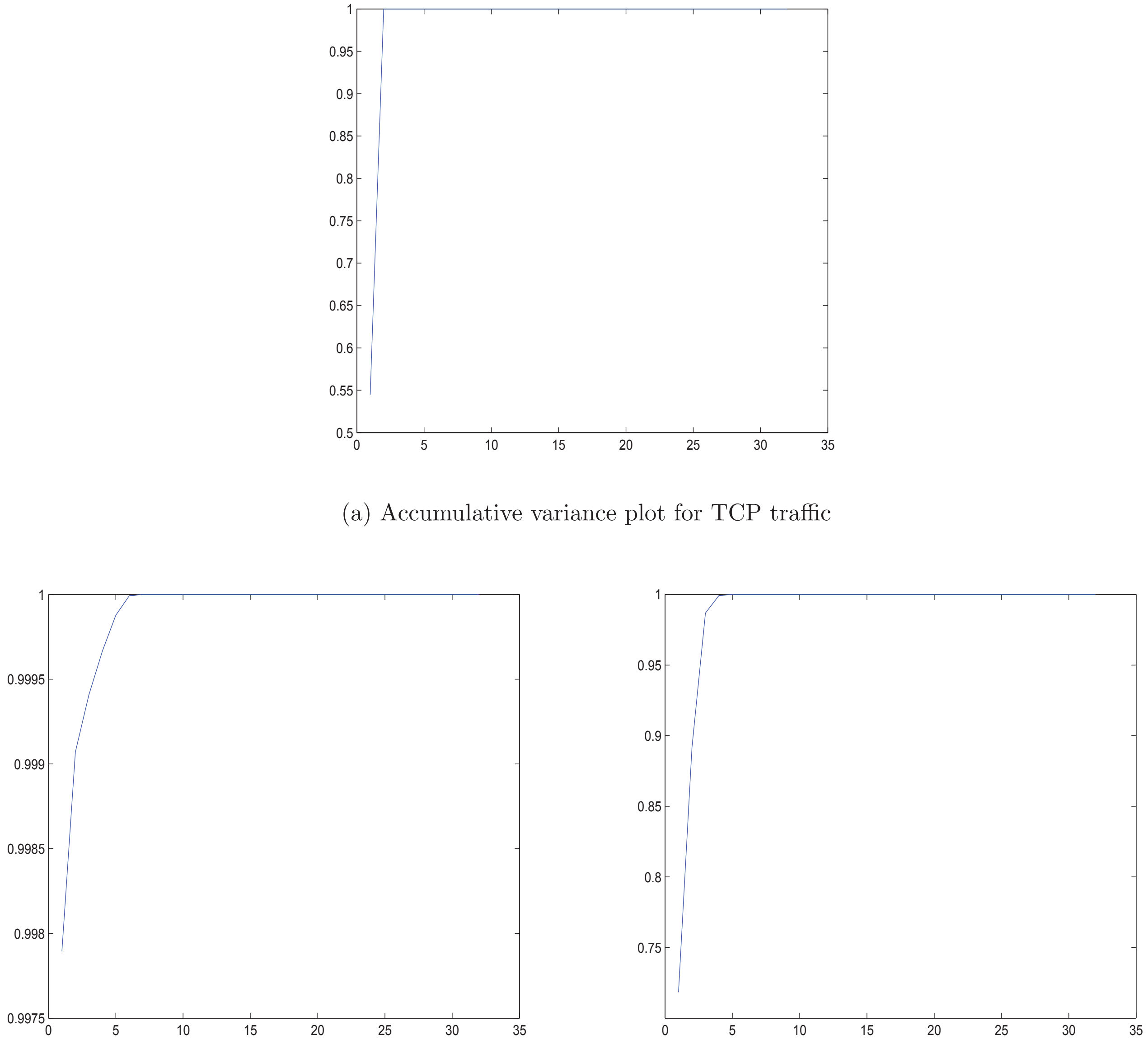
Four metrics, namely TNR, DR, FPR and Accuracy (i.e. the proportion of the overall samples which are classified correctly), are used to quantitatively estimate the performance of our proposed system.

6.4.2 Evaluations on Detection Performance

A 10-fold cross-validation is conducted to evaluate the performance of our proposed DoS attack detection system. We randomly select 70% of the filtered records shown in Table 4.1 to form an evaluation dataset. This helps avoid the bias hiding in the sequential data affecting the normal profile generation and the detection performance of the proposed system. The detailed evaluations to our proposed detection system are presented in the following.

Dimensionality Reduction

Analysis on the selected filtered legitimate (Normal) traffic is conducted using the algorithm given in Fig. 6.3 to help determine the optimal feature subspace for data representation for the entire training dataset. Three feature subspaces are chosen with respect to normal TCP, UDP and ICMP traffic. The selected feature subspaces are used in Training Phase (Section 6.4.2) and the Test Phase (Section 6.4.2) to supply with accurate representation for all records. The new lower dimensional representations of the records are used to train and to test the proposed DoS detection system.



(a) Accumulative variance plot for TCP traffic

(b) Accumulative variance plot for UDP traffic

(c) Accumulative variance plot for ICMP traffic

Figure 6.6: Accumulative variance plots for TCP, UDP and ICMP traffic

As proposed in Section 6.2.2, we apply the plot of accumulative variances in the election of the optimal feature subspaces. The up-slope on the plot indicates the potential optimal subspace for data representation. Thus, we can eliminate these less important PCs and retain only the first a few critical PCs to form a new low dimensional feature space.

To determine the number of critical PCs to be retained for various types of network traffic in our evaluators, the accumulative variance plots for normal TCP, UDP and ICMP traffic are shown in Figs. 6.6a-6.6c respectively. The horizontal axes of the figures stand for the number of PCs, and the vertical axes of the figures represent the accumulative variances with respect to the numbers of PCs shown on the horizontal axes. Table 6.1 shows where the up-slopes on the plots for TCP, UDP and ICMP traffic are found.

However, these numbers are not always practicable, and the best performance may be achieved around these numbers. For instance, using only the first two PCs to represent the TCP traffic is not applicable in our detection system. This is because the maps (i.e., EDM and TAM) constructed using only two features are always identical for all records after normalisation. Hence, we will choose the first three PCs instead of the first two PCs.

Table 6.1: The Numbers of Principle Components for Various Network Traffic

TCP	UDP	ICMP
2 PCs	6 PCs	4 PCs

Training Phase

In the Training Phase of the Decision Marking (Step 3) shown in Fig. 6.2, profiles are generated with respect to various types (i.e., TCP, UDP and ICMP) of Normal traffic records. Moreover, as the plots of the accumulative variances only suggest the preliminary results, we need to conduct further selection based on the suggestion from the preliminary outcomes from the previous section. In this work, we test three sets of PCs for each type of traffic, except TCP traffic. According to the reason given in the previous section, we decide to use the first three PCs for TCP traffic only. The numbers of PCs used in the further selection are given in Table 6.2. Normal profiles are built with respect to the chosen feature subspaces (i.e., the aforementioned numbers of PCs). Then, the generated normal profiles are utilised in the Test Phase.

Table 6.2: The Numbers of Principle Components Using in the Training and Test for Various Network Traffic

TCP	UDP			ICMP		
3 PCs	5 PCs	6 PCs	7 PCs	3 PCs	4 PCs	5 PCs

Test Phase

During the Test Phase of the Decision Marking shown in Fig. 6.2, we test our proposed detection system against both the Normal records and the attack records in the evaluation dataset. The thresholds with respect to different normal profiles are determined given the parameter α varying from 1 to 3 with an increment of 0.5. The tests run against the various sets of PCs (i.e., the selected lower dimensional subspaces) shown in Table 6.2.

The best performance is achieved on three PCs for TCP traffic and five PCs for both UDP and ICMP traffic. Tables 6.3 and 6.4 present the corresponding experimental results for the proposed detection systems based on EDM and TAM respectively.

Table 6.3: False Positive Rates, Detection Rates and Accuracies Achieved by the Proposed System Based on the EDM-based MCA Approach

	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
FPR	2.02%	1.00%	0.60%	0.56%	0.56%
DR	100.00%	99.91%	99.74%	99.72%	99.68%
Accuracy	99.95%	99.89%	99.73%	99.71%	99.68%

Table 6.4: False Positive Rates, Detection Rates and Accuracies Achieved by the Proposed System Based on the TAM-based MCA Approach

	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
FPR	1.93%	1.19%	0.63%	0.60%	0.58%
DR	100.00%	99.83%	99.68%	99.68%	93.35%
Accuracy	99.95%	99.81%	99.67%	99.67%	93.50%

As shown in the above tables, both the proposed detection system based on the EDM-based MCA approach and the one based on the TAM-based MCA approach achieve encouraging results. The threshold controls the degree of the dissimilarity, which is accepted by the system, between a test object and the respective learnt normal profile. If the dissimilarity is beyond the determined threshold, the test object is classified as an attack. On one hand, it can be seen clearly from the Tables 6.3 and 6.4 that a better FPR is achieved when a greater threshold is accepted. On the other hand, greater thresholds produce lower DRs.

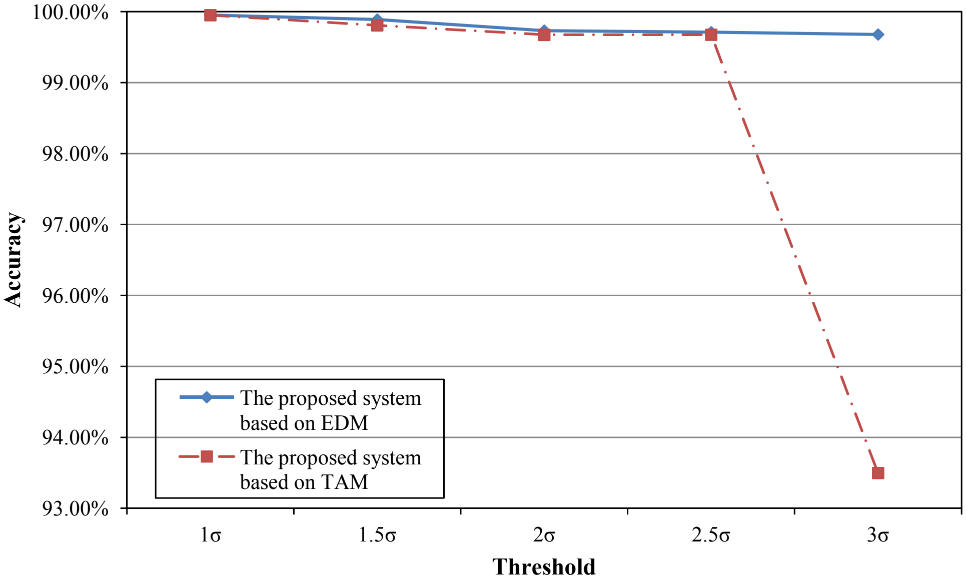


Figure 6.7: Detection accuracy versus threshold

To provide a visualisation for the relationship between Accuracy and Threshold, Fig. 6.7 is given above. The figure reveals that the greater the threshold is, the lower the detection accuracy is. It is also clearly seen from Fig. 6.7 that both the proposed detection system based on EDM and the one based on TAM enjoy promising performance with 99.95% accuracy when the threshold is set to 1σ. The accuracy of the both systems declines stably to 99.71% and 99.67% respectively at the threshold of 2.5σ. After this point, the proposed detection system based on TAM drops significantly to 93.50%, but the system based on EDM manages to achieve an accuracy of 99.68%.

6.4.3 Comparison of Performance

To show a clearer picture of how our proposed DoS attack detection system performs, we make comparisons with two other state-of-the-art detection systems in this section. These two systems are covariance feature space based network intrusion detection system [48] and network intrusion detection using triangle-area-based nearest neighbours approach [98].

In the comparisons, the best performance of these systems is selected and shown in Table 6.5. The comparison results illustrate that our proposed detection system in cooperation with either EDM or TAM achieves 99.95% accuracy which considerably outperforms the other two systems in terms of detection accuracy. Covariance feature space based network intrusion detection system [48] achieves 97.89% and network intrusion detection using triangle-area-based nearest neighbours approach delivers a 92.15% accuracy.

Although, in comparison with the DoS attack detection systems proposed in Chapters 4 and 5, this new DoS attack detection system does not show an significant advance in terms of detection accuracy. It is worth notice that the proposed system easily achieves the equal performance requiring significantly less information (i.e., fewer features involved in analysis and detection). This reduces the computational overhead.

Table 6.5: Performance Comparisons with Different Detection Approaches

	Network intrusion detection system based on covariance feature space [48] (Threshold approach with 4D principle and Cov_len3_150)	Intrusion detection system using nearest neighbour based on triangle area [98]	The proposed detection system based on EDM (Threshold = 1σ)	The proposed detection system based on TAM (Threshold = 1σ)
Accuracy	97.89%	92.15%	99.95%	99.95%

6.4.4 Analysis on Computational Complexity and Time Cost

In this section, we conduct an analysis on the computational complexity of our proposed detection system in two folds, namely the complexity of the feature extraction and the complexity of the detection.

As discussed in Section 6.1.2, during feature extraction, Euclidean distances of all possible combinations of two distinct features in a traffic record need to be computed when processing the EDM-based MCA. Since each traffic record has m features (or dimensions), m^2 Euclidean distances are generated and are used to construct a EDM. Thus, EDM-based MCA has a computational complexity of $O(m^2)$. Equally, the TAM-based MCA presented in Section 6.1.2 delivers a computational complexity of $O(m^2)$ due to the fact that m^2 triangle areas are generated and are used to construct a TAM as well. However, as both the EDM and the TAM are symmetric matrices and the elements along the main diagonals of the matrices are zeros, the numbers of the computations of these two MCA approaches can be reduced by more than 50% when they are put into practise. Whereas, this does not reduce their computational complexities. In attack detection, EMD-L_1 [61] is applied. As explained in Section 6.1.3, EMD-L_1 incurs a complexity of $O(N^2)$, where $N = m^2$ is the number of elements within a EDM or a TAM. Thus, taking the computational complexities of the feature extraction and the detection into account, the overall computational complexity of the proposed detection system is $O(m^2) + O(m^4) = O(m^4)$.

Network intrusion detection system based on covariance feature space [48] incurs a computational complexity of $O(2n \times \frac{m\times(m+1)}{2}) = O(nm^2)$ in data preprocessing, where n is the number of sequential samples in a group and m is the number of physical features of a sample. In attack detection, the observed covariance matrix of a group of sequential samples needs to be compared with all l known classes/clusters. Therefore, it has a computational complexity of $O(lm^2)$. The overall computational complexity of the network intrusion detection system based on covariance feature space is $O(nm^2) + O(lm^2) = O(lm^2)$

Triangle-area-based nearest neighbours approach [98] has an overall computational complexity of $O(ml^2)+O(l^2n^2)$, in which $O(ml^2)$ and $O(l^2n^2)$ are complexities of the data preprocessing and the attack detection respectively (m is the number of features in a traffic record, l is the number of clusters used in generating triangle areas and n is the number of training samples). The complexity can be rewritten as $O(l^2n^2)$.

In general, our proposed detection system can achieve comparable computational complexity to the two other approaches. Table 6.6 is provided to summarize the computational complexities of the above discussed approaches.

Moreover, time cost is discussed to demonstrate the capability of our proposed detection system in data processing. Approximately 58,944 traffic records and 59,738 traffic records can be proceeded per second by our DoS attack detection system in cooperation with EDM-based MCA and TAM-based MCA respectively.

Table 6.6: Computational Complexities of Different State-of-the-art Detection Approaches

The proposed DoS attack detection system based on computer vision techniques	Network intrusion detection system based on covariance feature space [48]	Intrusion detection system using nearest neighbour based on triangle area [98]
$O(m^4)$	$O(lm^2)$	$O(l^2n^2)$

6.5 Summary

This chapter has proposed a DoS attack detection system which is equipped with our previously developed MCA techniques and the EMD-L_1. The former techniques help extract the correlations between individual pairs of two distinct features within each network traffic record and offer more accurate characterization for network traffic behaviours. The latter technique facilitates our system to be able to effectively distinguish both known and unknown DoS attacks from legitimate network traffic.

Evaluation has been conducted using the KDD Cup 99 data set to verify the effectiveness and performance of the proposed DoS attack detection system. The results have revealed that our detection system achieves maximum 99.95% detection accuracy while working with either the EDM-based MCA technique or the TAM-based MCA technique. It outperforms two state-of-the-art approaches. Moreover, we have analysed the computational complexity of the proposed detection system, which achieves comparable performance in comparison with the two state-of-the-art approaches. The time cost analysis shows that the proposed detection system is able to cope with high speed network segments.

Chapter 7

Conclusions

Over the recent two decades, DoS attacks have emerged as one type of the most severe network intrusive behaviours and have posed serious threats to the infrastructures of computer networks and various network-based services. Accurate and efficient network security schemes against these attacks are essential to the availability of computer networks and network-based services.

The effective schemes to prevent the DoS attacks exploiting system vulnerabilities can be as simple as patching the systems in a timely manner. However, the flooding-based DoS attacks are hard to be handled, due to the underlying mechanisms of computer networks, which specify that connected devices need to process any network traffic addressed to them.

Among the various proposed network security schemes (i.e., detection, prevention, mitigation and response) for DoS attacks, detection is the first line in defence, which is mainly because of the nature of its functionality that provides accurate recognition of any malicious behaviours in the protected environments. The success in recognition of anomalies is a prerequisite for all the other network security schemes, including prevention, mitigation and response, to function properly. The detection of DoS attacks is required to be prompt and accurate.

To achieve the aforementioned objectives, we have conducted in-depth research on DoS attacks and developed effective schemes to analyse and to detect the DoS attacks in this thesis. A summary of the research conducted for this thesis is provided in Section 7.1, and potential future work is discussed in Section 7.2.

7.1 Summary

The review of general DoS attack detection has been conducted in Chapter 2, followed by the evaluation on the recent research contributions and achievements on network-based detection using correlation analysis techniques. Chapter 2 has also reviewed the detection approaches based on computer vision techniques proposed in the literature.

Chapter 3 has proposed a general system framework for DoS attack detection. The various detection mechanisms (i.e., network traffic monitoring at destination network, attack detection based on individual traffic records, multivariate correlation analysis, anomaly-based intrusion detection and traffic classification based on computer vision techniques) have been detailed in this chapter as well. These detection mechanisms equip all detection systems, which comply with the proposed framework, with the following desirable properties. First, these detection systems provide best-fit protections to the protected networks. Second, they can achieve a higher probability in accurate classification of a sample than any other detection systems applying the group-based detection mechanism in a general network scenario. Finally, these detection systems are capable of labelling intrusive network traffic samples individually, which is not supported by any detection system designed based on the group-based detection mechanism.

In Chapter 4, the MCA approach based on EDM has been proposed to help extract the multivariate correlations between any two distinct features of a network traffic record. The EDM-based MCA approach stands out from other existing MCA approaches, owing to its independence on prior knowledge of network traffic and its effectiveness of network traffic characterisation. The proposed EDM-based MCA approach has been evaluated using a benchmark dataset (i.e., the KDD Cup 99 dataset) on the effectiveness of network traffic characterisation. The evaluation results show that information extracted using the EDM-based MCA approach can clearly reveal the correlations between different features and accurately characterise the various types of traffic. In addition, this extracted information effectively discloses the changes of network traffic behaviours caused by DoS attacks and supplies with highly discriminative features for network traffic classification. Besides, Chapter 4 has proposed a DoS attack detection system using the EDM-based MCA approach. This detection system strictly coincides with the system framework proposed in Chapter 3. Thus, it inherits all the properties highlighted in Chapter 3. The proposed attack detection system has been evaluated using the KDD Cup 99 dataset as well. It has achieved encouraging detection accuracy on both the original data and the normalised data, and outperforms the other two state-of-the-art systems (i.e., the network intrusion detection system based on covariance feature space and the intrusion detection system using nearest neighbour based on triangle area) in terms of detection accuracy and computational complexity completely.

Chapter 5 has proposed a novel technique (i.e., TAM) to enhance and to speed up the process of MCA. This new MCA approach based on TAM is designated to study the geometrical correlations (i.e., triangle areas) between any two distinct features, and requires less computation than measuring the space distance. In the section of evaluation, it has been proven that the TAM-based MCA approach is as promising in network traffic characterisation as the EDM-based MCA approach, and consumes fewer CPU circles in processing.

In addition, another new DoS attack detection system, powered by the TAM-based MCA technique and the anomaly-based detection technique, has been suggested in Chapter 5. These two techniques equip the proposed DoS attack detection system with the capability of distinguishing both known and unknown DoS attacks from legitimate network traffic with high accuracy. The density estimation has been used to find the close boundary on one-dimensional data space for the separation of the legitimate and the attack traffic. The evaluations have been conducted using the KDD Cup 99 dataset to verify the effectiveness and the performance of the proposed DoS attack detection system. The influence of original (non-normalised) and normalised data has been studied in Chapter 5. The results have revealed that utilising statistical normalisation technique eliminates the bias from the data and boosts up the detection accuracy. Besides, the comparison result has proven that our detection system outperforms three state-of-the-art approaches (i.e., the network intrusion detection system based on covariance feature space, the intrusion detection system using nearest neighbour based on triangle area and the approach proposed in Chapter 4) in terms of detection accuracy and computational complexity. Moreover, the proposed DoS attack detection system achieves better performance in terms of time cost in comparison with the approach shown in Chapter 4.

In Chapter 6, a DoS attack detection system using computer vision techniques has been proposed, and the task of DoS attack detection has been innovatively reformulated as a computer vision task. Network traffic records are treated as images in the proposed DoS attack detection system. Legitimate traffic to DoS attack detection is equivalent to queries to image retrieval tasks or object shape recognition tasks. DoS attacks to our detection task can be interpreted as the images or the object shapes that do not match the queries. To achieve this reformulation, our previously developed MCA techniques and the EMD-L_1 are introduced to the proposed DoS attack detection system. The fusion of our proposed MCA approaches and the EMD-L_1 is unique in research literature, and the use of the EMD-L_1 in the task of DoS attack detection is also a novel attempt. The EMD-L_1 provides an unique feature (i.e., flexible and robust partial matching) to our detection system. Moreover, evaluation has been conducted using the KDD Cup 99 dataset to verify the effectiveness and performance of the proposed DoS attack detection system. The results have revealed that our detection system achieves maximum 99.95% detection accuracy while working with either the EDM-based MCA technique or the TAM-based MCA technique. It outperforms two state-of-the-art approaches (i.e., the network intrusion detection system based on covariance feature space and the intrusion detection system using nearest neighbour based on triangle area). Furthermore, we have analysed the computational complexity of the proposed detection system, which achieves comparable performance in comparison with the two state-of-the-art approaches. Last but not least, the time cost analysis shows that the proposed detection system is able to cope with high speed network segments.

7.2 Future Work

Within the realm of a set of network security schemes, Intrusion Detection Systems (IDSs) are playing an increasingly important role. Most modern-day Anomaly-based IDSs (AIDSs) have incorporated various machine learning and statistical techniques to discover the latent underlying structures of the network traffic data. With the knowledge of these underlying structures, it can then be used to achieve various purposes, such as the classification between various types of intrusions.

However, as intrusion countermeasures become more sophisticated, so do the intrusion techniques themselves. It is apparent that many of the intrusions can occur collaboratively and simultaneously on nodes throughout a network. Nowadays, attackers can initiate automated attacks targeting all vulnerable services within a network simultaneously, rather than just focusing on a specific service. Therefore, it makes traditional AIDSs developed for single node attacks susceptible to these types of attacks, and hence, unsuitable to be in a collaborative environments, such as a Cloud Computing environment.

In order to detect the coordinated attacks, Collaborative Intrusion Detection Systems (CIDSs) have been proposed to correlate suspicious evidence between different IDSs to improve the efficiency of intrusion detection. In CIDSs, network traffic summarisation is of an important precursor [41] towards reliable intrusion detection. However, traditionally, network information is collected and processed by IDS-alike software built on a single network device dealing with only the traffic flow in and out from that device. The traffic information, which the network device is capable of knowing, is hence limited, and the computation is proportional to the amount of traffic flow that the device experiences. The drawback of such approach can be found both in terms of both accuracy and efficiency:

In terms of accuracy, without the knowledge of network data from other nodes, any summarisation is built specific to some partial, insignificant portion of all available data over the entire network. The effort of exchanging and combining these summarisations alone in a later stage without the data itself is of course having a minimal gain in information.

In terms of efficiency, for a node with denser traffic, an additional computation is required to process summarisation. As summarisation itself is of a pure overhead operation, therefore, in an ideal environment, one would prefer a node having less traffic (subsequently requires lesser processing) to spend more time in performing summarisation tasks.

With the large dense network of nodes forming a cloud environment, firstly, it presents us with the unprecedented opportunities where network data from all nodes can be made readily available. At the same time, the challenge itself is also unprecedented in a sense that one must perform summarisation and combine the results in a distributed and parallel manner, by utilising all available processing powers within the network. At the same time, as we are now dealing with all network data of the entire cloud, where an unknown number of categories can possibly exist. Therefore, the summarisation algorithms will need to expand its categories in an “on-demand” fashion, that is to automatically creates new clusters, once it discovers new types of traffic is emerging.

It is a potential future work in network intrusion detection to build on the statistical theories recently developed from parallel inference and to reformulate and propose novel mathematical models for parallel summarisation of network traffic for a large, dense, dynamic and cloud computing environment.

Bibliography

[1] *Towards a taxonomy of intrusion-detection systems*, Comput. Netw. **31** (1999), no. 9, 805–822.

[2] Raz Abramov and Amir Herzberg, *TCP Ack storm DoS attacks*, Computers & Security **33** (2013), no. 0, 12 – 27, Future Challenges in Security and Privacy for Academia and Industry.

[3] PwC Austarlia, *Australian online shopping market and digital insights*, 2012.

[4] M. Bando, N.S. Artan, and H.J. Chao, *Scalable lookahead regular expression detection system for deep packet inspection*, Networking, IEEE/ACM Transactions on **20** (2012), no. 3, 699–714.

[5] Mokhtar S Bazaraa, John J Jarvis, and Hanif D Sherali, *Linear programming and network flows*, Wiley. com, 2011.

[6] Robert Beverly and Steven Bauer, *The spoofer project: Inferring the extent of source address filtering on the internet*, Proceedings of USENIX Steps to Reducing Unwanted Traffic on the Internet (SRUTI) Workshop, July 2005, pp. 53–59.

[7] Damiano Bolzoni and Sandro Etalle, *Aphrodite: an anomaly-based architecture for false positive reduction*, CoRR **abs/cs/0604026** (2006).

[8] Bernhard E. Boser, Isabelle M. Guyon, and Vladimir N. Vapnik, *A training algorithm for optimal margin classifiers*, Proceedings of the Fifth Annual Workshop on Computational Learning Theory (New York, NY, USA), COLT '92, ACM, 1992, pp. 144–152.

[9] A. Bremler-Barr and Y. Koral, *Accelerating multipattern matching on compressed http traffic*, Networking, IEEE/ACM Transactions on **20** (2012), no. 3, 970–983.

[10] Christopher J. C. Burges, *A tutorial on support vector machines for pattern recognition*, Data Min. Knowl. Discov. **2** (1998), no. 2, 121–167.

[11] A.A. Cardenas, J.S. Baras, and V. Ramezani, *Distributed change detection for worms, DDoS and other network attacks*, American Control Conference, 2004. Proceedings of the 2004, vol. 2, 2004, pp. 1008–1013 vol.2.

[12] CERT Coordination Center, *CERT Advisory CA-1996-01 UDP Port Denial-of-Service Attack*.

[13] CERT Coordination Center, *CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks*.

[14] CERT Coordination Center, *CERT Advisory CA-1996-26 Denial-of-Service Attack via ping*.

[15] CERT Coordination Center, *CERT Advisory CA-1997-28 IP Denial-of-Service Attacks*, December.

[16] CERT Coordination Center, *CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks*.

[17] Yu Chen, Kai Hwang, and Wei-Shinn Ku, *Collaborative Detection of DDoS Attacks over Multiple Network Domains*, Parallel and Distributed Systems, IEEE Transactions on **18** (2007), no. 12, 1649–1662.

[18] Yu Chen, Kai Hwang, and Wei-Shinn Ku, *Collaborative detection of ddos attacks over multiple network domains*, Parallel and Distributed Systems, IEEE Transactions on **18** (2007), no. 12, 1649–1662.

[19] Evan Cooke, Farnam Jahanian, and Danny McPherson, *The zombie roundup: understanding, detecting, and disrupting botnets*, Proceedings of the Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop (Berkeley, CA, USA), SRUTI'05, USENIX Association, 2005, pp. 6–6.

[20] route daemon9 and infinity, *Project Neptune*, 1990.

[21] Dorothy E. Denning, *An intrusion-detection model*, IEEE Trans. Softw. Eng. **13** (1987), no. 2, 222–232.

[22] J.E. Dickerson and J.A. Dickerson, *Fuzzy network profiling for intrusion detection*, Fuzzy Information Processing Society, 2000. NAFIPS. 19th International Conference of the North American, 2000, pp. 301–306.

[23] J.E. Dickerson, J. Juslin, O. Koukousoula, and J.A. Dickerson, *Fuzzy intrusion detection*, IFSA World Congress and 20th NAFIPS International Conference, 2001. Joint 9th, vol. 3, 2001, pp. 1506–1510 vol.3.

[24] Gavrilis Dimitris, Tsoulos Ioannis, and Dermatas Evangelos, *Feature selection for robust detection of distributed denial-of-service attacks using genetic algorithms*, Methods and Applications of Artificial Intelligence (GeorgeA. Vouros and Themistoklis Panayiotopoulos, eds.), Lecture Notes in Computer Science, vol. 3025, Springer Berlin Heidelberg, 2004, pp. 276–281.

[25] Christos Douligeris and Aikaterini Mitrokotsa, *DDoS attacks and defense mechanisms: classification and state-of-the-art*, Computer Networks **44** (2004), no. 5, 643 – 666.

[26] Christos Douligeris and Aikaterini Mitrokotsa, *DDoS attacks and defense mechanisms: classification and state-of-the-art*, Computer Networks **44** (2004), no. 5, 643 – 666.

[27] Vegard Engen, Jonathan Vincent, and Keith Phalp, *Exploring discrepancies in findings obtained with the kdd cup '99 data set*, Intell. Data Anal. **15** (2011), no. 2, 251–276.

[28] Eleazar Eskin, Andrew Arnold, Michael Prerau, Leonid Portnoy, and Sal Stolfo, *A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data*, Applications of Data Mining in Computer Security, Kluwer, 2002.

[29] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, *Statistical approaches to ddos attack detection and response*, DARPA Information Survivability Conference and Exposition, 2003. Proceedings, vol. 1, 2003, pp. 303–314 vol.1.

[30] P. Ferguson and D. Senie, *Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing*, 1998.

[31] Yoav Freund and Robert E Schapire, *A decision-theoretic generalization of on-line learning and an application to boosting*, Journal of Computer and System Sciences **55** (1997), no. 1, 119 – 139.

[32] A.Y. Fu, Liu Wenyin, and Xiaotie Deng, *Detecting phishing web pages with visual similarity assessment based on earth mover's distance (emd)*, Dependable and Secure Computing, IEEE Transactions on **3** (2006), no. 4, 301–311.

[33] Dimitris Gavrilis and Evangelos Dermatas, *Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features*, Computer Networks **48** (2005), no. 2, 235 – 245.

[34] V.D. Gligor, *A note on denial-of-service in operating systems*, Software Engineering, IEEE Transactions on **SE-10** (1984), no. 3, 320–324.

[35] Dieter Gollmann, *Computer security*, Wiley Interdisciplinary Reviews: Computational Statistics **2** (2010), no. 5, 544–554.

[36] Lawrence A Gordon, Mar-tin P Loeb, William Lucyshyn, and Robert Richardson, *2005 csi-/fbi computer crime and security survey*, Computer Security Institute, 2005.

[37] K. Grauman and T. Darrell, *Fast contour matching using approximate earth mover's distance*, Computer Vision and Pattern Recognition, 2004. CVPR 2004. Proceedings of the 2004 IEEE Computer Society Conference on, vol. 1, 2004, pp. I–220–I–227 Vol.1.

[38] Y. Guan, A.A. Ghorbani, and N. Belacel, *Y-means: a clustering method for intrusion detection*, Electrical and Computer Engineering, 2003. IEEE CCECE 2003. Canadian Conference on, vol. 2, 2003, pp. 1083–1086 vol.2.

[39] F.S. Hillier and G.J. Lieberman, *Introduction to mathematical programming*, McGraw-Hill series in industrial engineering and management science, McGraw-Hill, 1995.

[40] Frank L Hitchcock, *The distribution of a product from several sources to numerous localities*, J. Math. Phys **20** (1941), no. 2, 224–230.

[41] Demetris Hoplaros, Zahir Tari, and Ibrahim Khalil, *Data summarization for network traffic monitoring*, Journal of Network and Computer Applications (2013), no. 0, –.

[42] Weiming Hu, Wei Hu, and S. Maybank, *AdaBoost-Based Algorithm for Network Intrusion Detection*, Trans. Sys. Man Cyber. Part B **38** (2008), no. 2, 577–583.

[43] Harold Edwin Hurst, Robert Pearson Black, and YM Simaika, *Long-term storage: an experimental study*, Constable, 1965.

[44] A. Hussain, J. Heidemann, and C. Papadopoulos, *Identification of repeated denial of service attacks*, INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings, 2006, pp. 1–15.

[45] Aruna Jamdagni, Zhiyuan Tan, Xiangjian He, Priyadarsi Nanda, and Ren Ping Liu, *Repids: A multi tier real-time payload-based intrusion detection system*, Computer Networks **57** (2013), no. 3, 811 – 824.

[46] Aruna Jamdagni, Zhiyuan Tan, Priyadarsi Nanda, Xiangjian He, and Ren Ping Liu, *Intrusion detection using GSAD model for HTTP traffic on web services*, Proceedings of the 6th International Wireless Communications and Mobile Computing Conference (New York, NY, USA), IWCMC '10, ACM, 2010, pp. 1193–1197.

[47] Muhammad Asim Jamshed, Jihyung Lee, Sangwoo Moon, Insu Yun, Deokjin Kim, Sungryoul Lee, Yung Yi, and KyoungSoo Park, *Kargus: a highly-scalable software-based intrusion detection system*, Proceedings of the 2012 ACM conference on Computer and communications security (New York, NY, USA), CCS '12, ACM, 2012, pp. 317–328.

[48] Shuyuan Jin, Daniel So Yeung, and Xizhao Wang, *Network intrusion detection in covariance feature space*, Pattern Recognition **40** (2007), no. 8, 2185 – 2197, Part Special Issue on Visual Information Processing.

[49] Juniper Networks, Inc., *Understanding ICMP Flood Attacks*.

[50] Juniper Networks, Inc., *Understanding Teardrop Attacks*, 2013.

[51] R.A. Kemmerer and G. Vigna, *Intrusion detection: a brief history and overview*, Computer **35** (2002), no. 4, 27–30.

[52] Seong Soo Kim and A. L. Narasimha Reddy, *Statistical techniques for detecting traffic anomalies through packet header data*, IEEE/ACM Trans. Netw. **16** (2008), no. 3, 562–575.

[53] Donald E. Knuth, *The art of computer programming, volume 1 (3rd ed.): fundamental algorithms*, Addison Wesley Longman Publishing Co., Inc., Redwood City, CA, USA, 1997.

[54] Christopher Krugel, Fredrik Valeur, and Giovanni Vigna, *Intrusion detection and correlation : challenges and solutions*, vol. 14, Springer, 2005.

[55] Keunsoo Lee, Juhyun Kim, Ki Hoon Kwon, Younggoo Han, and Sehun Kim, *DDoS attack detection method using cluster analysis*, Expert Systems with Applications **34** (2008), no. 3, 1659 – 1665.

[56] Wenke Lee and Dong Xiang, *Information-theoretic measures for anomaly detection*, Proceedings of the 2001 IEEE Symposium on Security and Privacy (Washington, DC, USA), SP '01, IEEE Computer Society, 2001, pp. 130–.

[57] John Zhong Lei and Ali A. Ghorbani, *Improved competitive learning neural networks for network intrusion and fraud detection*, Neurocomputing **75** (2012), no. 1, 135 – 145.

[58] E. Levy, *Approaching zero [attack trends]*, Security Privacy, IEEE **2** (2004), no. 4, 65–66.

[59] Ming Li, *An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition*, Computers & Security **23** (2004), no. 7, 549 – 558.

[60] Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung, *Intrusion detection system: A comprehensive review*, Journal of Network and Computer Applications **36** (2013), no. 1, 16 – 24.

[61] Haibin Ling and K. Okada, *An efficient earth mover's distance algorithm for robust histogram comparison*, Pattern Analysis and Machine Intelligence, IEEE Transactions on **29** (2007), no. 5, 840–853.

[62] Georgios Loukas and Gülay Öke, *Protection against denial of service attacks*, Comput. J. **53** (2010), no. 7, 1020–1037.

[63] Charles E Metz et al., *Receiver operating characteristic analysis: a tool for the quantitative evaluation of observer performance and imaging systems*, Journal of the American College of Radiology **3** (2006), no. 6, 413–422.

[64] Alessandro Micarelli and Giuseppe Sansonetti, *A case-based approach to anomaly intrusion detection*, Machine Learning and Data Mining in Pattern Recognition (Petra Perner, ed.), Lecture Notes in Computer Science, vol. 4571, Springer Berlin Heidelberg, 2007, pp. 434–448.

[65] Jelena Mirkovic and Peter Reiher, *D-WARD: A source-end defense against flooding denial-of-service attacks*, IEEE Transactions on Dependable and Secure Computing **2** (2005), no. 3, 216–232.

[66] G.V. Moustakides, *Quickest detection of abrupt changes for a class of random processes*, Information Theory, IEEE Transactions on **44** (1998), no. 5, 1965–1968.

[67] Srinivas Mukkamala, Andrew H. Sung, and Ajith Abraham, *Intrusion detection using an ensemble of intelligent paradigms*, Journal of Network and Computer Applications **28** (2005), no. 2, 167 – 182.

[68] John Nagle, *Congestion control in ip/tcp internetworks*, (1984).

[69] Sanguk Noh, Cheolho Lee, Kyunghee Choi, and Gihyun Jung, *Detecting distributed denial of service (ddos) attacks through inductive learning*, Intelligent

Data Engineering and Automated Learning (Jiming Liu, Yiu-ming Cheung, and Hujun Yin, eds.), Lecture Notes in Computer Science, vol. 2690, Springer Berlin Heidelberg, 2003, pp. 286–295.

[70] Australian Bureau of Statistics, *8146.0 - Household Use of Information Technology, Australia, 2010-11 - Internet Acitvities at Home*, 2012.

[71] Animesh Patcha and Jung-Min Park, *An overview of anomaly detection techniques: Existing solutions and latest technological trends*, Computer Networks **51** (2007), no. 12, 3448 – 3470.

[72] Vern Paxson, *Bro: a system for detecting network intruders in real-time*, Computer Netowrks **31** (1999), no. 23-24, 2435–2463.

[73] Vern Paxson, *An analysis of using reflectors for distributed denial-of-service attacks*, SIGCOMM Comput. Commun. Rev. **31** (2001), no. 3, 38–47.

[74] Dai ping Liu, Ming wei Zhang, and Tao Li, *Network traffic analysis using refined bayesian reasoning to detect flooding and port scan attacks*, Advanced Computer Theory and Engineering, 2008. ICACTE '08. International Conference on, 2008, pp. 1000–1004.

[75] Leonid Portnoy, Eleazar Eskin, and Sal Stolfo, *Intrusion detection with unlabeled data using clustering*, In Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001, 2001, pp. 5–8.

[76] Martin Roesch, *Snort - lightweight intrusion detection for networks*, Proceedings of the 13th USENIX conference on System administration (Berkeley, CA, USA), LISA '99, USENIX Association, 1999, pp. 229–238.

[77] Y. Rubner, C. Tomasi, and L.J. Guibas, *A metric for distributions with applications to image databases*, Com-puter Vision, 1998. Sixth International Conference on, 1998, pp. 59–66.

[78] Yossi Rubner, Carlo Tomasi, and LeonidasJ. Guibas, *The earth mover's distance as a metric for image retrieval*, International Journal of Computer Vision **40** (2000), no. 2, 99–121 (English).

[79] Benjamin Sangster, T OConnor, Thomas Cook, Robert Fanelli, Erik Dean, William J Adams, Chris Morrell, and Gregory Conti, *Toward instrumenting network warfare competitions to generate labeled datasets*, Proc. of the 2nd Workshop on Cyber Security Experimentation and Test (CSET09), 2009.

[80] S.T. Sarasamma, Q.A. Zhu, and J. Huff, *Hierarchical kohonenen Net for anomaly detection in network security*, Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on **35** (2005), no. 2, 302–312.

[81] Bernhard Schölkopf, John C. Platt, John C. Shawe-Taylor, Alex J. Smola, and Robert C. Williamson, *Estimating the support of a high-dimensional distribution*, Neural Comput. **13** (2001), no. 7, 1443–1471.

[82] Ali Shiravi, Hadi Shiravi, Mahbod Tavallaee, and Ali A. Ghorbani, *Toward developing a systematic approach to generate benchmark datasets for intrusion detection*, Computers

[83] Jungsuk Song, Kenji Ohira, Hiroki Takakura, Yasuo Okabe, and Yongjin Kwon, *A clustering method for improving performance of anomaly-based intrusion detection system*, IEICE - Trans. Inf. Syst. **E91-D** (2008), no. 5, 1282–1291.

[84] S.J. Stolfo, Wei Fan, Wenke Lee, A. Prodromidis, and P.K. Chan, *Cost-based modeling for fraud and intrusion detection: results from the jam project*, DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00. Proceedings, vol. 2, 2000, pp. 130–144 vol.2.

[85] S. Surisetty and S. Kumar, *Is mcafee securitycenter/firewall software providing complete security for your computer?*, Digital Society, 2010. ICDS '10. Fourth International Conference on, 2010, pp. 178–181.

[86] Arman Tajbakhsh, Mohammad Rahmati, and Abdolreza Mirzaei, *Intrusion detection using fuzzy association rules*, Applied Soft Computing **9** (2009), no. 2, 462 – 469.

[87] Zhiyuan Tan, A. Jamdagni, Xiangjian He, and P. Nanda, *Network Intrusion Detection based on LDA for payload feature selection*, GLOBECOM Workshops (GC Wkshps), 2010 IEEE, 2010, pp. 1545–1549.

[88] Zhiyuan Tan, A. Jamdagni, Xiangjian He, P. Nanda, and Ren Ping Liu, *Triangle-area-based multivariate correlation analysis for effective denial-of-service attack detection*, Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, 2012, pp. 33–40.

[89] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda, and Ren Ping Liu, *Detection of denial-of-service attacks based on computer vision techniques*, Networking, IEEE /ACM Transactions on, Submitted for review on 25th May 2013.

[90] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda, and RenPing Liu, *Denial-of-service attack detection based on multivariate correlation analysis*, Neural Information Processing (Bao-Liang Lu, Liqing Zhang, and James Kwok, eds.), Lecture Notes in Computer Science, vol. 7064, Springer Berlin Heidelberg, 2011, pp. 756–765.

[91] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda, and RenPing Liu, *Multivariate correlation analysis technique based on euclidean distance map*

for network traffic characterization, Information and Communications Security (Sihan Qing, Willy Susilo, Guilin Wang, and Dongmei Liu, eds.), Lecture Notes in Computer Science, vol. 7043, Springer Berlin Heidelberg, 2011, pp. 388–398.

[92] Zhiyuan Tan, Aruna Jamdagni, Priyadarsi Nanda, Xiangjian He, and Ren Ping Liu, *Evaluation on multivariate correlation analysis based denial-of-service attack detection system*, Proceedings of the First International Conference on Security of Internet of Things (New York, NY, USA), SecurIT '12, ACM, 2012, pp. 160–164.

[93] Zhiyuan Tan, Priyadarsi Nanda, Ren Ping Liu, Aruna Jamdagni, and Xiangjian He, *A system for denial-of-service attack detection based on multivariate correlation analysis*, IEEE Transactions on Parallel and Distributed Systems (2013), 1.

[94] M. Tavallaee, E. Bagheri, Wei Lu, and A.A. Ghorbani, *A detailed analysis of the kdd cup 99 data set*, Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on, 2009, pp. 1–6.

[95] M. Tavallaee, Wei Lu, S.A. Iqbal, and A.A. Ghorbani, *A novel covariance matrix based approach for detecting network anomalies*, Communication Networks and Services Research Conference, 2008. CNSR 2008. 6th Annual, 2008, pp. 75–81.

[96] Gautam Thatte, Urbashi Mitra, and John Heidemann, *Parametric methods for anomaly detection in aggregate traffic*, IEEE/ACM Trans. Netw. **19** (2011), no. 2, 512–525.

[97] M. Thottan and Chuanyi Ji, *Anomaly detection in ip networks*, Signal Processing, IEEE Transactions on **51** (2003), no. 8, 2191–2204.

[98] Chih-Fong Tsai and Chia-Ying Lin, *A triangle area based nearest neighbors approach to intrusion detection*, Pattern Recognition **43** (2010), no. 1, 222 – 229.

[99] B. Tsybakov and Nicolas D. Georganas, *Self-similar processes in communications networks*, Information Theory, IEEE Transactions on **44** (1998), no. 5, 1713–1725.

[100] K.K.K. Wan and R.K.C. Chang, *Engineering of a global defense infrastructure for ddos attacks*, Networks, 2002. ICON 2002. 10th IEEE International Conference on, 2002, pp. 419–427.

[101] Haining Wang, Danlu Zhang, and K.G. Shin, *Change-point monitoring for the detection of dos attacks*, Dependable and Secure Computing, IEEE Transactions on **1** (2004), no. 4, 193–208.

[102] Wei Wang, Xiangliang Zhang, S. Gombault, and S.J. Knapskog, *Attribute normalization in network intrusion detection*, Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on, 2009, pp. 448–453.

[103] X. Yang, W. Zhou, M. Chowdhury, and Deakin University. School of Information Technology, *A survey of active and passive defence mechanisms against ddos attacks*, Technical reports. Computing series, Deakin University, School of Information Technology, 2004.

[104] Ting-Fang Yen and M.K. Reiter, *Are Your Hosts Trading or Plotting Telling P2P File-Sharing and Bots Apart*, Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on, 2010, pp. 241–252.

[105] D.S. Yeung, Shuyuan Jin, and Xizhao Wang, *Covariance-matrix modeling and detecting various flooding attacks*, Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on **37** (2007), no. 2, 157–169.

[106] C.-F. Yu and V.D. Gligor, *A specification and verification method for preventing denial of service*, Software Engineering, IEEE Transactions on **16** (1990), no. 6, 581–592.

[107] Jaehak Yu, Hansung Lee, Myung-Sup Kim, and Daihee Park, *Traffic flooding attack detection with SNMP MIB using SVM*, Computer Communications **31** (2008), no. 17, 4212 – 4219.

[108] Shui Yu, Wanlei Zhou, Weijia Jia, Song Guo, Yong Xiang, and Feilong Tang, *Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient*, Parallel and Distributed Systems, IEEE Transactions on **23** (2012), no. 6, 1073–1080.

[109] Qi Zhao, Zhi Yang, and Hai Tao, *Differential earth mover's distance with its applications to visual tracking*, Pattern Analysis and Machine Intelligence, IEEE Transactions on **32** (2010), no. 2, 274–287.