Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 1542657, 9 pages
https://doi.org/10.1155/2021/1542657

Research Article

Intelligent Detection System Enabled Attack Probability Using Markov Chain in Aerial Networks

Inam Ullah Khan,[1] **Asrin Abdollahi**,[2] **Ryan Alturki**,[3] **Mohammad Dahman Alshehri**,[4] **Mohammed Abdulaziz Ikram**,[5] **Hasan J. Alyamani**,[6] **and Shahzad Khan**[7]

[1]*Department of Electronic Engineering, School of Engineering and Applied Sciences, Isra University, Islamabad, Pakistan*
[2]*Department of Electrical Engineering, University of Kurdistan, Sanandaj, Iran*
[3]*Department of Information Science, College of Computer and Information Systems, Umm AlQura University, Makkah, Saudi Arabia*
[4]*Department of Computer Science, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia*
[5]*Computer Science Department, University College in Al-Jamoum, Umm Al-Qura University, Saudi Arabia*
[6]*Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Rabigh, Saudi Arabia*
[7]*Department of Computer Science, Abdul Wali Khan University Mardan, 23200 Mardan, KPK, Pakistan*

Correspondence should be addressed to Asrin Abdollahi; a.abdollahi@eng.uok.ac.ir

Received 13 April 2021; Accepted 18 August 2021; Published 9 September 2021

Academic Editor: Ihsan Ali

The Internet of Things (IoT) plays an important role to connect people, data, processes, and things. From linked supply chains to big data produced by a large number of IoT devices to industrial control systems where cybersecurity has become a critical problem in IoT-powered systems. Denial of Service (DoS), distributed denial of service (DDoS), and ping of death attacks are significant threats to flying networks. This paper presents an intrusion detection system (IDS) based on attack probability using the Markov chain to detect flooding attacks. While the paper includes buffer queue length by using queuing theory concept to evaluate the network safety. Also, the network scenario will change due to the dynamic nature of flying vehicles. Simulation describes the queue length when the ground station is under attack. The proposed IDS utilizes the optimal threshold to make a tradeoff between false positive and false negative states with Markov binomial and Markov chain distribution stochastic models. However, at each time slot, the results demonstrate maintaining queue length in normal mode with less packet loss and high attack detection.

1. Introduction

Flying ad hoc networks have changed human life where wireless communication is utilized as a backbone technology. Flying networks have remote nodes that can switch along with all three directions [1]. The term "flying ad hoc network" represents a complex pattern of mobility with constantly changing physical structures [2].

Secure communication channels must be designed to improve connectivity within the network. Dealing with false data injection attacks, an intruder can take data during remote surgery, which can lead to the death of a patient. Also, in defense operations, aerial vehicles are used to trigger false data attacks in the surrounding environment, which causes very serious destruction [3]. However, the probability of Poisson distribution is used for the detection of ping of

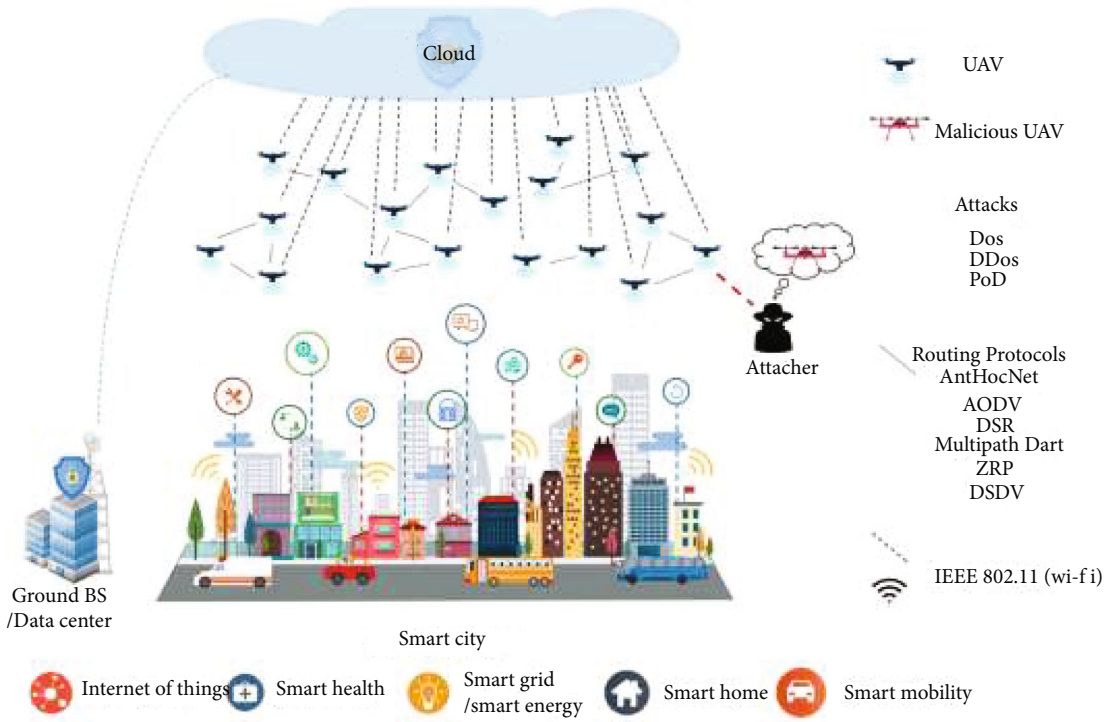

Figure 1: Intruder/attacker within IoT network.

death attacks that secure data packets [4]. Several security attacks are recorded from 1982 till now in different industries. In 2014, a special type of attack occurred, which was later on called Trojan, where the main target was petroleum pipeline networks [5].

Detecting cybercrimes over the internet can be identified using an intrusion detection system by using different techniques and tools [6]. However, a swarm of drones can protect an entire IoT network [7]. Detection of security attacks is a major problem; this research study formulates the scenario on quadcopter using open-source software [8]. Therefore, a tree-based strategy can easily portray the moves of intruders/attackers; also, for risk evaluation, a game-theory scheme is used [9]. Every technology is just made to facilitate mankind; for this purpose, aerial vehicles can be used to safeguard women [10].

The proposed scheme is focused on reducing queue data packets in flying networks which is a tough task to tackle. The aim of this paper is to explore the IDS model and how it can be improved using a Markov chain approach. Using flying networks, the IDS architecture has been developed to reduce data packets in the queue at different stages. Figure 1 explains the concept of an intruder within an IoT network to demonstrate a practical scenario. The main contributions of this study include some important points, which are given below.

(1) For the identification of security threats, an intrusion detection system is modeled

(2) Denial-off-service, distributed denial of service, and ping of death attacks are simulated in flying vehicles

(3) Markov chain distribution is used to enhance security countermeasures

The rest of the article is organized as follows. In Section 1, brief literature relevant to the problem is studied. The proposed scheme is elaborated in Section 3, followed by simulation results and theoretical analysis in Section 4. The future research directions and paper's conclusion are given in Section 5.

2. Literature Survey

Every new technology is first used by military, later on, it becomes commercialized. However, in US, due to flying vehicles, some accidents take place, like if a drone comes in the way of airplane while landing. Apart from that, many other issues occur due to the technical fault in quadcopters or small UAV's. As communication plays an important role but major issue in day-to-day life is to secure transmission links [11]. The demand of aerial vehicles is increasing on daily basis. In normal flying systems, there is the concept of pilot but drone is basically unmanned which makes them unsafe or unprotected [12]. The two popular areas like machine learning and software-define-networks can provide a pathway to address the challenges related to security in terms of internet of everything [13, 14].

Wireless vision (Wi-Vi) sensors are put in service for self-controlled flying vehicles [15]. The indoor scenario is very much mature using the wireless network; therefore, channel state information can give accurate data about location coordinates [16]. A novel framework is introduced,

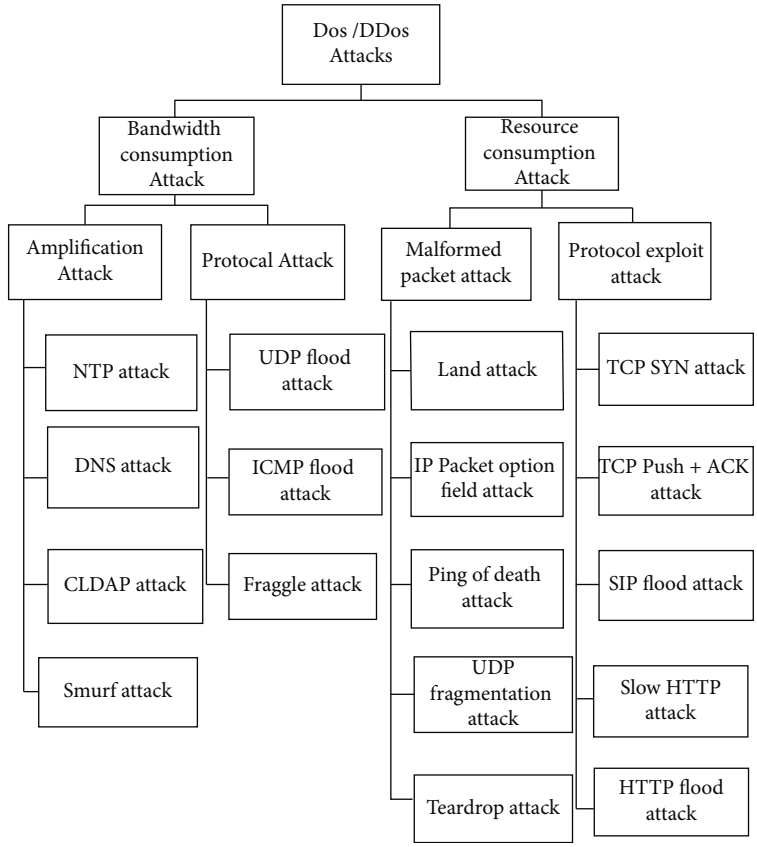

Figure 2: Classification of DoS/D-DoS security threats.

which has flying vehicle-enabled IoT using a 5G communication network. Human safety is the prime focus of every technology. In this context, if the flying drone having sensitive information is hijacked or attacked, it may result a big threat to the environment. Flying thing-based architecture is initiated which gives a solution mechanism for security and privacy to secure U2U communication [17]. Heuristic computational drone-based projects must be having pragmatic results in civil and military fields [18]. While working on false alarm threat, intrusion detection system can be utilized [4]. Furthermore, the classifications of DoS/D-DoS security threats are shown in Figure 2.

3. Intelligent Detection System (Proposed Scheme)

The proposed study is having physical topology with thirty drones ($N = 30$) and one ground station. Two major scenarios are mentioned either "no attack" or "with attack." Assuming that our internetwork is secure and there is no intruder inside the system. For this purpose, aerial vehicles send data packets having an average length which is cited as λ_l. Apart from that, aerial network modeling can be concluded for generating information of arrival data net which lined up in the entry to pinpoint land station. Figure 3 shows the physical structure of IDS in land station where malicious data packets can be removed easily.

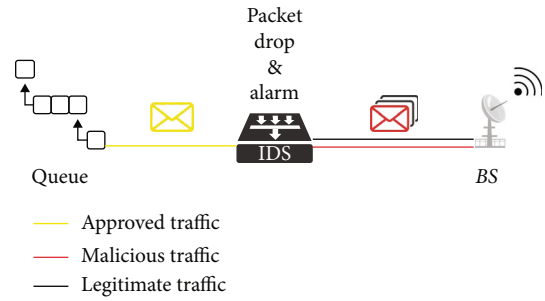

Figure 3: Physical structure of IDS in land station.

The evolution of queue length is calculated using the following equation:

$$Q(t+1) = Q(t) + \lambda(t) - \mu(t), \tag{1}$$

where $Q(t) > 0$, $Q(t)$ is queue length, $\lambda(t)$ is arrival rate, $\mu(t)$ is out rate or departed data rate.

The above metric values can be either constant or random. Furthermore, the randomness can be generated using Poisson distribution. The four probabilistic options are practically demonstrated in Figure 4 as mentioned.

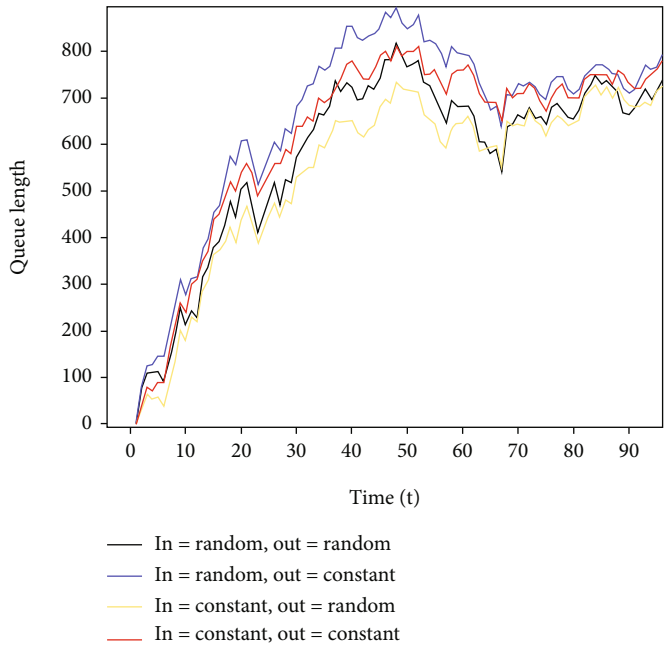

Figure 4: Probabilistic experimentation for generating queue.

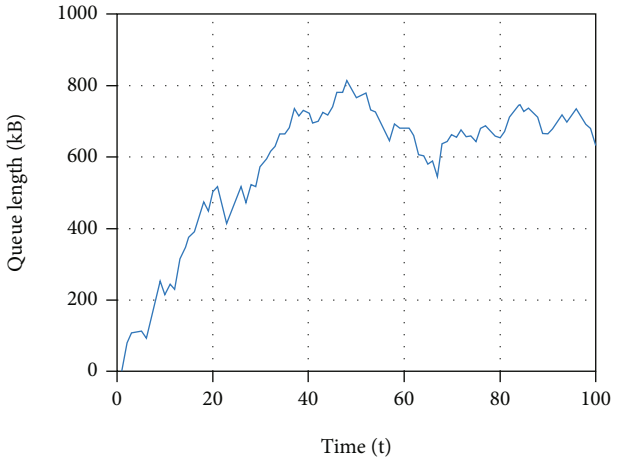

Figure 5: Queue length with Poisson variable.

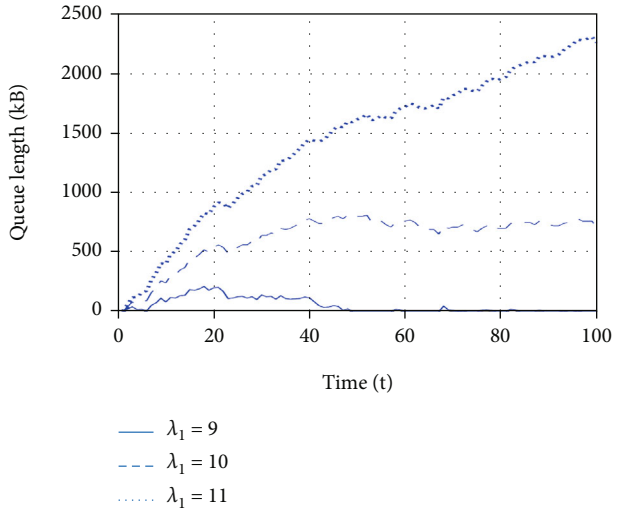

Figure 6: Impact λ_l on the queue length without μ_{avg}.

For $t = 100$ sec, the Poisson random variable with queued length is followed in Figure 5.

Inside the flying networks, once in a while, there might be no unwanted nodes to attack on the dynamic networks. But in the proposed network simulation, the input rate and flying nodes (N) are shown in Figure 6, which shows a high rise while flipping λ_l. By achieving the optimal results in between input and output queue rates which is presented in Figure 7. In the simulated work, by utilizing throughput, metric value can be effective in terms of outcome.

$$\mu_{\text{avg}} = \frac{N\lambda_l}{2}. \tag{2}$$

3.1. Markov Chain Distribution. Markov chain is a fundamental part of stochastic processes that use memory distribution in discrete-time steps that recall discrete-time Markov chain (DTMC). Suppose $X = \{X_t : t = 0, 1, 2, \cdots, T\}$ be the state of Markov chain stochastic process at time t with finite state spaces $S = \{1, 2\}$, where "1" represents "no attack level" which means normal, and "2" stands for the attack level.

$$P = (X_t = S_t \mid X_{t-1} = S_{t-1}, \cdots, X_0 = S_0) = P(X_t = S_t \mid X_{t-1} = S_{t-1}). \tag{3}$$

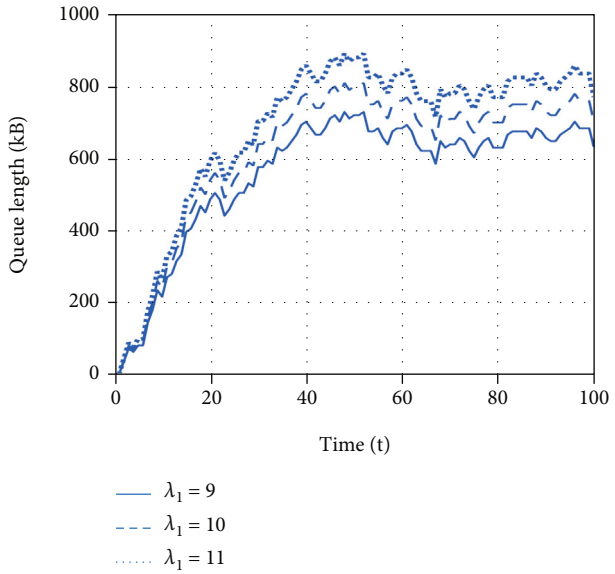

FIGURE 7: Impact λ_l on the queue length with μ_{avg}.

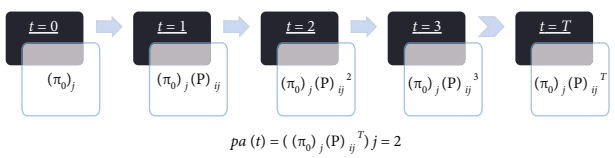

FIGURE 8: Attack probability at each time slot for desired Markov chain.

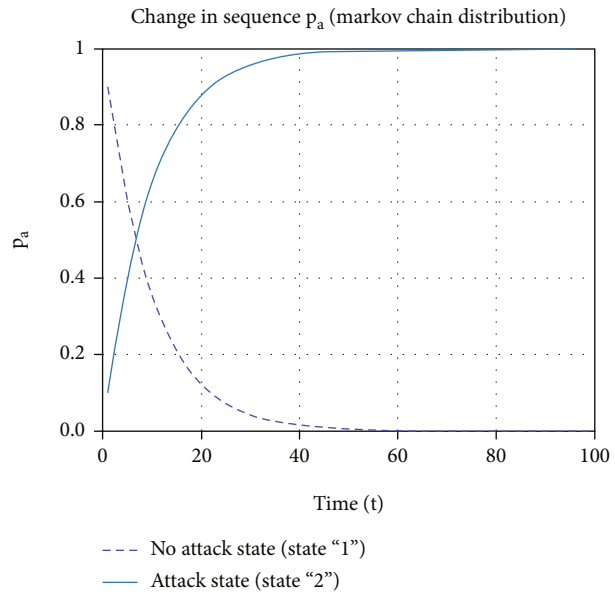

FIGURE 9: Attack probability versus time in Markov chain distribution.

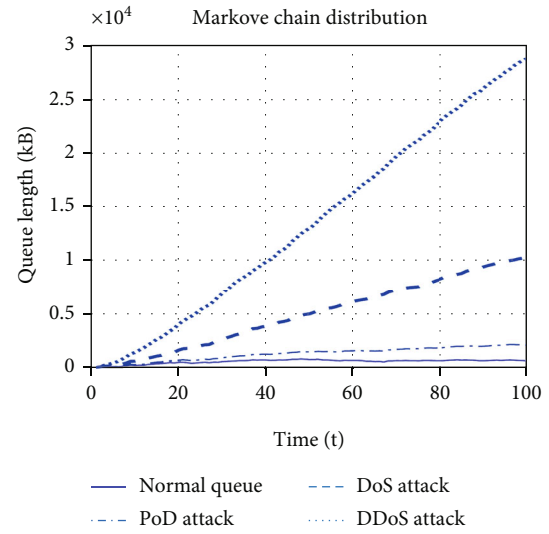

FIGURE 10: Queue length generation using cyberattacks for Markov chain.

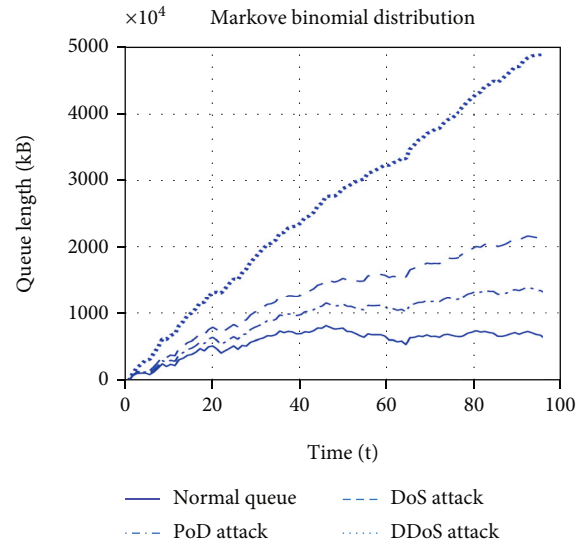

FIGURE 11: Queue length generation using cyberattacks for Markov binomial chain.

Equation (3) shows the formulation of Markov chain where for distribution X_t just having dependency on X_{t-1}. Finding the probability of being in state "1" or "2" at time t. In DoS, the attacker injects illegal packets to the network security systems by spoofing one node and attempts to increase the numbers of packets by utilizing the ratio $1 + \gamma$ p_a (γ is a positive constant). Apart from that modeling probability is p_a being changed in the first scenario where Markov chain with following transition matrix where α and β, respectively, is p_{a_0}, and 1 is proposed in the matrix.

$$(P)_{ij} = \left(p_{ij}\right) = \begin{bmatrix} 1-\alpha & \alpha \\ 1-\beta & \beta \end{bmatrix} = \begin{bmatrix} p_{a_0} & 1-p_{a_0} \\ 0 & 1 \end{bmatrix}. \quad (4)$$

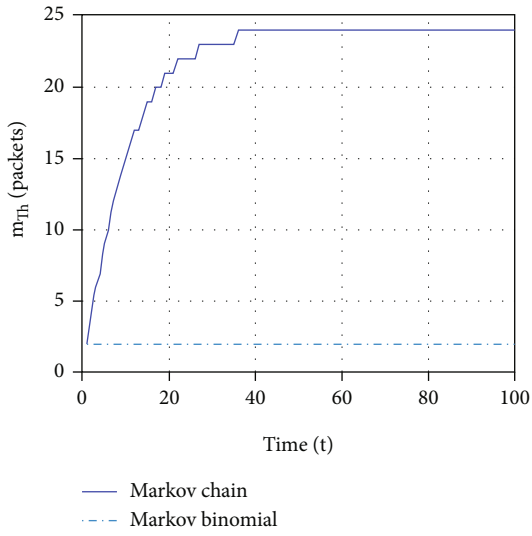

Figure 12: Certain level versus time in Markov chain distribution.

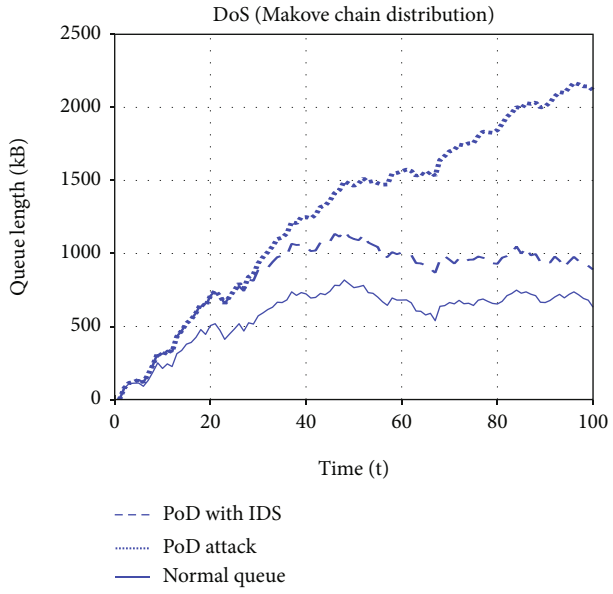

Figure 13: Queue length using PoD (Markov chain) with IDS.

Attack probability of being in state "2" at time "t" is proofed mathematically as

$$\begin{aligned} P(X_t = m) &= P(X_t = m, \cdots, X_0 = n) \\ &= \sum_{m,k,n \in S} P(X_t = m \mid X_{t-1} = k, \cdots, X_0 = m) \times P(X_{t-1} = k) \\ &= \sum_{m,k,h,n \in S} P(X_t = m \mid X_{t-1} = k) \times P(X_{t-1} = k \mid X_{t-2} \\ &= h, \cdots, X_0 = n) \times P(X_{t-2} = h) = \sum_{m,k,h,g,n \in S} P(X_0 = n) \\ &\times p_{ng} \times \cdots \times p_{hk} \times p_{km} = \left((\pi_0)_j (P)_{ij}^t\right)_{j=2}. \end{aligned} \tag{5}$$

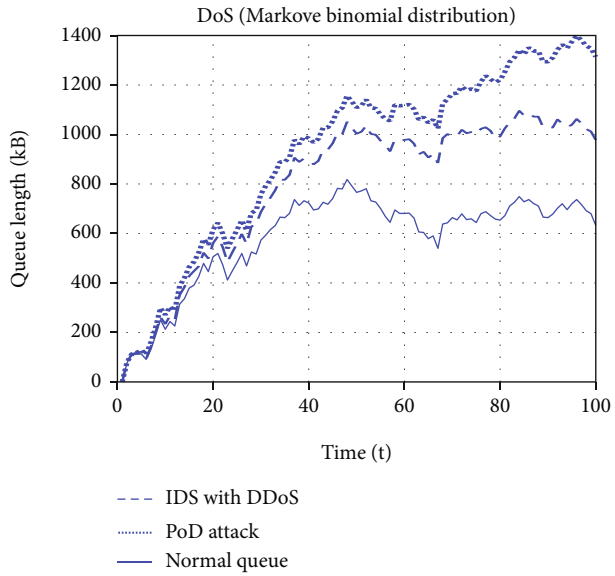

Figure 14: Queue length using PoD (Markov binomial) with IDS.

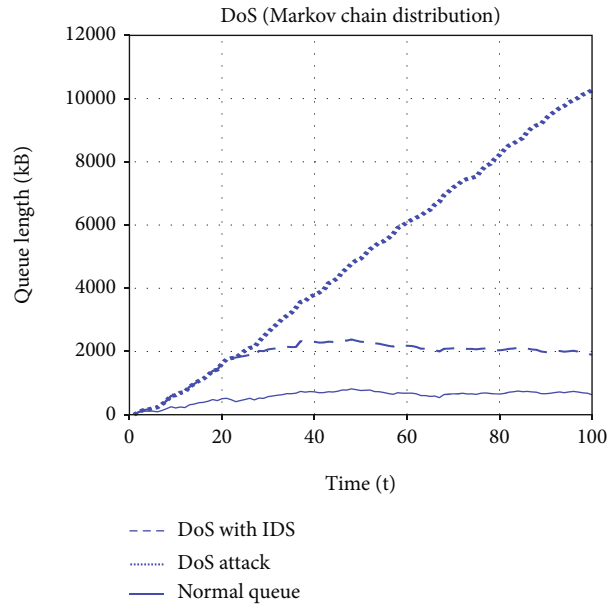

Figure 15: Queue length using DoS (Markov chain) with IDS.

Whereas,

$$\begin{aligned} (\pi_0)_i = (P(X_0 = n))_i &= P\left(\text{Attacker choose state } n = '1' \text{ to start}\right) \\ &= \begin{bmatrix} \pi_{0_1} \\ \pi_{0_2} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}. \end{aligned} \tag{6}$$

However, the attack probability p_a at each time slot will change in sequence using random variables according to

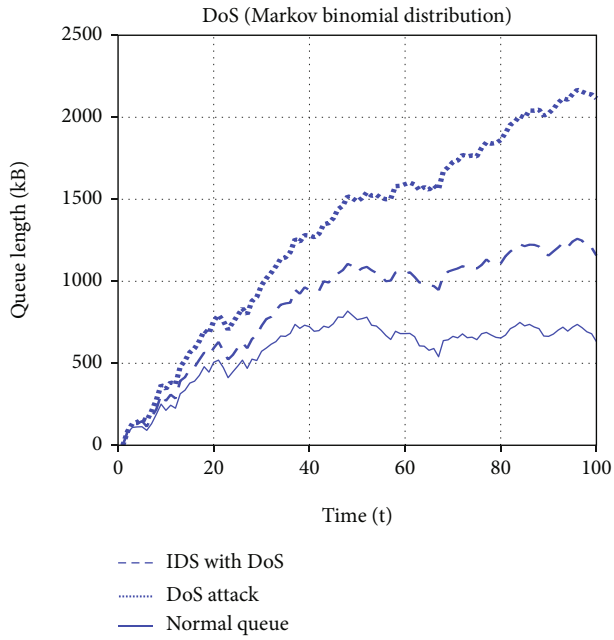

Figure 16: Queue length using DoS (Markov binomial) with IDS.

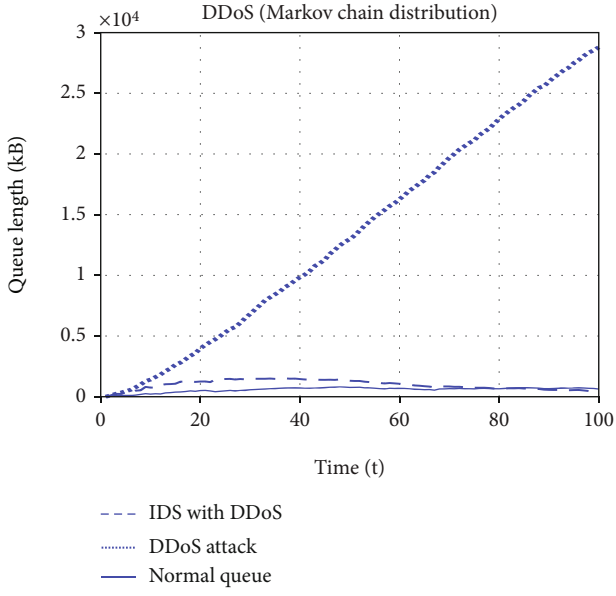

Figure 17: Queue length using DDoS (Markov) with IDS.

DTMC in blocks, and attack probability is shown in below Figure 8.

3.2. Markov Binomial Distribution. Binomial distribution is memory less scheme with having probability p_a, where attack at each time slot is stationary which can be symbolized as p_{a_0}. By simulating Markov binomial distribution, $\alpha = \beta = p_{a_0}$ are shown in below matrix from

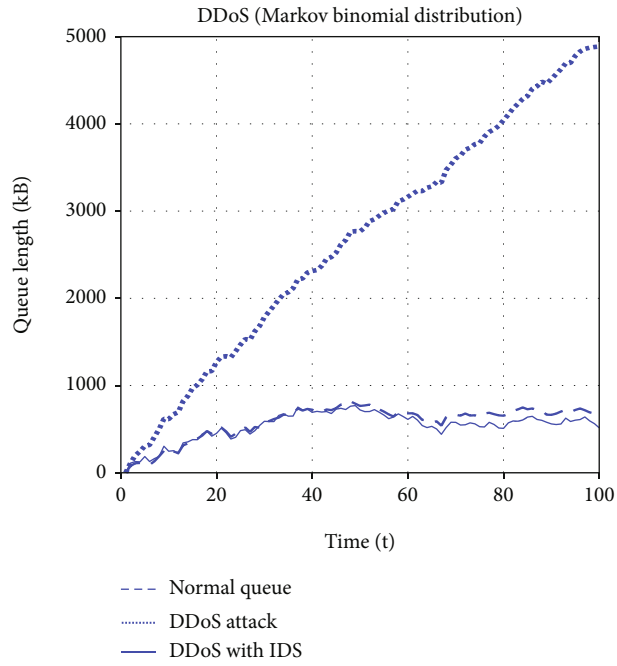

Figure 18: Queue length using DDoS (Markov binomial) with IDS.

$$(P)_{ij} = \left(p_{ij}\right) = \begin{bmatrix} 1 - p_{a_0} & p_{a_0} \\ 1 - p_{a_0} & p_{a_0} \end{bmatrix}. \quad (7)$$

Figure 8 elaborates attack probability changes with the passage of time, and the results are discussed using Figure 9 in which two states are discussed. Where state "1" is used for no attack, and state "2" represents attack.

4. Simulation Results

4.1. Without IDS. In simulation results, the attacker is attempting to use various flooding attacks such as DoS, DDoS, and PoD. Due to the aforementioned attacks, the ground BS is heavily buffered in a queue. The length of the queue for various attacks in order to impact the effect of attack probability on queue length for Markov chain and Markov binomial distribution, respectively, is shown in Figures 10 and 11. Markov chain distribution p_a attack is changing with the stream of time; due to that, queue length will escalate. Where using binomial distribution p_a attack probability must be constant; because of this reason, queue length will become very less in comparison with Markov chain distribution.

4.2. With IDS. Optimization of connection links will reshape the entire planet; therefore, safety of this society needs countermeasures to make the information-age secure. For the security of modeled smart IoT network having drones to stabilize path-flying things, detection system is launched to detect some cyber threats. Due to high network performance, the detection system attempts to trade-off between false positive and false negative probability. This concept

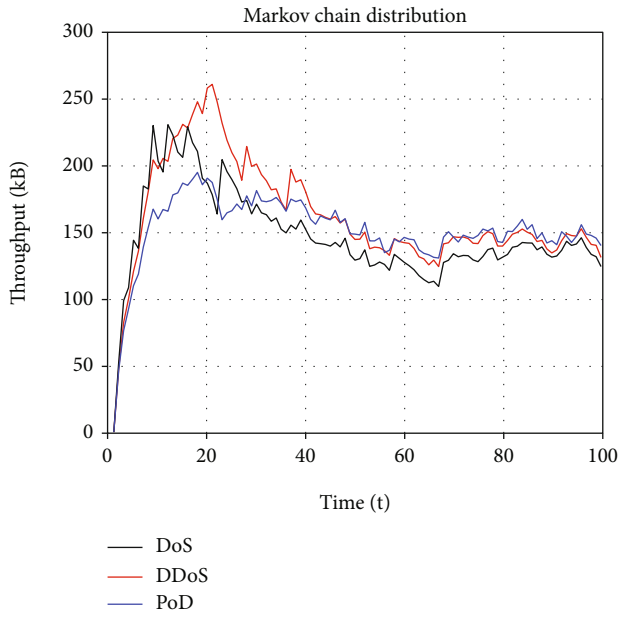

Figure 19: Average throughput using Markov chain.

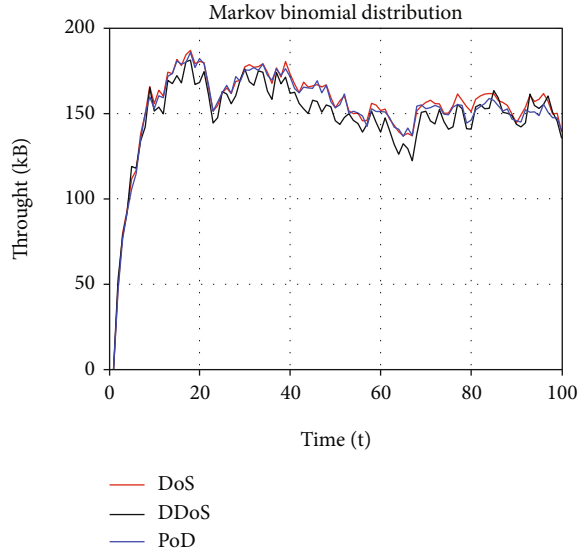

Figure 20: Average throughput using Markov binomial distribution.

assists researchers to have interconnectivity having maximum missed detection probability along with minimum false alarm prospects. The proposed IDS based on certain level m_{Th} try to prevent gateway queue lengths from rapidly increasing and maintaining them at the predictable level. Figure 12 shows the optimized certain level value per time for Markov chain and Markov binomial distributions.

The PoD with Markov chain using queue length is shown in Figure 13; while for Markov binomial distribution using security, attacks are discussed using Figure 14. Respectively, in Figures 15 and 16, the same techniques are utilized for DoS attack. However, similar schemes are incorporated for D-DoS threat in Figures 17 and 18. Throughput study of security attacks using Markov distribution and Markov binomial are having great impact on the data analysis which is shown in Figures 19 and 20.

5. Conclusion

Aerial ad hoc networks use to perform variety of tasks which include monitoring and collection of data from IoT networks. In flying networks, our main focus is to protect ground station from security attacks. While communication comprises drone-2-drone and land-station-2-aerial-vehicles which use IEEE 802.11 wireless technology to improve transmission routes. Intrusion detection system is the optimal way to deal with cyber threats. The proposed intrusion detection monitors incoming packets and filters them using Markov distribution. Markov chain stochastic process assists to find the gateway approach for flying vehicles. Intelligent intrusion detection controls flying networks to filter queue length data packets. The possibility of missed detection and false alarm is easily minimized. While buffer queue length will be maintained to normal level as demonstrated in the simulations. However, in future, machine learning techniques can be used to improve the aerial network security.

Data Availability

All the data is available in the paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by Taif University Researchers Supporting Project number (TURSP-2020/126), Taif University, Taif, Saudi Arabia.

References

[1] A. Qayyum, L. Viennot, and A. Laouiti, "Multipoint relaying for flooding broadcast messages in mobile wireless networks," in *Proceedings of the 35th annual Hawaii international conference on system sciences*, pp. 3866–3875, Big Island, HI, USA, 2002.

[2] I. U. Khan, I. M. Qureshi, M. A. Aziz, T. A. Cheema, and S. B. H. Shah, "Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET)," *IEEE Access*, vol. 8, pp. 56371–56378, 2020.

[3] M. Ahmed and A. K. Pathan, "False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure," *Complex Adaptive Systems Modeling*, vol. 8, no. 1, p. 4, 2020.

[4] A. Abdollahi and M. Fathi, "An intrusion detection system on ping of death attacks in IoT networks," *Wireless Personal Communications*, vol. 112, no. 4, pp. 2057–2070, 2020.

[5] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on SCADA systems: secure protocols, incidents, threats and tactics," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1942–1976, 2020.

[6] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, "Comprehensive review of cybercrime detection techniques," *IEEE Access*, vol. 8, pp. 137293–137311, 2020.

[7] M. Albalawi and H. Song, "Data security and privacy issues in swarms of drones," in *2019 Integrated communications, navigation and surveillance conference (ICNS)*, pp. 1–11, Herndon, VA, USA, 2019.

[8] J. Chen, Z. Feng, J. Wen, B. Liu, and L. Sha, "A container-based DoS attack-resilient control framework for real-time UAV systems," in *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 1222–1227, Florence, Italy, 2019.

[9] S. Garg, G. S. Aujla, N. Kumar, and S. Batra, "Tree-based attack–defense model for risk assessment in multi-UAV networks," *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 35–41, 2019.

[10] R. Mohan, C. V. Raj, P. Aswathi, and R. R. Bhavani, "UAV based security system for prevention of harassment against woman," in *2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, pp. 874–879, Kannur, 2017.

[11] M. Podhradsky, C. Coopmans, and N. Hoffer, "Improving communication security of open source UAVs: encrypting radio control link," in *2017 International Conference on Unmanned Aircraft Systems (ICUAS)*, pp. 1153–1159, Miami, FL, USA, 2017.

[12] C. Rani, H. Modares, R. Sriram, D. Mikulski, and F. L. Lewis, "Security of unmanned aerial vehicle systems against cyber-physical attacks," *Journal of Defense Modeling and Simulation*, vol. 13, no. 3, pp. 331–342, 2016.

[13] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the internet of things in the age of machine learning and software-defined networking," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4829–4842, 2018.

[14] F. E. Salamh, U. Karabiyik, M. Rogers, and F. Al-Hazemi, "Drone disrupted denial of service attack (3DOS): towards an incident response and forensic analysis of remotely piloted aerial systems (RPASs)," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 704–710, Tangier, Morocco, 2019.

[15] A. Sehrawat, T. A. Choudhury, and G. Raj, "Surveillance drone for disaster management and military security," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 470–475, Greater Noida, 2017.

[16] C. Wang, L. Zhu, L. Gong et al., "Accurate sybil attack detection based on fine-grained physical channel information," *Sensors*, vol. 18, no. 3, p. 878, 2018.

[17] T. Lagkas, V. Argyriou, S. Bibi, and P. Sarigiannidis, "UAV IoT framework views and challenges: towards protecting drones as "things"," *Sensors*, vol. 18, p. 4015, 2018.

[18] Z. Zaheer, A. Usmani, E. Khan, and M. A. Qadeer, "Aerial surveillance system using UAV," in *2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN)*, pp. 1–7, Hyderabad, 2016.