Hybrid blockchain-based Authentication Handover and Flow Rule Validation for Secure Software Defined 5G HetNets

Asad Faraz Khan
School Of Engineering and IT
University Of Technology Sydney
Sydney,Australia
Asadfaraz.khan@student.uts.edu.au

Priyadarsi Nanda
School Of Engineering and IT
University Of Technolgy Sydney
Sydney,Australia
priyadarsi.nanda@uts.edu.au

***Abstract*- 5G networks provide high data rates, high bandwidth, high coverage, and low latency compared to 4G networks. However, 5G includes some challenges such as privacy, network management, security. To overcome these issues, we propose SDN-5G HetNet (Software Defined Network-based 5G Heterogeneous network) model which addresses three issues such as handover authentication, flow rule validation, and hybrid intrusion detection and mitigation. Authentication is performed by Bio-Signature Validation Authentication mechanism for validating the users. User credentials are stored in the public blockchain for security. Handover is performed by the Dual Constraints Chaotic Radial Movement Optimization algorithm using User Entity and Access Network constraints. Flow rules are hashed and stored in the private blockchain for validation. Also, flow rules are monitored using Hidden Markov Model (HMM). Simulation is performed using NS-3.26 network simulator, which demonstrates our proposed work achieves better performance in terms of detection accuracy, handover delay, switch failure rate, packet loss rate, delay, and throughput compared to other state-of-the -art works.**

Keywords—5G, Software Defined Network (SDN), Heterogeneous network, Hybrid blockchain, flow rule validation, ***authentication handover***

I. INTRODUCTION

5G networks are expected to support heterogeneous networks through higher reliable transmission, data rates, and huge device connectivity [1]. Internet usage has met phenomenal growth using the 5G technology [2]. Software-defined network is an emerging technology to overcome the recent challenges of networks that are used with 5G network technologies. The communication between controllers in SDN is performed with the help of switches with well-developed flow rules [3]. However, there are numerous challenges involving security in flow rules, i.e., compromise of flow rules that reduce the security of the network [4],[5]. The continuous communication between the data plane and control plane consumes more bandwidth with huge traffic instances which leads to overload of the controller [6]. To overcome the flow rule compromising attack, flow rule validation is performed. Various machine learning and deep learning techniques are used in SDN to improve security [7], [8].

Blockchain is an emerging technology whose main purpose is to increase security aspects in peer-to-peer (P2P) communications, such as, sharing critical files [9]. However, malicious users may be able to breach the public blockchain loosing critical data in the transaction [10]. To overcome this issue hybrid blockchain is introduced providing high security by mitigating various attacks such as replay attack, DOS attack, DDOS attack, spoofing attack, control plane saturation, man-in-the-middle attack, table-miss striking attack, and impersonation [11], [12].

In recent times many research works contribute their efforts to improve the security of SDN-5G networks. The main aim of this research work is to improve the security level of the SDN-5G network, particularly the control plane from saturation and DDoS attacks. Our research objectives are formulated as following:

- To provide user validation and prevent malicious users' involvement in the network
- To secure Hand Over (HO) process without increasing delay and number of handovers
- To validate the flow rules by deploying optimal virtual monitors in the network
- To design a hybrid IDS in control plane to monitor overall security level with high-level accuracy

In order to address above research questions, our main contributions are listed as following.

- We propose authenticated handover mechanism providing security during handover. For this user credentials are hashed and stored in the public blockchain, which provide bio-signature using the Montgomery curve. Our proposed scheme selects optimal network using Dual Constraints Chaotic Radial Movement Optimization algorithm by considering User entity (UE) and Access Network (AN) constraints.
- In our second step, flow rules are hashed and stored in the private blockchain and are continuously monitored by the Flow Rule Monitor (FRM). Here, the load level of the switches is evaluated by Hidden Markov Model (HMM). Based on load level, Virtual FRMs are deployed for reducing control plane overloading.
- Finally, the global controller detects the normal and malicious flows using SqueezeNet-Fuzzy II (SNet-Fuzzy) algorithm which detects the malicious flows based on the packet-based features. Then Type-II Fuzzy method is used for deciding on attack mitigation.

Our paper is organized as follows. Section II illustrates existing works and major problem statement. Section III presents proposed solution and system model which includes research procedure, pseudocode, and mathematical representation of the proposed SDN-5G HetNet model. Section IV demonstrates experimental results and Section V concludes the paper along with our future research scopes.

II. EXISTING WORKS AND MAJOR PROBLEM STATEMENT

5G is an emerging cellular technology that aims at providing high-level data rates [13]. In a 5G network environment, large numbers of 5G users with diverse characteristics are involved. Hence, security is increasingly important to improve 5G network performance. In particular, distributed denial of service (DDoS) is a harmful attack that directly affects all levels of the network by sending enormous unwanted packets. For monitoring and analyzing network flows, software-defined networking (SDN) is integrated with 5G networks. The 5G network packets are analyzed through SELFNET which is a deep learning technique for DDoS detection. However, there are limitations of this technique as, lack of initial authentication increases the number of attackers in the network and the technique does not support large-scale networks.

In the handover process, optimal target network selection plays a major role [14]. A smart SDN based Factory handoff (SFSH) technique is proposed to satisfy the quality of service (QoS) requirements for IoT based applications. The proposed handover procedure considers received signal strength (RSS) as the major criteria for target network selection. As additional parameters, handoff delay and location credentials are utilized, the handover process is initialized by comparing the current RSS level with the threshold value. When the RSS value is lower than the threshold, the user decides to perform a handover. However, lack of security increases packet overheads and resource consumption by malicious users. Blockchain is a distributed ledger technology that assures high-level security for SDN applications[15]. Authors in proposed a scheme to achieve high-level accuracy minimizing forecasting errors in security-based traffic management using blockchain based technique. However, use of SHA-256 in the blockchain could increase computational complexity and non-optimal network selection may lead to frequent handovers affecting performance.

Security in control plane is important in SDN based networks since the controller is responsible to maintain the overall network [16]. If the controller is compromised or failed to maintain security, then, overall network function will be failed. To overcome this issue, authors in proposed scheme to secure the control plane from several attacks including denial of service (DoS). The new metric is defined based on the rate of packets received at control plane and if attack is detected, then the flow rules are modified to defend against the attack. However, attack detection accuracy is poor since it considers only packet rate which can also be increased due to large number of legitimate flows. Security is provided for higher layers only which means lower layer security is still ineffective that may lead to huge load in control plane.

In SDN-5G networks, security provisioning becomes major issue due to large number of user involvement and need for higher data rates. In recent times, security schemes at the control plane have been developed to defend against DDoS, control plane saturation and also on other attacks. In all these works, the following research problems are still unsolved.

- Existing control plane security methodologies only focus on intrusion detection and prevention in higher level layers (i.e.) control plane. However, the attackers could launch attack on any layers of the SDN control plane resulting control plane saturation.
- To saturate domain controllers, attackers not only launch enormous packet but, also inject malicious flow rules into the data plane. The switches can also be compromised by executing malicious or injected flow rules. Thus, the second problem concerning absence of flow rule validation also increases vulnerability of control plane".
- Non-optimal network selection in handover (HO) increases frequent handovers which also increases time and energy consumption. On the other hand, generation of security credentials at each handover increases HO delay. Thus, the third problem to be addressed in this paper is to support better mobility management.

Authors in [17] proposed a multi-layer security approach using data acquisition layer, switches layer, domain controller layer, smart controller layer and virtualization layer. However, the scheme has major flaws such as; a. single point of failure maintaining centralized management of security credentials, b. use of entropy based scheme demands substantial number of samples for computation, and c. GM-SOM based scheme needs optimal and accurate initial weight value to improve accuracy level. Based on the limitations as discussed, we propose our solution in next section of the paper.

III. Proposed solution and System Model

A. Research Solution

In this research, hybrid blockchain based user authentication is performed which constructs a distributed environment. Authentication works upon MAC, ID, PW and BioM which are secure, and our scheme validates the users accurately. Optimal network selection is performed by DC-CRM optimization algorithm upon dual constraints for authentication handover. For encryption and signature generation, Montgomery based ECC algorithm which is lightweight and assures high-level security is proposed. Initial user validation is performed in network edge level in APs which limits the involvement of attackers in the network. Data plane load is balanced continuously through flow offloading procedure. Flow rule validation is performed by domain controllers in private blockchain which accurately detects and eliminates malicious and injected flow rules. Hybrid IDS is proposed with SqueezeNet and Type-II fuzzy to analyze the flows deeply which improves accuracy level.

B. System Model

To overcome the aforesaid research problems, this research work presents a Hybrid Blockchain-based Multi-Level Security Scheme for SDN-5G HetNets. The overall network is constructed with 5G Device Plane, SDN Data Plane, Control Plane and Application Plane along with a Hybrid Security Plane. The Hybrid Security Plane is built with Hybrid Blockchain which is the integration of Private and Public Blockchain to improve security level. Proposed Hybrid Blockchain plane secures the overall network. Fig 1 represents the overall architecture of the proposed work.

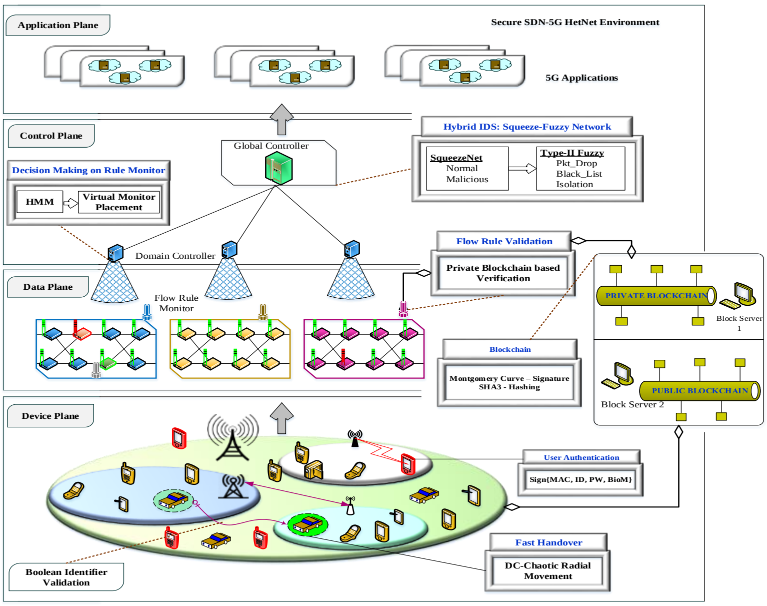


Fig.1 SDN-5G HetNet Model

The entities of the proposed SDN-5G HetNet model is explained as follows,

(i)5G device plane: It includes various user devices, and network base station. The proposed HetNet includes 5G base station, access point and number of switches.

(ii) SDN-Data plane: It includes multiple switches and flow rule monitors that are used to monitor the flow rules of the user data for reducing controller overload.

(iii) Control plane: It includes multiple domain controllers and a single global controller. Every domain controller includes multiple switches and flow rule monitors, which is used to detect the suspicious, normal, and affected switches for providing security to the environment.

(iv) Application Plane: It provides multiple 5G applications to the users over the network. The applications are developed by software modules that are easily accessed by the users.

(v) Hybrid Security plane: The hybrid security includes private blockchain and public blockchain. Here, flow rules are validated by the private blockchain that ensures the security of the switches.

A. Level-1 Security: Authentication Handover

Level-1 security concentrates on securing the data plane from attacks such as spoofing, impersonation, and so on. Initially, all 5G-HetNet users have registered their identity in Hybrid Security Plane (Public Blockchain). We propose Bio-Signature Validation Authentication (BioSVA) mechanism to validate the users initially. The Bio-SVA scheme involves the verification of MAC Address, ID, Password, and Bio-Signature. Here, all the credentials are hashed by SHA-3 and stored in the Public Blockchain which ensures high-level security. The bio-signature of the users is derived from the biometrics (we have used finger vein & iris) and Montgomery Curve. Here, BioSVA is proposed for generating a digital signature for authentication. Signature is generated based on the Montgomery curve which is a form of elliptic curve that is defined as follows,

$$C_{(a,b)}: by^2 = X(X^2 + aX + 1) \qquad (1)$$

Where a and b represent the parameters in the Montgomery curve which satisfies $b \neq 0$ and $a^2 \neq 4$. The plane coordination $(x: y: z)$ of the curve is defined as follows,

$$X = x/z \;\; and \; Y = y/z \qquad (2)$$

The Projective model of the curve is defined as follows,

$$C_{(a,b)}: by^2 z = x(x^2 + axz + z^2) \subseteq p^2 \qquad (3)$$

Where p is a prime number that is used to generate the Montgomery curve for signature generation. The procedure of signature generation is defined as follows;

- Initially, random integer r is selected from $[1, n-1]$.
- Then calculate the elliptic curve base point $kB = (X, Y)$ which generates the subclass of prime numbers and calculate $t = X(mod\, n)$, if the value of $s = 0$, then go back to the previous step.
- Calculate $e = H(M)$, where H represents the hash algorithm. In our work, we proposed SHA-3 hashing algorithm.
- Calculate signature as defined as follows,
  $$S = k^{-1}(e + td)(mod\, n) \qquad (4)$$
  If the value of S is equal to zero then go back to the first step and reselect k.
- Finally, a signature is generated on the message with the pair(t, S).

Authentication is performed based on the signature, which is verified by the public blockchain. If the user moves from one network to another, then the HO procedure is initiated. Once the HO decision is made, then optimal network selection is triggered by the current access network 5G base station (BS). The optimization algorithm achieves randomness using the distribution of probability. To overcome this randomness, we include a chaotic map with radial movement optimization. The calculation of chaotic map is defined as follows,

$$\begin{cases} R_N + 1 = \propto R_N(n - \frac{R_N}{N})/n - R_N/2 \\ P_{N+1} = \delta(n - |n - P_N|) \end{cases} \quad (5)$$

where $R \in (0, N \times M), \propto \in [0,4], P(0,2 \times n), \delta \in [1,2], n = 2^i$ and $N = 2^i$ with integers 1 and 1[25]. Based on the chaotic map initial particles in the search space are generated. The initial population is defined as follows,

$$x_i^0, y_i^0 = (x_{Min}, y_{Min}) + p_i(x_{Max} - x_{Min}) + Round[p_i(y_{Max} - y_{Min})] \quad (6)$$

The velocity vector as defined as follows,

$$U_{ij} = Round\ (Rand\ (0,1) \times U_{Max(j)}) \quad (7)$$

Where, $i = 1,2,3 \ldots . n$ and $j = 1,2,3, \ldots m$ for integer $m + 1 \ldots . s$ for real. $U_{Max(j)} = Round\left(\frac{x_{Max(j)} - x_{Min(j)}}{k}\right)$ for real variables, and k represent the integer value that is selected carefully, $U_{Max(j)}$ and $U_{Min(j)}$ are the maximum and minimum values of the j^{th} variable. Then evaluate the fitness value of every particle in the population for locating the center point which is estimated as follows,

$$\aleph = \sum_{r=1}^{R} \sum_{i=1}^{n_s} \{v, (i, r) fc(i, r) + Sc(i, r) + \sum_{y=1}^{n_c} \emptyset |V_y| \quad (8)$$

Where $\emptyset_y$ represent the penalty function, and it provides the minimum fitness and selects the center point (CP) by considering both UE and AN constraints. Finally, particle radial movement is evaluated from the CP which is defined as follows,

$$V_{ij} = Round(w \times U_{ij} + Center\ (j)) \quad (9)$$

Where w represents the weight value of the features. Finally, the fitness value of every particle (network) is defined as follows,

$$Center^{k+1} = Round(Center^k + (c_1[g_{best} - Center^k]) + (c_2[r_{best} - Center^k])) \quad (10)$$

Where k represents the iteration number and $j = 1,2, \ldots . s\ and\ j = 1,2, \ldots . s + 1$ m and r_{best} is better than g_{best}. The convergence of the optimization is improved based on the trail number of $gbest$, which is defined as follows,

$$U_{ij} = Round(g_{best} + u(0,1) * (V_{r1j} - U_{r2j})) \quad (11)$$

Where, $i = 1,2, \ldots n; j = 1,2, \ldots n$, and $r1$, $r2$ selected randomly which are different from one another. Based on the fitness value optimal network is selected for handover. In HO, the target optimal AN BS validates the user's Boolean identifier without any heavy crypto functions. In this manner, level-1 security is assured in the network.

B. Level-2 Security: Flow Rule Validation

Level-2 security focuses on providing security for the data plane by validating flow rules. This level assures that none of the switches in the data plane is compromised. Level-2 security is executed by the Domain Controllers (DCs) for the corresponding switches. Each DC has certain switches and Flow Rule Monitor (FRM). Flow rules in the switches are hashed and stored in the Private Blockchain during flow rule deployment. The FRM continuously monitors the flow rules of each switch and validates the rules in the blockchain. As the proposed work needs to support a large-scale network, the DC monitors the load level of switches by Hidden Markov Model (HMM) which is defined as follows,

$$H = (a, b, \pi, x, y) \quad (12)$$

Where a represents the number of states, and the value of a is 2. In our work, we have two states where virtual FRM is deployed or not, and b represents the symbol of observation and π is an initial state distribution, x is a probability of transition function and y represents the observation probability.

The probability of load detection is mentioned as below,

$$Y = [X_{ij}]_{n \times n} \quad (13)$$

Where, $X_{ij} = P(u_{t+1} = C | u_t = C), \quad 1 \leq i, j \geq n.$ The matrix format of observation probability is defined as follows,

$$Z = [W_{ij}]_{n \times m} \quad (14)$$

$$W_{ij} = P(v_{t+1} = O | v_t = O), \quad 1 \leq i \leq n, j \leq m \quad (15)$$

The mathematical representation of the initial condition probability vector is defined as below,

$$\pi = P(u_t = C), 1 \leq i \ \leq n \quad (16)$$

C. Level-3 Security: Hybrid Intrusion Detection & Mitigation

The final level of security intends to provide security by abstracting the global network information. Level-3 security is executed by a global controller (GC) which is responsible to detect normal and malicious flows from suspicious flows. We present a novel Squeeze Net-Fuzzy II (SNet-Fuzzy) model for attack detection and mitigation. The SqueezeNet which is the fast and lightweight deep learning first detects the malicious switch based on packet features (packet interval time, packet size, packet type, payload length, and timestamp) and added feature. The SqueezeNet includes ten layers such as Convolution layers, fire layers, max pool layer, and SoftMax layer. Input block of the SqueezeNet is defined as follows,

$$\mathrm{F_i} = \mathrm{C_f}(\mathrm{I_i}) \quad (17)$$

Where, $\mathrm{F_i}$ is a feature block and $\mathrm{C_f}$ is a convolutional layer function in fire 9 blocks. After completed feature extraction, the weight values of the features are evaluated as follows,

$$\mathrm{w_i} = \propto [\mathrm{w_{Mat}} \mathrm{A_g}\ \mathrm{O_i}] \quad (18)$$

Where, $\mathrm{w_{Mat}}$ represent the weight values of the metrics of the fully connected layer and $\mathrm{A_g}$ represent the global average pooling function and $\propto$ represent the sigmoid function with [0,1] range. Based on the weight values of the feature, the SoftMax layer classifies the flow rule is normal or malicious which is defined as follows,

$$\mathrm{X_i} = \mathrm{F}[\mathrm{G_P}(\mathrm{W_i} \times \mathrm{O_i})] \quad (19)$$

Then Type-II Fuzzy makes mitigation decisions as Packet_Drop, Blacklist_Update, Switch_Block, and Isolation based on level of the attack, affected switch status, and authentication status. The membership function ($m_p(x,\mu)$) of Type-II Fuzzy inference system is defined as follows,

$$P = \int_{x \in X} \left[\int_{\mu \in J_x} m_p(x,\mu)/\mu \right] /\mu, \; J_x \subseteq m_p \subseteq (x,\mu) \int [0,1] \tag{20}$$

Where, J_x represent the membership function of the primary variable x with the interval of $[0,1]$, and μ represent the secondary variable and $\int_{\mu \in J_x} (x,\mu)/\mu$ represent the secondary membership function. While all the secondary grades are equal to one, then P is observed as the type 2 fuzzy set. From Eqn (20) the primary variable x in P is no lengthier than a crisp number, however, type-1 fuzzy set is defined as follows,

$$P_x = \int_{\mu \in J_x} m_p(x,\mu)/\mu \tag{21}$$

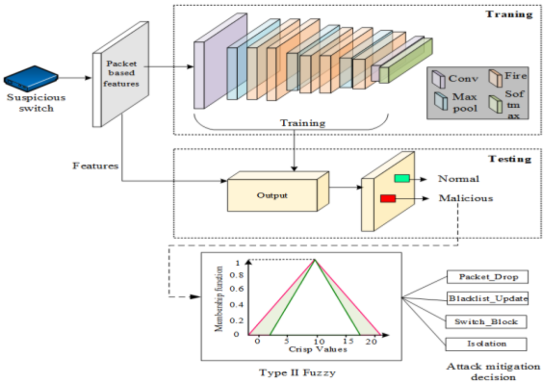
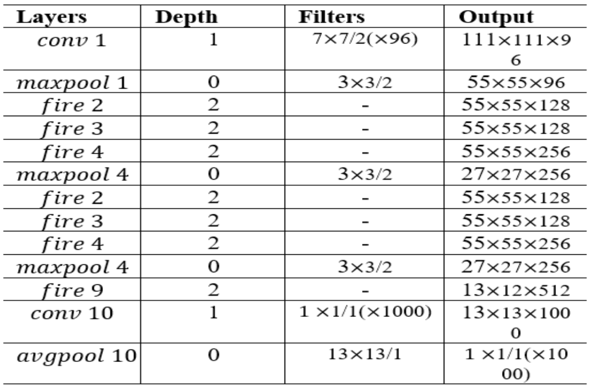


Fig.2 Process of Intrusion Detection and Mitigation



Layers	Depth	Filters	Output
conv 1	1	7×7/2(×96)	111×111×96
maxpool 1	0	3×3/2	55×55×96
fire 2	2	-	55×55×128
fire 3	2	-	55×55×128
fire 4	2	-	55×55×256
maxpool 4	0	3×3/2	27×27×256
fire 2	2	-	55×55×128
fire 3	2	-	55×55×128
fire 4	2	-	55×55×256
maxpool 4	0	3×3/2	27×27×256
fire 9	2	-	13×12×512
conv 10	1	1 ×1/1(×1000)	13×13×1000
avgpool 10	0	13×13/1	1 ×1/1(×1000)

IV. Experimental Study

This section explains the experimentation of the proposed SDN-5G HetNet model is carried out to measure the performance. This section includes three subsections such as simulation study, comparative analysis, and research summary.

A. Simulation Setup

The proposed SDN-5G HetNet model is simulated using network simulator NS-3.26. The NS3 tool has a better network structure and provides all the specifications of 5SDN-5G HetNet. The proposed model experiments in $500m \times 600m$ simulation environments. The system configurations are illustrated in table 2. The simulation parameters are illustrated in table 3.

Table.2. Hardware and Software configuration

Hardware Specifications	Hard Disk	500GB
	RAM	4GB
Software Specifications	Network simulator	NS-3.26
	OS	Ubuntu 14.04LTS

Table.3 Simulation parameter

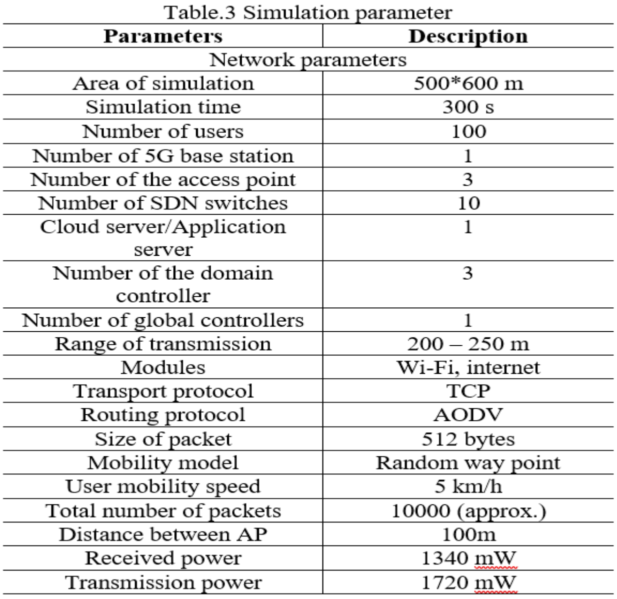


Table.3 Simulation parameter

Parameters	Description
Network parameters	
Area of simulation	500*600 m
Simulation time	300 s
Number of users	100
Number of 5G base station	1
Number of the access point	3
Number of SDN switches	10
Cloud server/Application server	1
Number of the domain controller	3
Number of global controllers	1
Range of transmission	200 – 250 m
Modules	Wi-Fi, internet
Transport protocol	TCP
Routing protocol	AODV
Size of packet	512 bytes
Mobility model	Random way point
User mobility speed	5 km/h
Total number of packets	10000 (approx.)
Distance between AP	100m
Received power	1340 mW
Transmission power	1720 mW

Fig 4 represents the simulation environment of the proposed SDN-5G HetNet, which includes four planes such as device plane, data plane, control plane, and application plane. In which the data plane includes multiple devices, three access points and one 5G base station. The data plane includes a number of switches and flow, rule monitors, in which the switch collects the data from the device plane. The control plane includes three domain controllers for controlling the switch flow and one global controller to control the domain controllers. Finally, the application plane provides the services or applications to the users.

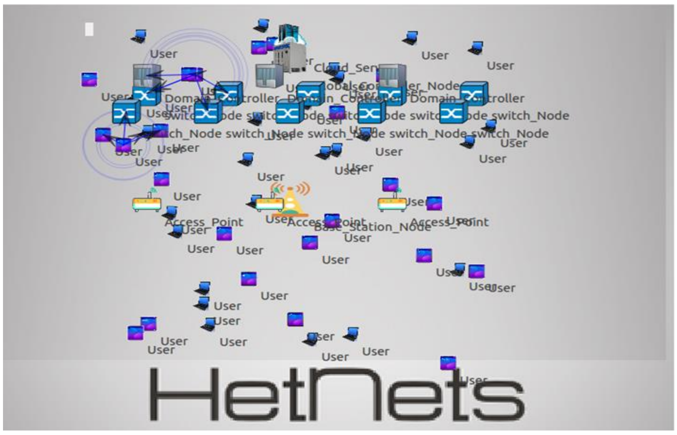


Fig.4 Simulation environment of SDN-5G HetNet model

B. *Comparative Analysis*

This section explains the comparison of the proposed SDN-5G HetNet model and existing models such as ML-IDS [18] NT-IDS [19] and EAP-HetNet [20] in terms of detection accuracy, handover delay, switch failure rate, packet lost rate, delay and throughput.

a) Impact of detection accuracy

Detection accuracy is used to measure number of attacks detected from the overall samples and is defined as follows:

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \qquad (22)$$

Where, TN represent true negative, and TP represent true positive, FP represent the false positive and FN represent false negative.

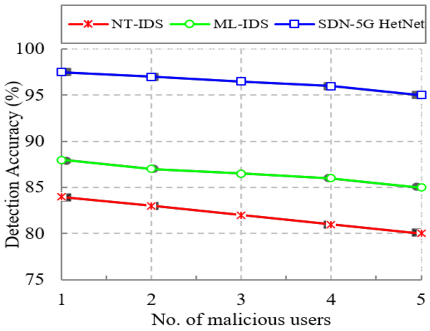


Fig.6 Comparison of Detection Accuracy

Fig 6 represents the comparison of proposed and existing approaches detection accuracy. The figure clearly states that the proposed work achieves high accuracy compared to existing works because the proposed work provides three levels of security to the network that perform against various attacks. In addition, the flow rules are validated by the private blockchain that also increases detection accuracy compared to existing approaches. Our proposed SDN-5G HetNet achieves 96.4% detection accuracy compared to existing work.

b) Impact of handover delay

Fig.7 represents the comparison of handover delay concerning several users. The figure clearly states that the proposed work achieved less handover delay compared to existing work such as EAP-HetNet

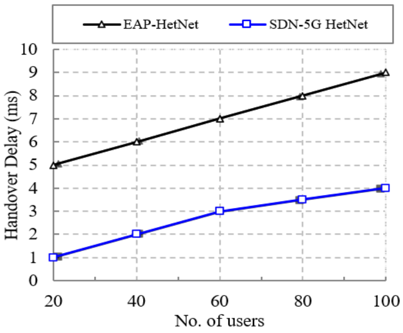


Fig.7 Comparison of Handover Delay

Table 4 illustrates numerical analysis of the proposed SDN-5G HetNet handover delay.

Table.4 Analysis of Handover delay

Methods	Handover delay
EAP-HetNet	6.9±0.2
SDN-5G HetNet	2.7±0.1

c) Switch failure rate

It states that the numbers of switch failures are occur in a total time. The calculation of switch failure is defined as follows,

$$S_f = \frac{n_s}{t} \qquad (23)$$

Where, S_f represent the switch failure rate and n_s represent the number of switches and t is the total time. Fig 8 represents the comparison of switch failure rate concerning the number of users. The figure clearly states that the proposed work achieves less failure rate compared to existing work. Because the proposed work performed authentication handover in an earlier stage that eliminates the malicious users which help to reduce switch failure compromised by attackers. In addition, the flow rule monitor monitored the load level of the switch, if the load level is high then we place a virtual flow rule monitor for performing load balancing that reduces switch failure due to overload. In addition, flow rules are hashed and stored in the private blockchain for classifying the switch into three classes such as normal, attacked, and compromised.

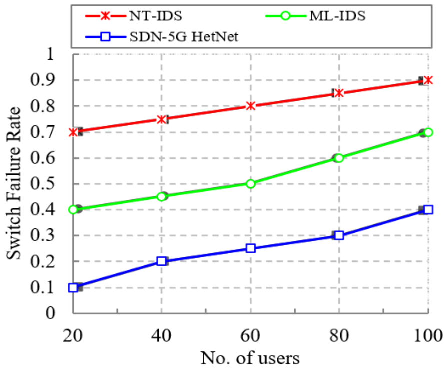


Fig.8 Comparison of Switch Failure Rate

d) Packet loss rate

d) Packet loss rate

This metric is defined as ratio of the number of packets not received and the total number of packets,

$$\text{PLR} = \frac{\text{ԉ}}{\acute{\varepsilon}} \qquad (24)$$

Where PLR represent the packet loss rate and ԉ represent several not received packets and έ represent a total number of packets. Fig 9 represents the comparison of the proposed and existing work for packet loss rate. It shows that the proposed SDN-5G HetNet achieved less packet loss rate compared to existing approaches such as ML-IDS and NT-IDS. The proposed work used hybrid security model for providing high security.

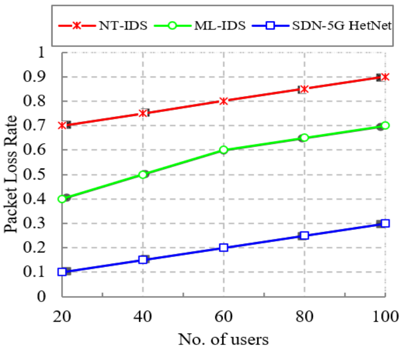


Fig.9 Comparison of Packet Loss Rate

e) Delay

Delay represents, how much additional time to deliver the packets from the data plane to the control plane. The calculation of delay is defined as,

$$D = ɳ - ȡ \tag{25}$$

Where D represents the delay and ɳ represents the completed time and ȡ represents the expected time.

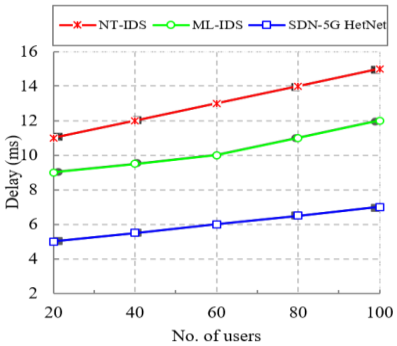


Fig.10 Comparison of Delay

Fig 10 represents the comparison of delay for both proposed and existing approaches. Results show that the proposed SDN-5G HetNet model achieved less delay compared to existing works, because, we eliminate malicious users in an earlier stage that reduce authentication delay. In layer 2, all the flow rules are hashed and stored in the private blockchain for providing security, which can easily classify the switches into normal, affected, and suspicious by performing validation. In this way, the proposed work detects the affected switch within the minimum amount of time

f) Throughput

Throughput is defined as follows,

$$T = \frac{ὰ}{ʋ̋} \tag{26}$$

Where T represents the throughput and ὰ represents the amount of data delivered from the transmitter to the receiver and ʋ̋ represents the time taken for delivering the data. Fig 11 represents the comparison of proposed and existing throughput concerning several users. The comparison results shows that the proposed scheme achieves high throughput compared to existing works. The proposed work used hybrid blockchain for providing security to the network that increases high data delivery ratio and throughput.

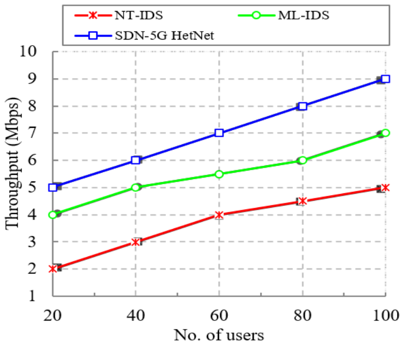


Fig.11 Comparison of Throughput

C. Analysis of experimental results

In this section, we present a summary of our findings for various attack scenarios. This research mitigates various attacks in the network which are defined as follows,

- Spoofing attack- In this attack, attacker participates in the network by misusing the identity of the users. This attack is mitigated by performing authentication handover, in which the user credentials are hashed and stored in the public blockchain which is not compromised by the attackers.
- Replay attack- Detection of replay attacks is difficult because the attacker acts like normal user. Our proposed hybrid security model provides high security and less complex to mitigate replay attack.
- DDoS attack- In the proposed scheme, our work performs flow validation through private blockchain which increases high security and defending against DDoS attack.

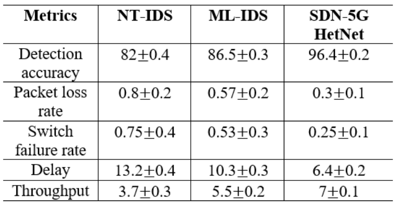
Research Summary

This section summarizes the performance of the proposed work.

- In first level security, authentication handover is performed for ensuring network security. For authentication, we proposed a Bio-SVA algorithm which generates bio-signature using Montgomery Curve using a public blockchain. For handover, the optimal network is selected using DC-CRMO algorithm by considering UE and AN constraints which increase security and perform against spoofing attacks.
- In second-level security, flow rule validation is performed for reducing the controller overload. For that purpose, the flow rules are monitored by the flow rule monitor, based on the flow rules switches are classified into three levels, in which the attacked switch flows are stopped to provide security and load balancing.
- In third level security, a lightweight deep learning algorithm is proposed for mitigating the attacks and provides the mitigation decision based on the attack level. Switch status and authentication status provide high security to the network.

Table 5 illustrates the average values of the performance metrics. From the numerical result, our proposed work achieves better performance compared to existing works.

Table.5 Numerical Analysis of proposed and existing approaches



Metrics	NT-IDS	ML-IDS	SDN-5G HetNet
Detection accuracy	82±0.4	86.5±0.3	96.4±0.2
Packet loss rate	0.8±0.2	0.57±0.2	0.3±0.1
Switch failure rate	0.75±0.4	0.53±0.3	0.25±0.1
Delay	13.2±0.4	10.3±0.3	6.4±0.2
Throughput	3.7±0.3	5.5±0.2	7±0.1

V. CONCLUSION AND FUTURE WORK

In this paper, hybrid blockchain-based authentication handover and flow rule validation is performed in SDN-5G HetNet. The main aim of this research is to provide security using hybrid blockchain. The private blockchain is used for validating the flow rules of the switches and public blockchain is used for ensuring the legitimacy of the users. Authentication handover is performed for providing security during handover. For ensuring the legitimacy of the users the proposed work performs Bio-SVA mechanism which provides the bio-Signature using Montgomery curve. FRM is used for monitoring load level of the switch by using HMM. Based on the flow rules proposed work classifies the switch into three classes such as normal, attacked, and suspicious, in which the attacked switch flows are dropped for enhancing security. Finally, intrusion detection and mitigation are performed by SNet-Fuzzy which classifies the suspicious switch flow into normal and malicious.

REFERENCES

[1] Bagaa, M., Dutra, D.L., Taleb, T., & Samdanis, K. (2020). On SDN-Driven Network Optimization and QoS Aware Routing Using Multiple Paths. *IEEE Transactions on Wireless Communications, 19*, 4700-4714.

[2] Sankar, S.P., Subash, T.D., Vishwanath, N.A., & Geroge, D.E. (2021). Security improvement in block chain technique enabled peer to peer network for beyond 5G and internet of things. *Peer-to-Peer Networking and Applications*, *14*, 392-402.

[3] Matheu, S.N., Robles Enciso, A., Molina Zarca, A., Garcia-Carrillo, D., Hernández-Ramos, J.L., Bernal Bernabe, J., & Skarmeta, A.F. (2020). Security Architecture for Defining and Enforcing Security Profiles in DLT/SDN-Based IoT Systems. *Sensors (Basel, Switzerland), 20*.

[4] Ibrahim, A.A., Hashim, F., Noordin, N.K., Sali, A., Navaie, K., & Fadul, S.M. (2021). Heuristic Resource Allocation Algorithm for Controller Placement in Multi-Control 5G Based on SDN/NFV Architecture. *IEEE Access, 9*, 2602-2617.

[5] Alshaer, H., & Haas, H. (2020). Software-Defined Networking-Enabled Heterogeneous Wireless Networks and Applications Convergence. *IEEE Access, 8*, 66672-66692.

[6] Hassan, N., & Fernando, X.N. (2020). An Optimum User Association Algorithm in Heterogeneous 5G Networks Using Standard Deviation of the Load. *Electronics, 9*, 1495.

[7] Hadem, P., Saikia, D.K., & Moulik, S. (2021). An SDN-based Intrusion Detection System using SVM with Selective Logging for IP Traceback. *Comput. Networks, 191*, 108015.

[8] Elsayed, M.S., Le-Khac, N., Albahar, M.A., & Jurcut, A.D. (2021). A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique. *Journal of Network and Computer Applications*, *191*, 103160.

[9] Podili, P., & Kataoka, K. (2021). TRAQR: Trust aware End-to-End QoS routing in multi-domain SDN using Blockchain. *J. Netw. Comput. Appl., 182*, 103055.

[10] Shi, N., Tan, L., Li, W., Qi, X., & Yu, K. (2020). A blockchain-empowered AAA scheme in the large-scale HetNet. *Digital Communications and Networks*.

[11] Imran, M., Durad, M.H., Khan, F.A., & Abbas, H. (2020). DAISY: A Detection and Mitigation System Against Denial-of-Service Attacks in Software-Defined Networks. *IEEE Systems Journal, 14*, 1933-1944.

[12] Li, N., Xia, S., Tao, X., Zhiyuan, Z., & Wang, X. (2020). An area based physical layer authentication framework to detect spoofing attacks. *Science in China Series F: Information Sciences*, *63*, 1-14.

[13] Monge, M.A., González, A.H., Fernández, B.L., Vidal, D.M., García, G.R., & Vidal, J.M. (2019). Traffic-flow analysis for source-side DDoS recognition on 5G environments. *J. Netw. Comput. Appl., 136*, 114-131.

[14] Park, D.G., Oh, J.W., & Jeong, J. (2020). SFSH: a novel smart factory SDN-layer handoff scheme in 5G-enabled mobile networks. *Journal of Ambient Intelligence and Humanized Computing*, 1-13.

[15] Huo, L., Jiang, D., Qi, S., & Miao, L. (2021). A Blockchain-Based Security Traffic Measurement Approach to Software Defined Networking. *Mob. Networks Appl., 26*, 586-596.

[16] Khellah, F.M. (2019). Control Plane Packet-In Arrival Rate Analysis for Denial-of-Service Saturation Attacks Detection and Mitigation in Software-Defined Networks. *Arabian Journal for Science and Engineering*.

[17] Abdulqadder, I.H., Zou, D., Aziz, I.T., Yuan, B., & Dai, W. (2021). Deployment of Robust Security Scheme in SDN Based 5G Network over NFV Enabled Cloud Environment. *IEEE Transactions on Emerging Topics in Computing*, *9*, 866-877.

[18] Ihsan H Abdulqadder, Shijie Zhou, Deqing Zou, Israa T. Aziz, Syed Muhammad Abrar Akber. (2020). Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms. Computer Networks, 179.

[19] Alezabi, K.A., Hashim, F., Hashim, S., Ali, B.M., & Jamalipour, A. (2020). Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks. EURASIP Journal on Wireless Communications and Networking, 2020, 1-34.

[20] Ali, A., & Yousaf, M.M. (2020). Novel Three-Tier Intrusion Detection and Prevention System in Software Defined Network. IEEE Access, 8, 109662-109676.