Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.019121
Article

Cyber-Attack Detection and Mitigation Using SVM for 5G Network

Sulaiman Yousef Alshunaifi, Shailendra Mishra* and Mohammed Alshehri

Department of Information Technology, College of Computer and Information Sciences Majmaah University, Majmaah, 11952, Saudi Arabia
*Corresponding Author: Shailendra Mishra. Email: s.mishra@mu.edu.sa
Received: 03 April 2021; Accepted: 05 May 2021

Abstract: 5G technology is widely seen as a game-changer for the IT and telecommunications sectors. Benefits expected from 5G include lower latency, higher capacity, and greater levels of bandwidth. 5G also has the potential to provide additional bandwidth in terms of AI support, further increasing the benefits to the IT and telecom sectors. There are many security threats and organizational vulnerabilities that can be exploited by fraudsters to take over or damage corporate data. This research addresses cybersecurity issues and vulnerabilities in 4G (LTE) and 5G technology. The findings in this research were obtained by using primary and secondary data. Secondary data was collected by reviewing literature and conducting surveys. Primary data were obtained by conducting an experimental simulation using the support vector machine (SVM) approach. The results show that cybersecurity issues related to 4G and 5G need to be addressed to ensure integrity, confidentiality, and availability. All enterprises are constantly exposed to a variety of risks. Also implemented an efficient SVM-based attack detection and mitigation system for 5G network. The proposed intrusion detection system defends against security attacks in the 5G environment. The results show that the throughput and intrusion detection rate is higher while the latency, energy consumption, and packet loss ratio are low, indicating that the proposed intrusion detection and defense system has achieved better QoS. The security solutions are fast and effective in detecting and mitigating cyber-attacks.

Keywords: Cybersecurity; cyberattack; vulnerability; threat; SVM; IDS

1 Introduction

The progressive adoption of technologies such as 4G and 5G has also brought some risk as they attract more attacks from hackers. For example, 5G can be considered insecure to some extent as it has many vectors through which the information and processes can be hacked from time to time. Therefore, it is important that regulators first acknowledge and accept the existence of threats so that appropriate mitigation measures can be taken. It is also expected that features such as network slicing will further enhance the security of 5G [1]. With the additional benefits of 5G also come additional risks. 5G creates a higher level of security threats, mainly because there are additional vectors through which attackers can attack. Another factor to consider in this context is 5G's ability to enable numerous connected devices known as the Internet of Things [2].

Machine learning techniques help in detecting attacks. There is an urgent need to develop machine learning techniques for network attack detection. Random Forest (RF), k-Nearest Neighbors (KNN), and Logistic Regression (LR) classifiers can be useful tools for detecting a distributed denial-of-service (DDoS) attack [3]. These Machine techniques could greatly facilitate attack surface malicious activity detection and disruption, improve social analysis, and automate repetitive security tasks in IoT networks [4]. In addition to linear classification, Support Vector Machine (SVM) can also use kernels to perform non-linear classification. It classifies traffic between normal and abnormal packets, and attacks can be classified based on traffic characteristics such as source port speed and standard deviation of flow packets. SVM has been used for a very simple but obvious reason, which is the fact that it has its development mechanism when it comes to algorithms, and its static prediction techniques lift it above most frameworks, not to mention how quickly and intelligently it can train and learn algorithms in both linear and nonlinear capacities. SVM is popular among all other techniques because it can very quickly separate the linear space from the supposedly nonlinear space [5].

The distributed denial-of-service (DDoS) detection rates are reported in [5–8] using the SVM algorithm are in the range of 93% to 98%. Therefore, the high efficiency of DDOS attacks and their ability to disrupt normal network functions is the main motivation for starting this research using SVM. One of the problems that have been studied in this research concerns the fact that as technologies such as 4G and 5G continue to develop and evolve, there are more and more security issues. 5G creates a higher level of security threats mainly because there are additional vectors through which attackers can attack [9]. The other factor to consider in this context is the ability of 5G to enable numerous connected devices known as the Internet of Things. So the overall problem is to find ways to maximize the benefits of 5G and on the other hand minimize the challenges. Given the increasing cybersecurity issues arising from the use of 4G and 5G networks, new approaches need to be adopted and applied to deal with these issues. A lack of focus on security can prove to be a disaster.

Therefore, in this regard, it is very important to have a comprehensive infrastructure in terms of connectivity and network security to effectively deal with the growing issues for cybersecurity [10]. Apart from this, an in-depth analysis of this problem is likely to be helpful for future researchers who want to conduct further analysis on this topic. Threats related to cybersecurity refer to the possibilities of an action leading to the corruption or theft of data and causing disruptions in various online and network activities [11,12].

This research is a step forward in identifying the cybersecurity issues and vulnerabilities associated with 4G and 5G telecommunication networks, the impact of cybersecurity issues and vulnerabilities associated with 4G and 5G telecommunication networks, and identifying the ways through which the cybersecurity issues and vulnerabilities associated with the use of 4G and 5G can be avoided. The results obtained from the primary and secondary data show that there are some important cybersecurity issues related to the use of 4G and 5G telecommunication networks that need to be considered by the regulators. The result was compared with the results of previous work reported in [13,14] for validation. The intrusion detection rate in the proposed approach can be varied according to the number of nodes that arrived in the network. Moreover, the proposed intrusion detection system can be used to defend against security attacks in LTE and 5G environments.

The paper is divided into six sections. Section one covers the background of the research, the purpose to be achieved by this particular study and the questions to be answered. Section two addresses the literature review by reviewing the analysis of previous research on this particular topic along with highlighting the main gaps of the study. The research process and methods providing an overview of the methods used in the research and their rationale are discussed in section three. The test and result analysis and conducting evaluations and validations based on a particular theme are discussed in section four. Interpretation of the results is discussed in terms of the purpose to be achieved. The paper is concluded in section five.

2 Related Work

The development of 4G LTE technology is beneficial in containing the identity of users through 4G network services. The range of data that can be taken by the hackers from virtually all users around the world is endless and it could involve tracking the location of a user from the nearest cell tower data and create problems for the identities of users from their networks [15]. This can be complex as the identity hackers would then be able to obtain the information about the users' identities and subsequently use this information for a wide range of digital misdeeds including money forgery, data theft, and identity cloning as this is dangerous at a random point at the time of exchanging identities through 4G network technology [16].

In Alshouiliy et al. [17] researchers state that the services provided by 4G network technology may not have a proper security system to protect the services of 4G LTE services and can be stolen by hackers who can illegally gain access to the services, which is a major threat to 4G LTE network providers. Unauthorized access to 4G LTE services can be difficult and complex for users, and the attackers can gain access to 4G services without authorization, which is a challenge for 4G providers [18]. The hacker can gain unauthorized access due to weak passwords, low security against social design recently infiltrated datasets, and insider threats. The attacks on 4G services can be carried out by hackers within the services in the form of traffic disruption, either between the user's network and external targets or within the user's network [18]. 4G LTE network services can be attacked by the hackers using a range of passive and dynamic digital attacks including eavesdropping or packet sniffing, remote convention attacks, port inspection, jamming and denial of administration, fake validation, replay attacks, vulnerability abuse, traffic investigation and unauthorized access to 4G technology [19].

The 5th generation wireless network infrastructure is based on improving existing mobile networks and their connectivity to unprecedented levels. Together with the increasing internet connectivity worldwide and smarter devices than ever before, 5G networks aim to achieve widespread and mass connectivity at optimal levels. In addition to the numerous benefits expected from the potential of 5G in everyday life, there are also some risks and challenges that need to be addressed accordingly to achieve maximum benefits. These include understanding the complexity of the massive network and the corresponding security concerns and threats to which it is vulnerable [20,21].

One of the cybersecurity issues identified about the use of 5G networks is the reduction of the level of encryption in early connections. The term "encryption" in this context refers to the encryption of the communication between a 5G network and a specific device. This level of security during the communication process is critical to prevent cyber attackers or other dangerous parties from easily intercepting the communication and using this information to harm the user. On the other hand, if the encryption during the initial connection is low, the hackers can easily gain access to critical information about the devices and the network [22]. The advances in 5G have led to cybersecurity issues related to the increase in load level in terms of bandwidth of the current infrastructure [23].

Threats related to IoT connections have also been identified as a major cybersecurity concern related to 5G networks. Artificial intelligence-equipped devices can effectively and automatically share data and adjust their performance. Threats related to IoT connections have also been identified as a major cybersecurity concern related to 5G networks. Artificial intelligence-equipped devices can effectively and automatically exchange data and adjust their performance to achieve an optimal level of efficiency [24]. Therefore, in addition to smart device manufacturers and the public, mobile companies must also do their part to ensure security in a 5G network. Otherwise, it could cause serious problems for the majority of its users without being the direct target of an attack itself [25].

During the pandemic, the 5G and 4G networks should merge the personal information in an approach that focuses on services and privacy. There are several ways in which the concept of crowdsourcing can be used to address cybersecurity issues related to 5G networks, such as use for commercial purposes, use for the

rapid response after natural disasters [26]. Therefore, it is important to identify how the risks associated with 4G and 5G can be avoided. However, the analysis also shows that it is important for users to be aware of the challenges so that they can take the necessary preventive measures to avoid the vulnerabilities of 4G and 5G.

The related work analysis has shown that although the magnitude of cybersecurity problems and threats has increased with the advances in technology, more analysis needs to be done in this regard to reduce the threats from the cybersecurity problems and vulnerabilities in the future. Based on this information, it can be said that it is important to conduct further research to find out how to maximize the benefits of 4G and 5G with special reference to the telecommunication sector and other industries to provide maximum benefits to the users.

3 Research Methodology

3.1 Qualitative Approach

In this research, both qualitative and quantitative data are used. Qualitative data will be collected by extracting data from secondary sources, such as a literature review, and by extracting data from various online sources and articles. The reason for obtaining secondary data in the study is to obtain detailed and in-depth information about the topic understudy in the research related to the study of cybersecurity issues and vulnerabilities associated with 4G and 5G networks. The survey in this research was conducted among the strategic level managers in the telecommunication and IT industry. Data analysis was done using SPSS, which is considered to be an extremely useful software for performing this type of calculation and analysis. The process started with the identification of cybersecurity issues and challenges which led to the identification of 4G and 5G challenges.

3.2 Quantitative Approach

In today's world, the mobile device market has grown tremendously due to the creation of 4G, 5G, and beyond 5G architecture which plays a major role in wireless *ad hoc* networks. In recent years, an intrusion detection system (IDS) has been widely used to mitigate misbehaving users in a cellular environment. A IDS detects attacks on the network as early as possible and takes appropriate action [27–29]. A IDS detects actions, but it does not take preventive action when an intrusion is detected. IDS collects all packets from the network and finds attack patterns. IDS can send an alert to the administrator or a respected device to prevent intrusion. The flow chart of the proposed intrusion detection system to prevent security attacks in 5G environments is shown in Fig. 1.

3.2.1 Nodes Authentication

We used elliptic curve cryptography (ECC) to authenticate the node. The elliptic curves are used for encryption, digital signatures, and pseudo-random generators [30]. It uses small key sizes compared to other asymmetric encryption algorithms. ECC generates public and private keys depending on the elliptic curve theory. The elliptic curve theory builds on the elliptic curve Eq. (1) as follows.

$$y^2 = x^3 + ax + b \tag{1}$$

The corresponding elliptic curve for the Eq. (1) can be plotted as shown in Fig. 2, the following terms are used: E (elliptic curve), P (point on the curve), and n (maximum limit for the prime number).

3.2.2 Key Generation

From the elliptic curve, the public key (Q) is generated as follows,

$$Q = Pr * P \tag{2}$$

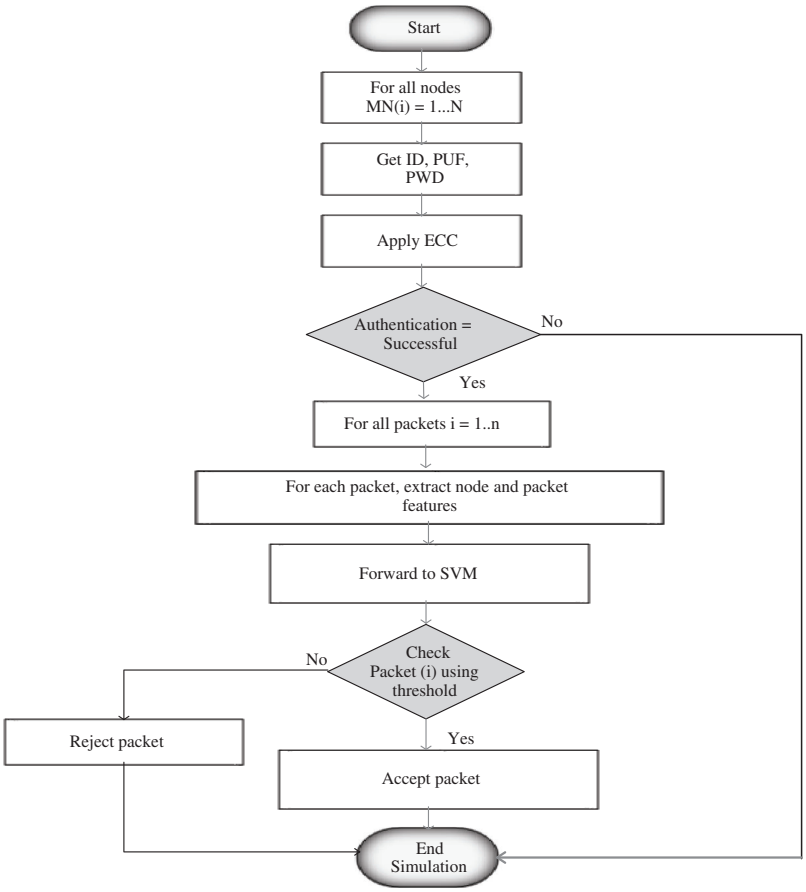

Figure 1: The flow chart of the proposed intrusion detection system to prevent security attacks in the 5G environment

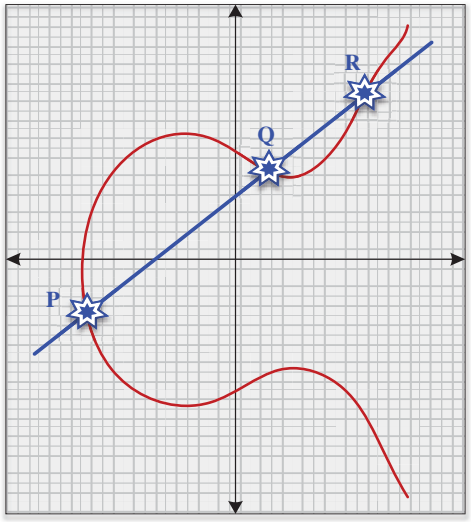

Figure 2: Elliptic curve

Here Pr is the random number that resides within the range of n. And P is the point of the elliptic curve. In the above equation, Q is the public key and Pr represents the private key.

3.2.3 Encryption

Consider a data D on the elliptic curve. Then, a random number k is selected from $[1,(n-1)]$. Upon these parameters, two ciphertexts Ct_1 and Ct_2 are generated for d as follows,

$$Ct_1 = k * P \tag{3}$$

$$Ct_2 = D + k * Q \tag{4}$$

3.2.4 Decryption

For received Ct_1, Ct_2 the original data is extracted as follows,

$$D = Ct_2 - Pr * Ct_1 \tag{5}$$

The ECC algorithm generates public and private keys and performs encryption and decryption operations. The user U_i who wants to access the cloud submits the {ID,PW} to the TA. The TA first verifies the ID and PW for the corresponding user. If ID and PW are correct, TA generates random ID (R_ ID ^t (U_i)). Where t represents the sequence of randomly generated ID for U_i. The first time t = 1, then it is incremented for each authentication request received from U_i. The random value ID is generated at each time and is variable. Physically Unclonable Function (PUF) is a strong security metric. To provide faster and efficient authentication, PUF is presented which is a lightweight authentication. This PUF is one of the most suitable security solutions for resource-constrained IoT devices. In this PUF, the designed circuit receives a set of bits with which the response is generated. Based on the challenges received by the circuit, the response is generated and the particular device is authenticated. In this process, authentication in PUF is done through two phases as follows.

3.2.4.1 Enrollment Phase

In this phase, the IoT device and the server communicate with each other by establishing a connexion between them. A challenge is sent from the server to the PUF to ensure that the device is legitimate. After receiving the challenge from the server, the PUF responds with the appropriate response. In this way, all challenges are answered by the PUF. The server stores all the challenge and response pairs used in authenticating the IoT device.

3.2.4.2 Authentication Phase

After registering each IoT device, they are ready for data transmission with authentication. For a random generation of ID, TA uses the ECC equation as in Eq. (4). The graph generates multiple IDs at the same time. The random ID is two points such as X,Y that satisfy the curve equation. This step is formulated as follows,

$$U_i \rightarrow \{ID \oplus PW\} \rightarrow TA \tag{6}$$

$$TA \rightarrow \left\{R^t_{ID}(U_i),\ if\ (ID\&\&PW\&\&PUF\&\&SK == True)\right\} \tag{7}$$

where, $R^t_{ID}(U_i) = \{X, Y\}$. ECC generates the curve points in a fast manner and also generates multiple random IDs. Thus, using the ECC curve for random ID generation minimizes the time consumption and also increases the security level. If the ID and PW are invalid or mismatched, then the authentication request received from U_i is ignored. This step only allows valid users to the next level.

3.3 Intrusion Detection from Packets Processing

In wireless networks, there are two steps, namely, data collection and packet analysis for intrusion detection.

3.3.1 Data Collection

From the network environment, different packet streams are collected at different times. From the packet stream Packet Size, Packet Type, Host Type, and Protocol Type are extracted. When packet streams are collected they are stored in the database.

3.3.2 Packet Analysis for Intrusion Detection

This step plays a crucial role in determining whether the input packet stream is an attack or not. Due to the dynamic nature of mobile nodes, the input packet stream varies in size and context. Therefore, packet analysis is the first step of intrusion detection, which must be performed adaptively to enable late intrusion detection. In this step, the process of intrusion detection takes place which analyzes the packet features and takes the appropriate action. Various packet characteristics such as sender IP address, destination IP address, protocol type, number of packets sent, time of communication, packet type, and packet size are used for classification purposes.

Fig. 3, describes how intrusion detection and prevention using SVM, the feature sets are directly derived from the SVM technique. Intrusion prevention by authentication and can be considered as the first key to block the existence of misbehaving nodes, and it minimizes the possibility of misbehaving nodes and also their effects. Symmetric and asymmetric cryptography methods have been proposed as intrusion prevention methods.

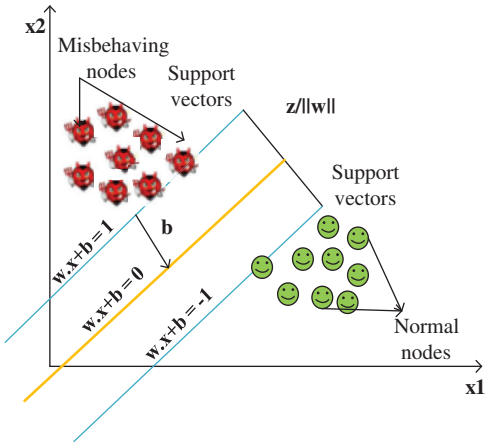

Figure 3: Intrusion detection using SVM

3.4 Experimental Setup

Network simulator NS3.26 and OS Ubuntu 14.04 LTS are used for simulation. The proposed intrusion detection system is considered as 1000 m × 1000 m simulation environment for testing various security attacks. The simulation environment for the proposed system is shown in Fig. 1. To test the proposed approach, the NSL-KDD dataset is used [31]. From the NSL-KDD dataset, all the features are tested and classified into attacks/normal packets.

Step 1: Create a 5 G-based network which consists of 1-5G Base Station, 1-Server, 2-LTE eNodeB, 2-AP, and 100 User Nodes.

Step 2: All user nodes are registered with a node ID, PUF, and secret key, where the generation of the secret key is based on the ECC method.

Step 3: The communication between the user nodes is performed.

Step 4: Based on the communication, the protocol/traffic details are collected, such as IP address of sender and receiver, port number, communication data size, packet type, etc. (Extract the packet header information for attack detection).

Step 5: Load the collected dataset (NSL-KDD dataset) and perform the classification process using SVM (binary classes - normal and malicious).

Step 6: Analyze the generated traffic data and detect the malicious nodes.

Step 7: Plot the graph;

- Throughput (Mbps) in terms of the number of users.
- Latency with respect to the number of users
- Energy consumption with respect to the number of users
- Packet Loss Rate (%) with respect to the number of users
- Intrusion Detection Rate (%) In terms of the number of users

4 Test Result and Analysis

The data was collected from various experts in the IT and telecom industry who are involved in the deployment of 4G and 5G technology. The analysis of primary data was done using SPSS, high-quality software for analysis of quantitative and primary data. The tools used for the analysis are frequency analysis to identify the trend of the respondents' answers. Regarding the question of the role of technological advancement in the increase of cybersecurity issues and vulnerabilities, 60% of the respondents agreed with this statement, which highlights the role of technology and the development of networks such as 4G and 5G in the increase of cybersecurity issues and vulnerabilities. In terms of increasing customer usage causing cybersecurity issues related to 4G and 5G, more than 68% of respondents agreed that increasing customer usage has paved the way for increased levels of cybersecurity issues and vulnerabilities. For the third question (cybersecurity issues impacting the integrity of 4G and 5G networks), the results show that overall 50% agreed with this statement, while 34% disagreed and 16% remained neutral towards this statement. One of the security threats related to 4G that is discussed is user identity theft. The results in this regard show that 45% of the respondents agreed with the existence of this particular threat, while 34% disagreed with this statement and the remaining respondents remained neutral.

The other question asked in relation to 4G related to hacking attacks as part of the main cybersecurity issues. Overall, 58% of respondents agreed with this issue, while 31% disagreed. Denial of Service is an important cybersecurity issue. The results for Denial of Service were almost identical to those for Hacking, as 58% of respondents agreed with this theme. Encryption is an important issue when using 5G. The results show that 60% of the respondents agreed with the statements in the questionnaire that encryption is an important issue when using 5G. When the respondents were asked about the issue of bandwidth stress when using 5G telecommunication networks, 60% of the respondents agreed with the fact that this problem exists for the users and therefore appropriate steps are required to solve it. Only 29% of respondents disagreed with the existence of this particular problem.

The lack of central security is another issue that was included in the questionnaire because it was present in the results of the literature. Slightly more than 50% of the professionals who participated in the survey agreed with this particular statement that was part of the questionnaire. One of the main threats

highlighted in the literature and included in the survey was related to the lack of awareness of customers or users. Of the 100 respondents who participated in the survey, 65% agreed with the statement while 25% disagreed and the rest were neutral. In terms of whether IoT connectivity creates cybersecurity issues, there were mixed results on this statement as 44% of respondents agreed with the existence of this issue related to 4G and 5G telecommunication networks. Privacy Issues associated with cybersecurity issues and vulnerabilities, out of the 100 respondents, 56% of the respondents agreed that privacy issues are important in the context of cybersecurity issues and vulnerabilities.

Since it is important to deal with cybersecurity issues effectively, the focus of the survey was also to determine the importance of the solutions stated in the literature. Therefore, after the analysis, 63% of the respondents agreed that training the people who operate 4G and 5G networks is very important to deal with all the issues effectively and reduce the negative impact of the security issues. The last question asked to the respondents during the survey was related to the importance of taking action on regulatory and technical adjustments and policies. The results show that 64% of respondents agreed with this statement, which highlights the need for regulators to successfully implement these measures to reduce cybersecurity problems and threats.

The simulated 5G network consists of 1-5G Base Station, 1-server, 2-LTE eNodeB, 2-AP, and 100 User Nodes. All user nodes with a node ID, Physically Unclonable Functions (PUF), and a secret key, the generation of the secret key is based on the ECC method. Based on the communication between user nodes, the protocol/traffic details are collected, such as the IP address of sender and receiver, port number, communication data size, packet type, etc. (Extract packet header information for attack detection). Load the collected dataset (NSL-KDD dataset) and perform the classification process using SVM (binary classes - normal and malicious). Perform the packet flow-based feature extraction and the extracted features are classified using SVM. SVM classifies the packets into normal or malicious as shown in Fig. 4.

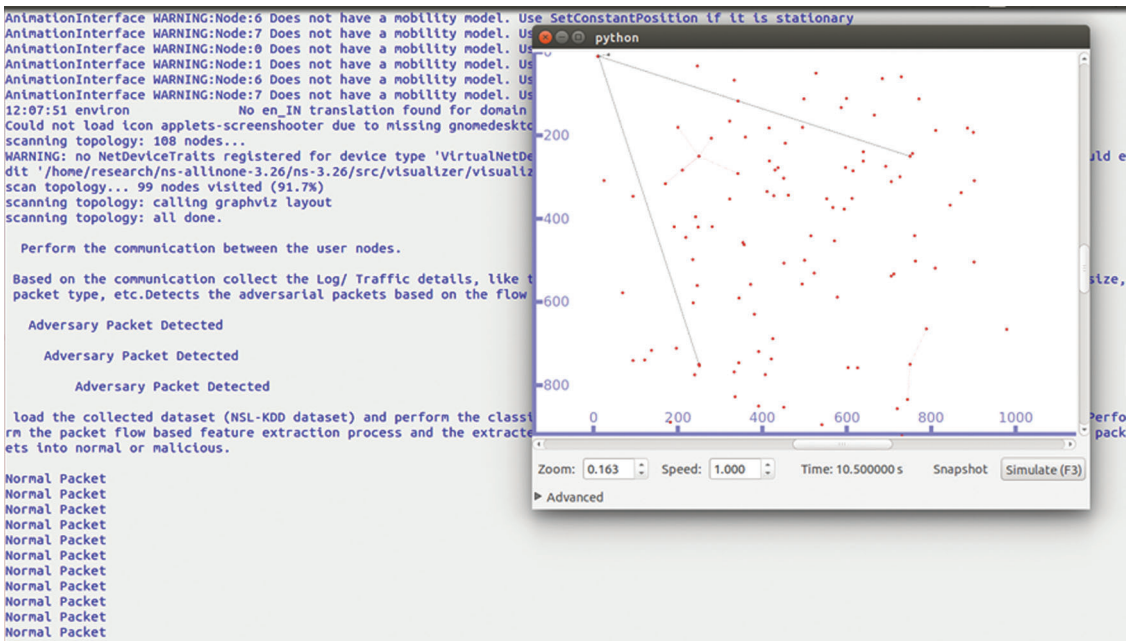

Figure 4: All dataset packets classification

Generated data traffic is analyzed and malicious nodes are detected. The classification is performed and classifies the type of attacks, like, DDoS, the man in the middle, Phishing, SQL injection, and false data injection with the number of counts as shown in Tab. 1 and Fig. 5.

Table 1: Attacks classification

Attack	Count
DDoS	892
Man to the Middle	3599
Phishing	3633
SQL Injection	41214
False Data Injection	2931
Normal Count	73704

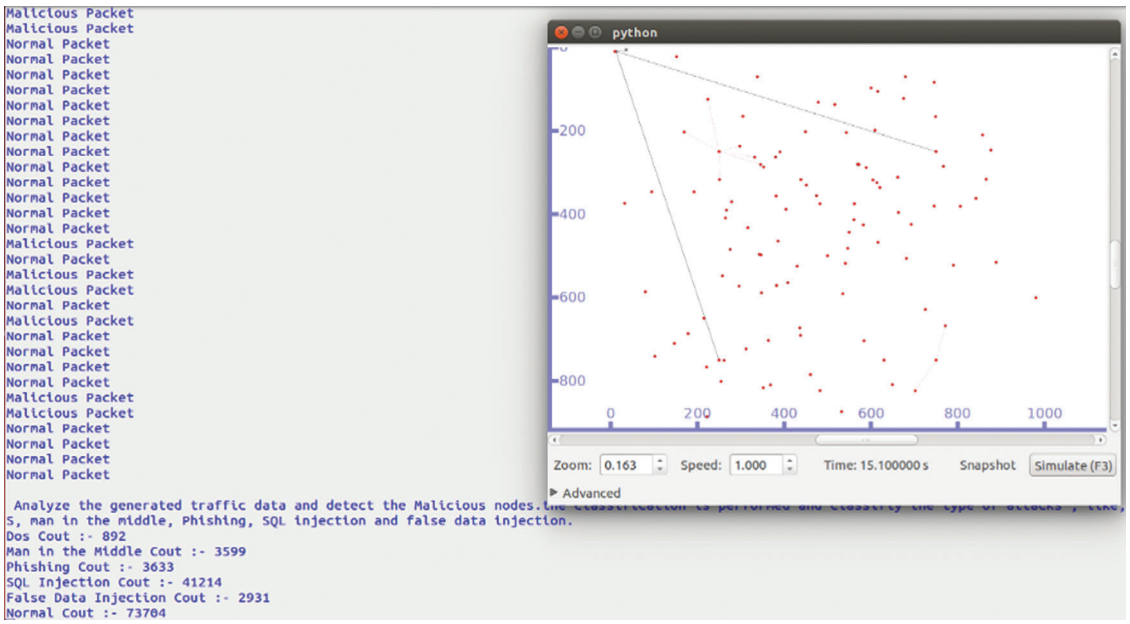

Figure 5: Attacks classification

In a network, the packets are delivered via wireless links and also transmitted through either single-hop or multi-hop communication. It is measured in bits per second (Bit/s or BPS), which can be measured as data packets per second or per time slot.

$$Throughput = \sum_{i=1}^{n} NPR / \sum_{i=1}^{n} NPS \times Num\_H \tag{8}$$

where NPR represents the number of packets received, NPS represents the number of packets sent, and Num_H represents the number of hops from the origin to the destination node. The resulting graph for throughput (Mbps) for the number of users. Throughput is calculated by the successful transmission rate of packets from the source to the destination node. It is a positive metric that is higher to indicate that the IDPS has achieved the better QoS (Fig. 6).

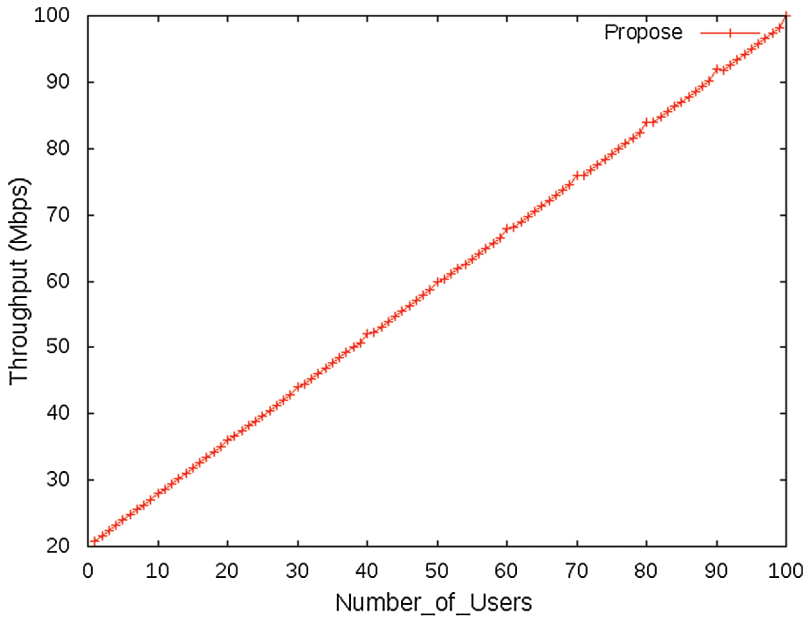

Figure 6: Throughput *vs*. number of users

Latency refers to the time required to detect the total number of attack packets at time Δt by SVM. In other words, it is the attack detection starting time (AD_{ST}) and ending time (AD_{ET}).

$$Latency = AD_{ET} - AD_{ST} \tag{9}$$

The resulting graph for latency with respect to the number of users. Latency is an important factor in designing an intrusion detection scheme, as timely detection of attacks can help to avoid major damage to the network or severe losses due to attackers. In this study, latency is considered an important criterion to represent the performance (Fig. 7.).

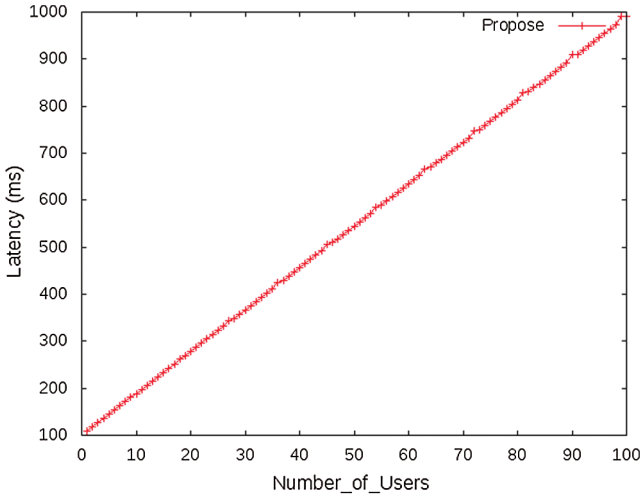

Figure 7: Latency *vs*. number of users

For any kind of wireless network, energy consumption is a significant metric that is defined as the rate of energy spend for processing a single packet from the source to a destination node. Hence, energy consumption (EC) as Joules is computed by,

$$EC = E_{Adv} + E_{Dis} + E_{Syn} + E_{Res} \tag{10}$$

where E_{Adv} represents the energy consumption rate for packets advertisement, E_{Dis} represents the energy consumption rate for packets discovery, E_{Syn} represents the energy consumption rate required to synchronizing the packets and E_{Res} represents the rate of energy consumption for packets acknowledgment. The resulting graph for Energy Consumption for the number of users. Energy consideration is a vital asset to enrich network QoS. Most of the attackers aiming to reduce the resources of mobile nodes. Due to low energy value, nodes are not capable to send a packet from the source to the destination node (Fig. 8). By proposing novel and lightweight algorithms for intrusion detection, the rate of energy consumption is reduced.

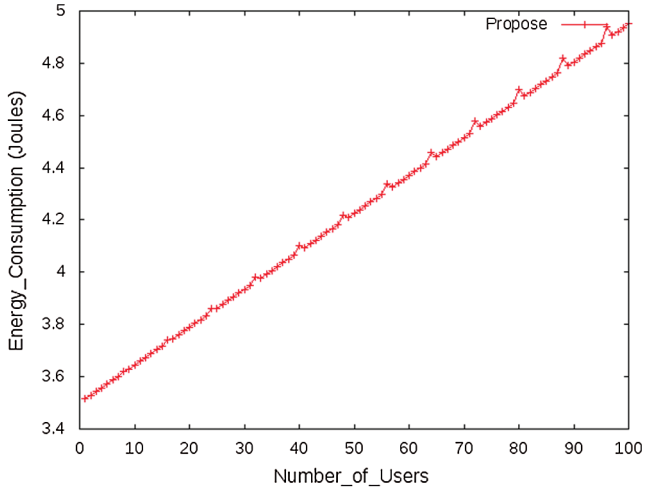

Figure 8: Energy consumption *vs*. number of users

Packet loss ratio is defined as the rate of packets that are not obtained to the destination successfully in a network to the total number of packets sent from the source node (Fig. 9).

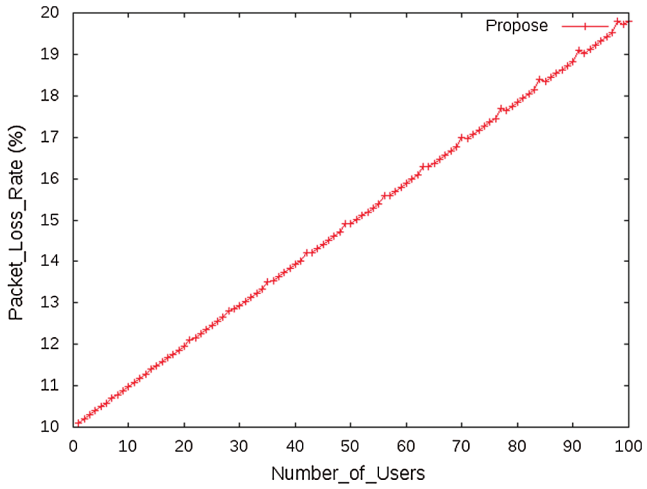

Figure 9: Packet loss rate *vs*. number of users

$$PLR = Num\ of\ packets\ sent - Num\ of\ packets\ delivered \tag{11}$$

PLR is the significant QoS metric in MANET that needs to show greater performance during intrusion detection. A node's historical behavior is an essential term that represents the collection of activities (transmission and reception) for a node. The resulting graph for Packet Loss Rate (%) Concerning the number of users. With the use of True Positive (TP) attack detection rate is calculated. It is defined by the sum of packets categorized correctly as attacks as a total number of attacks originally present. It is computed by:

$$IDR = \frac{\#\ of\ detected\ attacks}{\#\ of\ attacks} \times 100\% \tag{12}$$

$$IDR = TPR = \frac{TP}{TP + FN} \tag{13}$$

The resulting graph for Intrusion Detection Rate (%) Concerning the Number of users is illustrated in Fig. 10.

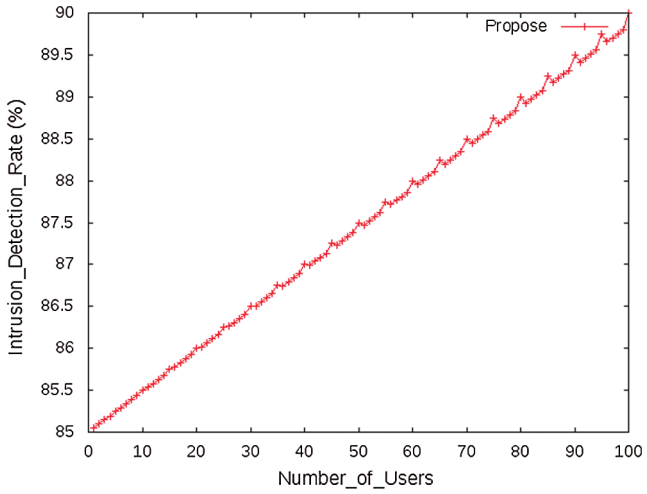

Figure 10: Intrusion detection rate *vs*. number of users

The intrusion detection rate can be varied according to the number of nodes that arrived in the network. On the account of SVM usage, both intrusion detection and prevention are worked out and it finds the attackers inside the network.

5 Conclusions

Cybersecurity issues and vulnerabilities are important because they greatly compromise the use of 4G and 5G technologies. One of the ways through which users are affected by the use of 4G and 5G is through invasion of their privacy. In the case of 5G, there is a location data privacy issue that occurs mainly due to the fact that 5G has a much smaller coverage area, which creates a situation where many cell towers are close together within a small radius. The cybersecurity challenges can affect users in the form of attacks that are carried out in different categories. These include privacy attacks, integrity attacks, availability attacks, and authentication attacks. The presence of attacks on a significant scale has created considerable doubt among users about the use of these technologies and how they can be used safely in the future. The use

of mixed methodology is a challenge as the researcher needs to use both qualitative and quantitative methodologies effectively and appropriately. The other challenge identified in relation to the process of data collection and analysis is the ethical considerations that may have affected the validity and authenticity of the overall findings. The results obtained through the primary and secondary data show that there are some important cybersecurity issues related to the use of 4G and 5G networks that need to be considered by regulators. The problem with these challenges is that they affect user privacy and create issues related to the integrity of 4G and 5G networks. Another important finding was the role of technological advancement in increasing the level of cybersecurity issues and vulnerabilities. The resulting analysis of the survey showed that the lack of user awareness is perhaps the most important issue that needs to be addressed to improve the integrity of 4G and 5G networks. Some other findings presented in this context include securing end-to-end data along with developing collaboration with stakeholders so that the required solutions can be identified and implemented appropriately. Simulation results based on the protocol, traffic details, sender and receiver IP address, port number, communication data size, packet type etc. The SVM classifiers classify the packets into normal or malicious packets. The classification is performed and classifies the type of attacks such as DDoS, Man in the Middle, Phishing, SQL Injection, and False Data Injection. The calculated throughput and intrusion detection rate are higher while the latency, energy consumption, and packet loss rate are lower indicating that the IDPS has achieved better QoS. In addition to theoretical designs and implementations, we must recognize that intrusion detection and prevention is an emerging and growing technology that supports many real-time and non-real-time applications in all major domains. The main role of intrusion detection is based on providing security during the communication between the sources and the destination node. However, in a 5G environment, security is the first and foremost requirement as there is no centralized environment and also high dynamic mobility. Although Physically Unclonable Function (PUF) is considered a very expensive option in today's market, our simulation has shown that it is a very strong security metric and one of the most recommended and suitable security solutions for resource-constrained IoT devices. Consequently, it is fair to say that the results of the research will be important for improving the use of 4G and 5G telecommunication technology.

Acknowledgement: The authors sincerely acknowledge the support from Majmaah University, Saudi Arabia for this research.

Funding Statement: The authors would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work under Project Number No -R-2021-122.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. Mrabet, S. Belguith, A. Alhomoud and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors*, vol. 20, no. 13, pp. 3625, 2020.

[2] K. Bouraqia, E. Sabir, M. Sadik and L. Ladid, "Quality of experience for streaming services: Measurements, challenges and insights," *IEEE Access*, vol. 8, pp. 13341–13361, 2020.

[3] A. Churcher, R. Ullah, J. Ahmad, F. Masood, M. Gogate *et al.,* "An experimental analysis of attack classification using machine learning in IoT networks," *Sensors*, vol. 21, no. 2, pp. 446, 2021.

[4] P. Arora, B. Kaur and M. A. Teixeira, "Evaluation of machine learning algorithms used on attacks detection in industrial control systems," *Journal of The Institution of Engineers (India): Series B*, vol. 102, pp. 1–12, 2021.

[5] S. Mishra, S. K. Sharma and M. A. Alowaidi, "Multilayer self-defense system to protect enterprise cloud," *CMC-Computer Materials & Continua*, vol. 66, no. 1, pp. 71–85, 2021.

[6] A. Mubarakali, K. Srinivasan, R. Mukhalid, S. C. Jaganathan and N. Marina, "Security challenges in internet of things: Distributed denial of service attack detection using support vector machine-based expert systems," *Computational Intelligence*, vol. 44, no. 1, pp. 41, 2020.

[7] K. S. Sahoo, B. K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy *et al.,* "An evolutionary SVM model for DDOS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 132502–132513, 2020.

[8] S. Mishra, "SDN-based secure architecture for IoT," *International Journal of Knowledge and Systems Science (IJKSS)*, vol. 11, no. 4, pp. 1–16, 2020.

[9] Z. Qadir, F. Ullah, H. S. Munawar and F. Al-Turjman, "Addressing disasters in smart cities through UAVs path planning and 5G communications: A systematic review," *Computer Communications*, vol. 168, pp. 114–135, 2021.

[10] J. Moysen and L. Giupponi, "From 4G to 5G: Self-organized network management meets machine learning," *Computer Communications*, vol. 129, pp. 248–268, 2018.

[11] M. Humayun, M. Niazi, N. Zaman, M. Alshayeb and S. Mahmood, "Cyber security threats and vulnerabilities: A systematic mapping study," *Arabian Journal for Science and Engineering*, vol. 45, pp. 3171–3189, 2020.

[12] S. Mishra, M. A. Alowaidi and S. K. Sharma, "Impact of security standards and policies on the credibility of e-government," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 1–12, 2021.

[13] R. Prasad, S. Lakshminarayanan and S. Arumugam, "Market dynamics and security considerations of 5G," *Journal of ICT*, vol. 5, no. 3, pp. 225–250, 2018.

[14] E. Connell, D. Moore and T. Newe, "Challenges associated with implementing 5G in manufacturing," *Telecom*, vol. 1, no. 1, pp. 48–67, 2020.

[15] M. Suryanegara, F. Andriyanto and B. Winarko, "What changes after switching to 4G-LTE? findings from the indonesian market," *IEEE Access*, vol. 5, pp. 17070–17076, 2017.

[16] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: analysis, challenges and solutions," *Computers & Security*, vol. 68, pp. 81–97, 2017.

[17] K. Alshouiliy and D. P. Agrawal, "Confluence of 4G LTE, 5G, fog, and cloud computing and understanding security Issues," in *Fog/Edge Computing for Security, Privacy, and Applications*, pp. 3–32, 2021.

[18] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Vehicular Communications*, vol. 20, pp. 100–182, 2019.

[19] R. Hussain, F. Hussain and S. Zeadally, "Integration of VANET and 5G security: A review of design and implementation issues," *Future Generation Computer Systems*, vol. 101, pp. 843–864, 2019.

[20] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Blockchain for 5G and beyond networks: A State of the Art Survey," *Journal of Network and Computer Applications*, vol. 166, pp. 102693, 2020.

[21] M. Noura and R. Nordin, "A survey on interference management for device-to-device (D2D) communication and its challenges in 5G networks," *Journal of Network and Computer Applications*, vol. 71, pp. 130–150, 2016.

[22] A. A. Abd El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5G internet of things scenario," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 118–131, 2020.

[23] A. Gupta, R. K. Jha, P. Gandotra and S. Jain, "Bandwidth spoofing and intrusion detection system for multi stage 5G wireless communication network," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 618–632, 2017.

[24] J. Cao, M. Ma, H. Li, Y. Sun, L. Xiong *et al.,* "A survey on security aspects for 3GPP 5G networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 170–195, 2019.

[25] D. Minoli and B. Occhiogrosso, "Practical aspects for the integration of 5G networks and IoT applications in smart cities environments," *Wireless Communications and Mobile Computing*, vol. 6, pp. 1–30, 2019.

[26] A. Nieto, A. Acien and G. Fernandez, "Crowdsourcing analysis in 5g IoT: Cybersecurity threats and mitigation," *Mobile Networks and Applications*, vol. 24, pp. 881–889, 2019.

[27] Y. Benslimen, H. Sedjelmaci and A. C. Manenti, "Attacks and failures prediction framework for a collaborative 5G mobile network," *Computing*, vol. 103, pp. 1–17, 2021.

[28] I. Essop, J. C. Ribeiro, M. Papaioannou, G. Zachos, G. Mantas *et al.,* "Generating datasets for anomaly-based intrusion detection systems in IoT and industrial IoT networks," *Sensors*, vol. 21, no. 4, pp. 1528, 2021.

[29] T. Su, H. Sun, J. Zhu, S. Wang, Y. Li *et al.,* "Deep learning methods on network intrusion detection using NSL-KDD dataset," *IEEE Access*, vol. 8, pp. 29575–29585, 2020.

[30] S. K. Mousavi, A. Ghaffari, S. Besharat and H. Afshar, "Improving the security of internet of things using cryptographic algorithms: A case of smart irrigation systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 2, pp. 2033–2051, 2021.

[31] NSL-KDD, [Online]. Available: https://web.archive.org/web/20150205070216/http://nsl.cs.unb.ca/NSL-KDD/.