Journal of Scientific & Industrial Research
Vol. 80, January 2021, pp. 60-65

A New Efficient Method for the Detection of Intrusion in 5G and beyond Networks using ML

Vikash Yadav[1]*, Mayur Rahul[2] and Rishika Yadav[3]
[1]ABES Engineering College, Ghaziabad, Uttar Pradesh, India
[2]Department of Computer Application, UIET, CSJM University, Kanpur, India
[3]Graphic Era Hill University, Dehradun, India

Received 01 August 2020; revised 19 November 2020; accepted 26 November 2020

The 5G networks are very important to support complex application by connecting different types of machines and devices, which provide the platform for different spoofing attacks. Traditional physical layer and cryptography authentication methods are facing problems in dynamic complex environment, including less reliability, security overhead also problem in predefined authentication system, giving protection and learn about time-varying attributes. In this paper, intrusion detection framework has been designed using various machine learning methods with the help of physical layer attributes and to provide more efficient system to increase the security. Machine learning methods for the intelligent intrusion detection are introduced, especially for supervised and non-supervised methods. Our machine learning based intelligent intrusion detection technique for the 5G and beyond networks is evaluated in terms of recall, precision, accuracy and f-value are validated for unpredictable dynamics and unknown conditions of networks.

Keywords: Authentication, Cryptography, Machine Learning, Physical layer, Reliability

Introduction

The 5g-and-beyond networks have received lot of attention from the researchers and academician, which will provide different types of application by connecting various types of machines and devices.[1] The adequate increasing quantity of low-cost machine and devices, increasing number of access points and heterogeneity produce complicated and complex environment of 5G networks. Due to global nature of radio signals propagation, internet communication properties, widely used transmission protocols and wireless communication provides extremely easy target for the spoofing attacks and interceptions.[2] The 5G technology mentioned to us as afar 2020 communication system denotes the next generation of the global communication system, with modern successful application in various areas in every continent. The characteristics of the 5G networks are described by three main components: ultra-reliable communication services, improved mobile broadband and massive based communication.[3] Due to rapid growth in intelligent mobile and high-speed development of communication techniques, 5G can be a backbone for the excess of modern business chances and applications, provide the facility of endless association between billion of devices interconnected. The 5G network becomes revolution for the global organisations and gives immediate effect on the business shareholders and customers. The important objective of 5G network is to give advanced and customize user-oriented services and provide connection to the humans covering all requirements and make the maximum utilities of emerging services and user traffic.[4] To achieve these goals, several techniques use to enable 5G technology such as edge computing, cloud computing, Network Function Virtualization (NFV), Software Defined Networking (SDN), D2D communication and Network Slicing.[5] However, quick gush and high-speed evolution of 5G services in terms of capacity, scale and speed produce new problems such as data stability, privacy and network reliability must be resolved before wide implementations.[6]

Many safety and security techniques have been proposed in earlier 4G version of computer networks. Some protocols used in physical layer are used for detection of intrusion in the networks. However, detection of errors data compression, data storage and data communication, cyclic redundancy check (CRC)

*Author for Correspondence
E-mail: vikash.yadav@abes.ac.in

has been incorporated in radio link control (RLC) for the reliable delivery of data. The above security methods and design are not suitable for the 5G, due to the following purpose:

(1) An important reason is that above methods used in the previous generations are less efficient to deal with data security for example alteration, injection and deletion in 5G technologies.

(2) Another problem is the incorporation of latest technologies and structure of 5G, which create new problem for privacy and security to protect from data integrity.

The growing technologies of 5G such as network slicing, D2D communication NFV, SDN will carry new models for all services and further security challenges. Except the endowment of cellular networks, 5G networks are going to found all over the place and separated services and have primary focus on privacy and security requirement for the reliable services. The management in services of 5G are more complicated due to enormous amount of different device connected. The big challenge for researchers is to provide architecture, which is capable of data sharing, multiuser access and spectrum sharing. Also, able to preserve the global services of 5G like transparency and large data immutability is the important issue. The security architecture of the previous technologies is unable to preserve the services to safe 5G networks. The classification of intrusion detection system is presented in Table 1.

In the modern era of 5G/6G, decentralization, transparency and immutability are the key features secure the successful incorporation of new latest services such as driverless cars, IOT, Federated Learning (FL), Unmanned Aerial Vehicles (UAV). Among different technologies present these days, machine learning is the best technique to detect the intrusion and attacks in 5G/6G technologies and to reshape the technology requirements.[7] Further, 5G requires machine learning to protect from attacks from outside world. Every part of the 5G/6G is the easy target for the cyber attackers. The machine learning methods are used to enhance the performance of intrusion detection system in 5G/6G technologies. The devices are connected using access point in big distributed network in isolation environment. Therefore, attackers can target any of the hardware and software component resides in the globally distributed network including wireless channels, wireless end systems, access points and wired distribution network. It is very important to identify and resolve these problems to protect the whole system.

The main findings of the paper are:

1 We proposed a new model for detection of intrusion in 5G and beyond Network.

2 Our model is evaluated with the help of various machine learning techniques such as decision trees, linear regression, k-nearest neighbour, support vector machine, random forest and neural networks.

3 The performance of our model is evaluated by the metrics like recall, precision and f-measure.

4 The potential of our model has checked in three instances of datasets such as sth1-room, sth2-room and stch3-room developed by Silicon Valley campus of Carnegie Mellon University.[8–10]

Related Works

In the last few decades, there has been a continuous development in the communication network, starting from the 1G network and going towards 4G networks. The traffic of global network and communication has manifest tremendous growth in modern years and look forward to carry on, which activate the emergence of building new era of network called 5G. The 5G network overcomes the limitations of previous generation networks by increasing the scope and standards with large increase in the network

Table 1 — Classification of intrusion detection systems

Misuse detection System	**Specification-based systems**	**Anomaly-based systems**
	Advantages	
High detection rate	Efficient determination of correct behaviour	Detection unexpected attacks
Allow rule sharing	Detection of unpredicted actions	Able to detect zero day attacks
Low false alarm rates	Good for resource limited systems	
	Disadvantages	
Unable to detect new attacks	Specific for certain attacks	High false alarm rates
Unable to keep update	Unable to detect attacks that mimic the legitimate behaviour	Not good for complex and dynamic systems

capacity. The 5G network surpass the previous version of communication technology and able to provide different services as well as invigorate networking in different countries.[11] 5G networks also give solutions for cost-effective and efficient set-up for new services and adapt for different types of markets with various requirements. The development of 5G networks are imagined as starting of new application in different fields having large impact on every aspect of life, for example smart healthcare, vehicular networks, IOT, smart city, smart grid. The 5G and beyond network is capable of following possibilities:

(1) Gives up to 10 gbps of speed at end points and up to 20 gbps in certain situations.
(2) Gives ultra-low latency with less than 1ms.
(3) High mobility.
(4) Supports denser network and machine-type communication.
(5) Supports perception of 99.99% availability.
(6) Supports 100 x numbers of connected devices.

In order to get the above target, the 5G network uses various technologies such as Software-Defined Network (SDN), edge computing, cloud computing, Device-to-Device Communications, network slicing, millimetre wave communications.

Cloud Computing

The increasing demands of mobile sensing, data storage and resource management in recent years. The cloud computing takes the responsibility to fulfil these demands. More precisely, the cloud computing framework having resourceful computation centres works virtually can assist 5G services like sensing services, resource offloading, and network management in various applications areas.[12]

Edge Computing

It is called next to cloud computing. The edge computing appears to be encouraging technology to the potential of the 5G ecosystems. It supports various services to the mobile network edge with reference to the IOT devices, which favours storage services and computation with less transmission delays.[12]

Software Defined Network (SDN)

The SDN is used to smoothly run the 5G network with the help of software instead of hardware. It is also used to create the partition between data planes and control, which is further used to incorporate flexibility and swiftness in 5G networks.

Network Slicing

The 5G network is also used to provide facilities for the different networks for different applications called slicing. The use of SDN makes it possible for the applications to choose the network according to their requirement.

Device-to-Device Communications

It is useful for the IOT devices to make direct to each other for the communication instead of signal transmission. The data between different devices is transferred between mobile devices with the help of D2D, which maintains ultra-low latency between users. Further, it is also used to maintain flexibility between two users with respect to offloading traffic, decrease energy loss during long transmission, enhance spectral efficiency.[13]

Millimetre Wave Communication

This technology provides very high amount of spectrum for the 5G and beyond network to fulfil the demands of mobile devices. Also, it is used to provide narrow beam, huge bandwidth, high data access and improved transmission quality to resolve the problem of big growth in traffic volumes and high connected devices.[14] Above technologies are used as per the demand of heterogeneous devices attach to the network and varied applications from high traffic boom due to large interconnected devices.

Motivations

In 5G wireless environment, there is no fixed perimeter, therefore administrator unable to impose security strategy even with the presence of encryption and firewalls. This problem is added to the properties of the broadcasting channels, device mobility, extensive use of multi-domain applications, and limited number of wireless devices. In the 5G network, there is a possibility of some malware infected devices, others are either actively or passively hacking. Attackers only need to create vulnerability to attack the whole network. Therefore, the level of security in entire network is high as level of security in other points, everywhere it should be same. The wireless devices in the larger network are joined using isolated environment with the help of some access points. The hardware and software components of the network became very easy target for the cyber attackers as well as for the access points, wireless channels, wireless distribution networks and end systems. It is very challenging for the administrator to detect and resolve these attacks in order to prevent whole system.

Proposed Method

The block diagram for the intrusion detection system is depicted in Fig 1. The explanation of all three steps is described below

Step 1: The time-based multi-dimensional attributes are obtained from the dataset created by developed by Silicon Valley campus of Carnegie Mellon University. The datasets obtained is not perfect due to some measurement errors and noises for example choosing network from heterogeneous networks, mobility patterns and attributes from physical layer. The attributes which gives more information for intrusion detection system should be chosen first in order to obtain the efficient results. Moreover, the independent attributes have high estimation of accuracy rate and high distribution range provide more relevant information to discriminate between different transmitters. To take advantage of multi-dimensional information and attributes sharing between various networks and layers, the reliability of IDS will improved. Further, the design of efficient IDS depends only on estimated information of attributes and not on specific arrangement of time-based attributes.

Step 2: The combination of multi-dimensional attributes are very useful for IDS using machine learning methods. The dataset is captured from the room experiment took place on the Silicon Valley campus of Carnegie Mellon University in order to analyse the security of Zigbee-enabled smart homes. Based on the time-varying environment for network under the condition that limitation of uncertainties and resources happens, the attributes are collected to deal with both security management and communication overhead. However, the design of machine learning based IDS and important feature selection from the datas *et al.* so improves the detection performance. Therefore, cost-saving detection is obtained.

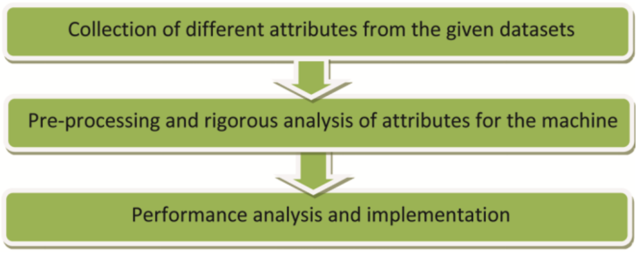
Collection of different attributes from the given datasets
Pre-processing and rigorous analysis of attributes for the machine
Performance analysis and implementation

Fig. 1 — Block diagram of proposed system

Step 3: The intrusion detection in 5G and beyond networks is conducted depends on the multi-dimensional attributes obtained from the datasets. The classification and regression based model are created depends on the train/test data obtained from datasets. After that performance of different machine learning methods have been evaluated and IDS can be applied to the time-based conditions to get the variations of different attributes. Therefore, efficient and effective process has been proposed for IDS in 5G and beyond network applications.

Experiment and Results

For the rigorous evaluation of our proposed method, we used two datasets such as sth2-room and stch3-room developed by Silicon Valley campus of Carnegie Mellon University[8–10], Th4 description of attributes of datasets is given in Table 2. These datasets were Captured Zigbee packets during the experiment where the third generation of the Smart Things Hub (IM6001-V3P01) and eight other devices were placed in a single room. The sth2-room, sth3-room experiment took place on the Silicon Valley campus of Carnegie Mellon University in order to analyse the security of Zigbee-enabled smart homes.[15] The sth2-room and sth3-room dataset contains total 88822 and 88323 fields respectively. We divided it into 15 sub datasets in order to get more rigorous simulation of the proposed method for IDS in 5G and beyond networks.

Table 2 — Description of attributes in datasets

Notation	Name	Type	Statistics		Description
			Min	Max	
A0	S.No.	Numeric	1	—	No. of attempts
A1	Time	Numeric	1	—	Connection length in sec
A2	Source	Octal	—	—	Source address
A3	Destination	Octal	—	—	Destination Address
A4	Protocol	Category	—	—	ZigBee/IEEE
A5	Length	Numeric	1	116	Length
A6	Info	Information	—	—	Packet Information

The proposed method is simulated in python 3.1.8 and runs in windows environment with configuration of I5 processor, 6 GB RAM. We applied our proposed method to the above datasets using without attribute selection method. We perform a study to compare six machine learning algorithms such as linear regression, decision trees, k-nearest neighbour, support vector machine, random forest and neural networks in the above datasets using n-cross validation rule. This rule overcomes the problem of over fitting in the classification process of supervised learning.

The proposed method used six machine learning methods for IDS in 5G and beyond networks. The performances of all machine learning methods using sth2-room and sth3-room datasets are depicted in Fig. 2 and Fig. 3. The graph in Fig 2 shows the results obtained from sth3-room dataset. The plot shows that linear regression is least performer and neural network is the best performer. The line graph of neural network shows the partition set 10 gives the maximum accuracy for IDS.

The results obtained from sth2-room dataset has shown in Fig. 3 in the form of a graph. The plot shows that linear regression is least performer and neural network is the best performer. The line graph of neural network shows the partition set 15 gives the maximum accuracy for IDS. We concluded from the Fig. 4 that the performance of our proposed method works well with neural network. It is also concluded from the fig 6 that the accuracy of our method with sth3-room is higher than the sth2-room dataset for IDS in 5G and beyond networks.

The performance of proposed method is also evaluated using sth3-room and sth2-room dataset in terms of f-measure, precision and recall in Figs 4, 5, 6. The performance of evaluation metric is also shown in the given plots. We conclude from the above Fig 6 that our proposed method is very accurate if there is sufficient data samples exist. Further, performance of sth3-room dataset with our proposed method is better than sth2-room dataset.

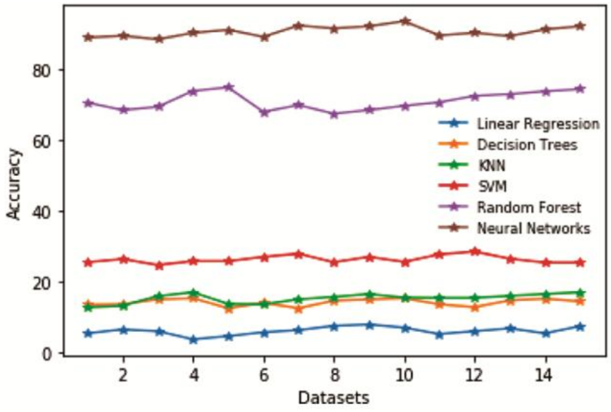

Fig. 2 — Accuracy comparison in sth3-room dataset

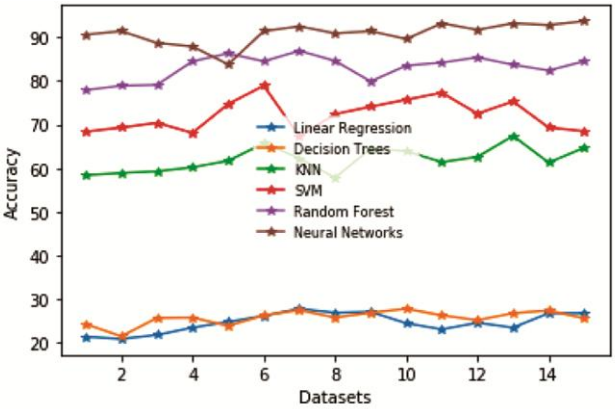

Fig. 3 — Accuracy comparison in sth2-room dataset

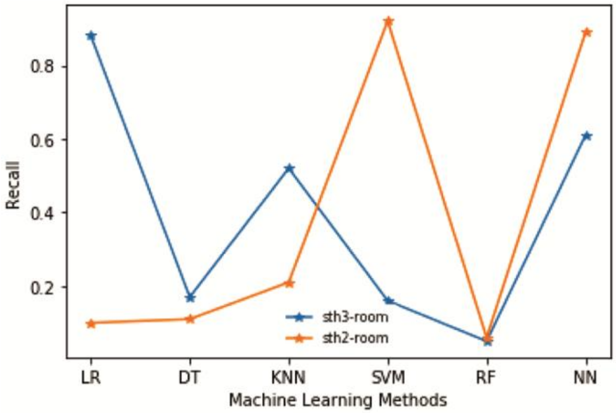

Fig. 4 — Average precision for all classification methods

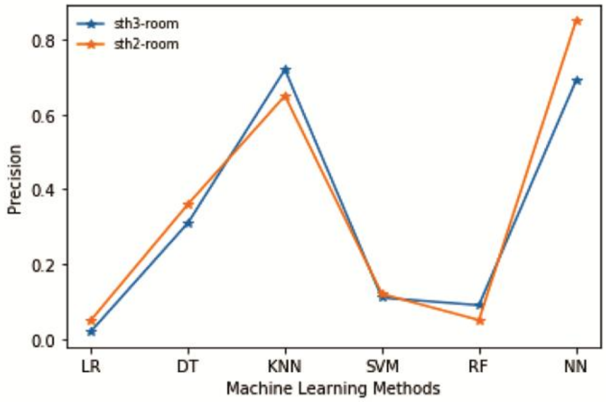

Fig. 5 — Average recall for all classification methods

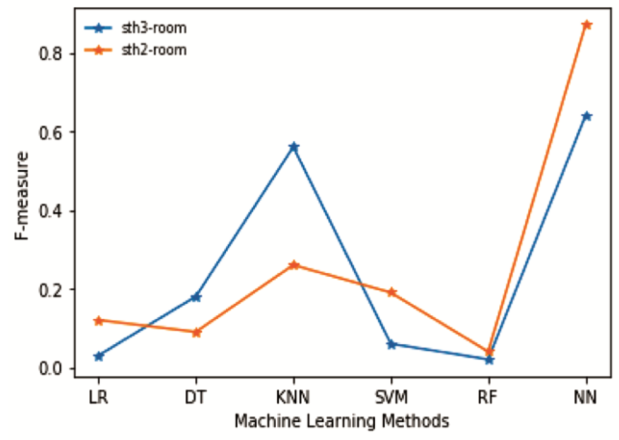

Fig. 6 — Average F-measure for all classification methods

Conclusions and Future Work

This paper introduced novel security technique for IDS in 5G and beyond network using two datasets such as sth2-room and stch3-room developed by Silicon Valley campus of Carnegie Mellon University. We tested our proposed method with machine learning methods like linear regression, decision trees, k-nearest neighbour, support vector machine, random forest and neural networks and found that it gives best result with neural networks. We have also tested it with metrics like recall, precision and f-measure. It is concluded from the experiment that the proposed method is efficient and effective to detect intrusion in 5G and beyond network. Results also showed the consistent performance of our method in all datasets. However, it is low with some other machine learning methods. In future, we incorporate some more machine learning methods and datasets also try to investigate the problems occurring during simulation of IDS with other datasets. It is very important for the researchers to make a critical assessment of the pattern found in improvement of accuracy of IDS in 5G and beyond network using machine learning techniques. The researchers during experiment keep in mind the variation in costliness, time, latency, and delay to develop model for IDS.

References

1 Jiang C, Zhang H, Ren Y, Han Z, Chen K C, Hanzo L, Machine Learning Paradigms for Next-Generation Wireless Networks, *IEEE Wirel Commun Mag*, **24(2)** (2018) 98–105.

2 Fang H, Wang X, Hanzo L, Learning-aided Physical Layer Authentication as an Intelligent Process, *IEEE Trans Commun*, **67(3)** (2019) 2260–2273.

3 Agiwal M, Roy A, Saxena N N, Next generation 5G wireless networks: A comprehensive survey, *IEEE Commun Surv Tutor*, **18(3)** (2016) 1617–1655.

4 Panwar N, Sharma S, Singh A K, A survey on 5G: The next generation of mobile communication, *Phys Commun-Amst* **18** (2016) 64–84.

5 Gupta A, Jha R K, A survey of 5G network: Architecture and emerging technologies, *IEEE Access*, **3** (2015) 1206–1232.

6 Chin W H, Fan Z, Haines R, Emerging technologies and research challenges for 5G wireless networks, *IEEE Wirel Commun*, **21(2)** (2014) 106–112.

7 Restuccia F, D'Oro S, Melodia T, Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking, *IEEE Internet Things J*, **5(6)** (2018) 4829–4842.

8 Akestoridis D G, Harishankar M, Weber M, Tague P, Zigator: Analyzing the Security of Zigbee-Enabled Smart Homes, *WiSec '20: Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, (*2020) 77–88.

9 Alliance Z (2015) Zig Bee Specification. ZigBee Document, 05-3474-21.

10 Alliance Z (2016) Base Device Behavior Specification. ZigBee Document, 13-0402-13.

11 Andrews J G, Buzzi S, Choi W, Hanly S V, Lozano A, Soong A C, Zhang J C, What will 5G be?, *IEEE J Sel Areas Commun*, **32(6)** (2014) 1065–1082.

12 Khan A N, Kiah M M, Khan S U, Madani S A, Towards secure mobile cloud computing: A survey, *Future Gener Comp Sy*, **29(5)** (2013) 1278–1299.

13 Kar U N, Sanyal D K, An overview of device-to-device communication in cellular networks, *ICT Express*, **4(4)**, 2017.

14 Wang X, Kong L, Kong F, Qiu F, Xia M, Arnon S, Chen G, Millimeter wave communication: A Comprehensive Survey, *IEEE Commun Surv Tutor*, **20(3)** (2018) 1616–1653.

15 Akestoridis D G, Harishankar M, Weber M, Tague P, CRAWDAD dataset cmu/zigbee-smarthome (v. 2020-05-26), downloaded from https://crawdad.org/cmu/zigbee-smarthome/ 20200526, May 2020.