Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Deep Learning Model For Predicting Context Information For Authentication

Amit Jaykumar Chinchawade[1*] , Onkar Singh Lamba[2]

[1,2]Department of Electronics & Communication, Suresh Gyan Vihar University, Jaipur, India.

Abstract: Authenticating devices in a network with a large number of them is a difficult task. A huge number of data generating and data collecting devices may be connected in the internet of things (IoE). The authentication of each device is critical in a network with so many devices. The user equipment can be connected to the network via a fixed cable or wireless connection. The challenge of identifying such equipment or devices is difficult. Based on device address authentication is a crucial stage in every form of network that is practically familiar to every attacker approach and thus susceptible to being duplicated. With the periodic authentication system suggested in this research, duplication of devices that can steal crucial data can be avoided. This study presents a strategy based on the context of the user's equipment. The distance between the device and the connecting media affects the device's channel impulse response. The device's physical location and channel impulse response can be mathematically modelled and used as authentication context information. The experimental setup with deep learning-based channel impulse response prediction achieves excellent results in identifying the original device in a network emulation tool.

Keywords: IoE, Device authentication, Deep learning, Context information, channel impulse response.

1. Introduction

A large number of devices are connected through the internet in the Internet of Everything (IoE). Some equipment are in charge of producing data, which is then transferred to data collection devices or servers. User authentication is based on passwords and log in ids, and end device authentication is based on device address information when accessing the network. Continuous authentication may be required to prevent devices in networks from replicating each other. The use of traditional log in credentials for device identification is a typical solution, however it is vulnerable to attacks using various tactics such as brute force attacks. Continual authentication processes may help to avoid such issues.

5G technology is ushering in a new era of wireless communication [1]. Due to the development of ubiquitous computing, users can be connected to many wireless access technologies at the same time. Compatibility for Virtual Private Networks (VPNs), Wireless World Wide Web (WWWWW) support, and flat IP are all key elements of 5G. The use of flat IP allows devices to be identified using symbolic names, making 5G suitable for a variety of technologies. Because flat IP is used, the number of elements in the data stream is minimised. As a result, capital expenditures (Cap Ex) and operational expenditures (Op Ex) are minimal [2-3].

All of these advantages come with the risk that 5G may present new issues in terms of security and privacy [4]. Despite these obstacles, 5G will support a wide range of applications, including vehicle-to-vehicle and vehicle-to-infrastructure communications, smart cities, industrial automation, smart homes, health services, and many others [5]. Support for new industry applications, as well as traditional voice and data communication, as well as a diverse variety of devices and apps to connect the entire society [6]. 5G wireless services will improve mobile broadband connectivity by supporting IoT [7-8] and vital services. Because of the vast range of applications that 5G supports, it is the most promising technology for meeting today's market demands.

Wireless network virtualization (WNV) is the most promising technology for meeting future internet demands, according to Future Internet. WNV is being actively used in Internet research test beds. The infrastructure must be isolated from the services it provides for ultra-dense 5G networks with massive wireless traffic and service requirements. Allowing varied services to share the same underlying infrastructure can increase network utilisation. WNV can enable new products and technologies with legacy products by isolating a portion of the network. The growing number of heterogeneous wireless networks need a more robust network management system. Wireless network virtualization is required to do this [9-12].

The processing of information such as device context information may be used to establish the continuous authentication process. The device's location and channel characteristics are one-of-a-kind and cannot be duplicated in any way. There are a variety of context-based approaches available these days, but the most effective procedure in terms of processing complexity and latency in device authentication procedures can be evaluated. Furthermore, the authentication methods may increase network overhead, lowering end-to-end system performance [13].

This paper focuses on development of channel impulse response prediction model using deep learning approach for authentication of user equipment’s. The device authentication in hybrid network which constitutes wired and wireless devices in the network is implemented using emulation tool and performance is evaluated. The proposed work section provides the network composition and proposed deep learning model for authentication scheme. The results and analysis section provides the details of performance of proposed scheme [14].

2. Proposed work

The channel-based transmitter-to-receiver communication is influenced by a number of factors. It's crucial to know where the receiver and transmitter are in order to calculate the channel's impact on each bit of communication. The influence of a channel is determined by factors such as fading, noise addition, channel impulse response, and communication frequency interference. The verification strategy for these attributes can be used to construct an authentication strategy. To provide security and privacy, authentication is essential when transmitter to receiver communication is to be established. The network should not be burdened by this process. The performance of bandwidth usage and network resource use should not deteriorate. This can be accomplished through the use of a quick authentication approach, which will be discussed further.

Let X be the vector of contextual information, which contains channel impulse response vectors such as, x_1, x_2, …, x_n.

$$X = \begin{matrix} x_{11} & \dots & x_{1n} \\ x_{21} & \dots & x_{2n} \\ x_{31} & \dots & x_{3n} \end{matrix}$$

(1)

In this method, we estimate the channel impulse response for a multipath fading channel that varies in time and distance. Let X'(t,) be the practical channel impulse response. Where t is a time-varying signal caused by equipment motion, and denotes multipath delays. Let x(t) and y(t) be the fixed coordinates functions used to estimate the stored channel impulse response at each device t. The X' is calculated at the UE and relayed to the base station in a packet along with the location for authentication.

When authentication process is required, base station equipment can calculate the impulse response using x(t) and y(t) from the database and location sent by the UE. The vector X obtained as in equation (1) is then compared with received vector X'.

Where,

$$X' = \begin{matrix} x'_{11} & \dots & x_{\prime 1n} \\ x'_{21} & \dots & x_{\prime 2n} \\ x'_{31} & \dots & x'_{3n} \end{matrix}$$

Let, ΔX be the difference between the calculated and received vectors given as,

ΔX= X-X'

(2)

In case of normal environmental conditions, the channel impulse response varies randomly up to certain limit compared to calculated values using sent and received data. Let Th be the threshold allowed to compensate tolerance of the difference between calculated impulse response and received impulse response in normal environmental conditions. By comparing ΔX with Th two conditions are possible,

If ΔX <Th then UE is authenticated, else not authenticated.

3. CRC based UE authentication

Until now, 3G or LTE-based networks have used the Cyclic Redundancy Check to address security vulnerabilities by using message authentication. For CRC encoding and decoding, the Linear Feedback Shift Register with g(x) as a connection polynomial has been efficiently constructed. Traditional CRCs are used to detect random errors, with the drawback that they do not provide a strong mechanism for malicious advice.

we first fix the polynomial multiplier in generator polynomial, to bring the randomness, by using channel impulse response vector as shown in equation (3). The message polynomial is multiplied by x^n and divided by generator polynomial g(x).

$g(x) = x^3+x+1$

…(3)

By considering polynomial in (3) code word is calculated as,

$r(x) = M(x).\ x^n \bmod g(x)$

$c(x) = M(x) + r(x)$

… (4)

Where, r(x) is remainder, M(x) is message, and c(x) is codeword.

4. Proposed approach of authenticating UE

Selecting fixed generator polynomial, leads to easy identification of the code words for the attackers. Hence we keep the generator polynomial as random as possible to make it difficult to guess for the attacker. Hence g(x) can be given as,

$g(x)= (x^3+x+1) \cdot X'$

… (5)

Where, X' is impulse response vector used for generator polynomial.

The algorithm of proposed system is as detailed further.

Calculation of the impulse response procedure is necessary for the first time.

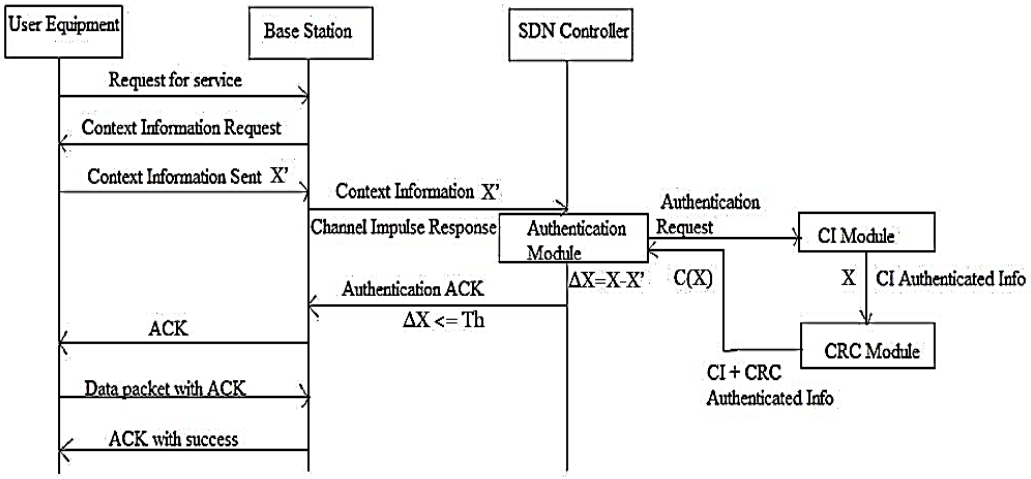

Figure 1: Communication process for authentication

With verified labeled dataset, neural network-based congestion event prediction model is proposed. The proposed authentic node detection model is shown in figure in which multiple neural network models are compared based on performance of predicting the congestion event. Figure 2 shows the congestion detection work proposed in this paper.

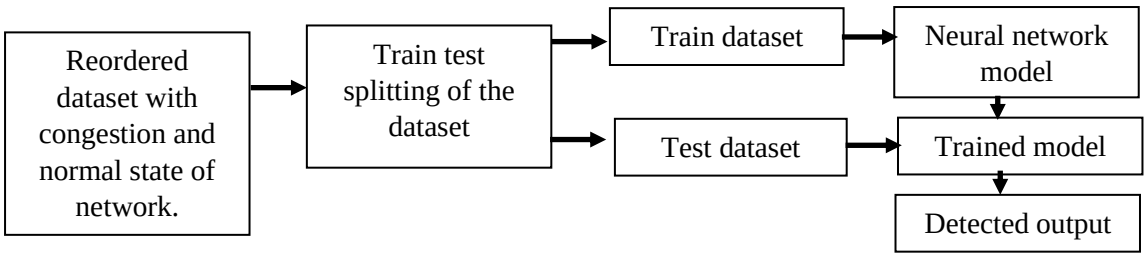

Figure 2: Proposed neural network work flow

The neural network models used for the experimentation are, recurrent neural network models developed with the use of LSTM and GRU based model is configured as shown in table 1.

Table 1: Proposed Neural Network Layer Model configuration

Layer	Output Shape	Parameters
Gru (LSTM)	(None,1,7)	70656
Dropout	(None,1,128)	0
lstm_1(LSTM)	(None,64)	8256
Dropout_1	(None,64)	0
Dense_1	(None,2)	130
Total Parameters:	8256	
Trainable Parameters	210,626	
Non-trainable Parameters	0	

The malicious node is identified based on true or false event prediction. To avoid the congestion state, an adaptive window management approach is also implemented. Unauthentic nodes are predicted for every packet transmitted and received, which does not need network communication of control packets, but network congestion condition is predicted to determine the window size.

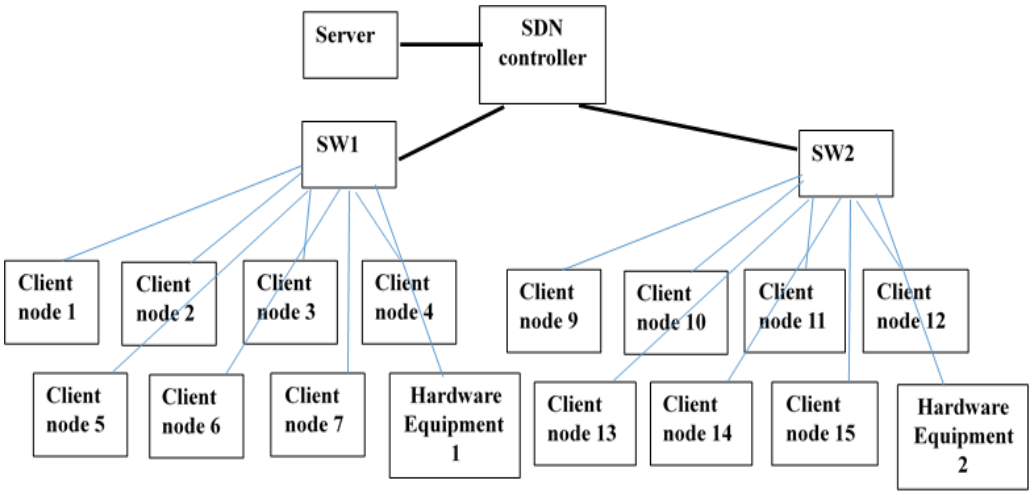

Figure 3: Proposed System and Experimental Setup

5. Result

The experiments are conducted using Mininet, an open flow modelling tool, with nodes installed as shown in Figure 3. The Mininet allows real and virtual nodes to be implemented in the network by using multiple instances of network interface cards. The Raspberry Pi board is also connected to the network via an external Wi Fi interface, which is validated via an Ethernet switch and router. The results of the performance evaluation for SVM prediction are shown in Table 2.

Table 2: Performance Evaluation for Prediction using SVM

Number of attempts of authentication	Number of authenticated Detected Correctly	Number of attempts authentication Detected Incorrectly	Accuracy
103	99	4	96.11%
111	107	4	96.39%
120	115	5	95.83%
150	141	9	94.23%
Total:			**95.28%**

For this work true positive, true negative, false positive and false negative annotations are used for analysis. Results are shown in figures 4 and 5 respectively.

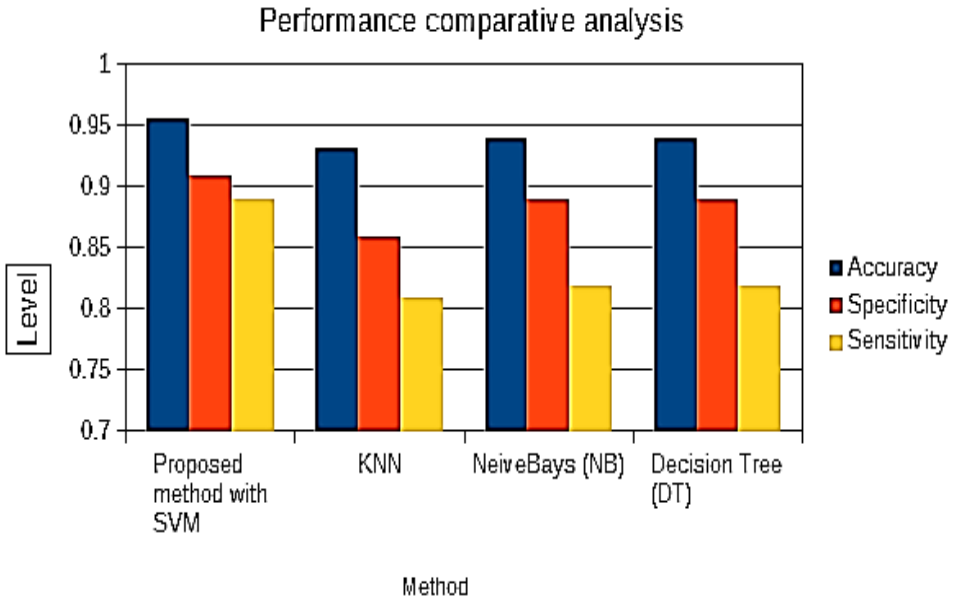

Figure 4: Performance of Machine Learning Conventional Classifiers

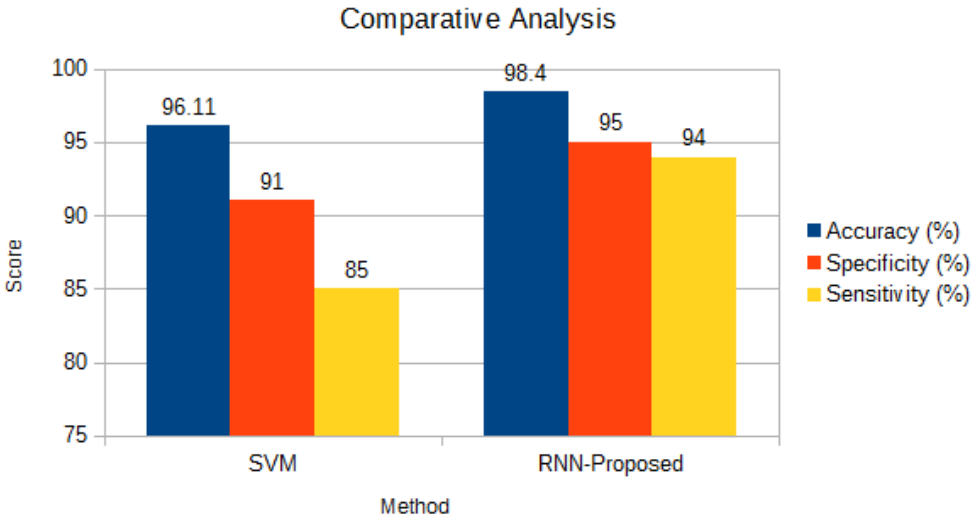

Figure 5: Performance Comparison of the authentication prediction

The suggested system, which employs an RNN-based model, can reliably anticipate device context information, such as channel impulse response, and authenticate the device. For authenticating the device, which is hardware equipment connected to the network, the accuracy is around 98.4 percent.

6. Conclusions

In IoE, channel characteristics vary in accordance with allocation factors based on spectrum characteristics. The allocated channel to UE is required to be authenticated for every time UE interacts with BS. This paper shows a novel approach for authentication using context information of channel for allocated for UE. In generalized scenarios, there are limitations of authentication using CRC based approach with fixed generator polynomial and hence random

generator polynomial can provide solution to the challenge. The combination of CI and CRC approaches along with sufficient randomness in generator polynomial along with less complexity in computation can provide greater security level compared each in individual case. Due to this, probability of prediction of generator polynomial is quiet less and depends on actual location of the user equipment thereby increasing robustness and reliability of the authentication scheme. Channel characteristics in the Internet of Things vary according to allocation parameters based on spectrum characteristics. Every time UE communicates with BS, the allocated channel to UE must be verified. This paper demonstrates a As a result, the likelihood of predicting the generator polynomial is much lower and is dependent on the real location of the user equipment, boosting the authentication scheme's robustness and dependability. When compared to individual CI and CRC based approaches, the results indicate improved security and low amounts of added latency, indicating a path for practical implementation viability.

References:

[1] N. Panwar, S. Sharma and A. K. Singh, "A Suvery on 5G: The Next Generation of Mobile Communication", Physical Communication, vol. 18, no. 2, pp. 64-84, 2016.
[2] "5G Vision", 5G PPP, February, 2015.
[3] "Understanding 5G: Perspectives on future technological advancements in mobile", GSMA Intelligence, December, 2014.
[4] "5G Security: Forward Thinking Huawei White Paper", HUAWEI WHITE PAPER, 2015.
[5] "The Road to 5G: Drivers, Applications, Requirements and Technical Development", GSA, November, 2015.
[6] "5G SECURITY", ERICSSON WHITE PAPER, June, 2015.
[7] "Leading the world to 5G", QUALCOMM, February, 2016.
[8] J. G. Andrews et al., "What Will 5G Be?", IEEE Journal on Selected Areas in Communications, vol. 32, no. 6, pp. 1065-1082, 2014.
[9] H. Wen. P. K. Tiwary, and L.-N. Tho, "Current trends and perspectives in wireless virtualization," in Proc. Int. Conf. Sel. Topics Mo W Net, Montreal, Canada, Aug. 2013, pp. 62-67.
[10] EDVIN J. KITINDI, SHU FU, YUNJIAN JIA, (Member, IEEE), ASIF KABIR, AND YING WANG "Wireless Network Virtualization With SDN and C-RAN for 5G Networks: Requirements, Opportunities, and Challenges" Digital Object Identifier 10.1109/ACCESS.2017.2744672, IEEE 2017.
[11] Open Networking Foundation, "Onf white paper: Software-defined networking: The new norm for networks," Palo Alto, CA, USA, 2012, Tech. Rep.
[12] N. Mc Keownet al., "Open flow: Enabling innovation in campus networks," SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69-74, Apr. 2008.
[13] Fang, Y. Qian and Rose Hu, "Security for 5G Mobile Wireless Networks" DOI 10.1109/ACCESS.2017.2779146, IEEE Access.

[14] N. Xie and S. Zhang, “Blind Authentication at the Physical Layer under Time-Varying Fading Channels” DOI 10.1109/JSAC.2018.2824583, IEEE Journal on Selected Areas in Communications.