Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

Improving the state of materials in cybersecurity attack detection in 5G wireless systems using machine learning

S. Sumathy [a], M. Revathy [b], R. Manikandan [c,*]

[a] Assistant Professor & Head, Department of Computer Science, Sir Theagaraya College(Shift II), Chennai, India
[b] Assistant Professor, Department of Computer Science, Sir Theagaraya College(Shift II), Chennai, India
[c] Academic Co-Ordinator & Head, Dept. of Computer Science, The Quaide Milleth College, Chennai, India

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Internet of Things (IoT)
5G
Machine learning
Physical layer

ABSTRACT

The utilization of information from the radio channel is useful in detecting the spoofing attacksin 5G wireless communications. This concept has been used for a wide range of uses for the Internet of Things (IoT) environment by users and their IoT devices. But how these tasks can minimise the effects of cyber threats in genuinely complex networks has not yet been sufficiently addressed. These are seriously exposed, as is the case with 5G broadband networks due to a wide variety of technology at various abstract stages. As 5G IoT is the 5G environment, including the IoT background, in this article, we are an artificial intelligence (AI) intended to minimise the impact of 5G IoT threats, when extended to the participants involved on a number of levels.This paper uses Support Vector Machine (SVM) based PHY-layer authentication algorithm to detect the possible security attacks in 5G wireless communication at physical layer. It is utilized in increasing the rate of authentication with test features. The detection rate is improved further with test statistic features. The model is implemented on multiple-input multiple-output (MIMO) channel. The simulation results shows that the proposed method yield the high detection rate on all attacks.

Selection and peer-review under responsibility of the scientific committee of the International Virtual Conference on Sustainable Materials (IVCSM-2k20).

1. Introduction

The fifth generation (5G) delivers high bandwidth, high performance and security standards in 3 common scenarios: enhanced mobile connectivity, wide-scale stuff web and low-latency connections [1 2]. The special situation for mobile broadband and high-frequency, is used in indoor or urban environments in which wide-ranging mobile network signals are continuously secured in rural areas. Meantime, the 5G calls for a large range of devices and installations to be integrated, and this is an integral necessity for IoT service[3]. Manual portable devices join a cellular network, which ensures that wireless authentication is also heavily employed. Therefore, lightweight networking approaches for intensive deployment scenarios of 5G networks.

Cybersecurity represents a set of systems and techniques intended for the avoidance, alteration or destruction of attacks and unwanted access, networks, programming and documents. A safety network framework includes a network security and control mechanism. Both computers are firewalls, antivirus and intrusion detection systems (IDS). The risks to the protection of IT networks depends on a lack of confidentiality, completeness and access. The right of unauthorised users to keep information private is in particular a matter of secrecy which ensures that the data disclosure can lead to loss of confidential care. Integrity to ensure the confidentiality of the information or resources leading to disappointment attacks where it is not maintained. In this scenario, records or documents, and lack of data, can be changed. Flexibility assures the functioning of a system at the end of the day which can be controlled on request; hence, operational negation can occur where system availability is not guaranteed.

For physical layer authentication, many approaches are recommended.The channel impulse response (CIR) and received signal strength indicator (RSSI) are found in [3-8] with channel state information (CSI), while wireless network attacks. The method in [9] offers a PHY-authentication to adjust the multicarrier transmission. In methods [10-12] analysed channel spatial decorrelation characteristics by comparing two or more frame channels and

[*] Corresponding author.
E-mail address: manisankar27@gmail.com (R. Manikandan).

https://doi.org/10.1016/j.matpr.2021.04.171
2214-7853/© 2021 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the International Virtual Conference on Sustainable Materials (IVCSM-2k20).

Please cite this article as: S. Sumathy, M. Revathy and R. Manikandan, Improving the state of materials in cybersecurity attack detection in 5G wireless systems using machine learning, Materials Today: Proceedings, https://doi.org/10.1016/j.matpr.2021.04.171

validated the channel authentication efficiency to identify spoofing within the MIMO system.In these methods, artificial intelligence (AI) thresholding is necessary to detect spoofing attacks. Currently it is not possible to verify the threshold range accurately with low precision.

The major contributions of this paper are summarized as follows:

- The authors use artificial intelligence (AI) intended to minimise the impact of 5G IoT threats, when extended to the participants involved on a number of levels.
- This paper uses Support Vector Machine (SVM) based PHY-layer authentication algorithm to detect the possible security attacks in 5G wireless communication at physical layer.
- It is utilized in increasing the rate of authentication with test features. The detection rate is improved further with test statistic features.
- The model is implemented on multiple-input multiple-output (MIMO) channel.

2. System model

In this section, we use detection model for spoofing attack in the physical layer.

As seen in Fig. 1, a MIMO-system is analysed using legal transmitter-spoof node-receiver model, where Legal transmitter and Spoof node are legitimate N_T and N_R antennas. Receiver manages to spoof Legal transmitter into her persona with antennas. Their place is expected to be spatially isolated. Spoof node tracks the peculiar existence of wireless reactions to distinguish between legal transmitter signals and illegal receiver signals in order to counter this spoofing identification. This is an authentication of the physical layer. The precise authentication procedure for the physical layer shall be as follows: signals are sent to the recipient through the wireless multipath channel using pilots for estimation of the channel response of transmitter. The data transfer requires N-frames and each frame is made up of OFDM symbols.Fig. 2.

Overall, if the cumulative number of user accounts is fewer, the recommendation list would not be affected. In the other hand, once the total number of user accounts is high, the recommendation list is significantly updated. In spite of this, the attack profiles that influence the list of recommendations are kept and vice versa. In order for the reduction of false positive rate (FPR) of these data, a spoofing attack identification system is proposed. This is a two-step framework where the initial phase senses the attack profile and the attack profile collection, and in the final phase the profile review, the objects are subject to possible attacks. It uses rough identification technique and the latter refines the objects to delete actual profiles from the set of an attack profile. The decline in the incidence of false positives is important.This section addresses the category properties of the SVM classifier. In its initial phase, the two stage techniques use a pruning model to solve the uneven class problem during the SVM classification process. This process produces a fine tuning effect and in the final phase the target persons in the attack profile are evaluated.

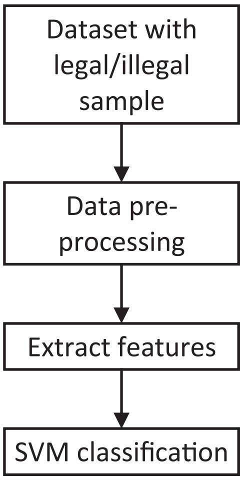


Fig. 1. Authentication with SVM(a) 1% spoofing attack with varying training data size (b) 3% attack with varying training data size (c) 5% spoofing attack with training data size (d) 7% spoofing attack with training data size.

The whole process at the receiver has three elements. The initial component follows the attributes extraction using a ranking matrix that ranks the extracted attributes. The goal of SVM is to identify the ideal division between hyper-plane and two groups. This improves the division of the attack from actual groups. If the sample data points are not linearlydivided, then in its input sample space the data points belong to two different groups.

In order to resolve the problems of non-linearity among the classes, the study transforms the data points through nonlinear mapping $\varphi(x)$ into high dimensional space. The N point(x_i) in the dataset with the data label $y_i$is resolved using SVM that results in an optimization problem.

$$\min_{w,b,\xi_i} 0.5w^T w + c\sum_{i=1}^{N}\xi_i \tag{1}$$

s.t. $y_i\left(w^T\phi(x)+b\right) \geqslant 1-\xi_i$ (2)

$i = 1, 2, \ldots N$

$\xi_i$is the positive variables

c is considered as the tradeoff between complexity and training error. Further, SVM optimization problem is resolved using the following expression,

$$\min_{\alpha} 0.5\sum_{i=1}^{N}\sum_{j=1}^{N} y_i y_j K(x_i, x_j)\alpha_i\alpha_j - \sum_{j=1}^{N}\alpha_i 0 \leqslant \alpha_i \leqslant C \tag{3}$$

$$\text{s.t.} \quad \sum\nolimits_{j=1}^{N}\alpha_i y_i = 0 \tag{4}$$

where, K is considered as the kernel vector

$$K(x_i,x_j) = <\varphi(x_i),\ \varphi(x_j)> \tag{5}$$

<$\varphi(x_i)$, $\varphi(x_j)$ > is the dot product between x and y.

Finally, for a data point x , thepredicted class is formulated as:

$$sign \quad \sum_{j=1}^{N}\alpha_i y_i K(x, x_i) + b\Big) \tag{6}$$

By removing the irrelevant support vectors, the data points about to get attacked are removed via SVM. Increased separation cap by SVM is used to detect irrelevant data points of the attack profile. The precision boundary points in SVM are established according to the genuine feature set and the assault profile. Therefore, the data points of their respective groups are said to be deeper. The insignificant points have no impact on the border between the hyperplanes.

The hyper plane separation prefers to see data points lying on the opposite side if they are linearly splitting between two distinct groups. Thus, hyperplanes are defined by points near the hyperplanes boundary. The lengths from the frontier are considered trivial and can be omitted from the grades. Furthermore, if on linear separation of training data samples a minimal tension is created, points from both groups cross tree edges from both sides. The insignificant points are then discarded with remainder for the preparation of the SVM classification.

By considering points on neighbourhood boundaries, SVM raises the classification rate. Thus, the class boundaries has to be improved, and the cumulative number of neighbours is thus expanded. Algorithm 1 displays the proposed SVM model.

Algorithm 1: SVM

```
Input: Relevant Points ($RP$), testing set ($T$), Adjacent Points ($AP$), Data Points ($DP$), minimum spanning tree ($tree$) and Parameter ($P$)
Output: accuracy
Create the initial folds using $t_i$-$T_i$
Create the second fold $t_i$ using $t_{ij}$ -$T_{ij}$
For $i$ = 1:10 do
    For $j$ = 1:10 do
        $MST_{ij}$ = Build $tree$ on $t_{ij}$
        $RP_{ij}$ = $DP$ in $tree_{ij}$ of different classes
        For$p$ = 1 : level do
            $AP$ = $DP$ $adjacent$ to $RP_{ij}$
            $RP_{ij} = RP_{ij} \cup AP$
        Endfor
        For all combinations do
            $SVM_{ij}$ = Train $SVM$ on $t_{ij}$
            $SVM\_TP_{ij}$ = Test $T_{ij}$ through $SVM_{ij}$
            $SVM_{ij}$ = Train SVM on $RP_{ij}$
            $SVM\_TP_{ij}$ = Test $t_{ij}$ through $SVM_{ij}$
        Endfor
    Endfor
    SVM_$P_i$ = argmax($SVM\_TP_{ij}$)
    $SVM\_P_i$ = argmax($SVM\_TP_{ij}$)
    $MST_i$ = Build $tree$ on $t_i$
    $RP_i$ = adjacent$DP$in $tree_i$ of various classes
    For$p$ = 1 to neighboring level do
        $AP$ = $DP$ adjacentto $RP_i$
        $RP_i = RP_i \cup AP$
    Endfor
    $SVM_i$ = Train $SVM$ with $SVM\_P_i$on $t_i$
    $SVM_i$ = Train $SVM$ with $SVM\_P_i$on $RP_i$
Endfor
```

3. Results and discussions

The spoofing attack detection is enable at the receiver with a legal transmitter and a spoof node considered for simulation purpose. A rectangular cross-sectional area is used for the simulation which is placed with many user friendly wireless device like mobile phone, desktop and printers. The rectangular cross-sectional area is built with refraction and scattering phenomenon to induce interference in wireless channel between the legal transmitter and legal receiver. The experiments are conducted in indoor and outdoor environment, while the implementation is carried out on USRP. The simulation takes into account 2 × 2 MIMO antennas for transmission and 8 × 8 MIMO antennas for reception. The spoofing node is then equipped with 2 × 2 MIMO antennas. The center frequency is maintained at 3.8 GHz, which is send over two antennas of bandwidth 2 MHz. The entire experimental is conducted in Matlab environment with the plots generated with excel interface.

During simulation, the following steps are amended:

The receiver is allowed to extraction the channel state information from the legal transmitter and spoofing node using conventional channel estimation mechanism.
The receiver is allowed to pre-process the datasets within its threshold level i.e. [0,1] normalisation
Training dataset is generated at the receiver end for the purpose of classification
Train the receiver to strengthen the SVM classifier using training dataset.
Finally, test the receiver with testing dataset
Obtain the detection rate of receiver authentication

The proposed SVM authentication model over 5G systems is evaluated using three different metrics that includes accuracy, recall and false positive rate.

The recall is the ratio of total attack profiles detected with overall attack profiles in 5G systems.

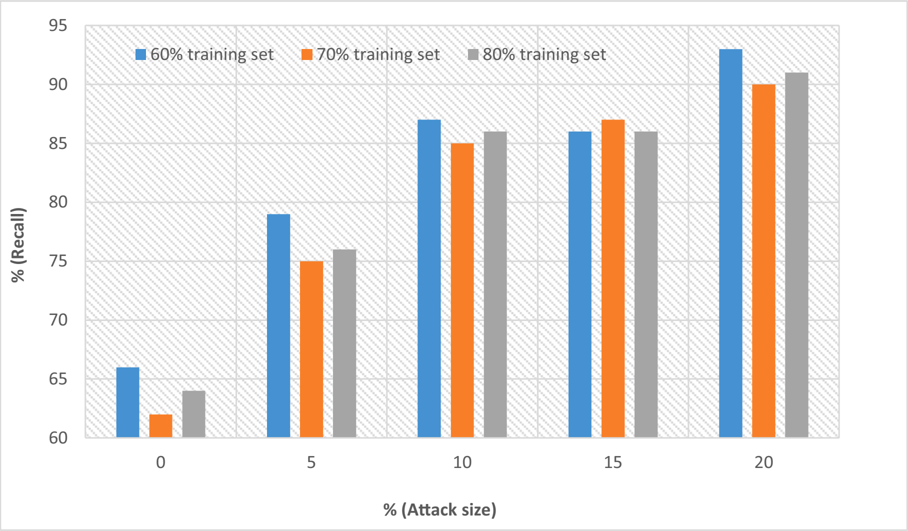
$$\text{Recall} = \frac{no\ of\ TP}{no\ of\ TP + FN} \tag{11}$$

The FPR is the ratio of false positive instances with total attacks in 5G systems.

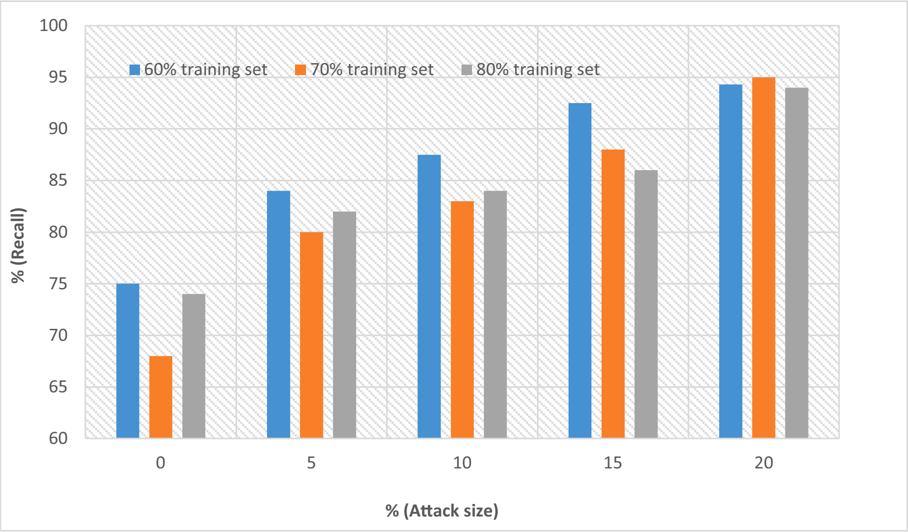
$$FPR = \frac{no\ of\ FP}{no\ of\ TP} \tag{13}$$

The SVM identification rate for spoofing attacks is discussed in this section. The efficiency is checked by adjusting the dataset and the attack scale against two separate studies. By choosing 200 genuine profiles from the data collection, which are deemed to be genuine instances, the training set is created changed. Several assaults, which involves average attack, random assault and section attack, build the attack profile samples. A significant number of legitimate profiles and attacks are retained in the training data collection. This is achieved generally by the development of acceptable attack profiles of different attack sizes. The detection results are determined about 20 times by running the detection process and the average value of the results is finally noted. The identification items are generated randomly when the attack profile is generated. Fig. 3 indicates the retrieval rate of the detested attack model by means of the proposed detection model. But the attack size is identical. With increasing dataset size, the reminder value increases.

Fig. 3 displays the FPR of the attack-model with various attack and training data sizes using the suggested detection model. The FPR gates may be inferred that collapse as the attack size increases. Therefore, with increasing attack sizes the reliability of the FPR is decreased. Furthermore, the false positive probability reduces when the attack scale is the same, as the training data increases. It was finished that with a limited number of attack profiles the false positive identification rate using the proposed approach was high.

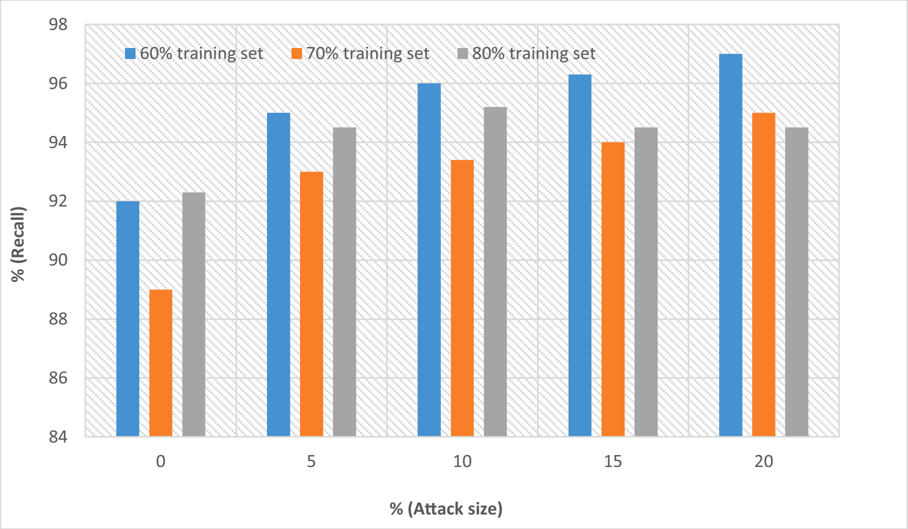


(a) 1% spoofing attack with varying training data size

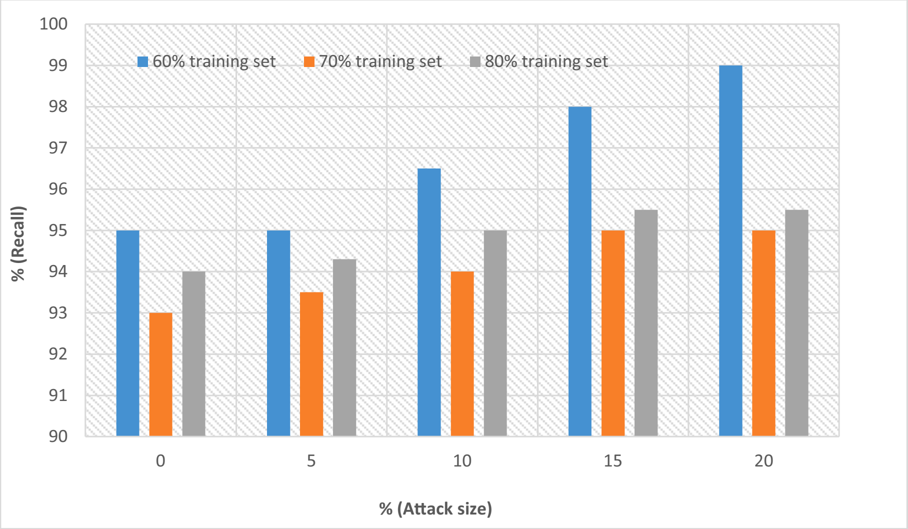


(b) 3% attack with varying training data size

Fig. 2. Detection rate of SVM Authentication model at the receiver end (a) 1% spoofing attack with training data sizes (b) 3% spoofing attack with training data sizes (c) 5% spoofing attack with training data sizes (d) 7% spoofing attack with training data sizes.

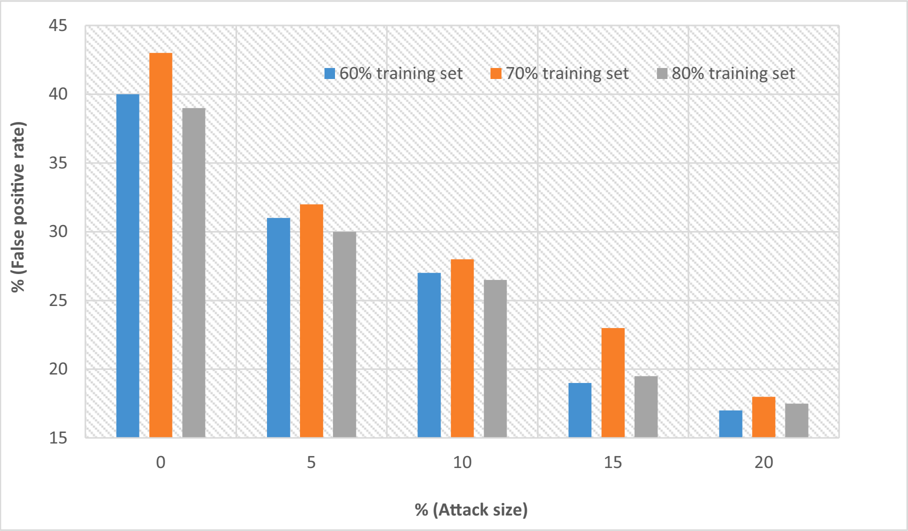


(c) 5% spoofing attack with training data size

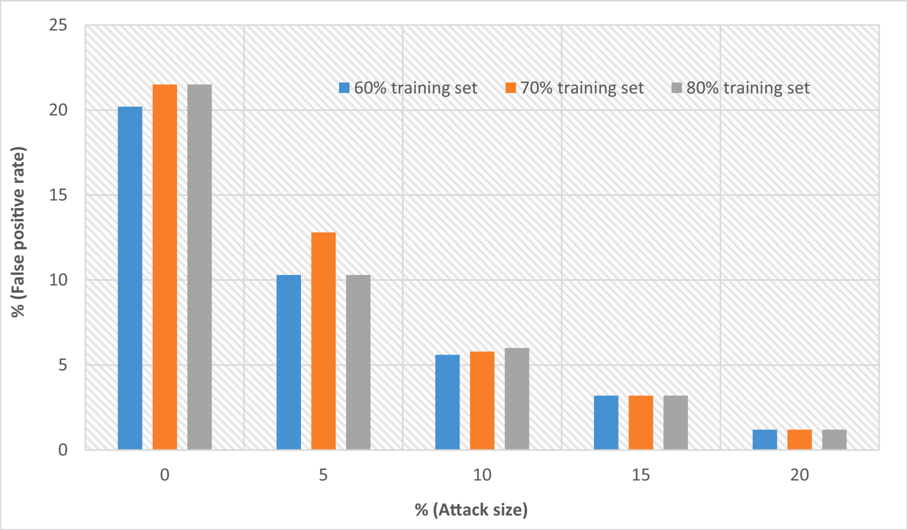


(d) 7% spoofing attack with training data size

Fig. 2 (*continued*)

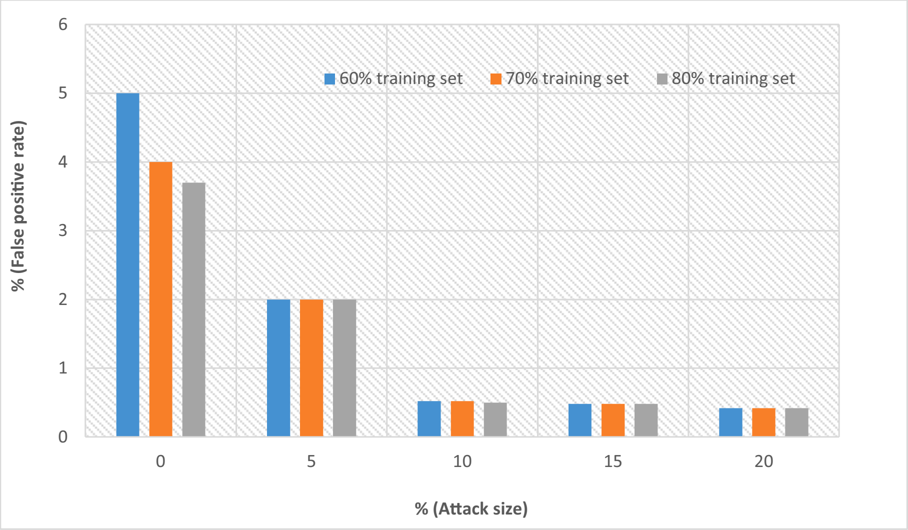


(a) 1% spoofing attack with training data sizes

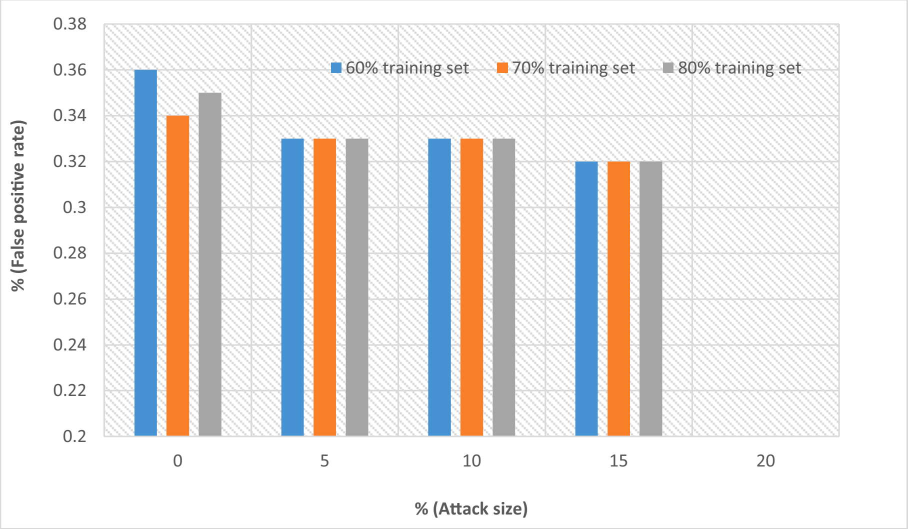


(b) 3% spoofing attack with training data sizes

Fig. 3. FPR of SVM Authentication model at the receiver end.



(c) 5% spoofing attack with training data sizes



(d) 7% spoofing attack with training data sizes

Fig. 3 (*continued*)

4. Conclusions

In this paper, we use SVM based PHY-layer authentication algorithm to detect the possible security attacks in 5G wireless communication. It is utilized at the physical layer to increase the authentication rate with test features. The detection rate at the receiver is improved further with test statistic features. The model is implemented on MIMO channel. The simulation results shows that the proposed method yield the high performance with improved detection rate.

CRediT authorship contribution statement

S. Sumathy: Workdone by Author. **M. Revathy:** Introduction, Collection of literature, Material properties, Testing, Test result comparison. **R. Manikandan:** Conclusion.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] J. Thompson, X. Ge, H.-C. Wu, R. Irmer, H. Jiang, G. Fettweis, S. Alamouti, 5G wireless communication systems: Prospects and challenges [Guest Editorial], IEEE Commun. Mag. 52 (2) (2014) 62–64.

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

[3] M. Demirbas and Y. Song, “An RSSI-based scheme for sybil attack detection in wireless sensor networks,” in Proceedings of the WoWMoM 2006: 2006 International Symposium on a World of Wireless, Mobile Multimed. Networ., pp. 564–568, June 2006.

[4] M. Demirbas and Y. Song, ‘‘An RSSI-based scheme for sybil attack detection in wireless sensor networks,” in Proceedings of the WoWMoM 2006: 2006 International Symposium on a World of Wireless, Mobile Multimed. Network., pp. 564–568, June 2006.

[5] D. B. Faria and D. R. Cheriton, ‘‘Detecting identity-based attacks in wireless networks using signalprints,” in Proceedings of the ACM Workshop on Wireless Security, pp. 43–52, Los Angeles, Calif, USA, 2006.

[6] Y. Chen, W. Trappe, and R. P. Martin, ‘‘Detecting and localizing wireless spoofing attacks,” in Proceedings of the 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON, pp. 193–202, San Diego, Calif, USA, June 2007.

[7] N. Patwari, S.K. Kasera, Robust location distinction using temporal link signatures, in: in Proceedings of the ACM International Conference on Mobile Computing and Networking, 2007, pp. 111–122.

[8] J.K. Tugnait, Wireless user authentication via comparison of power spectral densities, IEEE J. Sel. Areas Commun. 31 (9) (2013) 1791–1802.

[9] Z. Jiang, J. Zhao, X. Li, J. Han, and W. Xi, ‘‘Rejecting the attack: Source authentication for Wi-Fi management frames using CSI Information,” in Proceedings of the IEEE INFOCOM 2013 - IEEE Conference on Computer Communications, pp. 2544–2552, Turin, Italy, April 2013.

[10] X. Wu, Z. Yang, Physical-layer authentication for multi-carrier transmission, IEEE Commun. Lett. 19 (1) (2015) 74–77.

[11] S. Chen et al., ‘‘Machine-to-Machine communications in ultra-dense networks—A survey,” IEEE Communications Surveys & Tutorials, vol. 1, no. 1, 99 pages, 2017.

[12] L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, Channel-based detection of sybil attacks in wireless networks, IEEE Trans. Inf. Forensics Secur. 4 (3) (2009) 492–503.

Further reading

[13] H. Wen, P.-H. Ho, C. Qi, G. Gong, Physical layer assisted authentication for distributed ad hoc wireless sensor networks, IET Inf. Secur. 4 (4) (2010) 390–396.

[14] W. Serrano, The Blockchain Random Neural Network for cybersecure IoT and 5G infrastructure in Smart Cities, J. Network Comput. Appl. 175 (2021) 102909, https://doi.org/10.1016/j.jnca.2020.102909.

[15] Y. Shah, N. Chelvachandran, S. Kendzierskyj, H. Jahankhani, R. Janoso, 5G Cybersecurity Vulnerabilities with IoT and Smart Societies. In Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity, Springer, Cham, 2020, pp. 159–176.

[16] P.K. Sharma, J. Park, J.H. Park, K. Cho, Wearable Computing for Defence Automation: Opportunities and Challenges in 5G Network, IEEE Access 8 (2020) 65993–66002.

[17] B.I. Qinbo, Z.H.A.O. Chengdong, Research and Application of 5G Cybersecurity Threat Modeling Based on STRIDE-LM, Netinfo Security 20 (9) (2020) 72.

[18] Y. Arjoune, S. Faruque, Artificial Intelligence for 5G Wireless Systems: Opportunities, Challenges, and Future Research Direction. In 2020 10th Annual Computing and Communication Workshop and Conference (CCWC) 2020, January, (pp. 1023-1028). IEEE.

[19] P.K. Sharma, J. Park, J.H. Park, K. Cho, Wearable Computing for Defence Automation: Opportunities and Challenges in 5G Network. IEEE Access, 2020, 8, 65993-66002.

[20] M. Bartock, J. Cichonski, M. Souppaya, 5G Cybersecurity: Preparing a Secure Evolution to 5G (pp. 24-24). National Institute of Standards and Technology, 2020.

[21] A.M. Barani, R. Latha, R. Manikandan, Implementation of Artificial Fish Swarm Optimization for Cardiovascular Heart Disease, Int. J. Rec. Technol. Eng. (IJRTE) Vol. 08, No. 4S5 (2019) 134–136.

[22] R. Manikandan, Dr.R. Latha, ‘‘A literature survey of existing map matching algorithm for navigation technology. Int. J. Eng. Sci. Res. Technol.”, 2017, 6(9), 326-331.Retrieved September 15, 2017.

[23] R. Sathish, R. Manikandan, S. Silvia Priscila, B. V. Sara and R. Mahaveerakannan, ‘‘A Report on the Impact of Information Technology and Social Media on Covid–19,” 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 224-230, doi: 10.1109/ICISS49785.2020.9316046.

[24] R. Manikandan, R. Latha, C. Ambethraj (1). An Analysis of Map Matching Algorithm for Recent Intelligent Transport System. Asian J. Appl. Sci., 5(1). Retrieved from https://www.ajouronline.com/index.php/AJAS/article/view/4642.