Solid State Technology
Volume: 63 Issue: 4
Publication Year: 2020

An Enhanced Deep Learning Approach for Preventing Replay Attacks in Wireless Sensor Network

Rajaram P[1], Sathishkumar A[2], Khadirkumar N[3]
[1]Department Computer Science and Engineering, A.K.T Memorial College of Engineering and Technology, Kallakurichi, India
[2]Department Electronics and Communication Engineering, The Kavery Engineering College, Salem, India
[3]Department Computer Science and Engineering, MahaBarathi Engineering College, Chinnasalem, India
E-mail: rajaramnov82@gmail.com, sat090579@gmail.com, khadir_n@yahoo.co.in

ABSTRACT
The nature of Wireless Sensor Networks has established wide range of security threats due to minimal usage of hardware resources and nil infrastructures. Replay attack belongs to the category of Denial of service attack taking place in the network layer. The paper focuses on developing an enhanced deep learning approach for detecting and preventing the replay attack. Decision trees along with assistance of support vector machine (SVM) is implemented on the dataset to prove its efficiency. Many research has proved that SVM has achieved above 98% success rate in detecting and preventing attacks on WSN. Solution for replay attack is less compared to other category of attacks belonging to Denial of service attack (DoS). A wireless sensor network is comprised of minimal hardware platform accelerated with radio communication involved in applications of agriculture and industry for measuring physical properties involved. In replay attack a piece of previously sent information is recorded and re-transmitted after some interval of time. The basic principle of this attack is adapted by more effective attacks like Sinkhole and Blackhole. The crucial role of this attack relies on incapacitating the effective functionality of the network. In this attack bogus packets covers the entire path from sensor node to base station. As a result of which a simulated time of propagation and fake signal strength is generated on receiver side where irrelevant location and fake distance is estimated based on arrival time of the signal. The best solution can be obtained by authentication accompanied with deep learning approach can be against replay attacks.
Keywords: Dos attack, wireless sensor network, deep learning, support vector machine, decision tree.

I. INTRODUCTION

Wireless sensor network collects scalar parameters from sensors utilized which has the potential to extract and process the signal for transmitting. Enormous restrictions are fixed for resources involving storage and computational factors for developing sensors. They are

utilized from household to scientific applications. The factors involved that cannot be ignored in WSN are energy competence attained by the protocols functioning in the layers. As we are focussing on the category of Denial of Service a replay attack, its motive is to consume rapid energy of the resources participating in WSN. Since many sensors are involved we will fail if we find an alternate for all the sensors which do not function properly and sensors cannot be refreshed often. In order to increase the lifespan of the sensors the battery of the nodes has to be preserved. By preserving lifespan can be extended if attack fail[1,2,3]. Implementation of symmetric keys and hash functions are performed for ensuring authentication in WSN. Certain malicious nodes are eligible for symmetric keys and they can access information belonging to the base station[4]. As a result of which the nodes involved cannot recognize the data belonging to the base station which provides opportunity for the intruder to steal the data from cluster heads. Replay attack is one among the common attack which has mere solutions in recent researches, here already sent information is recorded by the intruder and re-transmitted by him later after certain interval of time. This attack serves as a base for many complicated attacks. Preserving security and energy efficiency are two major aspects of research in the field of WSN. A paradigm which is Receiver Initiated was proposed for proving energy efficient platform for link-layer connection [5]. For Receiver-Initiated MAC(Medium Access Control) protocol the communication is initiated by a fake frame called beacon, to the receiver. The attacker adopts for replay attack due to its minimal cost of implementation and its complicated for detecting the source of the attack. Malicious attacker pretends to send legitimate node to entrap the neighbouring nodes and minimizes the lifetime of the nodes.

II. RELATED WORK

The existing contributions on replay attacks has addressed and mitigated replay attacks by providing a wide adopted solution by making the packet to be sent with a unique identity by including factors like counter or timestamps. But timestamps are found to be complicated technique which is harder to implement since it undergoes an agreement process with both sender and receiver for forwarding the packets. Another conventional technique is increasing the amount of counters accompanied with message authentication code where every message is different from one another. The contribution research by Alessio Di Mauro et al[6] is they havedefined a beacon replay attack which is specific only for **MAC** protocol which is receiver-initiated and energy-efficient WSNs**.**They have analysed the attack in various perspectives harming the sensor network and how their solution plays a major role in ensuring security for the network. They have introduced Receiver Authentication protocol(RAP) which comes under the category of challenge- response authentication protocol for detecting and preventing the attack created by beacon replay. A verification methodology is also included for RAP by automated verification tools and overhead assessment is done on energy consumption.

Perrig et al[7] proposed two techniques dedicated to each part of the protocol. MAC code is added to SNEP counter, herein time synchronization and hash chains are utilized by µTesla. Liu.D et al[8] created sequence number while exchanging messages. K.E BAvar[9]

and his team implemented two step scheme with hash chains consisting of response and detection. As far as detection phase is taken into account every node has a unique ID value for the message to be sent with increasing hop count.

Ghosal, A and Heinzelman.W et al[10,11]used LEACH protocol for query driven paradigm and developed based on the mechanism exploiting organization of the cluster and depends on the cluster heads from comparing timings among the messages from the nodes that are registered. Zhu, S et al[11] proposed a scheme based on time synchronization where beacon messages plays a role as done in receiver initiated paradigm.

Security prevails to be both functional and non-functional requirement for WSN systems for preventing unauthorized access to the network. DoS is one among those access where many research methodologies are suggested to find solutions for preventing the attack. The methodologies adopted by wired networks are found to be non-preferable for wireless networks since they have constrained resources. Compared to external attack internal attack creates a critical security issue for WSN framework. Shi et al[13] develop a method for detecting internal attacks through epidemiological model. Here the detection rate is measured by rate of transition from compromised state to response state. Utility based calculation for state transitions of sensors are achieved by Bellman equation in the forms of dynamic programming.

The functionalities of WSN can be terminated or stopped due to replay attacks and they are difficult to recover from such scenarios. K.Kanchan[14] and team categorized DoS attack into three main categories based on their tendency of attack on the network. The attacks are made on the protocol packets like Internet Control Message Protocol (ICMP) protocol packets or User Datagram Protocol (UDP) floods packets where large number of packets are sent to the target server to occupy the bandwidth by putting the server down. Next is protocol-based attacks where many requests dumps into the server and there are no resources left to respond for those request. The resources involved are load balancer, firewalls and other services are consumed and disabled. The application based attacks happen in application layer where the attacker attempts to spoof packets which requires low bandwidth for attacking the target server. Thus proposed methodologies overcome DoS attacks in various ways and certain attacks under that category are not focussed like replay attacks. This paper extends the existing methodology by deep learning approach with support vector machines to overcome the threat caused by replay attacks.

Dong et al. [15] made use of hash chains in which each node consists of hash value and its own node-id and forwards the combined value to its next higher node on hop count. The node at the receiving end detects the replay attack while observing the node-id and hash value. The drawback of this scheme was the computation of hash value consumes more time.

Soroush et al. [16] created a scheme for defending the replay attacks by increasing the counter which maintains and keeps record of the old replayed messages. This scheme

maintains a counter storing the timing information of the available nodes but the memory space occupied is more for constrained sensor nodes.

III. DEEP LEARNING CONTRIBUTIONS ON DoS ATTACKS

Deep learning has contributed immense number of solutions for Denial of Service attacks (DoS) in wireless sensor networks. Among many attacks replay attack holds minimal number of solutions in conventional methodologies. On deep learning perspective research contribution is less on this attacks. The solution provided in this paper will dynamically study the imperfections of wireless sensor networks by uniquely classifying the necessary nodes for the receiver and find the nodes that are replayed by the attackers. The neural networks involved studies hierarchical non-linear features which discovers hidden structures of the data compared to other methods. The model can be adapted to wireless network and it remains to be inexpensive. In conventional methodologies imperfections are observed in hardware factors which includes offsets in the frequency of the carrier leading to affect the signals involved. In general deep learning techniques are involved in identifying automatic speech recognition and data prediction. They are designed in such a way to support dependencies for long term and are more suitable for wireless sensor networks.

3.1. IMPACT OF REPLAY ATTACK

Wireless sensor networks prove to be effectively increase wide range of applications like military, recovery from disaster and environmental monitoring. They obviously lead to security challenges due to their infrastructure, communications that is open, dynamic topology and minimal resource. Along with eavesdropping and tampering of message replay or spoofing is also possible. Replay attack targets by attacking the traffic by sending already sent packet again and again. The attacker performs certain analysis to obtain location as well as information from data packets. They can also obtain cryptographic keys and disturb the normal flow in the network. The mission of replay attack is tracking all the messages sent among the nodes and to waste the resources of the node which is targeted, as a result of which target node will not be able to complete its own task which leads to denial-of service.

3.2. MONITORING OF NODES AND THEIR LOCATIONS FOR DETECTING REPLAY ATTACKS

Monitoring of nodes is the initial stage for detecting the replay attacks. Monitoring the traffic of local nodes along with its neighbours serves as collaborative detection strategy. Let us assume a node x to monitor a node y which must be the neighbour of both y and previous hop from y, say l. therefore let x be a guard node for y. To denote the nodes which are within the range x toy we use R(y) and the guard nodes are represented as G(y,z). Here information from one node to another is available in watch buffer at every guard node. The guards expect that y forwards the packet towards the destination. Every entry corresponding to watch buffer has a time stamped with a level of threshold based on which transmission occurs. The packet which are forwarded along with its previous hop is verified for the information available in the watch buffer. The packets can be verified if they are duplicated, corrupted, dropped or

delayed. If a malicious node is determined they are maintained in malicious counter with a certain window length. If growth in the value of the counter is maintained by guard node becomes high than the threshold rate, an alert message is sent to all nodes reporting malicious node. When the neighbour receives an alert, an authenticity of the alert message is verified.

3.3 DEEP LEARNING BASEDLONG SHORT TERM MEMORY (LSTM) DETECTION ON REPLAY ATTACKS

The proposed deep learning based long short term memory detection accurately detects the replay attacks in WSN. This can widely be used in applications including information security, defence and biometrics to improve the security of the network. The previous works on replay attacks focus on audio replay detection in noisy environments and ensuring basic security by preventing replay attacks in a query processing application domain in WSN. This paper aims to improve the replay detection algorithm for the packets transmitted from sender to receiver. The motivation is summarized as follows:

(i) The packets to be transmitted chose LSTM for obtaining the representation based on the statements. Through LSTM the packets are easily transformed into a vector which serves as an input to the classifier.

(ii) Packet length differs contributing different perspectives on replay detection. Packet length is also observed and maintained for further authentication.

(iii) When recurrent neural network(RNN) is programmed through sensor flow the input packets i.e packet to be transmitted from one node to another are measured and length of the packets are maintained. The research on LSTM and RNN has a great impact based on the length of the packets.

(iv) The splitting or padding of packets are divided into segments to recognize whether the packets are original or repeated packets. Based on the individual segments used in ensemble learning we will be able to predict the original packet which is transmitted to the destination.

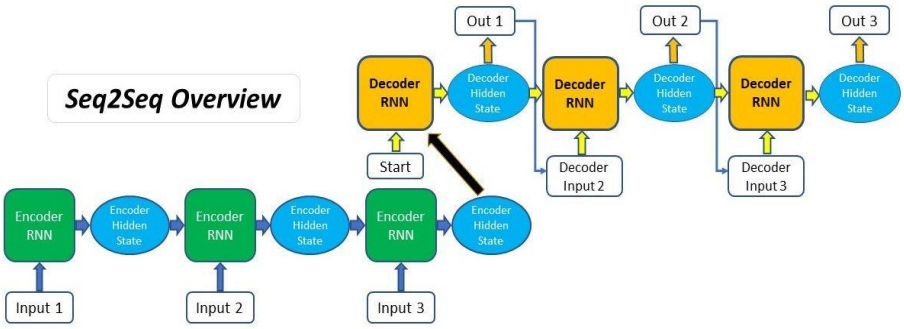

Fig 1: Packet transmission sequence to sequence overview through encoder and decoder

4. MECHANISM INVOLVED IN DETECTING REPLAY ATTACKS

The mechanism proposed for detection is attention based LSTM method. The network architecture is presented below.

4.1 Attention based mechanism

The attention based mechanism has proved its efficiency in various applications like speech recognition, natural language processing and machine translation. The mechanism can observe the relationship of the nodes transmitted and predict the current time step using the vector related to weight recognition. For a sequence of packets the state is indicated by p_j at every step, the effective vector e_t can be found by,

$$e_t = \sum_{j=1}^{T} a_{tj} \; p_j \qquad (1)$$

Here T represents the total number of packets transmitted and a_{tj} is the weight vector obtained by step by step p_j. The weight vector a_{tj} is computed through intermediate node m_{tj}.

$$M_{tj} = \varphi (s_{t-1}, p_j) \qquad (2)$$

s_{t-1} represents the output of steps until t-1 and φ is learned function performing the scalar factors determined by p_j and s_{t-1}. After computing the above equations the weight vector a_{tj} is obtained by

$$a_{tj} = \frac{\exp(m_{tj})}{\sum_{k=1}^{T} \exp(e_{tk})} \qquad (3)$$

The mechanism on attention recursively generates vectors on weight based on the current state. The packets contributing to the destination have higher weights among the other vectors, while the packets providing less tend to have lower weights. Equations (1) to (3) is considered as encoded utterance to efficient vector acting as an input to classify the repeating packets in the network.

ATTENTION THROUGH FEED-FORWARD

The conventional methodologies described in above section has generated a value for learnable function depending on newly generated output, s_{t-1} along with current state p_j. Combining equations (2) and (3) we obtain

$$e_t = \varphi(p_j) \qquad (4)$$

and

$$a_t = \frac{\exp(e_t)}{\sum_{k=1}^{T} \exp(e_k)} \;, \qquad (5)$$

Here a_t represent the value of weight vectors, m_t and $m_j$indicate the intermediate vectors. The mechanism is developed by an efficient vector according to the input sequence by calculating average of adaptive weighted factor based on the state sequence.

5. ARCHITECTURE FOR DETECTING REPLAY ATTACKS

The framework proposed is depicted below in Figure 1 where the first stage is extracting related features from the information packets transmitted and the hidden features are acquired from LSTM. The next stage is normalization occurring in packets where incomplete packets are filtered out for improving model performance. Efficient vector produces hidden factors of the packets and it is also connected to layer for detecting the

packets which are replayed. The layer reveals the packets which are genuine as well as packets that are replayed.

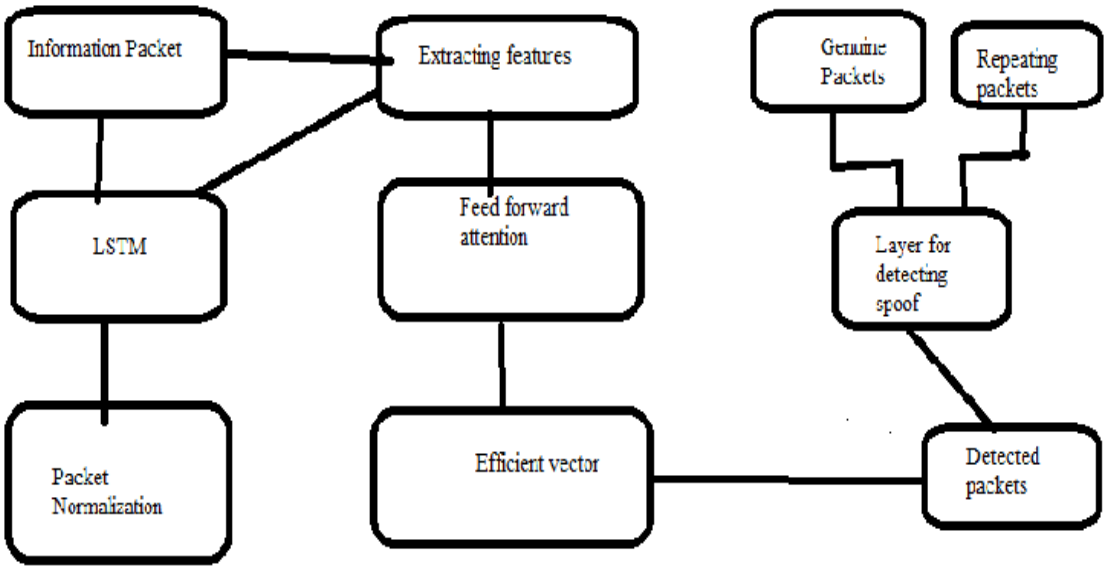

Fig 1: Architecture for detecting replay attacks

Let us assume a surveillance system which is edge based and it allows the attacker to access the information packets. The method proposes consists of two modules where one module detects the replay and the other one deploying the attack.

Algorithm 1: Monitoring the frames that are replayed in WSN
Step 1: Each and every packet is monitored independently
Step 2: Collecting the spoof packets to monitor separately,
Step 3: If the packet involves multimedia data (audio and video), the process checks for them separately by collecting duplicate recording in both independently.
Step 4: If video is encountered the motion in the frame is checked, if during the process static frame is detected its automatically recorded in the background.
Step 5: Gaussian blur is performed on the frames to minimize the errors caused due to noise, based on which intensities of the pixels are compared for detecting a threshold in identifying the motion.
Step 6: If audio packets are involved in transmission, the monitoring process looks for noise in the environment. Thereby both data packet and multimedia packets are collected and stored for verification on replay.

Algorithm 2: Deployment of attack- Phase of triggering and launching an attack on WSN.
Step 1: When the trigger is encountered, the samples of multimedia or general data packets are deployed by collecting pre-recorded samples.
Step 2: The samples are used when an attack is triggered on the environment.

Step 3: Considering the video packets, static frame is compared with consecutive frame, certain changes will be reflected on the pixels leading to different threshold values.

Step 4: Gaussian blur here observes the changes in the incoming frames by performing convolution on the image, disguising as a low pass filter and attenuating the components which have high frequency. Removal of noise performs better in detecting the changes.

Step 5: For audio frames Fast Fourier transform is implemented on the samples for obtaining frequency in incoming audio packets.

Step 6: The detection of noise is done by considering mean volume of all frequencies and comparing with the threshold.

Step 7: The gradients of the frames are trained by deep learning algorithm where each packet has unique encoding, which is trained in detecting the trigger created on the environment.

Step 8: The algorithm alerts the sender and the receiver about the packets being replayed.

Evaluating the performance of deep learning method

The metrics to evaluate the performance is described based on the factors like authenticated nodes, all the nodes involved in the network, packets transmitted and available.

$$\text{Authentication factor} = \frac{Authenticated\ \ nodes\ in\ WSN}{Number\ \ of\ nodes\ in\ the\ WSN} \quad (6)$$

$$\text{Novelty} = \frac{Packets\ received\ \ currently\ \ involved\ \ data}{Packets\ \ sent\ \ in\ \ WSN} * 100 \quad (7)$$

6. AUTHENTICATION BASED ON MACHINE LEARNING

Conventional methodologies are not always applicable to WSN which has limited computation and hardware resources for detecting spoofing attacks like replay attacks. Authentication techniques on physical layer exploits spatial decorrelation in the radio channels and transmitters with received signal strength indicators, strength of received signal, impulse responses observed in the channel, state information regarding state of the channel, MAC address security protectionfor WSN devices with minimalcomputation and overhead in communication without leaking information about the user[17]. Machine learning techniques helps in building light weight access control for preserving energy and extending lifetime of the sensors. Outlier detection scheme applies K-NN for addressing issues in unsupervised learning for the sensor networks. It offers flexibility for defining outliers with minimal energy consumption of 62% compared with centralized scheme of similar energy consumption [18]. The multilayer perceptron based access control presented in [19] makes use of neural network with two neurons in the hidden layer for training connection weights of the MLP and identify the suspicion factor indicating whether the sensor network is the victim of DoS replay attacks. The scheme utilizes backpropagation applying forward computation and error backpropogation which applies forward computation and particle swarm optimization as an evolutionary computation technique. Here the particle utilized uses adjustable velocities for updating connection weights of the MLP. The sensor under test shuts the functions of MAC and physical layer for preserving the energy and expand the lifetime of the network if the output of MLP goes beyond the threshold[20].

7. METHODOLOGY

The complication in detecting the reliability of replay attack can be due to the recording and the packets getting intertwined with other irrelevant sources of variability formed due to capturing of packets, environmental noise etc. Hence the model proposed identifies the essential packets by recording and capturing the packets as well as overcome the variability caused by other factors. Here we introduce packet delay grams acquired from including a group delay function over consecutive packets as a representation of time frequency based on the occurrence in machine learning framework for detecting the replay attack. By using delay in packet factor provides frequency of time with spectral resolution required for spoofing detection. The method allows to focus on the region of the spectrum where spoofing is highly possible. ASV spoof 2017 dataset is used and we have achieved a minimal error rate on development and evaluation set.

Decision Tree in machine learning

Decision tree algorithm plays a major role for making decisions. There are numerous classifications involved in DoS attacks, those attacks has to be classified and replay attack has be uniquely identified for our research. Hence decision trees plays a major role in classifying major attacks. It provides a graphical representation for solving a problem by providing solutions to a given problem. The tree comprises of a leaf based on final decision choice where decision requires moving through a bath from root to leaf. The path opted is based on the queries provided. This process highly supports the decision making process. The below segment provides evaluation metrics, they are listed below:

True Positive (TP) here is defined as the rate of packets which are truly affected by replay attack. False positive (FP) are the ones which are falsely labelled by the classifier of decision tree that the packets are affected. True negative (TN) packets are really affected due to the attack. False negative are the number of packets that are truly affected but wrongly labelled as negative. Precision (P) is the measure of cent percent accuracy which are classified by decision tree as positive. Retraction is defined as the ratio of total number of packets that are correctly classified as correct samples.

Type of attack	**TP**	**FP**	**Precision factor**	**Retraction factor**
Normal	0.99	0.020	0.98	0.99
Flood	0.97	0.001	0.95	0.97
TDMA	0.92	0.001	0.99	0.92
Replay Attack	0.99	0.00	0.98	0.99

Table 1: Accuracy of the decision tree on different categories of DoS.

Uncertainty matrixis another factor which is included for summarizing the performance of the classification algorithm which classifies the type of attack based on the impact. This is useful when there are more than two classes in dataset which can be misleading while calculating. Hence its necessary to calculate the uncertainty factor which ensures that the decision made is accurate.

I	II	III	IV	Classification
339719	159	27	150	I-Normal
83	3229	0	0	II-Flooding
478	0	6151	5	III-TDMA
122	0	4	14408	IV- Replay attack

Table 2: Uncertainty matrix of the decision table using the available packets in the network.

The proposed work focusses on detecting the replay attacks through deep learning mechanism, apart from replay attack there are other categories of DoS attacks. There are classified as Normal, flooding, TDMA. The methodology categorizes the attacks which has affected the WSN environment. The above table 1 and 2 provides us a view on minimal error rate achieved by the deep learning methodology and the uncertainty matrix predicted as per the values obtained through decision trees.

7.1 EXPERIMENTS

Here we focus on ASV spoof 2017 replay attack dataset which contains both training and development sets of genuine and replayed multimedia packets.
The replay configuration holds a replay and recording device and a session refers to set of source files which shares same replay configuration. Various quality of multimedia packets are used for simulating spoofing attack along with evaluation and detection.

7.2 RESULTS AND EVALUATION FACTORS

Based on the dataset computing the error rate requires assuming a score to each packet being transmitted. If the score is high the file is genuine and the error rate depends on two metrics one is acceptance of false rate(FA) and its rejection rate(RR). Let us assume the threshold value as *t, s* represents score *r* is replay, *g* is genuine for calculating both the rates:

$$FA(t) = \frac{S(r)>t}{s(r)}, \quad FR(t)=\frac{s(g)\leq t}{s(g)} \qquad (8)$$

TECHNIQUES	ERROR RATE ON DEVELOPMENT	ERROR RATE ON EVALUATION
LCCN	3.95%	6.73%
Baseline	10.35	30.60
Grand Ensemble	-	2.76%
Packet group delay in ML (Fusion system)	0.0%	0.0%

Table 3: Comparison of error rate based on the results on ASV spoof 2017 dataset.

8. Comparison of resultant error rates between conventional and proposed methodology

The table above depicts the comparison between baseline, ensemble and proposed packet group delay technique provided in this paper. Error rate is analysed based on ASV spoof baseline system. The system uses expectation maximization algorithm accompanied with random initialisation. The individual system LCCN identifies genuine and replay spoofing using high level feature space in simple Gaussian models. The packet group delay proposed in this paper has achieved zero percent error rate.

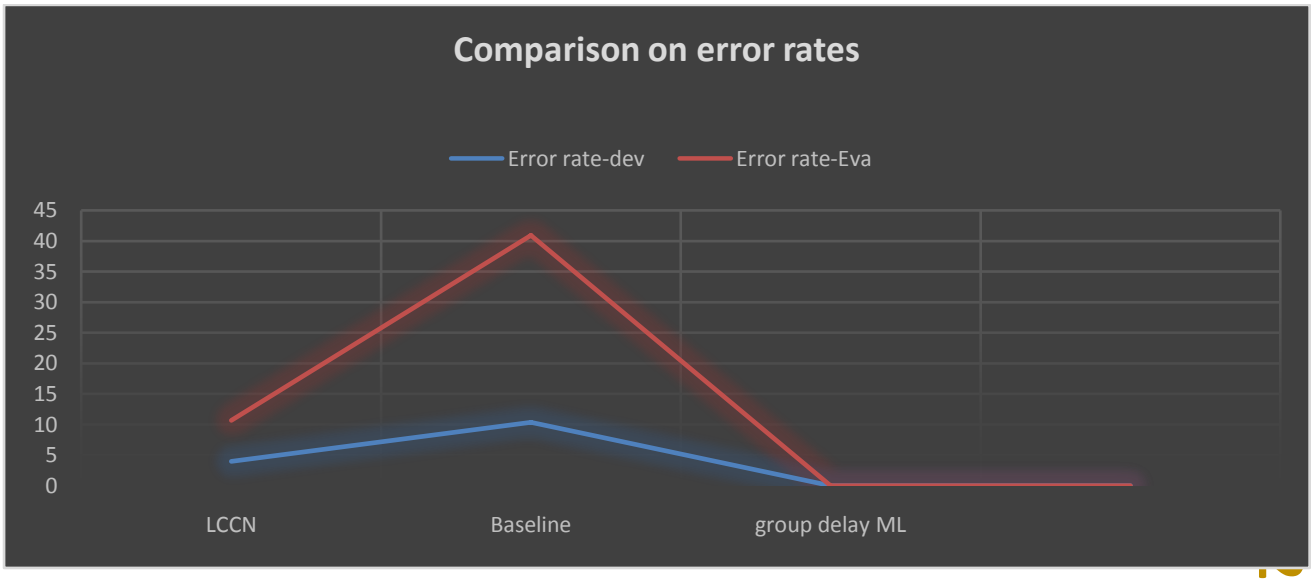

Fig 2 : Error rate comparison on existing and proposed methodology.

The above Fig 2 is a graph depicting the error rates where group delay packets when fused with machine learning technique has achieved zero error rate and the conventional methodology has a spike in error rate. This ensures the success rate on detecting the replay attack in WSN environment using LSTM technique.

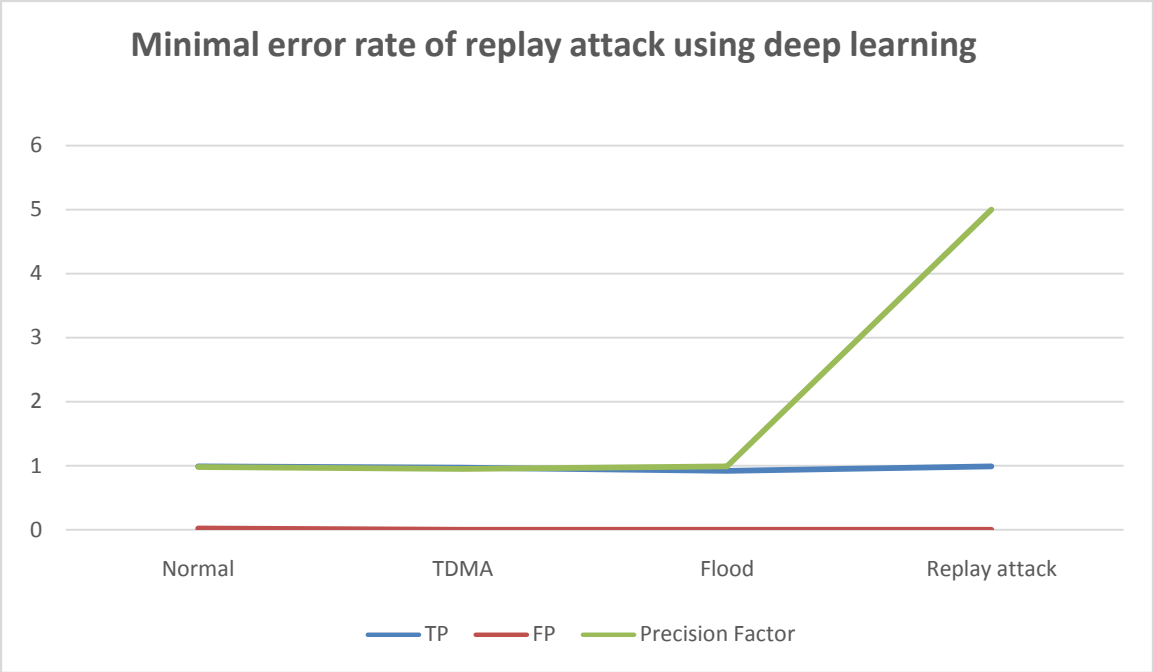

Fig 3 : Minimal error rate of replay attack using decision tree.

Fig 3 depicts that the evaluation factors of decision trees prove that the deep learning mechanism uniquely identifies the replay attack with minimal error rate. The graph is the other dimension on the success factor of the proposed technique.

9. Conclusion

In detecting the packets whether they are replayed its necessary to consider the packets that are prone to spoofing. By using the proposed deep learning algorithms spoof detection is performed using ASV spoof dataset including noises in the environment. Minimal error rate is achieved by the proposed methodology at end-to-end deep learning framework based on group delay available in the packets. Importance of information available in specific regions where replay occurs have been identified along with time frequency representation of the packets with their replay detection. We have achieved zero percent error rate on development and evaluation phases on spoof dataset available.

References:

1. Raymond, D. R., Marchany, R. C., Brownfield, M. I., &Midkiff, S. F. 2008). Effects of denial-ofsleep attacks on wireless sensor network MAC protocols. *IEEE Transactions on Vehicular Technology,58*(1), 367–380.

2. Noroozi, E., &Kadivar, J. (2010). Energy analysis for wireless sensor networks. In *2010 2nd international conference on mechanical and electronics engineering* (Vol. 2, pp. V2–382). IEEE.
3. Raymond, D. R., &Midkiff, S. F. (2007). Clustered adaptive rate limiting: Defeating denial-ofsleep attacks in wireless sensor networks. In *MILCOM 2007-IEEE military communications conference* (pp. 1–7). IEEE.
SVM[3]
4. Frunza, M., &Scripcariu, L. (2007). Improved RSA encryption algorithm for increased security of wireless networks. In *2007 International symposium on signals, circuits and systems* (Vol. 2, pp.1–4). IEEE.
5. Lin, E.Y.A., Rabaey, J.M., Wolisz, A.: Power-efficient rendez-vous schemes for dense wireless sensor networks. In: Proc. IEEE Int. Conf. on Communn. (ICC), vol. 7, pp. 3769–3776. IEEE (2004).
6. Detecting and Preventing Beacon Replay Attacks in Receiver-Initiated MAC Protocols for Energy Efficient WSNs, Alessio Di Mauro, XenofonFafoutis, Sebastian M¨odersheim, and Nicola Dragoni
7. Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V., Culler, D.E.: Spins: security protocols for sensor networks. Wirel. Netw. 8(5), 521–534 (2002)
8. Liu, D., Ning, P.: Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. Tech. rep. (2002)
9. Dong, J., Ackermann, K.E., Bavar, B., Nita-Rotaru, C.: Mitigating attacks against virtual coordinate based routing in wireless sensor networks. In: Proc. of the First ACM Conf. on Wireless Network Security, pp. 89–99. ACM (2008).
10. Ghosal, A., Halder, S., Sur, S., Dan, A., DasBit, S.: Ensuring basic security and preventing replay attack in a query processing application domain in WSN. In: Taniar, D., Gervasi, O., Murgante, B., Pardede, E., Apduhan, B.O. (eds.) ICCSA 2010, Part III. LNCS, vol. 6018, pp. 321–335. Springer, Heidelberg (2010)
11. Heinzelman, W., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: Proc. of the 33rd Annual Hawaii Int. Conf. on System Sciences, vol. 2, p. 10 (2000).
12. Song, H., Zhu, S., Cao, G.: Attack-resilient time synchronization for wireless sensor networks. In: Int. Conf. on Mobile Adhoc and Sensor Systems, pp. 765–772 (2005)
13. Q. Shi, L. Qin, L. Song, R. Zhang, and Y. Jia, "A Dynamic Programming Model for Internal Attack Detection in Wireless Sensor Networks," in Discrete Dynamics in Nature and Society, vol. 2017, Article ID 5743801, 9 pages, 2017. https://doi.org/10.1155/2017/5743801.
14. K. Kanchan, and S. Varsha, "Early Detection of DDoS Attack in WSN," in International Journal of Computer Applications, vo. 134, no. 13, pp. 14-18, January 2016. 10.5120/ijca2016908117
15. Dong, J., Ackermann, K.E., Bavar, B., Nita-Rotaru, C.: Mitigating Attacks against Virtual Coordinate Based Routing in Wireless Sensor Networks. In: Proceedings of 1st ACM conference on Wireless Network Security, pp. 89–99 (2008)

16. Soroush, H., Salajegheh, M., Dimitriou, T.: Providing Transparent Security Services to Sensor Networks. In: Proceedings of IEEE International Conference on Communications, pp. 3431–3436 (2007).
17. L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," IEEE Trans. Vehicular Technology, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.
18. J. W. Branch, C. Giannella, B. Szymanski, R. Wolff, and H. Kargupta, "In-network outlier detection in wireless sensor networks," Knowledge and Information Systems, vol. 34, no. 1, pp. 23–54, Jan. 2013.
19. F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," Soft Computing, vol. 20, no. 1, pp. 343–357, Jan. 2016.
20. Liang Xiao, Xiaoyue Wan, XiaozhenLu,Yanyong Zhang, Di Wu, "IoT Security Techniques Based on Machine Learning"