ISSN 2347 - 3983
Volume 8. No. 5, May 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter05852020.pdf
https://doi.org/10.30534/ijeter/2020/05852020

Handling of Man-In-The-Middle Attack in WSN Through Intrusion Detection System

Hitesh Mohapatra[1*], Subhashree Rath[2], Subarna Panda[2], Ranjan Kumar[2]
[1*]Assistant Professor,Jain Deemed to be University, Jayanagar, Bengaluru, India, E-mail: hiteshmahapatra@mail.com.
[2]Assistant Professor, Jain Deemed to be University, Jayanagar, Bengaluru, India

ABSTRACT

The wireless sensor network (WSN) is one the most convenient and easily adoptable ad-hoc technique for data transmission. With many flexibilities of WSN there are many loop holes. The decentralized architecture of WSN invites many types of attacks like man-in-the-middle (MITM) and black holes etc. In this paper, we propose a MITM-Intrusion Detection System (MITM-IDS) model for detection, isolation of attack and reconfiguration for attacked nodes. The IDS technique helps to train the nodes with the possible attacks. The simulation shows the rate of 89.147\%, of productivity in way to perform MITM attacks. This work aims to develop an attack tolerant IDS.

Key words: MITM, Wireless Sensor Network, Fault Tolerance, Cyber attack

1. INTRODUCTION

Advanced technology has become the integral part of our life [1]. To satisfy the need of the society, almost in each work, we use the technology[2][3]. In current era computer science is major subject [4]. It has many real life applications such as cloud computing[5], artificial intelligence[6], remote monitoring[7], Wireless sensor network[8, 9, 10], internet of things[11, 12, 13], Neural network[14, 15], FSPP[16, 17, 18], NSPP [19, 20, 21, 22, 23], TP[24, 25, 26], internet Security[27], uncertainty [28, 29, 30, 31, 32] and so on. Technology is the mode by which user can store, fetch, communicate and utilize the information[33]. So, all the organizations, industries and also every individual are using computer systems to preserve and share the information. The internet security plays a major role in all computer related applications. The internet security appears in many real-life applications, e.g., home security, banking system, education sector, defense system, Railway, and so on.

In this manuscript we discuss about the protection of authentication which is a part of internet security. Regardless of all decent applications of WSN its most vulnerable to intruder attacks such as Man in Middle attack (MITM) [34]. In case of MITM attack an uninvited third party penetrates the conversation as a legitimate user[35]. The intruder or attacker acts like proxy user and manipulates the data as his/her needs[36]. In the past literature the MITM is abbreviated in various ways such as MIM, MitM or MIM etc. The generic architecture of MITM is illustrated in Figure 1 illustrates a real-time demonstration of pipeline operations.

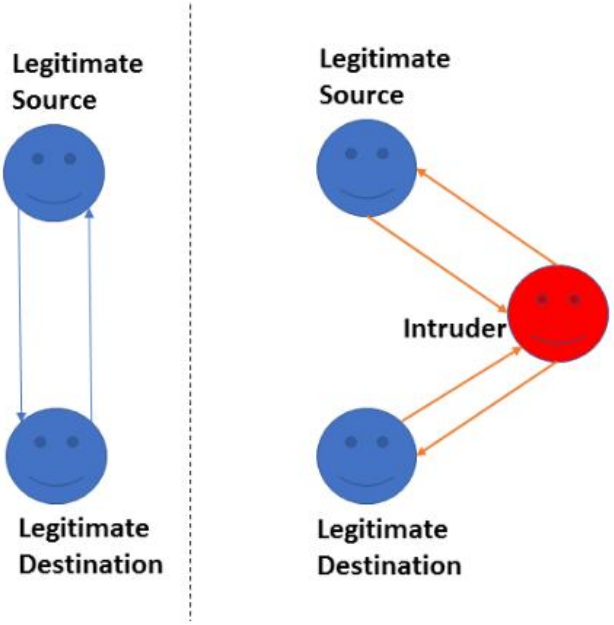

Figure 1: MITM attack

MITM is a type of eavesdropping attack where the attackers secretly listen the conversation between two legitimate users. At the of need, the attacker pretends as a legitimate user and hack the data or information for manipulation. Normally, during MITM attack, the intruder targets the real-time transactions, conversations or transfer of information. Without proper security, both of legitimate users will never come to know about the authenticity of data[37]. This paper primarily focuses on MITM intrusion detection system (MITM-IDS) based on deep learning with centralized database network. The whole process tries to develop an attack-tolerant MITM-IDS that ensures attack free communications with detection of malicious signatures.

The rest of the paper is organized as follows; Section 2, explores literature review, Section.3 discusses the proposed model, Section 4, highlights the results and Section 5 concludes the paper followed by references.

1.1 Man-in-the-Middle Attack

MITM attacks is one of the well-known attacks in computer security, which have attracted many researchers. In paper[38]the authors have explored MITM attacks on physically connected networks. The outcome of this paper represented a taxonomy of MITM on https by classifying the attacker in to four types such as state, vulnerability, behavior and target. In this line of thought a mathematical model on MITM attacks with secure socket layer protocol that has been explored [39]. In addition to the research work many studies also has been presented on MITM attacks by considering OSI layers and UMTS. Further, more the impact of MITM attack in association with MAC layer for ad-hoc mesh topology has been discussed [40]. The author exploited the network properties to expose and detect infected nodes through MITM attacks with less false positive value with high detection rate[41]. Further, in paper[42],another solution to handle MITM attacks over Wi-Fi network has beenbriefed.

The in-depth study on MITM concludes us that both wired and wireless network is vulnerable to MITM attack. The very real time instance of MITM can be derived from a basketball scenario where the third player tried to intercept while other two players try to pass it. The MITM attack jeopardize the communication alter the messages with legitimate nodes. Such attacks invite catastrophic consequences. In WSN the attacker satisfies two primary conditions such as message must contain significant information and the attacker must able to interpret the data [43]. The MITM attack can be classified into two types such as 1) passive attack and 2) active attack [44].

- Passive Attack: In this type, the attacker eavesdrops the communication link between two legitimate users.
- Active Attack: In this type, the attacker mainly modifies the content of packet through delay, drops and manipulation.

When any event occurs in WSN the transmitted packet PG message contains at least the following three inputted components i.e. location of generated event, occurrences of the event in terms of time and content of the event along with extra information like message ID, protocol version, flag value etc. This can be presented as:

$$P_g = \{Location, Time, Content\} \quad (1)$$

Where, location = li, time = ti, content = Ci. So, i ϵ Ti, i = {1,2,3...}.

$$P_G = \{li, Ci, Ti\} \quad (2)$$

The sensor nodes in WSN can be deployed in two ways, either in static or in dynamic way. In static scenario the sensor nodes contain static coordinates in terms of x, y, z whereas in dynamic environment a GPS module can be integrated with sensors. Further in both the environment the generated message at time $\mathbf{t_{send}}$ can be represented as:

$$P_G = \{safety, non-safety, li, ti, Ci, t_{send}\} \quad (3)$$

During MITM, attack the malicious node can compromise the contents by using Eq 1. This comptonization can invite disaster in the network. Similarly tampering of location can also lead to a confusing state for both sender and receiver. Further changing of time can also have same impact on the same network by ignoring the messages, which are old and outdated. Actively, attacker launches MITM attack in three ways like:

1. Delay the authentic message.
2. Drop the authentic message.
3. Tamper the authentic message.

1.2 Types of MITM

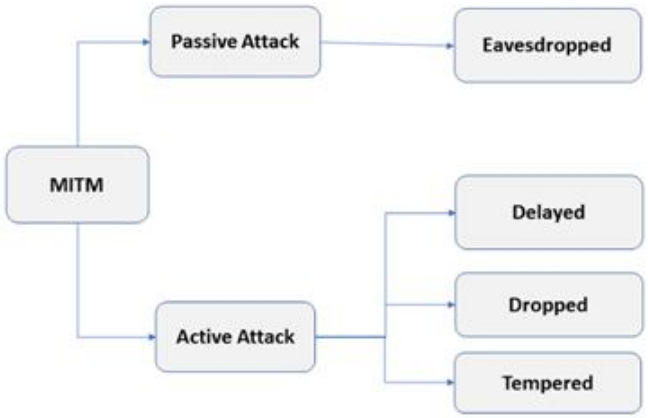

Figure 2: Types of MITM attack

Figure 2 illustrates the classification of MITM attack. The MITM attack primarily divided into two types such as active and passive attack. Further, active attack is segregated into three types such as delayed, dropped and tempered. The eavesdropped attack belongs to passive attack.

1.2.1 Delayed Message in MITM

The applications like VANET (Vehicular network), banking transactions and battlefield are severely affected with MITM with message delay due to sensitive nature of messages delay due to sensitive nature of messages it can create. For instance, consider a battlefield scenario where delay of single message by a malicious node can cause catastrophic situations where legitimate nodes are unable to receive the message on time. As a result, such situations can also put human life in danger.

1.2.2 Dropped message in MITM

During dropped message attack, the attacker intentionally drops the authentic message PG by suppressing the further propagation of PG. As a consequence, the attacker obstructs the authentic user (AU) from receiving messages related to safety and non-safety measures. For example, during VANET when a vehicle broadcasts legitimate information about road conditions, and if that information get dropped then human life will be in danger.

1.2.3 Tempered message in MITM

In this attack, the attacker has targeted the content of the received message. Whenever the intruder node receives the content, the attacker manipulates the sensitive information. For instance, in banking transactions the broadcasting of messages during any serious declaration affects seriously to society act. In this case, the tampering of sensitive content can lead to serious consequences. This intruder message is misleading the legitimate nodes and creates disaster in the network. Further every message of WSN contains three important components i.e. data, time and location. This kind of attack enables the attacker to manipulate the data like location timings and contents. The outcome of such attacks can be as follows.

- Manipulating data leads to compromising data transmission in to compromised transmission time by changing garbage time (**Tg**).
- The coordinates of sender location loc (a, b, c) → loc (**Pa**, **Qb, Rc**).

In this manuscript, we implemented the above three ways of MITM attack. It won't be wrong by saying that MITM compromises integrity, authentication, confidentiality and availability for WSN. In this attack, the attacker adopts two different strategies.

- The attacker is distributed randomly across the networks.
- The attacker exists in fleet structure in a collaborative manner.

2. LITERATURE REVIEW

The WSN is resource constrained self-organizing network that is mostly preferred for harsh and hostile environment. The deployment pattern of WSN mostly vulnerable to the many types of fault. These faults may happen due to several causes such as software glitch, hardware malfunction, isolation of node, or due to surrounding circumstances (environmental factors). Hence, adoption of appropriate fault tolerant techniques may mitigate all these possible faults and its causes. Form, all possible attacks, in this paper we focus on MITM attack. In this sub-section we present all existing ways to handle MITM in WSN.

MITM is not a new concept to be deal with. In [45], the author has proposed a detection approach for MITM by considering the clock synchronization and location as factors. Location is one of the important factors, by considering location the interference of attacker node can be detected. In [46], the authors have explored a machine learning based IoT security mechanism where authentication, secure offloading, malware has been taken care of. In the IoT the attacks are possible in several layers like network layer, physical layer, data processing layer and application layer. These attacks are need to be handled individually. In [35], the authors have studied and presented a holistic security model for IoT where the attacks are managed separately based on their layers of occurring. In [37], the authors have explored the MITM attack in fog computing environment. Usually, the fog nodes are constrained with all resources hence these nodes are more vulnerable to attacks. These fog nodes normally deployed as edge computing devices in the cloud services. The exponential growth of IoT devices gradually increases the latency in cloud services. The use of fog nodes reduces the latency by processing part of data at its own end. The fusion of intrusion detection system (IDS) and intrusion prevention system (IPS) helps to handle the MITM attack in for computing.

The MITM attack is also can be detected by analyzing the strength of received signal (RSS) and round-trip time (RTT) from the client end[47]. The presence of MITM attacks influences the RSS by longer delay and the RTT by larger standard deviations. The investigation on these factors can help to detect the presence of malicious node in the process of communication. In paper[48], the authors have proposed a received signal strength indicator (RSSI)-based detection mechanism for MITM attacks. In this method, the RSSI value has been processed via a sliding-window to get static information about the signals like mean and standard deviation profiles. This method helps to detect the MITM access point. When we compare the wired network with wireless network, it was found that wireless network is more vulnerable to the attack as it is not protected by any cable transmission medium. As the information broadcast over the air medium so it can intercept by any one whoever exist in the transmission range.

The MITM attack is a catastrophic situation for wireless network. In the process of MITM attack there are many versions of MITM attack has been evolved like stealth MITM (SMITM). This short of attacks mostly happens by targeting address resolution protocol (ARP). In this method the forging happens by manipulating ARP response frame by exploiting Wi-Fi Protected Access 2 (WPA2) protocol [49]. The wireless network has many variations like WLAN, WAN, MANET etc. A Mobile Ad-Hoc Network (MANET) is a convenient way wireless networking which presents many benefits in the communication process. The decentralized architecture of wireless networks invites many attacks due to its decentralized architecture. In paper [50], the authors have proposed an ANN classification technique for intrusion detection over MANET. The MITM attack is also possible in cloud environment. In this context, the authors of [51] have proposed a man-made consciousness-based structure to recognize the MITM attack on first attempt. The MITM attack can also be handled through cyber security mechanism. The cyber-attack primarily made possible during key exchange phase [52]. The key exchange process can be strengthened then by utilizing Elliptic Curve Cryptography (ECC) method[53][54].

3. SECURITY PROBLEM WITH WSN

WSN is an emerging trend for many advanced applications. The deployment of WSN can be stretched out from domestic

too harsh and hostile environment. Nowadays, the use of WSN can be found in several sectors of society like defense, agriculture, transportation, medical, industrial, etc. Though, WSN is so popular still it can be seriously vulnerable to the several security threats. So, this vulnerability needs immediate attention to avoid the negative consequences. The cyber-attackers can cause serious disasters by exploiting the weakness of WSN. The weakness of WSN can be defined as the resource constraint environment in terms of memory, energy, computational capacity etc. The type of attacks which are possible in WSN is:

- Man, in the middle (MITM)
- DDoS
- DOS
- Password attack
- Data injection

3.1 Intrusion Detection System (IDS)

The function of IDS can be defined as the monitoring on network transactions and to identify the malicious behaviors. The input parameters to IDS can be in two forms such as anomaly and signatures. In anomaly the behavioral pattern of transactions gets recorded, if any transaction deviates from the regular pattern then that can be included under suspicious activity. In case of signature based, each activity is assigned with a unique ID based template which is used to differentiate between legitimate users and fraudulent users.

4. PROPOSED WORK

In this paper, we propose and MITM-IDS system to detect the attackers. In this MITM-IDS the attacker is getting monitored based on signature-ID templates. The simulation has been carried out on a data set which contains both malicious and legitimates nodes ID. The deployed MITM-IDS is responsible to validate the authenticity of signatures of nodes. It differentiates between legitimates nodes and fraudulent nodes. Figure 3, illustrates the architecture of MITM-IDS functionality.

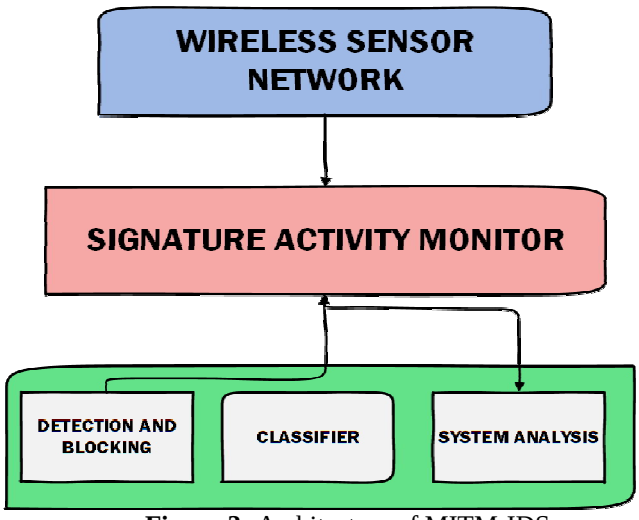

Figure 3: Architecture of MITM-IDS

According to this model, it able to differentiate between legitimate users and fraudulent user (attacker) by using the features of the MITM-IDS for WSN. The existing approaches for MITM are based on neural-network, genetic algorithms, fuzzy logic etc. are more complex enough which is not suitable for WSN. Because, the WSN is resource constraint architecture. The WSN network have limited resources and operates on battery. Additionally, the existing soft-computing based models are not efficient enough to handle voluminous attacks.The proposed MITM-IDS is working based on a centralized database network (CDN). The CDN contains the entire IDS for WSN setup. This helps to provide a strong back up by considering the resource constraint environment of WSN. The MITM-IDS uses network intrusion detection system (NIDS) and packet sniffer tools to examine the network traffic. The NIDS mostly driven by rules hence, the rules can be updated based on the situation. Instead of storing total log file, the NIDS captures only selective data based on the predefined rules. The integration of CDN and NIDS helps to create a resource of signatures.

In MITM-IDS with deep learning (DL) approach become more intelligent than the approaches based genetic algorithm, neural network, fuzzy logic, etc. The use of DL enhances the performance in comparison to the traditional approaches. The flexibility of learning in DL overcomes the drawbacks of the conventional approaches. The DL approach works smoothly both in homogeneous and heterogeneous environment. The accumulated data from various points are feed into DL programs to generate a refined signatures-based classification rules to catch the malicious activities. The DL based MITM-IDS analyzes the network by applying intelligent refined signature rules. The packet from WSN pass through a CrowdStrike application to WSN domain. The CDN controls all these switches of the network. The centralized view of network. The Long Short-Term Memory(LSTM) based DL approach enhances the performance of CDN.

Normally, the attackers don't try to crack the passwords or to access the root rather they use few well-known cyber-attack tools. Through these tools the attackers create duplicate signatures as the computer programs executes same block of instructions repeatedly. For this we have used CrowdStrike IDS software. Figure 4 illustrates the user interface of CrowdStrike Software.

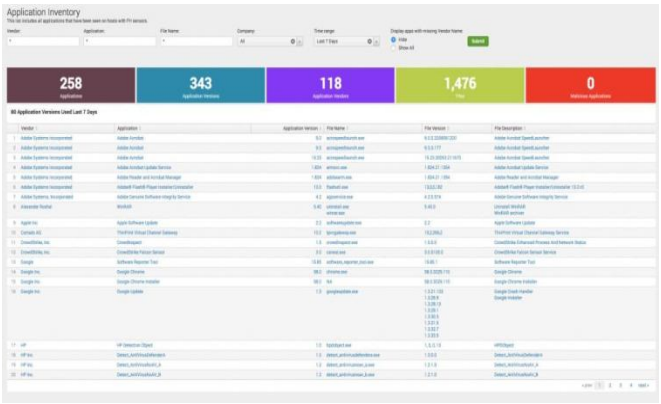

Figure 4: Interface of CrowdStrike IDS

4.1 LSTM

The LSTM neural network contain different blocks or cells. The cells are responsible for storing of information about the network activities. The LSTM maintains two states like hidden state and cell state. These two states getting operated through three functions like forget, input and output. These operations on these cells helps to identify manipulated behavior of cells. The input operation adds recent information into the cells. The output operation selects only required information from the cells. The forget operation removes the unnecessary information from the cells.

4.2MITM-IDS with CDN

The major components of MITM-IDS are:

- Operation Monitor (OM)
- Operation Analyzer (OA)
- Operation Classifier (OC)

The following units performs the following functions such as:

- Traffic Capturing
- Traffic Analyzer
- Feature Extraction
- Malicious Signature Detection

The accumulated statistical information through CrowdStrike application get passed to the OA. The working of MITM-IDS is represented in algorithmic manner. The OA analyzes the given input and extracts the suspicious signatures. The presence of CDN helps to creates a wide range of detection activity so that all possible attacks can be avoided.

Algorithm 1:

……

Input: Traffic Flow
Output: Malicious Signature Detection
Initiate: Traffic Capturing
Determine: Features (F)
Extract: Selected Features (SF)
Feed: SF → Classifier (*For Training*)
Run: Classifier
{Within time bound scenario} // Time Frame
If (Number of Suspicious Case ≥ Prefixed Threshold Value)
End If
Cancel: The Host
Else:
Repeat: All the steps with new time frame

Algorithm 2:

……

Input: Number of Suspicious Case
Output: Intrusion Detection
If (Suspicious Activity == Attack)
Raise: Alert
Remove: Suspicious Activities
End If
Else: False Flag
Terminate: The Process

4.3MITM-IDS Simulation

A 100-node based network has been presented for simulation in Figure 5. In the total network a particular node N9 was used as administrator which monitors the malicious activities over the network. The simulation has been done with RMATLAB2017. The language Python has been used along with script for the demonstration of performance of MITM-IDS. Initially, the CrowdStrike application reads the logged data from every layers of TCP-IP protocol stack. The extracted features from these logged details are used for feature extraction by using DL approach. This step is required to train the DL model with the association of CDN. The CDN provide the global view of the network. The OM, monitors the traffic flow within WSN. The CrowdStrike application provides the detail logged data for the analyzation of network behavior. The CDN generates the static data based on CrowdStrike performance.

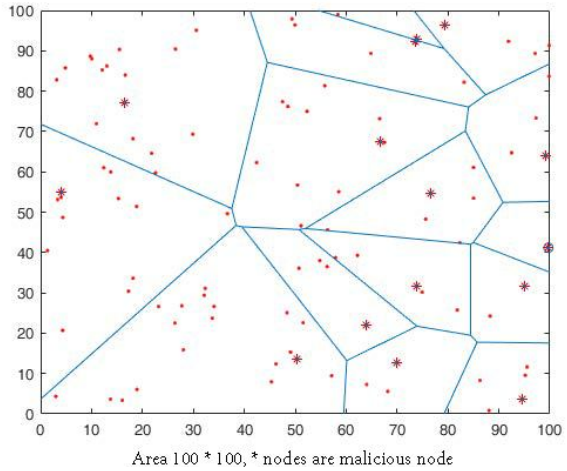

Figure 5: Deployment of both genuine node and malicious node in the different clusters of WSN.

4.4Result Discussion

The output of the proposed model is validated by considering two factors such as throughput and packet loss. Figure 6 illustrates the two colors, where red color represents the throughput with MITM-IDS and the green color represents the throughput without any security mechanism. Figure 7 illustrates the packet loss scenario where red color represents packet loss with MITM-IDS mechanism and green color represent the packet loss without any security mechanism. Both results have been obtained against the threshold value. The simulation results in Figure 6 shows that the throughput rate is high incased of proposed method. Same way Figure 7 shows that packet loss count is low in our proposed method. Throughput can be defined as the successful transmission of packets in a stipulated amount time. The term packet loss can be defined as the loss or failing of packets to reach its intended destination. High throughput and low packet loss are the attribute of healthy networking. The successful detection of attacks and fraudulent activity enhances the overall performances of the network.

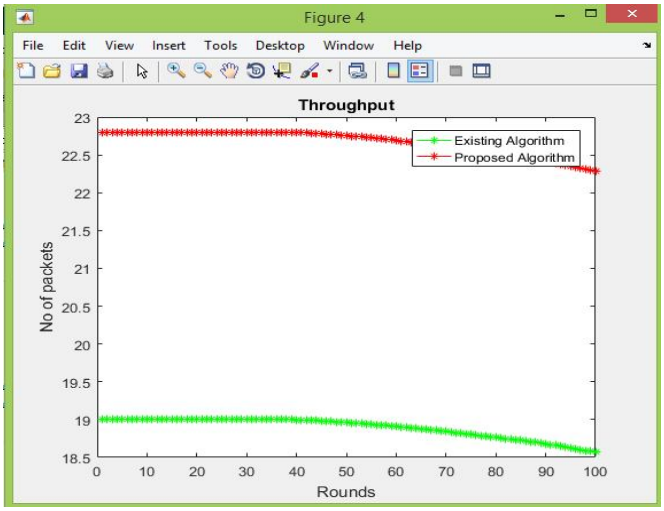

Figure 6: Throughout comparison

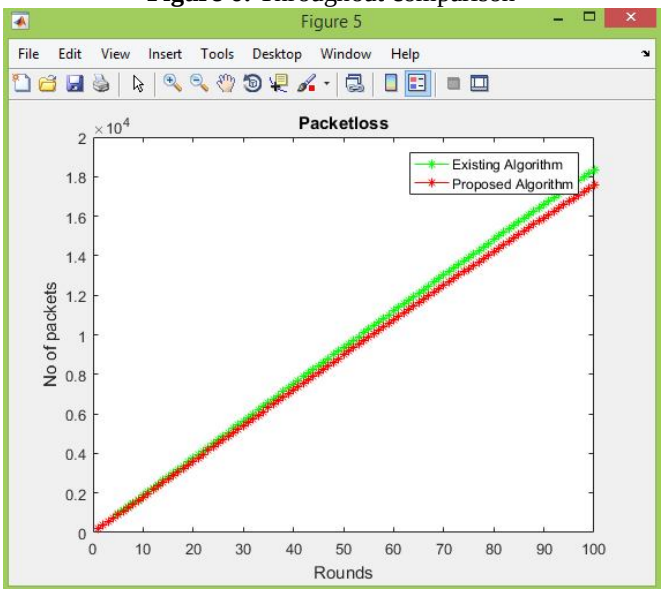

Figure 7: Packet loss comparison

5. CONCLUSION

The wireless sensor network can be homogeneous type or heterogeneous type. The deployed sensors sense the surrounding and accumulate the data. Further, the same data get forwarded to the base station. The resource constraint environment of WSN always makes vulnerable to the several types of attacks. The MITM attack is a more likely attack in WSN environment. In this paper, we have proposed and deep learning-based IDS to handle the MITM attacks. The simulation results show the performance of MITM-IDS in comparison to the non-security environment. The key strength of this model is it detects the malicious behavior with less time because of its less complexity.

REFERENCES

[1] M. BM and H. Mohapatra, "Human centric software engineering," *International Journal of Innovations &Advancement in Computer Science (IJIACS)*, vol. 4, no. 7, pp. 86-95, 2015.

[2] H. Mohapatra, C Programming: Practice, Vols. ISBN: 1726820874, 9781726820875, Kindle, 2018.

[3] H. Mohapatra and A. Rath, Advancing generation Z employability through new forms of learning: quality assurance and recognition of alternative credentials, ResearchGate, 2020.

[4] H. Mohapatra and A. Rath, Fundamentals of software engineering: Designed to provide an insight into the software engineering concepts, BPB, 2020.

[5] V. Ande and H. Mohapatra, "SSO mechanism in distributed environment," *International Journal of Innovations & Advancement in Computer Science*, vol. 4, no. 6, pp. 133-136, 2015.

[6] H. Mohapatra, "Ground level survey on sambalpur in the perspective of smart water," *EasyChair*, vol. 1918, p. 6, 2019.

[7] H. Mohapatra, S. Panda, A. Rath, S. Edalatpanah and R. Kumar, "A tutorial on powershell pipeline and its loopholes," *International Journal of Emerging Trends in Engineering Research*, vol. 8, no. 4, 2020.

[8] H. Mohapatra and A. Rath, "Fault tolerance in WSN through PE-LEACH protocol," *IET Wireless Sensor Systems*, vol. 9, no. 6, pp. 358-365, 2019. https://doi.org/10.1049/iet-wss.2018.5229

[9] H. Mohapatra, S. Debnath and A. Rath, "Energy management in wireless sensor network through EB-LEACH," *International Journal of Research and Analytical Reviews (IJRAR)*, pp. 56-61, 2019.

[10] H. Mohapatra and A. Rath, "Fault-tolerant mechanism for wireless sensor network," *IET Wireless Sensor Systems*, vol. 10, no. 1, pp. 23-30, 2020. https://doi.org/10.1049/iet-wss.2019.0106

[11] H. Mohapatra and A. Rath, "Detection and avoidance of water loss through municipality taps in india by using smart tap and ict," *IET Wireless Sensor Systems*, vol. 9, no. 6, pp. 447-457, 2019.

[12] M. Panda, P. Pradhan, H. Mohapatra and N. Barpanda, "Fault tolerant routing in heterogeneous environment," *International Journal of Scientific & Technology Research*, vol. 8, pp. 1009-1013, 2019.

[13] D. Swain, G. Ramkrishna, H. Mahapatra, P. Patra and P. Dhandrao, "A novel sorting technique to sort elements in ascending order," *International Journal of Engineering and Advanced Technology*, vol. 3, pp. 212-126, 2013.

[14] H. Mohapatra, "HCR using neural network," 2009.

[15] V. Nirgude, H. Mahapatra and S. Shivarkar, "Face recognition system using principal component analysis & linear discriminant analysis method simultaneously with 3d morphable model and neural network BPNN method," *Global Journal of Advanced Engineering Technologies and Sciences*, vol. 4, p. 1, 2017.

[16] R. Kumar, S. Edalatpanah, S. Jha, S. Gayen and R. Singh, "Shortest path problems using fuzzy weighted arc

length," *International Journal of Innovative Technology and Exploring Engineering,* vol. 8, pp. 724-731, 2019.

[17] R. Kumar, S. Jha and R. Singh, "A different approach for solving the shortest path problem under mixed fuzzy environment," *International Journal of fuzzy system Applications,* vol. 9, no. 2, pp. 132-161, 2020. https://doi.org/10.4018/IJFSA.2020040106

[18] R. Kumar, S. Jha and R. Singh, "Shortest path problem in network with type-2 triangular fuzzy arc length," *Journal of Applied Research on Industrial Engineering,* vol. 4, pp. 1-7, 2017.

[19] S. Broumi, A. Dey, M. Talea, A. Bakali, F. Smarandache, D. Nagarajan, M. Lathamaheswari and R. Kumar, "Shortest path problem using Bellman algorithm under neutrosophic environment," *Complex & Intelligent Systems,* vol. 5, pp. 409--416, 2019. https://doi.org/10.1007/s40747-019-0101-8

[20] R. Kumar, S. Edalatpanah, S. Jha, S. Broumi, R. Singh and A. Dey, "A multi objective programming approach to solve integer valued neutrosophic shortest path problems," *Neutrosophic Sets and Systems,* vol. 24, pp. 134-149, 2019.

[21] R. Kumar, A. Dey, F. Smarandache and S. Broumi, "A study of neutrosophic shortest path problem," in *Neutrosophic Graph Theory and Algorithms,* F. Smarandache and S. Broumi, Eds., IGI-Global, 2019, pp. 144-175.

[22] R. Kumar, S. Edalatpanah, S. Jha and R. Singh, "A novel approach to solve gaussian valued neutrosophic shortest path problems," *International Journal of Engineering and Advanced Technology,* vol. 8, pp. 347-353, 2019.

[23] R. Kumar, S. Edaltpanah, S. Jha, S. Broumi and A. Dey, "Neutrosophic shortest path problem," *Neutrosophic Sets and Systems,* vol. 23, pp. 5-15, 2018.

[24] R. Kumar, S. Edalatpanah, S. Jha and R. Singh, "A Pythagorean fuzzy approach to the transportation problem," *Complex and Intelligent System,* vol. 5, pp. 255-263, 2019. https://doi.org/10.1007/s40747-019-0108-1

[25] J. Pratihar, R. Kumar, A. Dey and S. Broumi, "Transportation problem in neutrosophic environment," in *Neutrosophic Graph Theory and Algorithms,* F. Smarandache and S. Broumi, Eds., IGI-Global, 2019, pp. 176-208.

[26] J. Pratihar, S. E. R. Kumar and A. Dey, "Modified Vogel's Approximation Method algorithm for transportation problem under uncertain environment," *Complex & Intelligent Systems (Communicated).*

[27] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. Parizi and G. Srivastava, "Security aspects of Internet of Things aided smart grids: A bibliometric survey," *Internet of Things,* pp. 100-111, 2019.

[28] S. Gayen, F. Smarandache, S. Jha and R. Kumar, "Interval-valued neutrosophic subgroup based on interval-valued triple t-norm," in *Neutrosophic Sets in Decision Analysis and Operations Research,* M. Abdel-Basset and F. Smarandache, Eds., IGI-Global, 2019, p. 300. https://doi.org/10.4018/978-1-7998-2555-5.ch010

[29] S. Gayen, F. Smarandache, S. Jha, M. Singh, S. Broumi and R. Kumar, "Introduction to plithogenic subgroup," in *Neutrosophic Graph Theory and Algoritm,* F. Smarandache and S. Broumi, Eds., IGI-Global, 2020, pp. 209-233.

[30] S. Gayen, S. Jha, M. Singh and R. Kumar, "On a generalized notion of anti-fuzzy subgroup and some characterizations," *International Journal of Engineering and Advanced Technology,* vol. 8, pp. 385-390, 2019.

[31] S. Gayen, F. Smarandache, S. Jha, M. K. Singh, S. Broumi and R. Kumar, "Introduction to plithogenic hypersoft subgroup," *Neutrosophic Sets and Systems,* vol. 33, p. Accepted, 2020.

[32] S. Gayen, S. Jha and M. Singh, "On direct product of a fuzzy subgroup with an anti-fuzzy subgroup," *International Journal of Recent Technology and Engineering,* vol. 8, pp. 1105-1111, 2019. https://doi.org/10.35940/ijrte.B1502.078219

[33] A. Behura and H. Mohapatra, "IoT Based Smart City with Vehicular Safety Monitoring," *EasyChair,* vol. 1535, 2019.

[34] Z. Xu, R. A. Sowah, K. B. Ofori-Amanfo, G. A. Mills and K. M. Koumadi, "Detection and Prevention of Man-in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in Artificial Neural Networks (ANN)," *Journal of Computer Networks and Communications, Hindawi,* p. 14, 1 2019.

[35] M. Aydos, Y. Vural and A. Tekerek, "Assessing risks and threats with layered approach to Internet of Things security," *Measurement and Control,* vol. 52, pp. 338-353, 2019.

[36] M. Saqib, F. Z. Khan, M. Ahmed and R. M. Mehmood, "A critical review on security approaches to software-defined wireless sensor networking," *International Journal of Distributed Sensor Networks,* vol. 15, p. 1550147719889906, 2019.

[37] F. Aliyu, T. Sheltami and E. M. Shakshuki, "A Detection and Prevention Technique for Man in the Middle Attack in Fog Computing," *Procedia Computer Science,* vol. 141, pp. 24-31, 2018. https://doi.org/10.1016/j.procs.2018.10.125

[38] F. Ahmad, A. Adnane, V. N. L. Franqueira, F. Kurugollu and L. Liu, "Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies," *Sensors,* vol. 18, 2018.

[39] F. Ahmad, A. Adnane and V. N. L. Franqueira, "A Systematic Approach for Cyber Security in Vehicular Networks," *Journal of Computer and Communications,* vol. 04, pp. 38-62, 2016.

[40] L. Rahman, "Detecting MITM Based on Challenge Request Protocol," in *2015 IEEE 39th Annual Computer Software and Applications Conference,* 2015.

[41] M. Chliah, G. Orhanou and S. E. Hajji, "New secure

routing method applications facing MitM attacks," in *2014 International Conference on Next Generation Networks and Services (NGNS)*, 2014.

[42] N. R. Samineni, F. A. Barbhuiya and S. Nandi, "Stealth and semi-stealth MITM attacks, detection and defense in IPv4 networks," in *2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, 2012.

[43] C. Ouseph and B. R. Chandavarkar, "Prevention of MITM attack caused by rogue router advertisements in IPv6," in *2016 IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, 2016.

[44] D. A. Abri, "Detection of MITM attack in LAN environment using payload matching," in *2015 IEEE International Conference on Industrial Technology (ICIT)*, 2015.
https://doi.org/10.1109/ICIT.2015.7125367

[45] M. A. Salam, "Dectability of MITM attacker in mobile sensor network," *International Journal of Advanced Computer Science*, pp. 99-103, 2013.

[46] L. Xiao, X. Wan, X. Lu, Y. Zhang and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?," *IEEE Signal Processing Magazine*, vol. 35, pp. 41-49, 9 2018.

[47] Z. (. Dong, R. Espejo, Y. Wan and W. Zhuang, "Detecting and Locating Man-in-the-Middle Attacks in Fixed Wireless Networks," *Journal of Computing and Information Technology*, vol. 23, p. 283, 2015.

[48] L. Wang and A. M. Wyglinski, "Detection of Man-in-the-Middle Attacks Using Physical Layer Wireless Security Techniques," *Wirel. Commun. Mob. Comput.*, vol. 16, p. 408–426, 3 2016.

[49] V. Kumar, S. Chakraborty, F. A. Barbhuiya and S. Nandi, "Detection of stealth Man-in-the-Middle attack in wireless LAN," in *2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, 2012.
https://doi.org/10.1109/PDGC.2012.6449834

[50] R. A. Sowah, K. B. Ofori-Amanfo, G. A. Mills and K. M. Koumadi, "Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in Artificial Neural Networks (ANN)," *Journal of Computer Networks and Communications*, vol. 2019, 2019.

[51] P. Chowdary, Y. Challa and J. Mukkamala, "Identification of MITM Attack by Utilizing Artificial Intelligence Mechanism in Cloud Environments," *Journal of Physics: Conference Series*, vol. 1228, p. 012044, 5 2019.

[52] N. Saqib, "Key exchange protocol for WSN resilient against man in the middle attack," in *2016 IEEE International Conference on Advances in Computer Applications (ICACA)*, 2016.

[53] R. R. Chintala, L. S. R. Janjanam, S. K. G and S. P. S, "FPGA Implementation of Katan Block Cipher for Security in Wireless Sensor Networks," *International Journal of Emerging Trends in Engineering Research*, vol. 7, no. 5, pp. 492 - 497, 2019.
https://doi.org/10.30534/ijeter/2019/157112019

[54] K.Sreelatha and D. V. K. Reddy, "A Comprehensive review of Security Challenges for Data Deduplication and Integrity Auditing," *International Journal of Emerging Trends in Engineering Research*, vol. 7, no. 5, pp. 725 - 732, 2019.
https://doi.org/10.30534/ijeter/2019/527112019