IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Mathematical Modelling of Engineering Problems
Vol. 10, No. 2, April, 2023, pp. 663-670
Journal homepage: http://iieta.org/journals/mmep

Zigbee-Based Intrusion Detection System for Wormhole Attack in Internet of Things

Snehal Bhosale[1*], Harshal Patil[2]

[1] E&TC Department, Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune 412115, India
[2] Computer Science Department, Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune 412115, India

Corresponding Author Email: snehal.bhosale@sitpune.edu.in

https://doi.org/10.18280/mmep.100237

Received: 29 November 2022
Accepted: 13 March 2023

Keywords:
Arduino, IDS, IoT, security, wormhole attack, Zigbee, Arduino

ABSTRACT

Internet of Things (IoT) network security is impacted significantly by routing errors present in IoT network. In IoT, routing errors caused by wormhole attacks affect badly on network performance. Out of several attacks, the wormhole attack is one of the most uncompromising attacks in IoT network. The wormhole attack can be launched using any protocol and also against the encrypted traffic hence it is very challenging to address it. In addition to altering routing algorithms by introducing incorrect routes, the wormhole attack also attacks location-dependent protocols, making routing algorithms useless. This paper presents the development of an Intrusion Detection System (IDS) for detecting and removing wormhole attack. Temperature sensors, Zigbee communication module, and Arduino modules are used in the implementation of the IDS for the detection of wormhole attacks with hardware. In order to detect attacks, a sudden increase in transmitted packets and changes in routing tables are taken into account. In the proposed system, the Received Signal Strength Indicator (RSSI) values of transmitted packets are used to detect the attack and attacker nodes.

1. INTRODUCTION

Internet of Things (IoT) has grown rapidly in recent years, making it possible to integrate a wireless network of sensors into existing infrastructures through internet access. The majority of researchers in this field estimate that there will be over 30 billion connected devices by 2025. IoT is used in many demanding applications like smart homes, smart cities, smart healthcare, smart agriculture and smart grids [1, 2].

IoT networks consist of multiple devices with different security features. Hence maintaining information security is challenging, resulting in a larger security gap. In addition, it is difficult to implement security measures, such as strong cryptographic algorithms, because IoT devices have restricted processing power and memory due to their resource-constrained nature. While numerous research studies have demonstrated vulnerabilities and security threats associated with IoT network, the potentially damaging effect is on the integrity, availability, and confidentiality of the information [3]. Many security attacks are inserted in IoT network to cause unwanted behaviours in IoT elements. Due to its importance for national security, e-commerce and data protection, securing the network infrastructure has become a high priority [4, 5].

In IoT, the network layer is a target of some of these threats like sinkhole attack, selective forwarding attack and wormhole attack. Sinkhole and selective forwarding attacks modify the data and intercepts the network in real-time. A wormhole attack disrupts routing processes by inserting fake routing information and incorrect routing paths into legitimate nodes [6-8]. Among all wormhole attack is one of the most dangerous attacks taking place at the network layer. In order to protect end users' privacy and data from wormhole attacks, we need to address and reduce these security gaps. In this paper, we have developed a system that detects the presence of wormhole attack in the IoT network [9, 10]. The proposed system IoT network uses 6LoWPAN [11, 12], RPL [13-15] and AODV protocol for communication [16-18].

This research paper demonstrates the detection of wormhole attack with physical implementation using hardware components. As network attacks become more complex and sophisticated, stronger and more effective solutions are required. There has been a noticeable decline in the performance of security software in recent years because of the increased amount of data that needs to be processed. In order to overcome this performance gap, hardware units can be used to accelerate security task realization. This research paper describes the hardware implementation of wormhole attack detection.

For hardware implementation, we have used temperature sensors LM35 [19], Zigbee modules [20] as communication standard, Arduino-nano and Arduino-mega boards as controllers that run the attack detection algorithms [21, 22]. In IoT, a wormhole attack is detected by considering the symptoms like an abrupt increase in transmitted packets and frequent changes in the routing table. When the attack is inserted in the network, attacker nodes misguide the legitimate nodes to send data packets through them which may cover long distances. The presence of attack ultimately reduces the strength of the signal by lowering the Received Signal Strength Indicator (RSSI) value to the threshold value. If the RSSI values are below -60 dBm then the attack is confirmed. The Arduino processor declares the existence of the wormhole attack along with the attacker node ID. Once attacker nodes

are identified then they are removed from the network.

A range-based localization is an easy and cost-effective localization technique that measures RSSI to estimate distance. It is mostly used from 0 to -120 dBm. When the RSSI value is closer to 0, it indicates the good quality of the received signal [23-27]. Each sensor node has a radio that measures the signal strength, so when the data is transferred between nodes, the RSSI values can also be shared. As it does not require any extra hardware, the existing network will not be modified and the size will remain the same. Eq. (1) gives the distance of transmitter and receiver nodes where the strength of the signal is used to calculate it. If the signal is weakened, the distance estimation changes through which we can understand the presence of a wormhole attack. In this case, the RSSI value represents received power, and N represents constant, based on the environmental factor between 2 to 4. In current experimentation, it is considered as '2'.

$$\text{Distance} = 10^{\left(\frac{\text{Transmitted Power}-\text{Received Power}}{10*N}\right)} \quad (1)$$

1.1 Wormhole attack

In the presence of a wormhole attack, a tunnel between two distant nodes is formed to pretend they are closer to each other and only one hop away. When a packet is transmitted, attacker nodes attract the traffic by advertising less hop count and when packets come at either of the nodes, they involve intermediate legitimate nodes for packet transmission. Despite not being part of the communication, these legitimate nodes get involved in transmission due to the wormhole attack and drain their batteries which is not good for resource-constrained nodes in IoT. It is difficult to detect this attack at an early stage. Its presence is identified after a significant loss. The key to preventing wormhole attacks is to design strong IDS systems that detect the attack and the attacker nodes as soon as possible [28-30]. In this paper, a wormhole attack detection system using hardware is discussed which detects wormhole attack efficiently and gives a good True Positive Detection Rate and optimum False Positive Detection Rate. Furthermore, it gives a very good result when we calculate accuracy, Mathew's coefficient of correlation, and F1-score.

As a result of wormhole attacks, path delay between networks increases and hop count decreases abruptly. In presence of wormhole attack, data packets are received from faraway nodes and the number of neighbor requests is increased. Additionally, some links are more frequently utilized than others. During the development of the IDS for detecting wormhole attacks, these symptoms are taken into consideration. In our system, we have considered the RSSI value of the received packet. As this value changes when the above symptoms are present in the network. The strength of the signal is checked when there is no attack. It is compared with the strength of the received packet when a wormhole attack is present. When there is a change in the RSSI value beyond the threshold value, the presence of wormhole attack is marked.

The organization of the rest of the paper is as follows: Section 2 discusses hardware implementation of the wormhole attack detection. In section 3, we discuss about the simulation of nodes in the 'Zigbee simulation' window. Section 4, 'Wormhole attack activation and detection algorithm' explains the algorithms for the activation and detection of wormhole attack. In section 5, 'Experimental set-up', the hardware interfacing is discussed. Section 6 contains a brief conclusion of the final part of the paper.

2. HARDWARE IMPLEMENTATION

2.1 Related work

According to Amish and Vaghela [31], wormhole attacks can be detected by counting the number of hops and comparing the delay between the origin and destination nodes. Using modifications to the DSR routing protocol, Qazi et al. [32] propose automatically calculating the Round Trip Time (RTT) delay value between source and destination nodes during a particular period. According to Bhagat and Panse [33], the transmission force from a source node can be calculated using a modified version of the AODV routing protocol. In alternative modifications of the AODV protocol [34], the RREQ packet contains the hash of the hop addresses and hop counts along the path from source to destination. With the use of statistical calculation and node connectivity, Zheng et al. [35] present a wormhole detection algorithm.

The above studies assessed the effectiveness of different detection and prevention algorithms in WSNs and IoT networks by evaluating the impact of wormhole attacks in simulation environments. Due to the lack of devices with the required features, they cannot be implemented in real environments because they are based on simulations of routing protocol attacks. It is necessary to develop intrusion detection systems for real sensor nodes in the wake of existing and potential cyber threats to IoT networks. Lastly, since most IoT security studies rely on simulation results, future characterizations of IoT network threats should match actual devices, in order to create real-world security solutions.

To detect wormhole attack using hardware, the symptoms of the abrupt changes in route records and increase in transmitted packets are considered as hypotheses to detect the wormhole attack. Also, if no new node is joining after the beacon packet is sent by any node then that node is considered a suspicious node. For hardware implementation, Zigbee as the communication standard, LM 35 as temperature sensor, Arduino-nano and Arduino-mega boards for processing are used. By using the RSSI value, the distance of the suspicious node from the victim node is calculated. If the suspicious node is out of range than the victim node, the attacker node is identified and removed from the network.

This paper covers the hardware implementation of the wormhole attack detection system without and with a wormhole attack where Arduino-nano and Arduino-mega boards are used as the attacker nodes and coordinator node respectively. We have implemented an IDS based on hardware after achieving good results with simulation [30]. In the implemented system, Coordinator and end devices are used to form a ZigBee network.

2.2 Block diagram of experimental setup for attack detection

The connection diagram of the experimental set-up for wormhole attack is as shown in Figure 1. The diagram shows the sensor nodes (LM35) are connected to the coordinator node through the ZigBee module. The temperature data is collected by the coordinator node along with its RSSI value. Without attack, packets are transmitted through the default route which is the shortest route that gives RSSI value of more than -40 dBm. The accepted RSSI values are higher than -60

dBm. The threshold value considered for the attack detection is -60 dBm.

When the attacker node is inserted in the network, it sends the beacon frame to discover the coordinator node, network ID and addresses of devices of the network. The attacker node then selects the victim node and by capturing its address and frequency, it catches the victim node's packets to modify the data. The attacker node extracts the sensitive information as a source address, a destination address, routing information from the victim node and modifies it to form a wormhole tunnel. It mainly changes the hop-count and other information. Hence destination node will receive the attacker node's data. The procedure is repeated indefinitely by increasing the victim nodes from the network.

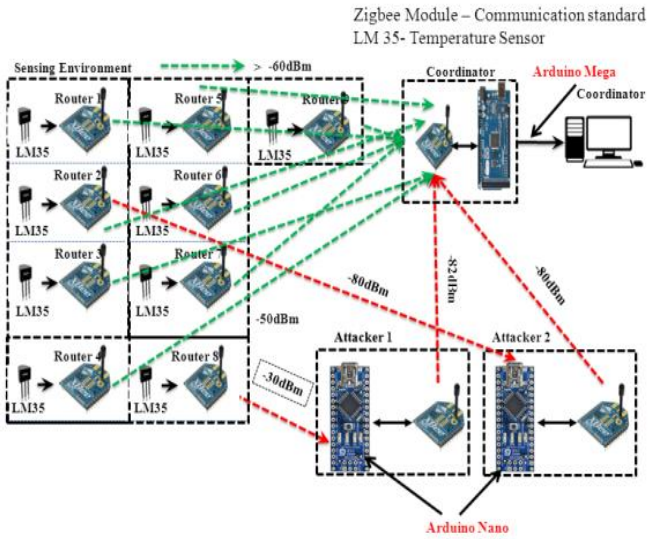

Figure 1. Experimental setup for attack detection

When Attacker nodes are added to the network, the temperature data by all sensor nodes are transmitted to the coordinator node through attacker nodes which reduces the RSSI value below -60 dBm. This happens because attacker nodes send the data packets through them, resulting in a long route. That ultimately weakens the strength of the signal. Attacker nodes advertise less hop-count to the destination through it. As shown in the Figure 1, the RSSI values through attacker nodes are around -80 dBm which are not acceptable. After checking the routing table, it is observed the specific nodes are part of the communication unnecessarily and reduces the RSSI values of the transmitted packets. These nodes are added to the blacklist of the database and communication through those nodes is avoided.

3. SIMULATION OF NODES IN ZIGBEE SIMULATION WINDOW

Figure 2 shows the connection diagram of the nodes in the ZigBee simulation window. It shows one coordinator node and other normal nodes having physically connected. If any connection problem is present, then this window helps to identify it.

3.1 RSSI values variations without and with attack

Figure 3(a), shows the response of RSSI values without and with the attack. In Figure 3(a), when there is no attack, RSSI values are higher than -60 dBm and no loss of packets is observed with 100% efficiency.

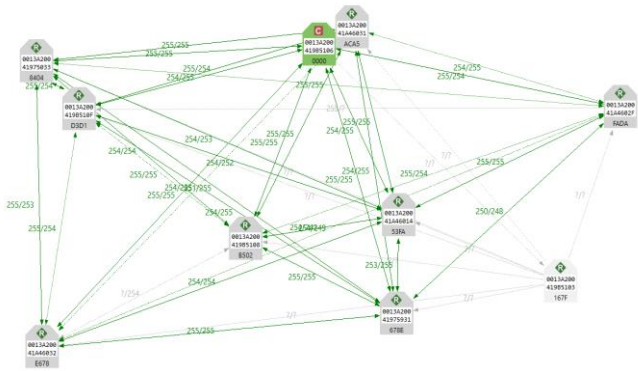

Figure 2. Connection diagram of the nodes in ZigBee simulation window

Figure 3(a). RSSI Values when no attack

Once the attack is launched, the response is observed as shown in Figure 3(b) where RSSI values reduce and give the output lower than -80 dBm with packet loss and efficiency as 77%.

Figure 3(b). RSSI values in presence of attack

4. WORMHOLE ATTACK ACTIVATION AND DETECTION ALGORITHM

4.1 Wormhole attack activation

i. **Attacker insertion:**
In this phase, the attacker node sends a beacon frame to discover the coordinator node, routing path, network ID and devices addressed in the network.

ii. **Capturing the packet:**

At this step, the attacker selects the victim node and captures the node address, frequency, the network address and channel, and catches the transmitted packets to modify essential data.

iii. Desired traffic:

A packet is sent from or to the victim node defined by the attacker, it is known as desired traffic. In desired traffic, the attacker node extracts the information of data addressing and compares it with the victim node's address.

iv. Modifying routing packet:

Once the attacker extracts most of the sensitive information from the victim node, the routing information of the captured packet is changed to form a tunnel. It modifies sequence number, hop-count and relay list from route record information.

v. Modifying and forwarding the data packets:

At this stage of the attack, the attacker node modifies routing information; hence destination node will receive the attacker node's data. This process is repeated in indefinitely by inserting fake routes for modification of data packets to maintain the wormhole tunnel.

4.1.1 Algorithm for attack activation

The beacon frame discovers the coordinator node, routing path, network ID and devices addressed in the network. Algorithm 4.1 explains the steps of attack activation.

Algorithm 4.1 Algorithm for activation of attack

```
1)  if packet is source_routing_packet then
        if packet is victim_address then
2)          end new_packet with victim_address
3)          new-packet is injected
4)      else normal traffic
5)      endif
6)  if src_addr = victim address then
7)    extract critical information
8)    Change new_packet.hop-count to 0
9)    new_packet.src address = victim address
10)   new_packet.relay list
11)   new_packet.destn address= victim address
12) else normal traffic
13)   if compare (pkt, victim_address) then
14)       pkt.data = new_data
  //destination node receives attacker node data by
  adding fake routes in the network
15)  endif
16) endif
        17) endif
```

4.2 Wormhole attack detection

i. Duplication of routing packets

Source routes of ZigBee devices are updated when the packet is received by the destination or requested a Network Discovery (ND) command. For every modified packet transmitted from source to destination, a false route is inserted that makes nodes receive two source routing packets. Detecting wormhole attacks in the network is done by observing the symptoms like the abrupt changes in route records and the increase in packets transmitted.

ii. The request for multiple beacon frames

In ZigBee/ IEEE 802.15.4 network, 'beacon frames' are sent in the network which is responded by a router and Coordinator when new nodes join the network. But when a suspicious node sends 'beacon frames', no new node joins the network. To identify the attack, the monitoring system could be maintained which detects the presence of the attack.

iii. Link-status packets and neighborhood table

In the ZigBee network, link-status packets are sent regularly to maintain the first half neighbor table. Link status packets cannot be shared by remote nodes. In order to detect the wormhole attack, previous link status messages of nodes with zero route records can be checked. An attack is identified if there are no previous link status messages. If the link status messages are already shared by the nodes which are involved in the transmitted packet, then the existence of wormhole attack is confirmed. The steps for attack identification are explained in algorithm 4.2.

4.2.1 Algorithm and flowchart for attack detection

The following Section gives the algorithm and flowchart for wormhole attack detection.

Algorithm 4.2 Attack detection algorithm

```
1)  if packet is received by destination then,
2)    if network discovery command is requested then
3)      zigbee_src_route is updated
4)    endif
       // for every modified packet,
5)    if packet transmitted for zigbee_src to zigbee_destn,
        then false route is inserted and node receives two
        src_routing_packet
6)      if abrupt modification in route_record = true and
          abrupt increase in transmitted packet = true then
7)        generate alert for attack
8)      else normal traffic
9)    endif
10)  for new beacon frame is in network then
11)     if new node has joined then
12)       normal traffic
13)     else alert for attack
14)     endif
15)  end for
16)     if previous link_status_msg available then
17)       normal traffic
18)     else confirm the attack in network
19)       check RSSI_Reg_Value for attacker nodes
20)       if rssi for nodes of suspicious link is < -70 dBm
            then confirm attacker nodes.
21)       else normal traffic
22)       endif
23)     endif
24)   endif
25) endif
```

The discussed method is formed by combining many subtasks that can be modified as per the need of the network. At the initial stage, the network interface is used to capture the packets where these packets are filtered and extraction of relevant transmission and reception of data is made at the data extraction module. Further, with filtering rules, a comparison is made where IDs (Identifiers) of known nodes are sent to the white list and suspicious nodes IDs are sent to the blacklist. With detection criteria, RSSI values are used as a signature to identify whether traffic is malicious. If malicious activity is observed, an alert is generated.

4.3 Wormhole attack generation/detection using Arduino and Zigbee module

Wormhole Attack Generation and Detection using Arduino and ZigbeeModulecovers three steps as Router Initialization, Attacker Node Activation and attacker Detection. The maximum RSSI value collected in 15 minutes is stored and compared with RSSI values after the insertion of the attacker nodes. The presence of an attack is declared if the next RSSI value is lower than the stored maximum value of the RSSI which is -60 dBm. By using 16 bits address attacker node is identified. The attacker node also is a part of the system by using its PAN ID the way legitimate nodes are added to the network.

4.3.1 Wormhole attack detection set-up

We have considered 20 nodes for hardware implementation where the proposed algorithm is applied on. For the first 10 nodes, a single attacker node is considered. When the number of nodes is increased from 11 to 20, we increased the attacker nodes from 1 to 2. Similarly, as the network size increases, attacker nodes can be increased accordingly to check the efficiency of the proposed model. The system runs twice the number of nodes which is known as no. of iterations as shown in Table 1. We iterate the system to get the correct prediction.

5. EXPERIMENTAL SET-UP

In the absence of an attack, temperature from the sensors with their node ID and RSSI values is observed. A coordinator node monitors the activity of all other nodes in the network. These nodes are identified with their unique hardware ID. The coordinator node and other nodes share the same PAN ID as they are part of a single network. Attacker nodes use the same PAN ID to enter the network. When they become part of the system, they advertise that they are closer to the coordinator node and other nodes can transmit the data through them. When the RSSI of the packets are sent through the attacker nodes, the RSSI value reduces which is an indication of the longer route than the original route.

Figure 4 shows the connection of legitimate nodes, the border router and the attacker node. When the attacker node is inserted in the network, it gets immediately detected. In the set-up, ten nodes act as legitimate nodes, two attacker nodes and one border router node are used. When the RSSI value reduces than -70 dBm, the presence of attack is declared. With the help of the hardware address of the attacker node, attacker nodes are identified.

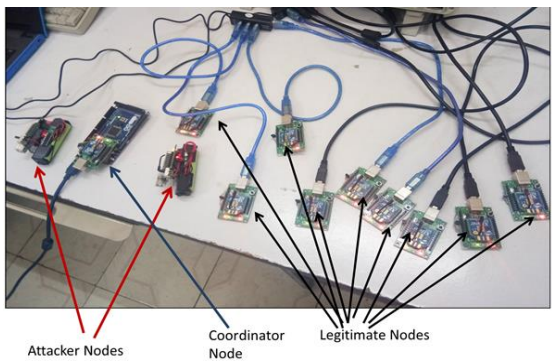

Figure 4. Attack detection with hardware implementation

5.1 Results and observations

To check the effectiveness of the proposed system, we have checked the Attack Detection Rate and Security Evaluation Metrics. We have taken the base of the Confusion Matrix to calculate these values. It is discussed in the next section.

5.1.1 Confusion matrix

We have used a confusion matrix to check the performance of the implemented IDS. The confusion matrix is shown in Figure 5.

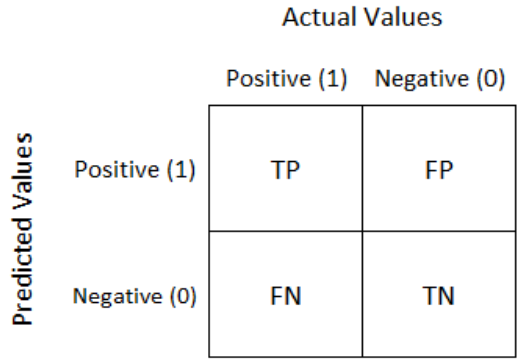

Figure 5. Confusion matrix

As shown in the matrix there are two classes: Actual and predicted. Based on the outcome we get four outputs. Those are,

- TP: True Positive: Predicted values correctly predicted as actual positive
- FP: Predicted values incorrectly predicted an actual positive. i.e., Negative values predicted as positive
- FN: False Negative: Positive values predicted as negative
- TN: True Negative: Predicted values correctly predicted as an actual negative

These values are used to calculate the Accuracy, F1-score and Mathews Coefficient of Correlation (MCC) of the implemented IDS as discussed in the next section.

5.1.2 Attack detection rate

The set-up has run from 3 to 20 nodes to observe the True-Positive Detection Rate (TPR) and False-Positive Detection Rate (FPR). It is noted that in all cases system has detected wormhole attack with 100% accuracy. Thus a conclusion is made that the implemented system is solved the purpose of wormhole attack detection.

In a few cases, where number of nodes is more, the implemented system gives the indication for presence of the attack where in reality there is no attack is present. This increases the FPR [36].

For attack detection, various parameters are considered such as, TPR, FPR, Accuracy, F1-score, MCC. These terms are calculated as shown in below equations.

$$TPR = \frac{TP}{TP+FN} \quad (2)$$

where, TP is True positive which means attack is correctly identified. FN is False Negative that means though attack is present but it is not identified. Ideally TPR must be 100% or nearer to it.

Table 1. Detection rate for hardware implementation and security analysis

No. of nodes	No. of Attacker Nodes	No. of iterations	Attack Activated	TP	FN	FP	TN	TPR	FPR	Accuracy	F1 Score	MCC
3	1	6	3	3	0	0	3	1	0	1.0000	1.0000	1.0000
6	1	12	5	5	0	0	7	1	0	1.0000	1.0000	1.0000
10	1	20	9	9	0	1	10	1	0.091	0.9500	0.9474	0.9045
15	2	30	15	15	0	2	13	1	0.133	0.9300	0.9375	0.8745
20	2	40	18	18	0	3	19	1	0.143	0.9250	0.9231	0.8567

where,
TP -Attack detected
FN - Attack not detected
FP - No attack still attack detected
TN -No attack no Detection
TPR - True-Positive Detection Rate
FPR - False Positive Detection Rate

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}} \tag{3}$$

where, FP is False Positive that means the system predicts the presence of attack when there is no attack present. And TN is True Negative which means there is no attack and system has predicted the absentee of attack correctly. Ideally, TPR must be 0% or nearer to it.

For hardware implementation, the network is formed with legitimate nodes, attacker nodes and one coordinator node. For experimentation, the number of legitimate nodes is considered from 3 to 20 and the developed algorithm is applied on networked nodes. Table 1 gives the observations for said number of nodes. After experimentation, TPR and FPR are calculated as per Eqns. (2) and (3) respectively. It is observed and concluded that TPR in all cases is 100%. The graph shown in Figure 6 elaborates the attack detection rates. Here we can see that TPR is 100% (Which is ideal) for all the cases which indicates that for the number of nodes from 3 to 20, every time attack is present it is detected. However, FPR has increased slightly as nodes increased (Ideally it must be 0), indicating that as network size increases, falsely identified attackers are also increasing.

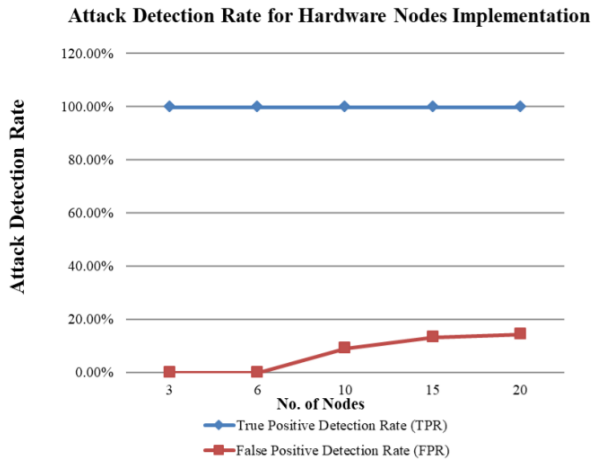

Figure 6. Detection rates for hardware implementation

- **Security evaluation metrics**

We have considered Accuracy, F1 score and Mathews Coefficient of Correlation (MCC) to evaluate the wormhole attack detection IDS under the Security Evaluation Technique [36-38].

i. **Accuracy:** Accuracy is how effectively wormhole attack is detected. It is given by Eq. (4).

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \tag{4}$$

ii. **F1-Score:** The harmonic mean of recall and precision is F1-score. When it is 1, precision and recall are perfect. Else when it is 0, they are worst. It is given by Eq. (5).

$$\text{F1 Score} = \frac{2*\text{TP}}{2*\text{TP+FP+FN}} \tag{5}$$

iii. **MCC:** MCC gives correlation between actual and predicted wormhole nodes which has range from -1 to 1. When MCC has value nearer to 1 it indicates better efficiency.

$$\text{MCC} = \frac{\text{TP+TN+FP+FN}}{\sqrt{(\text{TP+FP})*(\text{TP+FN})+(\text{TN+FP})*(\text{TN+FN})}} \tag{6}$$

5.1.3 Security-based metrics

Accuracy, F1 score and Mathew's correlation coefficient (MCC) are calculated using Eqns. (4), (5) and (6) respectively by referring the values from Table 1. The security-based metrics analysis is as shown in Figure 7.

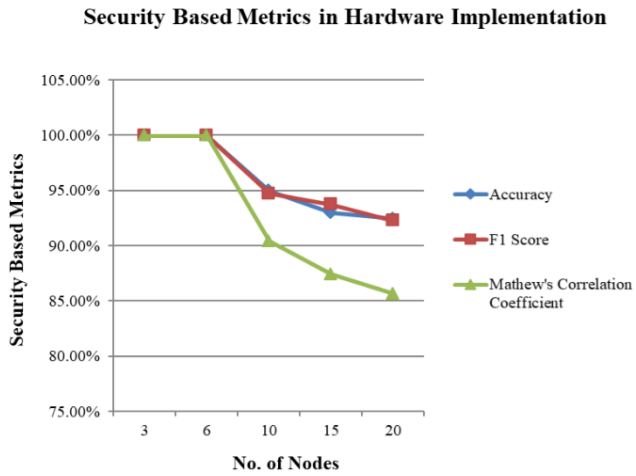

Figure 7. Analysis of security-based metrics

The average value of Accuracy is 96%, whereas the average value of the F1 score and MCC is 96.16% and 92.71% respectively. In summary, these values indicate that the designed IDS works well at detecting the wormhole attack. Based on Figure 5 and Figure 6, we can conclude that the research carried out in this paper provides the most efficient means of detecting wormhole attack. In this example, we obtained optimum values for TPRs and FPRs. We also got very good results for accuracy, F1 score and MCC.

6. CONCLUSION AND FUTURE SCOPE

This paper focuses on two events: First is Attack Activation Technique and second is Attack Detection Technique. A wormhole attack detection system is implemented with temperature sensors LM35, Zigbee networks as communication standard, and Arduino-nano and Arduino-mega boards as controllers that run the attack detection algorithms. For the wormhole attack activation in the network, the attack starts capturing the interesting data and modifies the routing information of victim nodes. In order to detect wormhole attacks, changes in the routing table and an abrupt increase in transmitted packets are monitored. Also, a check of beacon frames is maintained because beacon frames are transmitted when a new node is joined in the network. However, when an attacker node sends the beacon packet, no new node joins the network. So with these symptoms attack is identified and malicious nodes are removed from the routing table.

This paper covers interfacing of all physical elements and their working for attack detection. The overall observation of this experimentation is that the implemented method gives 100% TPR and 7.34% FPR. The results for accuracy, F1 score and MCC are 96%, 96.16% and 92.71% respectively. The obtained result proves that the proposed system is effective in identification of wormhole attack present in the network. With a few modifications, the developed system can detect other attacks in IoT networks in addition to wormhole attacks. If a dedicated chipset with minimum memory is used, the size could be further reduced by reducing the overall project's cost and energy consumption. To design a new chipset with support of IoT protocols and various communication standards is one more future scope of the implemented methods.

REFERENCES

[1] Nguyen, K.T., Laurent, M., Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. Ad Hoc Networks, 32: 17-31. https://doi.org/10.1016/j.adhoc.2015.01.006

[2] Kumar, S., Tiwari, Zymbler, M. (2019). Internet of Kumar, S., Tiwari, P., Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: A review. Journal of Big Data, 6(1): 1-21. https://doi.org/10.1186/s40537-019-0268-2

[3] Khan, M.A., Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82: 395-411. https://doi.org/10.1016/j.future.2017.11.022

[4] Hernandez, G., Arias, O., Buentello, D., Jin, Y. (2014) SmartNest Thermostat: A Smart Spy in Your Home. Black Hat USA: Las Vegas, NV, USA.

[5] Trappe, W., Howard, R., Moore, R.S. (2015). Low-energy security: Limits and opportunities in the Internet of Things. IEEE Security & Privacy, 13(1): 14-21. https://doi.org/10.1109/MSP.2015.7

[6] Tahboush, M., Agoyi, M. (2021). A hybrid wormhole attack detection in mobile ad-hoc network (MANET). IEEE Access, 9: 11872-11883. https://doi.org/10.1109/ACCESS.2021.3051491

[7] Bhosale, S.D., Sonavane, S.S. (2018). Wormhole attack detection in Internet of Things. International Journal of Engineering & Technology, 7(2.33): 749-751.

[8] Sahu, M., Sethi, N., Das, S.K. (2022). Secure data transmission in wireless sensor networks with secure system for identification of trusted route with node behavior analysis. Revue d'Intelligence Artificielle, 36(2): 289-295. https://doi.org/10.18280/ria.360213

[9] El-Hajj, M., Chamoun, M., Fadlallah, A., Serhrouchni, A. (2017). Analysis of authentication techniques in Internet of Things (IoT). In 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, pp. 1-3. https://doi.org/10.1109/CSNET.2017.8242006

[10] Shang, W., Yu, Y., Droms, R., Zhang, L. (2016). Challenges in IoT networking via TCP/IP architecture. NDN Project.

[11] Verma, A., Ranga, V. (2020). Security of RPL based 6LoWPAN networks in the Internet of Things: A review. IEEE Sensors Journal, 20(11): 5666-5690. https://doi.org/10.1109/JSEN.2020.2973677

[12] Kasinathan, P., Pastrone, C., Spirito, M.A., Vinkovits, M. (2013). Denial-of-service detection in 6LoWPAN based Internet of Things. 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France, pp. 600-607. https://doi.org/10.1109/WiMOB.2013.6673419.

[13] Challa, R.K., Rao, K.S. (2022). Resource based attacks security using RPL protocol in Internet of things. Ingénierie des Systèmes d'Information, 27(1): 165-170. https://doi.org/10.18280/isi.270120

[14] Simoglou, G., Violettas, G., Petridou, S., Mamatas, L. (2021). Intrusion detection systems for RPL security: A comparative analysis. Computers & Security, 104: 102219. https://doi.org/10.1016/j.cose.2021.102219.

[15] Perrey, H., Landsmann, M., Ugus, O., Schmidt, T.C., Wählisch, M. (2013). TRAIL: Topology authentication in RPL. arXiv preprint arXiv:1312.0984. https://doi.org/10.48550/arXiv.1312.0984

[16] van Glabbeek, R., Höfner, P., Portmann, M., Tan, W.L. (2016). Modeling and verifying the AODV routing protocol. Distributed Computing, 29: 279-315. https://doi.org/10.1007/s00446-015-0262-7

[17] Xin, H.M., Yang, K. (2015). Routing protocols analysis for Internet of Things. 2015 2nd International Conference on Information Science and Control Engineering, Shanghai, China, pp. 447-450. https://doi.org/10.1109/ICISCE.2015.104

[18] Sharma, R., Sharma, P. (2016). Detection and prevention of wormhole attack in MANETs: A review. International Journal of Science, Engineering and Technology Research (IJSETR), 5(5).

[19] https://www.alldatasheet.com/view.jsp?SearchwordLm35%20datasheet&gclid=EAIaIQobChMI47jFldW16AIVSo2PCh13gADOEAAYASAAEgKvsfD_BwE, accessed on June 22, 2022.

[20] Hebel, M., Bricker, G., Harris, D. (2010). Getting started with XBee RF modules. Parallax Inc, 30.

[21] http://eprints.polsri.ac.id/4598/8/File%20VIII%20%28Lampiran%29.pdf, accessed on June 22, 2022.

[22] https://components101.com/microcontrollers/arduino-nano, accessed on June 22, 2022.

[23] Li, G., Geng, E., Ye, Z., Xu, Y., Lin, J., Pang, Y. (2018). Indoor positioning algorithm based on the improved RSSI distance model. Sensors, 18(9): 2820. https://doi.org/10.3390/s18092820

[24] Singh, N., Choe, S., Punmiya, R. (2021). Machine

learning based indoor localization using Wi-Fi RSSI fingerprints: An overview. IEEE Access, 9: 127150-127174. https://doi.org/10.1109/ACCESS.2021.3111083

[25] Shue, S., Johnson, L.E., Conrad, J.M. (2017). Utilization of XBee ZigBee modules and MATLAB for RSSI localization applications. In SoutheastCon 2017, Concord, NC, USA, pp. 1-6. https://doi.org/10.1109/SECON.2017.7925305

[26] Yiu, S., Dashti, M., Claussen, H., Perez-Cruz, F. (2017). Wireless RSSI fingerprinting localization. Signal Processing, 131: 235-244. https://doi.org/10.1016/j.sigpro.2016.07.005

[27] Savazzi, P., Goldoni, E., Vizziello, A., Favalli, L., Gamba, P. (2019). A Wiener-based RSSI localization algorithm exploiting modulation diversity in LoRa networks. IEEE Sensors Journal, 19(24): 12381-12388. https://doi.org/10.1109/JSEN.2019.2936764

[28] Goyal, M., Dutta, M. (2018). Intrusion detection of wormhole attack in IoT: A review. In 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), Kottayam, India, pp. 1-5. https://doi.org/10.1109/ICCSDET.2018.8821160

[29] Perazzo, P., Vallati, C., Varano, D., Anastasi, G., Dini, G. (2018). Implementation of a wormhole attack against a RPL network: Challenges and effects. In 2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS), Isola 2000, France, pp. 95-102. https://doi.org/10.23919/WONS.2018.8311669

[30] Bhosale, S.A., Sonavane, S.S. (2022). Wormhole attack detection system for IoT network: A hybrid approach. Wireless Personal Communications, 124(2): 1081-1108. https://doi.org/10.1007/s11277-021-09395-y

[31] Amish, P., Vaghela, V.B. (2016). Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol. Procedia Computer Science, 79: 700-707. https://doi.org/10.1016/j.procs.2016.03.092

[32] Qazi, S., Raad, R., Mu, Y., Susilo, W. (2013). Securing DSR against wormhole attacks in multirate ad hoc networks. Journal of Network and Computer Applications, 36(2): 582-592. https://doi.org/10.1016/j.jnca.2012.12.019

[33] Bhagat, S., Panse, T. (2016). A detection and prevention of wormhole attack in homogeneous Wireless sensor Network. In 2016 International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, pp. 1-6. https://doi.org/10.1109/ICTBIG.2016.7892696

[34] Patel, A., Patel, N., Patel, R. (2015). Defending against Wormhole Attack in MANET. In 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, pp. 674-678. https://doi.org/10.1109/CSNT.2015.253

[35] Zheng, J., Qian, H., Wang, L. (2015). Defense technology of wormhole attacks based on node connectivity. In 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), Chengdu, China, pp. 421-425. https://doi.org/10.1109/SmartCity.2015.107

[36] Kumar, G. (2014). Evaluation metrics for intrusion detection systems-a study. Evaluation, 2(11): 11-17.

[37] Hossin, M., Sulaiman, M.N. (2015). A review on evaluation metrics for data classification evaluations. International Journal of Data Mining & Knowledge Management Process, 5(2): 1-11. https://doi.org/10.5121/ijdkp.2015.5201

[38] Elhamahmy, M.E., Elmahdy, H.N., Saroit, I.A. (2010). A new approach for evaluating intrusion detection system. CiiT International Journal of Artificial Intelligent Systems and Machine Learning, 2(11): 290-298.