Design and Implementation of RSSI Based Intrusion Detection System for RPL based IoT Network

Mrs. Snehal Deshmukh-Bhosale [1†] **and Dr. S. S. Sonavane** [2††],
sa_bhosale@yahoo.com sssonavane@gmail.com
[†] *Asst. Professor, RMD Sinhgad School of Engg, Warje, Pune, India*
Research Scholar, Raisoni College of Engg and Management, Wagholi, Pune, India
[††] *Director, School of Mechatronics Engineering, Symbiosis Skill and OpenUniversity, Pune, India*

Summary
Internet of Things (IoT) is formed by connecting many heterogeneous smart devices through the internet using IPv6 Low Power Wireless Protocol for Personal Area Network (6LoWPAN) and Routing Protocol for LoW Power and Lossy Network (RPL) protocol explicitly designed for the IoT network. IoT is a constrained network in terms of battery life, processing power, memory capacity, cost, size, etc. Because of which, it invites many security attacks that affect the performance of the IoT network. A lot of research is going on concerning the security improvement in IoT. Wormhole attack is one of the most severe attacks, which adds a delay in the transmission of packets by involving many legitimate nodes unnecessarily and degrades their battery life. The proposed study introduces a novel intrusion detection system that uses Received Signal Strength Indicator (RSSI) from a range-based type of localization and hop count from a range-free type of localization system to detect the attack as well as the attacker nodes in IoT based network. The proposed algorithm is designed and developed using Contiki OS and Cooja simulator that forms energy efficient Intrusion Detection System (IDS). In addition to minimum energy consumption and transmission delay, the simulation results of the proposed system demonstrate a precise false positive detection rate.

Key words:
IoT, Security, Wormhole Attack, 6LoWPAN, RPL, RSSI, IDS.

1. Introduction

Internet of Things (IoT) is an emerging technology nowadays with a wireless interconnection of sensory devices in the existing infrastructure. Most of the researchers in this field claim that more than 30 billion devices are expected to connect to the internet by 2020. Smart cities, smart homes, smart grids, smart medical treatments, smart agriculture, etc. are the demanding applications of IoT [1-2]. Sensory devices are uniquely identified by IP addresses viz IPv4 and IPv6. IPv4 has limitations of providing IP addresses to the network with a large number of devices whereasIPv6 protocol offers an infinite number of unique IP addresses. The performance of all these smart devices is being affected by battery power, memory, communication ranges, size, etc. For the optimal performance of the network, all the above constraints are considered by avoiding the use of bulky and battery consuming encryption or security algorithms [3].

IoT network is vulnerable from internal (within the network) & external (through the internet) attacks. Currently, no IDSs are reported fulfilling the requirements of security in the IoT network efficiently. The existing IDSs are utilized either for Wireless Sensor Network (WSN) or conventional internet. A need for security in IoT and various security attacks on RPL and 6LoWPAN are discussed in a few research papers [4-6].

To design a security solution for IoT network is a challenging task due to many new protocols like DTLS [7], IPsec [8], IEEE 802.15.4 link-layer security[9], RPL [10], 6LoWPAN [11], etc. involved in IoT communication. Also, the links used in IoT are lossy with resource-constrained devices connected to insecure internet. The attacks like wormhole attack, sinkhole attack, blackhole attack, selective forwarding attack, etc. affect the performance of IoT network adversely [12-13].

Because of the severity of wormhole attack at the network layer of IoT protocol stack, the proposed research work focuses on the removal of the said attack. This attack adds the transmission delay by misguiding the transmission path between the nodes, which affects the battery life of network devices, resulting in less life of IoT devices. The 6LoWPAN and RPL protocols are used for data transmission are discussed in the next section.

1.1 IoT Protocols

i. 6LoWPAN:

IoT devices are connected to the internet with IPv6 protocol where packets are routed through the network such as IEEE 802.15.4 network. Original IPv6 protocol is not compatible with a resource-constrained network like IoT due to its heavyweight characteristics. For compatibility with IoT network, 6LoWPAN standard proposes a header compression mechanism as IP header compression (IPHC) for IPv6 header, a next header

Manuscript received January 5, 2019
Manuscript revised January 20, 2019

compression (NHC) for IPv6 extension header and User Datagram Protocol (UDP) header. Along with compression, 6LoWPAN also enables routing of IPv6 packets in fragmented form. A physical layer protocol IEEE 802.15.4 has a Maximum Transfer Unit (MTU) size is 127 bytes while IPv6 MTU size is 1280 bytes. To well match MTU size of IPv6 with IEEE 802.15.4, fragmentation is required at the network layer.

For fragmentation and reassembly of a datagram, a reassembly tag and offset is maintained by every fragment. 6LoWPAN connects smart objects network to the internet through 6LoWPAN Border Router (6BR) which is analogs to a sink node in Wireless Sensor Network (WSN). 6BR maintains a routing table and routes the packet to proper destinations. It does fragmentation/assembly of datagrams apart from compression and decompression. There are many attacks like fragmentation attack, authentication attack, confidentiality attack, blackhole attack, denial of service attack, wormhole attack, etc. which affect the performance of the 6LoWPAN network [11] [14-15].

ii. RPL

As the name suggests, the RPL protocol is mostly used for low power and lossy network, which is a significant attribute of IoT. It is designed for the 6LoWPAN protocol, primarily used in the IoT network. RPL is present at the network layer, data link layer and physical layer of IoT protocol stack [16-17].

RPL protocol uses the ICMPv6 protocol which is compatible with the IPv6 protocol to exchange routing information within the network. In RPL, DODAG Information Objects (DIO) messages are used to build RPL Destination-Oriented Directed Acyclic Graph (DODAG) by advertising the information. Destination Advertisement Object (DAO) messages in RPL are used to forward the data from the root node towards the leaf node. Nodes transmit DODAG Information Object (DIO) messages after a periodic time. Other nodes after receiving DIO messages update their routing table and also decide whether to join a new network or not. The most recent and popular commercial protocol like, Zigbee also supports RPL. Zigbee protocol is compatible with resource-constrained devices in IoT by offering low cost and low power characteristics. RPL protocol also suffers from various security attacks as a hello flooding attack, selective forwarding attack, clone ID and sybil attack, sinkhole attack, etc. that disturbs the communication in RPL based network [18-21]. To detect these attacks, many Intrusion Detection Systems (IDS) are developed which are discussed in next section.

1.2 Intrusion Detection System

Intrusion Detection System detects the abnormal behavior of data communication, which is a result of various security attacks in the network. IDSs are of three types: i. Anomaly-Based IDS, ii. Signature-Based IDS iii. Hybrid IDS. A detailed theory of these attacks is discussed in paper [22-25]. IoT is connected to the non-secure network and the internet is one of the prominent sources for attack generation. IDSs in WSN which detect the security attacks successfully cannot be used for IoT networks directly due to few IoT specific protocols like RPL, 6LoWPAN, CoAP, etc. These protocols are not compatible with WSN technology and designed considering internet characteristics. IDS of WSN are not suitable for IoT networks as they do not consider internet properties for attack detection. It is a rigorous need to design IDS in IoT network to achieve better security so is to improve IoT performance. Till now, no IDS is designed that will remove wormhole attack efficiently. In proposed work, IDS for wormhole attack is developed. A theory of the said attack is discussed next section.

1.3 Wormhole Attack

Out of many attacks at 6LoWPAN and RPL protocol, wormhole attack is a grievous attack. In the wormhole attack, attacker nodes broadcast wrong routing information using the ICMPv6 protocol and form a tunnel between two attacker nodes that are remotely placed to each other. This characteristic of wormhole attack makes all the nodes in the network to change their routing table and follow the path advertised by attacker nodes. Attacker nodes advertise their location in the network showing that they are directly connected and nearer to each other. These nodes misguide their neighbors to send packets through the tunnel formed by them. The packet is transmitted through legitimate nodes between these two attacker nodes. This process adds an unnecessary delay in data transmission and also consumes more energy of valid nodes that are not needed in the communication by reducing their battery life.

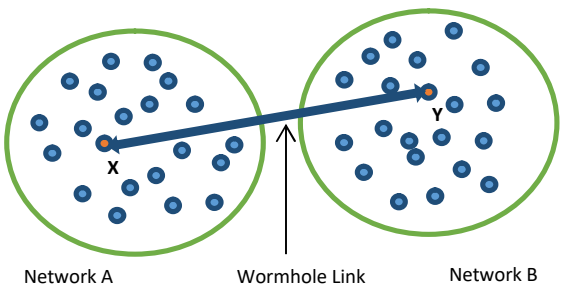

Fig. 1: Wormhole Attack

The remotely placed X and Y attacker nodes form a tunnel, which are placed in two different networks, as

shown in Fig.1. When two nodes from network A want to communicate with each other without attack, they directly send packets in network A. However, in presence of attack their communication happens through a tunnel formed by node X and Y nodes and packet is unnecessarily routed through network B. This adds delay is transmission.

1.4 Localization

In IoT applications, precise and quick self-localization of any node is very important. Researchers developed a variety of approaches discussed in [29][30]. Localization techniques are classified as *range-based method* and *range-free method*. Range-based methods such as RSSI [31], Angle of Arrival (AoA), Time of Arrival (ToA) and Time Difference of Arrival (TDoA) [32] depend on range measurement information and connectivity information. These methods need high computational complexity in their algorithm to give accurate values of the location of the node. On the other hand, range-free methods such as hop count and point in triangle, try to guess approximate values and use those for calculating the sensor node's location. In range-free localization method, less computational complexity is used; hence this is cost-effective and energy-efficient method. However, it gives less accurate results [33].

In the proposed system, the advantages of both the localization systems are taken into consideration to locate the attacker node. By combining hop count and RSSI values which map signal strength into the distance, a novel algorithm is developed RSSI finds the distance between two sensors using power in the radio signal received by the receiver after the antenna and cable loss. RSSI values are measured in decibels per meter (dBm) hence; it comes in negative terms (e.g., -120dB). Nearer the value of RSSI to zero, stronger is the signal. Till -40 dB signal is considered as a stronger signal and it is acceptable. Beyond -100 dB it is weak; hence it is rejected by the sensor node. The proposed algorithm gives energy-efficient and accurate solution to locate the attacker node by increasing the true positive detection rate and reducing false positive detection rate. Many researchers contributed to designing IDS to detect and remove wormhole attack in WSN. The related research work about wormhole attack detection is mentioned next.

The contents of the paper are as follows: Section 2 discusses the literature review on various wormhole attack detection techniques. Section 3 and 4 discuss the methodology of implementation of IDS for wormhole attack detection followed by a conclusion in section 5.

2. Literature Review

There are many methods proposed to remove the wormhole attack in WSN. Comparatively less research work is observed regarding the design of IDS in the IoT, which detects the wormhole attack and the attacker. Song N et al. [34] proposed a statistical analysis based approach that works on the theory that wormhole links offer the shortest path from particular links between source to destination hence they will be found in a higher percentage than other links. However, this method is not sufficient for attack detection for complex networks. H. S. Chiu et al. [35] proposed an algorithm named as DELPHI, which calculates delay per hop count for packet transmission is also used to detect wormhole attack. The limitation of this method is that it detects only the attack and not the attacker.

L.Hu et al. [36] used directional antennas that avoid nodes that give incorrect location information. It is a wormhole attack prevention scheme than avoidance of attack. The requirement of directional antennas and line of sight requirement makes it difficult for implementation. Farid Naït-Abdesselam et al. [37] proposed a mechanism that uses geographic leashes and temporal leashes to detect the wormhole attack. Geographic leashes will not accept the packet from the node which is at the unreasonable distance and temporal leashes will ignore any packet with an unreasonable time stamp. This method requires a synchronized clock, which is challenging to incorporate in IoT network.

Sun Choi et al. [38] proposed the Wormhole Attack Prevention (WAP) method in which Round Trip Time (RTT) is measured between source and destination node to detect the desired attack. If nodes are found out of communication range, then the occurrence of wormhole attack is detected. This method works only for large size networks. Vijayalaxmi et al. [39] developed Cumulative Threshold Transmission (CTT) method where, three characteristics, namely transmission rate, hop count mismatch and cache mismatch values are compared before and after the insertion of attack. This method works only for the static network. Sakthivel T. et al. [40] proposed a technique in which a path tracing algorithm detects the presence of wormhole attack by calculating the distance traveled by a packet concerning the speed of light. This distance is used for the identification of abnormal routes in the network. This method uses timestamp hence requires clock synchronization. The clock synchronization and the distance calculation seem to be hard to achieve due to disconnected nature of the ad-hoc network.

Dhurandher et al. [41] proposed a method, E2SIW (Energy Efficient Scheme Immune to Wormhole attack) that prevents wormhole attack using GPS hardware by detecting the location of the node. This method requires extra GPS hardware, which is not suitable for IoT network. Raju et al. [42] in their research work used average hops RTT to calculate the average

time of path delay. If the average time of path is higher than average RTT time, then a link is considered as suspicious and withdrawn from further communication. This method may fail when there is congestion in a network and if attacker nodes are connected through high-speed links.

Shalabh Jain et al. [43] used electromagnetic wave propagation and channel state information for the detection of the wormhole attack in the network. This approach seems computationally heavy and needs extra processing power. Markus Okunlola et al [28] utilized neighbor discovery and path verification methods using AODV routing protocol for detection of the wormhole attack. They considered neighbor monitoring information and hop count information to detect and removal of attack. The system gives promising results in throughput and delay and packet delivery ratio. But it raises the alarm for attack detection when no attack takes place by generating a high false positive rate. Pericle Perazzo et al. [44] developed IDS for Wireless Sensor and Actuator Network (WSAN) system for attack detection which gives good simulation results but complex to implement in practice.

Maximum methods discussed above are working on WSN. There are very few IDSs are available in IoT those working to remove wormhole attack from network efficiently. The proposed system is an innovative wormhole attack detection system, which is energy efficient and gives optimum results in attack and attacker detection.

3. System Architecture

Under this section, architecture of IDS to detect wormhole attack is discussed. It requires general sensor nodes and a node with extra features of battery, processing power, etc. which is treated as a border router. Sensor nodes are connected to the internet through border router depicted as 6BR, as shown in Fig. 2. The IDS module is placed at the border router. The proposed system monitors the behavior of nodes before and after the insertion of attack in the network. In proposed work, the border router is acting as a root node through which hop count is calculated using the RPL protocol. RSSI value plays a significant role to locate the attacker node. RSSI value of each packet from source to the destination node is converted into distance as per equation (1). When the discrepancy in RSSI amount and hop count are observed with a large extent then attack and attacker nodes are identified [45-47]. The detailed procedure is explained in Illustration section.

$$Distance = 10^{\left(\frac{MeasuredPower - RSSI}{10*N}\right)} \quad (1)$$

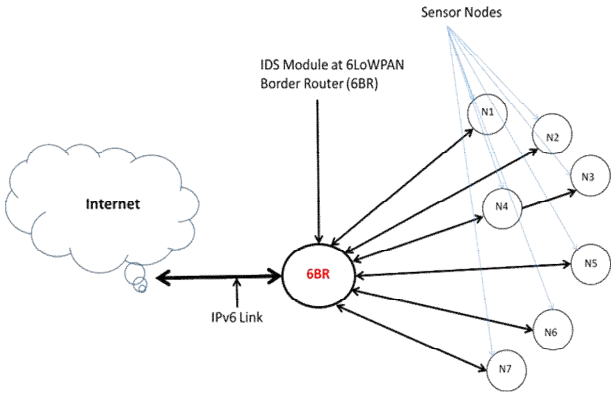

Fig. 2: System Architecture

3.1 Mechanism of Wormhole Attack Detection

It is known that the wormhole attack disturbs the routing topology and misguides the legitimate nodes to transmit the packets through attacker nodes. These colluding nodes pass these packets through the wrong path by adding the delay in transmission. Wormhole attack involves the valid nodes which are not needed in the communication and reduces their battery power by concerning them in the communication. These colluding nodes are neither in transmission range nor neighbors of each other. Hence transmission delay between them is higher than original neighbor nodes. This link is considered a suspicious link. The presence of the attack is confirmed by sending a test packet that calculates the hop count of suspicious links. RSSI value and hop count value are compared with already stored values in routing table shown in table 1 and if mismatch to large extent is observed, then attack is declared. If these attacker nodes are observed in next three cycles of transmission, then these nodes are disabled by deleting their entries from the routing table.

i. Assumptions:

In the proposed system, the following assumptions are made: The simulated network is static where node 1 is acting as a border router and node 6 and node 16 are the attacker nodes. A threshold value for maximum hop count is assumed as 10 and the maximum RSSI value is -90 dBm (2 meters of diameter) for all topologies ranging from 20 nodes to 100 nodes. Measured power is considered as -20dBm. The routing table is updated every 10 minutes. A wormhole attack is inserted in the network after 30 minutes of network settlement and formation of a routing table.

ii. Illustration:

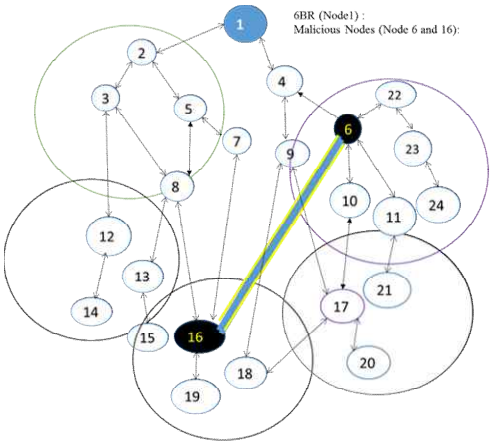

Fig. 3: Wormhole attack detection scenario in the RPL network

To illustrate the working of proposed IDS, the topology of 24 nodes is considered as shown in Fig. 3. All nodes information is stored in 6BR which is a sink node in the network. Node 6 and node 16 are attacker nodes that form a tunnel between them, as shown in Fig.3. When neighbor nodes send a data packet through node 6 or node 16, it reaches to another end of the tunnel. In such a case, nodes which are original neighbors of node 6 and node 16 will get new neighbor requests. From another end of the tunnel, the neighbor information is forwarded to 6BR for validation. Using range and location information, the 6BR detects that both the nodes are not in the transmission range of each other hence generates the alert of the presence of an attack.

To identify the attacker nodes, the 6BR sends control packets to nodes 10 and 19 which are original neighbors of nodes 6 and 16 respectively. Here the control packet collects RSSI values from all its neighbor nodes. Original neighbors of these two nodes send their RSSI values to nodes 10 and 19, respectively. Node 10 will never get RSSI value from node 16 as both are not in the transmission range of each other. Similarly, node 19 will never get it from node 6. Apart from the RSSI amount of the nodes, the control packet also collects the hop count of each node, where it is observed that attacker nodes are far away from the legitimate nodes which give higher hop count. The distance between node 6 and 16 are calculated using Euclidean distance. If this distance is higher than the transmission range of these two nodes, then they are declared as suspicious nodes. In this way, nodes having a high probability of suspect are declared as attacker nodes by 6BR. A routing table for 24 nodes is shown in Table 1. Similarly all nodes will update their routing table as per Table 1 and same will be maintained by border router for next communication. It is observed that the packet transmission time required by attacker nodes is always higher than two legitimate nodes and due to attacker nodes, many neighboring nodes are introduced in the network that are far away from each other.

Table 1: Routing Table reference with node 1

Sr. No.	Neighbor Node ID	Hop Count (Reference with self node)	RSSI value between self and neighbor node (dBm)	Distance (m)
1	1	0	0	0
2	2	1	-5	0.8659
3	3	2	-10	0.9076
4	4	1	-5	0.8659
5	5	2	-10	0.9076
6	6	2	-15	0.9531
7	7	3	-15	0.9531
8	8	3	-20	1
9	9	2	-10	0.9076
10	10	3	-20	1
11	11	3	-25	1.0492
12	12	3	-25	1.0492
13	13	5	-30	1.1007
14	14	4	-30	1.1007
15	15	5	-35	1.1547
16	16	4	-35	1.1547
17	17	3	-35	1.1547
18	18	3	-40	1.2114
19	19	5	-45	1.2711
20	20	4	-45	1.2711
21	21	4	-30	1.1007
22	22	3	-10	0.9076
23	23	4	-15	0.9531
24	24	5	-20	1

4. Simulation Platform

The algorithm for the proposed system is developed using Contiki OS and Cooja Simulator specifically designed for IoT applications. Cooja runs deployable Contiki code. For the simulation purpose, Tmote Sky nodes are used. CC 2420 is used as a radio interface, and Sicsmac is used at Radio Duty Cycling. Sicslowpan and RPL are used at the network layer and the routing layer, respectively. At the transport layer, UDP protocol is used [48].

4.1 Simulation Results and Observations

After simulating the proposed IDS using the Cooja simulator, three network characteristics: energy consumption, propagation delay, true and false positive detection rates are observed. Topology for N=24 and 100 is as shown in Fig 4(a) and 4(b) respectively.

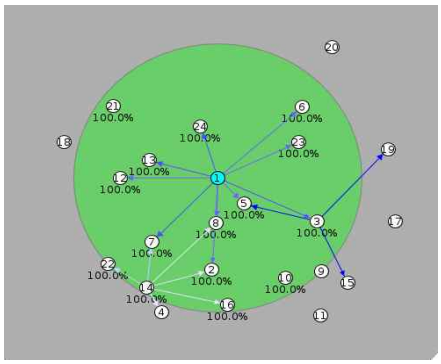

Fig 4(a) N=24

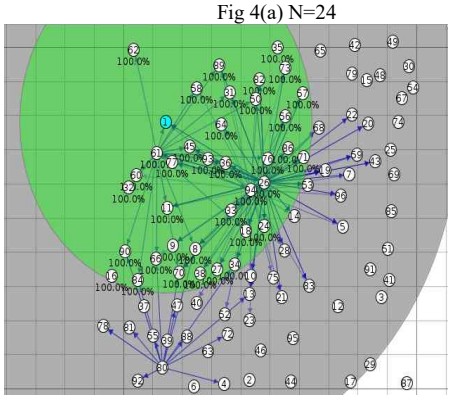

Fig 4(b) N=100

Fig. 4: Various topologies for Wormhole Attack Detection

Energy consumption is defined as the amount of energy required per unit second for data processing and transmission. In the IoT, nodes are battery-powered therefore, energy efficiency is an essential aspect in IoT devices. Contiki power-trace tool is used to measure the power consumption of IDS [51]. Time instant when the radio receives and transmits the data with Microcontroller Unit (MCU) referred to listening and transmits respectively. For calculation, working voltage is considered as 3V. When MCU is ON and radio is in OFF condition, it is considered as CPU time whereas when MCU is idle and radio is OFF, it is considered as Low Power Mode (LPM) time. By running the system for 30 minutes for all topologies, Network-wide energy usage by all nodes for IDS and hello world is shown in Fig 5(a). Energy consumption is calculated using the nominal values of the Tmote sky, as shown in equation 2. Where transmit and listen are TX and RX values respectively [25].

*Energy (mJ) =((transmit * 19.5mA + listen * 21.8 mA+ LPM *0.0545 mA+ CPU*1.8 mA) * 3 V)/(4096 * 8)* (2)

It is observed from the graph in Fig 5(a) that for small network size (Number of nodes less than 60), IDS consumes almost equal energy as much consumed by running a *hello world* application, which proves that proposed IDS is energy efficient. The average difference is 33,332.8 mJ. However, it is also noticed from Fig. 5(a) that, as network complexity increases (Number of nodes more than 60), energy consumption required for running the IDS is higher compared to *hello world* application with average difference is 2,65,256 mJ. Higher energy consumption for complex networks is one of the aspects, which need to be addressed in future.

A ***propagation delay*** in WSN is defined as a time taken by a packet to be transmitted from source to destination in the wireless environment. In the proposed system, propagation delay is calculated using RSSI value received along with each packet. In the presence of a wormhole attack, delay of packet transmission is increased by the average amount of 38.55%, which reduces the efficiency of the communication network. It happens because; in the presence of wormhole attack, attacker node misguides the valid nodes to transmit the packet through the wrong route by changing the routing table. After the proposed IDS is introduced in the network, the delay is 8.89% more than the original propagation delay, as shown in figure 5(b) which is a reasonable amount.

The ***true positive and false positive detection rates*** of wormhole attack are also observed. *True positive detection rate* is defined as how correctly IDS identifies the presence of the attack and attacker. The developed system detects the wormhole attack successfully when the attack is present in the system. The detection rate reduces as per the increase in the complexity of the network. *False positive detection rate* is defined as how many times the IDS falsely raises the alarm for attack when no attack in the network. Ideally this value must be nearer to zero. In the developed system, the average amount of false positive detection rate is very precise. The result for the true positive and false positive detection rate of wormhole attack is shown in Fig 5 (c)

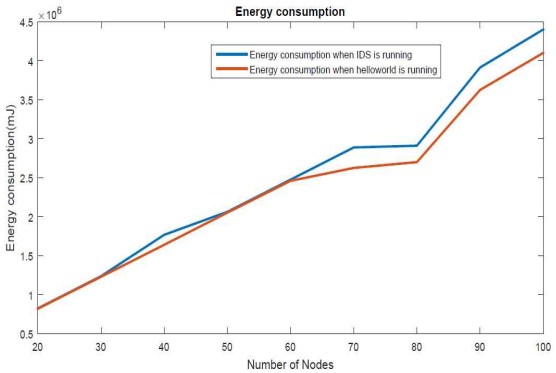

Fig 5(a): Energy Consumption

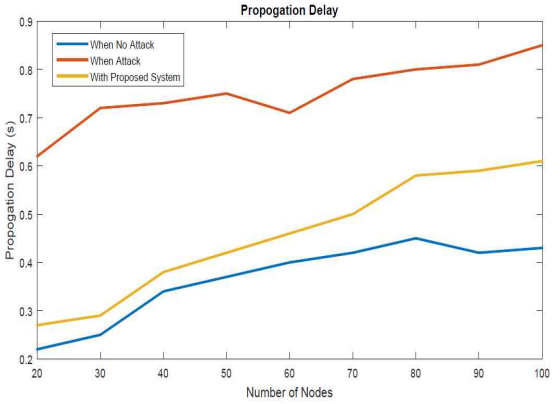

Fig 5((b): Propagation Delay

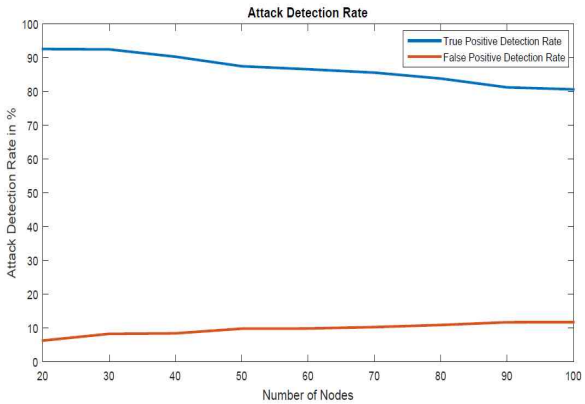

Fig 5(c) Attack Detection Rate

Fig. 5 Performance Analysis of the proposed system:
(a) Energy Consumption
(b) Propagation Delay (c) Attack Detection Rate

Many researchers worked to detect the wormhole attack in the field of the wireless sensor network. Few researchers got more than 90% true positive detection rate and less than 10% false positive detection rate [53][54]. However, no researchers worked to get these results using 6LoWPAN and RPL protocols of IoT. In the proposed system, energy-efficient IDS is designed to detect wormhole attack in IoT with precise true and false positive detection rate. After implementing one of the existing wormhole attack detection methods in IoT, it is observed that it gives more than 25% of false positive detection rate, which is not desirable value [44]. In other hand, implemented system provides an average value of 86.68% of true positive detection rate and 9.63% false positive detection rate for number of nodes ranging from 20 to 100.

5. Conclusion

A novel energy-efficient Intrusion Detection System (IDS) that detects the presence of wormhole attack and attacker nodes in RPL based network is successfully demonstrated in this paper. The proposed method uses hop count and RSSI value, which is proportional to the distance between two nodes to detect the presence of attack and attacker nodes. Because of minimum overhead and less complexity in the proposed IDS, it consumes very less energy. It provides less propagation delay very efficiently. Most of the IDS proposed in the literature fail to get effective results in wormhole attack detection in IoT. Those systems have given a reasonable true positive detection rate; but their false positive detection rate is more than 25%, which is not desirable. When the proposed system is implemented, it is observed that the false positive detection rate is reduced very precisely. In the implemented system the value of false positive detection rate is lesser than 10%, which is lowest compared to all the existing IDSs developed in IoT system for wormhole attack detection. The simulated IDS can be implemented using hardware as Rasberry Pi and nrf52 nodes for real-time applications.

References

[1] Kim Thuat Nguyen, Maryline Laurent, Nouha Oualha, “Survey on secure communication protocols for the Internet of Things”, Ad Hoc Network, Volume 32, September 2015, Pages 17-31, Published by Elsevier B.V., DOI: 10.1016/j.adhoc.2015.01.006, 1570-8705/_2015

[2] J. Gubbi, R.Buyya, S.Marusic, M.Palaniswami, “Internet of Things (IoT): vision, architectural elements, and future directions”, Future Generation Computer Systems, Volume 29, Issue 7, September 2013, Pages 1645-1660, Published by Elsevier B.V., DOI: 10.1016/j.future.2013.01.010

[3] Davar PISHVA, “Internet of Things: Security and Privacy Issues and Possible Solution”, Published in 2017 19th International Conference on Advanced Communication Technology (ICACT), Published by IEEE in March 2017, DOI: 10.23919/ICACT.2017.7890229

[4] Snehal Deshmukh, Dr. S. S. Sonavane, “Security Protocols for Internet of Things: A Survey”, Published in 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2), Published by IEEE in October 2017, DOI:10.1109/ICNETS2.2017.8067900

[5] Pavan Pongle, Gurunath Chavan, “A survey: Attacks on RPL and 6LoWPAN in IoT”, Published in 2015 International Conference on Pervasive Computing (ICPC), Published by IEEE in April 2015, DOI: 10.1109/PERVASIVE.2015.708703

[6] SNEHAL DESHMUKH-BHOSALE, DR. S. S. SONAVANE “A REAL-TIME INTRUSION DETECTION SYSTEM FOR WORMHOLE ATTACK IN THE RPL BASED INTERNET OF THINGS”, PROCEDIA MANUFACTURING, VOLUME 32, 2019, PAGES 840-847, PUBLISHED BY ELSEVIER B.V., DOI: 10.1016/J.PROMFG.2019.02.292.

[7] T. Kothmayr, W. Hu, C. Schmitt, M. Bruenig, G. Carle, “Securing the internet of things with DTLS”, Proceedings of the 9th ACM, Conference on Embedded Networked Sensor Systems, ACM, 2011, pp. 345–346.

[8] S. Raza, S. Duquennoy, A. Chung, D. Yazar, T. Voigt, U. Roedig, "Securing communication in 6LoWPAN with compressed IPsec", Published in 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), Published by IEEE in August 20111, DOI: 10.1109/DCOSS.2011.5982177

[9] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, T. Voigt, "Secure Communication for the Internet of Things – A Comparison of Link Layer Security and IPsec for 6LoWPAN", Security and Communication Networks, Published online 18 January 2012 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.406

[10] IETF, RPL. "Routing Over Low Power and Lossy Networks.", Accessed on Aug' 18

[11] N. Kushalnagar, G. Montenegro, C. Schumacher, "IPv6 over Low-power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", IETF, RFC 4919 (2007).

[12] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qiu, "Security of the Internet of Things: perspectives and challenges", Wireless Network, Published by Springer, November 2014, Volume 20, Issue 8, pp 2481–2501, DOI: 10.1007/s11276-014-0761-7

[13] Rolf H.Weber, "Internet of Things – New security and privacy challenges", Computer Law & Security Review, Volume 26, Issue 1, January 2010, Pages 23-30, Published by Elsevier B.V., DOI: 10.1016/j.clsr.2009.11.008.

[14] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A. Spirito, Mark Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things", Published in 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Published by IEEE in November 2013, DOI: 10.1109/WiMOB.2013.6673419

[15] Prabhakaran Kasinathan, Gianfranco Costamagna, Hussein Khaleel, Claudio Pastrone, Maurizio A. Spirito, "DEMO: An IDS Framework for Internet of Things Empowered by 6LoWPAN", Proceedings of the ACM SIGSAC conference on Computer & communications security, 2013, DOI: 10.1145/2508859.2512494.

[16] Amit Dvir, Tamas Holczer, Levente Buttyan, "VeRA - Version Number and Rank Authentication in RPL", Published in 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, Published by IEEE in November 2011, DOI: 10.1109/MASS.2011.76

[17] Heiner Perrey, Martin Landsmann, Osman Ugus, Thomas C. Schmidt, Matthias Whlisch, "TRAIL: Topology Authentication in RPL", Published in Proceeding EWSN '16 Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks, Pages 59-64

[18] Anhtuan Le, Jonathan Loo, Yuan Luo, Aboubaker Lasebae, "The impacts of internal threats towards Routing Protocol for Low power and lossy network performance.", Published in: 2013 IEEE Symposium on Computers and Communications (ISCC), published by IEEE in March 2014, DOI: 10.1109/ISCC.2013.6755045

[19] Walgreen, Linus, Shahid Raza, and Thiemo Voigt. "Routing Attacks and Countermeasures in the RPL-based Internet of Things", International Journal of Distributed Sensor Networks, 2013, DOI: 10.1155/2013/794326.

[20] Perazzo P., Vallati C., Arena A., Anastasi G., Dini G. (2017) "An Implementation and Evaluation of the Security Features of RPL" In Puliafito A., Bruneo D., Distefano S., Longo F. (eds) Ad-hoc, Mobile, and Wireless Networks. ADHOC-NOW 2017. Lecture Notes in Computer Science, vol 10517. Springer, Cham, DOI: 10.1007/978-3-319-67910-5_6

[21] Anthéa Mayzaud, Anuj Sehgal, Rémi Badonnel, Isabelle Chrisment, Jürgen Schönwälder, "A Study of RPL DODAG Version Attacks", 8th IFIP International Conference on Autonomous Infrastructure, Management and Security (AIMS), Jun 2014, Brno, Czech Republic. pp.92-104, DOI:10.1007/978-3-662- 43862-6_12.

[22] Amrita Ghosal, Subir Halder, "A survey on energy efficient intrusion detection in wireless sensor networks", Journal of Ambient Intelligence and Smart Environments 9 (2017) 239–261, DOI 10.3233/AIS-170426

[23] Anhtuan Le, Jonathan Loo, Kok Keong Chai, Mahdi Aiash, "A Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology", Information 2016, 7, 25; DOI:10.3390/info7020025.

[24] Chen Jun, Chen Chi, "Design of Complex Event-Processing IDS in Internet of Things", Published in 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation, Published by IEEE April 2014, DOI: 10.1109/ICMTMA.2014.57

[25] Shahid Raza, Linus Wallgren, Thiemo Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things", Ad hoc networks, Volume 11, Issue 8, November 2013, Pages 2661-2674, Published by Elsevier, DOI:10.1016/j.adhoc.2013.04.014

[26] YIH-CHUN HU; A. PERRIG ; D.B. JOHNSON, "WORMHOLE ATTACKS IN WIRELESS NETWORKS", PUBLISHED IN IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (VOLUME: 24, ISSUE: 2, FEB. 2006), DOI: 10.1109/JSAC.2005.861394

[27] Snehal Deshmukh-Bhosale, Dr. S. S. Sonavane, "Wormhole attack detection in internet of things", International Journal of Engineering & Technology, International Journal of Engineering & Technology, Volume 7 (2.33) (2018) 749-751, March 2018, DOI: 10.14419/ijet.v7i2.33.15488

[28] Marcus Okunlola Johnson, Arish Siddiqui, Amin Karami, "A Wormhole Attack Detection and Prevention Technique in Wireless Sensor Networks", International Journal of Computer Applications (0975 - 8887), Volume 174 - No.4, September 2017

[29] Shailaja Patil, Mukesh Zaveri, "MDS and Trilateration Based Localization in Wireless Sensor Network", Scientific Research, Wireless Sensor Network, 2011, 3, 198-208, Published Online June 2011, DOI:10.4236/wsn.2011.36023

[30] G. Q. Mao, B. Fidan and B. D. O. Anderson, "Wireless Sensor Network Localization Techniques", Computer Networks, Volume 51, Issue 10, 11 July 2007, Pages 2529-2553, Published by Elsevier, DOI: 10.1016/j.comnet.2006.11.018

[31] X. Li, H. Shi and Y. Shang, "A Sorted RSSI Quantization Based Algorithm for Sensor Network Localization", Published in 11th International Conference on Parallel and Distributed Systems (ICPADS'05), published by IEEE in November 2005, DOI: 10.1109/ICPADS.2005.53

[32] P. Xing, H. Yu and Y. Zhang, "An Assisting Localization Method for Wireless Sensor Networks", Published in 2005 2nd Asia Pacific Conference on Mobile Technology, Applications and Systems, published by IEEE in November 2005, DOI: 10.1109/MTAS.2005.207192

[33] Tian He, C. Huang, B. Blum, J. Stankovic and T. Abdelzaher, "Range-Free Localization Schemes for Large Scale Sensor Networks", Proceedings of the Ninth Annual International Conference on Mobile Computing and Networking (ACM Mobicom), San Diego, September 2003, pp. 81-95, DOI: 10.1145/938985.938995

[34] Song N, Qian L, Li X, "Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach", Published in 19th IEEE International Parallel and Distributed Processing Symposium, published by IEEE in April 2005, DOI: 10.1109/IPDPS.2005.471

[35] H. S. Chiu and K. Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", Published in 2006 1st

International Symposium on Wireless Pervasive Computing, published by IEEE in April 2007, DOI: 10.1109/ISWPC.2006.1613586

[36] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks", In Network and Distributed System Security Symposium (NDSS 2004), San Diego, California, USA. February 2004.

[37] Farid Nait-Abdesselam, Brahim Bensaou, Tarik Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks", Published in IEEE Communications Magazine (Volume: 46, Issue: 4, April 2008), published by IEEE in April 2008, DOI: 10.1109/MCOM.2008.4481351

[38] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", Published in 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008), published by IEEE in June 2008, DOI: 10.1109/SUTC.2008.49

[39] Vijayalakshmi, S., and P. Annadurai, "Arresting Wormhole Attack in Ad hoc Network using Cumulative Threshold Transmission Rate", International Journal of Computer Applications (0975 – 8887) Volume 54– No.18, September 2012

[40] Sakthivel, T., and R. M. Chandrasekaran, "Detection and Prevention of Wormhole Attacks in MANETs using Path Tracing Approach", International Journal of Communication and Networking System Volume: 01 Issue: 02 December 2012, Pages No.59-62 ISSN: 2278-2427

[41] Dhurandher, Sanjay Kumar, et al., "E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks.", Published in 2012 26th International Conference on Advanced Information Networking and Applications Workshops, Published by IEEE in April 2012, DOI: 10.1109/WAINA.2012.85

[42] V. Karthik Raju; K. Vinay Kumar, "A Simple and Efficient Mechanism to Detect and Avoid Wormhole Attacks In Mobile Ad Hoc Networks", Published in 2012 International Conference on Computing Sciences, Published by IEEE in December 2012, DOI: 10.1109/ICCS.2012.4

[43] Shalabh Jain, Tuan Ta, John S. Baras, "Wormhole Detection Using Channel Characteristics", Published in 2012 IEEE International Conference on Communications (ICC), Published by IEEE in November 2012, DOI: 10.1109/ICC.2012.6364768

[44] Pericle Perazzo, Carlo Vallati, Dario Varano, Giuseppe Anastasi and Gianluca Dini, "Implementation of a Wormhole Attack Against a RPL Network: Challenges and Effects", 2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS), ISBN 978-3-903176-02-7 © 2018 IFIP 95

[45] Snehal Deshmukh-Bhosale, Dr. S. S. Sonavane, "Implementation of 6LoWPAN Border Router (6BR) in Internet of Things", International Journal of Innovations & Advancement in Computer Science IJIACS, ISSN 2347 – 8616 Volume 7, Issue 3, March 2018

[46] Tsung-Han Lee, Xiang-Shen Xie, Lin-Huang Chang, "RSSI-Based IPv6 Routing Metrics for RPL in Low power and Lossy Networks", Published in 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Published by IEEE in December 2014, DOI: 10.1109/SMC.2014.6974164

[47] Alireza Shojaifar, A thesis on "Evaluation and Improvement of the RSSI- based Localization Algorithm", 2015, Faculty of Computing Blekinge Institute of Technology SE-371 79 Karlskrona Sweden.

[48] Texas Instruments CC2420 Simple Link™ Multi standard Wireless MCU. [Online]. Available: http://www.ti.com/lit/ds/symlink/cc2420.pdf [Online; accessed December-2018].

[49] A. Dunkels, B. Grönvall, T. Voigt, "Contiki – a lightweight and flexible operating system for tiny networked sensors", in EMNets'04, Tampa, USA, 2004, pp. 455–462.

[50] Ing Pietro Gonizzi and Simon Duquennoy. Hands-on Contiki OS and Cooja Simulator: Exercises (Part II). https://team.inria.fr/fun/files/2014/04/slides_partI.pdf, 2013. [Online; accessed January 2019].

[51] A. Dunkels, J. Eriksson, N. Finne, N. Tsiftes, "Powertrace: Network Level Power Profiling for Low-Power Wireless Networks", March 2011 SICS Technical Report T2011:05 ISSN 1100-3154.

[52] http://www.eecs.harvard.edu/~konrad/projects/shimmer/references/Tmote-sky-datasheet.pdf

[53] Saswati Mukherjee, Matangini Chattopadhyay, Samiran Chattopadhyay, Pragma Kar, "Wormhole Detection Based on Ordinal MDS Using RTT in Wireless Sensor Network", Hindawi Publishing Corporation Journal of Computer Networks and Communications Volume 2016, Article ID 3405264, 15 pages DOI:10.1155/2016/3405264

[54] Jayashree Padmanabhan, Venkatesh Manickavasagam, "Scalable and Distributed Detection Analysis on Wormhole Links in Wireless Sensor Networks for Networked Systems", Published in IEEE Access, Published by IEEE in December 2017, DOI: 10.1109/ACCESS.2017.2780188

Mrs. Snehal Deshmukh-Bhosale, Pursuing PhD in SPPU, Pune. She is working as Asst. Professor, E&TC Dept, RMDSSOE, Pune. She has published more than 30 research papers in national and international journals. She has also published two patents on current research work, She has received best paper award twice for current research work. She is having more than 18 years of experience in the field of education, To fulfill the work of PhD Mrs. Bhosale with her guide have developed an Intrusion Detection System (IDS), using Contiki OS and Cooja Simulator. They have got the optimum result in terms of throughput, delay and attack detection in terms of positive and negative attack detection. For hardware implementation she has used Raspberry Pi and node nRF52 nodes. Her research areas are Wireless Communication, Wireless Sensor Network, Internet of Things.

Dr. S. S. Sonavane, Director, School of Mechatronics Engineering, Symbiosis Skill and OpenUniversity, Pune, India, He is having 20 years of experience in educational field and served in many well-known organizations. He has a successful academia and published 2 books at International level (Austria and Germany). He had more than 75 International and National publications on his name in reputed peer Reviewed Journals. Published more than 5 patents on his name. He is the registered PhD guide in SPPU, Pune.He is also Reviewer of many Electronics International Journals including IEEE Sensor Journal and IEEE Communication Letters. He had successfully completed two Research Projects funded by University of Pune. Research Areas: Wireless Sensor Network, Internet of Things.