International Journal of Engineering & Technology, 7 (3.27) (2018) 147-150

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Wormhole Attack: a Major Security Concern in Internet of Things (Iot)

Swetha Palacharla[1]*, M.Chandan[2], K.GnanaSuryaTeja[3], G.Varshitha[4]

[1]Computer Science and Engineering, Koneru Lakshmaiah Education Foundation,Vaddeswaram,India
[2]Proffesor Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram,India
[3]Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India
[4]Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India
**Corresponding author E-mail: swetha.palacharla@gmail.com*

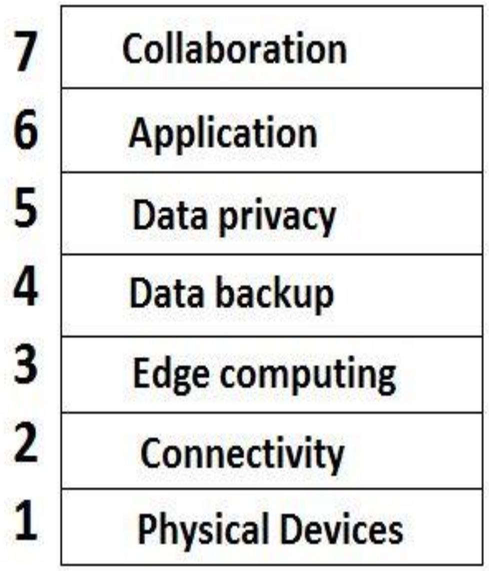
Abstract

The Internet of Things (IoT) is nothing but a collection of wireless and wired devices, commonly termed as nodes operated remotely. This operation is done by assuming these nodes as the sensors in a wireless sensor network (WSN) administered through a base station. We start with briefing about IoT and then briefing IoT layer models. After this, we discuss attacks with regard to IoT namely Sinkhole attack, Sybil attack, HELLO flood attack, Acknowledgement spoofing attack and their respective detection methods. This paper is systematic review of existing mechanism for the detection of wormhole attack and a new method is proposed.

Keywords: *Wormhole attack ; Wsn – wireless network ; WSN CAPS*

1. Introduction

The Internet of Things (IoT) is nothing but a collection of wireless and wired devices, commonly termed as nodes operated remotely. This operation is done by assuming these nodes as the sensors in a wireless sensor network (WSN) administered through a base station. Firstly, the IoT layer model is explained in detail for the better understanding the security vulnerabilities. This model describes IoT as seven layer model to help secure every device, provide security for communication between each level. [1] Layer 7(Collaboration) - This layer involves users and requirement processes. Layer 6(Application) – involves reporting, analyzing and authorization. Layer 5(Data privacy) – involves accessing and secure storage of data. Layer 4(Data Backup) – This layer involves backup data storage. Layer 3(Edge Computing) – this is the layer where network connects to cloud. Layer 2(Connectivity) – involves connecting of hardware to the network. Layer 1(Physical Devices) – in this layer are the devices (nodes/sensors) in IoT. One more important concept for better understanding the security vulnerabilities is the topology. [1] There are three types of topologies: point-to-point, star, mesh. Among these, the mesh topology is best due to its localization. It has a node to act as a Gatekeeper, nodes as sensors and nodes as both sensors and routers. The localized architecture is dynamic and can assign the network roles arbitrarily. Here, information about the routing is maintained at every node. This paper deals with various attacks in IoT and their detection methods.



7	Collaboration
6	Application
5	Data privacy
4	Data backup
3	Edge computing
2	Connectivity
1	Physical Devices

Figure 1: (IoT Layer Models)

2. IoT Attacks and Detection Methods

The attacks described in this paper are Sinkhole Attack, Acknowledgement Spoofing, Sybil Attack, Wormhole Attack, HELLO flood attack.

2.1 Sinkhole Attack:

The Sinkhole attack works by representing a node look welcoming to surrounding nodes i.e, the node which has the best path to base station is identified to be the adversary node. This could spoof the other nodes for a high quality route.

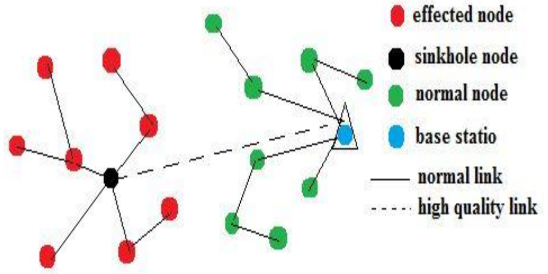


Fig 2: Sinkhole Attack

To detect a sinkhole, we [2] need to find the suspected nodes by observing the data and identify the attacker in the list by analyzing the network traffic. This is done in two steps -

- By calculating the area of attack estimate the area influenced, the network is organized into several underdomains and data inside each of them are compared. The attacker cannot change the data starting in each and every node in the network. So, in some of the sub-domains the attack has to be found. As the area of attack may have lots of nodes, to identify the attacker we need to examine the routing model in the influenced area.
- Identify by attacker the base station gets a request message, which has IDs of the influenced nodes. They should contain their own ID; the next-hop node which are already present with BS. By looking at the next hop and cost Previously the attack can be identified. So, the reply message can be transferred through reverse path in flooding which takes original route without intruding.

2.2 Sybil Attack

This is a malicious attack which disintegrates the network model. In this scenario, a node or a device takes many identities i.e, the id of another node from several other nodes which leads to redundancy in the routing protocol. This results in loss of data integrity, security and resource utilization. Though there are encryption methods to prevent external attack on the nodes but there may be an internal attack. The Sybil node S spoofs the other node N. The neighboring nodes receive messages with identity of other nodes from the Sybil node. This creates misbehavior in the network and it gets broken down.

The Sybil attacks are classified [7] based on their attack on the network.

1. Direct attack and indirect attack:

In a direct attack, the nodes move directly with attack nodes, wherever in associate in nursing indirect attack, the interaction happens through the malicious node.

2. Fabricated attack and stolen identity attack:

Duplicate nodes are created using original identities of nodes.. For example, a sensor node which has an ID of 8-bit creates the same of 8-bits, which are fake nodes.

Detection and Prevention [7]:

Let us consider number of nodes are present in the network under the control of and an administrator. At the time of creating a node, it will receive a HELLO message from base station with its creation time in the network as a timestamp. The node replies to the base station with a message containing ID, timestamp and location which is stored in an INODEINFO table at the administration. Location of each node in the network is given as (Ni) = (rand(x), rand(y)), (x, y).

For instance, in a network N, if a node S needs to transmit data to a node D which occurs through N-hop intermediate nodes. The irouting table stores the instant information about the nodes in the middle as (ID, timestamp). When data is sent, the entries in irouting table are compared with the INODEINFO table's entries to identify duplicate nodes. In order to avoid the Sybil attack, MAP algorithm [7] is used.

2.3 HELLO flood attack

In some routing protocols, the nodes broadcast the messages with HELLO to represent themselves as neighbors. Any node which receives the messages like these assumes that the node is in the transmission range of the sender which may or may not be true. Sometimes if the attacker has a high transmission capacity then he may resemble to the other nodes as their neighbor. The protocols which depend on localized information exchange maybe affected.

Detection and Prevention:

We [5] first take some standard input signal strength. The node sending the hello message is considers as node T. If the signal strength of the received hello message is equal to standard signal strength in transmission range then the node T is called as neighbor and the HELLO message is accepted and necessary operations are performed. If the received HELLO message signal strength is approximately equal to the fixed signal strength, then it sends a puzzle to the node T. If the reply message consists of correct answers and comes in the fixed threshold time then the node T is termed to be a friend and accepts request and performs required action. If the received message's signal strength is greater than fixed signal strength then it is not termed as a neighbor and rejects the future requests from node T.

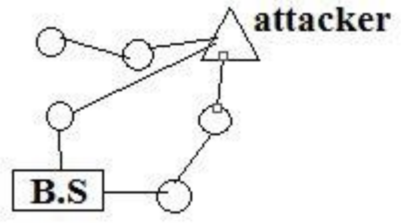


Fig 3: Attacker broadcasting HELLO messages

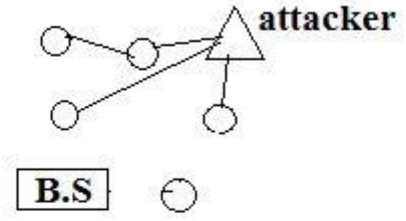


Fig4: Nodes accepting attacker as a neighbor

2.4. Acknowledgement Spoofing Attack

Many wireless sensor network algorithms depend on the acknowledgements. Any arbitrary node may spoof this acknowledgement for the packets intended to neighboring nodes. The protocols that are based on the next hop are vulnerable to acknowledgement spoofing [8]. There may be loss of packets during transmission along such links. The attacker convinces the sender node that a weak or dead link is alive to receive the messages.

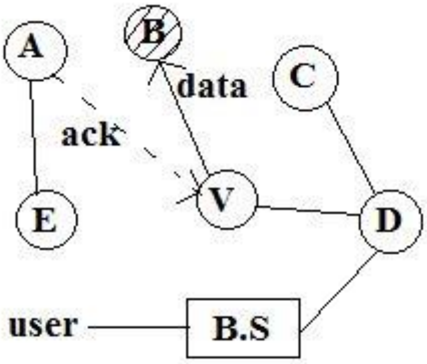


Fig 5: Acknowledgement spoofing

Here, node V transmits data to a node B which is down but node A gives acknowledgement to V, knowing that B is dead. This convinces V that B is still active and V acts according to the acknowledgement received.

Detection and Prevention:[6] There is no separate methodology to prevent this rather effective authentication is to be used by all the nodes present in the network.

3. Worm Hole Attack

In this attack, one or more than one malicious node is present. These malicious nodes have a bridge / tunnel between them. These nodes which are to attack the others, capture the packets from one point and tunnel them to some arbitrary point and the attacker node present there distributes it. This leads to either early arrival or delayed arrival or in some cases non-arrival of the packet to the appropriate node. Routing algorithms which depend on the path length between the nodes are effected due to these wormhole nodes. For instance, consider there is a series of nodes from A to B as A, n1, S1, S2, S3, n2, B. Now, a wormhole attack can occur at n1 and n2 thereby forming a tunnel from n1 to n2. So, the packets sent from A to B which have to traverse as A – n1 – S1 – S2 – S3 – n2 – B, traverse the path shown in the following figure.

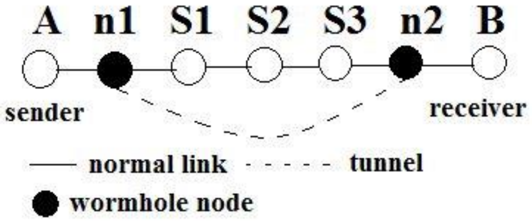


Fig 5: Wormhole attack

Here, the n1 node is transmitting the packet directly to n2 whichthen forwards it to B. As a result there may be early arrival of the packet at node B which may cause a network traffic at node B and may also lead to its crash.

3.1 Existing Methodology for Detection of the WORMHOLE ATTACK

Parmar Amish [3] proposed a mechanism called Ad-hoc on-demand Multipath Distance Vector routing protocol (AOMDV) for detection of the wormhole attack. In this method, a threshold round trip time is calculated alongside hop count and compared to the total round trip time. If the threshold round trip time is greater than total round trip time and the hop count with respect to that route is two then a wormhole link is detected.[9][10]

The 'packet leashes' technique restricts the packets from being transmitted farther than a transmission range. The wormhole attack can be detected [4] by time delay or location. By restricting the maximum distance of transmission the wormhole attack is removed which can be performed by using either local information or time synchronization. The temporal leash ensures an upper limit on packet's lifetime. Whenever a packet is transmitted by a to the destination, the packet consists of the time at which it was sent and is compared with the value time at which it received by the receiving node. A Geographical leash ensures the receiver is within known distance from sender node. The packet being sent includes its sending time and the sender node's location. After the packet reach the receiver node, the distance between and its own and the sender is computed by the receiver. The temporal leashes require fairly synchronized clocks and for the geographical leashes, each node should know its location and every node needs to have loosely synchronized clock which are their respective drawbacks.

3.2 Drawbacks of the Existing Methods

The AOMDV and packet leashes methods are not able to precisely give the ids of the nodes in wormhole attack or the nodes present between the two or more wormhole nodes.

Also, the AOMDV and packet leashes methods are scanning the entire network every time a packet is being sent which takes a lot of time.

3.3 Proposed Method to Detect the WORMHOLE ATTACK

This method uses cryptography as a back end to detect the wormhole attack. In order to better understand this, we need take some assumptions –

- Every node has the details of its path from every other node.
- All the nodes present in the network rely on same asymmetric key cryptographic algorithm.
- Every node has the public keys of every other node.
- Once the packet reaches a node, it adds its id to the packet and encrypts it (id) with its (node) private key.

3.4. Algorithm

- The sender node adds its id to the packet, encrypts the packet with its private key and forwards the packet in the path towards the receiver.
- Every time the packet passes through a node, it adds its id to the packet, encrypts and forwards it.
- After reaching the destination, the receiver decrypts the packet in reverse order the packet reached the node using the public keys to get the previous ids.
- If the packet doesn't provide all the ids present in the path, then the wormhole attack is marked in the path.
- All the ids in the path except those obtained by repeated decrypting of the packet are marked as the wormhole nodes by the receiver.
- Now, the receiver tansmits a dummy packet to the sender which carries the information about these wormhole nodes.
- Upon receiving this dummy packet, the sender node also marks the wormhole nodes accordingly.
- Thus, the nodes under the wormhole attack can easily identified.

4. Advantages of Proposed Method over Existing Method

- The proposed method checks the path dynamically without working on all the nodes at a time which makes it more efficient such that even if a wormhole occurs in between two transmissions, wormhole attack can be detected.
- The proposed algorithm also lists about the wormhole nodes to the sender which are not covered by the existing methodologies.
- As the receiver and sender nodes are detecting the wormhole nodes, the base station or the network admin need not cross verify.

5. Conclusion and Future Scope

Major security concerns are discussed and focus is given on Wormhole attack. The efficient algorithm is proposed to detect the wormhole attack not only discloses the wormhole attack but also lists the nodes under this attack dynamically. The security issues presently bothering are discussed and there may be vulnerabilities which can occur with the increasing technology which may be due hardware or software

Refrences

[1] Network Security Issues in the Internet of Things (IoT) Stuart Millar, PhD Cyber Security Student, 13616005, Queen's Uni versity of Belfast

[2] Detection of Sinkhole Attack in Wireless Sensor Network by Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala, Faculty of Computing, Universiti Technologi of Malaysia (UTM), Skudai, Malsia

[3] Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol by Parmar Amisha ,V.B.Vaghelab, Student, Sankalchand Patel College of Engineering, Visnagar-384315, India

[4] Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Wormhole At tacks in Wireless Networks", IEEE journal on selected areas in com munications, Vol.24, No.2, pp. 370-380,February 2006.

[5] Hello Flood Attack and its Countermeasures in Wireless Sensor Net works by Virendra Pal Singh1, Sweta Jain2 and Jyoti Singhai, Depart ment of Computer Science and Engineering, MANIT, Bhopal, M.P.,India

[6] Security issues in wireless sensor network data gathering protocols:A survey by Prabhudutta mohanty,Sangram panigrahi, Nityananda sarma and Siddhartha sankar satapathy Department of Computer Science and Engineering,Tezpur University, Tezpur, India

[7] Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method by Udaya Suriya Raj Kumar Dhamodharan1 and Rajamani Vayanaperumal, Department of Computer Science and Engineering, Sathyabama University, Chen nai, Tamil Nadu 600 119, India

[8] G, Abikhanova, A Ahmetbekova, E Bayat, A Donbaeva, G Burkitbay (2018). International motifs and plots in the Kazakh epics in China (on the materials of the Kazakh epics in China), Opción, Año 33, No. 85. 20-43.

[9]G, Abikhanova, A Ahmetbekova, E Bayat, A Donbaeva, G Burkitbay (2018). International motifs and plots in the Kazakh epics in China (on the materials of the Kazakh epics in China), Opción, Año 33, No. 85. 20-43.

[10]Akhpanov, S. Sabitov, R. Shaykhadenov (2018). Criminal pre-trial proceedings in the Republic of Kazakhstan: Trend of the institutional transformations. Opción, Año 33. 107-125.