International Journal of Engineering & Technology, 7 (2.33) (2018) 749-751

International Journal of Engineering & Technology

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

Research paper

Wormhole attack detection in internet of things

Mrs. Sneha Deshmukh Bhosale [1] *, Dr. S. S. Sonavane [2]

[1] Asst. Professor Pune , Research Scholar, Raisoni College of Egg, Pune, Dr. D. Y. Patil Technical campus
[2] Director Lohgaon, RMD Sinhgad School of Engg
**Corresponding author E-mail: sa_bhosale@yahoo.com*

Abstract

Number of devices connected to the internet will increase in near future because of more applications arising in Internet of Things (IoT). These devices are resource constrained in terms of battery and processing power hence inserting security in constrained devices is going to be very challenging. There are many attacks taking place in Internet of Things like wormhole attack, sinkhole attack, hello flooding attack, cybil and clone ID attack etc. In this paper we are proposing a method to identify the wormhole attack taking place at routing layer of IoT. Wormhole attack is one such attack that has been recently discovered. Wormhole attack is a very severe and challenging attack because of the fact that it can be launched against any protocol and also due to its ability to be effective in case of encrypted traffic. Threats due to Wormhole attack are alterations in network, can cause failure of location dependent protocols, can penetrate wrong route/topology information into the network and defeating the purpose of routing algorithms. In this paper we are discussing various types of Intrusion Detection Systems available for IoT attacks. We have also proposed an Intrusion Detection System (IDS) for Wormhole Attack.

Keywords: *Internet of Things; Security Attacks; Wormhole Attack; IDS.*

1. Introduction

a) Internet of Things (IoT)

The scope of the internet in IoT is going to be expanded beyond computing and computers, being connected. It is going to interconnect different things like physical objects that we see around us, the different objects such as the lighting system in a room, the lights, the fans, the air conditioners and anything and everything including things such as the toothbrush, the microwave oven, the refrigerator. And not only in our homes, but also in our businesses such as internetworking of different machines, internetworking different equipment etc. So, each and everything that we see around us that we use at our home in businesses, in workplaces, everything being internet worked. So, this is the whole vision of internet work of things, internet of things.

Now, there are several challenges that are going to arise after implementation of IoT. The reason of popularity of IoT is that IoT is envisaged to be able to provide advanced level of service to the society and the business. [1] [2].

b) Need of Security in IOT

Hamid Bostani et el (2016) have explained need of security in IoT very effectively in their paper. Earlier human was connected to internet with computer but now the devices around him are connected to internet through the new technology Internet of Things. As these devices will be directly connected to insecure internet, there are many chances of attacks taking place in the network. As an example we can consider a baby monitor which can be hacked very easily giving the information of whereabouts of the person at home making it easier to burglarize.

Along with the rapid growth of IoT application and devices, cyber-attacks will also be improved and pose a more serious threat to security and privacy than ever before. Furthermore, as the IoT devices become widely used in industry, military, and other key areas, hackers can endanger public and national security. It is very difficult to implement a system which will fix the attack in Internet of Things as IoT is formed by constrained network in terms of memory, processing speed and battery life. [1] .

We in this paper are focusing more on routing/network layer attacks. RPL and 6LoWPAN are the protocols which are mainly working at routing layer. This paper contains the details of our ongoing research on design of IDS for detecting threat in IoT.

Out of various attacks taking place at routing layer of IoT protocol suite, we are mainly concentrating on wormhole attack and attacker's detection in our work. This paper is organised as follows, Section 2 contains IoT protocols at Routing Layer. Section 3 explains the Intrusion Detection System followed by details of Wormhole Attack in section 4. Section 5 has Proposed System of the IDS Design.

2. IOT protocols

a) RPL (Routing Protocol for Low Power and Lossy Network)

David Airehrour ET el (2016) explained about RPL protocol in their article. RPL is a IPv6 protocol designed especially for constrained devices in Internet of Things at network layer. This protocol is used to exchange packets between two separate networks with bidirectional communication pattern. They uses directed tree graph where nodes communicate in terms of reply to messages and forward other messages in both the directions of the tree.

RPL is a Distance Vector IPv6 routing protocol for LLNs (Low Power and Lossy Networks).In RPL network path information is organized as a set of Directed Acyclic Graphs (DAGs) and this is further classified as a set of Destination Oriented Directed Acyclic Graphs (DODAG). A DODAG built a tree like structure from root node, also known as sink node in the network. RPL has four dif-

ferent messages to operate the path between the nodes also to maintain and to exchange the data within the network.

i) DODAG Information Object (DIO): maintains information of routing graph.
ii) .DODAG Advertisement Object (DAO): routing information advertised upwards from node to sink
iii) DODAG Information Solicitation (DIS): used when new node require DIO messages from another existing node to join the network.
iv) .Destination Advertisement Object Acknowledgment (DAO-ACK): used for acknowledgement message from nodes after receiving DAO message [3].

b) 6LOWPAN (IPV6 over Low Power Wireless Personal Area Network):

Johan Becker (2017) explained about various protocols in IoT in his thesis. IoT is made up of vast heterogeneous network hence it always have limitations in terms of interoperability, among its various objects. To have less overhead compared to IPv6, a 6LoWPAN has been used in IoT with limited functionality. This protocol comes at 6LoWPAN layer of IoT network suite which acts as an adaption layer between IPv6 protocol and 802.15.4 protocol. 6LoWPAN provides supports fragmentation support to convert IPv6 packets into 127 bytes frame size which is the requirement of low power network. [4]

3. Types of IDS

Several IDSs have been proposed for Wireless Sensor Network (WSN), but those cannot be directly use for Internet of Things as IDS for WSN are not considering internet parameters such as 6LoWPAN. In IoT, unlike WSN things are directly connected to unsecured internet hence there are more chances of attacks in IoT.
Raza et el proposed the first IDS in IoT using Contiki OS named as SVELTE. In his paper he has addressed routing attacks like sinkhole attacks and selective forwarding attack. They have done the simulation using Cooja Simulator. [5]
Ghosal et el (2017) explained types of IDS in their recent paper. The four types of IDS explained by authors are Signature Based, Anomaly based, Specification Based and Hybrid based IDS.

i) Signature Based IDS

In this type of IDS, an attack pattern for specific attack is already stored. As soon as network parameters matches with the attack pattern already saved, an attack detection alarm is raised. Drawback of this method is that we cannot detect new attack which is unknown to the system.

ii) Anomaly Based IDS

This IDS overcomes the drawback of signature based IDS by detecting the attacks which are not stored by the system. It detects attack when system behaves differently from normal behavior. For this a threshold can be set for normal behavior of the system. If the network starts behaving abnormally by crossing the threshold value, a attack is detected. Anomaly based IDS cannot suitable for large network as it has to be static with its behavior to detect the abnormal reading in the network. This is one of the disadvantages of this type of IDS.

iii) Specification Based IDS

It is a combination of signature based and anomaly based IDSs. In this type it will check for specific attacks as per pattern saved and it also check with any abnormal behavior of the system. [7]

4. Overview of wormhole attack

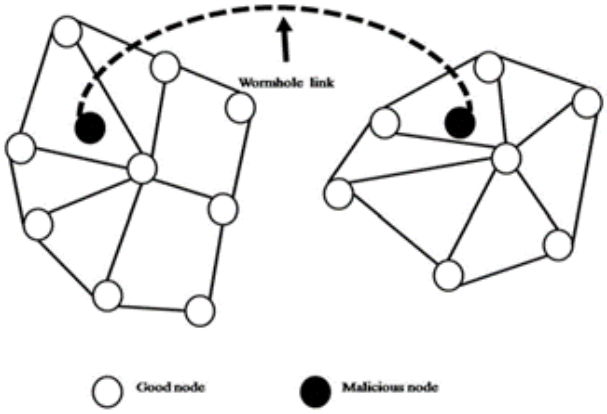

Fig. 1: Generalized Diagram of Wormhole Attack.

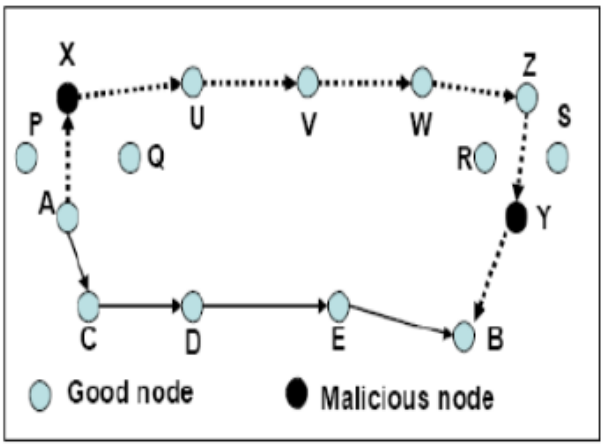

Fig. 2: Wormhole Attack Scenario.

Marianne Azer et el (2009) have given full explanation about Wormhole attack in their paper. Wormhole attack is considered to be severe attacks on IoT routing. In this attack a tunnel is established between two nodes and packet is forwarded among each other. These distant malicious nodes pretend that they are very close to each other so that neighbor nodes forward packets through them. In Fig 2 node X and Y are malicious nodes who form a tunnel from X to Y to exchange the packets. In Fig 2 if node A wants to send packet to node B, X falsely advertise that to reach B a shortest path is within X. But physically B is at far distance from node X. So packet transmission takes more time to reach to destination which is one of the symptoms of wormhole attack.
If wormhole attack is triggered in the more number of neighbor gets formed and these new neighbors are all from other end of wormhole tunnel and not in transmission range of node because, during the attack lots of control packets are going to exchange from one end of tunnel to other in that neighbor advertisement, neighbor solicitation and DIO helps in formation of neighbors beyond the transmission range. [7][8].

5. Proposed system

The proposed system is the novel Wormhole attack Detection System, basically designed for the IoT environment.

a) Architecture of the System

The proposed system's architecture is as shown in fig 3. In this architecture sensor nodes are connected to the internet using IPv6 link through the IPv6 Border Router (6BR). In centralised approach IDS can be placed at border router and in distributed approach it is placed at sensor nodes. In our architecture we are using hybrid approach where IDS is placed at both ie at border router as well as sensor nodes.

b) Distributed Module

In distribution module we are proposing following four steps:

i) Neighbour Validation: In this step neighbour Information from all sensor nodes is collected which contains destination node ID and neighbour's node ID.

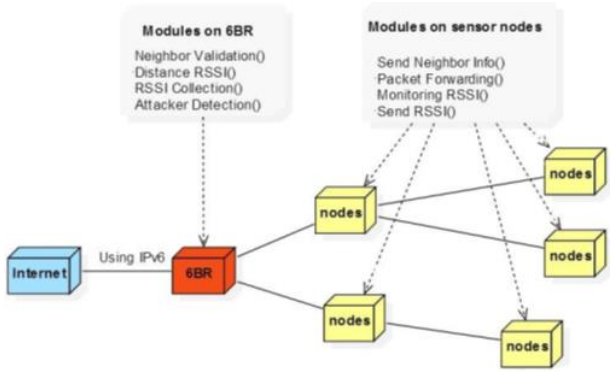

Fig. 3: Proposed System.

ii) Distance Calculation: This step calculates the distance between to nodes using euclidean distance method. For this we are using Received Signal Strength Indicator (RSSI) value which will be used to give value of distance between two coordinates.

iii) Identification of Attack: In this step, RSSI value received from victim node and neighbour node is compared with the threshold value. The RSSI value is converted into distance and vice a versa. In this step module checks whether the node has connected to valid parent, or it is connected to the parent through wormhole link. When it confirms that node has parent through wormhole tunnel, its starts hidden wormhole detection approach. And when it detects the packet dropping violation it start the exposed kind of wormhole detection method.

iv) Attacker Detection: If the distance between two nodes found to be more than transmission range of the node, then attacker node is identified. RSSI value is used to find the distance between node and the neighbour.

c) Centralized Module

i. Topology Construction: Client sends rank and ID information of node, its parent and its children's to 6BR for constriction of network topology and for detection of attack.

ii. Attack Detection: In this module node cooperates with Detection module at 6BR to detect the hidden and exposed kind of wormhole attack. Also for detection of malicious node producing wormhole tunnel.

iii. Locating Attacker Node: When a node receives the victim packet from root node or through broadcasting, it broadcasts the packet further. The two nodes record the RSSI value of each other and broadcast the victim packets to locate the attacker node.

6. Conclusion

Security is very necessary in IoT network implementation as many things which people are using daily are connected to unsecured internet. In IoT networks, secure routing plays an essential role in the seamless and safe functioning of the entire network. In this paper we have explained various security attacks in IoT. Our main focus is at wormhole attack taking place at routing layer. We have presented mathematical model which we will implement in Contiki OS with Cooja simulator and will compare the result with results obtained with other platform. We are working further to add more features in IDS design so that more attacks like sinkhole attack and selective attack will be detected.

References

[1] Hamid Bostani , Mansour Sheikhan, "Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach ", 0140-3664/© 2016, Elsevier.

[2] Ms. Snehal Deshmukh, Dr. S. S. Sonavane, "Security Protocols for Internet of Things: A Survey", ICNETS2, VIT University, Chennai, 2017, 978-1-5090-5913-3/17/$31.00_c 2017 IEEE.

[3] David Airehrour, Jairo Gutierrez, Sayan Kumar Ray, "Secure Routing for Internet of Things: A Survey", Journal of Network and Computer Applications, 2016.

[4] Johan Becker, "Intrusion Detection System Framework for Internet of Things", Thesis submitted University of Gothenburg, Sweden 2017.

[5] Shahid Raza, Linus Wallgren, and Thiemo Voigt. "SVELTE: Real-time intrusion detection in The Internet of Things."Ad hoc networks 11.8 (2013): 2661-2674.

[6] 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

[7] Marianne Azer, Sherif El-Kassas, Magdy El-Soudani, "A full of the Wormhole Attack", International Journal of Computer Science and Information Security, 2009.

[8] Weekly, Kevin, and Kristofer Pister."Evaluating sinkhole defence techniques in RPL networks." Network Protocols (ICNP), 2012 20th IEEE International Conference on. IEEE, 2012.