International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Intrusion Detection and Prevention System for IoT

Sali Pooja Anilbhai[1], Chandresh Parekh[2]
[1]M.Tech, IT & Telecommunication Department, RSU, Ahmedabad, India
[2]Assistant Professor, IT & Telecommunication Department, RSU, Ahmedabad, India

ABSTRACT

The Internet of Things (IoT) is fast emerging network of smart objects and devices. IoT infrastructure is vulnerable to various attacks, security and privacy are the key issues for IoT applications. IoT requires various security solutions where the communication is secured with confidentiality, integrity, and authentication services; the network is protected against intrusions and disruptions; and the data inside a sensor node is stored in an encrypted form. Therefore, the challenge of implementing secure and protected communication in the IoT network must be addressed. The IoT network is secured with encryption and authentication, but it cannot be protected and secured against cyber-attacks. Hence, an Intrusion Detection and Prevention System is needed. This Paper presents a design of Intrusion Detection and Prevention System to detect and prevent Hello flood attack and Sybil attack in IoT network which is implemented in Contiki OS with Cooja simulator.

Keywords: Internet of things, IDS, IPS, Security, Hello Flood Attack, Sybil Attack

I. INTRODUCTION

IoT is considered as a part of the Internet of the future and will comprise many more intelligent communicating 'things'. It refers to the physical objects that are capable of exchanging information with other physical objects and virtual components. The Internet of Things (IoT) will empower the connected things and entities with new capabilities.[1] It introduces various services and human's routine life fully depends on its available and reliable activities. Due to the fast advancing technologies of network communication, the Internet is going to connect everything from everywhere. IoT connects a large number of heterogeneous devices, such as "instance cameras", "wireless sensor network" (WSN), "smart meters," and "vehicles," while providing open access system to a variety of data generated by such devices to provide new services to civilian and companies.[2] However, as the resources of IoT's devices are constrained, many security mechanisms are hard to be implemented to protect the IoT networks. Other kinds of security enforcement methods, such as intrusion detection and prevention system should be considered to protect the IoT networks.[3]

If security issues are not addressed then the confidential and private information may be leaked at any time. Thus, the security problems must be addressed. In this, we mainly focus on the problem of achieving some of all of the following security services:

- ✓ **Confidentiality:** An attacker can easily intercept the message passing from source to the destination so that privacy can be leaked and content can be modified. So that secure message transmission is required in IoT.
- ✓ **Integrity:** Integrity means the validity of a transmitted message from sender node. Message integrity means that a message has not been tampered or altered by adversary.
- ✓ **Availability:** Data, Resources or Services must be available when required. Attackers can flood the bandwidth of system to damage the availability of resources. Availability can be damage by malicious attacks like Denial of service (DOS) attack, flooding attack, jamming attacks etc.
- ✓ **Authenticity:** **Authenticity** concerns the truthfulness of correct user on node. Users should be able to identify each other's identity with which they are communicating. So that unauthorized user or entity can't send data.
- ✓ **Authorization:** It denotes that only authorized nodes can be accessed to network services or resources.

- ✓ **Non-Repudiation:** Non-repudiation assures that the sender and receiver cannot deny having sent and received the message respectively.[4]

II. INTRUSION DETECTION SYSTEM

An intrusion is basically any sort of illegal activity which is carried out by attackers to destroy network resources or sensor nodes. An IDS is a mechanism to detect such malicious and unauthorized activities. The basic functions of IDS are to monitor users' activities and network behaviour at different layers. A single perfect defence is neither feasible nor possible in sensor networks, as there always remain some weaknesses, software bugs, or design flaws which may be compromised by intruders. It is used as a passive defence, as it is not intended to prevent attacks; instead of that it alerts network administrators about possible attacks well in time to stop or reduce the impact of the attack. The accuracy of intrusion detection is generally measured in terms of false positives (false alarms) and false negatives (attacks not detected), where the IDSs attempt to minimize this attacks.

IDS can operate in many modes. Apart from that main two operate modes are standalone operation and cooperative cluster based operation.

- ✓ A standalone IDS operates on every node or sensor to detect unwanted activities.
- ✓ Cooperative cluster based IDS are mostly distributed in nature in which every node monitors its neighbors and surrounding nodes activities; in case of any malicious activity detection, the cluster head is informed about that malicious activity.

IDS have three main components or activities as given below.

(i) Monitoring component is used for local events monitoring as well as neighbours event monitoring. This component mostly monitors traffic patterns, internal events, and resource utilization in the network.

(ii) Analysis and detection module is the main component of IDS which is based on modelling algorithm. Network operations, behaviour, events and activities are analyzed, and decisions are made to declare them as illegal or not.

(iii) Alarm component is a response generating component, which generates an alarm in case of detection of an intrusion.[5]

Types of IDS

There are two important classes of IDSs.

A.) Signature-Based Intrusion Detection Systems

These are also known as **Rule-Based IDS**, has predefined rules of different security attacks. When the network's behaviour shows any variation or gives different results from the predefined rules, it is classified as an attack. Signature-based IDSs are well suited for known intrusions. It is host based IDS in which every node has IDS system. [7]The proposed IDS are hosted on each sensor node. The IDS is basically designed for routing attacks and is capable of detecting packet-dropping attacks in network. An IDS for detection of sink-hole attack is presented in this type of system.[6]

However they can't detect new security attacks in network or those attacks having no predefined rules. Thus, this approach is very expensive. This technique can't identify new attacks unless their signatures or patterns are manually added into the database of that system. So it needs up-gradation of system database regularly with new signatures of attacks. Thus, it is a static approach. This approach has two main disadvantages: a) it requires the knowledge to form attack patterns. b) It cannot find new and previously unknown attacks.

B.) Anomaly-Based Intrusion Detection Systems

These are also known as **event-based detection** monitors network activities and classifies them as either normal or malicious using heuristic approach. [6]Most of anomaly-based IDSs identify intrusions using threshold values; that is, any activity below a threshold is normal, while any condition or activity above a threshold is classified as an intrusion. The main advantage of anomaly-based IDS is its ability to detect new and unknown attacks; however sometimes it fails to detect even well-known security attacks. This mechanism is capable of building a normal traffic model, which is used to differentiate between normal and abnormal traffic in the network .This mechanism monitors and learns normal traffic patterns in order to detect any intrusion present or not in case of deviation.

C) Hybrid Intrusion Detection Systems

These are a combination of both anomaly-based and signature-based IDS approaches. Hybrid mechanisms usually contain two detection modules; that is, one module is responsible of detecting well-known attacks using signatures, while the other is responsible for detecting and learning normal and malicious patterns or monitor network behaviour deviation from normal profile behaviour. Hybrid IDSs are more accurate in terms of attack detection with less number of false positives.[7]

III. INTRUSION PREVENTION SYSTEM

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, report it and attempt to block or stop that activity.

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity in the network. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prohibit or block intrusions that are detected.IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.[9]

Classification of IPS

Intrusion prevention systems can be classified into four different types:

1. **Network-based intrusion prevention system (NIPS)**: it monitors the entire network for suspicious traffic by analysing protocol activity.
2. **Wireless intrusion prevention systems (WIPS)**: it monitor a wireless network for suspicious traffic by analysing wireless networking protocols.
3. **Network behaviour analysis (NBA)**: it examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations.
4. **Host-based intrusion prevention system (HIPS)**: an installed software package which monitors a single host for suspicious activity by analysing events occurring within that particular host.

IV. CYBER ATTACKS ON IOT

IoT networks are exposed to different types of attacks both from internal and external. Attacks are mainly classified by two types inside and outside attacks. In an outside attack, the attacker is not a part of the network while in an inside attack, the attack can be perpetrated by compromised or malicious nodes that are part of the network. In the following, we discuss some cyber-attacks on IoT applications.[12]

A.) Spoofed, Altered, or Replayed Routing Information

One straight attack against a routing protocol is to target the routing information exchanged between nodes by spoofing, altering, or replaying routing information. Adversaries may be capable to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end to- end latency by using this type of attack.

B.) Selective Forwarding

In this particular attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any more. A simple form of this attack is: when a malicious node acts like a black hole and refuses to forward every packet it receives. However, such an attacker runs the risk that neighbouring nodes will conclude that this node has failed and decides to follow another route. A more perceptive form of this attack is when an adversary selectively forwards packets. An attacker interested in suppressing or modifying packets originating from few selected nodes can reliably forward the remaining traffic and limit suspicion of its wrongdoing.

C.) Sinkhole Attacks

In a Sinkhole attack, an attacker comes to an agreement with a node or introduces a fake node inside the network and uses that node to occur an attack. The attacker listen route requests of nodes and tries to satisfy that it has the shortest path for the base station. When the agreed node or fake node achieves to attract network traffic itself, it will create an attack. After malicious node (agreed, introduced node) achieve, they can do whatever it wants such as dropping all packets, dropping selected packets, changing content of all the packets.

D.) Wormhole Attacks

A Wormhole attack can easily be launched by the attacker without having knowledge of the entire network or compromising any legitimate nodes or cryptographic mechanisms. The attacking node captures the packets from one location and transmits them to other distant located node which distributes them locally through virtual tunnel. The wormhole puts the attacker nodes in a very strong position compared to other nodes in the network.

E.) Sybil Attacks

In Sybil attack, a single node presents multiple identities to rest of the nodes in the network either by fabricating or stealing the identities of legitimate nodes. So the base station cannot distinguish the legitimate and the forged node. This confuses other nodes and the network performance degrades. This attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage, multipath routing, and topology maintenance. Wireless sensor networks are more prone to Sybil attack because of the open and broadcast communication medium and the same frequency is being shared among all nodes in the network. [10]

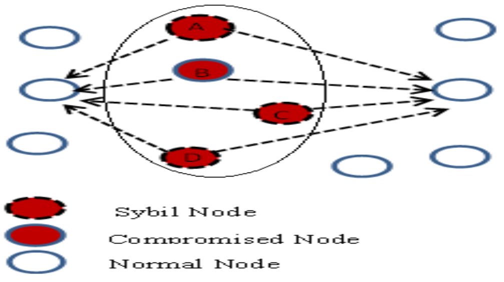

Figure 1. Sybil node

F.) Hello Flood Attacks

Hello flood attack is an attack on the network layer. Many routing protocols require nodes to broadcast Hello message to announce themselves to their neighbours, and a node receiving such a packet may assume that it is within normal radio range of the sender. This assumption may sometimes be false. For example, an adversary advertising a very high quality route to the base station to every node in the network could cause a large number of nodes to attempt to use this route, but those nodes sufficiently far away from the adversary would be sending packets into oblivion. Thus the network is left in a state of confusion. A node realizing the link to the adversary, which is not genuine, could be left with few options: all its neighbors might be attempting to forward packets to the adversary as well. Protocols which depend on localized information exchange between neighboring nodes for topology maintenance or flow control are also subject to hello flood attack.[11]

An adversary does not necessarily need to be able to construct legitimate traffic in order to use this attack. It can simply re-broadcast or retransmit overhead packets with enough power to be received by every node in the network. Hello floods can also be thought of as one-way, broadcast wormholes in the network.[10]

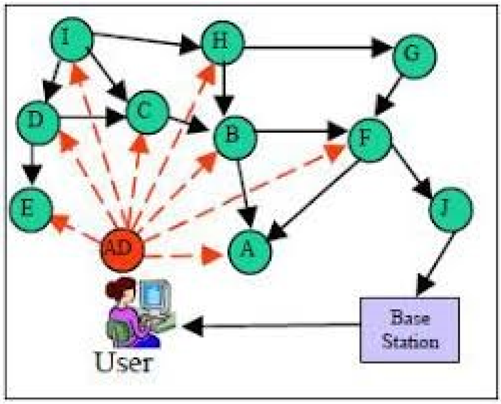

Figure 2. shows that a legitimate node considers attacker as its neighbour and also as an initiator

V. PROPOSED SYSTEM FOR VARIOUS ATTACKS

Many researchers have been working on emerging technology IoT and sensor areas to provide the best security mechanism. In this section, we described various intrusion detection and prevention systems which are proposed in recent years.

✓ P. Pongle [13] proposed novel IDS to detect wormhole attack in IoT and attacker which is implemented in Contiki OS with Cooja simulator. The proposed system in this novel uses centralized and distributed architecture for placement of IDS. In this approach, wormhole attack detected by using location information and attacker node identified by using neighbor information.

- ✓ Kasinathan [14] proposed a network based DOS attack detection IDS architecture on ebbits network framework. In this approach, IDS can listen or monitor 6LoWPAN traffic by using IDS probe. They use hybrid approach for placement of IDS. DOS protection manager is core component of proposed system which raised an alert by using information available on network manager component.
- ✓ S. Razaa [15] proposed a real-time intrusion detection system in IoT system called as SVELTE which is implemented in Contiki OS. In this approach, they proposed three main centralized elements which are placed in 6LoWPAN Border Router. The first element is 6LoWPAN Mapper which collects information about the RPL protocol in the network and rebuilds the networks in 6BR. The second element is intrusion detection element which detects the intrusion in the network by analyzing the mapped data. The third element is a distributed mini firewall which filters the malicious traffic present in the network before it reaches to the network.
- ✓ Chen Jun [16] proposed event processing based IDS to solve the problem of real time of Intrusion detection in IoT network. In this approach, they designed the IDS system on the basis of Event Processing Model (EPM). It is rule-based IDS in which rules are stored in Rule Pattern Repository and takes SQL and EPL of Epser as a reference.
- ✓ Caiming Liu, Jin Yang [17] proposed Research on Immunity-based IDS Technology for the Internet of Things. In this paper, they proposed good mechanisms in AIS (Artificial immune system) are introduced into the intrusion detection technology in the IoT environment. Through simulating and defining the immune elements in the IoT system, the applying method based on the immune theory is constructed. Math method is used to deduce the theory process of the IoT intrusion detection. The theory analysis shows that the proposed method provides a new effective approach for the IoT intrusion detection technology.

VI. CONCLUSION

Security is most important parameter in all the IoT devices and security issues of IoT cannot be ignored. We understand various security attacks and its impact on IoT applications. We found various IDS approaches to detect those attacks in related work. Those approaches have some limitations like requires more computational resources and energy for detection of attacks, no centralized mechanism is available to detect such type of attacks. There are some algorithm are available to detect Hello flood attack and Sybil attack in IoT network. But they require more energy and time. There is no prevention for such type of attacks. We hope our proposed solution will greatly help to detect and prevent hello flood attack and Sybil attack in IoT. Here we are trying to give a solution which will provide more security to the IoT network. In future we will implement the proposed method in Contiki OS with Cooja simulator.

VII. REFERENCES

[1]. Shancang Li,Li Da Xu,Shanshan Zhao,"The internet of things:a survey",Springer Information Systems Frontiers,Volume 17,Issue 2,pp 243-259,April 2015.

[2]. Yulong Fu,Zheng Yan,Jin Cao,Ousmane Kone,and Xuefei Ca,"Research Article an Automata Based Intrusion Detection Method for Internet of Things".

[3]. Shahid Raza,M¨alardalen University Doctoral Thesis"Lightweight Security Solutions bfor the Internet of Things"2013.

[4]. M.Patel and A.Aggarwal,"Security attacks in wireless sensor networks:A survey",2013 International Conference on Intelligent Systems and Signal Processing (ISSP),2013.

[5]. S.Khan,K.K.Loo,and Z.U.Din,"Framework for intrusion detection in IEEE 802.11 wireless mesh networks,"International Arab Journal of Information Technology,vol.7,no.4,pp.435-440,2010.

[6]. V.Jyothsna,V.V.Rama Prasad,"A Review of Anomaly based Intrusion Detection Systems",International Journal of Computer Applications,2011.

[7]. Nabil Ali Alrajeh,S.Khan,and Bilal Shams "Intrusion Detection Systems in Wireless Sensor Networks:A Review"Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013.

[8]. I.Krontiris,T.Dimitriou,T.Giannetsos,and M.Mpasoukos,"Intrusion detection of Sinkhole attacks in wireless sensor International Journal of Distributed Sensor Networks 7 networks,"in

Algorithmic Aspects of Wireless Sensor Networks ALGOSENSORS,vol.4837 of LectureNotes in Computer Science,pp.150-161,Springer,2008.

[9]. Suchita P.Patil,Dr.B.B.Meshram "Intrusion Prevention System"issue-2,Vol.4.May,VJTI Mumbai,India,2012.

[10]. Chris Karlof,David Wagner,"Secure Routing in Wireless Sensor Networks:Attacks and Countermeasures,"Elsevier Ad Hoc Networks 1 pp 293-315,2003.

[11]. A Hamid,S Hong,(2006) Defense against Lap-top Class Attacker in Wireless Sensor Network,ICACT.

[12]. Okan CAN,Ozgur Koray SAHINGOZ,"A Survey of Intrusion Detection Systems in Wireless Sensor Networks",6th International Conference on Modelling,Simulation,and Applied Optimization (ICMSAO),2015.

[13]. P.Pongle,G.Chavan,"Real Time Intrusion and Wormhole Attack Detection in Internet of Things",International Journal of Computer Applications (0975 -8887),July 2015.

[14]. Kasinathan,Prabhakaran,et al."Denial-of-Service detection in 6LoWPAN based internet of things."Wireless and Mobile Computing,Networking and Communications (WiMob),2013 IEEE 9th International Conference on.IEEE,2013.

[15]. S.Razaa and L.Wallgrena,"SVELTE:Real-time Intrusion Detection in the Internet of Things",Ad Hoc Networks (Elsevier),vol.11,no.8,pp.2661-2674,2013.

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

[17]. Caiming Liu,Jin Yang "Research on Immunity-based Intrusion Detection Technology for the Internet of Things",Seventh International Conference on Natural Computation 2011.