Intrusion Detection System for Internet of Things

Tariqahmad Sherasiya[1], Hardik Upadhyay[2]

[1] Research Scholar, Computer Engineering, GTU PG School, Gujarat, India
[2] Assistant Professor, Computer Engineering, GPERI, Gujarat, India

ABSTRACT

The Internet of Things (IoT) is an ever-growing network of smart objects. It refers to the physical objects are capable of exchanging information with other physical objects. It introduce various services and human's routine life depends on its available and reliable activities. The IoT requires multi-facet 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 communication in the IoT network must be addressed. The IoT network is secured with encryption and authentication, but it cannot be protected against cyber-attacks. Hence, an Intrusion Detection System is needed. In this paper we proposed a Lightweight Intrusion Detection System to detect Hello flood attack and Sybil attack in IoT network.

Keyword: - *Internet of things, IDS, Security, WSN, 6LoWPAN, Hello Flood Attack, Sybil Attack.*

1. INTRODUCTION

The Internet of Things (IoT) is a smart network which connects all things to the internet for the purpose of exchanging information with agreed protocols [1]. So, anyone can access anything, at any time and from anywhere [2]. In IoT network, things or objects are wirelessly connected with smart tiny sensors. IoT devices can interact with each other without human intervention [3]. IoT uses unique addressing schemes to interact with other objects/things and cooperate with objects to create new applications or services. IoT introduces various applications like smart homes, smart cities, health monitoring, smart environment, and smart water [4]. With the development of IoT applications, there are so many issues raised. Among many other issues, security issue of IoT cannot be ignored. IoT devices are accessed from anywhere via untrusted network like the internet so IoT networks are unprotected against a wide range of malicious attacks. If security issues are not addressed then the confidential information may be leaked at any time. Thus, the security problem must be addressed.

- **Confidentiality:** An attacker can easily intercept the message passing from sender to the receiver so that privacy can be leaked and content can be modified [5]. So that secure message passing is required in IoT.
- **Integrity:** The message must not be altered in transit; it should be received at receiver node same as it is sent at sender node. Integrity guarantees that message has not been altered by unauthorized persons while in transmission [5].
- **Availability:** Data or resources must be available when required [5]. Attackers can flood the bandwidth of resources to damage the availability. Availability can be damage by malicious attacks like Denial of service (DOS) attack, flooding attack, black hole attack, jamming attacks etc.
- **Authenticity:** Authenticity involves proof of identity [6]. Users should be able to identify each other's identity with which they are interacting. It can be verified through authentication process so the unauthorized entity cannot participate in the communication [7].
- **Non-Repudiation:** Non-repudiation ensures that the sender and receiver cannot deny having sent and received the message respectively [8].

- **Data Freshness:** Data must be recent whenever required. It guarantees that the no old messages replayed by an adversary [9].

1.1 Intrusion Detection System

Intrusion Detection System (IDS) is used to monitor the malicious traffic in particular node and network. It can act as a second line of defense which can defend the network from intruders [10]. Intrusion is an unwanted or malicious activity which is harmful to sensor nodes. IDS can be a software or hardware tools. IDS can inspect and investigate machines and user actions, detect signatures of well-known attacks and identify malicious network activity. The goal of IDS is to observe the networks and nodes, detect various intrusions in the network, and alert the users after intrusions had been detected. The IDS works as an alarm or network observer. It avoids damage of the systems by generating an alert before the attackers begin to attack. It can detect both internal and external attacks. Internal attacks are launched by malicious or compromised nodes that belong to the network whereas external attacks are launched by third parties which are initiated by outside network. IDS detects the network packets and determine whether they are intruders or legitimate users. There mainly three components of IDS: Monitoring, Analysis and detection, Alarm [11]. The monitoring module monitors the network traffics, patterns and resources. Analysis and Detection is a core component of IDS which detects the intrusions according to specified algorithm. Alarm module raised an alarm if intrusion is detected [11].

1.2 Types of IDS

1) **Signature Based IDS:** Signature based IDS matches the existing profile of the network against pre-defined attack patterns or signatures. It is also known as a rule-based detection technique. Signatures or patterns are pre-defined, stored in the database and each attack can be detected according to patterns or signatures. This technique is simple to use. This technique only requires patterns of individual attacks and must also store those patterns in some database. This approach needs specific knowledge of the individual attack. It needs more storage space with increasing the number of attacks. Thus, this approach is very expensive. This technique cannot identify new attacks unless their signatures or patterns are manually added into the database. So it needs up-gradation of database regularly with new signatures of attacks [12]. Thus, it is a static approach. This approach has two main disadvantages: a) it needs the knowledge to form attack patterns. b) It cannot discover new and previously unknown attacks [13].
2) **Anomaly Based IDS:** This technique is also known as event-based detection. This technique identifies malicious activities by analyzing the event. Firstly, it defines the normal behaviour of the network. Then, if any activity differs from normal behaviour then its mark as an intrusion [14]. In this approach, a malicious node can be detected by matching the current protocol specification with previously defined protocol state. This approach detects attacks more efficiently than Signature based IDS. The main concepts behind this kind of security mechanisms are copied from statistical behaviour modelling, which identifies malicious contents in a precise and reliable way with giving a little incorrect positives rates. Automated training is generally used to define a normal behaviour of the system. It is a very costly method for resource-constrained objects [13].
3) **Specification Based IDS:** This technique is somewhat similar to anomaly detection technique. In this technique, the normal behaviour of the network is defined by manually, so it gives less incorrect positives rate. This technique attempts to excerpt best between signature-based and anomaly based detection approaches by trying to clarify deviations from normal behavioural patterns that are created neither by the training data nor by the machine learning method. The development of attack or protocol specification is done by manually so it takes more time. So, this can be a disadvantage of this approach [13].

2. CYBER ATTACKS ON IOT APPLICATIONS

IoT networks are exposed to various 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 initiated by compromised or malicious nodes that are part of the network. In the following, we discuss some potential cyber-attacks on IoT applications.

- **Sinkhole Attack:** In this attack, malicious node at-tracts network traffic towards it. To launch these types of attack, a malicious node attract all adjacent nodes to forward their packets through the malicious node by showing its routing cost minimum. The attacker creates an attack by introducing false node inside a network [15].

- **Wormhole Attack**: In this attack, the adversary node creates a virtual tunnel between two ends. An adversary node acts as a forwarding node between two actual nodes. The two malicious nodes usually claim that they are one hop away from the base station. The wormhole attack can also be used to convince two distinct nodes that they are the neighbors by relaying packets between two of them [15], [16].
- **Selective Forwarding Attack:** In this attack, malicious node acts as a normal node but it selectively drops some packets [15]. Black hole attack is the simplest form of selective forwarding attack in which all packets are dropped by the malicious node.
- **Sybil Attack:** In this attack, the node has multiple identities. The routing protocol, detection algorithm and co-operation processes can be attacked by a malicious node [15].
- **Hello Flood Attack:** In a sensor network, the routing protocol broadcast hello message to announce its presence to its neighbors. A node which receives the hello message may assume that the source node is within its communication range and add this source node to its neighbor list [16].
- **Denial of Service (DOS) Attack:** This attack can damage the availability of resources. When this attack is made, resources are not available to legitimate users. Such type of attacks, when launched by various malicious nodes is called DDoS. This attack may affect the network resources, bandwidth, CPU time etc.

3. LITERATURE REVIEW

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

P. Pongle [17] proposed a novel IDS to detect wormhole attack and attacker which is implemented in Contiki OS with Cooja simulator. The proposed system 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 [18] proposed a network based DOS detection IDS architecture on ebbits network framework. In this approach, IDS can listen or monitor 6LoWPAN traffic by using IDS probe. They used 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.

Le [19] proposed an IDS to detect topology attacks like rank and local repair attack. Finite state machine approach is used in proposed system. FSM is monitors the flow of the object which is implemented on each monitor node. If any malicious node breaks the rule rank then attack is detected. If there is no change in rank rule then monitor node checks the behaviour of suspected nodes and identifies the attacker. For detection of local repair attack, there is one threshold used. If there are threshold exceeds then alarm is raised of local repair attack.

S. Razaa [20] proposed a real-time intrusion detection system in IoT called as SVELTE which is implemented in Contiki OS. In this approach, there are three main centralized elements which are placed in 6LoWPAN Border Router. The first element is 6LoWPAN Mapper which collects information about the RPL protocol and rebuild the networks in 6BR. The second element is intrusion detection element which detects the intrusion by analyzing the mapped data. The third element is a distributed mini firewall which filters the malicious traffic before it reaches to the network.

Chen Jun [21] proposed event processing based IDS to solve the problem of real time of IDS in IoT network. In this approach, they designed the IDS architecture 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.

4. PROPOSED METHOD

This section contains the description of proposed solution for detection of Hello flood attack and Sybil attack. All the above approaches are limited to mobile ad-hoc network. Those approaches have some limitations in terms of computational overhead. Thus, those approaches are heavyweight so it is not suitable for IoT environment. There is no centralized approach available to detect hello flood attack and Sybil attack in IoT network. To overcome these limitations we propose lightweight approach to detect hello flood attack and Sybil attack in IoT network. Our proposed system is designed to detect Hello flood attack and Sybil attack in IoT environment. We used hybrid approach for placement of IDS in the IoT network. The architecture of IDS is show in Fig-1 in which all sensor nodes are connected to internet using IPv6 border router (6BR). The placement for IDS system uses hybrid approach, in which Centralized module on 6BR (GIDS) and Distributed module (NIDS) on the sensor nodes which

cooperates with each other to detect attacks. Centralized module detects the hello flood attack and distributed module detects the Sybil attack and attacker.

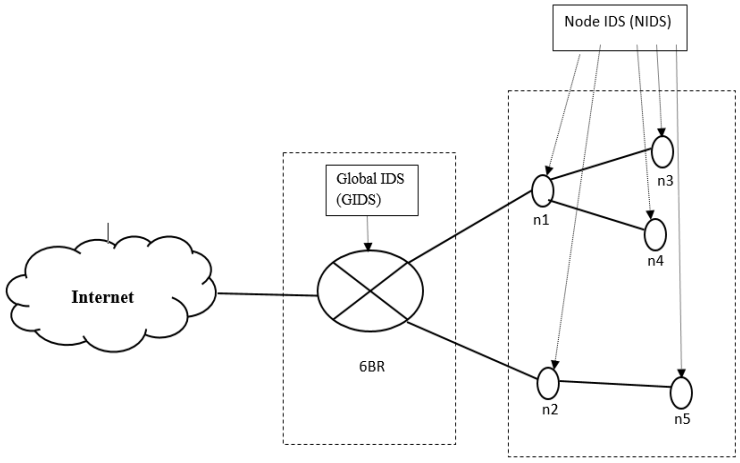

Fig-1: Architecture of IDS

4.1 Proposed Algorithm

Our proposed algorithm is mainly divided into two parts, one for hello flood attack detection on centralized module (6BR) and another for Sybil attack detection on each sensor node.

1) Algorithm for detection of Hello Flood attack on 6BR

Following are some assumptions which take care before implementing algorithm.

- Communication is within fixed transmission range.
- All the nodes in a fixed transmission range have same transmitting and receiving signal strength.
- Initially, fixed signal strength is calculated using two ray propagation model.
  - $P_r=(P_t*G_t*G_r*H_t^2*H_r^2) / (d^4*L)$ [22]
- RSSI is a Receive Signal Strength Indicator.

Algorithm:

1. Collect RSSI value of each node
2. **If** RSSI value = Fixed Signal Strength (Pr) **then**
   - Add the node to the network
3. **Else:**
   - Add node into blacklist
   -Generate an alert for attack
4. **End**

2) Algorithm for detection of Sybil Attack on the sensor node

1. Each node gets secret key from 6BR node.
2. Each node sends test message to all its neighbors. This message contains id, location and secret key.
3. Each node maintains a table which stores the information received from neighboring nodes.
4. When new message received by any node it compares the id, location and secret key with available information in the table.
5. If match is found then message will be stored otherwise node is removed from the network.

5. CONCLUSIONS

The Internet of Things is a smart network which connects physical objects to the internet for the purpose of communication. With the development of IoT, there are so many issues raised. Here we conclude that by end of this

report, security issues of IoT cannot be ignored. We understand various security attacks and its impact which are made 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 for detection of attacks, no centralized mechanism is available to detect attacks. There is no solution available to detect Hello flood attack and Sybil attack in IoT network. We hope our proposed solution will greatly help to detect hello flood attack and Sybil attack in IoT. Here we are trying to give a solution which will add more security to the IoT network. In future we will implement the proposed method in Contiki OS with Cooja simulator.

6. REFERENCES

[1]. Shanzhi Chen, Hui Xu, Dake Liu, Bo Hu, Hucheng Wang, "A Vision of IoT: Applications, Challenges, and Opportunities with China Perspective", IEEE Internet of Things Journal, Vol. 1, No. 4, August 2014.
[2]. Raja Benabdessalem1, Mohamed Hamdi1, Tai-Hoon Kim2,"A Survey on Security Models, Techniques, and Tools for the Internet of Things", 7th International Conference on Advanced Software Engineering & Its Applications, 2014.
[3]. 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.
[4]. P. Gokul Sai Sreeram, Chandra Mohan Reddy Sivappagari, "Development of Industrial Intrusion Detection and Moni-toring Using Internet of Things", International Journal of Technical Research and Applications, 2015.
[5]. M. Patel and A. Aggarwal, "Security attacks in wireless sensor networks: A survey", 2013 International Conference on Intelligent Systems and Signal Processing (ISSP), 2013.
[6]. L. Clemmer, Information Security Concepts: Authenticity. http://www.brighthub.com/computing/smb-security/articles/31234.aspx.
[7]. Shyam Nandan Kumar, "Review on Network Security and Cryptography", International Transaction of Electrical and Computer Engineers System, vol. 3, no. 1, pp. 1-11, 2015.
[8]. Mrs. V. Umadevi Chezhian, Dr. Ramar2, Mr.Zaheer Uddin Khan, "Security Requirements in Mobile Ad Hoc Networks", International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, no. 2, pp. 45-49, 2012.
[9]. M. Hossain, M. Fotouhi and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", 2015 IEEE World Congress on Services, 2015.
[10]. A. Anand, B. Patel, "An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols", International Journal of Advanced Re-search in Computer Science and Software Engineering, vol. 2, no. 8, 2012.
[11]. Nabil Ali Alrajeh, S. Khan, and Bilal Shams, "Intrusion Detection Systems in Wireless Sensor Networks: A Review", International Journal of Distributed Sensor Networks, vol. 2013, Article ID 167575, 7 pages, 2013.
[12]. Neha Maharaj, Pooja Khanna, "A Comparative Analysis of Different Classification Techniques for Intrusion Detection System", International Journal of Computer Applications, 2014.
[13]. Joo P. Amaral, Lus M. Oliveira, Joel J. P. C. Rodrigues, Guangjie Han, Lei Shu, "Policy and Network-based Intrusion Detection System for IPv6-enabled Wireless Sensor Net-works", IEEE ICC 2014 - Communications Software, Ser-vices and Multimedia Applications Symposium, IEEE DOI: 10.1109/ICC.2014.6883583.
[14]. V. Jyothsna, V. V. Rama Prasad, "A Review of Anomaly based Intrusion Detection Systems", International Journal of Computer Applications, 2011.
[15]. Okan CAN, Ozgur Koray SAHINGOZ, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks", 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), 2015.
[16]. Abdur Rahaman Sardar, Rashmi Ranjan Sahoo, Moutushi Singh, Souvik Sarkar, Jamuna Kanta Singh, and Koushik Ma-jumder, "Intelligent Intrusion Detection System in Wireless Sensor Network", Proc. of the 3rd Int. Conf. on Front. Of Intell. Comput. (FICTA), 2014 Vol. 2, Advances in Intelligent Systems and Computing 328, Springer DOI: 10.1007/978-3-319-12012-6 78.
[17]. P. Pongle, G. Chavan, "Real Time Intrusion and Wormhole Attack Detection in Internet of Things", International Journal of Computer Applications (0975 - 8887), July 2015.
[18]. 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.
[19]. Le, Anhtuan, et al. "Specification-based IDS for securing RPL from topology attacks." Wireless Days (WD), 2011 IFIP. IEEE, 2011.
[20]. 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.
[21]. 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.
[22]. T.S.Rappaport, (200), Wireless communication: Principles and practice, prentice hall 2nd edition.