International Journal of Computer Science and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 5, Issue 2, Feb - Mar 2016, 91-98

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

A SURVEY: INTRUSION DETECTION SYSTEM FOR INTERNET OF THINGS

TARIQAHMAD SHERASIYA[1], HARDIK UPADHYAY[2] & HIREN B PATEL[3]

[1]Research Scholar, GTU PG School, Ahmadabad, India

[2]Assistant Professor, GPERI, Mehsana, India

[3]Professor, Sankalchand Patel College of Engineering, Visnagar, 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 introduces various services and human's routine life depends on its available and reliable activities. 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, the Intrusion Detection System (IDS) is needed. In this paper, we discuss some security attacks and various intrusion detection approaches to mitigate those attacks.

KEYWORDS: Internet of Things, IDS, Security, WSN, 6LoWPAN

INTRODUCTION

Internet of Things

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 [25]. 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 entrusted 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 [19]. 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 [19].
- **Availability:** Data or resources must be available when required [19]. 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 [20]. 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 [21].
- **Non-Repudiation:** Non-repudiation ensures that the sender and receiver cannot deny having sent and received the message respectively [22].
- **Data Freshness:** Data must be recent whenever required. It guarantees that the no old messages replayed by an adversary [23].

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 [26]. 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 who are initiated by outside network. IDS detect the network packets and determine whether they are intruders or legitimate users. There mainly three components of IDS: Monitoring, Analysis and detection, Alarm [24]. 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 [24].

Types of IDS

- **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 [29]. 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 [4].
- **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 behavior of the network. Then, if any activity differs from normal behavior then its mark as an intrusion [30] 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 behavior modeling, which identifies malicious contents in a precise and reliable way with

giving little incorrect positives rates. Automated training is generally used to define a normal behavior of the system. It is a very costly method for resource- constrained objects [4].

- **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 behavioral 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 [4].

INTERNET OF THINGS ARCHITECTURE

There are three main layers of IoT system architecture as shown in Figure 1: Application (Service) layer, Network (Transportation) layer and Perception layer

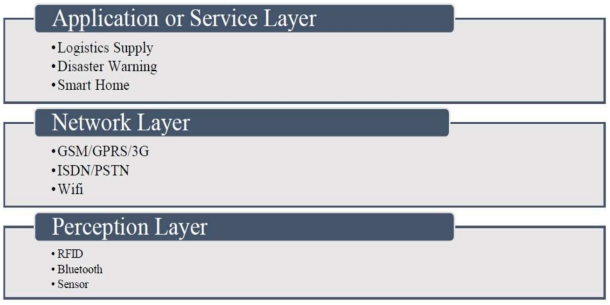

Figure 1: Internet of Things Architecture [5]

The Perception Layer

It is the primary layer of IOT. This layer can collect and observes all types of information which are used in IoT environment. This information can be captured by using the sound sensors, RFID sensors, temperature sensors, camera, GPS etc. [5] There are two parts of perception layer: i) the perception node which is used for data control and ii) the perception network which is used to sends data to the controller [18].

The Network (Transportation) Layer

This layer also known as transportation layer. This layer has transmission capabilities to transfer data from lower layer to upper layer [5]. This layer can also transmit the information or data via the internet. So this layer can combine various heterogeneous networks [18].

The Application (Service) Layer

This layer also known as a service layer this layer converts information into content and provides a good user interface (UI) to a higher level or end users. The main problem with this layer is share information with communities in a secure way so no unauthorized person can read it [5].

CYBER ATTACKS ON IOT APPLICATIONS

Sensor 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 [6].
- **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 [6], [7].
- **Selective Forwarding Attack:** In this attack, malicious node acts as a normal node but it selectively drops some packets [6]. 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 [6].
- **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 [7].
- **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.

EXISTING IDS APPROACHES

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.

Rule-Based Approaches

Chen Jun [8] 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. According to obtained result, this approach consumed more CPU resources, consumed less memory and took less processing time than traditional IDS.

Ms. T. Eswari [9] proposed a rule-based intrusion detection system framework for wireless sensor network. There are three main phases of this approach. The first phase is local auditing phase which validates the packets to verify that packet is arriving from a valid neighboring node or not. The second phase is rule application phase which works in promiscuous mode. The third phase is intrusion detection phase which detects routing attacks by validating data collected from content suppression unit. This security mechanism can be able to detect only routing attacks.

Anomaly Based Approaches

Abdulaziz Alsadhan [10] proposed an optimized intrusion detection system using soft computing technique. The main objective of proposed security mechanism is to increase the performance of the system and identify each activity in a robust way. They proposed and implemented soft computing techniques like PCA, LDA, LBP, PSO, Greedy Search, SVM and MLP. In this approach, the number of features is reduced with the increasing of detection rates.

Yousef EL Mourabit [11] proposed an intrusion detection system in WSN based on mobile agent. This approach uses multi-agent and a classification based approach for detection of intrusions. There are three mobile agents are used to detect the intrusions. The first agent is collector agent which collects the data from the wireless environment and gives feedback to the misuse detection agent. The second agent is misuse detection agent which detects the known attacks using misuse detection technique. The third agent is anomaly detection agent which detects the unknown attacks by using SVM classification algorithm. The proposed system has fewer parameters to characterize the attacks so work can be enhanced by creating more complex detection parameters and using statistical anomalies detection and enabling the creation of attack signatures.

Sandhya G [12] proposed IDS in wireless sensor network using genetic k-means algorithm. In this approach, the false positive rate is reduced and high detection rate is achieved. This algorithm is more suit- able for dynamic topologies. It acts as intelligent IDS that can analyze generated intrusion alerts and it also can detect new attacks without any pre-defined patterns or signatures.

Hierarchical Energy Efficient Based Approaches

Samir Athmani [13] proposed a hierarchical energy efficient IDS to detect black hole attacks in WSN which is implemented in NS2 network simulator. In this approach, sensor node and base station are ex- changing control packets with each other. Each control packet contains the node id and number of packets sent to the cluster head. The base station is working on monitor mode to detect black hole attacks. This approach also consumes the less energy for intrusion detection. They don't give a guarantee that proposed approach can detect all black hole attacks, but it can reduce the impact of attacks.

A. Babu Karuppiah [14] proposed an energy efficient IDS to detect Sybil node in WSN. The proposed system defines two cases. In the first case, centralized approach is implemented to send and acknowledge the query of data packets. Cluster head maintains a table which is used to store identities and positions of all nodes. In the second case, all legitimate nodes reply to the cluster head with their identities and current position coordinates. Sybil node also sends their identities and current position so cluster head matches those data in a table with legitimate nodes data. Sybil node is detected if any conflict rose. Simulation result shows that proposed system improves the energy efficiency and it detects the Sybil node accurately.

Distributed Detection Based Approach

N. Dharini [15] proposed a distributed detection approach to detect flooding and gray whole attacks in WSN which is implemented in NS2 simulator with MANNASIM framework. In this approach, abnormality of the nodes behaviour observed by a light weight energy prediction algorithm. In this system cluster head is responsible for energy prediction for all nodes in the cluster. The attack can be detected by abnormalities between predicted and actual energy. Detection accuracy is achieved by obtaining high prediction accuracy. According to the result, we can say that this

mechanism is energy saving mechanism. This approach can only detect gray whole and flooding attacks.

Cluster-Based Approach

Christian Cervantes [16] proposed IDS to detect sinkhole attacks for IoT called as INTI which is implemented in Cooja simulator. The proposed system defines four modules. The first module is Cluster con- figure ration module which is responsible for classifying a node like members, leaders and associated according to their network functions. The second one is monitoring of routing module in which observer node monitors the number of transmissions is performed. The third one is attacker detection module which detects the sinkhole attacking node. The fourth module is the isolation of attacker module which isolates the malicious node from the cluster and it also raised an alarm to inform its neighboring nodes. The simulation result shows that 92% detection rate is achieved. This approach only detects sinkhole attacks so work can be enhanced by detection of other types of attacks.

Hybrid Approach

Shahid Raza [17] proposed a real-time intrusion detection system in IoT called as SVELTE. SVELTE is only IDS available in IoT 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 Mapped 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. This approach can only detect spoofing attacks inside the network, sinkhole and selective forwarding attacks.

CONCLUSIONS

In this paper, we made an attempt to provide a survey on the intrusion detection system for the internet of things. With the development of IoT, there are so many issues raised. Among many other issues, security issues cannot be ignored. Here we discussed some potential security attacks which are made on IoT applications and various intrusion detection approaches which are available to mitigate those attacks. Still those approaches cannot be able to detect all types of cyber-attacks and are not feasible for IoT network because it requires more processing power, memory and bandwidth for intrusion detection. Thus, future research in this direction would be to develop lightweight security mechanism which will take fewer resources for intrusion detection.

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. 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.

5. Xiaolin Jia, Quanyuan Feng, Taihua Fan, Quanshui Lei, "RFID technology and its applications in Internet of Things (IoT)", 2nd International Conference on Consumer Electron- ics, Communications and Networks (CECNet), IEEE DOI: 10.1109/CECNet.2012.6201508, 2012.
6. 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.
7. 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.
8. 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.
9. Ms. T. Eswari, Dr. V. Vanitha, "A novel Rule Based Intrusion Detection Framework For Wireless Sensor Networks", International Conference on Information Communication and Embedded Systems (ICICES), IEEE DOI: 10.1109/ICI- CES.2013.6508172, 2013.
10. Abdulaziz Alsadhan, Naveed Khan," A Proposed Optimized and Efficient Intrusion Detection System for Wireless Sensor Network", World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, Vol: 7, No: 12, 2013.
11. Yousef EL Mourabit, Ahmed Toumanari, Anouar Bouirden, Hicham zougagh, Rachid Latif, "Intrusion Detection System In wireless Sensor network Based On Mobile Agent", Second World Conference on Complex Systems (WCCS), IEEE DOI: 10.1109/ICoCS.2014.7060910, 2014.
12. Sandhya G, Anitha Julian,"Intrusion Detection in Wireless Sensor Network Using Genetic K-Means Algorithm", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), IEEE DOI: 10.1109/ICACCCT.2014.7019418, 2014.
13. Samir Athmani, Djallel Eddine Boubiche and Azeddine Bilami, "Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs", Published in Computer and Information Technology (WCCIT), 2013.
14. A. Babu Karuppiah, J. Dalfiah, K. Yuvashri, S. Rajaram, Al-Sakib Khan Pathan, "A Novel Energy-Efficient Sybil Node Detection Algorithm for Intrusion Detection System in Wireless Sensor Networks" 3rd International Conference on Eco-friendly Computing and Communication Systems, 2014.
15. N. Dharini, Ranjith Balakrishnan and A. Pravin Renold, "Distributed Detection of Flooding and Gray Hole Attacks in Wireless Sensor Network", International Conference on Smart Technologies and Management for Computing, Com- munication, Controls, Energy and Materials (ICSTM), 2015.

16. Christian Cervantes, Diego Poplade, Michele Nogueira and Aldri Santos,"Detection of Sinkhole Attacks for Support- ing Secure Routing on 6LoWPAN for Internet of Things", IFIP/IEEE International Symposium on Integrated Network Management (IM), 2015.
17. Shahid Raza and Linus Wallgrena, Thiemo Voigt," SVELTE: Real-time Intrusion Detection in the Internet of Things," Ad Hoc Networks (Elsevier), Vol. 11, No. 8, pp. 2661-2674, 2013.
18. Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qiu, "Security of the Internet of Things: perspectives and challenges", Published in Springer journal of Mobile Communication, Computation and Information, November 2014, Volume 20, Issue 8, pp 2481-2501.
19. M. Patel and A. Aggarwal," Security attacks in wireless sensor networks: A survey", 2013 International Conference on Intelligent Systems and Signal Processing (ISSP), 2013.
20. L. Clemmer, Information Security Concepts:Authenticity. [Online] Available:

    http://www.brighthub.com/computing/smb- security/articles/31234.aspx.
21. 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
22. 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.
23. 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.
24. 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.
25. 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
26. 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
27. A. Sen and P. Jain," Technique of intrusion detection based on Neural Network- A review", 2014 Conference on IT in Business, Industry and Government (CSIBIG), 2014.
28. Sans.org, Intrusion Detection Systems: Definition, Need and Challenges. [On- line]. Available:

    https://www.sans.org/reading- room/whitepapers/detection/intrusion-detection-systems- definition-challenges-343
29. Neha Maharaj, Pooja Khanna," A Comparative Analysis of Different Classification Techniques for Intrusion Detection System", International Journal of Computer Applications, 2014.
30. V. Jyothsna, V. V. Rama Prasad," A Review of Anomaly based Intrusion Detection Systems", International Journal of Computer Applications, 2011.