International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 24 (2019) pp. 4462-4466


# Intrusion Detection Techniques Used For Internet of Things

**M.Bhargavi[1], M.Nandha Kumar[2], N. Venkata Meenakshi[3], and N.Lasya[4]**

*[1] Associate Professor, [2]Student, [3]Student, [4]Student,*

*[1,2,3,4]Department of Computer Science and Engineering, Audisankara College of Engineering & Technology (ASCET), Gudur, Nellore District, Andhra Pradesh, India.*

**Abstract**

Internet of Things (IoT) is a collection of embedded devices as a network in daily life. It comprises of electronics, connectivity and coding. Users are communicating with these devices but enable to control or access information. Providing security and privacy to the data in these networks is a crucial task and there is a need of intrusion detection systems (IDSs) developed for the IoT related security attacks. This article provides a study of new IDSs techniques developed for the IoT network model and to the layers. Key considerations for the development of such IDSs square measure introduced as a future outlook at the tip of this survey.

**Keywords:** Internet of Things, IDS, Detection, Techniques.

## 1. INTRODUCTION

### 1.1 Internet of Things

One of the leading technical progressions of computing is "Internet of Things" (IoT). The IoT carries in numerous services, promising individuals' personal lives obtained from the reliable process. It is forecasted that by 2022 trillion IP objects (addresses) will be associated with the internet. Low accessibility and obscurity of many devices in the massive heterogeneous network makes it problematic to observe the flow of data. However, to protect networks, the intruders who are unauthorized should be identified within the limitations of each kind of device before distributing the system information [3].

The concept of IoT is rapidly increasing into different industrial areas comprising automotive, logistics and health care. IoT environment attains enormous prominence for ensuring security and safety of both connectivity and information [4]. Contemporarily, the security of data is maintained via authenticating and encrypting mechanism. Nevertheless, the tools which are used for security cannot guarantee the complete protection in contrast to malevolent intruders. Consequently, an efficient and appropriate Intrusion detection system (IDS) is obligatory for ensuring the security in the IoT.

There are lightweight encryption techniques that have been regarded as the main technology for building IoT's security mechanism. However, taking into consideration the rapid rise in the computation capacity of the hackers, which generally include the application of Distributed Computing, Cloud Computing, and Quantum computation among others, lightweight cryptography techniques will stop being used in the coming years. The other types of security enforcement techniques like the use of systems for detecting intrusion ought to be used to ensure that IoT networks are protected in the right manner [5-6].

### 1.2 Cyber Attacks On IoT Applications

Sensor networks square measure exposed to numerous varieties of attacks each from internal and external. Attacks are mainly classified by two types inside and outside attacks. In an out of doors 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**: during this attack, malicious node at- tracts network traffic towards it. To launch these kinds 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 [1].

**Wormhole Attack**: during this attack, the adversary node creates a virtual tunnel between two ends. An person node acts as a forwarding node between 2 actual nodes. The two malicious nodes sometimes claim that they're one hop off from the bottom 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 [1], [2].

**Selective Forwarding Attack**: In this attack, malicious node acts as a normal node but it selectively drops some packets [1]. Black hole attack is that the simplest style of selective forwarding attack during which all packets square measure born by the malicious node.

**Sybil Attack**: during this attack, the node has multiple identities. The routing protocol, detection algorithm and cooperation processes can be attacked by a malicious node [2].

**Hello Flood Attack**: in a very sensing element 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 [2].

**Denial of Service (DOS) Attack**: This attack will harm the supply of resources. When this attack is created, resources are not available to legitimate users. Such kind of attacks, when launched by various malicious nodes is called DDoS. This attack might have an effect on the network resources, bandwidth, CPU time etc.

### 1.3 Intrusion Detection System

Intrusion Detection System is used to monitor the malicious traffic in particular node and network. It will act as a second line of defense which may defend the network from intruders [26]. Intrusion is associate unwanted or malicious activity that is harmful to sensing element nodes. IDS can be a software or hardware tools. IDS will examine and investigate machines and user actions, detect signatures of well-known attacks and identify malicious network activity. The goal of IDS is to watch the networks and nodes, detect various intrusions in the network, and alert the users after intrusions had been detected. The IDS works as associate alarm or network observer it avoids harm of the systems by generating associate alert before the attackers begin to attack. It can detect both internal and external attacks.

Internal attacks square measure launched by malicious or compromised nodes that belong to the network whereas external attacks square measure launched by third parties UN agency square measure initiated by outside network. IDS find the network packets and confirm whether or not they square measure intruders or legitimate users.

There chiefly 3 elements of IDS: observance, Analysis and detection, Alarm [24]. The monitoring module monitors the network traffics, patterns and resources. Analysis and Detection may be a core element of IDS that detects the intrusions in keeping with nominative algorithmic rule. Alarm module raised associate alarm if intrusion is detected [24].

## 2. EXISTING IDS APPROACHES

Many researchers are performing on IoT and wireless sensing element areas to produce the most effective security mechanism. In this section, we tend to delineated numerous intrusion detection systems that area unit planned in recent years.

An IDS depends on algorithms for implementing the assorted stages of intrusion detection. There area unit a massive range of algorithms for all IDS sorts and ways. Some of these IDS algorithms are going to be mentioned in short within the section titled 'IDSs Designed for IoT Systems'. Additionally, a number of these IDS algorithms is used for multiple totally different detection techniques. Thus this section focuses on light-weight anomaly-based IDS algorithms which will be utilized in IoT-based environments counting on the complexness, execution time and detection time necessities. Principal component analysis (PCA) is a lightweight algorithm that can be used for various detection techniques in IDSs; thus, In IDSs, PCA is used as a dimensionality reduction and detection technique. Elrawy et al. used the PCA approach to make AN anomaly-based applied mathematics and data processing IDS that depends on the division of the principal elements into the foremost and least important principal components [7,8].

In this system, the detection stage depends on the main principal element score and also the minor principal element score. In addition, PCA has been used in intrusion detection techniques based on payload modeling, statistical modeling, data mining and machine learning [7-9].

**Misuse-based intrusion detection**

A misuse-based intrusion detection technique uses a database of known signatures and patterns of malicious codes and intrusions to detect well-known attacks [11]. Network packet overload, the high cost of signature matching, and the large number of false alarms are three disadvantages of misuse-based IDSs [12]. In addition, the severe memory constraints in some styles of networks, such as WSNs, result in low performance of misuse-based IDSs because of their need to store a large database of attack signatures [13]. Moreover, the signature and pattern databases in signature-based IDSs and pattern-matching IDSs got to be unceasingly updated. Such misuse-based IDSs area unit designed to find malicious attacks and intrusions supported previous data.

**Anomaly-based intrusion detection**

In AN anomaly-based intrusion detection technique, a normal data pattern is created based on data from normal users and is then compared against current data patterns in an online manner to detect anomalies [14]. Such anomalies arise due to noise or other phenomena that have some probability of being created by hacking tool. Thus, anomalies are unusual behaviors caused by intruders that leave footprints in the computing environment [15]. These footprints area unit detected so as to spot attacks, particularly unknown attacks.

An anomaly-based IDS operates by creating a model of the normal behavior in the computing environment, which is continuously updated, based on data from normal users and using this model to detect any deviation from normal behavior [16].

**a.** A **data mining approach** is a means for extracting knowledge from a large amount of data, analogous to extracting gold from numerous rocks and sand [17]. The extracted knowledge is defined as interesting patterns in the data [18]. Such a pattern will describe the behavior of knowledge from users or networks in an exceedingly computing surroundings. The ability to mechanically generate models that rely upon the traffic description is one in all the benefits of the info mining approach.

Moreover, this approach is applied in generalized IDSs and in any computing surroundings. The knowledge mining approach works utterly for a web data stream that's boundless, continuous and rapidly increasing in volume. A procedure consisting of a rule learning stage, a clustering stage, a classification stage, and a regression stage is applied in the design of an IDS based on this approach [19].

**b. Machine learning** is a technique that depends on two stages: the training or learning stage and the detection or testing stage [20]. The coaching stage depends on mathematical algorithms or functions that use traditional knowledge as a reference input to find out the characteristics of the computing surroundings. Then, in the detection stage, these characteristics are used for detection and classification [21].

Supervised learning is one form of machine learning technique during which the characteristics of the coaching dataset area unit utilized in the educational section to make a classification model, which is then used to classify new unseen instances. Unsupervised learning is a type of machine learning technique that depends on the features of the data without using clustered training data [22].

**c.** A **pattern classification method** in machine learning depends on pattern recognition, whereas a single classifier method depends on a single machine learning algorithm [23, 24].

**d.** The **statistical model approach** depends on statistical mathematical operations [25]. The statistics of historical user behavior area unit accustomed produce a traditional model, and any deviations from this model are then detected. These deviations are considered abnormal data. The applied mathematics model approach uses applied mathematics mathematical operations applied to a coaching dataset to find abnormal traffic from the determined traffic patterns [26].

**e.** The **rule model approach** depends on the creation of rules for the computing environment. These rules are extracted from data traffic patterns. A rule-model based mostly IDS detects ANy abnormal knowledge traffic that breaks these rules and considers any such anomaly as an attack. The rule creation method depends on the historical system behavior. Thus, the system must be monitored for a long time to avoid an excessively high false positive rate [27, 28].

**f.** The **payload model** approach depends on the packet traffic of a specific port or user for a given application. In signature-based IDS, the payload model is based on pattern matching to identify attack packets with specific characteristics [29]. By distinction, AN anomaly based mostly IDS that uses the payload model approach creates a model that depends on bytes or calculations from bytes that describe the conventional characteristics of the packet payload.

**g.** The **protocol model** approach depends on monitoring protocols in different layers of the computing environment. An IDS supported this approach detects anomalies related to a selected protocol or a protocol that's not gift within the traditional model. A specification-based approach, a parser-based approach or an approach based on application protocol keywords can be used to analyze the protocols in a computing environment [30].

**h.** The **signal processing model** approach depends on traffic analysis using signal processing methods. An IDS supported this approach creates traditional|a traditional|a standard} pattern by capturing the statistics of normal information traffic and also the information distribution over time, and any deviation from this pattern is considered to be an anomaly [31].

The advantages and disadvantages of various anomaly-based intrusion detection techniques are shown in Table 1. These techniques will be discussed in the following.

| Technique | Advantage | Disadvantage |
|---|---|---|
| Data Mining | 1.Models are created automatically<br>2.applicable in different environments<br>3. suitable for online datasets | 1. based on historical data<br>2.Depends on complex algorithms |
| Machine Learning | 1.High Detection Accuracy<br>2. Suitable for massive data volumes | 1.Requires training data<br>2.Long training time |
| Statistical Model | 1.Suitable for online datasets<br>2.Systems simplicity | 1.Based on historical behavior<br>2.Detection accuracy depends on statistical and mathematical operations |
| Rule Model | 1.Suitable for online datasets<br>2.Systems simplicity | 1. Based on set of rules<br>2.High false positive rates |
| Payload Model | 1.High detection accuracy with known attacks | 1.Privacy Issues |
| Protocol Model | 1.High detection accuracy for a specific type of attacks | 1. Designed for a Specific type of protocol |
| Signal Processing Model | 1.High detection accuracy<br>2.Low false positive rate | 1.Depends on complex pattern recognition methods |

**Specification-based intrusion detection**

The concept of specification-based IDS was proposed by Ko et al. in 1997[32]. They proposed a monitoring and detection system based on security specifications that determine the normal behavior of the system to be protected. These security specifications area unit created supported the functions and security policies for this technique. Thus, operating sequences that are not included in the system behavior are considered security violations [33].

The most important challenge in designing robust specification-based IDS is creating a formalism that captures the valid operating sequences of the system. Therefore, the cost of defining the specification "trace policy" and the difficulty of evaluating and verifying the specifications limit the real-world applicability of specification based IDSs. A specification-based IDS learns the basis characteristics of attacks and detects better-known attacks sort of a misuse-

based IDS, and it additionally has the flexibility of anomaly primarily based IDSs to observe unknown attacks, such as operating sequences that are not included in the normal behavior of the system[34-36].

**Hybrid Intrusion Detection method**

This methodology of intrusion detection in web of things was projected by Sedjelmaci et al. In based on the use of Game Theory. This methodology mixed the usage of signature and anomaly ways in which for IoT intrusion detection. It achieves this by creating the game model of intruder and normal user.

**An Automata Based Intrusion Detection Method**

This is a standardized intrusion detection methodology for the Brobdingnagian heterogeneous IoT networks supported associate degree automata model. This methodology will observe and report the attainable IoT attacks with 3 types: jam-attack, false-attack, and reply-attack automatically.

**Complex Event-Processing IDS**

It is a real-time pattern matching system for IoT devices was proposed by J. Chen and C. Chen. This method uses the Complex Event Processing (CEP) that focuses on the use of the features of the events flows to judge the intrusions, which can reduce the false alarm rate comparison with the normal intrusion detection strategies.

**Artificial Neural Network (ANN) Intrusion Detection System**

It is a multi-level perceptron, a type of supervised ANN, is trained using internet packet traces and was assessed on its ability to thwart Distributed Denial of Service (DDoS/DoS) attacks on IoT devices. The detection was supported classifying traditional and threat patterns. It was able to establish with success differing kinds of attacks and showed smart performances in terms of true and false positive rates.

## 3. CONCLUSION

In this paper, we tend to created a shot to supply a survey on the intrusion detection system for the net of things. With the event of IoT, there are so many issues raised. Among many other issues, security issues cannot be ignored. Here we have a tendency to mentioned some potential security attacks that area unit created on IoT applications and numerous intrusion detection approaches that area unit accessible to mitigate those attacks. Still those approaches can't be able to observe all sorts of Cyber-attacks and aren't possible for IoT network as a result of it needs additional process power, memory and bandwidth for intrusion detection. Thus, future analysis during this direction would be to develop light-weight security mechanism which can take fewer resources for intrusion detection.

## REFERENCES

1. 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.
2. 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.
3. P. Gokul Sai Sreeram, Chandra Mohan Reddy Sivappagari," Development of Industrial Intrusion Detection and Monitoring Using Internet of Things", International Journal of Technical Research and Applications, 2015
4. 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
5. 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.
6. Mori Y, Kuroda M, Makino N (2016) Nonlinear Principal Component Analysis and Its Applications, JSS Research Series in Statistics. Springer, Singapore
7. Jolliffe IT (2002) Principal Component Analysis, Springer Series in Statistics, vol. 2. Springer, New York
8. Elrawy MF, Awad AI, Hamed HFA (2016) Flow-based features for a robust intrusion detection system targeting mobile traffic. In: 2016 23rd International Conference on Telecommunications (ICT). IEEE, Thessaloniki. pp 1–6
9. Nwanze N, i. Kim S, Summerville DH (2009) Payload modeling for network intrusion detection systems. In: MILCOM 2009 - 2009 IEEE Military Communications Conference. IEEE, Boston. pp 1–7
10. Chabathula KJ, Jaidhar CD, Kumara MAA (2015) Comparative study of principal component analysis based intrusion detection approach using machine learning algorithms. In: 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN). IEEE, Chennai. pp 1–6
11. Bul'ajoul W, James A, Pannu M (2015) Improving network intrusion detection system performance through quality of service configuration and parallel technology. J Comput Syst Sci 81(6):981–999
12. Meng W, Li W, Kwok L-F (2014) Efm: Enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism. Comput Secur 43:189–204
13. Abduvaliyev A, Pathan ASK, Zhou J, Roman R, Wong WC (2013) On the vital areas of intrusion

detection systems in wireless sensor networks. IEEE Commun Surv Tutor 15(3):1223–1237.
14. Bhuyan MH, Bhattacharyya DK, Kalita JK (2014) Network anomaly detection: Methods, systems and tools. IEEE Commun Surv Tutor 16(1):303–336
15. Hong J, Liu C, Govindarasu M (2014) Integrated anomaly detection for cyber security of the substations. IEEE Trans Smart Grid 5(4):1643–1653
16. Mishra P, Pilli ES, Varadharajan V, Tupakula U (2017) Intrusion detection techniques in cloud environment: A survey. J Netw Comput Appl 77:18–47
17. Han J, Kamber M, Pei J (eds) (2012) Data mining: concepts and techniques. Morgan Kaufmann, Boston
18. Duque S, bin Omar MN (2015) Using data mining algorithms for developing a model for intrusion detection system (IDS). ProcediaComput Sci 61:46–51
19. Feng W, Zhang Q, Hu G, Huang JX (2014) Mining network data for intrusion detection through combining SVMs with ant colony networks. Futur Gener Comput Syst 37:127–140
20. Alseiari FAA, Aung Z (2015) Real-time anomaly-based distributed intrusion detection systems for advanced metering infrastructure utilizing stream data mining. In: 2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE). IEEE, Offenburg.
21. Tsai JJP, Yu PS (eds) (2009) Machine Learning in Cyber Trust: Security, Privacy, andReliability. First edn. Springer US, Springer-Verlag US. pp 1–362
22. Nishani L, Biba M (2016) Machine learning for intrusion detection in MANET: a state-of-the-art survey. J Intell Inf Syst 46(2):391–407
23. Namdev N, Agrawal S, Silkari S (2015) Recent advancement in machine learning based internet traffic classification. Procedia Comput Sci 60:784–791
24. Tsai C-F, Hsu Y-F, Lin C-Y, Lin W-Y (2009) Intrusion detection by machine learning: A review. Expert Syst Appl 36(10):11994–12000
25. Weller-Fahy DJ, Borghetti BJ, Sodemann AA (2015) A survey of distance and similarity measures used within network intrusion anomaly detection. IEEE Commun Surv Tutor 17(1):70–91
26. Amin SO, Siddiqui MS, Hong CS, Lee S (2009) RIDES: Robust intrusion detection system for ip-based ubiquitous sensor networks. Sensors 9(5):3447
27. Muzammil MJ, Qazi S, Ali T (2013) Comparative analysis of classification algorithms performance for statistical based intrusion detection system. In: 2013 3rd IEEE International Conference on Computer, Control and Communication (IC4), Karachi.
28. Mabu S, Chen C, Lu N, Shimada K, Hirasawa K (2011) An intrusion-detection model based on fuzzy class-association-rule mining using genetic network programming,
29. Xu C, Chen S, Su J, Yiu SM, Hui LCK (2016) A survey on regular expression matching for deep packet inspection: Applications, algorithms, and hardware platforms. IEEE Commun Surv Tutor 18(4):2991–3029
30. Davis JJ, Clark AJ (2011) Data preprocessing for anomaly based network intrusion detection: A review. Comput Secur 30(6–7):353–375
31. Vancea F, Vancea C (2015) Some results on intrusion and anomaly detection using signal processing and NEAR system. In: 2015 38th International Conference on Telecommunications and Signal Processing (TSP). IEEE, Prague. pp 113–116
32. Ko C, Ruschitzka M, Levitt K (1997) Execution monitoring of security critical programs in distributed systems: a specification-based approach. In: 1997 IEEE Symposium on Security and Privacy, Oakland. pp 175–187
33. Berthier R, Sanders WH (2011) Specification-based intrusion detection for advanced metering infrastructures. In: 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing. IEEE, Pasadena. pp 184–193
34. Surendar M, Umamakeswari A (2016) InDReS: An intrusion detection and response system for internet of things with 6LoWPAN. In: 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai. pp 1903–1908
35. Le A, Loo J, Chai KK, Aiash M (2016) A specification-based IDS for detecting attacks on RPL-based network topology. Information 7(2):1–19
36. Bostani H, Sheikhan M (2017) Hybrid of anomaly-based and specification-based IDS for internet of things using unsupervised OPF based on MapReduce approach. Comput Commun 98:52–71