Journal of Physics: Conference Series

A Literature Review: Intrusion Detection Systems in Internet of Things

To cite this article: Anamika Chauhan *et al* 2020 *J. Phys.: Conf. Ser.* **1518** 012040

PRIME
PACIFIC RIM MEETING
ON ELECTROCHEMICAL AND SOLID STATE SCIENCE
HONOLULU, HI
Oct 6–11, 2024
Abstract submission deadline extended:
April 19, 2024
Learn more and submit!
Joint Meeting of
The Electrochemical Society
•
The Electrochemical Society of Japan
•
Korea Electrochemical Society

A Literature Review: Intrusion Detection Systems in Internet of Things

Anamika Chauhan[a], Rajyavardhan Singh[b] and Pratyush Jain[c]

Department of Information Technology, Delhi Technological University, Delhi, India

E-mail: [a]anamika@dce.ac.in; [b]rajyavardhan_bt2k16@dtu.ac.in; [c]pratyushjain98@gmail.com

Abstract. Internet of Things (IoT) is a new and surging technological advancement where in which the Internet is connected to various day-to-day physical objects belonging to various domains and making them "smart" like that of various machine dependent processes, manufacturing processes and healthcare. It is a system of interrelated computing devices, machines and people. Internet-connected IoT devices brings several benefits in our daily life but are susceptible to security issues. These vulnerabilities to IoT systems create security threats for any smart environment formed around the aforementioned concept. Thus, there is a need for intrusion detection systems (IDSs) which are designed specifically for IoT systems in order to combat these security related threats and create a secure network for the smart environment. IoT devices tend to have limited computing and storage capabilities. Hence, conventional IDSs might not be suitable for such networks. Due to the specifications and protocols of IoT devices, intrusion detection in IoT systems proves to be a challenging task. Thus, the field of intrusion detection systems in IoT systems is one that requires research and considerable effort to address the key security issues and security threats. A literature review is presented on the IDS in IoT topic, with emphasis on the present-day research, challenges and future directions.

1. Introduction

The Internet of Things (IoT) is a smart network that enables all things to setup a connection to the internet and allows them to exchange information using pre-defined protocols [1]. Giving the user a remote access to anything, at any time [2]. The basis of IoT is the use of smart sensors which connect physical objects with each other through a common platform. These smart sensors objectivity is to function without any or very less physical interaction with humans [3]. Physical objects and smart devices interact and corporate with each other using addressing schemes. The word "Smart" when added as a suffix to various physical objects indicates the usage of IoT. Some of the examples are smart environment, smart watches, smart house, smart TV and smart water [4]. IoT is taking the world by storm, it is predicted that by 2020 the number of smart devices would be six-times greater than the population. IoT[5] hold is the spear-head to all technological innovation and is deliberated as the fast growth. Along with the development and innovation IoT devices are getting prone to security vulnerability which is crucial in IoT devices. As these smart devices can be conveniently be used from any place, any network and at any distance, these "smart" devices are vulnerable to various malicious attacks. Because of the objects are accessible at any location via internet, then these objects and network remains unprotected against various intrusions. Hence maintaining security in the network of IoT is the most significant task to the researchers. Here there are some of important security aspects are:

1) **Privacy of data:** The data which is transmitted among the receiving node and sending node is

hacked by the intruders, as it is modifiable [6], confidentiality will be affected. Therefore, it is important to secure the data in IoT.

2) **Integrity:** In the process of transmission, information or data while transmitting should not be altered. There accuracy should be maintained in the message in the entire transmission process. The work [6] presents that in the IoT environment, integrity need to be ensured.

3) **Availability:** The work [6] presents that resources availability remains crucial for sensitive-time and the prospect information transmission. The bandwidth is loaded intentionally by the intruders to confine the resources availability through diverse means comprising black-hole intrusion, flooding, DoS intrusion etc.

4) **Authenticity:** The work [7] presents that both devices and data need to be accessible to the legitimate users only. End users should be able to detect the identity of others during the process of interaction. The work [8] presents that the procedure of verification should be free from error to make sure that the users who are illegitimate cannot access the devices or information.

5) **Non-repudiation:** The work [9] presents that this safeguards that the receivers or transmitters will not negate the receiving or transmitting the data respectively.

6) **Information Recentness:** According to the requirement, the information or data should be novel. The work [10] presents that IoT should safeguard that the information which is lagged by times should not be re-delivered by an intruder.

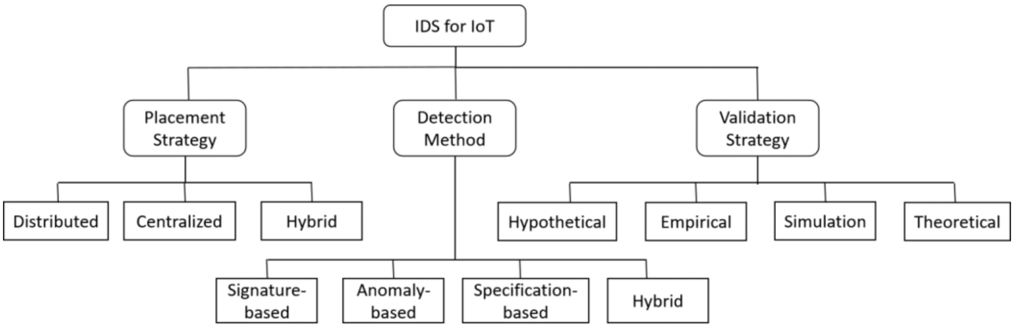

Figure 1. Classification of IDs

With the on-set usage of IoT devices or "smart" devices, Intrusion detection system is the pivotal tool to safe-guard from the various intruders. The present day scenarios of the IDS used in the IoT systems in not capable enough to tackle the diverse IoT environments. The development of IDS for IoT is complex and highly demanding as a result a comprehensive analysis in this particular field is required. Large quantity of resources are required by IDS which limits their usage on IoT devices. As a result, lightweight solutions that offer high degree of protection are required in IDS. The presented literature review is primarily based on [11], which is widely used and in the domain of computer science, and includes extensive information for the relevant analysis and presentation of the above-mentioned research works. The rest of the paper is divided into three sections. Section II defines important keywords related to intrusion detection system in IoT. Section III is the literature review where a taxonomy for attacks in IoT systems is analyzed. Lastly, section IV consists of the conclusions from the research work.

2. Taxonomy of intrusion detection in internet of things

In the following section a review is conducted on the currently proposed IDS for IoT. The works have been classified on the basis of the following categories: placement, detection, and validation methodology. Figure 1 depicts classification for Intrusion Detection in IoT.

2.1 Intrusion Detection Placement Strategies

- **Distributed IDS Placement Strategy**: When an IDS is placed on every physical object, then in that case the placement methodology is called as distributed IDS placement. For detecting attacks on the

IDS system, Oh et al. [12] suggested an alternative using a distributed lightweight IDS. The technique that were proposed were broadly classified into two namely, auxiliary shifting and early decision techniques. The objectivity was to reduces the number of matches required for detecting an attack. This methods result were compared with the results with WuManber algorithm. With the similar model of using a lightweight IDS, Lee et. al.[13] suggested to monitor the energy consumption by each node for detecting intrusions. This method controlled the inbound and outbound traffic by managing the node energy. The goal of the model was to minimize the resources required to detect intrusion. A broadcast message was send to all nodes if the IDS is under attack.

- **Centralized Ids Placement Strategy:** In the case of centralised IDS placement, as the name suggest the IDS is placed in the centralized component of the IDS. To analyse the packets passing the physical and the network domain of the border router Cho et al. [14] suggested a solution. The work was only concerning the packets in the border router. Keeping the same ideology in mind the Kasinathan et al. [15] deployed the analysis engine along with the IDS report generation system in a robust dedicated host. To monitor the traffic in the network infrastructure, powerful sensors were deployed in the Low power and Lossy Network or the LLN which would send the data for analysis to the IDS engine. The host and the IDS sensor are physically wired due to which it prohibits the transmission of IDS data in the same wireless network.
- **Hybrid Ids Placement:** A combination of centralized and distributed placement techniques is utilized in hybrid IDS placement, which allows us to get the best out of both. In hybrid placement demarcated sections of network are formed, and then an IDS instance is hosted on the prominent nodes of each section. Further, all the nodes in each section are checked via the prominent node. The design of hybrid placement IDS may allow it to utilize a higher range of resources as compared to distributed IDSs. Amaral et al. [16] proposed an IDS for IoT making use of this concept. Here, IDS is hosted only by some particular nodes. The chosen nodes target neighbouring nodes for potential intrusions. The designated node validates every other node following predefined protocols. All these designated nodes have different protocols owing to variable nature of network components. This concept has its benefits depending on the flexibility with which separate protocols are developed for each network section.

2.2 Detection Method

- **Signature Based IDS:** This technique uses a set of previously known attack patterns and signatures as references to check the profile of existing network. Thus it follows a system of rules to determine whether an intrusion has occurred. A database stores the aforementioned attack signatures or patterns so that any attack can be detected on this basis. This approach is easy to use. Since this technique relies on pattern matching, accurate information about each attack is required to be saved. This is an expensive approach as the required storage space rises with the increase in the number of attacks to be detected. New attacks are not detected by this strategy unless their signatures are manually entered into the database. This creates a demand for regular updates to the database[17]. Thus, it is a static approach. Thus the drawbacks of signature based IDS are: a) The specific pattern knowledge to detect attacks is needed. b) New or previously unknown attacks cannot be detected.[18]
- **Anomaly Based IDS:** This approach analyzes events to detect an intrusion and hence is known as event based detection. After a monitoring period, regular or normal behaviour of the network is defined. If any event occurs which isn't in accordance with the regular behaviour, it termed as an intrusion[19]. This is a more effective approach than signature based IDS. Nobakht et al. [20] proposed a host based IDS using Software Defined Technology (SDN). The work enlists three fundamental necessities for an Intrusion detection system in IoT, namely unobtrusive approach, negligible overheads, and scalability. In [21], Chordia and Gupta have discussed an anomaly based IDS. This IDS is based on data mining technique and its purpose is to minimize false positives as well as to provide an increase in efficiency of detection. K- NN, K-Means and Decision Table Majority Rule Based scheme are the techniques that the previously mentioned IDS employs in order to monitor network traffic.
- **Specification-based IDS:** Ko et al.[22] were the first to introduce a specification based IDS in 1997. Just like the anomaly based approach, their proposed system also works by detecting events that

are analogous to the regular behaviour which has been predetermined. This behaviour specification is obtained by considering the security features and policies of the system. Operations which do not align with these specifications are labelled as security violations[23]. However, the practical applicability of this technique is limited. This is due to challenges in evaluating the specifications. Specification based approach combines the techniques of misuse based IDS and anomaly based IDS to protect against regarded assault as well as to provide security against new or unknown threats[24-26].

- **Hybrid approaches:** As the name suggests, Hybrid approach uses a combination of previously discussed techniques to provide a highly effects detection system. Hybrid systems aim to maximize the advantageous properties of the approaches while limiting the drawbacks. Raza et al.[27] proposed a hybrid model in their work called SVELTE. Krimmling and Peter[28] have also discussed and evaluated IDSs on the basis of a framework introduced by them. The results show that no technique is completely fool proof, as each failed for some attack or the other. Thus, their solution involves taking an aggregation of all these techniques to provide protection against a larger set of attacks. Cervantes et al.[29] proposed INTI IDS to tackle sinkhole attacks. Instead of signature based method as in SVELTE, INTI uses a combination of specification based method and anomaly based method

2.3 Validation Strategy

If the model so designed or implemented conducts according to the objectivity of the study with decent accuracy, it is what validation implies by D.Chrun[30]. Though there are various validation methodology they can be distinguished broadly on the basis of source of information: experts and data. In the case of expert source of information gives subjective and qualitative model accreditation, on the other hand the data source of information the objectivity and quantitative validation is given. The objectivity is to study the validation strategy which are applied on intrusion detection. Verendel [31] classified validation methods on the basis of:

Hypothetical:- Hypothetical as the name suggests is when the observations are not real and based on a model.

Empirical:- Data is gathered from various operational settings to conduct systematic tests

Simulation:- Some IoT models are validated using simulated implementation.

Theoretical:- Theoretical arguments that are precise and capable of supporting the results.

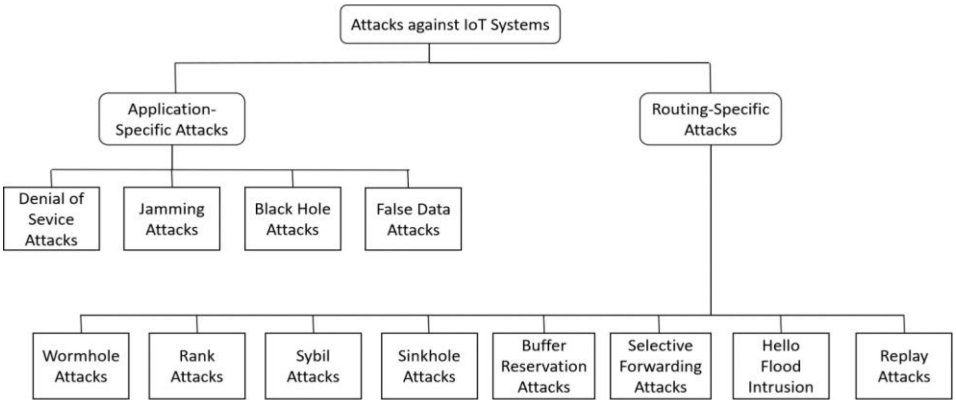

Figure 2. Classification of Attacks against IoT

3. Taxonomy of attack for IoT system

Even though IoTs model is a relatively new paradigm, the genesis of the software base for IoT software comes from the existing software paradigms. As seen the existing infrastructure such as IPv6 and IPv5 still hold the building blocks for IoT specific stacks (such as Routing Protocol for Low-Power and Lossy Networks or RPL, Zigbee, 6LoWPAN). IoT network are prone to various attacks from intruders both internal and external. In the following section, we discuss some cyber-attacks on IoT applications. **Figure 2** illustrates the proposed attacks against IoT systems.

- **Wormhole attack:** It is a type of attack in which the target node is breached from two opposite directions, here the positioning of attackers is crucial. The compromised nodes mutually declare they are adjacent to the base station. On top of that a wormhole attack may be used to mimic a neighbourhood environment between two distinctly located nodes [32], [33].
- **Rank attack**: Ranking is a concept in Routing Protocol for Low power and lossy networks (RPL). These node ranks are updated and the updated values travel to all the nodes in the network. The rank rule is used by the RPL to avoid loop creation, create the best topology and to manage overhead. This type of attack messes with the rank data as discussed in [34]-[36]. The attacker alters the rank data so that the node with the worst rank value is chosen, which disrupts the topology of the network and creates hindrance in transmission.
- **Sybil Attack**: In this type of attack the node has multiple identities in which the infected node would attacks various routing protocol, detection algorithm and co-operation methods by spoofing. Sybil attack are broadly classified on the basis of attackers ability. The classification is further on the basis of graph-based detection called the Social graph based sybil attack or SGSD along with behaviour classification-based Sybil detection or BCSD for complete analysis. The author ends with the challenges and future scope for protection in IoT devices in terms of security.
- **Sinkhole attack:** In a sinkhole attack, the purpose of the compromised node is to attract the data from all other neighbouring nodes[38]. In this attack, the malicious node routes all the network data through itself, by showing its routing cost to be minimum to all other nodes. This type of attack is created by introducing a false node inside the network. R.Stephen et al.[39] proposed an Intrusion Detection System (IDS) to detect the sinkhole attack in the network which uses the RPL as a routing protocol. Number of packets received and transmitted is the metric which is used by the proposed algorithm in order to validate the Intrusion Ration (IR) by the IDS agent. If a malicious node is detected, the IDS sends alert messages to the leaf nodes to isolate the false node in the following transmission. The proposed work aims to minimize the Intrusion Ratio.
- **Buffer reservation attack:** A buffer reservation attack might be caused as an aftermath of a successful fragment duplication attack. As discussed in [40], this attacks takes advantage of the fact that the receiver is unaware if all the fragments have been received correctly or not in the case of a fragmented packet transmission. Hence a buffer space is reserved by the recipient node according to the 6LoWPAN header.
- **Denial Of Service (Dos) Attack**: As the name suggests, a malicious node denies resources to nearby nodes causing a lack of resources and thereby an inability to conduct service as normal. A DDoS attack is same as a DoS attack, but with multiple malicious nodes. In this type of attack, resources are made unavailable to legitimate users causing a degradation in service. A DDoS/DoS attack is capable of causing serious disorder and negatively affect usability of a network by sending data in particular samples, or just by flooding the network with a large volume of requests or packets. It is often possible for attackers to hinder the remote service [41]. Tasnuva Mahjabin et. Al [42] discuss a comprehensive survey of distributed denial-of-service attacks, their prevention and techniques to mitigate the threat. Their work provides an analytical study of these attacks, with emphasis on evolution, attack analysis, prevention measures and mitigation techniques.
- **Selective forwarding attack:** In this type of attack, a malicious node masquerades as a legitimate node. The purpose of this attack is to disturb standard transmission and routing[43]. The infected node forwards incoming messages on a selective basis, sinking certain data messages. The corrupt node blocks the transmission of certain packets, thereby disrupting the routing operations. As an example, an attacker can choose to forward all control messages, but block the remaining[44]. This attack paired with sinkhole attack can cause serious damage to a network. Such interrelated dependencies between attacks and their impacts act as motivation towards research in multi-stage IoT attacks, forming an importance research area with massive scope.
- **Hello Flood Intrusion:** The routing protocol transmits the hello message to indicate its presence to nearby nodes. The nearby node which receives this hello message considers that the source

- node is in proximity and therefore, includes the corrupt node to its nearby nodes list [45].
- **Replay attack:** In this attack, intrusion occurs from one time to another in which the data is collected. This collected data is then replayed [46].
- **Jamming attack:** The wireless medium is monitored by the attacker in these types of attacks. This is done to control the frequency of the receiving signal from sender by destination node[47]. Then, the attacker transmits a signal on this frequency in order to hinder the fault free receptor[47].
- **Black hole attack:** The request packets are observed by the attacker in case of a blackhole attack. This is done by observing the dynamic properties of the routing protocol so that the reply can be sent by using a fake reply packet[48].
- **False data attack:** The first step for the attacker in this type of attack is to define the current network structure and organization. Next, tampered measurements are inserted which affect the estimations, compromising the system[49].

Table 1- Overview of IDSs for various IoT devices

Reference	**Placement Strategy**	**Detection Type**	**Attacks**
Amaral et al.[16]	Hybrid	Specification	**-**
Cervantes et al.[29]	Distributed	Hybrid	Sinkhole
Chordia et al.[21]	Centralized	Anomaly	DoS
Fu et al.[50]	Distributed	Specification	Buffer Overflow
Indre et al.[51]	Centralized	Hybrid	DoS
Kasinathan et al.[15]	Distributed	Signature	DoS
Khan et al.[52]	Distributed	Anomaly	Sinkhole
Krimmling and Peter[28]	-	Hybrid	Routing
Le et al.[25]	Hybrid	Specification	Rank
Lee et al.[13]	Distributed	Anomaly	DoS
Oh et al.[12]	Distributed	Signature	-
Pongle and Chavan[53]	Hybrid	Anomaly	Wormhole
Raza et al.[27]	Hybrid	Hybrid	Sinkhole
Sedjelmaci et al.[54]	Distributed	Hybrid	DoS
Summerville et al.[55]	Distributed	Anomaly	Wormhole
Zhang et al. [56]	Distributed	Anomaly	DoS

4. Conclusion

With the surge increase in the IoT application and the security vulnerability it possess, there is an need for a strong, robust and light-weighted solution for the various IoT models. In this literature review various paper were studied which dealt with the implementation of IDSs in the range IoT and “smart” environment. The various IDS so studied have been summarized in accordance to most common grains. In the present literature review we analysed and explored the topic of Intrusion detection systems and its application in IoT paradigm. As shown in Table 1, 16 papers were selected which suggested IDS application for a particular IoT model. These papers were broadly divided into following grains: Detection methodology, Placement methodology and Validation methodology. IoT being an ever growing and developing stream with various heterogeneous use cases, IDS scheme are ever evolving. This work is used for the researchers these who are working in IDS to get a clear idea about IDS and IoT.

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] Evans, Dave. "The internet of things: How the next evolution of the internet is changing everything." CISCO white paper 1.2011 (2011): 1-11.

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

[7] L. Clemmer, Information Security Concepts: Authenticity. [Online] Available: http://www.brighthub.com/computing/smb- security/articles/31234.aspx

[8] Kumar, ShyamNandan. "Review on Network Security and Cryptography." International Transaction of Electrical and Computer Engineers System 3.1 (2015): 1-11.

[9] Chezhian, Umadevi, and Zaheer Uddin Khan. "Security Requirements In Mobile Ad Hoc Networks." International Journal of Advanced Research in Computer and Communication Engineering 1.2 (2012).

[10] Hossain, Md Mahmud, MaziarFotouhi, and RagibHasan. "Towards an analysis of security issues, challenges, and open problems in the internet of things." Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015.

[11] S. Keele, “Guidelines for performing systematic literature reviews in software engineering,” in Technical Report, Ver. 2.3 EBSE Technical Report. EBSE, ed, 2007.

[12] D. Oh, D. Kim, W. W. Ro, A malicious pattern detection engine for embedded security systems in the Internet of Things, Sensors 14 (12) (2014) 24188–24211.

[13] T.-H. Lee, C.-H. Wen, L.-H. Chang, H.-S. Chiang, M.-C. Hsieh, A lightweight intrusion detection scheme based on energy consumption analysis in 6LowPAN, in: Y.-M. Huang, H.-C. Chao, D.-J. Deng, J. J. J. H. Park (Eds.), Advanced Technologies, Embedded and Multimedia for Human-centric Computing, Vol. 260 of Lecture Notes in Electrical Engineering, Springer Netherlands, 2014, pp. 1205–1213.

[14] E. Cho, J. Kim, C. Hong, Attack model and detection scheme for botnet on 6LoWPAN, in: C. Hong, T. Tonouchi, Y. Ma, C.-S. Chao (Eds.), Management Enabling the Future Internet for Changing Business and New Computing Services, Vol. 5787 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2009, pp. 515–518.

[15] P. Kasinathan, C. Pastrone, M. Spirito, M. Vinkovits, Denial-of-service detection in 6LoWPAN based Internet of Things, in: Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on, 2013, pp. 600–607.

[16] J. Amaral, L. Oliveira, J. Rodrigues, G. Han, L. Shu, Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks, in: Communications (ICC), 2014 IEEE International Conference on, 2014, pp. 1796–1801

[17] Neha Maharaj, Pooja Khanna, “A Comparative Analysis of Different Classification Techniques for Intrusion Detection System”, International Journal of Computer Applications, 2014.

[18] 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

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

[20] M. Nobakht, V. Sivaraman, and R. Boreli, “A host-based intrusion detection and mitigation

framework for smart home iot using openflow," in 11th International Conference on Availability, Reliability and Security (ARES), 2016.

[21] A. S. Chordia and S. Gupta, "An effective model for anomaly ids to improve the efficiency," in International Conference on Green Computing and Internet of Things (ICGCIoT), 2015.

[22] Ko C, Ruschitzka M, Levitt K (1997) Execution monitoring of securitycritical programs in distributed systems: a specification-based approach. In: 1997 IEEE Symposium on Security and Privacy, Oakland. pp 175–187

[23] 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

[24] 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

[25] 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

[26] 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

[27] Raza, S., Wallgren, L., Voigt, T., 2013. SVELTE: real-time intrusion detection in the Internet of Things. Ad Hoc Netw. 11 (8), 2661–2674.

[28] Krimmling, J., Peter, S., 2014. Integration and evaluation of intrusion detection for CoAP in smart city applications. In: Communications and Network Security (CNS), 2014 IEEE Conference on, pp. 73–78

[29] Cervantes, C., Poplade, D., Nogueira, M., Santos, A., 2015. Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. In: 2015 IFIP/ IEEE International Symposium on Integrated Network Management (IM), pp. 606– 611.x

[30] D. Chrun, Model-Based Support for Information Technology Security Decision Making, Ph.D. thesis,University of Maryland (2011).

[31] V. Verendel, Quantified security is a weak hypothesis. In: Proceedings of the 2009 workshop on New security paradigms workshop - NSPW '09, pp. 37–49.

[32] 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.

[33] Abdur Rahaman Sardar, Rashmi Ranjan Sahoo, Moutushi Singh, Souvik Sarkar, Jamuna Kan ta 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

[34] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, "The impact of rank attack on network topology of routing protocol for low-power and lossy networks," IEEE Sensors Journal, vol. 13, pp. 3685–3692, 2013.

[35] W. Xie, M. Goyal, H. Hosseini, J. Martocci, Y. Bashir, E. Baccelli, and A. Durresi, "Routing loops in dag-based low power and lossy networks," in Proceedings of 2010 24th IEEE International Conference on Advanced Information Networking and Applications, 2010, pp. 888– 895.

[36] A. Dvir, T. Holczer, and L. Butty?n, "Vera-version number and rank authentication in rpl," pp. 709–714, 2011.

[37] Kuan zhang et.al, sybil attacks and their defenses In the internet of things, Ieee internet of things journal, vol. 1, no. 5, october 2014

[38] P. Goyal, S. Batra, A. Singh, A literature review of security attack in mobile ad-hoc networks, Int. J. Comput. Appl. 9 (12) (2010) 11–15.

[39] R. Stephen and Dr. L. Arockiam, "Intrusion Detection System to Detect Sinkhole Attack on RPL Protocol in Internet of Things" International Journal of Electrical Electronics & Computer Science Engineering Volume 4, Issue 4(August, 2017) | E-ISSN : 2348-2273

[40] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, "6lowpan fragmentation attacks and mitigation mechanisms," in Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, ser. WiSec '13, 2013.

[41] Tasnuva Mahjabin1, Yang Xiao1, Guang Sun2 and Wangdong Jiang, A survey of distributed denial-of-service attack, prevention, and mitigation techniques, International Journal of Distributed Sensor Networks, 2017, Vol.13(12).

[42] J. Lin. An analysis on DoS attack and defense technology. In: 7th Inter- national Conference on Computer Science & Education (ICCSE). IEEE, 2012. DOI: 10.1109/ICCSE.2012.6295258.

[43] L. Wallgren, "Routing attacks and countermeasures in the roll based internet of things," IJDSN, vol. 9, 2013.

[44] Can, Okan, and OzgurKoraySahingoz. "A survey of intrusion detection systems in wireless sensor networks." Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on. IEEE, 2015.

[45] Sardar, AbdurRahaman, et al. "Intelligent intrusion detection system in wireless sensor network." Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014. Springer, Cham, 2015.

[46] A. Teixeira , D. Pérez , H. Sandberg , K.H. Johansson , Attack models and scenar- ios for networked control systems, in: Proceedings of the 1st international conference on High Confidence Networked Systems, ACM, 2012, pp. 55–64 .

[47] P. Goyal , S. Batra , A. Singh , A literature review of security attack in mobile ad-hoc networks, Int. J. Comput. Appl. 9 (12) (2010) 11–15.

[48] A. Mathur , T. Newe , M. Rao , Defence against black hole and selective forward- ing attacks for medical WSNs in the IoT, Sensors 16 (1) (2016) 118

[49] Y. Liu , P. Ning , M.K. Reiter , False data injection attacks against state estimation in electric power grids, ACM Trans. Inf. Syst. Secur. (TISSEC) 14 (1) (2011) 13 .

[50] R. Fu, K. Zheng, D. Zhang, and Y. Yang, "An intrusion detection scheme based on anomaly mining in internet of things," in Proceedings of the 4th IET International Conference on Wireless, Mobile & Multimedia Networks (ICWMMN '11), pp. 315–320, IET, Beijing, China, November 2011

[51] I. Indre and C. Lemnaru, "Detection and prevention system against cyber attacks and botnet malware for information systems and internet of things," in IEEE 12th International Conference on Intelligent Computer Communication and Processing (ICCP), 2016

[52] Z. Khan and P. Herrmann, "Hive: Home automation system for intrusion detection," in IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)., 2017

[53] Pongle, P., Chavan, G., 2015. Real time intrusion and wormhole attack detection in Internet of Things. Int. J. Comput. Appl. 121 (9), 1–9

[54] H. Sedjelmaci and M. Feham, "Novel hybrid intrusion detection system for clustered wireless sensor network," International Journal of Network Security & Its Applications, vol. 3, no. 4, 2011

[55] D. H. Summerville, K. M. Zach, and Y. Chen, "Ultra-lightweight deep packet anomaly detection for internet of things devices," in Proceedings of the 34th IEEE International Performance Computing and Communications Conference (IPCCC '15), pp. 1– 8, IEEE Computer, Nanjing, China, December 2015

[56] Yan, Z., Zhang, P., Vasilakos, A.V., 2014. A survey on trust management for Internet of Things. J. Netw. Comput. Appl. 42 (0), 120–134.