Intrusion Detection Systems in Internet of Things

A literature review

Leonel Santos, Carlos Rabadão
School of Technology and Management,
Computer Science and Communication Research Centre,
Polytechnic Institute of Leiria, Portugal
leonel.santos@ipleiria.pt, carlos.rabadao@ipleiria.pt

Ramiro Gonçalves
Universidade de Trás-os-Montes e Alto Douro, Vila Real,
Portugal
INESC TEC (Formerly INESC Porto), Porto, Portugal
ramiro@utad.pt

Abstract — **The Internet of Things (IoT) is a new model that integrates physical objects and Internet and became one of the principal technological evolutions of computing. It is estimated that a trillion of physical objects will be connected to the Internet until 2022. The low accessibility and the lack of interoperability of many of these devices in a vast heterogenous landscape will make it very hard to design specific security measures and apply specific security mechanism. Moreover, IoT networks still exposed and vulnerable to attacks aimed to disrupt the network. Therefore, additional security tools specific to IoT are needed. Intrusion Detection System (IDS) could fulfill this purpose.**

In this paper, we present a literature review on the IDS in IoT topic, mainly focusing on the current state of research by examining the literature, identifying current trends and presenting open issues and future directions.

Keywords – Internet of Things; IoT; Intrusion Detection System; IDS; Cybersecurity.

I. INTRODUCTION

Internet of Things (IoT) is a new paradigm that enables many novel applications in different domains such as home automation, industrial process, human health and environmental monitoring. Despite IoT enables many novels applications, it also increases the risk of cyber security attacks.

Because IoT landscape is heterogenous, fragmented and not supportive of interoperability it is very hard to design specific security mechanism. Some solutions for enhancing IoT security have been developed and include methods for providing data confidentiality and authentication, access control within the IoT network, and trust and privacy among users and things. However, even with those mechanisms, IoT networks still vulnerable to attacks. Then, the development of more security tools specific to IoT are required and systems like Intrusion Detection System (IDS) could be used to address that necessity.

Despite the maturity of IDS technology for traditional networks, current solutions are inadequate for IoT because they will not be flexible enough against the complex and heterogenous IoT ecosystem. Characteristics such as constrained-resources devices, network architecture, specific protocol stacks and standards, explain the need for development of IDS for IoT.

Considering that the development of IDS for IoT systems is a new important challenge for the researches in this particularly field, the research team decided to undergo an extensive analysis on the existing literature related to the development of IDS solutions for IoT systems, aiming on achieving answers to the question: Are there any relevant works focusing their attention on the central topic of our research? If so, in what manner are those works being performed and what where their results?

The literature review process started with the “Intrusion Detection Systems in Internet of Things” topic being defined as the review topic and was then followed by a literature review. The literature review aimed works produced between 2009 and 2017 and was supported by scientific publications available in scientific repository’s (IEEE Xplore Digital Library, SCOPUS, ACM Digital Library, Web of Science, ScienceDirect, Springer Link, Google Scholar e B-on). The presented literature review was based in on [1] has a guide for the analysis and presentation of the identified and considered scientific works, because it is the most accepted and adopted in Computer Science field.

The rest of this paper is organized as follows. Section II introduces some relevant terms regarding IDS and IoT. Section III is the literature review section where the various works that focus their attention on the IDS in IoT topic are analyzed. Finally, in section IV, we present a brief set of conclusions complemented with a discussion of open issues and future work considerations.

II. RELEVANT TERMS

This section introduces the central concepts of this paper: Intrusion Detection Systems and Internet of Things.

A. Internet of Things

The IoT has wan attention recently because of the expansion of appliances connected to the Internet [2][3]. IoT simply means the interconnection of vast heterogeneous network frameworks and systems in different patterns of communication, such as human-to-human, human-to-thing, or thing-to-thing [4][5]. Moreover, the IoT is a realm where physical items are consistently integrated to form an information network with the specific end goal of providing advanced and smart services to users [6][7]. The connected “things” (for example, sensors or mobile devices) monitor and collect all types of environment data. They enable the collection of real-time data about properties, individuals, plants, and animals.

Typically, the architecture of IoT is divided into three basic layers [8]: 1) application layer; 2) network layer; and 3) perception layer, which are further described below:

This work was supported by Portuguese national funds through the FCT - Foundation for Science and Technology, I.P., under the project UID / CEC / 04524/2016

- Perception layer: also known as the sensor layer, is implemented as the bottom layer in IoT architecture [9]. Its main objectives are to connect things into IoT network, and to measure, collect, and process the state information associated with these things via deployed smart devices, transmitting the processed information into upper layer via layer interfaces.
- Network layer: It is also known as the transmission layer, is implemented as the middle layer in IoT architecture [10]. The network layer is used to receive the processed information provided by perception layer and determine the routes to transmit the data and information to the IoT hub, devices, and applications via integrated networks. The network layer is the most important layer in IoT architecture, because various devices (hub, switching, gateway, cloud computing perform, etc.), and various communication technologies (Bluetooth, Wi-Fi, long-term evolution, etc.) are integrated in this layer.
- Application layer: It is also known as the business layer, is implemented as the top layer in IoT architecture [5]. The application layer receives the data transmitted from network layer and uses the data to provide required services or operations. A number of applications exist in this layer, each having different requirements.

[11] propose three useful topologies: point to point, star and mesh. The latter is decentralized, and preferable for IoT systems but the nodes have a higher consume of resources to maintain routing protocols to forward packets in addition to the main sensor tasks. The star topology doesn't need so much resources in the standard nodes but has a weakness in providing a single point of failure in IoT system due to the use of a unique gateway.

Different alliances, consortiums, special interest groups, and standard development organizations have proposed a considerable amount of communication technologies for IoT, what may carry a big challenge for end-to-end security in IoT applications [12].

Most popular technologies for IoT include infrastructure protocols like IEEE 802.15.4, Bluetooth Low Energy (BLE), WirelessHART, Z-Wave, LoRaWAN, 6LoWPAN, DTLS and RPL, and application protocols like CoAP and MQTT (Message Queue Telemetry Transport).

In cyber security, the Confidentiality – Integrity – Availability (CIA) triad is well known. Just a few of the surveyed papers however relate CIA back to IoT. Besides CIA, [13] adds more features to be addressed like Identification and Authentication, Privacy and Trust. The Open Web Application Security Project (OWASP) also have a useful list of IoT Attack Surface Areas which they state should be understood by manufactures, developers, researchers and companies looking to deploy IoT in their organizations [14]. [13] and [15] outline some security challenges in each layer of IoT architecture presenting common vulnerabilities and attacks.

Perception layer: As the main purpose of the perception layer in IoT it to collect data, the security challenges in this layer focus on forging collected data and destroying perception devices by the following attacks: node capture; malicious code injection; false data injection; replay or freshness; cryptoanalysis and side channel; eavesdropping and interference; and sleep deprivation.

Network layer: As the main purpose of the network layer in IoT is to transmit collected data, the security challenges focus in the impact of the availability of network resources through the next attacks: denial of service (DoS); spoofing; sinkhole; wormhole; man-in-the-middle (MITM); routing information; sybil; and unauthorized access.

Application layer: As the main purpose of application layer is to support services requested by users, challenges in this layer focus on software attacks like phishing attack and malicious virus/worm and malicious scripts.

B. *Intrusion Detection System*

The concept of intrusion detection was first proposed by Anderson in the year of 1980 [16] and is introduced to network system by Heberlein in 1990 [17]. An IDS is a tool or mechanism used to prevent unauthorized access and to detect attacks against a system or a network by analyzing the activity I the network or in the system itself.

A typical IDS is composed of sensors, an analysis engine, and a reporting system. Sensors are positioned at different network places or hosts and their main task is to collect data. The data collected are sent to the analysis engine, which is responsible to examine the collected data and detect intrusions. If an intrusion is detected by analysis engine, the reporting system generates an alert to network administrator.

IDSs can be classified as Host-based IDS (HIDS) and Network-based IDS (NIDS). HIDS is attached to a device/host and monitors malicious activities occurring within the system. NIDS connects to one or more network segments and monitors network traffic for malicious activities. Unlike NIDS, the HIDS analyzes not only network traffic but also system calls, running processes, file-system changes, interprocess communication, and application logs.

IDS approaches may also be classified as signature-based, anomaly-based or specification based.

In signature-based approaches, IDSs detect attacks when system or network behavior matches an attack signature stored in the IDS internal databases. If any system or network activity matches with stored patterns/signatures, then an alert will be triggered. This approach is accurate and very effective at detecting known threats, and their mechanism is easy to understand. However, this approach is ineffective to detect new attacks and variants of known attacks, because a matching signature for these attacks is still unknown [18][19].

Anomaly-based IDSs compare the activities of a system at an instant against a normal behavior profile and generates the alert whenever a deviation from normal behavior exceeds a threshold. This approach is efficient to detect new attacks, however, anything that does not match to a normal behavior is considered an intrusion and learning the entire scope of the normal behavior is not a simple task. Thereby, this method usually has high false positive rates [20][21]. To construct the normal behavior profile, researchers usually employ statistical techniques or machine learning algorithms.

Specification is a set of rules and thresholds that define the expected behavior for network components such as nodes, protocols, and routing tables. Specification-based approaches detect intrusions when network behavior deviates from specification definitions. Therefore, specification-based detection has the same purpose of anomaly-based detection: identifying deviations from normal behavior. However, there is one important difference between these methods: in specification-based approaches, a human expert should manually define the rules of each specification [20][39][22]. Manually defined specifications usually provide lower false positive rates in comparison with the anomaly-based detection [20][39][22]. Besides, Specification-based detection systems do not need a training phase, since they can start working immediately after specification setup [39]. However, manually defined specifications may not adapt to different environments and could be time-consuming and error-prone [20][39][22].

III. INTRUSION DETECTION SYSTEM IN INTERNET OF THINGS

Over the recent years, several review articles have been published on IDSs for technologies related to IoT such as mobile ad hoc networks (MANETs) ([23]; [24]; [25]), wireless sensor networks (WSNs) ([26];[27];[22]), cloud computing ([28]) and cyber-physical systems (CPS) ([20]).

Although these articles primarily focus on the design of IDSs for several IoT related elements, only one presented by Zarpelao et al. [29] provide a study of IDS techniques specific for the IoT paradigm. xIn their survey article, they discuss placement strategies and detection methods of IDSs designed specifically for IoT. They also present common threats for IoT security and how IDSs might be used to detect them. Furthermore, they present a review of the common validation strategies employed in the intrusion detection methods for IoT and discuss open research issues and future trends.

Given that, the present article aims on studying the development of IDS in IoT and we concentrate our attentions on those works specifically targeting IoT systems and networks.

Our literature review of IDS in IoT classify every work concerning the following features of IDS: detection method, placement strategy and security threat. To classify IDSs for IoT, we will use the taxonomy proposed by [29] with regard of the attributes: detection method, placement strategy and security threat. The select works are listed and classified in Table I. In our opinion, by performing this analysis, we would not only improve our knowledge on the referred topics, but also create more opportunities for future researches in development of IDS in IoT.

TABLE I. SCIENTIFIC WORKS THAT STUDY IDS IN IOT

Work	Placement strategy	Detection method	Security threat
Cho et al. [30]	Centralized	Anomaly-based	Botnet
Le. et al. [31]	Hybrid	Specification-based	Routing attack
Liu et al. [32]	-	Signature-based	-
Misra et al. [33]	-	Specification-based	DoS
Gupta et al. [34]	-	Anomaly-based	-
Kasinathan et al. [35]	Centralized	Signature-based	DoS
Kasinathan et al. [36]	Centralized	Signature-based	-
Raza et al. [37]	Hybrid	Hybrid	Routing attack
Wallgren et al.[38]	Centralized	-	Routing attack
Amaral et al. [39]	Hybrid	Specification-based	-
Krimmling et al. [40]	-	Hybrid	Routing attack and Man-in-the-middle
Jun et al. [41]	Centralized	Specification-based	-
Lee et al. [42]	Distributed	Anomaly-based	DoS
Oh et al. [43]	Distributed	Signature-based	Multiple conventional attacks
Cervants et al. [44]	Distributed	Hybrid	Routing attack
Pongle et al. [45]	Hybrid	Anomaly-based	Routing attack
Summerville et al. [46]	-	Anomaly-based	Conventional
Le et al. [47]	Hybrid	Specification-based	Routing attack
Thanigaivelan et al. [48]	Hybrid	Anomaly-based	-
Midi et al. [49]	Centralized	Hybrid	-
Shreenivas et al. [50]	Hybrid	Hybrid	Routing attack

In the following stage, we present the analysis made to each of the works selected in our literature review.

By 2009, Cho, et al. [30] present a centralized IDS for IoT where packets that pass through the border router, between the physical and the network domain, are analyzed aiming to detect botnet attacks. They propose a detection scheme based on anomaly-based method and assume that botnets cause unexpected changes in the traffic of 6LoWAPN sensors. The proposed solution computes the average for three metrics to compose the normal behavior profile. When metrics from any node violate the computed averages, the system raises an alert.

In their 2011 work, Le et al. [31] followed the approach of organizing the network in regions. With this approach, they use a hybrid placement strategy to build a backbone of monitor nodes, one per region. The function of monitor nodes is to sniff the communication from its neighbors and define whether a node is compromised. One of the advantages of this solution is that there is no communication overhead. The detection method used is specification-based focused on detecting RPL attacks.

They use a finite state machine to specify the RPL behavior, which is used to detect malicious activity.

Also, in 2011, Liu et al. [32] propose a signature-based IDS that employs Artificial Immune System mechanisms. Detectors with attack signatures were modeled as immune cells that can classify datagrams as malicious or normal, non-self or self-element respectively. The article does not present which placement strategy should be adopted and doesn’t introduce the way that this approach could be implemented in IoT resource constraint networks. In this approach, the computational overhead needed to run learning algorithms might be a disadvantage.

In another 2011 work, Misra et al. [33] present a solution to prevent DDoS attacks over IoT middleware. This specification-based detection method, use the maximum capacity of each middleware layer to detect the attacks. The system will generate an alert when the number of requests to a layer exceeds the specified threshold. The placement strategy wasn’t presented by the authors.

In 2013, Gupta et al. [34] propose an architecture for a wireless IDS. In the architecture proposed, the normal behavior profiles for network devices would be constructed applying Computational Intelligence algorithms. Thus, there would be a specific behavior profile for each device with an IP address assigned. The placement strategy wasn’t presented by the authors neither the type of attacks that could be detected by their solution.

In another 2013 paper, Kasinathan et al. [35] propose a centralized solution where their main objective is to detect DoS attacks in 6LoWPAN-based networks. In order to implement the IDS, the authors adapted to 6LoWPAN networks a known signature-based, called Suricata. The attack confirmation depends on the analyzes made by a DoS protection manager after received an alert send by IDS. This verification is used to reduce false positive rate. Also, in 2013, Kasinathan et al. [36] also presented a centralized and signature-based approach, extending the approach proposed in Kasinathan et al. [35].

Also in 2013, Raza et al. [37] present an IDS for IoT named SVELTE whose objective is to detect sinkhole and selective forwarding attacks. This IDS had a hybrid placement strategy due to the participation of the border router and network nodes in the detection system. The border router runs IDS modules responsible to detect intrusions by analyzing RPL network data due to process intensive needs. On the other hand, network nodes are responsible for transmitting information to the border router, sending RPL network data and notifying about malicious traffic received. This work has also a hybrid approach on detection method, trying to balance the computing cost of the anomaly-based method and the storage cost of the signature-based method.

By analyzing the 2013 Wallgren et al. [38] article, it is possible to identify that the proposed work investigated protections capabilities of the RPL protocol against many types of routing attacks such as: sinkhole, selective forwarding hello flood, wormhole, clone ID, and Sybil. They proposed a IDS with a centralized placement strategy. The detection system is in the border router and, instead of monitoring the traffic crossing the border router, they suggest a heartbeat protocol to detect attacks within physical domain. According to the proposed protocol, the border router sends ICMPv6 echo requests to all nodes and expects the responses to detect attacks or availability issues.

On their 2014 paper, Amaral et al. [39] presented a IDS for IoT with a hybrid placement strategy. In their work, a group of selected nodes, called watchdogs, runs a IDS aiming to identify intrusions by sniffing the exchanged packets in their area. The watchdog uses a particular set of rules to decide whether a node is compromised. They defend that each component in the 6LoWPAN network might have a different behavior, so each area of the network could have a different set of rules. As it is a specification-based IDS, when a rule is violated, the watchdog sends an alert to a Event Management System (EMS) that is running on a node without resource constraints.

Also in 2014, Krimmling et al. [40] purpose a IDS for IoT. Although they did not indicate what placement strategy had been following, they tested a hybrid detection method combining signature-based and anomaly-based approach. The tests were done with their proposed evaluation framework and the results obtained show that each approach failed in detecting some attacks. For the authors, a combination of detection methods could detect a higher number of attacks such as routing and Man-in-the-Middle attacks.

Another 2014 work presented by Jun et al. [41] propose using Complex Event-Processing (CEP) techniques for intrusion detection in IoT. As placement strategy the authors use a centralized approach, since IDS is running on the border router to monitor network packets. It is a specification-based IDS which rules are stored in Rule Pattern Repository and takes SQL and EPL of Epser as a reference. The advantage of this work is that it uses the features of the events flows to judge the intrusions, which can reduce the false alarm rate. They found that their approach was more CPU intensive, consumed less memory and took less processing time than traditional IDS.

In 2014, Lee et al. [42] proposed a lightweight IDS for IoT. Their distributed placement strategy is based in a method that monitors the nodes energy consumption for detecting intrusions, namely DoS attacks. Each node monitors its energy consumption and when the energy consumption deviates from the expected value, the IDS classifies the node as malicious and removes it from the route table in 6LoWPAN. The authors use a anomaly-based method to analyze nodes behavior over energy consumption. By focusing only on a single node parameter, the authors attempted to minimize the computational resources needed for intrusion detection.

In their 2014 work, Oh et al. [43] also proposed a distributed lightweight IDS for IoT. They outline a algorithm that match packet payloads and attack signatures. In this signature-based approach, each node will inspect packet payloads using an algorithm design to skip a large number of unnecessary matching operations aimed to reduce the computational cost of comparison between packet payloads and attack signatures. Their tests focus in conventional attacks based on signatures from Snort, a traditional open-source IDS, and ClamAV, an open-source anti-virus. According to the authors, the proposed algorithm is faster than the Wu-Manber algorithm, which is one of the most faster pattern-matching algorithms, running on a resource-constrained scenario.

In 2015, Cervantes et al. [44] proposed an IDS for IoT named INTI (Intrusion detection of Sinkhole attacks in 6LoWPAN for Internet of Things). The placement strategy followed was a distributed system since they used a hierarchical structure of nodes. Each node as a role in the system, and the main task is to monitor a superior node estimating its traffic patterns. The approach combines concepts of trust and reputation in a specification-based method with anomaly-based method to monitor the exchange of packets between nodes. When a node detects a sinkhole attack, it broadcasts a message to alert the other nodes.

Also in 2015, Pongle et al. [45] proposed an IDS for IoT using a hybrid placement strategy. In their approach, network nodes must detect changes in their neighborhood and must send information to centralized modules running in the border router. The wormhole attacks are detected in the border router through three algorithms used to analyze the data sent by nodes and to detect such anomalies in the network. The results of tests performed by the authors showed that, apparently, their solution is appropriate for IoT systems since its power and memory consumption are low.

In their 2015 work, Summerville et al. [46] developed a IDS for IoT based in a deep-packet anomaly detection approach. The authors consider that IoT devices use simple and few protocols. That characteristic could result in a similar network payload. Their anomaly-based method uses a technique called bit-pattern matching to select feature selection. Network payloads are treated as a sequence of bytes, and the feature selection operates on overlapping tuples of bytes, called n-grams. A match between a bit-pattern and an n-gram occurs when the corresponding bits matches all positions. An experimental evaluation result shows that false-positive rates for four conventional attacks were very low.

In their 2016 work, Le et al. [47] design a lightweight IDS solution for IoT. Their hybrid placement strategy divides the network into small clusters. Each cluster has a cluster head that communicates with all other cluster members. The cluster head monitors the cluster members and had placed a IDS instance while the other cluster members only reports information to the cluster head. The border router had also placed an IDS instance and is responsible for tasks that need more computational resources. The authors use specification-based method extending their previous work [Le2011?????] on detection routing attacks.

Also in 2016, Thanigaivelan et al. [48] present an hybrid IDS for IoT. Their approach assigns different tasks to the network nodes and the border router, forcing them work cooperatively. Each node as a IDS module to monitor their neighborhoods and to send notifications of possible attacks to the IDS module on the border router. The IDS module in the border router receives he notifications from the nodes and decide if there were an intrusion or not. The anomaly-based method consists on looking for deviations of normal behavior learned from the monitoring information, but the authors did not provided much details about the method of determining the normal behavior.

In their 2017 work, Midi et al. [49] present an IDS for IoT called Knowledge-driven Adaptable Lightweight Intrusion Detection System (Kalis). The authors use a centralized placement strategy on which Kalis can be deployed on border router or as standalone tool on separated, external device. The hybrid approach for detecting intrusions is based on the fact that Kalis is a self-adapting, knowledge-driven IDS for IoT systems running different communication protocols. Kalis autonomously collects knowledge about the features of the monitored network and entities and leverages such knowledge to dynamically configure the most effective set of detection techniques. Other characteristics is that can be extended for new protocol standards and provides a knowledge sharing mechanism that enables collaborative incident detection. According to the authors, experimental tests show very good results on detection of DoS, routing and conventional attacks compared with traditional IDS.

Also in 2017, Shreenivas et al. [50] propose a solution on IDS for IoT. Their work is an extension of SVELTE, the work presented by Raza et al. [Raza2013 ????]. With the objective of improving the security within 6LoWPAN networks, the authors extend SVELTE with an intrusion detection module that uses the ETX (Expected Transmissions) metric. In RPL, ETX is a link reliability metric and monitoring the ETX value can prevent an intruder from actively engaging 6LoWPAN nodes in malicious activities. They also propose geographic hints to identify malicious nodes that conduct attacks against ETX-based networks. Their experimental results show that compared with rank-only mechanisms the overall true positive rate increases when they combine the EXT and rank based detection mechanisms.

IV. Conclusions

Internet of Things is an important part of the future due to its ability to connect physical objects to Internet in different application domains. Despite this, the security of IoT must be investigated and developed. However, as the resources of IoT devices are constrained, many security mechanisms are hard to be implemented to protect the security of IoT networks. As security mechanism, the IDS is one of the most important in traditional networks and should be used on IoT networks as well.

In this article, we presented a literature review about IDS research for IoT networks. In this review we analyze 20 works that were published between 2009 and 2017 that propose IDS solutions for IoT networks. We used a taxonomy based on characteristics like placement strategy, detection method and security threat.

We conclude that research in IDS in IoT are still in its infancy and incipient. The works reviewed do not cover a lot of IoT technologies and cannot detect a large variety of attacks.

Considering that placement strategy and detection method are so important characteristics of IDSs, we can also conclude that the analyzed works do not reach a consensus on which are the more proper options for that characteristics in IDSs in IoT.

In terms of future work we, as a research team, believe that will be important that future research's should concentrate attention on reach a consensus on which are the proper placement strategy and detection method. Increase the attack detection variety and address more IoT technologies should be also important to achieve in future research's.

REFERENCES

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

[2] A. Whitmore, A. Agarwal, L. Da Xu, "The Internet of Things-A survey of topics and trends", Information Systems Frontiers, pp. 1-14, March 2014.

[3] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer. Networks., vol. 54, no. 15, pp. 2787-2805, Oct. 2010.

[4] S. Horrow, and S. Anjali, "Identity Management Framework for Cloud Based Internet of Things", SecurIT '12 Proceedings of the First International Conference on Security of Internet of Things, 200-203, 2012.

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications", IEEE Communications Surveys and Tutorials, 17(4), 2347-2376, 2015.

[6] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of Cloud computing and Internet of Things: A survey", Future Generation Computer Systems, 56, 684-700, 2016.

[7] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey", IEEE Transactions on industrial informatics, 10(4), 2233-2243, 2014.

[8] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) security: Current status, challenges and prospective measures," in Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST), London, U.K., Dec. 2015, pp. 336-341.

[9] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social Internet of Things (SIoT) - When social networks meet the Internet of Things: Concept, architecture and network characterization," Computer Networks, vol. 56, no. 16, pp. 3594-3608, Nov. 2012.

[10] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in Proc. Euro Med Telco Conf. (EMTC), Naples, Italy, Nov. 2014, pp. 1-5.

[11] D. Zegzhda, T. Stepanova, "Achieving Internet of Things security via providing topological sustainability", 2015 Science and Information Conference (SAI), pp. 269-276, 2015.

[12] A. Meddeb, "Internet of Things standards: Who stands out from the crowd?", IEEE Communications Magazine, vol. 54, no. 7, pp. 40-47, Jul. 2016.

[13] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142, Oct. 2017.

[14] OWASP Internet of Things Project, https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf, accessed 19 December 2017

[15] F. A. Alaba, M. Othman, I. Hashem, and F. Alotaibi, "Internet of Things security: A survey", Journal of Network and Computer Applications, Volume 88, 2017, Pages 10-28.

[16] J. P. Anderson, "Computer security threat monitoring and surveillance", Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, 1980.

[17] L. T. Heberlein, "A network security monitor," in Proceedings of the IEEE Computer Society Symposium, Research in Security and Privacy, pp. 296-303, Oakland, Calif, USA, 1990.

[18] J. Vacca, 2013. Computer and Information Security Handbook. Morgan Kaufmann, Amsterdam, 2013.

[19] H. Liao, C. Lin, Y. Lin, and K. Tung, "Intrusion detection system: a comprehensive review", Journal of Network and Computer Applications, 36 (1), 16-24, 2013.

[20] R. Mitchell, and I. Chen, "A survey of intrusion detection techniques for cyber-physical systems", ACM Computing Surveys (CSUR), 46 (4), 55, 2014.

[21] K. Scarfone, and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)", Technical report, National Institute of Standards and Technology, special Publication 800-94, 2007.

[22] I. Butun, S. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks", Communications Surveys and Tutorials IEEE, 16 (1), 266-282, 2014.

[23] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks", IEEE Wireless Communications, 11 (1), 48-60, 2004.

[24] T. Anantvalee, and W. Jie, "A survey on intrusion detection systems in mobile ad hoc networks", Wireless Network Security, 2, 159-180, 2017.

[25] S. Kumar, and K. Dutta, "Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges", Security and Communication Networks, 9 (14), 2484-2556, 2016.

[26] A. Farooqi, and F. Khan, "Intrusion detection systems for wireless sensor networks: a survey", In Communication and Networking Communications in Computer and Information Science, 56, Springer, Berlin, Heidelberg, 234-241, 2009.

[27] A. Abduvaliyev, A. Pathan, Z. Jianying, R. Roman, and W. Wai-Choong2013, "On the vital areas of intrusion detection systems in wireless sensor networks", IEEE Communications Surveys & Tutorials, 15 (3), 1223-1237, 2013.

[28] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques", in Journal of Network and Computer Applications, 36 (1), 42-57, 2013.

[29] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in internet of things," Journal of Network and Computer Applications, vol. 84, pp. 25-37, 2017.

[30] E. Cho, J. Kim, and C. Hong, "Attack model and detection scheme for botnet on 6LoWPAN," In Management Enabling the Future Internet for Changing Business and New Computing Services, Lecture Notes in Computer Science 5787. Springer, Berlin, Heidelberg, 515-518, 2009.

[31] A. Le, J. Loo, Y. Luo, and A. Lasebae, "Specification-based IDS for securing RPL from topology attacks," In: Wireless Days (WD), 2011 IFIP, pp. 1-3, 2011.

[32] C. Liu, J. Yang, Y. Zhang, R. Chen, and J. Zeng, "Research on immunity-based intrusion detection technology for the Internet of Things," In: Natural Computation (ICNC), 2011 Proceedings of the Seventh International Conference, Vol. 1, pp. 212-216, 2011.

[33] S. Misra, P. Krishna, H. Agarwal, A. Saxena, and M. Obaidat, "A learning automata-based solution for preventing Distributed Denial of Service in Internet of Things," In: Internet of Things (iThings/CPSCom), 2011 International Conference on and Proceedings of the 4th International Conference on Cyber, Physical and Social Computing, pp. 114-122, 2011.

[34] A. Gupta, O. Pandey, M. Shukla, A. Dadhich, S. Mathur, and A. Ingle, "Computational intelligence-based intrusion detection systems for wireless communication and pervasive computing networks," In: Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, pp. 1-7, 2013.

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

[36] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. Spirito, "DEMO: an IDS framework for internet of things empowered by 6LoWPAN. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, CCS'13, ACM, New York, NY, USA, pp. 1337-1340, 2013.

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

[38] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based Internet of Things, International Journal of Distributed Sensor Networks, SAGE Publications, 2013.

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

[40] J. Krimmling, and S. Peter, “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, 2014.

[41] C. Jun, and C. Chi, “Design of Complex Event-Processing IDS in Internet of Things,” in Measuring Technology and Mechatronics Automation (ICMTMA), 2014 Sixth International Conference on, pp.226-229, Jan. 2014.

[42] T. Lee, C. Wen, L. Chang, H. Chiang, and M. Hsieh, “A lightweight intrusion detection scheme based on energy consumption analysis in 6LowPAN,” In: Advanced Technologies, Embedded and Multimedia for Human-centric Computing, Lecture Notes in Electrical Engineering, 260. Springer, Netherlands, 1205-1213, 2014.

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

[44] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, “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, 2015.

[45] P. Pongle, and G. Chavan, “Real time intrusion and wormhole attack detection in Internet of Things,” International Journal of Computer Applications, 121 (9), 1-9, 2015.

[46] D. Summerville, K. Zach, and Y. Chen, “Ultra-lightweight deep packet anomaly detection for Internet of Things devices,” In: 2015 IEEE Proceedings of the 34th International Performance Computing and Communications Conference (IPCCC), IEEE, pp.1-8, 2015.

[47] A. Le, J. Loo, K. Chai, and M. Aiash, “A specification-based IDS for detecting attacks on RPL-based network topology,” Information, 7 (2), 25, 2016.

[48] N. Thanigaivelan, E. Nigussie, R. Kanth, S. Virtanen, and J. Isoaho, “Distributed internal anomaly detection system for Internet-of-Things,” In: 2016 Proceedings of the 13th IEEE Annual Consumer Communications Networking Conference (CCNC), pp. 319-320, 2016.

[49] D. Midi, A. Rullo, A. Mudgerikar, and E. Bertino, “Kalis: A system for knowledge-driven adaptable intrusion detection for the Internet of Things,” In Proceedings of the IEEE 37th International Conference on Distributed Computing Systems (ICDCS’17), 2017.

[50] D. Shreenivas, S. Raza, and T. Voigt, “Intrusion Detection in the RPL-connected 6LoWPAN Networks,” Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, April 02-02, Abu Dhabi, United Arab Emirates, 2017.