The ISC Int'l Journal of Information Security
ISeCure

July 2018, Volume 10, Number 2 (pp. 79–92)
http://www.isecure-journal.org

Review Paper

A Survey of Anomaly Detection Approaches in Internet of Things

Morteza Behniafar [1,*], Alireza Nowroozi [2], and Hamid Reza Shahriari [3]

[1] *Faculty of Electronic and Computer Engineering, Malek Ashtar University of Technology, Tehran, Iran*
[2] *Computer Engineering Department, Sharif University of Technology, Tehran, Iran*
[3] *Department of Computer Engineering and Information Technology, Amirkabir University of Technology, Tehran, Iran*

ARTICLE INFO.

Article history:
Received: 23 February 2018
First Revised: 3 April 2018
Last Revised: 21 July 2018
Accepted: 30 July 2018
Published Online: 31 July 2018

Keywords:
Anomaly, Intrusion Detection, Internet of Things, IT Security.

ABSTRACT

Internet of Things is an ever-growing network of heterogeneous and constraint nodes which are connected to each other and Internet. Security plays an important role in such networks. Experience has proved that encryption and authentication are not enough for the security of networks and an Intrusion Detection System is required to detect and to prevent attacks from malicious nodes. In this regard, Anomaly based Intrusion Detection Systems identify anomalous behavior of the network and consequently detect possible intrusion, unknown and stealth attacks. To this end, this paper analyses, evaluates and classifies anomaly detection approaches and systems specific to Internet of Things. For this purpose, anomaly detection systems and approaches are analyzed in terms of engine architecture, application position and detection method and in each point of view, approaches are investigated considering the associated classification.

© 2018 ISC. All rights reserved.

1 Introduction

Analyzing security of Internet of Things (IoT) and its problems can be investigated from two viewpoints: 1) things and 2) network. At things level, IoT security faces different challenges compared to general computer networks due to its natural constraints of resources and computational power of things. Insecure communication channel, unsupervised operation in many applications and heterogeneity of the comprising things at network level makes the networks vulnerable against intruders and this makes security of such networks complicated. Thus, providing security for IoT and the implemented protocols is critical and requires lots of works to design and develop security mechanisms.

One of the security challenges in these networks is wireless communication which facilitates malicious operations of the adversary. Even when it is protected by cryptographic and authentication mechanisms, things are exposed to wireless attacks either from within the network (due to the physical intrusion in the network and nodes and things capturing as well as copying them) or from the Internet [1]. Another challenge is dynamic topology which provides the ground for the adoption of intruder nodes. In addition, routing protocols, flow control and access control layer protocols try to operate with less computational cost and overhead, therefore security challenges arise. Another

[*] Corresponding author.

Email addresses: mbehniafar@mut.ac.ir (M. Behniafar), nowroozi@ce.sharif.edu (A. Nowroozi), shahriari@aut.ac.ir (HR. Shahriari)

ISSN: 2008-2045 © 2018 ISC. All rights reserved.

challenge of IoT is energy constraint, for example, adversary can make nodes to wake up from sleep mode without any reason using an intruder node which broadcasts wake up beacons which makes nodes to lose their energy and their lifetime is shortened; therefore, IoT has special features which can be described as security challenges for these networks and this makes security attainment, a challenge towards developing such networks. Therefore, applying existing methods for detecting anomalies in the IoT are not directly possible and is faced with challenges [2, 3]. Anomaly detection from a large amount of heterogeneous data generated by various distributed sources with different data patterns and considering resource constraints are some of the main challenges [4].

Security and privacy are an afterthought on many things today, because manufacturers try to get products to market as quickly as possible. Also about device's firmware and different platforms and frameworks, the security evaluations have not been fully implemented. These and other issues cause vulnerabilities in different layers of IoT. OWASP cited top IoT vulnerabilities as follows [5]:

(1) Insecure Web Interface,
(2) Insufficient Authentication/Authorization,
(3) Insecure Network Services,
(4) Lack of Transport Encryption/Integrity Verification,
(5) Privacy Concerns,
(6) Insecure Cloud Interface,
(7) Insecure Mobile Interface,
(8) Insufficient Security Configurability,
(9) Insecure Software/Firmware,
(10) Poor Physical Security.

In this regard, with the exploitation of those vulnerabilities, there have been specific attacks on IoT-based network, among them, "2016 Dyn cyberattack" and "Persirai botnet attack" and Aidra can be mentioned. These botnets are also called the thingbots and comprise of all sort of devices ranging from smart phones to laptops and the new smart devices like TV and refrigerator. When infected by a botnet the IoT devices become part of an enormous DDoS[1] ecosystem and send requests to the target server to crash it. Such an attack makes it hard to trace the actual source as millions of connected devices are bombarding the network together. In 2016 Dyn cyberattack [6], Dyn came under attack by multiple large and complex DDoS attacks against their Managed DNS infrastructure originated from Mirai-based botnets by generated compounding recursive DNS retry traffic which caused major disruption of Internet services. The attack was a botnet coordinated through a large number of compromised IoT devices (more than 100,000 malicious endpoints), including Digital Video Recorders (DVRs), IP-cameras, printers, residential gateways and so on, that had been infected with Mirai malware. In 2017, a new IoT botnet called Persirai has been discovered targeting over 1000 IP camera models based on various Original Equipment Manufacturer (OEM) products by taking advantage of UPnP[2]. Persirai can perform UDP DDoS attack with SSDP packets without spoofing IP address. Trendmicro detected approximately 120,000 IP cameras that are vulnerable to Persirai [7].

In the context of IoT IDS survey, a few researches have been done [8] and in the context of anomaly based IDS in IoT, no significant work has been done until the preparation of this paper. Therefore, this paper reviews and surveys anomaly detection systems and approaches in the context of IoT and proposes a classification of works done from different points of view.

In the following, Section 2 describes anomaly detection and general classification of anomaly detection approaches in general computer networks. Section 3 investigates, analyzes and evaluates researches on anomaly detection in the context of IoT. Finally, the paper is concluded in Section 4.

2 Anomaly Detection

Cryptographic techniques are used as a deterrent security layer and defense frontline which can be broken due to weak security mechanisms in things and wireless environment. On the other hand, intruder nodes can make insider attacks without considering cryptography (due to authentication and having the encryption keys). For example, they can target system communications and interactions and disturb system communications or eavesdrop message contents or change them and change aggregated information of the network. Thus, a second defense layer is required to provide security of the network in which system interactions are monitored and relevant alarm are issued upon detecting anomalous behavior in the network. Indeed, this defense system not only monitors network behavior for detecting anomalous behavior of the insider attackers but also it is applied to detect malicious behaviors of unknown external network attackers. In fact, this system is able to analyze and identify normal behavior of the IoT network to detect attacks and threats of the insider things, external threats from Internet and hybrid attacks of these two in interactions of internal things and gateways so that whenever an anomaly is detected, the system is warned so that more damages are prevented. In this

[1] Distributed Denial of Service

[2] Universal Plug and Play

regard, system behavior and network status analysis is one of the main problems in managing IoT. This is why detecting anomalous behavior and anomaly from network flow is one of the main keys in identifying status and condition of the network. This is because detecting anomalous and malicious behavior results in anomaly level in two forms of labeling and scoring for blocking or eliminating adversary nodes [9]. Anomaly labeling leads to false positive or false negative errors, but the fuzzy consequence and the use of scoring and probabilistic methods in providing the result of anomaly detection is more appropriate.

By connecting a local network of things to Internet and migrating from M2M[3] inter-network communications to Internet-based communications, characteristics of the local wireless network of things and Internet are integrated and have created new characteristics. Thus, integrating Internet and local network of things changes challenges and existing solutions; which is due to considering characteristics of the closed local network of constrained nodes and Internet simultaneously and integrating them together. To mention some examples of these features for this network, open access to local network of things from Internet, physical access to network nodes to compromise the legitimated nodes, limited resources available for anomaly detection approaches (considering their overhead), unstable communication links in the network of things, wireless-specific attacks through insider intruder and outside of the network-Internet, considering IoT specific protocols (for instance, 6LoWPAN[4] is a lightweight protocol for using IPv6 in low power networks) and specific architecture of things and comprising a heterogeneous network of nodes can be named [9–11]. Aforementioned problems make conventional anomaly detection approaches not to be responsive for IoT and proposing new solutions, methods and designing new architectures based on specific architectures of IoT necessary so that lightweight anomaly detection approaches considering resource constraints proportionate to security challenges can be presented. Considering the discussion above for anomaly detection in IoT, there are strategic issues which should be analyzed specifically for IoT. To this end, the following issues can be mentioned:

- Analysis, design and extracting appropriate and efficient features: these features should be designed such that accuracy of detecting anomaly and attacks is efficiently high by reducing overhead of monitoring data due to constrained resources.
- Architecture of anomaly detection engine: designing, deployment structure, engine components structure and interactions, information collector agents, decision making agents and locating them in the network for maximum efficiency and minimum network overhead.
- Analysis mechanisms and anomaly detection techniques: analysis and design of processing procedures such that detection accuracy for anomaly detection specific for IoT is increased and computational cost is decreased.

Thus, the aforementioned issues are problems which should be analyzed specifically for these networks so that approaches proposed for anomaly detection in the context of IoT are identified well and these elements can be used to identify approaches which can be proposed to detect anomalies in IoT with high accuracy and low overhead.

After identifying principles of anomaly detection and its components, anomaly detection systems should be investigated in general computer networks so that studies in the context of anomaly detection in IoT can be analyzed with a good perspective of work done in this field; thus, in the following, principles of anomaly detection in general computer networks are presented.

Anomaly Detection in General Computer Networks

Researches in the context of anomaly detection in general computer networks are conducted to Intrusion Detection. In order to obtain a better understanding in the context of anomaly detection in IoT and analyze the researches in this field, principles of anomaly detection methods in general computer networks are given first and then studies in this field are analyzed and investigated. Understanding anomaly detection approaches in computer networks and recognizing their advantages and shortcomings provides the possibility for the researchers to analyze and compare the existing methods to propose an optimal mechanism for detecting anomalies in IoT.

Researches and studies in the context of anomaly detection in general computer networks have resulted in systems with different anomaly detection procedures. Most of these methods have employed procedures which require high computational and operational overhead to increase detection accuracy. This is because, in the conventional Internet, constrained energy and resources is not an acute problem; thus, focus is on increasing detection accuracy. Methods employed for anomaly detection can be classified into two groups of model-based and similarity-based methods [12]. In model-based methods, first a normal model

[3] Machine to Machine
[4] IPv6 over Low-Power Wireless Personal Area Networks

of the behavior of the network's elements is defined and then violations from the model are considered as an anomaly. In similarity-based models, each data is compared with other data of the network and collective data and non-similarity with other data of the network is identified as an anomaly.

In previous studies, some features are mentioned for monitoring and supervising for intrusion detection among which, the following can be mentioned [13–17]:

- Time interval between consequent messages for detecting speed of packet transmission.
- Content of the packet and number of modified packets for monitoring message integrity attacks.
- Transmission latency for detecting latency attacks in sending packets including black hole attack or selective forwarding attacks.
- Repeated packet transmission to detect denial of service.
- Transmitter node identity to detect attacks like Wormhole, Helloflood, and neighbor discovery attacks in IPv6 and Sybil.
- Number of collisions for detecting attacks like jamming.
- Number of packet loss for detecting attacks and symptoms of dropping, modifying or jamming.
- Amount of energy consumed by network components to prevent distribution of energy consumption in the whole network.

Each of the aforementioned parameters has higher efficiency in one or several threats or attacks and is not able to detect all attacks. In addition, it should be pointed out that a network with limited resources like limited energy and computational capacity like IoT is not able to monitor all of these parameters; thus, attacks and threats should be prioritized according to application and goal, thus on that basis, extract and monitor some of features. To this end, researches conducted in this field have extracted and monitored different parameters of the network according to their detection goal.

3 Literature Review

Principles of the methods employed for anomaly detection in general computer networks were studied in the above. In this section, previous work done in the context of anomaly detection in IoT are analyzed and classified. These studies are analyzed and investigated from three different viewpoints and in each section, investigations are presented considering the associated classification. First, in terms of engine architecture, hybrid intrusion detection systems (anomaly-based detection along with signature-based detection) and pure anomaly-based intrusion detection are identified. Second, anomaly detection in IoT has been investigated from another point of view; Functionality Position; in which two general groups are identified. One group is for detecting anomaly in transport and network layer which generally studies behavior of nodes and network in communication links, and transport layers and associated attacks including routing attacks. In another class, studies are conducted on anomaly detection at service and application level and interactions and data flow parameters are studied. Third, studies are classified in terms of the employed method to detect anomaly in detection engine. In this aspect, different mechanisms are used to detect anomaly where the most significant ones are anomaly detection methods based on statistical mechanisms. Indeed, methods based on SVM, neural network and artificial immune system are also proposed which are more limited. Figure 1 shows anomaly detection approaches classification presented in this paper and Table 1 show a brief review of researches done in anomaly detection in IoT networks.

3.1 Anomaly Detection in terms of Detection Engine's Architecture

In research done in this field, three approaches were proposed for Intrusion detection in IoT. In the first approach, intrusion detection based on signature is proposed. In this method, detection phase and attack classification are performed through predetermined patterns. In another class, approaches for intrusion detection in IoT are implemented by combining signature-based methods and anomaly detection methods which detect intrusion using these two methods simultaneously or sequentially. In the third class, only anomaly detection methods are used for intrusion detection and predefined signature attacks are not applicable. In this paper, studies performed in the two latter cases are investigated. Between these two methods, focus is on intrusion detection based on pure anomaly detection methods; thus, most studies and proposed systems are related to this part. For this reason and because all of them cannot be described in this section, therefore Researches conducted on the case of the hybrid method in this section will be presented by case and pure anomaly detection methods are described in the following sections related to the specific proposed method.

3.1.1 Anomaly-based Intrusion Detection System

In this class of systems, merely anomaly detection methods are used to detect attacks and identify intrusion in the network. First, the normal behavior of the

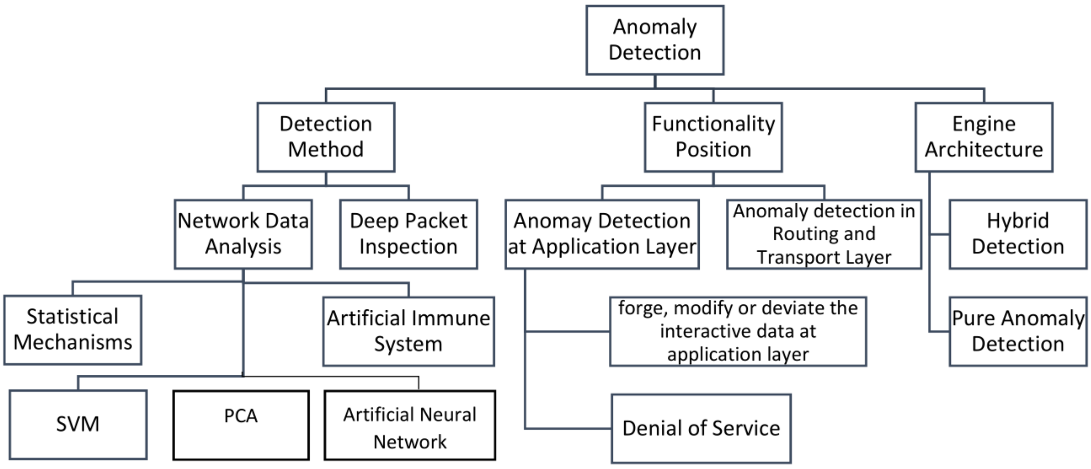

Figure 1. Anomaly Detection approaches in IoT

network is identified and then an intrusion is detected through identifying violations from normal behavior. In this method, the signature of attacks is not accessible and only approximation methods are used to detect intrusion. Thus, false negative is one of the challenges of this method but on the contrary, it is able to detect new attacks and changing behavior of the network in previously known attacks. Due to advantages of detecting new attacks and changing behavior of the network, studies have focused on this context. Thus, due to large number of research done in this field, studies considering the focus of the proposed method is presented in more details in the following. In this regard, authors of [62] have investigated intrusion detection approaches and have compared them together to apply them to cloud applications based on IoT and have concluded that intrusion detection systems based on statistical measures, anomaly-based detection methods and clustered architecture can be applied to IoT. It has been mentioned that IoT is a network of different components and things with different applications which are connected to each other. Thus, heterogeneous structure in the topology of IoT is very common. So, clustering network to different application classes is a suitable approach in mechanisms based on IoT.

3.1.2 Hybrid Intrusion Detection System

In these methods, intrusion detection engine combines anomaly and signature-based detection methods. This combination is implemented in two ways. In the first approach, signature-based intrusion detection is at the first layer and then anomaly-based intrusion detection operates as being suspected to the network or detecting an anomalous signature. Our analysis show that, in this approach, detecting suspicious states in the network is a challenge, because the advantage of anomaly detection in comparison to hybrid approach is in detecting states which signature-based systems are not able to detect. In another approach, signature-based and anomaly-based intrusion detection systems operate in parallel and their detection objective is different. In this regard, this section investigates intrusion detection systems which have employed anomaly detection and signature-based systems as a hybrid Intrusion detection approach.

Analysis of [8] indicates that for intrusion detection in IoT, a hybrid intrusion detection system is required in which 6LoWPAN is considered and multilateral detection mechanism based on anomaly detection and protocol analysis is offered.

Studies in [34, 35] are also of hybrid intrusion detection type and are proposed in details in section 3.2.2. In addition, authors of [44, 45] have proposed an intrusion detection system for IoT (Internet-based heterogeneous sensor networks) which is based on signature and anomaly. This paper has also investigated in section 3.3.1.

Authors of [36, 37] have proposed a hybrid intrusion detection system in another way. In the proposed approach, normal profile at activity intervals is detected first and then it is used to detect anomalies in the behavior of nodes. After this stage, this anomaly is compared with defined anomalies to extract its type, then by considering anomaly types that are detected; intrusion type is detected by predefined expert knowledge rules. These papers have defined and classified anomalies and attacks imposed on the network very well. In [36], results of intrusion detection and normal profile of each node are sent to the upper layer, based on which, network detects intrusion. In [37], employing rules resulting from expert knowledge in anomaly detection is described and generalization of the work remained for future works.

In [42, 43], A Hybrid Intrusion Detection System

	Engine Architecture	Functionality Position	Detection Method	Description
[18] Liu et. al	Pure Anomaly Detection	Network and Application Layer	Statistical network data analysis	Jacquard coefficient
[19] Kasinathan et. al				6LoWPAN DoS attacks detection
[20] Ding et. al				Latent correlation
[21] Yang et. al				Data aggregation anomaly detection
[22] Lyu et. al				Hyper-ellipsoidal clustering
[23] Ageev et al				******
[24] Chen et al				
[25] Eliseev et. al				
[26] Gunupudi et. al				
[27] Pacheco et. al				
[28] Onal et. al				
[13] Le at al	Pure Anomaly Detection	Routing and Transport Layer	Statistical network data analysis	RPL
[29] Thanigaivelan et al				
[30] Mayzaud et. al				
[31] Summerville et. al				Deep Packet Inspection
[32] Wang et al				*****
[33] Wang et al				
[34] Raza	Hybrid	Routing and Transport Layer	Statistical network data analysis	*****
[35] Raza et. al				
[36] Fu et al	Hybrid	Network and Application Layer	Statistical network data analysis	*****
[37] Desnitsky et al				
[38] Pongle et al	Pure Anomaly Detection	Routing and Transport Layer	****	Blackhole and wormhole detection
[39] Tsitsiroudi et al				
[40] Surendar et al				
[41] Sarigiannidis et al				
[42] Bostani et al	Hybrid	Routing and Transport Layer	****	Optimum-path forest algorithm
[43] Sheikhan et al				
[44] Amin et al	Hybrid	Network and Application Layer	Statistical network data analysis	Based on CUSUM algorithm
[45] Trilles et al	Pure Anomaly Detection			
[46] Machaka et al				
[47] Moshtaghi et al				
[48] Yu et al	Pure Anomaly Detection	Network and Application Layer	PCA	*****
[49] Hoang et al				
[50] Zhao et al				
[51] Zheng et al	Pure Anomaly Detection	Network and Application Layer	SVM	*****
[52] Shilton at al				
[53] Zissis et al				
[54] McDermott et al				
[55] Jain et al				
[56] Sedjelmaci et al	Hybrid	Network and Application Layer	Neural Network	Neuro-fuzzy
[57] Thing et al	Pure Anomaly Detection			****
[58] Granjal et al	Hybrid	Network and Application Layer Routing and Transport Layer	Statistical network data analysis	Threshold based method
[59] Domb et al	Hybrid	Network and Application Layer	******	Random-Forest algorithm
[60] Tama et al	Pure Anomaly Detection			
[61] Sedjelmaci et. al	Hybrid	Network and Application Layer	*******	Game theory

Table 1. IoT Anomaly detection literature

for Internet of Things based on MapReduce approach with the aim of distributed detection is proposed. The proposed model use supervised and unsupervised optimum-path forest model for intrusion detection.

Granjal and Pedroso [58] proposed a hybrid intrusion detection system for CoAP based network. This work design and implement various predefined rules and threshold for transport, network and application layers to detect malicious nodes and remove them from network interactions. Also intrusion prevention is done through node blacklists. The point is detection of new types of attacks and Internet side attacks by predefined scenario in the presented approach and it seems that defining new detection scenarios is required. Finally, they implemented and evaluated experimentally the proposed approach and impact on critical resources of sensing devices and of its efficiency in dealing with the considered attacks. Implementation and evaluation of resource usage is done by Contiki Simulator.

3.2 Anomaly Detection in terms of Application

As mentioned, a class of researches has studied anomaly detection and attacks at lower layers of the network and another class of researches has investigated anomaly detection at application and network layer. In this regard, first class detects routing related attacks including blackhole, wormhole. The second class detects attacks including application attacks, network attacks and attacks from Internet.

3.2.1 Anomaly Detection at Application Layer

In this class of studies, the focus is on detecting attacks on interactions data or network service. In the first class, attacks aim to destruct, forge, modify or deviate the interactive data at application layer. In the second class, attacks aim to disrupt the service and network function. Most researchers focus on detecting anomalies at application layer, so there are some works in this context, thus this section cannot investigate them all by case. Considering what the paper has focused on, details are described provided in the following sections. Some of the researches in this context are associated with detecting anomalies in industrial data [63–65] and Industrial-IoT [66]. In this class, a real application service of IoT like smart homes [67, 68] or application of IoT in industry [69]is considered and According to context and application, different techniques are employed for data anomaly detection.

3.2.2 Anomaly Detection in Routing and Transport Layer

In this class of researches, routing attacks in 6LoWPAN-based networks and attacks in transport and network layers are investigated. In this regard, [13, 35] have investigated detecting routing attacks in 6LoWPAN-based IoT networks. In this context, authors of [34, 35] have proposed SVELETE intrusion detection system for IoT aiming to detect routing attacks including wormhole, selective forwarding and so on. Authors of [13] have also investigated providing security of IoT using intrusion detection systems. In this study, the purpose is to make IoT resistant against vulnerabilities and security threats of quality of service on 6LoWPAN platform and focus is on attacks imposed on routing protocols considering QoS.

In [29, 30], a framework is proposed for anomaly detection in IoT in which nodes in distributed manner evaluate their neighbors by using RPL (Routing Protocol for Low-power and Lossy network) in their own way. In [29] nodes transmit evaluation results to their parent nodes through a control message on RPL platform and higher layer nodes transmit the message to edge router nodes or gateways. Finally, edge nodes are responsible to verify anomalies of nodes and notify nodes periodically. Evaluating and reporting anomalous behavior in network layer and isolating anomalous node is performed at link layer. This is due to prevent anomalous node's data does not enter the higher layers of the network for processing. Structure of detection modules and isolation of anomalous nodes in network layer might be beneficial for optimality of packets' data processing in network layer and preventing extra processing of anomalous nodes packets in link layer. This paper has not discussed implementation and evaluation of the mentioned method. In [30], a structure is proposed for distributed passive monitoring which multi-instance feature of RPL protocol is used to propose several network routing topologies. In this method, network nodes are divided into two groups. One group is constrained nodes and the other group is watchdog nodes which eavesdrop interactions of a homogenous network of things and monitor nodes passively and evaluate them and offer their results to the sink nodes for a comprehensive evaluation of the network status. These two networks are formed by two different topologies and two separate RPL samples forming the network and are linked to higher nodes.

EyeSim [39] and VisIoT [41] are intrusion detection systems with visual assistance for representing the status of nodes' links. Mentioned systems detect wormhole links to detect black hole attacks. Sink node is responsible for nodes monitoring in order to detect links of black-hole and monitor neighbors, routing tables of each node and next step in packet routing and transmission and detect intruder nodes through investigating this information. The main focus of these papers is based on graphical representation of nodes' links to each other for analyzing and monitoring nodes and network and representing results obtained from security evaluations like detecting black-hole links. Also in black-hole attack detection, InDReS [40] is a system which detects and prevents intrusion through emphasizing on detection of black-hole attacks and isolation of malicious node. In the proposed method, network nodes are divided into categories with a head as watching node which monitors packet drop count of its surrounding nodes and finally uses the information obtained from monitoring neighbors and scores each node using Dempster Shafer theory and detects the malicious nodes through comparing the score with a threshold and informs the network to isolate it. NS2 simulator is used to evaluate the proposed work. In the simulations, assumptions are: network nodes are homogeneous, the network is connected to the Internet and head is not captured.

3.3 Anomaly Detection in terms of Detection Method

Detection engine and the approach used for detecting anomaly apart from system architecture and its application and based on detection method plays the main role in anomaly detection approaches survey. Researches are divided into two groups in terms of detection mechanism. In one group which includes the most work done, detection approach is based on network data analysis. The other limited group studies deep packet inspection for anomaly detection.

3.3.1 Anomaly Detection based on Network Data Analysis

This method is based on applying different algorithms for supervising and monitoring network and application level data as anomaly detection feature. All network data including content of interaction data between nodes at application layer and the parameters of network traffic flow are monitored and analyzed so that if their values are changed whether in terms of values exchanged at application layer or values of traffic flow, deviation from normal behavior is detected. Different algorithms are proposed for detecting anomalies based on these data but most methods employ statistical mechanisms in detecting normal behavior of data at application and network layer and deviation from it. Some recent studies are also proposed, in which artificial immune system, SVM classifiers, neural network and PCA based approaches are applied to network data for detecting anomalies.

Anomaly Detection based on Artificial Immune System

Authors of [70–72] have investigated the overall review of the applying artificial immune algorithms for anomaly detection based on using network level data on IoT and their system architecture. In [70], a general architecture is proposed in which a central service provider and some agents are predicted for detecting anomalies at gateways. They proposed general architecture and application of artificial immune algorithms for anomaly detection and work on details of detection method and practical evaluation might be for future.

Anomaly Detection based on SVM

For detecting anomalies based on SVM classifiers, [52] has proposed DP1SVM which is a one class SVM with update feature for learning data model. This paper has focused on extracting the associated SVM and update method. A set of environmental features in a sensor network comprising 9 sensors is used for evaluation and data samples of a sensor during two-weeks are used for testing the proposed SVM and time curve required for learning and updating the model is also presented for data of that network. Also, authors of [51] have investigated applying a one-class SVM as a general structure. Applying the aforementioned methods for implementation in constrained nodes of IoT should be considered in terms of overhead and cost.

Anomaly Detection Based On Neural Network

Artificial Neural Network is another method used for anomaly detection for Internet of Things. In this method, an artificial neural network used to model network data and do clustering on aggregated data form end nodes. Advantage of this method is its usability in different and diverse area in supervised and unsupervised manner, so in different contexts, it can identify and learn network data model and detect anomaly data. This excellence requires providing more data to tune its neurons organization and weighted connections for identifying data pattern and overall data model. Some works used neural network along with and in comparison to other machine learning methods.

In this context [54, 55] investigated Neural Network and SVM method and compared their result in anomaly detection and demonstrated the promise of both computational intelligence techniques in effectively detecting intrusions; although SVM performs better results with smaller sample size than neural network. Authors of [57] study deep learning approach for anomaly detection in IEEE 802.11 Network. This work examined the utilization of different techniques as the activation functions for the hidden neurons in the proposed neural network for attack detection and classification.

Anomaly Detection based on Principal Component Analysis

Authors of [48–50] proposed a model for intrusion detection in IoT which is based on dimension reduction algorithm and a classifier. The proposed model uses Principal Component Analysis (PCA) to reduce dimensions and complexity of various data from a large number of features to a small number. After data complexity reduction, a classifier with less overhead and complexity can better detect the data anomalies. By applying this method, they hope to execute simpler detection method in IoT constraint nodes with less complexity and resource usage.

Anomaly Detection Based on Statistical Mechanisms

In this class of approaches, a statistical model of network's behavior parameters resulted from data flow processing of the network interactions is comprised implicitly or explicitly [16]. It is necessary that this statistical model or behavior profile is generated in a normal condition without anomaly. After this stage, in time intervals, the profile is updated based on network behavior. In order to detect anomaly, obtained data from network behavior is compared with reference profile and a degree of anomaly or a label is assigned to it according to the amount of deviation. Considering policy of the method in presenting the output, a degree of anomaly or a label is presented as anomaly result. Presenting anomaly label is done through comparison with a threshold where determining a threshold according to conditions is challenging.

Authors of [19] have presented an architecture for detecting denial of service attacks at network side which is proposed centrally in managerial component of Low Power networks based on 6LoWPAN. For detecting attacks, packets' size threshold rule is used. In order to evaluate the proposed approach, penetration test and flooding attacks traffic flow are used. Authors of [24] have proposed a general architecture for anomaly detection in IoT in which network nodes are divided into three groups. Local detection at node level is associated to working nodes and data collectors; after anomaly signs, associated node which detects anomalies and finally the decision maker node decides about its being anomalous considering prior scores of the node. For detection procedures, this work has mentioned comparing average of data with a threshold. Authors of [23] have investigated cumulative parameters of the statistical distribution of data flow and anomaly is analyzed and detected through fuzzy inference from cumulative statistical parameters like mean, variance and etc. this paper has focused on flow analysis technique and practical evaluation is performed through generating synthetic statistical data.

Liu et.al [18] have examined using of Jacquard coefficient as a measure for detecting data similarity and detecting distance between data instead of using similarity measures like Euclidean distance. In this paper, general data generated by MATLAB are used as statistical features for implementing and evaluating the proposed algorithm and anomaly detection.

[22] Proposed a Fog-Empowered anomaly detection scheme based on hyper-ellipsoidal clustering algorithm. In the fog computing model, the Fog layer and the Cloud layer nodes perform the clustering and anomaly detection process and end nodes do not run clustering process on the data. This anomaly detection scheme improves timely detection of anomalies and saves energy consumption in the network by reducing process end node process overhead.

Cumulative SUM algorithm is employed in several papers [44–46, 73] as a scoring classifier based on SPC for analyzing data series aiming for anomaly detection. In anomaly detection section of [44] which was presented in section3.1.2, this method is used to detect anomaly in data collected from the network. In order to evaluate the proposed method, a network with mesh topology is created randomly using NS2 which communicates data randomly and applies the proposed method to detect anomaly in data flow and attacks like denial of service. Authors of [45, 73] have proposed a framework for anomaly detection system in Internet of Things. An anomaly detection system based on this framework is proposed for environmental monitoring systems based on the above algorithm. In the proposed framework, a brokering approach is used to receive and process data from different types and protocols from different nodes with different standards in different processing layers. In fact, the proposed approach is to consider a broker for each class of nodes so data of that class is received and converted to the standard format and is offered to the detection module (CUSUM) for anomaly detection. Indeed, discussions in this paper point out that CUSUM has constraints and disadvantages in applying and implementing procedures for detecting some anomalies including trend change in the above system. As mentioned, this paper has proposed a framework for a data series analysis in a network of nodes and anomaly detection in IoT is an example of realizing this system. Detection algorithm parameters and deployment structure of detection modules and features being analyzed and details of anomaly detection method are issues which should be presented by authors of that paper. [46] Has also employed CUSUM to detect DDoS attacks emphasizing on detection of TCP SYN flooding attacks in IoT. In the proposed paper, the above method is applied for anomaly detection and investigate adjustment of algorithm parameters and their impact on the efficiency of the method and analyze balance between detection rate and false positive rate and balance between detection rate and latency in detection. In order to evaluate the proposed method, DARPA data are used and for simulating IoT, attack data are added to the data.

Papers [32, 33], evaluate efficiency and quality of service of the network to detect anomalies in qualitative parameters of the network and parameters associated to quality of service and efficiency are modeled in order to maximize utility. That is, parameters of QoS in all nodes of the network are measured in normal condition and if measured parameters are different from normal values, anomaly is detected. For instance, latency and hop count are mentioned as examples of the quality of service parameters.

LCAD [20] is an approach for anomaly detection in different data series based on Latent correlation method. In the proposed method, correlation vectors are computed first using correlation matrix which represents link between different sections of data. Using latent correlation vector (LCV), associated latent correlation probabilistic model among data is computed. Finally, applying the probability distribution model to data and estimating matching between data and the associated model, data anomaly is detected. It should be mentioned that using central limit theorem, it is assumed that there are a few numbers of anomalous vectors, accordingly, probabilistic distribution model which is used to detect anomaly, is constituted. In order to evaluate the proposed method, three outlier detection methods are compared to detect anomaly on industrial data. Analysis show that what should be considered about the proposed method is that its overhead and computational complexity on constrained nodes and online anomaly detection should be considered.

Eliseeve [25] has proposed a method for detecting anomaly from data flow in the central server without inspecting flow content. This method employs cross-correlation of request-response features in the server flow to analyze network behavior and evaluate it through correlation of requests and responses to the current flow of the network with its normal state. In order to evaluate this correlation, Pearson correlation coefficient and neural network one-class classifier are employed. Considering discussions in the proposed paper, the first method is not efficient if request content is not considered due to the dependency of response to request content, because different requests generate different responses even if they are of the same size, thus this method cannot be employed in heterogeneous networks. Thus, this method can be used in servers with simple and similar interactions and the paper has suggested using the second method. But it should be said that the second method is not suitable to be implemented in constrained nodes and it should be employed in high power nodes like edge router nodes.

3.3.2 Anomaly Detection through Deep Packet Inspection

Authors of [31] have detected anomalies through deep packet inspection of data being interchanged in the network and they have claimed that anomaly can be detected by comparing packets bit by bit and by pattern matching. In this method, first, the normal pattern is learned by data packets being transmitted among nodes of the same type and adjusts parameters of detection pattern through bit distribution of each class of nodes and finally, after learning phase, detects anomaly in packets data through pattern matching and using logical operation applied to bits. Finally, in order to evaluate the proposed method, assumed that communication protocols of nodes are simple, thus data packets are very similar to each other and can be compared at bit level to detect anomalies through pattern matching.

Heterogeneity in context, application and data being transmitted in IoT are the problems which should be considered in the above analysis. This is because, exchanged data at bit-level can be completely different by their contextual values to compare with others. Another issue that makes this method, challenging is Internet-side attacks that which are not necessarily recognizable by bit matching and bit level analysis.

4 Conclusion

As mentioned, works done investigated from three points of view. In engine architecture, most studies have focused on pure anomaly detection in contrast to hybrid IDS. In functionality position point of view, researches done both in the transport layer and detection of routing related attacks as well as application layer and data anomaly detection. In detection methods point of view, most works are done on statistical data anomaly detection. As a summary two field more taken into consideration: first, anomaly intrusion detection at transport layer and routing related attacks. The other one is statistical anomaly detection on the network and application layer data. Most studies in this context are general and have not considered specific features of heterogeneous and constrained networks of IoT and mostly a general model and framework without practical evaluations on IoT specific data and platform has been proposed.

The main issue with the proposed approaches in the literature is the detection approach overhead in terms of computation, communication and time complexity for execute in IoT-based limited nodes for real time anomaly detection. Another important issue of works done on IoT anomaly detection is the heterogeneity of things and context and applications. A general anomaly detection approach cannot provide a separate diagnostic model for any type of application and data and for different infrastructures and all the protocols and data exchanged can be completely different. Based on analysis of works done in the literature, simultaneously address these two issues and achieve high accuracy in detecting anomalies in IoT is an open problem. Thus, in order to propose a comprehensive anomaly detection system in IoT apart from infrastructure protocols for context independent and different applications to detect data and network anomaly, heavy work is required. In this regard, heterogeneity and constraint resources of IoT nodes and diversity of applications and contextual data types are significant issues that needs to be considered in order to achieve an all-purpose global anomaly detection approach for entire IoT network with heterogonous cluster of nodes.

References

[1] Prabhakaran Kasinathan, Gianfranco Costamagna, Hussein Khaleel, Claudio Pastrone, and Maurizio A Spirito. An ids framework for internet of things empowered by 6lowpan. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 1337–1340. ACM, 2013.

[2] Miao Xie, Song Han, Biming Tian, and Sazia Parvin. Anomaly detection in wireless sensor networks: A survey. *Journal of Network and Computer Applications*, 34(4):1302–1325, 2011.

[3] Sutharshan Rajasegarar, Christopher Leckie, and Marimuthu Palaniswami. Anomaly detection in wireless sensor networks. *IEEE Wireless Communications*, 15(4), 2008.

[4] Charu C Aggarwal, Naveen Ashish, and Amit Sheth. The internet of things: A survey from the data-centric perspective. In *Managing and mining sensor data*, pages 383–428. Springer, 2013.

[5] Top iot vulnerabilities. https://www.owasp.org/index.php/Top_IoT_Vulnerabilities. Accessed: 2018-07-10.

[6] Dyn analysis summary of friday october 21 attack. https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack. Accessed: 2018-07-10.

[7] Persirai: New internet of things (iot) botnet targets ip cameras. https://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/. Accessed: 2018-07-10.

[8] Audrey A Gendreau and Michael Moorman. Survey of intrusion detection systems towards an end to end secure internet of things. In *Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on*, pages 84–90. IEEE, 2016.

[9] Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection: A survey. *ACM computing surveys (CSUR)*, 41(3):15, 2009.

[10] ShiWei Chao Jiang Du. A study of information security for m2m of iot. In *Advanced Computer Theory and Engineering(ICACTE), 2010 3rd International Conference on*, pages 576–579. IEEE, 2010.

[11] Debasis Bandyopadhyay and Jaydip Sen. Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1):49–69, 2011.

[12] Ismail Butun, Salvatore D Morgera, and Ravi Sankar. A survey of intrusion detection systems in wireless sensor networks. *IEEE communications surveys & tutorials*, 16(1):266–282, 2014.

[13] Anhtuan Le, Jonathan Loo, Aboubaker Lasebae, Mahdi Aiash, and Yuan Luo. 6lowpan: a study on qos security threats and countermeasures using intrusion detection system approach. *International Journal of Communication Systems*, 25(9):1189–1212, 2012.

[14] Ana Paula R da Silva, Marcelo HT Martins, Bruno PS Rocha, Antonio AF Loureiro, Linnyer B Ruiz, and Hao Chi Wong. Decentralized intrusion detection in wireless sensor networks. In *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, pages 16–23. ACM, 2005.

[15] Andreas A Strikos. A full approach for intrusion detection in wireless sensor networks. *School of Information and Communication Technology*, 2007.

[16] Pedro Garcia-Teodoro, J Diaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. Anomaly-based network intrusion detection: Techniques, systems and challenges. *computers & security*, 28(1-2):18–28, 2009.

[17] Md Safiqul Islam and Syed Ashiqur Rahman. Anomaly intrusion detection system in wireless sensor networks: security threats and existing approaches. *International Journal of Advanced Science and Technology*, 36(1):1–8, 2011.

[18] Yanbing Liu and Qin Wu. A lightweight anomaly mining algorithm in the internet of things. In *Software Engineering and Service Science (ICSESS), 2014 5th IEEE International Conference on*, pages 1142–1145. IEEE, 2014.

[19] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A Spirito, and Mark Vinkovits. Denial-of-service detection in 6lowpan based internet of things. In *2013 IEEE 9th international conference on wireless and mobile computing, net-*

working and communications (WiMob), pages 600–607. IEEE, 2013.

[20] Jianwei Ding, Yingbo Liu, Li Zhang, and Jianmin Wang. Lcad: A correlation based abnormal pattern detection approach for large amount of monitor data. In *Asia-Pacific Web Conference*, pages 550–558. Springer, 2014.

[21] Lijun Yang, Chao Ding, Meng Wu, and Kun Wang. Robust detection of false data injection attacks for data aggregation in an internet of things-based environmental surveillance. *Computer Networks*, 129:410–428, 2017.

[22] Lingjuan Lyu, Jiong Jin, Sutharshan Rajasegarar, Xuanli He, and Marimuthu Palaniswami. Fog-empowered anomaly detection in iot using hyperellipsoidal clustering. *IEEE Internet of Things Journal*, 4(5):1174–1184, 2017.

[23] Sergey Ageev, Yan Kopchak, Igor Kotenko, and Igor Saenko. Abnormal traffic detection in networks of the internet of things based on fuzzy logical inference. In *Soft Computing and Measurements (SCM), 2015 XVIII International Conference on*, pages 5–8. IEEE, 2015.

[24] Zhenguo Chen, Liqin Tian, and Chuang Lin. A method for detection of anomaly node in iot. In *International Conference on Algorithms and Architectures for Parallel Processing*, pages 777–784. Springer, 2015.

[25] Vladimir Eliseev and Anastasiya Gurina. Algorithms for network server anomaly behavior detection without traffic content inspection. In *Proceedings of the 9th International Conference on Security of Information and Networks*, pages 67–71. ACM, 2016.

[26] Rajesh Kumar Gunupudi, Mangathayaru Nimmala, Narsimha Gugulothu, and Suresh Reddy Gali. Clapp: A self constructing feature clustering approach for anomaly detection. *Future Generation Computer Systems*, 74:417–429, 2017.

[27] Jesus Pacheco and Salim Hariri. Anomaly behavior analysis for iot sensors. *Transactions on Emerging Telecommunications Technologies*, 29(4):e3188, 2018.

[28] Aras Can Onal, Omer Berat Sezer, Murat Ozbayoglu, and Erdogan Dogdu. Weather data analysis and sensor fault detection using an extended iot framework with semantics, big data, and machine learning. In *Big Data (Big Data), 2017 IEEE International Conference on*, pages 2037–2046. IEEE, 2017.

[29] Nanda Kumar Thanigaivelan, Ethiopia Nigussie, Rajeev Kumar Kanth, Seppo Virtanen, and Jouni Isoaho. Distributed internal anomaly detection system for internet-of-things. In *Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual*, pages 319–320. IEEE, 2016.

[30] Anthéa Mayzaud, Anuj Sehgal, Rémi Badonnel, Isabelle Chrisment, and Jürgen Schönwälder. Using the rpl protocol for supporting passive monitoring in the internet of things. In *Network Operations and Management Symposium (NOMS), 2016 IEEE/IFIP*, pages 366–374. IEEE, 2016.

[31] Douglas H Summerville, Kenneth M Zach, and Yu Chen. Ultra-lightweight deep packet anomaly detection for internet of things devices. In *Computing and Communications Conference (IPCCC), 2015 IEEE 34th International Performance*, pages 1–8. IEEE, 2015.

[32] Junping Wang, Qiuming Kuang, and Shihui Duan. A new online anomaly learning and detection for large-scale service of internet of thing. *Personal and Ubiquitous Computing*, 19(7):1021–1031, 2015.

[33] Junping Wang and Shihui Duan. An online anomaly learning and forecasting model for large-scale service of internet of things. In *Identification, Information and Knowledge in the Internet of Things (IIKI), 2014 International Conference on*, pages 152–157. IEEE, 2014.

[34] Shahid Raza. *Lightweight security solutions for the internet of things*. PhD thesis, Mälardalen University, Västerås, Sweden, 2013.

[35] Shahid Raza, Linus Wallgren, and Thiemo Voigt. Svelte: Real-time intrusion detection in the internet of things. *Ad hoc networks*, 11(8):2661–2674, 2013.

[36] Rongrong Fu, Kangfeng Zheng, Dongmei Zhang, and Yixian Yang. An intrusion detection scheme based on anomaly mining in internet of things. 2011.

[37] VA Desnitsky, IV Kotenko, and SB Nogin. Detection of anomalies in data for monitoring of security components in the internet of things. In *Soft Computing and Measurements (SCM), 2015 XVIII International Conference on*, pages 189–192. IEEE, 2015.

[38] Pavan Pongle and Gurunath Chavan. Real time intrusion and wormhole attack detection in internet of things. *International Journal of Computer Applications*, 121(9), 2015.

[39] Niki Tsitsiroudi, Panagiotis Sarigiannidis, Eirini Karapistoli, and Anastasios A Economides. Eyesim: A mobile application for visual-assisted wormhole attack detection in iot-enabled wsns. In *Wireless and Mobile Networking Conference (WMNC), 2016 9th IFIP*, pages 103–109. IEEE, 2016.

[40] M Surendar and A Umamakeswari. Indres: An intrusion detection and response system for internet of things with 6lowpan. In *Wireless Communications, Signal Processing and Networking*

(WiSPNET), International Conference on, pages 1903–1908. IEEE, 2016.

[41] Panagiotis Sarigiannidis, Eirini Karapistoli, and Anastasios A Economides. Visiot: A threat visualisation tool for iot systems security. In *Communication Workshop (ICCW), 2015 IEEE International Conference on*, pages 2633–2638. IEEE, 2015.

[42] Hamid Bostani and Mansour Sheikhan. Hybrid of anomaly-based and specification-based ids for internet of things using unsupervised opf based on mapreduce approach. *Computer Communications*, 98:52–71, 2017.

[43] Mansour Sheikhan and Hamid Bostani. A hybrid intrusion detection architecture for internet of things. In *Telecommunications (IST), 2016 8th International Symposium on*, pages 601–606. IEEE, 2016.

[44] Syed Obaid Amin, Muhammad Shoaib Siddiqui, Choong Seon Hong, and Sungwon Lee. Rides: Robust intrusion detection system for ip-based ubiquitous sensor networks. *Sensors*, 9(5):3447–3468, 2009.

[45] Sergi Trilles Oliver, Óscar Belmonte Fernández, Sven Schade, and Joaquín Huerta Guijarro. A domain-independent methodology to analyze iot data streams in real-time. a proof of concept implementation for anomaly detection from environmental data. 2016.

[46] Pheeha Machaka, Andre McDonald, Fulufhelo Nelwamondo, and Antoine Bagula. Using the cumulative sum algorithm against distributed denial of service attacks in internet of things. In *International Conference on Context-Aware Systems and Applications*, pages 62–72. Springer, 2015.

[47] Masud Moshtaghi, Sarah M Erfani, Christopher Leckie, and James C Bezdek. Exponentially weighted ellipsoidal model for anomaly detection. *International Journal of Intelligent Systems*, 32(9):881–899, 2017.

[48] Tianqi Yu, Xianbin Wang, and Abdallah Shami. Recursive principal component analysis-based data outlier detection and sensor data aggregation in iot systems. *IEEE Internet of Things Journal*, 4(6):2207–2216, 2017.

[49] Dang Hai Hoang and Ha Duong Nguyen. A pca-based method for iot network traffic anomaly detection. In *Advanced Communication Technology (ICACT), 2018 20th International Conference on*, pages 381–386. IEEE, 2018.

[50] Shengchu Zhao, Wei Li, Tanveer Zia, and Albert Y Zomaya. A dimension reduction model and classifier for anomaly-based intrusion detection in internet of things. In *Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence & Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2017 IEEE 15th Intl*, pages 836–843. IEEE, 2017.

[51] Zibin Zheng, J Wang, and Ziyu Zhu. A general anomaly detection framework for internet of things. In *Proc. 41st IEEE/IFIP International Conference on Dependable Systems and Networks, Hong Kong*, 2011.

[52] Alistair Shilton, Sutharshan Rajasegarar, Christopher Leckie, and Marimuthu Palaniswami. Dp1svm: A dynamic planar one-class support vector machine for internet of things environment. In *Recent Advances in Internet of Things (RIoT), 2015 International Conference on*, pages 1–6. IEEE, 2015.

[53] Dimitrios Zissis. Intelligent security on the edge of the cloud. In *Engineering, Technology and Innovation (ICE/ITMC), 2017 International Conference on*, pages 1066–1070. IEEE, 2017.

[54] Christopher D McDermott and Andrei Petrovski. Investigation of computational intelligence techniques for intrusion detection in wireless sensor networks. 2017.

[55] Raj Jain and Hitesh Shah. An anomaly detection in smart cities modeled as wireless sensor network. In *Signal and Information Processing (IConSIP), International Conference on*, pages 1–5. IEEE, 2016.

[56] Hichem Sedjelmaci, Sidi Mohammed Senouci, and Mohamad Al-Bahri. A lightweight anomaly detection technique for low-resource iot devices: A game-theoretic methodology. In *Communications (ICC), 2016 IEEE International Conference on*, pages 1–6. IEEE, 2016.

[57] Vrizlynn LL Thing. Ieee 802.11 network anomaly detection and attack classification: A deep learning approach. In *Wireless Communications and Networking Conference (WCNC), 2017 IEEE*, pages 1–6. IEEE, 2017.

[58] Jorge Granjal and Artur Pedroso. An intrusion detection and prevention framework for internet-integrated coap wsn. *Security and Communication Networks*, 2018, 2018.

[59] Menachem Domb, Elisheva Bonchek-Dokow, and Guy Leshem. Lightweight adaptive random-forest for iot rule generation and execution. *Journal of Information Security and Applications*, 34:218–224, 2017.

[60] Bayu Adhi Tama and Kyung-Hyune Rhee. An integration of pso-based feature selection and random forest for anomaly detection in iot network. In *MATEC Web of Conferences*, volume 159, page 02021. EDP Sciences, 2018.

[61] Hichem Sedjelmaci, Sidi Mohamed Senouci, and

Tarik Taleb. An accurate security game for low-resource iot devices. *IEEE Transactions on Vehicular Technology*, 66(10):9381–9393, 2017.

[62] Ismail Butun, Burak Kantarci, and Melike Erol-Kantarci. Anomaly detection and privacy preservation in cloud-centric internet of things. In *Communication Workshop (ICCW), 2015 IEEE International Conference on*, pages 2610–2615. IEEE, 2015.

[63] Mee Lan Han, Jin Lee, Ah Reum Kang, Sungwook Kang, Jung Kyu Park, and Huy Kang Kim. A statistical-based anomaly detection method for connected cars in internet of things environment. In *International Conference on Internet of Vehicles*, pages 89–97. Springer, 2015.

[64] Sokratis Kartakis, Weiren Yu, Reza Akhavan, and Julie A McCann. Adaptive edge analytics for distributed networked control of water systems. In *Internet-of-Things Design and Implementation (IoTDI), 2016 IEEE First International Conference on*, pages 72–82. IEEE, 2016.

[65] Douglas L Goodman, James Hofmeister, and Robert Wagoner. Advanced diagnostics and anomaly detection for railroad safety applications: using a wireless, iot-enabled measurement system. In *IEEE AUTOTESTCON, 2015*, pages 273–279. IEEE, 2015.

[66] Li Da Xu, Wu He, and Shancang Li. Internet of things in industries: A survey. *IEEE Transactions on industrial informatics*, 10(4):2233–2243, 2014.

[67] Praveen Vijai and P Bagavathi Sivakumar. Design of iot systems and analytics in the context of smart city initiatives in india. *Procedia Computer Science*, 92:583–588, 2016.

[68] Chih-Wei Ho, Chun-Ting Chou, Yu-Chun Chien, and Chia-Fu Lee. Unsupervised anomaly detection using light switches for smart nursing homes. In *Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2016 IEEE 14th Intl C*, pages 803–810. IEEE, 2016.

[69] Arijit Ukil, Soma Bandyoapdhyay, Chetanya Puri, and Arpan Pal. Iot healthcare analytics: The importance of anomaly detection. In *Advanced Information Networking and Applications (AINA), 2016 IEEE 30th International Conference on*, pages 994–997. IEEE, 2016.

[70] Cai Ming Liu, Si Yu Chen, Yan Zhang, Run Chen, and Kui Liang Guo. An iot anomaly detection model based on artificial immunity. In *Advanced Materials Research*, volume 424, pages 625–628. Trans Tech Publ, 2012.

[71] Julie Greensmith. Securing the internet of things with responsive artificial immune systems. In *Proceedings of the 2015 Annual Conference on Genetic and Evolutionary Computation*, pages 113–120. ACM, 2015.

[72] Briana Arrington, LiEsa Barnett, Rahmira Rufus, and Albert Esterline. Behavioral modeling intrusion detection system (bmids) using internet of things (iot) behavior-based anomaly detection via immunity-inspired algorithms. In *Computer Communication and Networks (ICCCN), 2016 25th International Conference on*, pages 1–6. IEEE, 2016.

[73] Sergio Trilles, Òscar Belmonte, Sven Schade, and Joaquìn Huerta. A domain-independent methodology to analyze iot data streams in real-time. a proof of concept implementation for anomaly detection from environmental data. *International Journal of Digital Earth*, 10(1):103–120, 2017.

Morteza Behniafar is a Ph.D. candidate at Malek Ashtar University of Technology, Tehran, Iran. He received his B.S. and M.S. degrees in computer engineering from Isfahan University, Isfahan, Iran. His research interests include information security, intrusion detection systems, anomaly detection, trust and reputation models.

Alireza Norouzi is a freelance consultant advising government and private sector-related industries on information technology. He had four years experience as an academic staff and an IT post doctoral position in Sharif University of Technology. He is a specialist in artificial intelligence, cognitive science, software engineering, and IT security, and is co-founder of four IT startups.

Hamid Reza Shahriari is currently an assistant professor in the Department of Computer Engineering and Information Technology at Amirkabir University of Technology. He received his Ph.D. in computer engineering from Sharif University of Technology in 2007. His research interests include information security, especially data privacy, software vulnerability analysis, security in E-commerce, trust and reputation models, and database security.