Hindawi
Security and Communication Networks
Volume 2019, Article ID 4301409, 19 pages
https://doi.org/10.1155/2019/4301409

Review Article

Recent Advancements in Intrusion Detection Systems for the Internet of Things

Zeeshan Ali Khan [1] **and Peter Herrmann** [2]

[1] *School of Electrical Engineering, Minhaj University, Lahore, Pakistan*
[2] *Department of Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU), Trondheim, Norway*

Correspondence should be addressed to Peter Herrmann; herrmann@ntnu.no

Received 31 January 2019; Revised 20 May 2019; Accepted 29 May 2019; Published 3 July 2019

Guest Editor: Jose M. Alcaraz-Calero

Many Internet of Things (IoT) systems run on tiny connected devices that have to deal with severe processor and energy restrictions. Often, the limited processing resources do not allow the use of standard security mechanisms on the nodes, making IoT applications quite vulnerable to different types of attacks. This holds particularly for intrusion detection systems (IDS) that are usually too resource-heavy to be handled by small IoT devices. Thus, many IoT systems are not sufficiently protected against typical network attacks like Denial-of-Service (DoS) and routing attacks. On the other side, IDSs have already been successfully used in adjacent network types like Mobile Ad hoc Networks (MANET), Wireless Sensor Networks (WSN), and Cyber-Physical Systems (CPS) which, in part, face limitations similar to those of IoT applications. Moreover, there is research work ongoing that promises IDSs that may better fit to the limitations of IoT devices. In this article, we will give an overview about IDSs suited for IoT networks. Besides looking on approaches developed particularly for IoT, we introduce also work for the three similar network types mentioned above and discuss if they are also suitable for IoT systems. In addition, we present some suggestions for future research work that could be useful to make IoT networks more secure.

1. Introduction

The Internet of Things (IoT) is an emerging technology used in various fields of application like healthcare, transport, and smart grid. IoT (to improve the readability, we list in Table 1 the abbreviations used in our article) applications often make a difference since they comprise very small devices that can, e.g., be worn on the skin or attached to domestic appliances. The tininess of the devices and the fact that, to be mobile, they often have to rely on light batteries, however, limit their processing capabilities and restrict their energy supply. This makes traditional security mechanisms too heavy-weight to be efficiently applied on such systems. In consequence, the devices are used without sufficient protection such that they can either be attacked directly or utilized by attackers to launch attacks on third parties. For instance, multiple IoT devices were used to start a distributed Denial-of-Service (DDoS) attack on an American Internet services company that made it impossible for many customers to access certain Internet services; see Nordrum [1]. Cases like this reveal that there is an urgent need to build secure solutions that are suitable for IoT devices. In general, security of IoT networks is a relatively new research area that, however, can profit from related research carried out for similar networks like Mobile Ad hoc Networks (MANET), Wireless Sensor Networks (WSN), and Cyber-Physical Systems (CPS). At least some of the findings in these areas seem to be promising also for the development of protection mechanisms for IoT networks.

Intrusion Detection Systems (IDSs) are an important countermeasure against many types of network attacks. Most existing IDSs, however, require a significant amount of resources aggravating their usability on small IoT devices. Thus, there is a demand for special IDS solutions that are lightweight but, nevertheless, give a high degree of protection.

In this paper, we give a survey of existing IDS approaches that are suited for IoT networks. Since only relatively few IDSs

Table 1: List of abbreviations.

AI	Artificial Intelligence
AODV	Ad-hoc On-demand Distance Vector
API	Application Programming Interface
BS	Base Station
CH	Cluster Head
CPS	Cyber Physical System
DDoS	Distributed Denial of Service
DoS	Denial of Service
FSM	Finite State Machine
GPS	Global Positioning System
IDS	Intrusion Detection System
IMS	Intrusion Mitigation System
IoT	Internet of Things
IPS	Intrusion Prevention System
MANET	Mobile Ad-hoc Network
RPL	Routing Protocol for Low power and Lossy networks
SVM	Support Vector Machine
WSN	Wireless Sensor Networks

for IoT systems have, yet, been developed, we further extend our overview on IDSs proposed for WSNs, MANETs, and CPSs that have properties similar to IoT applications.

The article is structured as follows. First, we sketch some relevant aspects of security issues for IoT networks in Section 2. Thereafter, in Section 3 we give an introduction to IDSs including a scheme to characterize their properties that was developed by Anantvalee and Wu [2]. These characteristics can then be used to distinguish the presented IDS approaches and evaluate if they are appropriate for IoT networks. This is discussed in Section 4. Thereafter, we introduce IDS approaches for WSNs, MANETs, and CPSs in Section 5 and discuss whether and how the solutions for these akin network types can be adapted to IoT systems. This is followed by the introduction of the IDS approaches particularly developed for IoT networks in Section 6. Finally, we present two suggestions for interesting research areas in Section 7 followed by a conclusion.

This article is significantly different to others already published:

(i) Butun et al. [3] consider various types of IDSs that are implemented for WSNs. They, however, do not discuss the eligibility of these methods for IoT networks.

(ii) Granjal et al. [4] present a survey article that discusses IoT security issues in general, but does not focus on the development of IDSs.

(iii) Gendreau and Moorman [5] discuss IDSs for IoT networks but more with the focus on properties, these systems should have, and less a survey.

(iv) Benkhelifa et al. [6] discuss the advancements in intrusion detection systems for the IoT. However, they do not write about intrusion detection solutions for WSNs, MANETs, and CPSs that have the potential to be also implemented for IoT networks. Likewise, in contrast to this paper, they do not discuss implementation issues for the IoT networks.

(v) Ammar et al. [7] published another article related to IoT security. Yet, it is significantly different from ours as it only explains the security of IoT frameworks with regard to their internal architecture.

(vi) Restuccia et al. [8] provide a survey on IoT security research by considering the application of machine learning and software-defined networking only. Therefore, it is significantly different from our survey article, as we consider a lot more techniques that are suitable for IoT networks.

(vii) Ud Din et al. [9] only discuss a survey on trust management techniques for the IoT networks, without considering the advancements in other fields of IoT security. Further, the authors refrain from discussing the challenges faced in deploying IDSs on real platforms. Moreover, the article does not take advantage of considering work done in akin network types.

2. IoT Security

As mentioned above, important properties of IoT systems are the limited processing and energy resources of their nodes. That is based on the fact that many IoT devices shall be directly worn by people. This holds particularly for IoT systems used in healthcare and ambient assisted living that are seen as major fields of application for the technology. In consequence, it is often difficult to use well-known protection technology to safeguard IoT devices. For instance, encryption tends to be processing-intensive making it difficult to encrypt and sign data to be transmitted via an IoT network. Thus, encryption is often omitted making the wireless communication vulnerable against attacks; see Ngu et al. [10].

Another characteristic of these systems is their openness and flexibility. The devices are often placed in physically unsecured areas such that they can be easily accessed by attackers. Moreover, they use decentralized wireless communication making it easy to connect with them from the outside. In addition, many IoT applications need to be highly flexible in accepting new devices for further temporary or permanent usage. All this makes it relatively simple for attackers to add malicious behavior to the system. As discussed in Roosta et al. [11], utilizing these vulnerabilities, various kinds of physical tampering as well as network attacks can be launched. While some attacks compromise only few IoT nodes, others can be massive and bring down whole networks.

Further, due to the required flexibility and the heterogeneous nature of the devices, it is often challenging to develop correctly working, robust, and secure solutions. For example, the heterogeneity of the devices makes it difficult to embed them on well-understood infrastructures such that important functions like network access, routing, or encryption have to be built up from scratch. In addition, the developer of an IoT network has also to consider the

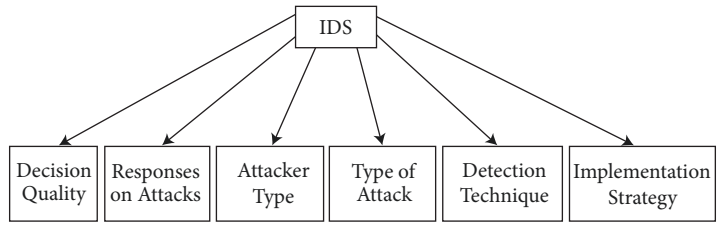

Figure 1: Classification of IDSs, taken in modified form from Anantvalee and Wu [2].

varying physical infrastructure. For instance, a patient may be riding in a car or train operating in a tunnel or in remote areas without cellular network access; see Balandina et al. [12]. Therefore, bandwidth and throughput of such networks need to be carefully utilized without draining the scarce battery resources of a device by too many transmissions. In spite of these limitations, IoT systems in healthcare have to be extremely robust and secure to avoid medical malpractice of their users. All these factors must be considered while designing, engineering, and deploying an IoT network. For all these reasons, IoT devices are subject to various kinds of malicious attacks.

Typical attacks based on physical access are the replacement of nodes or their batteries as well as the reprogramming of nodes; see Mohammadi and Jadidoleslamy [13]. With respect to network attacks, we can distinguish between active and passive attacks; see Khan and Loo [14]. Passive attacks only extract the vital information from the network without harming its integrity. In contrast, active attacks assail the communication of network nodes by tempering, dropping or misdirecting the data packets. An active attack can easily influence a large number of IoT devices since a network often consists of peripherally deployed units that cooperate with each other based on multihop communication. A well-known example is Denial-of-Service (DoS) attacks that try to disable the nodes from providing their tasks. Another active type of attack is radio jamming in which the communication is spoiled by the introduction of noise or faulty packets. A type of attack special to IoT systems with weak devices is battery exhaustion attacks. For instance, a device is kept busy by leading it to send or receive data unnecessarily in order to drain its battery power faster. Alternatively, one can attack the network layer that is responsible for sending the packet towards its destination using an appropriate route; see Popescu et al. [15]. In most IoT devices, the protocol mechanisms of the network layer are not protected such that software changes causing packet dropping and the misdirection of packets are possible.

The typical countermeasure against all these types of attack is intrusion detection systems (IDSs) that are introduced in the following.

3. Intrusion Detection Systems (IDSs)

The IDS is a well-known technique to protect networks against attacks as those named above. It is often seen as a solution for the second line of defense when attacks cannot be detected by other security mechanisms like encryption or access control; see Djenouri et al. [16]. The task of an IDS is to detect unusual activities that potentially indicate ongoing attacks.

To rate the IDSs presented in this paper, we use, in adapted form, the classification scheme from Anantvalee and Wu [2] that is depicted in Figure 1. Thus, we consider the six criteria *decision quality*, *Responses on Attacks*, *Attacker Type*, *Type of Attack*, *Detection Technique*, and *implementation strategy*. The first five are discussed in the following subsections. Since the selected implementation strategy of an IDS is very important for its usability for IoT networks, we look more in-depth on this criterion. This is done in Section 4.

3.1. Decision Quality. Important for the quality of an IDS is, of course, whether it detects all occurring attacks. Moreover, the IDS should report only actual attacks but not behavior that is benevolent but was misinterpreted as an attack. Particularly, the ratio between alerts given by an IDS and the actual appearance of attacks is relevant to evaluate the decision quality. In this context, the following terms are used; see Patcha and Park [17]:

(i) True positive: an attack is happening in the system which is correctly detected and alerted by the IDS.

(ii) True negative: no attack is happening in the system, and the IDS correctly considers the behavior as normal.

(iii) False positive: no attack is happening in the system, but the IDS misinterprets the behavior as an attack and gives a false alert.

(iv) False negative: an attack is happening in the system which, however, is not detected by the IDS such that no alert about the attack is given.

According to Zhang et al. [18], an IDS should have a "*low false positive rate, calculated as the percentage of normalcy variations detected as anomalies, and high true positive rate, calculated as the percentage of anomalies detected.*" Thus, it should have a minimum number of false positives and negatives. Moreover, an IDS should have low overhead and not degrade the system performance which is particularly relevant for the use in IoT networks. Further, it should not add new vulnerabilities.

3.2. Responses on Attacks. In its pure form, an IDS is not intended to antagonize attacks by itself but it shall only alert the network operators about ongoing attacks such that these

can decide about taking precautions and countermeasures. An IDS comprises three main components:

(i) Monitoring module: used to constantly monitor the network traffic and/or events happening at certain network nodes.

(ii) Detection module: tries to detect a malicious attack based on the monitored data.

(iii) Alarm module: raises an alarm if an intrusion activity has been detected.

Most systems used in practice are such IDSs without autonomous correction capabilities but two variants that can intervene themselves exist as well; see Fuchsberger [19]:

(i) An Intrusion Prevention System (IPS) automatically takes countermeasures after detecting an attack guaranteeing a timely reaction. On the other side, an IPS also reacts on false positives which can make the network unstable. These wrong reactions can be vulnerability in itself since sometimes false positives can be deliberately created by attackers who want to utilize the wrong countermeasures.

(ii) An Intruder Mitigation System (IMS) quarantines nodes that were detected as sources of malicious network attacks. As measures typically taken by an IMS, Butun et al. [3] name the generation of audit records to gain evidence, the information of network nodes about presumed attackers by revealing its location and identity, and the initiation of a mitigation process quarantining the attacker. Also this type is subject to false positives which might lead to wrong expulsions of correct working nodes.

The absence of reacting automatically on false positives is the main reason that pure IDSs are much more often used in practice than IPSs and IMSs. Indeed, all approaches, discussed in this article, are IDSs without the ability to correct autonomously.

3.3. Attacker Type. Like other network types, an IoT system can be threatened by both, attackers controlling one or more network nodes and those from the environment that do not have control over network devices. Thus, we define the following attacker types:

(i) External attacker: a node outside the network that connects to network nodes in order to launch a malicious attack.

(ii) Internal attacker: a node within the network that is compromised and tries to launch attacks on other nodes of the network.

One can distinguish whether an IDS is suited to detect attacks launched from only external attackers, internal ones, or both types.

3.4. Type of Attack. There are several kinds of attacks to be used against networks. With respect to the special properties of IoT networks, we see the following types of attack:

(i) Selective forwarding (see Karlof and Wagner [20]; Wallgren et al. [21]): due to the weakness of IoT devices, the strengths of their transmitters are often limited. Therefore, not all packets can be sent to their destination in a single hop but intermediate nodes have to be used to relay messages. By compromising an intermediate node, an attacker can block the forwarding of certain packets such that only those benefitting the attacker are forwarded.

(ii) Sinkhole/black hole/packet dropping (see Karlof and Wagner [20]; Wallgren et al. [21]): often, IoT networks organize themselves impromptu using special protocols like the *Routing Protocol for Low power and Lossy networks* (RPL) (see IETF [22]). In such protocols, a node often prefers neighbors that guarantee a short number of hops to the destination. By falsely claiming a shorter number of hops than it can provide in reality, a malicious node can attract a lot of traffic from its neighbors such that other attacks like selective forwarding have a greater impact.

(iii) Node selfishness (see Michiardi and Molva [23]): to conserve its limited resources, a node may falsely claim a higher number of hops to the destination such that it has to forward less packets. This selfish behavior strains the battery of neighboring nodes and degrades the overall network performance.

(iv) Version number (see Mayzaud et al. [24]): this type of attack is also relevant for ad hoc networks. If, due to changes in the topology or congestions, the routing structure of a network needs to be changed, in protocols like RPL, a new version number is assigned triggering a full rebuild of the network. Rebuilding, however, demands to exchange a relatively large number of packets such that the energy resources of the nodes are strained. In consequence, by initiating many rebuilds, a malicious node may attack the batteries of weaker nodes. Moreover, during the rebuilding process, the network tends to be unstable since data transfer in both versions is active at the same time which may lead to erroneous behavior like loops in the routing. These vulnerabilities can be used for other attacks.

(v) Resource depletion/battery exhaustion (see Onat and Miri [25]; Boubiche and Bilami [26]): as already mentioned, avoiding the straining of battery power is an important property of wireless devices. In this type of attack, the attacker explicitly tries to deplete these resources of the network by using multiple techniques. This may include the generation of high volumes of unnecessary data injected into the network.

The types of attack introduced above are particular to IoT networks with resource-constrained nodes. In addition, these systems are also subject to more standard types of network attacks that have to be addressed by IDSs, too. In the following, we name those more general attack types:

(i) Denial-of-Service (DoS) (see Abraham et al. [27]; Albers et al. [28]): an attacker may overwhelm the nodes of a network with duties such that they cannot provide their intended tasks anymore. While DoS attacks are critical for all network types, they are particularly problematic for IoT devices since they are often also Resource Depletion attacks.

(ii) Distributed Denial-of-Service (DDoS) (see Shamshirband et al. [29]): this is a variant of DoS in which an attack is carried out in a coordinated manner by a team of attackers. In this way, even larger damage can be done to the network and its nodes.

(iii) Jamming (see Bao et al. [30]; Sajjad et al. [31]): this is also a variant of a DoS attack. The attacker spoils the communication within a wireless network by intentionally transmitting interferences on the used communication band. Thus, the nodes in the network cannot cooperate anymore.

(iv) Unauthorized access (see Abraham et al. [27, 32]): this type of attack refers to gaining access to resources without permission.

(v) Remote-to-Local (see Tsang and Kwong [33]): this variant of unauthorized access attacks may happen if an attacker has the ability to send packets to a network from the outside, but does not have direct access to any of the network nodes. In this case, the attacker may utilize possible vulnerabilities to achieve unauthorized access to the system.

(vi) User-to-Root (see Tsang and Kwong [33]): this is also a kind of unauthorized access attack. The attacker has only access to a normal user account but utilizes vulnerabilities in the network to get also root access on the system.

(vii) Probing (see Tsang and Kwong [33]; Abraham et al. [32]): Attackers launch a collaborative attack by probing a node. This might give useful information helping to break its defense mechanisms.

(viii) Spoofing (see Boubiche and Bilami [26]; Chen et al. [34]): here, packets with a false source IP address are used to hide the identity of an attacker.

(ix) Packet repetition (see Da Silva et al. [35]): attackers construct fake packets which appear as if they are part of the normal communication. Amongst others, this will lead to an increase in network load and performance degradation.

(x) Packet delay (see Da Silva et al. [35]): valid data transmissions are maliciously delayed but, in contrast to selective forwarding attacks, not removed. Thus, the attack leads to delayed data delivery and, in consequence, to network performance degradation.

(xi) Wormhole (see Maleh et al. [36]; Da Silva et al. [35]): the attacker uses two or more malicious nodes which are linked by a nonlegitimate connection, a so-called tunnel, faking a route that is shorter than the original one within the network. Packets passing the tunnel can then be used for other kinds of attack.

(xii) Packet alteration/bad data injection (see Da Silva et al. [35]): these attacks try to alter the contents of a packet to inject malicious data into the network nodes.

(xiii) Periodic route error (see Eik Loo et al. [37]): here, a compromised node broadcasts special route error messages to neighboring nodes. These messages say that the route to the border router is down at the moment and there is a need to search a new path. This will lead to network performance degradation.

(xiv) Hello flooding, (see Maleh et al. [36]): most protocols supporting the dynamical adding of nodes to a network use *hello* messages to indicate that a node wants to join. An attacker with a strong transmitter unit may constantly transmit such hello packets to a large number of neighboring nodes. This may confuse the receiving nodes, reduce their performance, and decrease the overall network performance.

(xv) Routing misdirection and disruption (see Zhang et al. [18]): these attacks are launched by router nodes that forward traffic along wrong paths. As a consequence, the data transmission is delayed.

(xvi) Node capture (see Mitchell and Chen [38, 39]): a node is maliciously captured in order to help in launching other attacks in the network.

(xvii) Eavesdropping (see Shin et al. [40]): this attack is an unauthorized interception of data that may lead to the extraction of useful information.

Another group of attacks can apply to trust management systems that are used to rate the behavior of nodes in a network. A trust management system provides a computer system with mechanisms reflecting the natural trust and reputation gaining process of humans; see, e.g., Khare and Rifkin [41]. In particular, it allows us to describe the trust in an entity by a special trust value; see Jøsang [42]. Using certain metrics, these trust values are computed from the numbers of positive and negative experiences the system has with a trustee. Moreover, the trust values of several trusters in the same trustee can be aggregated such that one can rate the general reputation of this trustee. In IoT networks, one can build reputations of nodes depending on observations of their behavior by neighboring nodes. If a node proves to be distrustful, it can be quarantined; see Khan and Herrmann [43]. Further, one can use the reputation of a node for routing decisions. Trust management systems, however, are themselves vulnerable to certain attacks:

(i) Self-promotion (see Chen et al. [44]): a node can promote itself by either providing good recommendations for itself or inciting other nodes to do so. Thus, like with sinkhole attacks, it can gain more traffic that it may misuse to carry out selective forwarding attacks.

(ii) Bad-mouthing (see Chen et al. [44]): an attacker can issue baseless, bad trust evaluations about benevolent nodes reducing the traffic through them.

(iii) Sybil (see Karuppiah et al. [45]; Mitchell and Chen [46]): a malicious node creates a large number of

pseudonymous entities that all can rate other parties. Thus, the attacking node influences the reputation of other nodes disproportionately. This attack type can be utilized to target at routing, data storage, and fair resource allocation in the network.

(iv) Ballot stuffing (see Chen et al. [44]): this is a type of attack complementary to self-promotion attacks. Several malicious nodes can form an alliance, and each node provides positive trust recommendations about its allies increasing their reputation values. Promoting other bad nodes will eventually lead to higher traffic through them that can be misused, e.g., for selective forwarding or sinkhole attacks.

3.5. Detection Techniques. IDSs use signatures, anomalies, and hybrids between both of them as the main techniques to detect attacks. These three techniques will be introduced in the following.

3.5.1. Signature-Based IDSs. Systems following this strategy are also known as rule-based IDSs. A signature refers to system and network behavior that typically occurs when attacks of a certain kind are launched. A signature-based IDS keeps databases of these signatures and constantly checks the actual network behavior for compliance with them. If the observed behavior fits with one or more signatures, the IDS raises an alarm. Signature-based IDSs have often excellent false positive rates but are not able to detect novel types of attack for which they do not have signatures ready. Therefore, they tend to be subject to a large number of false negatives.

In order to implement this technique, profiles of known attacks are generated from which the signatures are formed. An example of a signature could be: "If there are 10 or more unsuccessful tries to login within 2 minutes, a brute force unauthorized access attack is on its way". Da Silva et al. [35] define a number of rules that are typical for signatures:

(i) Interval rule: the time difference between two consecutive packet arrivals is considered.

(ii) Retransmission rule: this rule measures the rate of correctly retransmitted transit messages by intermediate nodes.

(iii) Integrity rule: it is checked if a message is changed on its way towards the destination node.

(iv) Delay rule: this rule takes the time an intermediate node needs between receiving and further transmitting a message into account.

(v) Repetition rule: the number of retransmissions of a certain message by a node is checked.

(vi) Radio transmission range: in order to find newly deployed unauthorized nodes, the IDS tests if all messages are originated by known stations within a certain radio transmission range.

(vii) Jamming rule: the number of collisions faced by a node is counted. It should not exceed a certain threshold.

To detect also version number attacks one can add the following rule type:

(i) Version number check: if the version number of an ad hoc network changes, it is checked which node has initiated this amendment that leads to a reconfiguration of a network. Only certain nodes have the permission to trigger adaptations of the version.

3.5.2. Anomaly-Based IDSs. These IDSs use a set of rules to detect anomalies in the network behavior based on heuristic techniques. Often, thresholds for certain behavioral patterns are used to define whether the activity is an intrusion or not. In this way, a system can recognize not already known attacks. On the other side, these IDSs tend to produce a relatively high rate of false positives since, e.g., a threshold can also be exceeded for other reasons that do not result from malicious attacks. In addition, it is often difficult to frame a useful heuristic such that sometimes even well-known attacks can be hardly detected.

3.5.3. Hybrid IDSs. This type of IDS combines the signature- and anomaly-based approaches. A hybrid IDS uses two modules, one that detects attacks based on signatures while the other one finds anomalies from the normal network behavior profile. A hybrid IDS has a lower number of false positives and negatives compared to the singular approaches, but requires significantly higher computational resources since both modules have to run in parallel.

4. Implementation Strategies

An IDS may reside in a single node from which the network traffic is observed or distributed over several nodes. Since IoT applications are inherently distributed, stand-alone solutions in which an IDS resides in a local node and protects just this node are a bad fit. As a centralized solution, we name an IDS that is implemented on a single node but watches also other ones and makes its decisions based on the locally observed behavior. Also this layout does not seem suited for IoT networks consisting of many nodes since the IDS is quite processor-intensive such that the node executing it would be strained. Not surprisingly, we did not find any solutions using these technologies for the network types discussed in this paper. In consequence, all implementation strategies discussed below are distributed.

Altogether, the IDSs used for WSNs, MANETs, CPSs, and IoT networks follow nine different implementation strategies listed in Table 2. These strategies are not completely orthogonal. For instance, the mentioned *voting-based IDSs* and *reputation-based IDSs* are special forms of *distributed and collaborative IDSs* that, however, use particular methods to evaluate network behavior. Also the *statistical detection-based IDSs* and *machine learning-based IDSs* are related. Garcia-Teodoro et al. [47] distinguishes three main techniques allowing an anomaly-based IDS to detect the anomalies in the system. Two are the statistical- and the machine learning-based IDSs. The third one is knowledge-based IDSs. In this type of system, the differences with respect to network data and behavior are "learned" for normal as well as for attack

Table 2: IDS implementation schemes for IoT networks.

Implementation Strategy	Energy Consumption	Processor Requirements in a Net With Powerful Nodes	Processor Requirements in a Net Without Powerful Nodes	Detection Accuracy	Implementation on Resource-constrained Nodes
Hierarchical	B†	A	C	C	A
Distributed and Collaborative	D	B	B	C	C
Voting	A	A	A	D	A
Reputation	E	A	A	C	A
Cross Layer	F	F	F	A	D
Mobile Agent	E	E	E	C	F
Game Theory	E	E	E	B	F
Statistical Detection	E	B	F	B	F
Machine Learning	E	B	F	B	F

† The cluster head has a higher energy consumption that can be rated as E.

conditions. Such an IDS can be implemented using various techniques from Artificial Intelligence (AI) including Expert Systems, Finite State Machines, or Data Clustering and Outlier Detection. Since these AI methods tend to be highly processor-intensive, this strategy seems to be unsuited for IoT networks with their vast number of small and resource-restricted devices. We did not find any knowledge-based strategies for monitoring the four network types.

Analyzing the various IDSs, we found out that the type of nodes typically used in an IoT network plays an important role for deciding about the suitability of an approach. Some IDSs will only work in networks consisting of a mix of resource limited and more powerful nodes since the latter can take the more complex and resource-constraining system tasks. Other techniques seem to work well also in a network consisting only of performance-restricted nodes. In Table 2, we give an overview about how we rate the suitability of the different implementation strategies with respect to the energy consumption, the processor requirements, the accuracy of the methods, and the possibility of implementing the IDSs on IoTs with many resource-constrained nodes. The two configuration types, i.e., IoT networks with or without powerful nodes, are separated with respect to the processor requirements. In the table, we use letters from *A* to *F* as applied for grading in schools and universities in the US and other countries. The letter *A* gives the best rating while *F* is the worst.

In the following, we introduce the nine implementation strategies to greater detail. Further, we elaborate their impact on energy and processing resources. This determines whether IDSs using a certain strategy have the potential to be a good fit for IoT networks.

4.1. Hierarchical IDSs. The network is partitioned into clusters. Here, nodes that are close to each other usually belong to the same cluster. Each cluster is assigned a leader, the so-called cluster head (CH), that monitors the member nodes and participates in network-wide analyses.

The formation of the clusters is often a highly interactive process that requires a fair amount of communication between the nodes and is therefore energy-intensive. After completing the cluster building, however, most of the coordination necessary to find signatures or anomalies is performed within the clusters. Therefore, the resources to monitor a cluster and to process the observed results tend to be manageable and will likely not exceed the processor, storage, and energy restrictions of typical IoT nodes. In addition, energy is saved due to the smaller number of messages to be exchanged. On the other side, in spite of the fact that most of the communication takes place within the clusters, a CH often has to relay data between members of its cluster and other CHs. This additional communication can strain the resources of a CH.

Altogether, using this strategy for IoT networks consisting just of energy- and processing-restricted nodes will be problematic as those acting as CHs will probably be significantly strained over time. Nevertheless, hierarchical IDSs seem to fit well for IoT systems that contain some more powerful nodes since these can then take the role of the CHs.

4.2. Distributed and Collaborative IDSs. Here, an IDS is implemented on several nodes that observe separate aspects of a system. The locally observed data are then shared between the different nodes, which make a collaborative decision whether the network behavior should be rated as malicious.

This solution is promising for IoT systems without strong devices since signatures or anomalies are detected by several collaborating nodes. Thus, the processing effort is spread over several devices such that the stress for each one is reduced. On the other side, the coordination between the nodes requires a lot of data exchange which tends to consume energy.

4.3. Voting-Based IDSs. In this variant of Distributed and Collaborative IDSs, the decision about evaluating the current behavior as an intrusion is made collaboratively based on a ballot of the distributed components.

This type of scheme is lightweight in nature and friendly for the processor and battery of a node. Thus, it seems suited for typical IoT systems. However due to its simplistic nature, the rate of false negatives, i.e., not detected attacks, can be quite large.

4.4. Reputation-Based IDSs. That is another variant of the distributed and collaborative IDSs, in which the benevolence of nodes is rated based on their previous behavior. Thus, each node has a reputation that can be modeled and calculated using trust management mechanisms as described in Section 3.4.

In general, the trust values do not need a lot of storage, and the metrics for trust value computation and aggregation consist of relatively simple calculations that are processor-friendly. This makes the approach suited for IoT devices. A problem, however, is the way nodes observe their neighbors. For that, they often have not only to listen to their own network traffic but also to those of the observed nodes. That leads to long channel listening times which may drain the battery of the unit faster. This aspect is taken up in the suggestion for future research directions discussed in Section 7.2. Another issue is the exchange of trust values to compute a general reputation but, thanks to their compactness, that is less problematic.

Like other Distributed and Collaborative IDSs, this method seems to be a good fit to IoT networks thanks to the simple computation and storage mechanisms used but the potentially significant communication effort can be an impeding factor.

4.5. Cross Layer IDSs. Each of the implementation strategies mentioned above operates on a single layer of the OSI stack and detects attacks on this layer only. In contrast, a cross layer IDS observes different layers. Critical information is exchanged between the layers, and the decision about intrusions is made based on the synthesized observations.

The advantage of this method is a good decision quality. Realizing this strategy, however, demands to process data on several layers as well as a large amount of coordination between different nodes that has to cover all observed layers. Therefore, this technique tends to require a lot of energy and computational resources. Thus, this approach seems to be less suited to IoT networks with the processor and battery restrictions of their nodes.

4.6. Mobile Agent-Based IDSs. The IDS is realized as a mobile agent that may relocate itself between the nodes of the network. In the various positions, the agent may conduct the observations necessary to decide about the presence of attacks.

This technology mainly used for MANETs reduces the communication costs between nodes. On the other side, it requires lengthy transfers of the agent code and data which will drain battery power. Moreover, there can be significant congestions between the network coordinator and the agent node. The processing power of a node is unevenly strained by this mechanism since the node only carries out IDS-related computations when it bears the agent while all other nodes cannot contribute to the intrusion detection process. This can be a problem when nodes with weak processors slow down the overall analysis process. Finally, it can be quite problematic to realize the complex agent-handling functionality on devices with limited APIs.

In consequence, this strategy does not seem to be a good fit for IoT networks with many restricted devices.

4.7. Game Theory-Based IDSs. In this strategy, an IDS is realized using mathematical models of conflict and cooperation known from game theory; see Myerson [48].

The eligibility of this method for IoT systems is hard to predict since the processor and energy load depends heavily on the games used. If one applies games that only strain few devices in the network, it may be a fit for IoT networks with some more powerful devices. A more general problem is that game theory-based systems tend to be interactive since the network administrators need to adjust the detection rate from time to time. This makes them highly personal-intensive and therefore expensive.

4.8. Statistical Detection-Based IDSs. This is one of the three strategies mentioned above, where Garcia-Teodoro et al. [47] suggest to use for anomaly-based IDSs. It comprises the generation of a stochastic profile for the traffic to be observed. Thereafter the network is monitored and the real traffic is compared with the reference profile. The IDS flags an anomaly if the behavior exceeds a certain threshold in comparison with the pattern. The statistic models can be univariate, multivariate, and time series models.

The strategy includes the handling of large amounts of data which, however, requires strong processors and good storage abilities. In addition, the statistical computation tends to be computational intensive. Since the computations are usually done centrally, statistical detection, yet, can be applied when an IoT system uses some more powerful components like a border router. This device can then keep the information, compute it based on the detection model to be used, and, if necessary, forward relevant data from time to time to the other stations.

Like the hierarchical IDSs, this strategy seems only to fit to IoT networks that include a fair number of powerful nodes.

4.9. Machine Learning-Based IDSs. This is another strategy suggested by Garcia-Teodoro et al. [47] to categorize anomaly-based IDSs. In such an IDS, a model of the analyzed patterns is generated. These models are constantly updated to increase the detection rate of the IDS. Machine learning can be realized by various techniques such as Bayesian Networks, Markov Models, Fuzzy Logic, Genetic Algorithms, Neural Networks, and Principal Component Analysis.

Since machine learning uses processing-intensive algorithms, the same issues as for statistical detection will apply and the method seems to suit only IoT networks with a fair amount of powerful nodes.

5. IDSs for WSNs, MANETs, and CPSs

As discussed in the introduction, we will not only look on IDSs particularly developed for IoT networks but also look

on those protecting adjacent network types. In this respect, we see WSNs, MANETs, and CPSs as worthwhile since they have properties that, in part, resemble those of IoT networks. These three network types can be described as follows (see also Mitchell and Chen [49]):

(i) Wireless Sensor Networks (WSNs) are used to transport data from physically dislocated sensors to a common sink. Thus, the data flows tend to be more uniform than in IoT networks in which the devices often have both sensor and actuator functionality. Further, the WSN nodes are, in general, not connected to external networks and cannot be accessed through the Internet. Moreover, they are often screwed to fixed positions and not mobile. On the other side, like IoT devices, many WSN nodes have limited energy and processing capabilities.

(ii) Mobile Ad hoc Networks (MANET) are self-configuring networks without a central control unit that have mobile member nodes. Since IoT nodes can also be mobile; e.g., if they are used in transport vehicles, their structure is close to those of MANETs. A difference is, however, that not all IoT nodes cooperate in an ad hoc style with each other but can also have a stable network topology.

(iii) Cyber-Physical Systems (CPS) are heterogeneous control systems for technical systems acting in the physical space, e.g., transport systems, industrial plants, or robots. Often, these systems face multiple interacting control loops, varying networks and hard real-time properties to fulfill. In addition, many CPSs operate in hazardous locations with extreme temperature or in the vicinity of dangerous materials. Also, various units operate in close proximity to each other such that collisions have to be avoided.

Altogether, the three mentioned networks have properties that are quite close to those of IoT systems such that the conversion of IDSs developed for them to IoT networks seems promising. However, there are some significant differences that may aggravate this conversion:

(i) Computational capacity: MANET nodes are usually more powerful units, e.g., modern personal computers with powerful processors and a large storage capability. That is very different to the often very small nodes used in IoT or WSN networks.

(ii) Power supply: the same holds for the energy supply. MANET devices are often plugged or use large batteries while those in the other network types have to rely on small batteries that can be easily drained.

(iii) Mobility: IoT, MANET, and CPS nodes are often installed on mobile units while WSN nodes tend to be fixed.

(iv) Node density: since the nodes of IoT, WSN, and CPS networks are in many cases used to sense and influence physical environments, there are typically more of them in a geographical area than MANET nodes.

(v) Communication range: due to the physical limitations of their transmitters, the communication range for IoT and WSN devices is in the range of 20 to 30 meters, while MANET nodes can transmit data up to distances of 100 meters.

(vi) Communication bandwidth: likewise, the communication bandwidth of WSN and IoT devices is less than that of MANET nodes.

(vii) Internet connectivity: the IoT network and MANET nodes are often connected via the Internet using an IPv6-enabled border router, while WSNs and CPSs are usually private networks that are not connected to the outer world.

Keeping these differences in mind, we look in the following subsections for particular IDS solutions for WSNs, MANETs, and CPSs.

5.1. WSNs. The IDSs for Wireless Sensor Networks are realized using altogether seven of the nine implementation strategies introduced in Section 4. In each of the following subsections, we list all approaches realizing a certain strategy. Further, we discuss if our expectations about the suitability of the implementation strategies for IoT networks are met by the actual IDS realizations. To keep track of the various approaches, we also sketch them together with their most relevant properties in Table 3. There, we also mark if an IDS approach seems to be suitable for being used for IoT networks.

5.1.1. Hierarchical IDSs. In Shin et al. [40], the authors propose a one-hop clustering mechanism for intrusion detection. The target application for the proposed solution is industrial applications. Similarly, Chen et al. [34] talk about an energy-efficient way for intrusion detection in WSNs using an isolation table. In their solution, two levels of clustering are proposed to detect intrusions in a performance-effective way. When the leader of a lower level detects an intrusion in a subcluster, it forwards the according message to the leader of the higher level who forwards it to the base station. While this approach is performance-effective, since a leader has to observe smaller subclusters, the problem of hierarchical IDSs that a malicious leader may not pass an alert to the sink is not solved here. In Strikos [64], the author proposes a method to place intruder detectors to strategic positions of the network such that the whole network is covered. However, no simulation or experimental results proving his claims are provided. Rajasegarar et al. [62] discuss an anomaly detection algorithm for a clustered WSN that minimizes the communication overhead. The proposed scheme is evaluated using a real-world project. Eik Loo et al. [37] present a clustered IDS for WSNs that differentiates between normal and abnormal traffic using a normal traffic model. Thus, it is able to detect route errors and sinkhole attacks. Another approach distinguishing between normal and abnormal behavior is introduced in Mamun and Kabir [59]. It comprises a hybrid IDS for WSNs that are divided into hexagonal regions each having a cluster head. The attack signatures are propagated from the base station towards the

Table 3: Comparative analysis of IDSs implemented for WSNs.

IDS	Implementation	Detection	Attacks	IoT
Abraham et al. [27]	Statistical Detection	Signature	DoS, Unauthorized Access	✘
Abraham et al. [32]	Statistical Detection	Signature	Probing, Unauthorized Access	✘
Agah et al. [50]	Game Theory	Signature	N/A	✘
Agah and Das [51]	Game Theory	Signature	DoS, Selective Forwarding	✘
Bao et al. [30]	Reputation	Signature	Jamming, Sybil, DoS, Sinkhole	✔
Boubiche and Bilami [26]	Cross Layer	Signature	Sinkhole, Spoofing, Battery Exhaustion	✔
Chen et al. [44]	Hierarchical	Signature	Spoofing, Sinkhole	✔
Da Silva et al. [35]	Distributed and Collaborative	Signature	Repetition, Packet Delay, Wormhole, Packet, Alteration, Blackhole, Selective Forwarding	✔
Deng et al. [52]	Machine Learning	Anomaly	Blackhole	✘
Doumit and Agrawal [53]	Statistical Detection	Anomaly	N/A	✔
Eik Loo et al. [37]	Hierarchical	Anomaly	Periodic Route Error, Sinkhole	✔†
Guerroumi et al. [54]	Hierarchical	Signature	Sinkhole	✔†
Ioannis et al. [55]	Distributed and Collaborative	Signature	Selective Forwarding, Blackhole	✔
Jadidoleslamy [56]	Hierarchical	Signature	N/A	✔†
Khan and Loo [57]	Cross Layer	Signature	Hello Flooding	✔
Krontiris et al. [58]	Distributed and Collaborative	Signature	Selective Forwarding	✔
Maleh et al. [36]	Machine Learning	Hybrid	Blackhole, Wormhole, Hello Flooding, Selective Forwarding	✔†
Mamun and Kabir [59]	Hierarchical	Hybrid	N/A	✔†
Ngai et al. [60]	Statistical Detection	Anomaly	Sinkhole	✔
Onat and Miri [61]	Statistical Detection	Anomaly	Hello Flooding	✔
Onat and Miri [25]	Statistical Detection	Signature	Resource Depletion	✘
Rajasegarar et al. [62]	Hierarchical	Anomaly	N/A	✔†
Sedjelmaci and Feham [63]	Machine Learning	Hybrid	Routing Disruption	✔†
Shamshirband et al. [29]	Game Theory	Anomaly	Distributed DoS	✔
Shin et al. [40]	Hierarchical	Signature	Selective Forwarding	✔†
Strikos [64]	Hierarchical	Signature	DoS, Routing Disruption	✔†
Wang et al. [65]	Reputation	Signature	Selective Forwarding	✔

† Suited for IoT networks with some stations without energy limitations that can act as cluster heads.

leaf nodes and the mechanism has predefined specifications for normal and abnormal behavior. The anomaly detection is done by measuring deviations from the predefined specifications. A signature-based IDS is presented in Jadidoleslamy [56]. It is distributed and hierarchical making the detection of both active and passive response-based attacks possible. Guerroumi et al. [54] propose an intrusion detection system against sinkhole attacks on IDSs with mobile sinks. The scheme is implemented in a hierarchical topology using attack signatures.

Evaluating these approaches confirms our prediction about hierarchical IDSs made in Section 4.1. They seem to be a good fit also for IoT networks since each cluster consists of a limited number of nodes. Nevertheless, it is good if an IoT network also contains stronger nodes that can take the role of the CHs.

5.1.2. Distributed and Collaborative IDSs. In Ioannis et al. [55], a collaborative watching scheme is used for a distributed IDS implementation, in order to detect selective forwarding attacks. Krontiris et al. [58] present an IDS, which applies nodes equipped with a local detector that triggers suspicions about a neighbor. Moreover, the nodes collaborate to evaluate suspicions in order to detect whether a node in question is, indeed, an attacker. Similarly, Da Silva et al. [35] discuss a specification-based IDS that uses a decentralized detection process. In this algorithm, the collection of a data unit and its processing is performed in a distributed manner to make the IDS scalable and robust.

As predicted in Section 4.2, these IDSs seem to fit generally well to IoT networks while the extended data exchange necessary for coordination may have an impact on the energy resources.

5.1.3. Reputation-Based IDS. Wang et al. [65] propose an IDS that uses the idea of marking the exchanged packets while heuristic ranking algorithms identify malicious nodes in the network. When the sink receives a marked packet, it can compute the average dropping ratio for each node. If this ratio exceeds a threshold, the node is declared to be malicious. Bao et al. [30] propose a probability model-based technique to analyze subjective versus objective trust. The authors claim that the proposed scheme has a better detection capability than anomaly-based IDS. The two schemes are lightweight in nature. Therefore, as predicted in Section 4.4, they are suitable for IoT networks.

5.1.4. Cross Layer IDS. Boubiche and Bilami [26] introduce a cross layer IDS that uses an intrusion detection agent to exchange information between the physical, MAC, and network layers of a protocol stack. Comparing the observations on the different layers makes the agent capable of detecting multilayer attacks. Another cross layer design is proposed in Khan and Loo [57]. It detects flooding by using and comparing parameters from the MAC and network layers. In both approaches, the processing requirements seem moderate such that, in contrast to our predictions in Section 4.5, the IDSs might also be implemented on IoT networks.

5.1.5. Game Theory-Based IDSs. A noncooperative game for WSNs is presented in Agah et al. [50] and Agah and Das [51]. The goal of the game is to determine the weakest node in the network and thereafter to propose strategies to defend it against malicious attacks. A disadvantage of this approach is that the game detects only a single attack even in the presence of multiple ones, such that the others are left undetected. This weakness makes the approach less suited to IoT networks for which we expect simultaneous attacks on different network nodes. Shamshirband et al. [29] introduce a game theoretic strategy that adopts a combination of a fuzzy Q-learning algorithm and a game theoretic approach. The proposed model consists of sink nodes, a base station, and an attacker that are tested for distributed DoS attacks. The authors claim that the proposed model has a better defense rate than Markovian game theoretic solutions. Since the approach seems to be lightweight with respect to resources, it may also be applied to IoT devices.

5.1.6. Statistical Detection-Based IDSs. In Ngai et al. [60], an IDS for sinkhole attacks is presented that first identifies suspected nodes and then detects attackers using a network flow graph. This algorithm applies the Chi-square based multivariate analysis technique that is carried out using simulations and theoretical analysis. The authors claim that the proposed strategy has a low performance overhead which makes it suited to IoT networks. Doumit and Agrawal [53] use a hidden Markov Model to find unusual activities. The authors claim that their algorithm requires minimal processing resources using experimental scenario. Hence, it can also be used for an IoT based network. Onat and Miri [61] discuss an algorithm that is based on processing arrival traffic. In particular, the arrival traffic pattern for a node is observed, and, based on these studies, a technique to find anomalies is devised. Short term statistics are kept by the algorithm using a multilevel sliding window that reduces the resource requirement. Therefore, such a scheme can also be considered for resource-constrained IoT devices. Another algorithm by the same authors is introduced in Onat and Miri [25]. Here, each node develops a model for its neighbors based on their transceiver behavior and packet arrival rates. When there are major deviations, this is considered as abnormal behavior. This approach, however, may require monitoring every neighbor which can demand a lot of energy consumption. Thus, it might not be a feasible solution for IoT devices. Abraham et al. [27] present an IDS that is effective against Denial-of-Service (DoS) and unauthorized attacks. It is based on the Genetic Programming Technique. A fuzzy rule-based classifier for intrusion detection is shown in Abraham et al. [32]. It is claimed to have 100% accuracy for every type of attack. The technique, however, seems to be not very energy-efficient making it less suited for IoT networks.

5.1.7. Machine Learning-Based IDSs. In Deng et al. [52], an anomaly-based IDS using a Support Vector Machine (SVM) is implemented to detect routing attacks. A SVM is also proposed by Sedjelmaci and Feham [63] who distinguish between normal and abnormal patterns. The scheme seems to be energy consuming but it can run on an IoT node with larger processing capabilities. Thus, as predicted in Section 4.9, it fits with IoT networks containing more powerful nodes. The IDS presented in Maleh et al. [36] bridges machine learning with using clusters. It is basically a hierarchical IDS that, however, uses also SVMs to find out about attack signatures. So, it fits also for IoT networks with some stronger nodes that both can act as CH and can execute the machine learning computations.

5.2. MANETs. The approaches for Mobile Ad hoc Networks (MANETs) are also arranged with respect to the implementation strategies used. They are introduced below. Further, we depict the introduced approaches in Table 4. Here, we also mark approaches suited to be usable for IoT systems.

5.2.1. Hierarchical IDSs. Kachirski and Guha [68] present an approach in which only the cluster heads (CH) are responsible for making decisions such that the energy consumption is reduced. In Huang and Lee [67], clustering is used in monitors that are sparsely positioned over the network. Their purpose is to detect routing intrusions using anomaly detection. The CH is periodically elected to avoid that the energy of single nodes is drained too much. Thus, in contrast to our predictions in Section 4.1, this hierarchical IDS works also for IoT networks without stronger nodes. Sterne et al. [73] introduce a dynamic hierarchic scheme that reduces intrusion detection data packets by data aggregation. The proposed scheme is tested for intentional data dropping and attacks on network and higher layer protocols. In Sun et al. [74], an IDS is presented in which the network is divided into nonoverlapping physical zones. A local agent is responsible for broadcasting alerts in its zone. Moreover, a special gateway zone is defined that aggregates locally generated alerts and

Table 4: Comparative analysis of IDSs implemented for MANETs.

IDS	Implementation	Detection	Attacks	IoT
Albers et al. [28]	Mobile Agent	Signature	DoS	✘
Buchegger and Le Boudec [66]	Reputation	Signature	Packet Dropping	✔
Huang and Lee [67]	Hierarchical	Anomaly	Routing, DoS	✔
Kachirski and Guha [68]	Hierarchical	Anomaly	Packet Dropping	✔†
Michiardi and Molva [23]	Reputation	Anomaly	Node Selfishness	✔
Patcha and Park [69]	Game Theory	Signature	DoS	✔†
Puttini et al. [70]	Statistical Detection	Anomaly	Routing Disruption	✘
Rao and Kesidis [71]	Statistical Detection	Signature	Routing Disruption	✘
Shakshuki et al. [72]	Machine Learning	Signature	Routing Disruption	✘
Sterne et al. [73]	Hierarchical	Hybrid	Packet Dropping, Node Capture	✔†
Sun et al. [74]	Hierarchical	Anomaly	Routing Disruption	✘
Zhang and Lee [75]	Mobile Agent	Anomaly	DoS	✘
Zhang et al. [18]	Mobile Agent	Anomaly	Routing Misdirection, Packet Dropping	✘

†Suited for IoT networks with some stations without energy limitations that can act as cluster heads.

disseminates network-wide alarms. The purpose of such a system is to process the detection results in the zones locally while the gateway nodes process final system-wide results from the disseminated results in the various zones. Since the approach operates with GPS data, it cannot be directly transferred to IoT networks in which not all nodes can be expected to have GPS receivers available.

5.2.2. Reputation-Based IDSs. Michiardi and Molva [23] describe a mechanism that computes the reputation for each node in a network based on supervision of its behavior by other nodes. The reputation is used for the routing decisions, and a node selects neighbors with high reputation values. Further, a watchdog mechanism is used to deny communication with a node whose reputation falls below a certain threshold. In Buchegger and Le Boudec [66], a system for reactive source routing protocols is presented. The reputation of a node is updated based on input from fully trusted nodes that monitor their neighbors using a special watching scheme. As predicted in Section 4.4, both presented approaches are relatively lightweight and, with some modifications, can therefore be used for IoT networks.

5.2.3. Mobile Agent-Based IDSs. In Zhang and Lee [75], the authors propose an agent-based distributed and collaborative IDS. The approach uses a local data collection block that collects and analyzes the observed data in real-time. If it unambiguously detects an anomaly, it informs either a local or a global response block in order to initiate a remedy of a subsystem. If the result of the observations is inconclusive, the data collection block interacts with those in the neighboring nodes via a secure channel, and a collaborative decision is made. Each agent has a local detection engine that uses a modeling algorithm to decide based on predefined matching criteria whether an incidence is normal or anomalous. Depending on whether a decision was taken locally or after coordination with other nodes, either a local or a global response is initiated. In extension to this work, the authors introduce a cross layer IDS in Zhang et al. [18]. In this work, each layer has an IDS module but the detection on one layer may be initiated by those on the other layers such that attacks on different layers can be detected. As described in Section 4.6, due to the amount of coordination required and the somehow complex functionality to be implemented, we are skeptical about the usability of this approach on IoT networks with tiny devices. In Albers et al. [28], the authors describe a distributed mobile agent-based IDS in which the agents migrate to the various data sources. Thus, the work load of each node can be decreased. While this saves processing resources, the approach might, nevertheless, not be a suitable approach for IoT based networks since the freely migrating mobile agents might exceed the abilities of many IoT nodes.

5.2.4. Game Theory-Based IDSs. Patcha and Park [77] present an IDS that models interactions between nodes of a MANET as a noncooperative game with two players. The scheme requires a central processing unit computing the collected observations that runs on a high-performance microprocessor and demands a relatively large amount of memory for data storage and processing. Therefore, this scheme may only be usable for IoT networks with a border router that offers the necessary processing and storage capabilities.

5.2.5. Statistical Detection-Based IDSs. In Puttini et al. [70], the authors introduce an IDS based on Bayesian classification. It models reference behavior statistically observing various network applications. The behavioral model forms then the basis for the detection algorithm that monitors the network for anomalies. Rao and Kesidis [71] use the estimation of congestions to make decisions about the packet dropping problem. Their IDS is dedicated to networks without bandwidth constraints but that have security requirements. Due to this limitation, we do not think that this technique is suitable for resource-constrained IoT devices.

5.2.6. Machine Learning-Based IDSs. In Shakshuki et al. [72], evolutionary computation techniques are used to detect the

Table 5: Comparative analysis of IDSs implemented for CPSs.

IDS	Implementation	Detection	Attacks	IoT
Mitchell and Chen [39]	Voting	Signature	Spoofing, Bad Data Injection	✔
Porras and Neumann [76]	Statistical Detection	Hybrid	N/A	✘
Shin et al. [40]	Hierarchical	Hybrid	Eavesdropping, DoS, Routing Misdirection	✔
Tsang and Kwong [33]	Machine Learning	Anomaly	DoS, Remote-to-Local, User-to-Root, Probing	✔†

†Suited for IoT networks with some stations without energy limitations that can act as cluster heads.

presence of attackers in a MANET causing flooding and route disruption attacks. The performance of such a scheme is evaluated using simulations for different mobility and traffic patterns. This technique demands a high processing capability on all the nodes such that it seems not suitable for resource-constrained IoT networks.

5.3. CPSs. For Cyber-Physical Systems (CPSs), we found only four IDS solutions that each uses a separate implementation strategy. The approaches are described below and depicted in Table 5.

5.3.1. Hierarchical IDSs. Shin et al. [40] combine one-hop clustering for intrusion detection with multihop clustering for data aggregation, carefully balancing the efficiency of the procedure against the provided security. The approach uses a base station, gateways, cluster heads, and leaf nodes each playing a certain role in the IDS. The structure helps to detect a number of attack types carried out on the network. The performance for each node seems to be moderate such that, against our predictions in Section 4.1, the approach might be a suitable scheme also for resource-constrained IoT devices.

5.3.2. Voting-Based IDSs. The IDS presented in Mitchell and Chen [39] uses a voting-based mechanism for anomaly detection. The authors validate their design by considering spoofing and data manipulation attacks. The scheme is quite simple and, as predicted in Section 4.3, seems suited for being implemented also in IoT networks. Nevertheless, the detection rate for a particular network configuration should be analyzed thoroughly first.

5.3.3. Statistical Detection-Based IDSs. Porras and Neumann [76] discuss an IDS that applies hybrid analysis. A signature-based analysis checks nodes for compliance with a rule set. In addition, an anomaly-based analysis uses statistical analysis to detect intrusions that are not yet covered by the rules. The scheme is not dedicated to any specific attack type such that a complex analysis of the observed data is expected. That would make it difficult to implement this technique on IoT networks.

5.3.4. Machine Learning-Based IDSs. Tsang and Kwong [33] present an unsupervised machine learning-based approach to detect anomalies. A goal of this approach is to reduce the usually high rate of false positives in anomaly-based IDS. Since this machine learning approach requires significant computing resources, it is only suitable for IoT networks with efficient border routers.

6. IDSs for IoTs

In this section, we discuss IDS approaches that have been explicitly developed for the use in IoT systems. Since the Internet of Things is a relatively new technology, only few approaches have been published, yet. Nevertheless, we found some promising solutions that we again grouped according to the implementation strategies used. To give a summary, the approaches are further depicted in Table 6.

6.1. Distributed and Collaborative IDSs. Liu et al. [88] use artificial immunity mechanisms to protect IoT networks. Their approach comprehends an attack library to which the sensed behavior is compared. A similar IDS is introduced by Kasinathan et al. [84] who, however, use penetration testing to detect the DoS attacks. Raza et al. [91] introduce a hybrid IDS for IoT networks that targets typical routing attacks such as sinkhole, spoofed, and selective forwarding. The technique is based on network graph inconsistency detection. This approach is criticized by Matsunaga et al. [96] for its high rate of false positives. Arshad et al. [80] describe an intrusion detection mechanism using active collaboration between resource-constrained devices and border nodes, using a collaborative and distributed technique. The technique assigns processing-intensive tasks to the border nodes, in order to efficiently exploit their capabilities.

6.2. Reputation-Based IDSs. Cervantes et al. [82] present an IDS that uses trust-based solutions to detect anomalies in mobile IoT networks. The solution targets sinkhole attacks on the routing layer of IoT networks by using a watchdog and trust-based mechanism. If the trust of a device falls below a certain threshold, it is declared as a threat to the system. A similar approach but with particular consideration of the processing limitations of IoT devices is discussed by ourselves in Khan and Herrmann [43]. This approach is tailored to the Routing Protocol for Low power and Lossy networks (RPL) (see IETF [22]) that has become quite popular for IoT systems. The communication behavior of network nodes is observed by their neighbors for selective forwarding, sinkhole, and version number attacks. Based on the observations, a general reputation of a node is computed in a processor-friendly way using the Subjective Logic; see Jøsang [42]. If the amount of distrust in a node exceeds a certain threshold, it will be quarantined. In Khan et al. [85], we further show that our approach also addresses self-promotion, bad-mouthing, and ballot stuffing attacks successfully.

6.3. Game Theory-Based IDSs. Sedjelmaci et al. [92] introduce an anomaly detection approach that tries to minimize

Table 6: Comparative analysis of IDSs for IoT networks.

IDS	Implementation	Detection	Attacks
Anthi et al. [78]	Machine Learning	Anomaly	DoS, Hello Flood, Sybil, Sinkhole attacks
Arrington et al. [79]	Statistical Detection	Anomaly	N/A
Arshad et al. [80]	Distributed and Collaborative	Anomaly	Routing and application specific attacks
Azmoodeh et al. [81]	Machine Learning	Anomaly	Junk code insertion attacks
Cervantes et al. [82]	Reputation	Anomaly	Sinkhole Attacks
Fu et al. [83]	Statistical Detection	Anomaly	Bad Data Injection, DoS
Kasinathan et al. [84]	Distributed and Collaborative	Rule	DoS
Khan and Herrmann [43]	Reputation	Rule	Selective Forwarding, Sinkhole, Version Number
Khan et al. [85]	Reputation	Rule	Self Promoting, Bad Mouthing, Ballot Stuffing
La et al. [86]	Game Theory	Rule	N/A
Li et al. [87]	Machine Learning	Anomaly	Probing, DoS
Liu et al. [88]	Distributed and Collaborative	Rule	N/A
Liu and Wu [89]	Statistical Detection	Anomaly	N/A
Liu et al. [90]	Machine Learning	Anomaly	N/A
Raza et al. [91]	Distributed and Collaborative	Hybrid	Spoofing, Sinkhole, Selective Forwarding
Sedjelmaci et al. [92]	Game Theory	Anomaly	DoS
Summerville et al. [93]	Statistical Detection	Anomaly	Wormhole, Bad Data Injection, User-to-Root
Xiao et al. [94]	Machine Learning	Anomaly	Identity based, Malwares, Offloading attacks
Yang et al. [95]	Machine Learning	Anomaly	Packet dropping, hole attacks, eavesdropping

the energy consumption. In particular, game theory is used to find out whether the signature of a new attack is expected to occur. Only then, the energy-intensive anomaly detection is activated. La et al. [86] propose a model which comprehends attacks of varying seriousness that demand different degrees of action. The problem is modeled as a Bayesian game and its results determine the threshold to declare an activity as an intrusion. In this way, a lower rate of false positives and negatives shall be achieved.

6.4. Statistical Detection-Based IDSs. Arrington et al. [79] simulate IoT-driven smart homes in order to detect behavioral anomalies. The system constructs behavioral models using special immunity-inspired algorithms for anomaly detection. These models can then be compared with the data captured by the IoT sensors to detect deviations from the expected behavior. Fu et al. [83] present an anomaly mining IDS to detect anomalies at the perception layer. A distributed intrusion detection scheme uses the anomaly data to find out about attacks. A similar approach that, in addition, addresses the processing limitations of IoT networks, is introduced by Liu and Wu [89] who propose a very lightweight anomaly mining algorithm using the Jaccard coefficient. Summerville et al. [93] publish an anomaly-based approach that provides a discrimination between abnormal and normal packets. It relies on bit pattern matching using a lookup table. The processing limitations are addressed by making it possible to implement the algorithm not only traditionally in software but also directly on the hardware layer.

6.5. Machine Learning-Based IDSs. In recent literature, a number of machine learning approaches have been presented for the development of IDS. Yang et al. [95] discuss an active learning approach using human-in-the-loop for intrusion detection in the IoT systems. Instead of just using machine learning, the authors propose to combine machine and human intelligence which allows them to detect malicious nodes in the network more accurately. Li et al. [87] depict a software-defined IoT network for enhancing the performance of IoT applications, based on Artificial Intelligence-based two stage intrusion detection. The approach uses the Bat Algorithm with Swarm Division and Binary Differential Mutation for selecting features. However, this may also increase the overhead in comparison with existing similar solutions. Liu et al. [90] discuss intrusion detection using fuzzy clustering and Principal Component Analysis. The authors classify the data into low risk and high risk while analysis is performed using simulations. Although this approach may have better results in comparison with traditional techniques, it also increases the implementation overhead. Xiao et al. [94] explore IoT security using supervised learning, unsupervised learning, and reinforcement learning-based machine learning techniques. Anthi et al. [78] employ machine learning techniques for detecting network scanning probing and Denial-of-Service (DoS) attacks. Finally, Azmoodeh et al. [81] use deep learning methods to detect Internet Of Battlefield Things (IoBT) malware via the devices Operational Code (OpCode) sequence.

7. Future Directions

Based on the experience made during working for this publication, we found out two research directions for IDSs safeguarding IoT networks that, in our opinion, seem worthwhile to be pursued. They are introduced in the following.

7.1. Intrusion Detection As a Service in Fog Computing. Table 2 gives the impression that one has more possibilities to apply approaches existing for WSNs, MANETs, and CPSs also for an IoT network if it contains at least some nodes with sufficient processing and energy capabilities. That holds particularly when these high-performance nodes are plugged such that energy issues are alleviated. These devices can then execute the computing intensive centralized IDS approaches while the resource limited nodes only assist by delivering data. This fits well to the novel *Fog Computing* concept; see, e.g., Bonomi et al. [97]. Fog Computing is seen as an alternative to traditional Cloud Computing in which the various cloud services are not provided by remote data centers but by local machines that are under the control of the local network operator. For instance, local WLAN routers that are provided with greater processing power and storage facilities can, besides routing data packets between the wired and the wireless network segments, offer various services known from the cloud.

Since border routers connecting an IoT system with the outside world are often WLAN routers, the new Fog Computing technology can easily be integrated into the network. For instance, it could run a centralized IDS protecting the IoT network nodes to which it is connected or take processing- and energy-intensive tasks of the implementation strategies discussed in this paper. Moreover, if the IoT is larger and applies several border routers, one can use their Fog Computing capabilities to realize a hierarchical IDS. In consequence, we see the integration of IDSs on Fog Computing platforms as a promising future research direction. Following the highly virtual nature of the platforms, the IDS functionality can then, like other cloud-based functionality, be offered in form of services, which could be named *intrusion detection as a Service*.

7.2. Reducing Active Channel Listening Times When Rating Network Behavior. To realize an IDS is more difficult for IoT systems when all nodes are resource-constrained, Table 2 reveals for this case that there are three basic strategies available. One is voting-based IDSs that are already sufficiently lightweight to be used in a resource-friendly way. Unfortunately, their accuracy is still suboptimal and further research is needed to reduce the rate of false negatives.

The second strategy is to reduce the workload by splitting it into subtasks executed by different cooperating nodes. That is done by hierarchical IDSs as well as the Distributed and Collaborative IDSs. The problem here is that the reduction of computation efforts takes place at the expense of more data exchange which leads to a faster battery draining. To avoid that, one should investigate the research and development of IDSs that allow the nodes to cooperate with each other minimizing the amount of data to exchange. Here, recent developments in communication protocol technology will be of help. An example is the new IEEE 802.15.4 protocol (see Bhar [98]) that reduces active channel listening. For that, the data frames are divided into a number of slots, and a station has to only listen at time intervals when slots dedicated to itself are transmitted. For larger systems, that reduces the idle listening time of a station significantly.

The third strategy is to use reputation and trust management that provides IDSs with lightweight computation and storage mechanisms. The approaches using trust management, however, are subject to increased active channel listening since a node now also needs to listen to the communication towards its neighbors, the behavior of which shall be evaluated. If our node has to listen continuously, this can consume a lot of energy. Therefore, it might be helpful to conduct research in the combination of the approaches with resource-friendly communication protocols. For instance, a first analysis to adapt the approach presented in Khan and Herrmann [43] and Khan et al. [85] to the IEEE 802.15.4 protocol revealed that the active channel listening time can be easily reduced by two-thirds when the listening strategy is slightly changed. When our station wants to check if a message sent by itself to another station is correctly forwarded to rule a selective forwarding attack out, it only needs to listen to the slots to itself and the one through which the other node forwards the message of interest. Thus, the additional listening cost can be effectively limited. Altogether, the dedication of research in combining energy-efficient networking with reputation-based IDSs seems a promising field of research.

8. Conclusion

We provided an overview about recent trends in using Intrusion Detection Systems in the Internet of Things. In particular, we presented a number of solutions directly developed for IoT systems as well as those for the adjacent network types WSNs, MANETs, and CPSs. Based on this overview, we could name a number of issues for the various IDS types that reduce their applicability of the existing approaches. This allowed us to find out the schemes of IDSs that appear promising to the IoT. Moreover, we identified two research directions promising to alleviate the weaknesses of the IDSs for being used with IoT networks. Altogether, we got the impression that the majority of the existing IDSs are not completely suited for the resource limitations of the IoT but that the developments point into the right direction. After conducting some efforts into research and development, we see a high potential for adequate solutions that will protect the IoT and its users effectively.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] A. Nordrum, "What Is a Distributed Denial-of-Service Attack and How Did It Break Twitter?" 2016, https://spectrum.ieee.org/tech-talk/telecom/security/what-is-a-distributed-denialofservice-attack-and-how-did-it-break-twitter.

[2] T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks," in *Wireless Network Security*, chapter 7, pp. 159–180, Springer-Verlag, 2007.

[3] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 266–282, 2014.

[4] J. Granjal, E. Monteiro, and J. Sá Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[5] A. A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure internet of things," in *Proceedings of the 4th IEEE International Conference on Future Internet of Things and Cloud (FiCloud '16)*, pp. 84–90, IEEE Computer, Vienna, Austria, August 2016.

[6] E. Benkhelifa, T. Welsh, and W. Hamouda, "A critical review of practices and challenges in intrusion detection systems for IoT: towards universal and resilient systems," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, 2018.

[7] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: a survey on the security of IoT frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018.

[8] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the internet of things in the age of machine learning and software-defined networking," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4829–4842, 2018.

[9] I. Ud Din, M. Guizani, B. Kim, S. Hassan, and M. Khurram Khan, "Trust management techniques for the internet of things: a survey," *IEEE Access*, vol. 7, pp. 29763–29787, 2019.

[10] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT middleware: a survey on issues and enabling technologies," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 1–20, 2017.

[11] T. Roosta, S. Shieh, and S. Sastry, "Taxonomy of security attacks in sensor networks and countermeasures," in *Proceedings of the 1st IEEE International Conference on System Integration and Reliability Improvements*, vol. 25, pp. 13–15, 2006.

[12] E. Balandina, S. Balandin, Y. Koucheryavy, and D. Mouromtsev, "IoT use cases in healthcare and tourism," in *Proceedings of the 17th IEEE Conference on Business Informatics (CBI '15)*, vol. 2, pp. 37–44, IEEE Computer, Lisbon, Portugal, July 2015.

[13] S. Mohammadi and H. Jadidoleslamy, "A comparison of physical attacks on wireless sensor networks," *International Journal of Peer to Peer Networks*, vol. 2, no. 2, pp. 24–42, 2011.

[14] S. Khan and J. Loo, "Cross layer secure and resource-aware on-demand routing protocol for hybridwireless mesh networks," *Wireless Personal Communications*, vol. 62, no. 1, pp. 201–214, 2012.

[15] A. M. Popescu, I. G. Tudorache, B. Peng, and A. H. Kemp, "Surveying position based routing protocols for wireless sensor and ad-hoc networks," *International Journal of Communication Networks and Information Security*, vol. 4, no. 1, pp. 41–67, 2012.

[16] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 4, pp. 2–28, 2005.

[17] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: existing solutions and latest technological trends," *Computer Networks*, vol. 51, no. 12, pp. 3448–3470, 2007.

[18] Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion detection techniques for mobile wireless networks," *Wireless Networks*, vol. 9, no. 5, pp. 545–556, 2003.

[19] A. Fuchsberger, "Intrusion detection systems and intrusion prevention systems," *Information Security Technical Report*, vol. 10, no. 3, pp. 134–139, 2005.

[20] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[21] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based internet of things," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, 2013.

[22] IETF, RfC 6550 — RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, 2012, https://tools.ietf.org/html/rfc6550.

[23] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Advanced Communications and Multimedia Security*, vol. 100 of *IFIP — The International Federation for Information Processing*, pp. 107–121, Springer, New York, NY, USA, 2002.

[24] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "A study of RPL DODAG version attacks," in *Proceedings of the IFIP International Conference on Autonomous Infrastructure, Management and Security*, pp. 92–104, Springer-Verlag, 2014.

[25] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '05)*, vol. 3, pp. 253–259, IEEE Computer, Québec, Canada, August 2005.

[26] D. E. Boubiche and A. Bilami, "Cross layer intrusion detection system for wireless sensor network," *International Journal of Network Security & Its Applications*, vol. 4, no. 2, p. 35, 2012.

[27] A. Abraham, C. Grosan, and C. Martin-Vide, "Evolutionary design of intrusion detection programs," *International Journal of Network Security*, vol. 4, no. 3, pp. 328–339, 2007.

[28] P. Albers, O. Camp, J. M. Percher, B. Jouga, L. Me, and R. S. Puttini, "Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches," in *Wireless Information Systems*, pp. 1–12, 2002.

[29] S. Shamshirband, A. Patel, N. B. Anuar, M. L. M. Kiah, and A. Abraham, "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks," *Engineering Applications of Artificial Intelligence*, vol. 32, pp. 228–241, 2014.

[30] F. Bao, I. Chen, M. Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Transactions on Network and Service Management*, vol. 9, no. 2, pp. 169–183, 2012.

[31] S. M. Sajjad, S. H. Bouk, and M. Yousaf, "Neighbor node trust based intrusion detection system for WSN," *Procedia Computer Science*, vol. 63, pp. 183–188, 2015.

[32] A. Abraham, R. Jain, J. Thomas, and S. Y. Han, "D-SCIDS: distributed soft computing intrusion detection system," *Journal of Network and Computer Applications*, vol. 30, no. 1, pp. 81–98, 2007.

[33] C.-H. Tsang and S. Kwong, "Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction," in *Proceedings of the IEEE International Conference on Industrial Technology (ICIT '05)*, pp. 51–56, IEEE Computer, Hong Kong, December 2005.

[34] R.-C. Chen, C.-F. Hsieh, and Y.-F. Huang, "A new method for intrusion detection on hierarchical wireless sensor networks," in *Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication (ICUIMC '09)*, pp. 238–245, ACM, Suwon, Republic of Korea, January 2009.

[35] A. P. R. Da Silva, M. H. Martins, B. P. Rocha, A. A. Loureiro, L. B. Ruiz, and H. C. 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*, pp. 16–23, ACM, Quebec, Canada, October 2005.

[36] Y. Maleh, A. Ezzati, Y. Qasmaoui, and M. Mbida, "A global hybrid intrusion detection system for wireless sensor networks," *Procedia Computer Science*, vol. 52, pp. 1047–1052, 2015.

[37] C. E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami, "Intrusion detection for routing attacks in sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2, no. 4, pp. 313–332, 2006.

[38] R. Mitchell and I.-R. Chen, "A hierarchical performance model for intrusion detection in cyber-physical systems," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '11)*, pp. 2095–2100, IEEE Computer, Mexico, March 2011.

[39] R. Mitchell and I.-R. Chen, "On survivability of mobile cyber physical systems with intrusion detection," *Wireless Personal Communications*, vol. 68, no. 4, pp. 1377–1391, 2013.

[40] S. Shin, T. Kwon, G.-Y. Jo, Y. Park, and H. Rhy, "An experimental study of hierarchical intrusion detection for wireless industrial sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 6, no. 4, pp. 744–757, 2010.

[41] R. Khare and A. Rifkin, "Weaving a web of trust," *World Wide Web Journal*, vol. 2, pp. 77–112, 1997.

[42] A. Jøsang, "A logic for uncertain probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 9, no. 3, pp. 279–311, 2001.

[43] Z. A. Khan and P. Herrmann, "A trust based distributed intrusion detection mechanism for internet of things," in *Proceedings of the IEEE 31st International Conference on Advanced Information Networking and Applications (AINA '17)*, pp. 1169–1176, IEEE Computer, Taipei, Taiwan, March 2017.

[44] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1200–1210, 2014.

[45] A. B. Karuppiah, J. Dalfiah, K. Yuvashri, S. Rajaram, and A.-S. K. Pathan, "A novel energy-efficient sybil node detection algorithm for intrusion detection system in wireless sensor networks," in *Proceedings of the 3rd International Conference on Eco-Friendly Computing and Communication Systems (ICECCS '14)*, pp. 95–98, IEEE Computer, India, December 2014.

[46] R. Mitchell and I.-R. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems," *IEEE Transactions on Reliability*, vol. 62, no. 1, pp. 199–210, 2013.

[47] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: techniques, systems and challenges," *Computers & Security*, vol. 28, no. 1-2, pp. 18–28, 2009.

[48] R. B. Myerson, *Game Theory: Analysis of Conflict*, Harvard University Press, 1991.

[49] R. Mitchell and I.-R. Chen, "A survey of intrusion detection in wireless network applications," *Computer Communications*, vol. 42, pp. 1–23, 2014.

[50] A. Agah, S. K. Das, K. Basu, and M. Asadi, "Intrusion detection in sensor networks: a non-cooperative game approach," in *Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications (NCA '04)*, pp. 343–346, IEEE Computer, Cambridge, Mass, USA, September 2004.

[51] A. Agah and S. K. Das, "Preventing DoS attacks in wireless sensor networks: a repeated game theory approach," *International Journal of Network Security*, vol. 5, no. 2, pp. 145–153, 2007.

[52] H. Deng, Q.-A. Zeng, and D. P. Agrawal, "SVM-based intrusion detection system for wireless ad hoc networks," in *Proceedings of the 2003 IEEE 58th Vehicular Technology Conference, VTC2003-Fall*, vol. 3, pp. 2147–2151, IEEE Computer, Orlando, Fla, USA, October 2003.

[53] S. S. Doumit and D. P. Agrawal, "Self-organized criticality & stochastic learning based intrusion detection system for wireless sensor networks," in *Proceedings of the IEEE Military Communications Conference (MILCOM '03)*, vol. 1, pp. 609–614, IEEE Computer, Boston, Mass, USA, October 2003.

[54] M. Guerroumi, A. Derhab, and K. Saleem, "Intrusion detection system against sink hole attack in wireless sensor networks with mobile sink," in *Proceedings of the 12th International Conference on Information Technology: New Generations (ITNG '15)*, pp. 307–313, IEEE Computer, USA, April 2015.

[55] K. Ioannis, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in *Proceedings of the 13th European Wireless Conference*, pp. 1–10, 2007.

[56] H. Jadidoleslamy, "A hierarchical intrusion detection architecture for wireless sensor networks," *International Journal of Network Security & Its Applications*, vol. 3, no. 5, p. 131, 2011.

[57] S. Khan and K.-K. Loo, "Real-time cross-layer design for a large-scale flood detection and attack trace-back mechanism in IEEE 802.11 wireless mesh networks," *Network Security*, vol. 2009, no. 5, pp. 9–16, 2009.

[58] I. Krontiris, Z. Benenson, T. Giannetsos, F. C. Freiling, and T. Dimitriou, "Cooperative intrusion detection in wireless sensor networks," in *Proceedings of the 6th European Conference on Wireless Sensor Networks (EWSN '09)*, vol. 5432 of *Lecture Notes in Computer Science*, pp. 263–278, Springer-Verlag.

[59] M. S. I. Mamun and A. S. Kabir, "Hierarchical design based intrusion detection system for wireless ad hoc sensor network," *International Journal of Network Security & Its Applications*, vol. 2, no. 3, pp. 102–117, 2010.

[60] E. C. Ngai, J. Liu, and M. R. Lyu, "On the intruder detection for sinkhole attack in wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '06)*, vol. 8, pp. 3383–3389, IEEE Computer, Istanbul, Turkey, June 2006.

[61] I. Onat and A. Miri, "A real-time node-based traffic anomaly detection algorithm for wireless sensor networks," in *Proceedings of the International Conference on Systems Communications*, pp. 422–427, IEEE Computer, Ockland, Calif, USA, August 2005.

[62] S. Rajasegarar, C. Leckie, M. Palaniswami, and J. C. Bezdek, "Distributed anomaly detection in wireless sensor networks," in *Proceedings of the 10th IEEE Singapore International Conference on Communications Systems (ICCS '06)*, pp. 1–5, IEEE Computer, Singapore, November 2006.

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

[64] A. A. Strikos, "A Full Approach for Intrusion Detection in Wireless Sensor Networks," 2007, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.102.385.

[65] C. Wang, T. Feng, J. Kim, G. Wang, and W. Zhang, "Catching packet droppers and modifiers in wireless sensor networks," in *Proceedings of the 6th Annual IEEE Communications Society*

Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '09), pp. 1–9, IEEE Computer, Italy, June 2009.

[66] S. Buchegger and J. Y. Le Boudec, "Performance analysis of the CONFIDANT protocol," in *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc '02)*, pp. 226–236, ACM, Lausanne, Switzerland, June 2002.

[67] Y.-A. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor networks (in association with 10th ACM Conference on Computer and Communications Security)*, pp. 135–147, ACM, USA, October 2003.

[68] O. Kachirski and R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks," in *Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS '03)*, IEEE Computer, USA, January 2003.

[69] A. Patcha and J.-M. Park, "A game theoretic approach to modeling intrusion detection in mobile ad hoc networks," in *Proceedings of the 5th Annual IEEE System, Man and Cybernetics Information Assurance Workshop (SMC '04)*, pp. 280–284, IEEE Computer, USA, June 2004.

[70] R. Puttini, M. Hanashiro, F. Miziara, R. de Sousa, L. J. García-Villalba, and C. J. Barenco, "On the anomaly intrusion-detection in mobile ad hoc network environments," in *Proceedings of the 11th IFIP International Conference on Personal Wireless Communications (PWC '06)*, vol. 4217 of *Lecture Notes in Computer Science*, pp. 182–193, Springer, Albacete, Spain, September 2006.

[71] R. Rao and G. Kesidis, "Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '03)*, vol. 5, pp. 2957–2961, IEEE Computer, USA, December 2003.

[72] E. M. Shakshuki, N. Kang, and T. R. Sheltami, "EAACK — a secure intrusion-detection system for MANETs," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 3, pp. 1089–1098, 2013.

[73] D. Sterne, P. Balasubramanyam, D. Carman et al., "A general cooperative intrusion detection architecture for MANETs," in *Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA '05)*, pp. 57–70, IEEE Computer, College Park, Md, USA, March 2005.

[74] B. Sun, K. Wu, and U. W. Pooch, "Zone-based intrusion detection for mobile ad hoc networks," *International Journal of Ad Hoc and Sensor Wireless Networks*, vol. 2, no. 3, 2007.

[75] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00)*, pp. 257–283, ACM, Boston, Mass, USA, August 2000.

[76] P. A. Porras and P. G. Neumann, "EMERALD: event monitoring enabling response to anomalous live disturbances," in *Proceedings of the 20th National Information Systems Security Conference (NISSC '97)*, pp. 353–365, 1997.

[77] A. Patcha and J.-M. Park, "A game theoretic formulation for intrusion detection in mobile Ad hoc networks," *International Journal of Network Security*, vol. 2, no. 2, pp. 131–137, 2006.

[78] E. Anthi, L. Williams, and P. Burnap, "Pulse: an adaptive intrusion detection for the internet of things," in *Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT*, pp. 1–4, London, UK, March 2018.

[79] B. Arrington, L. E. Barnett, R. Rufus, and A. Esterline, "Behavioral modeling intrusion detection system (BMIDS) using internet of things (IoT) behavior-based anomaly detection via immunity-inspired algorithms," in *Proceedings of the 25th International Conference on Computer Communications and Networks (ICCCN '16)*, pp. 1–6, IEEE Computer, Waikoloa, Hawaii, USA, August 2016.

[80] J. Arshad, M. A. Azad, M. Mahmoud Abdellatif, M. H. Ur Rehman, and K. Salah, "COLIDE: a collaborative intrusion detection framework for Internet of Things," *IET Networks*, vol. 8, no. 1, pp. 3–14, 2019.

[81] A. Azmoodeh, A. Dehghantanha, and K. R. Choo, "Robust malware detection for internet of (Battlefield) things devices using deep eigenspace learning," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 1, pp. 88–95, 2019.

[82] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things," in *Proceedings of the 14th IFIP/IEEE International Symposium on Integrated Network Management (IM '15)*, pp. 606–611, IEEE Computer, Canada, May 2015.

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

[84] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6LoWPAN based internet of things," in *Proceedings of the 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '13)*, pp. 600–607, IEEE Computer, Lyon, France, October 2013.

[85] Z. A. Khan, J. Ullrich, A. G. Voyiatzis, and P. Herrmann, "A trust-based resilient routing mechanism for the internet of things," in *Proceedings of the 12th International Conference on Availability, Reliability, and Security (ARES '17)*, pp. 1–6, ACM, Reggio Calabria, Italy, August 2017.

[86] Q. D. La, T. Q. Quek, J. Lee, S. Jin, and H. Zhu, "Deceptive attack and defense game in honeypot-enabled networks for the internet of things," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1025–1035, 2016.

[87] J. Li, Z. Zhao, R. Li, and H. Zhang, "AI-based two-stage intrusion detection for software defined IoT networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2093–2102, 2019.

[88] C. Liu, J. Yang, R. Chen, Y. Zhang, and J. Zeng, "Research on immunity-based intrusion detection technology for the Internet of Things," in *Proceedings of the 7th International Conference on Natural Computation (ICNC '11)*, vol. 1, pp. 212–216, IEEE Computer, China, July 2011.

[89] Y. Liu and Q. Wu, "A lightweight anomaly mining algorithm in the Internet of Things," in *Proceedings of the 5th IEEE International Conference on Software Engineering and Service Science (ICSESS '14)*, pp. 1142–1145, IEEE Computer, China, June 2014.

[90] L. Liu, B. Xu, X. Zhang, and X. Wu, "An intrusion detection method for internet of things based on suppressed fuzzy clustering," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, p. 113, 2018.

[91] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: real-time intrusion detection in the internet of things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[92] H. Sedjelmaci, S. M. Senouci, and M. Al-Bahri, "A lightweight anomaly detection technique for low-resource IoT devices: a game-theoretic methodology," in *Proceedings of the IEEE*

International Conference on Communications (ICC '16), pp. 1–6, IEEE Computer, Kuala Lumpur, Malaysia, May 2016.

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

[94] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: how do IoT devices use AI to enhance security?" *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41–49, 2018.

[95] K. Yang, J. Ren, Y. Zhu, and W. Zhang, "Active learning for wireless IoT intrusion detection," *IEEE Wireless Communications Magazine*, vol. 25, no. 6, pp. 19–25, 2018.

[96] T. Matsunaga, K. Toyoda, and I. Sasase, "Low false alarm rate RPL network monitoring system by considering timing inconstancy between the rank measurements," in *Proceedings of the 11th International Symposium on Wireless Communications Systems (ISWCS '14)*, pp. 427–431, IEEE Computer, Spain, August 2014.

[97] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the 1st ACM Mobile Cloud Computing Workshop (MCC '12)*, pp. 13–15, ACM, Helsinki, Finland, August 2012.

[98] J. Bhar, "A mac protocol implementation for wireless sensor network," *Journal of Computer Networks and Communications*, vol. 2015, no. 1, 2015.