This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2844742, IEEE Communications Surveys & Tutorials

A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Towards Universal and Resilient Systems

Elhadj Benkhelifa, *Member, IEEE,* Thomas Welsh, *Member, IEEE,* and Walaa Hamouda, *Senior Member, IEEE*

***Abstract*—The Internet-of-Things (IoT) is rapidly becoming ubiquitous. However the heterogeneous nature of devices and protocols in use, the sensitivity of the data contained within; as well as legal and privacy issues, make security for the IoT a growing research priority and industry concern. With many security practices being unsuitable due to their resource intensive nature, it is deemed important to include 2nd line defences into IoT networks. These systems will also need to be assessed for their efficacy in a variety of different network types and protocols.**

This paper is concerned with advancements in intrusion detection practices in IoT. It provides a comprehensive review of current Intrusion Detection Systems (IDS) for IoT technologies, focusing upon architecture types. A proposal for future directions in IoT based IDS are then presented and evaluated. This then shows how traditional practices are unsuitable due to their inherent features providing poor coverage of the IoT domain. In order to develop a secure, robust and optimised solution for these networks, the current research for intrusion detection in IoT will need to move in a different direction. An example of which is proposed in order to illustrate how malicious nodes might be passively detected.

Keywords*—*Intrusion detection systems (IDS), IoT security, wireless sensor networks, universal IDS.

I. Introduction

The Internet-of-Things (IoT) is a novel paradigm concerned with building a pervasive environment of smart devices (or things), seeking to enhance everyday life through ubiquitous connectivity [1]. This is accomplished via the interconnectivity of sensors and actuators, in order to facilitate smart decisions made via analysis of an inherent wealth of data. The IoT technologies are expected to offer unprecedented opportunities to interconnect human-beings. Additionally, the proposed platform for the future IoT will be through Machine-to-Machine (M2M) communications, whereby sensors and networks allow all things to communicate directly with each other to share vital information. This will allow us to have a truly instrumented universe where accurate data is radially available to inform optimal decision making.

The IoT is typically considered to have partially evolved from the implementation of RFID (Radio Frequency Identification Devices) devices[1]. RFID consists of very low power, wireless tags used to electronically identify physical objects and animals. Whilst allowing the wireless intelligent tracking of objects within confined spaces, RFID tags are passive and unintelligent; features disallowing the ability to log and understand their environment [2]; preventing collaboration with other devices and generally stunting the evolution and further analysis of the inherent wealth of data. With the realization that the interconnection of these devices, coupled with intelligent data analytics, may enhance services and facilities in the physical world; such devices evolved from being passive objects to interactive, cooperative and smart devices. Although, still retaining the original mantra of low-power and wireless communication, these devices combine sensors with RFID tags to produce wireless devices capable of sensing their environment and thus producing dynamic data. However due to the low power nature of these devices, the range is limited. Therefore, by harnessing the enabling technologies from wireless computing networks, the capabilities to produce wide-scale sensor networks were achieved [1]. Also, in order to economize on this sensor usage, it is important to implement these networks in an efficient manner, which is accomplished by applying ad-hoc and distributed networking protocols.

As the need for a globalised access to networks of heterogeneous device types was realised in all facets of society, the IoT was born as a vision of global interconnectivity where embedded devices and sensors facilitate a new age where internet connected devices improve our lives. This is famed to be accomplished via a mass collection and analysis of data, however with this enhanced interconnectivity comes further issues.

Security within computer networks has always been a major issue. With sensor based networks being used in a variety of critical infrastructures and applications, the need to secure them is arguably greater than ever [3]-[4]. With the introduction of data protection laws decreeing the responsible collection and storage of data; coupled with issues relating to privacy of the individual and above, the secure handling of data contained within IoT based networks is vital to anyone. In addition, digital forensics is becoming an essential tool for the police as well as anyone wishing to protect their own legal interests. Therefore the correct logging of computer network activity is a must. IoT is an emerging technology, famed with being able to change and improve society life, as such its security is an important issue.

This paper focuses on providing a survey of a variety of intrusion detection solutions for the IoT. Each solution attempts to improve the efficacy of detection in a number

E. Benkhelifa and T. Welsh are with the School of Computing, Staffordshire University, Stafford, United Kingdom (e.benkhelifa@Staffs.ac.uk).

W. Hamouda is with the Department of Electrical and Computer Engineering at Concordia University, Montreal, Canada (hamouda@ece.concordia.ca)

of ways and/or minimise its resource footprint through varied combinations of architectures, detection methods and specific attacks detected. Primarily, this work focuses upon architecture types and the technologies which can be detected. This is driven by a fundamental characteristic of IoT which is related to the myriad of current and future technologies which support it.

This work is reviewed for its effectiveness so as to determine the state-of-the art for IDS in IoT. From this review comes the proposal for a security system which leverages passive sensor nodes to negate the currently poor security environment presented by the open-medium and constrained devices. In turn this enables any number or type of detection methods to be integrated into the system and thus increases accuracy and and coverage for a wide variety of use-cases.

The paper is structured as follows: In section II, standards and technologies for the IoT are introduced. Section III situates this survey within the body of work by reviewing related surveys. In section IV, a review of security threats to IoT devices is provided to support the state-of-the art survey of IDS for IoT in section V. which then facilitates some proposals for future directions in section V. Section VI provides an analysis of the survey which drives proposals presented in section VII. Finally section VIII concludes the work.

TABLE I. A NON-EXHAUSTIVE LIST OF STANDARDS AND PROTOCOLS USED IN IoT

Name	Layer	Description
COAP	Application	Constrained Application Protocol
HTTP	Application	HyperText Transport Protocol
MQTT	Application	MQ Telemetry Transport
XMPP	Application	Extensible Messaging and Presence Protocol
REST	Application	Representational State Transfer
IPV4/6	Network	Internet Protocol 4 / 6
RPL	Network	Routing Protocol for Low power and Lossy Networks
6Lowpan	Network	IPv6 over Low power Wireless Personal Area Networks
802.15.x	Link / Physical	IEEE Wireless Personal Network Standards
802.11	Link / Physical	IEEE Wireless Local Area Network Standards
802.3	Link / Physical	IEEE Local Area Network Standards
2G/3G/4G/5G	Link / Physical	2nd-5th Generation Mobile Telephony Standards
RFID	Link / Physical	Radio-frequency identification
NFC	Link / Physical	Near Field Communication
WiMax	Link / Physical	Broadband Wireless Metropolitan Area Networks
ZigBee	Link / Physical	High-level Wireless Personal Area Network Standard
GPS	Other	Global Positioning System

II. IoT Standards and Technologies

Despite the growing adoption and interest in IoT systems, the term IoT merely describes the idea of global connectivity among smart devices, i.e. it does not specifically define the way in which these devices should communicate. Therefore IoT might best be considered an umbrella term encompassing a variety of technologies and standards, both hardware and software, and does not denote any particular standardisation. IoT networks typically consist of heterogeneous, intercommunicating devices Or ”things” and their networks.

IoT networks are (in the majority) driven by and built upon wireless networking specifications. As stated previously, RFID is one of the founding hardware types for IoT devices. Other low-power wireless technologies used include Wireless Sensor Networks (WSNs), Near Field Communication (NFC), Zigbee, 6Lowpan etc. most of which are considered personal area network technologies due to their low range and bandwidth. Networks may also be constructed upon slightly longer range such as Wi-Fi and Bluetooth [5]. In addition, IoT devices may utilize wide area protocols such as General Packet Radio Service (GPRS), 3G, 4G, WiMax etc. or bridging with wired protocols to facilitate access to the internet and other external networks [6] Whilst these protocols and technologies are not specifically designed for IoT, their integration and potential use is illustrative of the array of protocols which will require consideration. An extensive survey of these technologies is given in [7].

IoT may be thought of as a 3-layer model. Consisting of the *perception*, *transportation* and *application* stages [6] [8] Where the perception stage consists of the sensing technologies such as RFID and GPS and short range transmission such as bluetooth and 802.15.4. The transportation stage consists of longer range communication such as IP, 802.3, 4g, etc. Whilst the final application phase, consists of platforms such as cloud architectures for data management and actuators e.g. traffic management systems.

Due to the resource constraints of the devices, some protocols have been designed specifically to support low power hardware. For example IEEE 802.15.4 is a low power physical and media access specification for resource constrained wireless hardware, Zigbee and 6Lowpan are both built upon this specification [9]. With networking protocol packets being mostly too large for constrained resources, 6lowpan was developed as a low resource replacement. Specifically designed to connect constrained devices to the internet; 6lowpan provides compression in order to accommodate IPv6 over IEEE 802.15.4 or other low power physical and media access protocols. In the literature, 6Lowpan is often discussed with the Routing Protocol for Low-Power and Lossy Networks (RPL), a multi-functional routing protocol for constrained devices, where both are considered the most common IoT based networking set-ups [10].

Within security specifically, this lack of standardization creates issues when attempting to develop generalized research solutions to determine exactly what must be secured. Therefore, this section described an overview of the characteristics of IoT technologies; including the networking technologies used and the specific device features. IoT based networking stacks may be considered as a typical layered networking stack; with each layer being dependent upon the other.

As IoT based networks may still be quite diverse, it is important to consider all types of IoT protocols. A non-exhaustive overview of protocols and standards which may be

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2844742, IEEE Communications Surveys & Tutorials

seen in current IoT systems are depicted in Figure 1. Here we focus on intrusion detection for those developed specifically for IoT networks (such as 6lowpan) in addition to short range wireless network protocols (personal area networks). For a more comprehensive coverage of IoT enabling protocols please see [6].

III. Related Surveys

Due to the key point made in the previous section regarding the diverse array of technologies composing the IoT, likewise there is a variety of surveys to match them. What follows is a non-exhaustive list of some surveys which are relevant to IoT.

Many reviews which cover traditional (predominately wired) networks can be found. However as a consequence of the maturity of the field, in addition to the diversity of techniques available, these surveys tend to focus on a particular aspect of IDS. The array of methods used to merely detect attacks is evidenced via the variety of surveys available. For example, machine learning and data mining techniques are often leveraged due to the vast array of networking data available.

The authors in [11] provide a survey of machine learning and data mining techniques focused upon IDS for general systems, which are regularly mentioned in literature specific to IoT and WSNs, although the survey is not inclusive of these WSNs. The authors highlight a number of issues with these methods, in particular the variety and complexity of these methods requiring optimisation according to the specific use-case and technique. Additionally they note that one of the driving factors for the success and validation of these methods, the availability of quality data, appears to be somewhat lacking.

IDS for WSNs have received considerable attention in literature, perhaps due to their resource constrained nature ensuring their security is difficult. In [12] the authors provide a very comprehensive survey of the characteristics of IDS in WSN (such as architecture, detection methods etc.) and highlight a number of interesting short comings in current work. Including low amounts of data available for validation, such as through simulation or implementation, poor energy consumption optimisation and the lack of universal attack detection. A key point which is relevant to IoT within this survey is that these WSN IDS solutions fail to take into account internet-enabled attacks (such as DDoS) which will often be launched external to the network. Therefore these solutions are only suited to one section of an IoT network.

A similar review, which focuses upon IDS for WSN, is given by the authors in [13]. Whilst still covering the fundamental characteristics of the IDS solutions, one of the main contributions in this work is the applicability of Mobile Ad-hoc Network (MANET) IDS to WSN. Noting that these solutions are not directly applicable to static WSNs. Additionally the authors conclude with a number of recommendations which allows the selection of the most appropriate architecture and detection method according to use-case. As with the previous studies, these use-cases fail to take into account heterogeneous technologies and use-cases which will be prevalent within the IoT.

Cyber Physical Systems (CPS) are related to IoT systems in that they are composed of both physical sensors and actuators networked with computer-based control systems. Some of the key differences include: the time and critical nature of the applications in addition to not requiring connection to the internet. A survey of IDS for CPS is given in [14]. After a classification of detection methods and the qualifying audit data, the authors propose a summary of their findings although many are intuitive and apply to all IDS solutions (such as the relationship between false positive/negatives against detection methods.) However the authors do indicate the most effective techniques for CPS according to use-case and additionally highlight a number of gaps in literature. These include: a lack of IDS metrics (validation issues as before), the lack of multitrust data, little research focusing on attacker behaviour, a lack of anomaly-based models and a lack of research focusing on specific CPS use-cases (e.g. automotive). Whilst this survey also lacks characteristics of IoT, the similarities prevalent within these areas provide some cross-over.

In contrast to the previously discussed reviews, the authors in [15] present a brief survey focused on IDS specific to IoT. They note that IDS cover a number of different technology types, including RFID, LANS, WANs, WLANs, AD-Hoc networks, cloud systems and mobile devices. The key point being that implementation and detection methods are different depending upon the particular technology type. This is a particularly important point in the context of IoT due to the variety of technology types available. They conclude by explaining that a successful IDS for IoT will require coverage of all service layers.

A less brief survey focusing on IDS in IoT is presented in [16]. The authors begin by discussing an overview of IoT devices, citing a previous work and suggest that the paradigm consists of 3 phases: 1) collection, 2) transmission, 3) processing, management and utilisation. They then proceed to discuss an array of technologies available to IoT devices with a focus upon novel wireless technologies. A review of similar surveys highlighted a lack of work which covered all IoT technologies which lead into a survey of detection methods and placement strategies. The survey concludes by highlighting a number of points including: the lack of solutions which cover a range of technology types, attack types and as with the previous studies, poor validation of solutions. Whilst this is correct, this study appears to be flawed at initiation by failing to consider the full range of technology types such as wired technologies.

Therefore these surveys highlight the following points:

- **Detection methods** - A variety of detection methods exist with varying effectiveness. Often they only detect specific attacks and for specific technologies.
- **Technologies Detected** - The vast majority of work appears to only cover one technology type, e.g. WSN, 6LowPan or RFID, there is a distinctive lack of works which universally covers the entire IoT domain.
- **Validation of use-cases** - whilst a vast array of techniques are shows, many are improperly validated via simulation. Additionally there is a lack of comparable datasets available.
- **Unsuitability of Traditional IDS** - a highlighted point agreed amongst numerous surveys is that traditional IDS

TABLE II. NETWORK LAYER INSECURITIES

Networking Layer	Attack Facilitating Features
Physical	External deployment, open wireless medium, embedded design, constrained resources
Link-Layer	Contention based access / collision avoidance
Network	Multi-hop routing, decentralization, broadcast transmissions
Application	Insecure-lower levels, lack of encryption

techniques are unsuitable for IoT networks. Not just due to the lack of technology coverage as detailed above but also due to the pervasive non-determinable nature of device traffic and location.

The diversity in the aforementioned surveys indicates that a review of security for IoT must be scoped effectively. Specifically none of these surveys will cover all technology aspects of IoT, which is deemed essential due to the heterogeneous nature of modern IoT environments. Therefore this survey will attempt to review IDS for IoT from a broader technological scale and propose advisories to these shortcomings.

IV. IoT Security: Threats and Practices

In this section, an overview of currently known security issues within IoT are critically reviewed. Predominately, these security issues relate to the CIA model.

Due to the heavy data collection and processing aspects of IoT, it is particularly prevalent to ensure data security (Availability, Integrity, Confidentiality). Types of attacks on data may be classified as being *passive* or *active* [17]. While passive attacks are concerned with the theft of data or privacy subversion, active attacks are concerned with the destruction, or subversion of data within the network. Table II lists the features at each networking layer which have been known to create security related issues within IoT networks.

A number of inherent characteristics of IoT cause security issues to be prevalent and varied from conventional security issues. These mostly stem from the perception layer, due to the constrained nature of these device. According to the authors in [18], all of these security issues could be thought of an extension of device power limitations. Something which conventional security solutions do not suffer from due to their non-mobile nature, which draws from fixed (and potentially unlimited) energy sources. As a unconstrained energy source is able to support large amounts of memory and processing, Cryptographic principles, which are the foundation of information security, require considerable processing and memory for key storage and processing in order for it to be effective [18].

However, technology and implementation related issues are not the only area which causes IoT devices to be insecure. Profit-driven business and a novel, competitive market causes device manufacturers to consider security as an afterthought, if at all [8]. Due to the predominate sensing nature of the devices, theft of data is considered the largest risk. Unfortunately, the data is often seen to be too trivial for concern. However this tends to be far from the truth e.g. Smart Meters can betray privacy and even physical security breaches through the leaking of data [19]. A deeper concern is with smart cities, where data privacy issues may cause ”an unequal society” through discrimination [20].

To manage the scope of this section, it primarily highlights threats within the perception layer of the IoT Model. This is as threats to traditional networks are covered extensively throughout literature and link with the transportation and application layers predominately.

A. Perception

Whilst the architectural features of IoT networks at the perception layer ensure that their applications are employed economically, efficiently and reliably; these networks still remain vulnerable to a variety of attacks due to inherent security issues relating to resource constrained devices, open-access network medium and the heterogeneity of the devices [21] [8].

When modelling IoT based devices upon a network protocol hierarchy (e.g. OSI), it should first be considered that many attacks may originate from the physical layer, which is where the perception layer lies on the IoT model These issues are similar to those found in WSNs [18] and fundamentally stem from device limitations such as limited battery life, constrained computational process and open wireless networking medium which cause the implementation of traditional security processes to be difficult [13].

Some solutions have been presented to mitigate issues at this layer, which predominately involve the inclusion of the aforementioned security features in a constrained form or physical security to the device itself. Many of these solutions have been shown to be flawed, due to the constrained nature as mentioned previously. Such as with 802.15.4 [22], bluetooth [23], RFID [24] or WiFi [25]. Additionally, these solutions do not protect attacks from the upper layers as this requires an adequate IDS. [8]

Due to subversion of this layer giving rise to exploitation of the above layers, this deems it essential to assess all layers within this model yet with a strong focus on the physical layer. A major attack surface is presented at this layer in which the devices are deployed in external areas ensuring they are open to attack. For example, physical access to the device provides an attacker with the ability to alter the integrity or availability of the device, whilst the open networking medium is susceptible to jamming or breach of confidentiality [26] [27].

A breakdown of known attacks on these systems is given in Table III

B. Transportation

In upper networking layers, such as those related to the transportation layer of IoT, characteristics of the networking protocols used create further issues: multi-hop or broadcast routing, an open network medium, decentralized architecture and many more are just some examples of the widely prevalent multi-layer insecurities [26].

To mitigate these issues, inspiration may be found within traditional computer security solutions within which application layer protocols and services are often protected by firewalls or IDS at the lower levels. Unfortunately, implementations of typical computing security practices are heavy in terms of resource usage; and resources on IoT devices are constrained so as to keep the cost of device to a minimum. In this way, security is often an afterthought of most manufacturers and not given priority over functionality [8].

Using protocols further away from the perception devices tends to be more secure, leveraging features such as IPSec for end-to-end, authentication and integration encryption in IPv4/6 which is feasible due to the larger resources available upon the devices. However as this traffic crosses from the less constrained to the highly constrained, novel solutions

Additionally some technologies still suffer from fundamental issues such as DNS spoofing [28], IPv4 and IPv6 [29] man-in-the-middle, and routing attacks [30]. Although these may be more easily detected with the use of an IDS than their constrained counterparts.

C. Application

IoT Application layer technologies typically involve those involved with the service themselves, often situated around message passing [8] and may traverse all areas of the network from the perception layer sensors to the back-end support systems. The result of which creates the variety of "SMART" solutions available such as smart cities [20]. Therefore the application layer will span a multitude of devices and therefore the security solutions will need to reflect this accordingly, through a holistic solution.

As with the transport layer, cryptography is easily deployed on the back-end or end-user devices but less supported on the perception devices, additionally IDS are also more easily supported [16]. Therefore protection at this layer will ideally need to span all networking layers, where interoperability amongst them is cited as a key issue for the security of the IoT [8] [31] [32]

V. State-of-the-Art Intrusion Detection in IoT

This section begins by an overview of Intrusion Detection Systems (IDS) followed by an extensive survey of IDS characteristics for IoT.

IDS are a widely established, networking security component. Although they are a form of detection (2nd line of defence), and not protection; their use in wireless networking is unparalleled, as preventative security measures are difficult to implement [40]. IDS may also be found in different forms: host-based and network-based, where host-based systems monitor activity on the system itself (API calls, disk activity, memory usage etc.) whereas network-based systems monitor network activity and communications. In a general sense, an IDS will monitor behaviour (either host activity or network traffic) for signs of attack; working under the assumption that nominal behaviour and malicious behaviour are distinct [41].

There are two prominent metrics for measuring the efficacy of an IDS. Referred to as *false positives* and *false negatives*. A false positive occurs when legitimate traffic is reported as illegitimate and false negatives occur when illegitimate activity is not detected at all. Although, due to the sparse availability of data sets for IDS; the efficacy of measuring their performance is contentious [42].

Many different techniques have been proposed in literature for building various types of IDS. The majority of these are particularly resource intensive due to the scale of both signature-based databases and anomaly models. [43] In addition, both of the aforementioned detection methods require aperiodic updates in order to keep the databases or models accurate. Due to this inherently heavy resource, both of the aforementioned detection methods are not well suited to the constrained resources of IoT embedded devices [15][14][13].

Different attack detection methods are covered widely across literature and other surveys. The review will catergorise the work upon architecture type employed but with a focus upon the technology detected. Detection types are typically classified as: *misuse*, *anomaly*, *specification* or a *hybrid* [13].

Misuse detection techniques employ a database of know attacks. Activities, such as network traffic or system-level actions, are compared to signatures within this database. If there is match then the activity is flagged as suspicious. Examples of suspicious network activity might be repeatedly testing for open ports, or the detection of shell code within network packets. Misuse detection is very successful at detecting attacks that are known (low false positives) but are poor at detecting attacks that are unknown (high false negatives). This is due to the lack of signature for novel attacks. Additionally, storing and updating databases of signatures is impractical on constrained devices. [12]

Anomaly detection techniques take a contrasting approach in which a model of typical activity is built which then enables current activity to be compared against this model where any discrepancies are flagged as suspicious. For example the model might record the time and usage of all applications on a system and if an application is used outside of normal hours (e.g. at midnight instead of during working hours) then anomalous activity will be flagged. Alternatively with networking based activity models, if a server is suddenly seen to be connecting to an address or service which is not typical then malicious activity will be flagged again. Anomaly detection techniques excel at detecting new attacks where misuse detection methods would typically fail and thus have low false positive rate. However they tend to suffer from a high rate of false positives if the model is not periodically updated. The varying nature of wireless communications may cause false positives. Additionally, periodically updating the models may be resource intensive and thus put strain on resource-constrained devices. [13]

Specification based techniques combine attributes of anomaly and misuse detection. As before, this involves the detection of anomalous activity from a pre-defined model. However in contrast, the activity must be confirmed as malicious by a human participant. [13] This technique is advantageous due to the increased accuracy but introduces a delay in the creation of a signature due to the human interaction, which causes the process to not be timely.

Hybrid detection techniques will involve any combination of the above. Whereby issues relating to the efficacy of one

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2844742, IEEE Communications Surveys & Tutorials

TABLE III. PERCEPTION LEVEL IOT ATTACK SUSCEPTIBILITY

Attack	Facilitated by IoT Feature	Result of attack	Type	Examples
Device Jamming [33]	Open wireless medium, embedded design,	Denial of service	Active	Random, reactive, constant, Deceptive
Network sniffing [34]	Open wireless medium, insecure routing, decentralization	Data disclosure, Privacy Invasion	Passive	-
Battery exhaustion [35]	Embedded design, open wireless medium	Denial of service	Active	Traffic flooding,
Device Cloning [36]	External deployment, open wireless medium	Denial of service, data disclosure	Active /Passive	-
Side-channel Analysis [37]	External deployment, embedded design	Data disclosure, advanced cryptographic attacks	Passive	-
Routing Attacks [38]	Multi-hop networking, decentralization	Denial of service, data misdirection, data subversion	Active	Selective forwarding, packet alteration, sinkhole
Cryptographic attacks [39]	Open wireless medium, constrained resources	Secured data disclosure,	Active/Passive	Brute force

technique is mitigated by the strengths of another. [16]

As mentioned previously, IoT technologies are wide and varied. The classification of work according to technology type can be difficult for a number of reasons. Often due to the vagueness of the solution such as a lack of implementation and pure theoretical proposal. A large amount of work merely lists WSNs, which themselves may be composed of differing protocols, whilst others list a specific device type such as mobile (smart phones, laptops) multi-layers / standards or merely atomic standards e.g. Bluetooth. The review as detailed in the following sections has attempted to list these as accurately as possible given the available information.

This section has noted that there is a variety of IDS architecture implementations. Therefore it is necessary to evaluate the efficacy of this software under varying conditions including: attack types. architecture, detection method and performance. This review classifies the work according to architecture type with a focus upon technology detected.

In contrast to previous surveys which classifies the IDS work into varying architecture types, this survey categorises them into the following:

- **Centralised** - the entire IDS is placed in a central, either remote or host-based location.
- **Distributed** - the IDS nodes are places among multiple or all nodes within the network and responsibility is divided amongst them.
- **Hierarchical** - may be stand alone or in combination with another architecture type in which some nodes have a greater responsibility for processing than others. Decentralised architectures are grouped under hierarchical.
- **Hybrid** - any combinations of the above. Often found in tandem with multiple detection types.

Figure 1 illustrates some examples of the architectural differences between IDS placement strategies reviewed. The following subsections will review the surveyed work following the categories as above.

A. Centralised

Systems which monitor data from a single location and conduct processing on an external device have advantages in that they do not impose an extra overhead on the sensor nodes. Moreover these single node systems do not create additional points for subversion and allow for greater depth of processing. However, by moving the data analysis to an external agent, they create a single point of failure.

In contrast, alternative methods involve providing monitoring at the sensor node level such as in [44], where the authors develop an anomaly based NIDS system where each sensor node contains a lightweight application to monitor its own and or others communication to detect ZiGBee devices only.

In [35], the authors present an anomaly HIDS which detects battery exhaustion attacks (a type of DoS) which targets one process, an attack particularly relevant to IoT devices due to their constrained power source but specific for mobile devices such as laptops. Whilst a similar approach is seen in [45]. Both of these methods use anomaly profiling as a HIDS. Although able to detect a specific attack the validity of the results is questionable due to potential subversion of the devices.

The authors in [46] develop methods to deploy misuse detection upon the constrained devices through optimised pattern matching algorithms. Whilst the methods were evaluated in a centralised manner upon one device, the value of this work shows that these techniques may permit *distributed* or *decentralised* distribution of an IDS over multiple constrained devices. However, arguably the hardware used has still greater resources than more constrained nodes such as those employed in WSN.

A similar approach which uses optimised matching algorithms for constrained devices but for anomaly detection, is presented in [47]. The method involves deep packet inspection and its accuracy and performance is shown to be rather effective. Such a centralised implementation would need to be deployed depending on particular use-case. For example, on a device which is constrained but relatively isolated from other constrained devices so as to not be able to leverage collaborative resources.

Two IDS [48] [49] which are concerned with Bluetooth technologies both employ misuse detection, in a centralised manner, as a remote NIDS. The efficacy of this approach is considered stronger than employing the system on the target nodes. This is due to the increased resources available for storage and processing of networking data.

In [50] the authors again deploy their misuse detection in a centralised remote server which monitors 6LowPan networks through the use of probes. As is often the shortcoming with

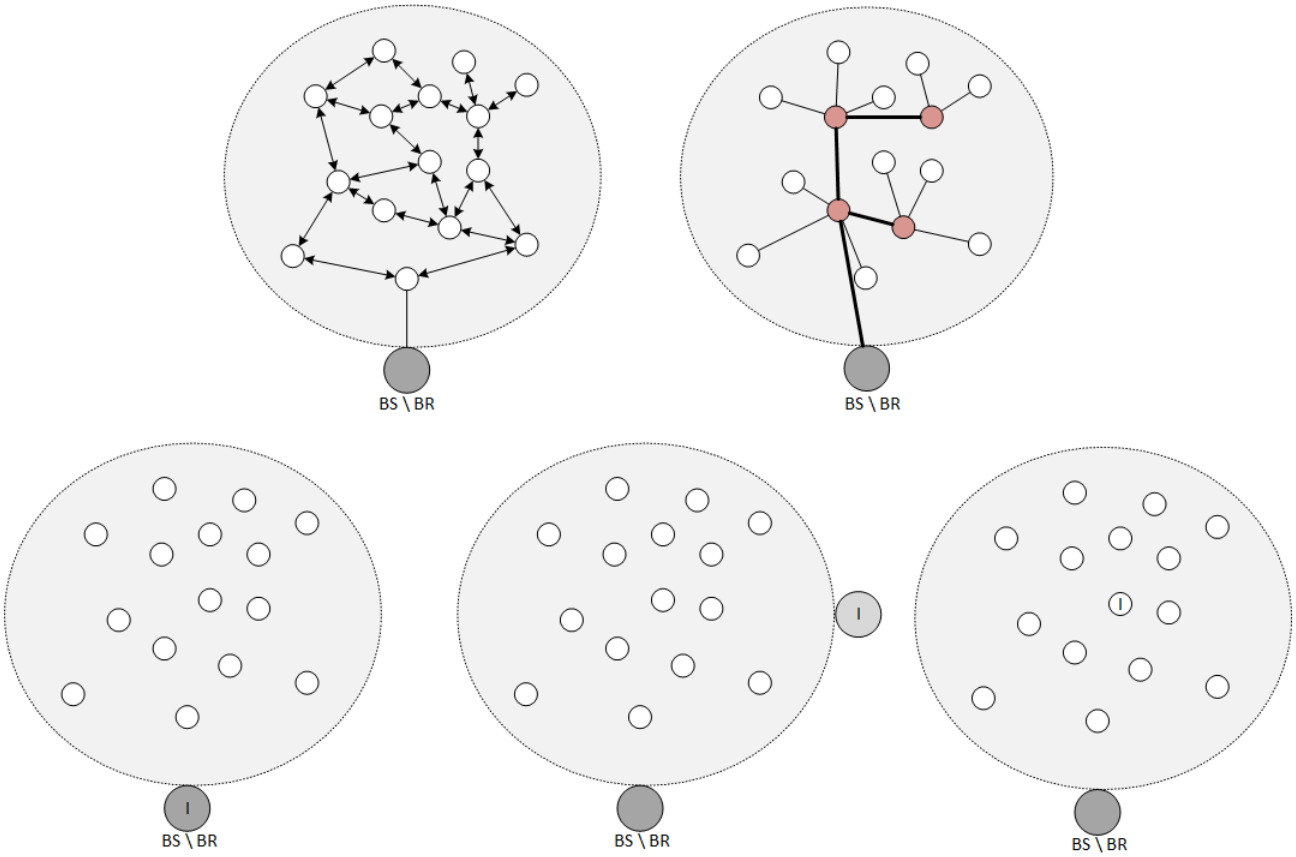

Fig. 1. The traditional architecture types which are currently proposed for IoT based networks. The letter I represents the placement of the IDS. The top two networks indicate a distributed and hierarchical architecture. The edges between nodes indicate available communication paths. The bottom diagrams indicate 3 possible solutions for centralised processing. The leftmost diagram indicates centralised processing upon the border router, the central on an external node and the third on a single node.

misuse detection, this technique only permits the detection of DDoS attacks and for only one technology although the authors explain that the platform has the ability to integrated as a hybrid detection method. Which would considerably improve the performance.

An improvement upon the host-based centralised detection is shown in [51] where the authors present a system to detect DoS attacks using a hybrid detection method. In that an external host monitors the network via secure, wired probes. Unlike previously discussed work, this system is designed for 6LowPan networks. Therefore its solution is dedicated to IoT based networks.

Using specialised hardware - smart batteries, the authors in [52] employ a HIDS for anomaly detection. Despite the additional expense, a method such as this indicates how trust can be employed locally through the application of ”trusted” hardware. Of course an adversary who might subvert the hardware would still be able to subvert the device at the physical layer. However an attack such as that would likely be costly.

B. Distributed

A number of anomaly detection techniques employ distributed architectures but in a *watch* dog based manner. This involves a subset of the network monitoring the other nodes. In [53] the authors employ a statistical trust-based method for attack detection in WSN which shows good levels of success against a variety of attacks. Whilst the authors in [54] attempt to minimise the resource consumption of the anomaly methods using weak hidden markov models in addition to the watch-dog technique. They employ both a NIDS and HIDS and show success in detecting some specific attacks although with variable accuracy. !!!Another watch dog based method presented by the authors in [55], detects attacks under the assumption that nodes in the local cluster will behave alike. Using a rule-based method for high accuracy and low false positive but only for selective attacks. Whilst the authors claim that this method is unlike anomaly and misuse methods, the method in is in fact a hybrid model. As a model of typical use is compared to behaviour of misuse. Whilst watch-dog based models may have benefits such as reducing the resource requirements of the overall IDS, the watchdog nodes themselves may still suffer from subversion and thus monitoring the other nodes may be untrusted.

In [56], the authors successfully leverage learning automata (LA) upon a distributed architecture to detect DDoS attacks. The method is particularly commendable as it designed for heterogeneous device types and network layers and therefore covers a wide area of the IoT. The solution fails, however, to take into account subversion of the system or protocol itself. For example by falsifying a DDoS it may be possible to cause a DoS against the network.

In [57] the authors propose a hybrid detection system which leverages Computation Intelligence (CI) in an attempt to overcome numerous shortcomings of traditional WIDS. The details of the proposal are slim so evaluating its success and performance is difficult. However encompassing multiple architectures and detection types is certainly of merit, although one might argue the complexity of such an architecture increases the attack surface of the system.

Through clustering, a specification method in [58] optimises resource consumption of the overall IDS, leveraging host and network monitoring. The downsides to this architecture is its difficulty in detecting other types of attacks.

In [59] the authors present an anomaly NIDS which utilises mobile-agents for IDS for enhanced resource optimisations and fault-tolerance. The authors explain that using purely distributed over hierarchical decreases the chance of subversion. However although the mobile agents decrease resource consumption for the IDS they increase energy consumption on the particular nodes they are active upon and thus skew the node's current work.

Whilst the authors in [60] describe an artificial immune system based machine learning approach "for the IoT". The method would appear to be a hybrid/specification based due to signatures created by the technique which then must be inserted by the administrator. Unfortunately the authors do not explain which particular technologies this system applies to. There is also little mentioned regarding the placement of the IDS. Similar work has shown that such techniques may be employed in a distributed manner but the resource requirements for constrained devices is questionable. However the authors present a practical implementation which is evaluated under simulation in their previous work [61] which is designed specifically for WSN. The authors note that false positives are often generated due to fluctuations in the RF signal quality.

C. Hierarchical

Artificial Immune Systems (AIS) have shown success as an anomalous detection in conventional networks. In [3], the the system spans multiple network scales in a hierarchical fashion. It utilises both NIDS, HIDS and WIDS showing success in interoperability across heterogeneous network types. The system takes into account the excessive false positives within anomaly based methods via cooperative information to dramatically increase accuracy. Systems of this form are likely to be highly deployable across large and heterogeneous IoT networks. Although there are many issues which must be considered here regarding the complexity of the system.

In [62] the authors claim to be using a distributed system although they use a hierarchical approach, applying datamining as an NIDS. The detection method is also hybrid by employing a modelling method which detects multiple attack types. The architecture employing a centralised agent creates a single point of failure in this system.

A hierarchical watch-dog based NIDS in [63] is employed to detect a multitude of attacks using a specification based scheme on IPv6 WSNs. A rule must first be detected but then approved by an administrator. The efficacy of the proposed latency in detection is a short-coming with this method. The watchdogs have attacks specific to their location, which aids in resource optimisation and minimisation of false positives.A watch-dog NIDS in [64] applied to hierarchical clusters is shown to detect sink-hole attacks using a trust method for 6LowPan networks the authors show good detection performance and state their intention to evaluate for further attack types. The concept for a distributed and hierarchical, watchdog-based NIDS use for anomaly detection in RPL is given in [65]. The hierarchical component which relies on the edge router's lack of subversion is a single point of failure within this system.

A NIDS for detecting sinkhole attacks for RPL, which deploys one component on the border router and others distributed across the remaining nodes is presented in [66]. The hierarchical nature of this system, which relies upon nodes forwarding packets for other nodes again creates an attack target for subversion.

The authors in [10] present NIDS described as specifically for the IoT. The IDS employs a hybrid of both anomaly and signature techniques to detect routing attacks via the RPL metric. Although the authors explain that the technique could easily employ other detection methods although only from the network layer and up. In [67] the authors provide an extension to this work which utilises another metric to detect attacks using an anomaly method. Despite this, the architecture covers only 6LoWPAN technologies. Whilst 6LoWPAN is arguably the most considered IoT technology it does not cover all types. The architecture is decentralised and hierarchical due to processing more data on higher resource edge node.

A hierarchical anomaly based NIDS in [68] uses learning automata upon resource (or energy) information of forwarded packet (routing) attacks in WSN only. A similar technique can be seen in [69] where the authors propose a NIDS which combines both misuse and anomaly detection to cover multiple attack types. Mitigating issues relating to accuracy via the hybrid method but also causes greater complexity and resource consumption on each node.

Whilst [70] also applies anomaly based machine-learning for detection in a hierarchical manner. However, this time the authors employ both HIDS and NIDS however the authors lack an implementation to indicate the efficacy of the solution.

Another anomaly method which leverages ant-colony optimisation upon cluster heads is [71]. The method detects routing attacks only, although the authors explain that their detection method is able to detect both internal and external attacks, as opposed to just one.

TABLE IV. OVERVIEW OF SURVEYED IDS FOR IOT LITERATURE

Reference	Architecture	Tech Focus	Detection Method	Type
[48]	Centralised	Bluetooth	Misuse	NIDS
[35]	Centralised	Mobile devices	Anomaly	HIDS
[45]	Centralised	Mobile devices	Anomaly	HIDS
[51]	Centralised	6LoWPAN	Hybrid	NIDS
[49]	Centralised	Bluetooth	misuse	NIDS
[52]	Centralised	Mobile devices	Anomaly	HIDS
[46]	Centralised	IP Wifi	misuse	NIDS
[47]	Centralised	IP application	anomaly	NDIS
[50]	Centralised with probe	6LoWPAN	misuse	NIDS
[72]	Distributed	WSNs	anomaly	HIDS
[59]	Distributed	WSNs	anomaly	NIDS
[73]	Distributed	WSNs	hybrid	NIDS
[56]	Distributed	Multi-Layer	specification	NDIS
[57]	Distributed	wireless protocols	hybrid	hybrid
[60]	Distributed	WSNs	signature	NDIS
[58]	Distributed	RPL	specification	hybrid
[53]	Distributed watchdog	WSNs	Anomaly	NIDS
[54]	Distributed watchdog	WSNs	Anomaly	HIDS, NIDS
[55]	Distributed watchdog	WSNs	Hybrid	NIDS
[70]	Hierarchichal	WSNs	Anomaly	HIDS, NIDS
[3]	Hierarchichal	802.15.4, 802.11, wired ethernet	Anomaly	HIDS,WIDS,NIDS
[66]	Hierarchichal	RPL	anomaly	NIDS
[65]	Hierarchichal	RPL based 6LoWPAN	anomaly	NDIS
[68]	Hierarchichal	WSN	anomaly	NIDS
[71]	Hierarchichal	WSNs	anomaly	NIDS
[69]	Hierarchichal	WSNs	hybrid	NIDS
[64]	Hierarchichal	6LoWPAN	hybrid	NDIS
[63]	Hierarchichal watchdog	Ipv6 wsn	specification	NIDS
[10]	Hybrid	RPL based 6LoWPAN	Hybrid	NIDS
[74]	Hybrid	RPL	specification	NIDS
[67]	Hybrid	RPL	anomaly	NIDS

VI. ANALYSIS

This section provides an analysis of the aforementioned review. Overall, there is considerable variety in the reviewed work. Table IV provides an overview of the key characteristics reviewed. A summary of key points is presented in the subsections below.

A. Technology Coverage

Overall, solutions are typically tailored to a specific protocol e.g. Bluetooth, 6LowPan or WSNs in general. Few works will focus entirely upon all proposed technologies within the IoT domain. Therefore proposing to name these works as IoT IDS is questionable and may lead to end-users being unaware of the scope of their products, or organisations requiring multiple products to cover multiple technology types and areas. Questions of interoperability and effectiveness between interactive components are not given, as such the future of this area is uncertain, giving rise to potential further issues relating to attack surface and solution complexity. Some works such as [3] and[50] attempt to mitigate these issues by encompassing a wide variety of components. However, even these solutions do not cover all 3-phases of the IoT layers and not in a holistic manner.

Wireless protocols of all types are the most prominent examined. WSNs in particular are given a lot of focus, most likely due to the mature life span of this technology. As stated within the previous surveys, WSNs share similar protocols, technologies and resources but fail to consider internet driven attacks, e.g. DDoS or additional protocols e.g. 802.3. WSN IDS are seen in all architecture forms except a centralised manner, perhaps due to physical resource constraints of covering vast areas. In contrast 802.11 standards (within a constrained and IoT context) are seen in a variety of architecture types, although work is considerably less than the WSNs. Similarly protocols for 6LowPan can be seen across all architecture types which perhaps evidences consideration from researchers of the enhanced need for internet based analysis.

Therefore we argue that the wide variety of technologies across the IoT is a driving issue for its security due to the aforementioned issues relating to detection and interoperability.

B. Detection Types, Effectiveness and Suitability

There is diversity in architecture and detection types; with varying degrees of effectiveness to the variety of attack types detected. NIDS are seen more than any other, often found with anomaly detection methods. HIDS are seen less commonly due, largely due to the excess resource consumption required on the already constrained nodes.

Anomaly based detection methods are seen more over misuse detection methods due to their smaller memory footprint and as such are proven more effective upon constrained protocols. One alternative and most promising methods to network activity monitoring appears to be the monitoring of device resources (e.g. [72]), as embedded devices are typically designed around their power usage. Determining incorrect usage for a lot of attacks is simple when examining resource usage. Numerous mitigation methods for false positives have also been proposed in literature, which is a large issue due to the variable nature of RF-based communications. In addition, unconventional AI based methods (such as with ACO [71]) may be seen with good levels of success but they will typically cover only a few types of attacks and not all layers.

Misuse techniques are seen less in the IoT work covered within this review and others. Largely due to the constraints upon the majority of these devices preventing the storage of database of signatures. This would explain why these techniques are mostly seen within centralised architecture types which provide greater resilience against subversion but which may maintain an incomplete picture of network activity if the area is not sufficiently covered. The fact that misuse-based methods are exemplar at detecting known attacks yet so little work is seen is likely due to these resource constraints and the ever increasing prominence of zero-day attacks negating their effectiveness.

Detection techniques cover a range of attack types and network layers but none appear to be comprehensive in terms of attack type detected, wireless technologies and networking layers. An IDS which was developed truly for IoT would be required to detect all of these. In addition, it could be argued that due to the previously discussed issues regarding the open and insecure physical layer, implementing an IDS on any sensor node itself, can never be guaranteed to be reliable. However these implementations which are implemented in software on the target device, as opposed to dedicated hardware, may be suitable for less mission critical applications. Although for networks with sensitive data which must be vitally protected (e.g. military, health or any other under jurisdiction of data-protection and privacy legislation's), this lack of guarantee is unacceptable and would hint at a hybrid detection method. At the minimum, it should be known whether such intrusion software is reliable or not which may be guaranteed via a 3rd party.

C. Architecture

In regards to architecture, the least commonly seen form is a centralised architecture. Typically data collection and/or analysis is conducted in a decentralised manner. The ad-hoc and distributed nature of the wireless networks being the most prominent reason for this. Primarily as wireless communications are difficult to comprehensively detect from a centralised location due to the nature of RF transmission. Additionally providing a more scalable and adaptable system is suited to this architecture type.

The majority of the work reviewed focuses upon minimizing the footprint of the application in order to economise on resource usage within these distributed applications. However it could be argued that employing such mechanisms creates multiple additional layers of complexity within the network and system. This has many disadvantages such as an increase in resource usage, increased attack surface, and general maintainability issues. Foremost, network overhead is considerably increased, which puts more strain on the already constrained bandwidth. Finally, additional strain is put onto the sensor nodes with increased processing and memory usage. Further issues occur during implementation of such a system, whereby each node to contain IDS software needs to have additional code developed for it. Whilst this might be justified for homogeneous network types, this proves more difficult for IoT based networks. Due to the various devices, architecture types vary considerably and thus; additional development time may increase with network complexity. Also this additional complexity creates new potential security vulnerabilities, which is not an ideal situation. High-level programming solutions may mitigate the majority of these issues but put considerable strain on the resources of these constrained devices.

An alternative to this distributed architecture is hierarchical systems which are also seen often within this work. They attempt to mitigate the aforementioned issues of resource consumption on constrained nodes through distributing this work more appropriately via node placement. For example, more resource intensive tasks will be undertaken by those nodes with more resources, or sometimes handled in the majority by a central node. Dependent upon the particular structure of the network, hierarchical structures may introduce multiple weak points in the architecture by having one or more points of failure/subversion for example through falsifying or nullifying alerts.

VII. Proposed IoT IDS Architecture

In the previous sections, we reviewed work within the area of IDS for IoT and provided an analysis of the work. In this section we look at ways of mitigating some of the seen issues via an architectural solution. All of the work presented proposes solutions which seek to minimise resource usage upon the resource constrained network whilst attempting to maximize the efficacy of the process. For most of the work seen, this is accomplished through adding additional software and or networking layer. Unfortunately this ensures additional overhead and complexity within the IoT network itself, which is arguably not acceptable in heterogeneous networks of the IoT. A more effective solution would remove this complexity and excess resource consumption away from the IoT network. In addition, whilst distributing the collection or analysis of data amongst nodes appears to be an effective method of solving scalability issues; poor physical security still leaves the issue of subvertable devices open. Therefore this does not comprehensively cover all network layers.

We summarise the following issues:

1) A wide variety of technology types amongst the IoT causes poor coverage of all 3 IoT layers from any solution. Multiple issues such as complexity and interoperability must be solved to mitigate this. Whilst individual solutions may be suitable for individual use-cases, issues of expandability and interoperability still exist.
2) A considerable amount of detection techniques have been presented with variable detection accuracy and attack coverage. None appear to be able to cover all attack types with good accuracy. This is partially due to the variability of RF-based communications and the resources available for capture and processing. The only real effective detection method are hybrid methods which require these resources
3) The distributed nature of these systems causes distributed or hierarchical IDS to be the most prominent.

However due to constrained resources these are difficult to implement effectively and securely.

4) Fundamentally, the open-medium and constrained nature of IoT devices leaves them liable to subversion at the physical layer, and thus all above layers. As such, they cannot be trusted security services.

Taking the above into account, it is proposed that the most effective and secure IDS solution would be one in which RF monitoring is passively conducted via network probes, similar to the work in [75] which applies this technique to WIFI networks and [50] which applies this to 6LoWPAN networks. Both of these techniques show merit and through various adaptions could be extended to cover a wide number of IoT technologies and attack scenarios.

Specifically, a novel and proposed system would use hard-wired or secure point-to-point links to connect network probes to an external site. These would be modular in nature and thus permit a wide variety of technology types in an extensible manner. Optimised antennas could provide varying levels of coverage across long distance and large areas and for differing protocol types. The probes could provide coverage of these communications to a back-end system which would permit a number of modular detection methods. A cloud-based system would be advantageous to provide scalability; with potentially unlimited processing facilitating any data analysis necessary. At the expense of greater financial investment, such a solution would have the following advantages over currently proposed solutions:

- Ability to externally process data and thus; conduct resource intensive detection methods and comprehensively detecting attack types as described throughout literature - mitigating the issue of varying detection methods.
- The ability to detect attacks on the physical layer and above, which will provide monitoring for the entire network and mitigate issues relating to the open-medium and untrustworthy nodes.
- Facilitate the monitoring of multiple node types whilst not requiring additional code through a universal monitoring solution. Modularisation would enable extensibility and negate issues relating to constrained technologies.
- Remote processing would negate any additional strain upon on the resource constrained network or devices, in addition to no additional layer of complexity.
- Create a more secure solution by moving the system to a different layer than that to be monitored.

It is believed that such a system would be the most comprehensive (in terms of attack and device types monitored) and a secure way to develop an IDS tailored specifically to IoT. However, the following negative aspects will need to be reviewed:

- Ensuring a secure connection between sniffer nodes (point to point wireless links, or hard-wired lines).
- The cost of additional hardware.
- The cost incurred of potentially monitoring multiple RF frequencies.
- The security of an external monitoring platform.
- The specific detection methods to employ.
- Lack of full coverage of a site and thus; getting an incomplete picture of the network traffic.

However it is believed that for many mission critical applications that such costs are negligible. The technology to implement such a system is already available, with success shown in similar systems for homogeneous WIFI networks [50].

A. System Description and Comparison

Figure2 illustrates the ideal solution and a description of its components and implementation considerations is given below.

Architecture from the perspective of an IoT network would be externally based in order to mitigate issues with the solutions reviewed within this paper. Whilst other architectures have issues relating to attack detection range and technology type, these will be negated via probes and long range antennas.

Other reviewed architectures were presented in a distributed or hierarchical form within only the perception layer. However these architectures may suffer from subversion due to placement in a hostile environment whilst hierarchical architectures suffer from varying single points of failure. Whilst a centralised architecture might also suffer from single point of a failure, the back of the proposed system could be supported by cloud/edge and other dynamic and scalable infrastructures which mitigate this issue.

The conceptualisation within fig 2. illustrates that the architecture encompasses all layers of the IoT model, as opposed to just one which is covered by the majority of the reviewed work.

Detection Methods traditionally vary in effectiveness across IDS work reviewed in the IoT. Through hosting this IDS on an external and scalable hardware, pluggable modules will permit a wide variety of detection methods, as dictated within literature, which will permit a wider range of attacks detected than any other previously cited. In fig. 2, the remote IDS is placed upon a cloud service which will permit the introduction of any and all detection methods required, with scalable resources able to support them. This is deemed essential to an IoT solution due to the constantly evolving attacks, technologies and environments. However, this method will only be able to utilise network and not host-based detection, which is considered more reliable and effective within this context. Despite many of the reviewed works have considerable merit with their method of detection, but the solutions suffer from poor architectural underpinnings.

Technology Coverage is a fundamental issue within IoT that drives security-based issues. Through external processing placement and passive probes, which may use wide spectrum and software defined radios, all technology types and protocols may be covered through minimal hardware adaptions. This enables highly adaptable, extensible and software-automated upgrades that were not provided in the reviewed solutions. In fig. 2, the proposed placement of the IDS also illustrates that monitoring of the other IoT layers including wired WAN protocols and those at the application layer. This provides

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2844742, IEEE Communications Surveys & Tutorials

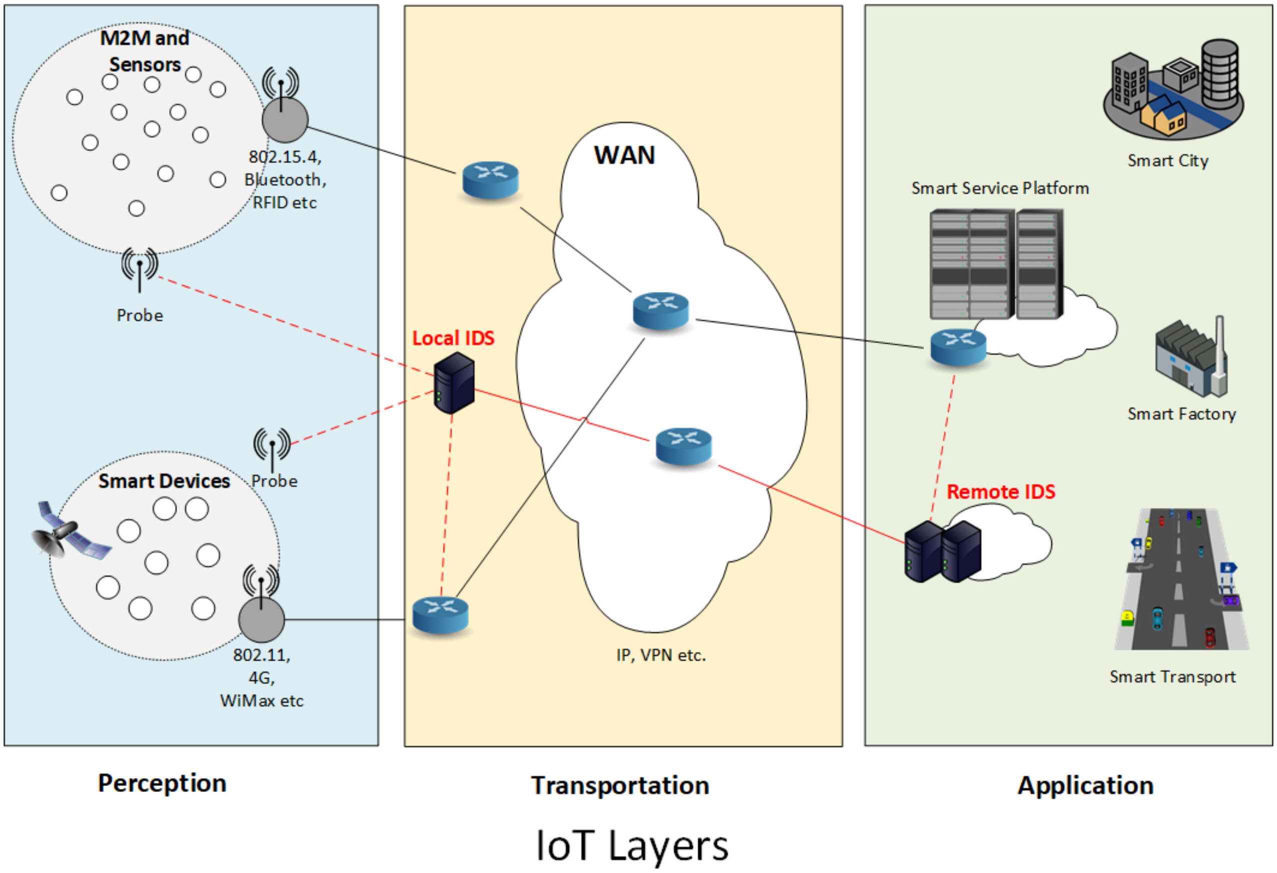

Fig. 2. This diagram illustrates the proposed IDS for IoT which covers all 3 layers of the IoT model. The proposed IDS placement is indicated in red. A local IDS sits close to the perception layer and provides static probes across the sensing environments to receive network data. Simultaneously it probes network traffic heading for the application layer. This data is collaborated with a remote IDS which sits within the application layer and monitors traffic from the service platform.

considerably enhanced coverage than those reviewed in literature. Additionally, through also applying an external IDS the integration of audit logs from multiple areas, (i.e. those covering the transmission and application phases of IoT) can provide a holistic intrusion detection analysis.

B. System Analysis

The ability to retrieve information passively and export it securely for remote processing gives great advantages. In the previous section's simplified example, it was shown that analysis of the data as it is being sent by each node greatly increases this capability. Purely transporting the raw, captured data permits any processing needed through accomplishing this on a remote server.

Many different attack types may be identified at an increased rate, whilst minimising any additional resource load or complexity within the IoT network itself. Overall, this creates a more secure IoT based network, albeit at a greater expense of introducing further hardware and requiring secure links to a remote server. However, as the set of use-cases of the IoT widens and societal infrastructure becomes more intertwined with these systems, this additional cost may outweigh the impact of a potential security breach. A final issue which may occur with such a passive system is, of course, subversion of the sniffer nodes themselves. This may be mitigated by multiple collection nodes which will compare data and secure links back to the remote processing site.

VIII. Conclusion

As interest in the IoT grows, its application will involve more data sensitive projects. As such, ensuring its security is a priority. With preventative measures difficult to implement due to inherent architectural constraints, solutions must turn to 2nd line methods of defence. We examine IDS as one such defence and determine that despite the variety of existing systems available; none are able to defend against all types of attacks (from the physical layer up) due to their architectural implementation. Therefore, we discuss the case that these methods are out-dated whilst not holistically covering the whole IoT model. In order to comprehensively secure IoT based networks built of heterogeneous device types a new approach must be taken. This involves the application of more

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2844742, IEEE Communications Surveys & Tutorials

physical hardware, using network probes to collect data and securely transport it to a remote server (likely cloud-based) so as to perform detection types as resource intensive as required.

Future works should consider full implementations through development of an IDS for IoT, where data processing will be computed upon a cloud system. The system will be tested on a variety of physical hardware to examine the effect of monitoring multiple different protocols in varied environments, upon the data collection and analysis process.

The adoption of IoT based networks is inevitable, with similar systems already seen for monitoring and control of industrial systems (energy, water etc.). It is essential that correct security solutions be found before wide-scale adoption of insecure processes which widely assist modern society. The solution presented here could be considered as a relatively simple one, although further development and research will need to take place to ensure it is optimal in a wide variety of situations.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, pp. 2787–2805, 2010.

[2] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart objects as building blocks for the Internet of things," *Internet Computing, IEEE*, vol. 14, pp. 44–51, 2010.

[3] Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, "Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid," in *Power and Energy Society General Meeting*, 2011, pp. 1–8.

[4] A. H. FathiNavid and A. B. Aghababa, "A protocol for intrusion detection based on learning automata in forwarding packets for distributed wireless sensor networks," in *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2012, pp. 373–380.

[5] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, Feb 2014.

[6] E. Borgia, "The internet of things vision: Key features, applications and open issues," *Computer Communications*, vol. 54, no. Supplement C, pp. 1 – 31, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366414003168

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015.

[8] M. FRUSTACI, P. PACE, G. ALOI, and G. FORTINO, "Evaluating critical security issues of the iot world: Present and future challenges," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–1, 2017.

[9] J. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile, "Ieee 802.15.4: a developing standard for low-power low-cost wireless personal area networks," *Network, IEEE*, vol. 15, no. 5, pp. 12–19, Sept 2001.

[10] S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real-time intrusion detection in the Internet of Things," *Ad Hoc Networks*, vol. 11, pp. 2661–2674, 2013.

[11] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1153–1176, Secondquarter 2016.

[12] A. Abduvaliyev, A. S. K. Pathan, J. Zhou, R. Roman, and W. C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys Tutorials*, vol. 15, no. 3, pp. 1223–1237, Third 2013.

[13] 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, First 2014.

[14] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surv.*, vol. 46, no. 4, pp. 55:1–55:29, Mar. 2014. [Online]. Available: http://doi.acm.org/10.1145/2542049

[15] A. A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure internet of things," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, Aug 2016, pp. 84–90.

[16] B. B. Zarpelo, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in internet of things," *Journal of Network and Computer Applications*, vol. 84, no. Supplement C, pp. 25 – 37, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804517300802

[17] H. Modares, R. Salleh, and A. Moravejosharieh, "Overview of security issues in wireless sensor networks," in *2011 Third International Conference on Computational Intelligence, Modelling Simulation*, Sept 2011, pp. 308–311.

[18] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the internet of things," *IEEE Security Privacy*, vol. 13, no. 1, pp. 14–21, Jan 2015.

[19] M. R. Asghar, G. Dn, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Communications Surveys Tutorials*, vol. 19, no. 4, pp. 2820–2835, Fourthquarter 2017.

[20] D. Eckhoff and I. Wagner, "Privacy in the smart city 2013; applications, technologies, challenges and solutions," *IEEE Communications Surveys Tutorials*, vol. PP, no. 99, pp. 1–1, 2017.

[21] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, Oct 2017.

[22] C. Hennebert and J. D. Santos, "Security protocols and privacy issues into 6lowpan stack: A synthesis," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 384–398, Oct 2014.

[23] Y. Qu and P. Chan, "Assessing vulnerabilities in bluetooth low energy (ble) wireless network based iot systems," in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, April 2016, pp. 42–48.

[24] N. Desai and M. L. Das, "On the security of rfid authentication protocols," in *2015 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, July 2015, pp. 1–5.

[25] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in wpa2," in *ACM Computer and Communications Security (CCS) 2017*, November 2017.

[26] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a review," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[27] Y. Zou, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances and future trends," *CoRR*, vol. abs/1505.07919, 2015. [Online]. Available: http://arxiv.org/abs/1505.07919

[28] M. A. Hussain, H. Jin, Z. A. Hussien, Z. A. Abduljabbar, S. H. Abbdal, and A. Ibrahim, "Dns protection against spoofing and poisoning attacks," in *2016 3rd International Conference on Information Science and Control Engineering (ICISCE)*, July 2016, pp. 1308–1312.

[29] C. Ouseph and B. R. Chandavarkar, "Prevention of mitm attack caused by rogue router advertisements in ipv6," in *2016 IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, May 2016, pp. 952–956.

[30] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle

attacks," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 2027–2051, thirdquarter 2016.

[31] S. Soursos, I. P. arko, P. Zwickl, I. Gojmerac, G. Bianchi, and G. Carrozzo, "Towards the cross-domain interoperability of iot platforms," in *2016 European Conference on Networks and Communications (EuCNC)*, June 2016, pp. 398–402.

[32] G. Cerullo, G. Mazzeo, G. Papale, B. Ragucci, and L. Sgaglione, "Chapter 4 - iot and sensor networks security," in *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*, ser. Intelligent Data-Centric Systems, M. Ficco and F. Palmieri, Eds. Academic Press, 2018, pp. 77 – 101. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128113738000045

[33] R. Dubey, V. Jain, R. S. Thakur, and S. D. Choubey, "Attacks in wireless sensor networks," *International Journal of Scientific & Engineering Research*, vol. 3, no. 3, pp. 1–4, 2012.

[34] D. G. Padmavathi, M. Shanmugapriya *et al.*, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *arXiv preprint arXiv:0909.0576*, 2009.

[35] D. C. Nash, T. L. Martin, D. S. Ha, and M. S. Hsiao, "Towards an intrusion detection system for battery exhaustion attacks on mobile computing devices," in *Pervasive Computing and Communications Workshops*, 2005, pp. 141–145.

[36] K. Xing, F. Liu, X. Cheng, and D. H. Du, "Real-time detection of clone attacks in wireless sensor networks," in *Distributed Computing Systems, 2008. ICDCS'08. The 28th International Conference on*. IEEE, 2008, pp. 3–10.

[37] K. Sharma and M. Ghose, "Wireless sensor networks: An overview on its security threats," *IJCA, Special Issue on Mobile Ad-hoc Networks MANETs*, pp. 42–45, 2010.

[38] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks*, vol. 1, no. 2, pp. 293–315, 2003.

[39] J.-S. Cho, S.-S. Yeo, and S. K. Kim, "Securing against brute-force attack: A hash-based rfid mutual authentication protocol using a secret value," *Computer Communications*, vol. 34, no. 3, pp. 391–397, 2011.

[40] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," *Wireless Communications, IEEE*, vol. 14, pp. 56–63, 2007.

[41] H. E. Poston, "A brief taxonomy of intrusion detection strategies," in *Aerospace and Electronics Conference (NAECON)*, 2012, pp. 255–263.

[42] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proceedings of the Second IEEE International Conference on Computational Intelligence for Security and Defense Applications, Ottawa, Ontario, Canada*, 2009, pp. 53–58.

[43] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer, and B. D. Payne, "Evaluating computer intrusion detection systems: A survey of common practices," *ACM Comput. Surv.*, vol. 48, no. 1, pp. 12:1–12:41, Sep. 2015.

[44] B. Stelte and G. D. Rodosek, "Thwarting attacks on ZigBee - removal of the KillerBee stinger," in *Network and Service Management (CNSM)*, 2013, pp. 219–226.

[45] B. R. Moyers, J. P. Dunning, R. C. Marchany, and J. G. Tront, "The multi-vector portable intrusion detection system (MVP-IDS): A hybrid approach to intrusion detection for portable information devices," in *Wireless Information Technology and Systems (ICWITS)*, 2010, pp. 1–4.

[46] D. Oh, D. Kim, and W. W. Ro, "A malicious pattern detection engine for embedded security systems in the internet of things," *Sensors*, vol. 14, no. 12, pp. 24 188–24 211, 2014. [Online]. Available: http://www.mdpi.com/1424-8220/14/12/24188

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

[48] T. OConnor and D. Reeves, "Bluetooth network-based misuse detection," in *Computer Security Applications Conference*, 2008, pp. 377–391.

[49] K. M. Haataja, "New efficient intrusion detection and prevention system for bluetooth networks," in *Proceedings of the 1st International Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications*, 2008, p. 16.

[50] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. A. Spirito, "Demo: An ids framework for internet of things empowered by 6lowpan," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer &#38; Communications Security*, ser. CCS '13. New York, NY, USA: ACM, 2013, pp. 1337–1340. [Online]. Available: http://doi.acm.org/10.1145/2508859.2512494

[51] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6LoWPAN based internet of things," in *Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2013, pp. 600–607.

[52] T. K. Buennemeyer, T. M. Nelson, L. M. Clagett, J. P. Dunning, R. C. Marchany, and J. G. Tront, "Mobile device profiling and intrusion detection using smart batteries," in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, 2008, pp. 296–296.

[53] K. Yadav and A. Srinivasan, "itrust: An integrated trust framework for wireless sensor networks," in *Proceedings of the 2010 ACM Symposium on Applied Computing*, 2010, pp. 1466–1471.

[54] X. Song, G. Chen, and X. Li, "A weak hidden markov model based intrusion detection method for wireless sensor networks," in *Intelligent Computing and Integrated Systems (ICISS)*, 2010, pp. 887–889.

[55] H. Sedjelmaci and S. M. Senouci, "Efficient and lightweight intrusion detection based on nodes' behaviors in wireless sensor networks," in *Global Information Infrastructure Symposium*, 2013, pp. 1–6.

[56] S. Misra, P. V. Krishna, H. Agarwal, A. Saxena, and M. S. Obaidat, "A learning automata based solution for preventing distributed denial of service in internet of things," in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, Oct 2011, pp. 114–122.

[57] A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, S. Mathur, and A. Ingle, "Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks," in *2013 IEEE International Conference on Computational Intelligence and Computing Research*, Dec 2013, pp. 1–7.

[58] A. Le, J. Loo, K. K. Chai, and M. Aiash, "A specification-based ids for detecting attacks on rpl-based network topology," *Information*, vol. 7, no. 2, 2016.

[59] S. I. Eludiora, O. O. Abiona, A. O. Oluwatope, S. A. Bello, M. L. Sanni, D. O. Ayanda, C. E. Onime, E. R. Adagunodo, and L. O. Kehinde, "A distributed intrusion detection scheme for wireless sensor networks," in *Electro/Information Technology (EIT)*, 2011, pp. 1–5.

[60] C. Liu, J. Yang, R. Chen, Y. Zhang, and J. Zeng, "Research on immunity-based intrusion detection technology for the internet of things," in *2011 Seventh International Conference on Natural Computation*, vol. 1, July 2011, pp. 212–216.

[61] Y. Liu and F. Yu, "Immunity-based intrusion detection for wireless sensor networks," in *Neural Networks*, 2008, pp. 439–444.

[62] L. Coppolino, S. D'Antonio, A. Garofalo, and L. Romano, "Applying data mining techniques to intrusion detection in wireless sensor networks," in *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, 2013, pp. 247–254.

[63] J. P. Amaral, L. M. Oliveira, J. J. P. C. Rodrigues, G. Han, and L. Shu, "Policy and network-based intrusion detection system for ipv6-enabled wireless sensor networks," in *2014 IEEE International Conference on Communications (ICC)*, June 2014, pp. 1796–1801.

[64] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet

of things," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, May 2015, pp. 606–611.

[65] N. K. Thanigaivelan, E. Nigussie, R. K. Kanth, S. Virtanen, and J. Isoaho, "Distributed internal anomaly detection system for internet-of-things," in *2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC)*, Jan 2016, pp. 319–320.

[66] P. Pongle and G. Chavan, "Article: Real time intrusion and wormhole attack detection in internet of things," *International Journal of Computer Applications*, vol. 121, no. 9, pp. 1–9, July 2015, full text available.

[67] D. Shreenivas, S. Raza, and T. Voigt, "Intrusion detection in the rpl-connected 6lowpan networks," in *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*, ser. IoTPTS '17. New York, NY, USA: ACM, 2017, pp. 31–38.

[68] A. Fathinavid and M. Ansari, "Claids: Cellular learning automata based approach for anomaly nodes detection in clustered mobile ad hoc networks," vol. 29, pp. 31–51, 01 2015.

[69] T. Jiang, G. Wang, and H. Yu, "A dynamic intrusion detection scheme for cluster-based wireless sensor networks," in *World Automation Congress (WAC)*, 2012, pp. 259–261.

[70] Z. Yu and J. J. Tsai, "A framework of machine learning based intrusion detection for wireless sensor networks," in *Sensor Networks, Ubiquitous and Trustworthy Computing*, 2008, pp. 272–279.

[71] H. A. Arolkar, S. P. Sheth, and V. P. Tamhane, "Ant colony based approach for intrusion detection on cluster heads in WSN," in *Proceedings of the 2011 International Conference on Communication, Computing; Security, Rourkela, Odisha, India*, 2011, pp. 523–526.

[72] G. Han, J. Jiang, W. Shen, L. Shu, and J. Rodrigues, "Idsep: a novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks," *Information Security, IET*, vol. 7, pp. 97–105, 2013.

[73] K. Gerrigagoitia, R. Uribeetxeberria, U. Zurutuza, and I. Arenaza, "Reputation-based intrusion detection system for wireless sensor networks," in *Complexity in Engineering (COMPENG)*, 2012, pp. 1–5.

[74] A. Le, J. Loo, Y. Luo, and A. Lasebae, "Specification-based ids for securing rpl from topology attacks," in *2011 IFIP Wireless Days (WD)*, Oct 2011, pp. 1–3.

[75] C. I. Ezeife, M. Ejelike, and A. K. Aggarwal, "Wids: A sensor-based online mining wireless intrusion detection system," in *Proceedings of the 2008 International Symposium on Database Engineering; Applications*, ser. IDEAS '08. New York, NY, USA: ACM, 2008, pp. 255–261.