A Review of Security and Privacy within Smart Cities - An Intrusion Detection Perspective

Junaid Arshad, Muhammad Ajmal Azad, Roohi Amad, Khaled Salah, Mamoun Alazab, Razi Iqbal

Abstract—Internet of Things (IoT) forms the foundation of next generation infrastructures, enabling development of future cities that are inherently sustainable. Intrusion detection for such paradigms is a non-trivial challenge which has attracted further significance due to extraordinary growth in the volume and variety of security threats for such systems. However, due to unique characteristics of such systems i.e., battery power, bandwidth and processor overheads and network dynamics, intrusion detection for IoT is a challenge, which requires taking into account the trade-off between detection accuracy and performance overheads. In this context, we are focused at highlighting this trade-off and its significance to achieve effective intrusion detection for IoT. Specifically, this paper presents a comprehensive study of existing intrusion detection systems for IoT systems in three aspects: computational overhead, energy consumption and privacy implications. Through extensive study of existing intrusion detection approaches, we have identified open challenges to achieve effective intrusion detection for IoT infrastructures. These include resource constraints, attack complexity, experimentation rigor and unavailability of relevant security data. Further, this paper is envisaged to highlight contributions and limitations of the state-of-the-art within intrusion detection for IoT, and aid the research community to advance it by identifying significant research directions.

Index Terms—Smart Cities, Internet of Things, Security and Privacy, Intrusion Detection, Performance Evaluation, Computation and Energy overhead

1 Introduction

Cyber-Physical Systems (CPS) are typically highly interconnected systems which are integrated to deliver novel functionalities in diverse disciplines such as healthcare, manufacturing, defence and energy [1]. Evolution of technologies such as 5G, artificial intelligence, and Internet of Things (IoT) has a profound role in this. These advancements have led to development of emerging paradigms such as smart cities, smart grids, and smart factories, which have contributed towards improving the overall quality of life in an efficient and cost-effective manner. Although this is still an emerging area, a number of early applications have demonstrated potential benefits of adopting this technological paradigm. For instance, smart grids enable improved management and maintenance of a countrys electric grid in a cost effective manner by incorporating smart elements throughout the power generation, distribution and consumption chain.

The evolution of smart cities and the role of CPS in this development is underpinned by IoT which are critical in realizing the next generation of infrastructures to develop technological solutions in a sustainable manner. Within this context, the ability of smart devices to communicate using internet connectivity is of fundamental significance, which has enabled IoT to achieve *connected* infrastructures.

- *Junaid Arshad is with Birmingham City University, UK, Muhammad Ajmal Azad is with University of Derby, UK, Roohi Amad is with NED University of Engineering and Technology, Pakistan. Khaled Salah is with Khalifa University, UAE. Mamoun Alazab is with Charles Darwin University, Australia. Razi Iqbal is with University of Engineering and Technology, Lahore, Pakistan.*

However, the open network architecture of IoT has also attracted significant increase in malicious threats for smart infrastructures as identified by [2], [3]. Furthermore, a recent study by Gartner [4] has predicted IoT-based attacks to form 25% of all enterprise attacks by 2020, highlighting the need for distinct protection mechanisms. Due to the proliferation of such devices in almost every aspect of our life, the threats posed due to their insufficient security are unique, as insecure devices expose end users to serious security and privacy threats. For instance, if an attacker is able to compromise an in-car WiFi; in-car devices and data will be at risk. Once inside the car's network, an attacker can spoof the car, connect to outside data sources, and steal the owners personal information including credit card data [5].

In view of such emerging threats, the need to address security challenges for infrastructures underpinning smart cities is paramount [6]. There have been a number of efforts to address different dimensions of security for IoT such as secure frameworks [7], [8], privacy of information [9], and authentication [10]. However, the challenge in the design of an effective secure system is two-fold: firstly, the devices which form these systems are typically resource constrained limiting their ability to implement sophisticated security management system to monitor device activities in real time; secondly, the ad-hoc nature of IoT systems allows devices to connect to other devices at run-time, typically for short time periods, thereby creating a collaborative network. Therefore, efforts to address security challenges for IoT systems should take into account these factors to ensure effectiveness and applicability.

Intrusion detection system (IDS) is one of the fundamental components of a typical security architecture, which provides visibility into the activities of a system, enabling

timely detection and response to any undesired events. An IDS can be categorized into the following main approaches: misuse/signature-based detection systems, behavioural or anomaly-based detection, specification-based intrusion detection, and hybrid intrusion detection systems [11]–[13]. Moreover, intrusion detection can be performed at the network or host level typically driven by the security policy of the monitored system. In recent years, IDS for IoT have received increased attention with number of notable efforts such as [14]–[17]. Within this context, the focus of our research is to investigate novel challenges to achieve efficient intrusion detection for IoT systems and explore potential solutions to address them. In particular, we emphasize the challenge of intrusion detection efficiency with respect to performance metrics such as CPU, energy and bandwidth utilization, and the trade-off with measures, such as detection accuracy, false positives and false negatives. This paper presents outcomes of our study of the state-of-the-art with respect to intrusion detection within IoT, identifying limitations of current approaches and highlighting future directions.

1.1 Scope of Survey and Contributions

Our research has identified existing efforts to study the state of the art for intrusion detection within IoT systems with [18], [19] and [20] being the most notable efforts. Although these efforts present a structured analysis of existing literature within IoT intrusion detection domain, these share a significant limitation in being agnostic of the performance overhead and privacy implications. For instance, using the *interaction ability* proposed by [18], Jun and Chi [21] scores high (three) indicating its efficiency to protect an IoT system. However, a deeper analysis of the system highlights that it is remarkably CPU intensive, which will affect its suitability for an IoT system. A detailed analysis of existing studies into intrusion detection for IoT is presented in section 2. In view of these limitations, we undertake rigorous analysis of the intrusion detection systems taking into account a number of performance metrics to present an exhaustive evaluation of existing approaches for intrusion detection in IoT systems.
In view of the limitations of existing studies, this paper makes following contributions:

- A comprehensive attack model for IoT systems is presented that is envisaged to inform state of the art for intrusion detection within IoT. The attack model comprises of threats across different dimensions of an IoT system aiming to aid improved classification.
- An extensive review of efforts with respect to intrusion detection for IoT systems is conducted. Extending the state of the art, this paper takes into account critical attributes, such as performance overhead and privacy implications.
- Identification of open challenges to achieve effective intrusion detection for IoT systems. This is informed by extensive review and analysis of existing intrusion detection research within IoT systems, and highlights significant research directions.

Rest of the paper is organized as follows: Section 2 includes a detailed discussion about the existing surveys of intrusion detection research within IoT highlighting unanswered questions. Section 3 introduces a comprehensive attack model for IoT systems. Extensive review of existing literature within intrusion detection for IoT is presented in Section 4 which is organized into different types of IDS and therefore provides a linkage with classification introduced in Section 3. Section 5 presents privacy implications of intrusion detection systems followed by 6, which provides a thorough analysis of the existing literature with respect to a number of attributes including intrusion detection and performance efficiency. Through the findings of our research, section 7 discusses open challenges which require further attention followed by conclusions and future aims of our research in section 8.

2 Existing Surveys Of Intrusion Detection for IoT

With the evolution of IoT and its application, the volume and variety of attacks for such systems have increased requiring dedicated efforts to investigate intrusion detection systems for IoT systems. Furthermore, IoT paradigm shares similarities with concepts, such as Mobile Adhoc Networks (MANETs) and Wireless Sensor Networks (WSN). Consequently, a number of studies have been performed to review state of the art within intrusion detection for these paradigms. For instance, [22]–[24] presented state of the art with respect to IDS for the MANETs, whereas [25], [26] have reviewed existing IDSs for WSNs. However, our focus in this paper is solely on the intrusion detection approaches for the IoT system taking into account unique characteristics of this paradigm.

Our research has identified [18], [19], [20], and [27] as existing efforts to review literature related to intrusion detection for IoT. A comprehensive analysis of these surveys is discussed below and summarized in Table 1, which also highlights limitation of these efforts to take into account performance overheads of existing intrusion detection approaches for IoT.

Gendreau et al. [18] defined a term called *Interaction Ability* of an IDS to assess the level of holistic detection intelligence. This parameter is defined as the ability of an IDS to interact with different service layers within the system i.e. Network Interface, Internet, Transport and Application layers with maximum achievable interaction ability score as four. Authors have attempted to review seven recent intrusion detection systems against the interaction ability metric to identify respective efficiency. Although interaction ability is a useful indicator, however, we believe the IoT intrusion detection landscape requires rigorous analysis of existing efforts. For instance, one of the unique features of IoT systems is their resource constraints and interaction ability is agnostic of this significant characteristic. For instance, although Jun and Chi [21] scores high (three) for interaction ability, indicating its efficiency to protect a IoT system however, a deeper analysis of the system highlights that it is remarkably CPU intensive which will affect its suitability for a typical IoT system.

Zarpelao et al. [19] presented a recent survey of IDS research efforts for IoT aiming to identify leading trends, open issues, and future research possibilities. The authors

Survey ID	Detection Approaches	Review Criteria	Performance Efficiency Considered
Gendreau et al [18]	Rule and Anomaly-based	Holistic Detection Intelligence	No
Zarpelao et al. [19]	Anomaly, Signature and Hyrbid	Security Threats & Validation Strategies	No
Chaabouni et al [20]	Network-based IDS	Threats, Placement, Validation Strategies	No
Kiennert et al. [27]	Game Theory-based IDS	TPR, FPR, FNR, TNR	No
This Study	Anomaly, Signature, Specification & Hybrid	Security and Performance Metrics	Yes

TABLE 1: Analysis of existing reviews of IDS for IoT

classified existing intrusion detection efforts based on detection method, IDS placement strategy, security threat and validation strategy. Although the authors present a comprehensive system to analyze existing intrusion detection efforts, however, similar to [18], this effort is agnostic of the performance overhead of intrusion detection systems. Chaabouni et al [20] presented a multidimensional review of efforts to achieve effective network based IDS for IoT. The study is significant as it presents a comparative review of existing NIDS tools and datasets available, which can help IoT security practitioners to evaluate different tools available. Furthermore, the authors have presented a brief review of select academic efforts for NIDS however the review is focused on security characteristics of these systems with limited coverage of literature and performance metrics.

In addition to the above, Kiennert et al. [27] studied game-theoretic approaches to intrusion detection within IoT systems, highlighting limitations of using game theory and Markov decision processes to perform effective intrusion detection. Authors conducted a comparative study of existing intrusion detection approaches analyzing metrics, such as true positive, false positive, true negative and false negative to assess the performance of the individual schemes. As with the other studies discussed earlier, authors do not take into account the performance characteristics of intrusion detection systems and therefore do not address the gap highlighted in this paper.

In summary, although existing surveys of intrusion detection for IoT highlight advancements and open challenges, these do not consider performance efficiency of IDS for IoT which is significant due to limited resources for these devices, such as CPU, memory, storage, bandwidth and battery. This paper is focused at addressing this gap and presents a thorough analysis of existing IDS efforts for IoT taking into consideration performance metrics, such as energy consumption, RAM, and CPU usage for these efforts.

3 Security Threats for IoT Systems

Although IoT is an emerging paradigm, a significant part of the software stack used by the IoT applications is adopted from existing software paradigms. This is also evident from the concept of integrating IoT specific stack (for instance, specific to Zigbee, 6LoWPAN and RPL) with the existing Internet infrastructure, such as IPv5 and IPv6. This has significant implications with respect to the attack surface for IoT infrastructures as it is not restricted to the threats specific to the new routing protocols, such as 6LoWPAN and RPL but also includes threats to existing infrastructure, such as IPv6, application specific attacks and attacks specific to the physical media, such as the radio spectrum. We present a taxonomy of different attacks for a typical IoT system and summarize in Fig 2.

3.1 Routing-specific threats

Routing information in an IoT system can be modified or spoofed in order to route the traffic in a malicious manner or to launch a further attack on the IoT network. These attacks are the most common in resource-constrained IoT networks. The most relevant routing attacks in IoT include the following:

Rank attack: A defining characteristic of 6LoWPAN networks is the use of ranking to establish optimal routing path. Within this context, *Node Rank* indicates the quality of the path from a node to the sink node. Every time a node updates its rank or preferred parent, it is required to inform other nodes by sending the updated information in the next Directed Acyclic Graph (DAG) Information Object (DIO). RPL uses the Rank rule i.e. *a node in the parent should always have lower rank than its children to prevent the loop creation*. In this way, the rank enables creating optimal topology, preventing loop creation and managing control overhead [28]. As identified by [28]–[30] the rank information can be maliciously tampered with by an attacker such that it chooses the node with worst Rank to be its parent. This will therefore result in disturbing the topology of the network, thereby causing delays in normal transmission.

Wormhole attack: A wormhole can be considered as a tunnel between two nodes using wired or wireless links and can be used to achieve faster transmission rates or dedicated connection between such nodes. As such, wormhole has legitimate applications, such as the connection between the local and global IDS modules within our architecture. However, wormhole can be used by an attacker to create a dedicated tunnel with a node on the Internet as identified by [31]. Wormhole attack is not novel to the IoT systems and has been historically identified as a potential threat for wireless sensor networks by [32]–[34].

Sinkhole attack: The objective of a sinkhole attack is to attract traffic through a designated node using illegitimate information making the node a lucrative routing sink (base station within a wireless network). As with the wormhole attack, literature around sinkhole attack is well established with [35] being an initial effort to identify and mitigate against such attack. Creating a sinkhole does not necessarily disrupt legitimate transmission within a 6LoWPAN, however, by diverting the traffic through a specific route creates opportunities to launch other attacks, such as wormhole and selective forwarding attack described below.

Selective forwarding attack: With selective forwarding attack, a malicious node attempts to disrupt legitimate

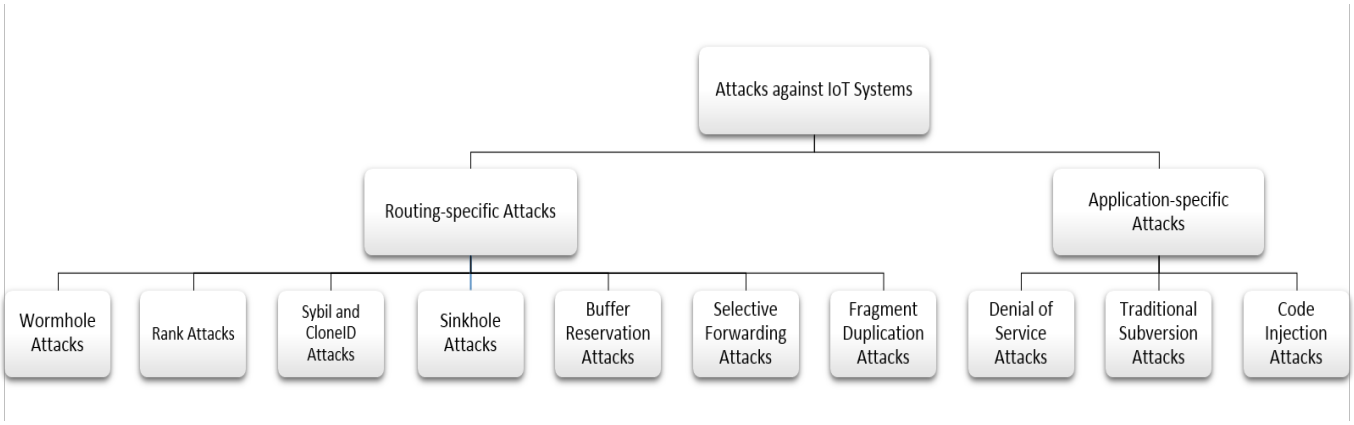

Fig. 1: A Taxonomy of attacks for IoT systems

transmission and routing path. The malicious node in this case attempts to block certain packets and forward selected packets, thereby affecting the routing to fulfil malicious objectives. For instance, an attacker can forward all RPL control messages but block the remaining messages [31]. As can be inferred, this attack can cause more damage when used in conjunction with sinkhole attack. Consequently, such dependencies among different attack types has motivated us to explore the impact of multi-stage attacks within IoT infrastructures with our initial efforts in this respect presented in [36].

Fragment duplication attack: The fragment duplication attack leverages a weakness within the 6LoWPAN layer with respect to how fragmented packets are received and assembled by an IoT node. Due to the integration of 6LoWPAN with IPv6 networks, larger packets supported by IPv6 have to be fragmented into smaller packets so as to be effectively processed by the resource-constrained nodes within an IoT system. However, as identified by [37], a recipient node cannot verify if two fragments of a packet were sent by the same source, therefore, the recipient node is unable to distinguish between legitimate and spoofed fragments. A malicious node can exploit this vulnerability to block reassembly of targeted packets, such as connection establishment packets. This may result in disrupting legitimate traffic as well as consuming resources available to the victim node.

Buffer reservation attack: The buffer reservation attack is closely linked to the fragment duplication attack and may be caused as a consequence of a successful fragment duplication attack. The buffer reservation attack also targets the vulnerability in the fragmentation mechanism employed by 6LoWPAN networks. As identified by [37], it leverages the fact that the recipient of a fragmented packet is unable to determine if all fragments will be received correctly. Therefore, a recipient node reserves a buffer space based on the information provided in the 6LoWPAN header with any additional fragments discarded. Taking advantage of this setting, a malicious node can send a victim single *FRAG1* to reserve arbitrary buffer space thereby consuming scarce memory of the resource-constrained node.

Sybil and clone ID attack: Sybil and Clone ID attacks are similar in that the objective of the attacker is to use spoofed logical identities within a network without deploying physical devices. In particular, for Clone ID attack, an attacker aims to use a victims logical identity within the network whereas in Sybil attack, the attacker aims to assume multiple logical identities within a network without deploying physical nodes. These logical identities may not be currently present in the network. A number of existing efforts, such as [31], [35] have identified these attacks for IoT and historically for wireless sensor networks.

3.2 Application specific threats

Although routing forms an essential component of the IoT system, the IoT devices are expected to run application software required by the function envisaged to be performed, such as temperature monitoring and supply chain management. We categorize these threats as application specific and present them below.

Denial of Service attack: Historically, Denial of Service (DoS) attacks are targeted at making the victim unavailable for legitimate service. This can be achieved by flooding the victim with extraordinarily large volume of requests or by exhausting resources, such as memory and computational power available to the victim. Within IoT, the threat of DoS attack is two-fold; the victim can be part of the network under threat that an attacker wishes to make unavailable, or the victim can be used as a zombie to launch a Distributed DoS (DDoS) on a target IoT network. In this context, Botnet attacks targeting IoT devices have recently attracted significant attention with Mirai [38] the pioneer Botnet attack. The significance of these threats within IoT systems have been identified by [39]–[41].

Malicious code injection: As identified by [40], [42], malicious code injection is another application specific threat to IoT systems. The attacker, in this case, attempts to inject malicious code to get privileged access to the victim. Consequently, the attacker can damage the normal operation by causing threat to the data or to the network using one of the routing specific attacks described in the previous section.

3.3 Traditional attacks

In addition to the above mentioned attacks, IoT systems are vulnerable to the existing attacks targeted at computer systems, such as message interception, fabrication, modification, subversion and phishing. As with the routing-specific attacks, these attacks can also form a part of a more complicated/sophisticated attack and therefore require efforts to protect against them.

4 State of the art in IDS for IoT

Through our research, we have identified that intrusion detection research for IoT systems can be categorized into: Anomaly, Signature, Specification, Hybrid, and Game-based models. Therefore, we present review of existing efforts using these categorization. In doing so, we summarize leading efforts for each category of intrusion detection which can indicate the cutting-edge within that domain.

4.1 Anomaly-based approaches to intrusion detection

With the notable advancements within the domains of artificial intelligence, machine learning and deep learning, anomaly-based approaches have been increasingly used for intrusion detection in general and for IoT in particular. Nobakht et al. [43] proposed a host-based IDS using Software Defined Technology (SDN) for smart homes. The authors have defined three basic requirements for an efficient IDS for IoT i.e. unobtrusive approach, negligible overheads, and scalability. The proposed approach uses sensors to host the intrusion detection module, which is envisioned to monitor network traffic visible at an IoT device. The detection can be performed using a choice of detection modules i.e. signature, anomaly or specification-based techniques. The authors claim that hosting the intrusion detection module within an IoT device reduces the communication overhead, however, it increases the processing overhead at the IoT device, which is critical for such low powered devices.

In [44], Chordia and Gupta proposed an anomaly-based IDS aiming to reduce false alarm rates and increase detection efficiency using data mining techniques. The proposed system aims to monitor network traffic and uses techniques, such as K-NN, K-Means and Decision Table Majority Rule-based scheme focusing on U2R ,R2R ,DoS and Probe attacks. The authors have used KDD99 dataset to evaluate the effectiveness of the approach, which highlights the unavailability of security events data from an IoT system to aid more rigorous and proportionate evaluation of IDS systems for IoT.

Khan and Herrmann [45] proposed intrusion detection for IoT via a trust management mechanism that collects information about neighboring devices and their reputation. The authors investigated patterns of normal use for the RPL protocol using these to devise trust among the IoT devices and the edge routers. The trust management algorithms devised as part of this approach aim to develop trust and reputation values, which are used to protect against routing-specific attacks, such as sinkhole, selective forwarding and version number. Similarly, [46] proposed a distributed IDS where each node monitors the working of nearby nodes for any abnormal activity. If some abnormality is detected, its packets are blocked and problem is reported to the parent node or root node by Distress Propagation Object (DPO). The system has three subsystems i.e. Monitoring and Grading Subsystem (MGSS), Reporting Subsystem (RSS) and Isolated Subsystem (ISS), which enable collaboration between an IoT device and edge router to facilitate IoT threat detection effectively.

Zhang et al. [47] proposed a hierarchical and distributed IDS (SGDIDS) that is focused at protection against cyber-physical attacks for smart grids systems. The proposed system leverages classification algorithms, such as support vector machine (SVM) and artificial immune system (AIS) in order to determine occurrence of an attack, its type, and its origin in the communication system. The SGDIDS shares some similarities with a typical IoT network in that an IoT network can be divided into two levels i.e. IoT devices and the edge routers with the possibility to adopt SGDIDS approach for a hierarchical IDS. Furthermore, the attack surface for smart grids overlaps significantly with that for a typical IoT network therefore the results of this research are relevant within a generic IDS for IoT.

[15] presented a network anomaly-based model for intrusion detection and two tier classification model, which is proposed to be used in IoT backbone networks. The authors have focused on two specific attack types i.e. User to Root (U2R) and Root to Local (R2L) demonstrating high detection accuracy with low false positive rates primarily due to introduction of a refinement feature and decreased computational complications. The authors have used both supervised and unsupervised reduction techniques, such as Linear Discriminant Analysis LDA(supervised) and Principal Component Analysis PCA (unsupervised), where PCA is used for feature selection and extraction, and LDA provides fast and efficient IDS. In [48], Summerville et al. presented a deep packet anomaly detection system involving feature selection conducted by pattern matching. The authors focused on two Internet-enabled devices i.e. a weather station and an interactive networked video camera, which simulate as sensor and actuator respectively. The evaluation of the approach demonstrated that the sensor was able to detect 99.9% of abnormal packets whereas IoT actuator demonstrated 92.9% detection accuracy.

A user-centric approach is proposed in [49] consisting of two major blocks i.e. a habit-based approach for anomaly detection system and semantic-based firewall for access control and security during communication. The authors consider use of IoT devices within a private setting, such as home networks with devices, including a wrist bracelet, a connected light bulb and a smart TV to model various user behaviours. Within this context, the authors focus on the personal data collected and communicated by the devices. The authors do not discuss details of the detection accuracy, performance efficiency, visibility for the intrusion detection and its placement. Yang et al. [50] propose using Bayesian Spatial Temporal (HBST) model to achieve effective and timely detection of a compromised node at an early stage. The system achieves high detection rate and low false positives rates with low detection samples.

As with other domains of computer and information security, recent efforts for intrusion detection have also attempted to leverage advancements in machine learning and artificial intelligence to improve efficiency and accuracy of the detection process. In this regard, Meidan et al. [51] present one of the first efforts focusing on protection against the IoT botnets which are one of the emerging threats for IoT systems. The authors use deep learning autoencoders to establish an anomaly detection engine which is evaluated against two major botnets i.e. Mirai and BASHLITE. With respect to placement of the IDS, authors use a hybrid approach where by a central unit coordinates with device level encoders (each encoder is responsible for profiling

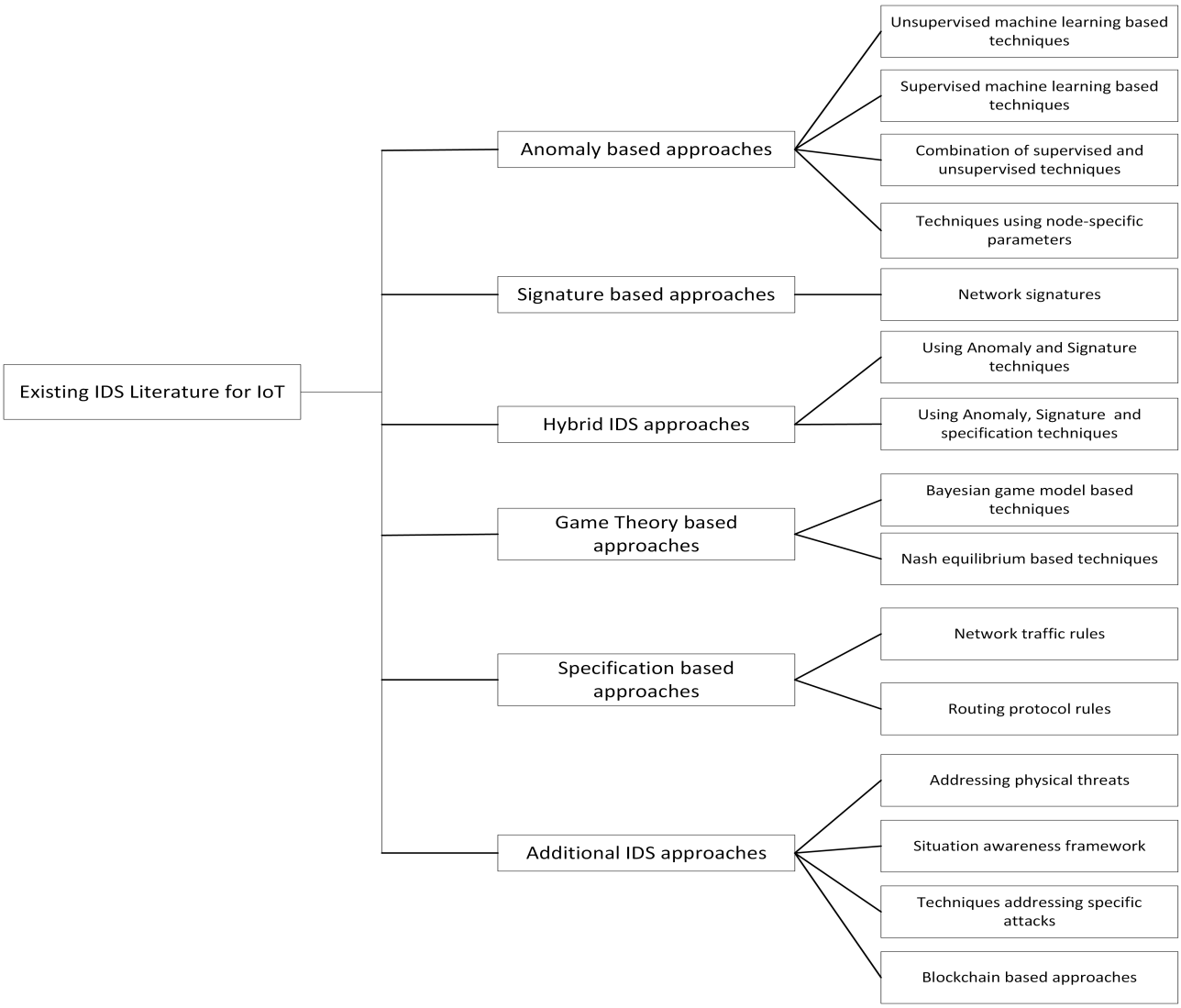

Fig. 2: Categorization of IDS for IoT systems

individual IoT device).

Similarly, authors in [52] use deep learning to achieve effective detection of IoT botnets. Furthermore, both approaches are similar in that they use patterns within network traffic to discover anomalous behavior representing infection caused by botnets. In terms of placement of the intrusion detection system, the authors have adopted a network-based approach employing deep packet inspection techniques. Moreover, Pandu et al. [53] presented an effort to achieve efficient intrusion detection and prevention for IoT systems. Authors have proposed an integrated system for detection and response with specific attention on directing attacks, such as hi surge, sinkhole and wormhole attacks. Although the proposed system has been implemented with Contiki, evaluation results especially with respect to performance efficiency are not available.

4.2 Signature-based approaches to intrusion detection

Signature-based techniques for intrusion detection are well-established especially for conventional computing systems. However, one of the critical factors for effectiveness of such schemes is the availability of trustworthy dataset simulating patterns/signatures of misuse, which has proved to be a challenge for IoT systems. In this respect, Kasinathan et al. [54] presented an IDS framework for 6LoWPAN focusing on detecting denial of service attacks by monitoring physical parameters of the device. The proposed IDS leverages existing IDS (Surricata) and monitors network traffic for both signatures and abnormal behaviour to identify malicious users to detect flooding attacks with an increased detection rate.

Forzin et al. [55] proposed leveraging Snort, a contemporary signature-based NIDS, to establish a portable, easy to use intrusion detection for IoT networks. The resultant IDS is packaged within a Raspberry Pi so it can be transported with the device, enabling it to work in collaboration to achieve detection of sophisticated attacks, such as those targeting network topology. Under this setup, an IDS node can request data captured by neighboring nodes to perform rigorous analysis and reduce false positives. In view of the increasing threats for IoT systems with respect to volume and sophistication, this observation will be crucial to an effective intrusion detection for IoT systems. Indre and Lemnaru [56] proposed a modular architecture for intrusion detection, which utilizes detection techniques, such as

signature, anomaly and specification-based systems with network traffic to achieve effective detection. In particular, signature-based detection uses rules based on packet headers whereas anomaly-based detection aims to identify abnormal data patterns, and specification-based detection focuses on botnet detection. However, the proposed approach envisages intrusion detection at the edge router level which compromises visibility of the system.

4.3 Game-based approaches to intrusion detection

Wang et al. [57] proposed an attack-defence game model to detect malicious nodes using repeated-game approach. The authors claim to have developed a tree model, which is used to formulate an optimal solution to the error detection problems focusing on the detection strategy and performance overhead for individual IoT devices. This is achieved by developing a repeated game method where attackers and defenders can alter strategies to achieve maximum pay-offs. The authors do not discuss challenges, such as placement of the IDS module, type of the detection engine and the level of visibility, which can contribute towards the overall effectiveness of an IDS for IoT networks.

La et al. [58] proposed a honeypot-based approach to improve defence against malicious attempts within an IoT infrastructure. In order to strengthen the defence, authors proposed using a game theoretic model with the defender using honeypot to deceive the attacker. The proposed system focuses on scenarios where the attacker is not known to the defender, therefore, the system does not take into account attempts, such as Rank Attack, which can be initiated by an insider node known to the system. The proposed system is designed and implemented in isolation to the specific challenges and requirements of the IoT infrastructures, such as the resource constraints, interactions between different IoT devices and the positioning of the system. The authors presented experimentation performed in Matlab, which models the overall concept of the system. We believe this to be a limitation, as an effective intrusion detection mechanism for IoT systems should ideally take into account the unique characteristics of such systems as those explained above.

4.4 Specification-based approaches to intrusion detection

Fu et al. [59] propose an IDS for Internet of Vehicles (IoV) i.e. an open and integrated network system connecting human intelligence, vehicles, things, environments and the Internet. Authors explain fundamental requirements for an IDS for IoV i.e. host protection via detection, constrained resources, and real-time detection. Through our research, we have identified these characteristics to be shared by a typical IoT system. Due to these requirements, conventional IDS is not feasible for IoT as it incurs significant overhead with respect to required resources and processing time. In order to fulfil these requirements, an FPGA-based IDS is proposed by [59] which can work in real time, however, it limits versatility of the approach as it is unclear if the system can be translated for other hardware. In [60] a Complex Event Processing (CEP)-based approach to intrusion detection for IoT is proposed with the aim to provide low latency and real time processing of security events. Although the use of CEP for intrusion detection is not novel, it is rather innovative concept within intrusion detection for IoT and this work can be considered as a means to assess the feasibility of CEP within IoT. The proposed system is developed as a rule-based IDS which collects network traffic data from the edge router, extracts events from this data and performs intrusion detection. Although the discussion of the approach is not detailed, we believe CEP can be explored further to address sophisticated or coordinated attacks within IoT which are a combination of simple attack steps.

Amaral et al. [61] present a network-based intrusion detection system for Internet-connected WSN which share close similarities with a typical IoT network. The authors adopted a distributed approach to their design in that the IDS is deployed as a module on randomly selected devices called *watchdogs* over a WSN, reporting to a centralised Event Management System (EMS). Although the IDS module is deployed on individual devices, it only monitors network traffic visible at the node. However, as the watchdogs devices are heterogeneous in location and function, this may have an impact on the types of threats encountered at a specific device. Therefore, each watchdog device is pre-configured with custom monitoring rules, which are designed to detect specific threats expected to be encountered by a device. We believe that the distributed approach adopted by the authors is symmetric with the inherent characteristics of a typical IoT network, however, the role of EMS is limited to information collection limiting its ability to monitor the overall state of a network and to detect coordinated attacks.

Le et al. [62] presented one of the early efforts to establish an IDS for IoT where authors proposed a host-based IDS for LoWPANs using Contiki OS and 6LowPAN [63], [64]. The proposed IDS is able to perform detection based on the information at the node-level which is transmitted to a centralized system for further analysis. The proposed system limits detection to events monitored at the individual devices and does not demonstrate effective detection under DDoS attacks, which not only overwhelm the device but also congest the communication channel between nodes and the centralized system.

Mudgerikar et al. [65] is one of the recent attempts to achieve intrusion detection for IoT where authors present an interesting approach which is similar to COLIDE project [17], [36] in that both advocate collaboration between sensor and edge devices to achieve effective intrusion detection. Authors have presented details of their implementation of the host component, which performs behavioral analysis to identify malicious attempts represented by the system calls executed by processes within a device. Although authors recognize the significance of performance costs for IoT devices, the evaluation reports performance in terms of computational costs, which does not provide in-depth insight into the performance efficiency of the proposed scheme. Sharma et al. [66] has proposed a specification-based approach for IoT intrusion detection aiming to protect against zero-day attacks. The authors argue that by using a specification-based approach, the proposed IDS achieves higher detection accuracy as well as performance efficiency (memory and communication overhead) whilst achieving

protection against previously unknown attacks. Although the authors have presented detailed analysis of their approach as well as performance with respect to detection accuracy, FPR and FNR, however, they have not included metrics to demonstrate performance efficiency of the proposed IDS.

TABLE 2: Comparative analysis of existing IDS approaches for IoT

Paper	Visibility	Time	Detection Engine	Architecture	Performance Overhead	Attack Types	Detection Performance	Scalability
Midi et al. [14]	Network	Offline	Hybrid	Collaborative	CPU usage:0.19%, RAM usage (KB)=13978.62%	ICMP Flooding, SMURF	Detection Rate: 91%, Accuracy: 100%	Yes
Fu et al. [59]	Network	Realtime	Specification-based	Distributed	Latency: 4.12us, power consumption: 7.5w	Buffer overflow, probing, finger printing	Not available	Yes
Kasi.et al. [54]	Network	Offline	Signature-based	Distributed	Not available	DoS	Accuracy:100%	Limited
Forzin et al. [55]	Network	Combined	Signature-based	Distributed	CPU usage: 100% for 70Mb/s, RAM usage: 475MB	IP Spoofing	Not available	Limited
Nobakth et al. [43]	Host	Realtime	Hybrid	Distributed	Not available	Masquareding	Accuracy: 94.25%, Recall: 85.05%	Limited
Chordia et al. [44]	Network	Offline	Anomaly-based	Centralised	CPU usage: 49%	U2R, R2L, DoS, Probe	Accuracy: 95.55%, Detection rate: 93.67%, FPR: 0.019	No
Jun et al.[60]	Network	Realtime	Specification based	Centralised	CPU usage: 48%, RAM usage: 684MB, processing time: 368ms	Generic	Not available	No
Khan et al. [45]	Network	Offline	Anomaly-based	Distributed	Not available	routing-specific attacks: sinkhole, selective forwarding and version number	For 300 nodes: FNR=26%, FPR=47%, Detection Rate= 50%	Yes
Indre et al. [56]	Network	Offline	Hybrid	Centralised	Not available	Probing and DoS	Detection Accuracy=98.4%	No
Thani. et al. [46]	Network	Offline	Anomaly-based	Distributed	Not available	Neighbouring node discrepancy	Not available	Yes
Amaral et al. [61]	Network	Offline	Specification based	Distributed	Not available	Signature mismatching	Not available	Yes
Zhang et al. [47]	Network	Offline	Anomaly-based	Distributed	Not available	DoS, U2R, R2L	FPR: 0.67, 0.7 and 1.3. FNR: 2.15, 21.02, 26.32%	Yes
Haddad et al.[15]	Network	Offline	Anomaly-based	Centralised	Not available	U2R and R2L	Detection accuracy: 81.97% and FPR: 5.44%	No
Summ. et al. [48]	Network	Offline	Anomaly-based	Distributed	Not available	Worm propagation, tunneling, SQL code injection	Detection accuracy: 100%	Yes
Tamani et al. [49]	Network	Offline	Anomaly-based	Distributed	Not available	Privacy Threats	Not available	Yes
Wang et al. [57]	Network	Offline	Game theory	Distributed	Energy consumption: avg 2.0J for 300 nodes, Energy consumption: avg 2.0J for 300 nodes	Not available	Detection accuracy: avg. 80%	Yes
Yang et al. [50]	Network	Offline	Anomaly-based	Not available	Energy consumption: 8,48mJ		Not available	Not available
Sedje. et al. [67]	Network	Offline	Hybrid	Distributed	Efficiency: 2s, energy consumption: approx 3000 mj for 300 nodes	DoS	Detection accuracy 92% for large number of nodes. FPR: 3%	Yes
Raza et al. [16]	Network	Realtime	Hybrid	Distributed	efficiecny: ¿150000mj for 64 nodes	sinkhole and selective forwarding attacks	TPR: approx 80% for 30 nodes on avg.	Yes
Le et al. [62]	Network	Realtime	Specification-based	Hybrid	energy consumption: 202J, power consumption: 6.3% increase (1.2mW)	Rank, sinkhole and neighbour attacks	TPR: 100%, FPR: aprix: 3% avg	Yes
Mayza. et al. [68]	Network	Offline	Other	Distributed	Not available	version number attacks	FPR: 0% for some simulations	Yes
Arshad et al. [69]	Both	Offline	Hybrid	Collaborative	energy consumption: avg 8.5mW for 1, 10, 100 and 1000 packets/sec	Generic	Not available	Yes
Meidan et al. [51]	Network	Offline	Anomaly-based	Distributed	Not available	Botnets	TPR: 100%, FPR: 0.007,	Yes
McDermott et al. [52]	Network	Offline	Anomaly-based	Centralized	Not available	Botnets	Detection Accuracy: Mirai: 99%, UDP:98%, DNS: 98%	No
Pandu et al. [53]	Network	Offline	Anomaly-based	Centralized	Not available	hi surge, sinkhole & wormhole attacks	Not available	No
Mudgerikar et al. [65]	Host	Offline	Specification-based	Distributed	Defined as High, Medium & Low Computational Costs	Multiple IoT attacks	Ranging between 79% and 100% for different modules	Yes
Sharma et al. [66]	Network	Offline	Specification-based	Centralized	Not available	zero-day attacks	Avg. FNR: 0.137. Avg. FPR: 0.045, Avg. TPR: 0.863	Limited
Li et al. [70]	Network	Offline	Feature Extraction	Centralized	Not available	DoS, U2R, R2L, Probe. Using KDD99 Data	DoS: 99.91%, Probe: 96.63%, R2L: 83.33%.	Not available
Bassey et al. [71]	RF Traces	Offline	RF Signatures	Centralized	Not available	Device impersonation	AMI: 0.56 to 0.79, Rand Index: 0.41 to 0.70	Not available

4.5 Hybrid approaches to intrusion detection

In addition to the approaches discussed earlier, current literature in this domain also includes efforts which combine multiple different approaches to achieve effective detection. In this respect, Midi et al. [14] proposed a self-adapting, knowledge-driven expert Intrusion Detection System (KALIS) which can improve its performance after evaluating its efficiency. It is focused on network features and its protocols to improve detection efficiency. KALIS automatically collects the information about the features and configures most suitable detection technique. All the KALIS components run independently with support for a wide variety of mediums and related protocols. The attacks considered by KALIS are variants of DoS attacks i.e ICMP Flood and SMURF which produce similar symptoms i.e. high amount of ICMP Echo Reply Messages directed to affect the machine.

Sedjelmaci et al. [67] proposed a hybrid approach for intrusion detection within IoT, which combines signature and anomaly-based techniques to achieve effective detection. The authors adopt a game theoretic approach based on Nash Equilibrium (NE) to determine the equilibrium state in which the IDS agent will activate its anomaly detection technique to train, classify and build a rule related to a new attacks signature. Furthermore, with respect to placement of IDS, both the signature and anomaly-based detection systems are based on individual IoT devices. The authors explain this decision to be motivated by the objective to reduce the communication overhead based on the assumption that the communication overhead is more resource-hungry as compared to computational overhead. However, this is expected to have significant computational overhead in the case of zero day attacks. Furthermore, the proposed system is limited in its visibility to the events occurring on the individual nodes and therefore limits its ability to effectively detect of sophisticated attacks which may be composed of multiple steps.

Raza et al. [16] proposed Svelte which is a lightweight hybrid intrusion detection system focused on Routing attacks, such as Spoofing, Sinkhole and Selective Forwarding. Svelte has three main modules i.e. 6LoWPAN Mapper (6 mapper), Intrusion Detection component and Distributed Mini Firewall. Although Svelte presents a hybrid approach, however, there are considerations that should be taken into account. For instance, although anomaly-based intrusion detection systems have the advantage of better detection accuracy for zero-day attacks, they are typically resource-hungry which can be a bottleneck when implementing them on resource constrained IoT devices. Furthermore, known attacks such as Rank attack, Sinkhole and spoofing are well established leading to an established signature for their detection. However, attacks such as multi-stage or zero-day require analysis from a wider perspective, analyzing behavioral and usage patterns which makes a case for using anomaly-based IDS. Therefore, an IDS for IoT should take these factors into consideration when making choices, such as the type of IDS, placement and the visibility of the data.

Arshad et al. [69] presents a recent effort to address intrusion detection for IoT systems particularly focusing at the constrained resources available at the IoT devices. The authors presented a collaborative approach where IDS modules are implemented at both device and edge-router level to improve visibility, detection rate and to reduce false positives. The authors propose signature-based IDS at the node level due to its performance efficiency and anomaly-based detection at the edge-router to enhance the detection accuracy. The approach is novel in that it proposes a innovative solution to achieve high detection accuracy whilst taking into account the limited resources available at the sensor devices.

4.6 Additional intrusion detection efforts within IoT

The resource constraints in general and the limited available of power in particular are one of the challenges for any IDS within IoT. To this end, Gendreau [72] seek to address this challenge by using an enhanced measurement of situation awareness in the IoT. The authors highlight the importance of awareness of state of monitoring system and propose a framework to enhance the energy efficiency of a self-reliant management and monitoring WSN cluster head selection algorithm. Although the experimental results demonstrate positive results for the approach, however, it is limited to assessing the energy efficiency for a cluster head selection algorithm and, therefore, require further efforts to assess its impact on the monitoring capabilities of individual nodes.

Daramas et al. [73] an enhanced and safe home based IDS HIVE is proposed having three parts i.e. a sensor manager, firebase as cloud database and user authentication service, and android application for monitoring, configuring and remote notification. The proposed system is especially design for a smart home with focus on detecting physical intrusion into a home. HIVE aims to detect a physical intrusion by using three sensors i.e. an infrared sensor to detect motions, a magnetic switch sensor to detect status of a door or window and a load cell sensor to detect pressure such as footsteps.

Mayzaud et al. [68] authors proposed a distributed system architecture for detecting the version number attacks in RPL-based networks and identifies malicious nodes. Furthermore, a number of intrusion detection system architectures have been developed in [74], [75] for resource-constrained 6LoWPAN devices-based systems focusing on the sinkhole and selective-forwarding attacks. Golomb et al. [76] present an innovative approach, CIOTA, to intrusion detection for IoT leveraging blockchain technology. The proposed approach is comprised of local agents and a central component which coordinates information (alerts) received from these agents. Authors use blockchain technology to achieve assurances about the authenticity of alerts generated by local agents.

Li et al. [70] presents a network-based intrusion detection approach for IoT focusing on the task of feature extraction for effective intrusion detection. Authors have used deep migration learning model to develop the proposed approach and have evaluated their scheme with the KDD 1999 dataset. Although the proposed approach demonstrates good detection accuracy as compared to existing schemes, however, the evaluation is limited to detection accuracy, TPR and FPR and does not take into account performance efficiency of the proposed scheme, which is a critical metric

due to the resource constraints of such devices. Similarly, Bassey et al. [71] presented one of the efforts focusing at detection of physical layer attacks on IoT networks. In particular, authors are focused at attacks whereby an attacker attempts to impersonate a victim IoT device through the use of Radio Frequency (RF) trace. Authors have proposed a deep learning-based method utilizing a dataset created through feature extraction of RF traces of similar devices to achieve device fingerprinting.

5 Privacy Implications of Intrusion Detection Systems

Intrusion detection systems are widely used to protect devices and end-users from malicious actors. The performance of these systems often depends on the type of data and architectural setup they use while preventing the attacker from misusing personal information of victims. The usage of data for the intrusion detection introduces the challenges of security and privacy. Therefore, we discuss the privacy implications of intrusion detection systems in this section.

5.1 Type of data

Intrusion detection systems can be categorized on the basis of network data they use to detect malicious actors. Identification of correct data type not only affects the performance of the system, but also has an impact on the privacy of the users. For instance, if the detection system uses IP-address to analyze the behavior of a device, it can be easily traced back to the owner of this IP-address. The challenge in this regard is two-fold: 1) identifying the data type that provides optimum performance in terms of detection rate, and 2) ensure protection of the privacy of the network users. The existing intrusion detection systems use two types of data for detecting the malicious actors i.e. 1) application layer data logs, and 2) network traces data. The first type is data originated at the application level and is normally associated with specific type of data set. This type of data can provide information about the device architecture and can help in fingerprinting malicious and non-malicious devices. The second data-type is the IP traces of the network traffic and contains much more details about the behavior of the devices. Another data type that can be used is the content or payload of the information exchanged among devices, such as a temperature reading, a web-page, or meta data.

5.2 System architecture

An intrusion detection system for IoT can operate in two modes i.e. 1) as the standalone system, or 2) as a collaborative system. The stand-alone detection systems rely on traffic patterns observed locally within the network domain or Internet service provider. These systems work independently within a service provider network. The stand-alone systems do not have any information about the behavior of its users in other domains and, therefore, can be easily circumvented by stealth techniques and smart attacker, such as by controlling the attack traffic to one domain but target large number of domains simultaneously. An effective intrusion detection system is envisaged to consider the collective behaviour of nodes across different domains to facilitate developing a collaborative network.

The collaborative solutions can be grouped in two types: 1) centralized - where alert information from the domain collaborators is reported to the the centralized system which classifies the behavior of traffic sender by analyzing traffic patterns from multiple domains, or 2) The distributed or decentralized settings - where alert information from each service provider is shared and processed in a completely distributed fashion without a centralized coordinator.

The major challenge towards the design of a collaborative IDS is regarding privacy protections for the data used for detection. The domain or Internet service provider are reluctant to share operational data of their users with each other as it risks privacy of their customers. A centralized trusted aggregation can overcome the problem of privacy if the centralized repository assures cooperating domain that their provided information would not be misused and disclosed to any one. Furthermore, use of cryptographic methods or addition of noise data can be considered to anonymize user data, however, this is expected to substantially increase the network load and computation time.

5.3 Analysis

In this section, we analyze the privacy implications of IoT intrusion detection system for two important features, the data type used for collaboration, and the system architecture.

Firstly, the system architecture of the detection system determines how data is transferred by the entities in the detection systems. Standalone detection system installed on the user device (e.g. IoT device) or installed at the edge router (entry point router to smart home or the corporate network) operate locally by recording data from the single source, only use data from the single source, therefore, does not have high performance accuracy. The collaborative system, however, operates in two modes i.e. the centralized architecture [44] [15] [56], and the distributed architecture [48] [49] [57]. In the centralized setup, it is envisaged to protect the privacy and integrity of the data provided to it. However, it may not be ideal as the attacker has to compromise only one device to breach the privacy of all collaborators. Furthermore, the centralized system introduces the challenge of single point of failure, which may inhibit efficient collaboration in case of failure.

The transfer of data to other parties or centralized system has a risk of privacy. In this setting, the collaborating device can operate in four settings: 1) transfer all raw data to the centralized system or other devices that process all the data for meaningful decision. This setting does not have any privacy assurance as data is exposed at other entity whilst also increasing computational workload, 2) transfer processed data for instance exchanging traffic statistics of host or IP-address, however, it still carries privacy threat but without requiring significant additional resources, and 3) the encrypted exchange of data. This setting assures privacy-preservation but requires extensive computation and communication overhead for the exchange of encrypted data.

Overall, privacy is an important feature which should be guaranteed by intrusion detection system especially within

a collaborative system. However, our analysis of the existing literature reveals that the research community has not given much attention to privacy preserving collaboration among the IoT domains or IoT devices. This may be due to resource-constrained nature of IoT devices which limits alert information and cryptographic processing of data due to computational overheads.

6 Analysis of Current IDS Approaches

In order to conduct a rigorous and methodical analysis of contemporary literature presented in the section 4, we have applied a thorough criteria with metrics, which are significant for effective intrusion detection for IoT. The individual element of the criteria along with a brief explanation are presented below. The comparative analysis of existing approaches for these criteria is presented in Table 1.

- **Placement:** As with the contemporary computing systems, the placement of an intrusion detection system is crucial as it determines the level of visibility it can offer to the activities within the monitored system. For instance, a network-based IDS is limited to monitoring the network traffic originated or destined for the monitored host and, therefore, cannot monitor any process subversion or privilege escalation within the monitored host. This is increasingly important for IoT systems with recent studies highlighting the lack of protection for IoT devices [77]. Furthermore, our analysis of existing intrusion detection approaches for IoT highlights that majority of these approaches are network-based, which restricts the depth of events visible to such systems. In view of emerging malware, such as Botnets, visibility of system-level events, including system calls is important to protect against such threats.
- **Detection Time frame:** One of the important characteristic of IoT systems is the dynamic nature of the system with the participating nodes following an adhoc pattern. Therefore, the time-frame of detection becomes even more important with the objective to detect an attack as soon as possible to avoid spreading infection to wider devices. Through analysis of existing literature, we have identified that majority of existing approaches are established and evaluated within isolated environments which has two-fold impact; i) the implementation and evaluation does not accurately represent an IoT environment, and ii) experimentation results conducted in isolated, simulated environment, such as Matlab or Contiki do not accurately simulate the challenges encountered within an real-world IoT environment. Therefore, majority of existing approaches are limited to offline detection which inhibits an IDS's ability to protect against malicious threats in timely manner.
- **Detection Engine:** An IDS can utilize a variety of detection engines, such as anomaly, signature and game based as highlighted in section 4. The choice of detection engine has two-fold impact i.e. i) it can affect the ability of an IDS to detect attacks, and ii) it impacts the performance overhead incurred by the engine. For instance, although signature-based IDS have been identified to be resource efficient, they do not have the ability to detect zero-day attacks. Analysis of literature presented in section 4 and summarized in Table 2 highlights that although existing approaches use variety of techniques, however, it also identifies an increase in the use of artificial intelligence and deep learning to achieve effective intrusion detection. In view of the extraordinary increase in volume and variety of attacks for IoT systems, these developments highlight future trends and require further advancements to fulfil the potential of these technological advancements.
- **Architecture:** The system architecture of an IDS specifies how the detection system carried out its detection functions. The system architecture not only affects the detection accuracy and performance but also affects user privacy. The standalone detection system mainly operates at the local machine or the device thereby susceptible to extended detection time because of the non-availability of enough data and stealthy nature of the attacker. However, a collaborative architecture utilizes data from different sources, such as IoT devices or network devices within the same or different organization. It can improve the detection accuracy, however, it introduces the challenge of privacy of the data shared between the entities. Furthermore, with regards to detection accuracy and performance, a typical IoT system is comprised of a number of IoT devices arranged into a local network such as a LoWPAN and an edge router which manages communication between local network and the Internet. Within this context, existing approaches can be categorized based on the location of the IDS module with distributed referring to IDS module implemented on IoT devices and centralized referring to IDS module implemented at the edge router. In this context, analysis of literature highlights emergence of schemes, which take into account distributed nature of a typical IoT architecture through collaboration between IoT devices and edge routers [17], [36]. We believe collaborative approaches can be beneficial in protecting against large-scale attacks, however, further work is required to enhance existing efforts to achieve effective and timely detection.
- **Performance Overhead:** A typical IoT device is constrained with respect to resources available for compute-hungry processes, such as intrusion detection. Therefore, we believe performance overhead caused by an IDS is one of the important criterion and can be measured in the form of energy consumption or CPU usage by the IDS. Our study of literature has highlighted that majority of existing approaches do not take into account performance overhead whilst evaluation effectiveness of these approaches. We believe, due to the resource-constrained nature of IoT devices, this is an important criteria to assess effectiveness of an IDS for IoT, and therefore, identifies a gap in literature which requires further efforts by the research community.
- **Attack types:** We have presented a comprehensive discussion about the potential attacks within an IoT

system supported by an attack model. These different types of attacks can be detected at different levels (network or host) and using different approaches, such as anomaly and signature-based. Furthermore, review of literature has also highlighted emergence of novel attack types, such as Botnets, which exploit specific vulnerabilities within a typical IoT system, and therefore, require further efforts to achieve effective protection mechanisms.

- **Detection Performance:** Detection performance represents the rate of with which an IDS can successfully detect a malicious attempt. It is one of the fundamental attributes of an IDS as it can be directly aligned to its effectiveness. Analysis of existing approaches summarized in Table 2 highlights that majority of these approaches report high detection performance in terms of detection accuracy, FPR and TPR. However, as highlighted earlier, a significant number of current efforts are implemented and evaluated in isolated environment which do not accurately reflect a real-world IoT environment and therefore require further efforts to address this limitation.
- **Scalability:** Typically, the number of devices within an IoT system is significantly higher compared with contemporary systems. In order to address the significant number of devices involved, the scalability of the IDS is an important criteria. As highlighted in Table 2, a number of existing efforts have adopted a centralized approach which affects scalability of such efforts and therefore require further work to address this limitation.

7 Open Challenges and Future Directions

As part of this research, we have performed a thorough review of existing efforts to address one of the critical aspects of IoT security i.e. intrusion detection. In previous sections, we have presented a comprehensive account of the state of the art within this domain and a thorough comparative analysis of individual approaches. In this section, we highlight important future research directions which require further investigation and efforts to improve overall security of an IoT system.

1) **Constrained resources:** A typical IoT device has limited resources such as constrained processing power, low storage capacity, and limited battery power. Within this context, resource-hungry intrusion detection system would drain the resources of an IoT system. Therefore, it is important to have a Intrusion detection system that fulfills two important characteristics: 1) any IDS should not incur significant computational and communication overhead, and 2) IDS should achieve high detection accuracy. In particular, the use of anomaly-based detection systems [50] [49] [48] requires considerably higher resources than the signature-based detection systems while having a trade-off between detection accuracy and overheads. For instance, anomaly detection is particularly effective against previously unknown attacks, but is expected to incur significant performance overhead. As an attempt to explore opportunities within this context, we have formulated a collaborative intrusion detection system in [69], which aims to use both anomaly and signature-based detection engines to achieve performance efficiency without compromising detection accuracy.
   Our analysis has revealed that many of the existing systems have not been designed for resource-constrained devices, however these approaches mainly focused on increasing the detection accuracy with small false positive. We believe there should be trade-off among three important factors 1) high detection accuracy, 2) performance overheads, and 3) privacy-preservation. Furthermore, dedicated efforts are required to devise approaches considering resource constraints that primarily focus on the energy consumption agnostic of resources and memory consumption.
2) **Multi-stage attacks:** A typical intrusion is carried out over multiple stage, each attempting to exploit a specific vulnerability. Such sophisticated attacks are termed as *multi-stage attacks*, and are common mechanisms for traditional and emerging computing systems such as IoT. Existing detection systems for IoT solely focus on the detection of individual threats agnostic of potential relationships between them. We believe the dynamic nature of the IoT systems makes the challenge of multi-stage attack detection non-trivial requiring explicit efforts to address it. Jun and Chi [21] represent one of the initial effort which recognize and explicitly seek to detect relationships between different malicious incidents. However, it represents a limited effort and further work is required to address detection and protection against multi-stage attacks within the IoT systems.
3) **Device protection:** As identified by [77], one of core issues with respect to the security of IoT systems is the security of the device as *"it is often neglected by the manufacturers and usually an afterthought"*. The lack of protection at device level within such systems has resulted in significant security attacks such as Mirai botnet in 2016 [38] and its more recent versions, such as Brickerbot [78] and Reaper [79]. In order to protect against such threats device-level security measures are paramount which can protect IoT systems. One such measure can be an effective intrusion detection installed within the IoT device. Through our research, we have identified efforts, such as [43] and [69], which propose to develop intrusion detection capability within the device however these efforts are generally limited in that these require further refinement to take into account unique characteristics of IoT devices such as those explained earlier in this section.
4) **Large-scale attacks:** With the widespread adoption of IoT systems, the number of IoT devices are increasing exponentially with some estimates predicting more than 50 billion IoT devices by the year 2020. The impact of this growth on securing the IoT system is is two-folds; firstly, the enormous scale makes IoT systems a lucrative target for malicious

actors, and secondly, it also presents IoT systems as a resource which can be used to launch a large-scale attacks. An example of such attacks is the botnets i.e. Mirai botnet and Brickerbot launched a Distributed Denial of Service (DDoS) which compromised the Domain Name System (DNS) service [38]. Moreover, due to the nature of the IoT systems, routing attacks are typically contagious i.e. affecting all the devices within a LoWPAN. These attacks demand a holistic approach to the intrusion detection which is able to monitor and detect the state of the overall network as well as the individual devices.

5) **Limited experimentation and evaluation:** In order to assess the effectiveness of intrusion detection efforts, rigorous experimentation is required for integrating multiple dimensions of the evaluation. Although, experiments have been conducted to demonstrate the effectiveness with respect to detection accuracy and false positive rate, but this evaluation is performed without using appropriate simulation software or hardware to replicate a real-life IoT setting. For instance, a number of efforts have used KDD 99 dataset [80] within an isolated environment to conduct experimentation, however, it has multiple limitations i.e. 1) the KDD 99 dataset does not accurately reflect the current threat types prevalent for the IoT systems and, 2) conducting evaluation in an isolated environment prohibits taking into account important factors such as resource constraints of a typical IoT device. These challenges require explicit efforts to improve state of the art with respect to the evaluation of intrusion detection schemes within IoT systems. Further, we believe that research into dedicated honeypots for IoT systems is required and will be significant in facilitating thorough evaluation of future intrusion detection approaches.
6) **Unavailability of accurate data:** Through our research, we have identified unavailability of real-world data from an IoT system as one of the bottlenecks to achieve rigorous evaluation. In absence of such data, a number of current approaches have used KDD99 datasets, which contains network traffic data for contemporary computing systems. We believe further research into dedicated honeypots for IoT systems is required and will be significant in facilitating thorough evaluation of future intrusion detection approaches.

8 Conclusions

Connected IoT provide foundation for next generation of infrastructures to facilitate development of future cities which are inherently sustainable with applications across smart homes, smart health and smart buildings. However, alongside the extraordinary evolution of IoT devices, the volume and variety of security threats for such systems have increased manifold, highlighting the importance of an efficient intrusion detection system. This paper has presented a comprehensive review of existing efforts within this domain aiming to identify open challenges and future directions. The paper has provided new focus on the performance overhead, energy consumption and privacy implications incurred by existing approaches. Highlighting challenges surrounding these aspects, this review has attempted to enthuse researchers to address key challenges identified in this article to achieve effective intrusion detection for IoT systems.

References

[1] Amirhassan Kermanshah, Hiba Baroud, and Mark Abkowitz. Cyber-physical technologies in freight operations and sustainability: A case study of smart gps technology in trucking. *Sustainable Cities and Society*, 55:102017, 2020.

[2] Hadi Habibzadeh, Brian H. Nussbaum, Fazel Anjomshoa, Burak Kantarci, and Tolga Soyata. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, 50:101660, 2019.

[3] Trevor Braun, Benjamin C.M. Fung, Farkhund Iqbal, and Babar Shah. Security and privacy challenges in smart cities. *Sustainable Cities and Society*, 39:499 – 507, 2018.

[4] Gartner. Gartners top 10 security predictions 2016. In *https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/*, 2016.

[5] D. Geer. The internet of things: Top five threats to iot devices.

[6] Ruth Ande, Bamidele Adebisi, Mohammad Hammoudeh, and Jibran Saleem. Internet of things: Evolution and technologies from a security perspective. *Sustainable Cities and Society*, page 101728, 2019.

[7] Enrico Natalizio Arbia Riahi, Yacine Challal. A systemic approach for iot security. In *2013 IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2013.

[8] Salim Hariri Jesus Pacheco. Iot security framework for smart cyber infrastructures. In *IEEE International Workshops on Foundations and Applications of Self* Systems*, 2016.

[9] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for iot security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017.

[10] Xiaojiang Du X. Yao, X. Han and X. Zhou. A lightweight multicast authentication mechanism for small scale iot applications. *IEEE Sensors*, 13:3693 – 3701, 2013.

[11] I. Butun, S. D. Morgera, and R. Sankar. A survey of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys Tutorials*, 16(1):266–282, First 2014.

[12] Guozhu Meng, Yang Liu, Jie Zhang, Alexander Pokluda, and Raouf Boutaba. Collaborative security: A survey and taxonomy. *ACM Comput. Surv.*, 48(1):1:1–1:42, July 2015.

[13] Herv Debar, Marc Dacier, and Andreas Wespi. Towards a taxonomy of intrusion-detection systems. *Computer Networks*, 31(8):805 – 822, 1999.

[14] D. Midi, A. Rullo, A. Mudgerikar, and E Bertino. Kalis - a system for knowledge-driven adaptable intrusion detection for the internet of things. In *IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, 2017.

[15] H. Haddad Pajouh, R. Javidan, R. Khayami, D. Ali, and K. Choo. A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in iot backbone networks. In *IEEE Transactions on Emerging Topics in Computing*, 2016.

[16] S. Raza, L. Wallgren, and T. Voigt. Svelte: Real-time intrusion detection in the internet of things. *AdHoc Networks*, 11(8):2661–2674, 2013.

[17] 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*, 8(1):3–14, 2019.

[18] A. A. Gendreau and M. Moorman. Survey of intrusion detection systems towards an end to end secure internet of things. In *IEEE 4th International Conference on Future Internet of Things and Cloud*, 2016.

[19] B. B. Zarpelao, R. S. Miani, C. T. Kawakani, and S. C. Alvarenga. A survey of intrusion detection in internet of things. *Journal of Network and Computer Applications*, 84:25–37, 2017.

[20] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki. Network intrusion detection for iot security based on learning techniques. *IEEE Communications Surveys Tutorials*, 21(3):2671–2701, thirdquarter 2019.

[21] C. Jun and C. Chi. Design of complex event-processing ids in internet of things. In *Proceedings of 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation*, pages 226–229, Jan 2014.

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

[23] T.Anantvalee and W.Jie. A survey on intrusion detection systems in mobile ad-hoc networks. *Wireless Network Security*, 2:159–180, 2007.

[24] S. Kumar and K. Dutta. Intrusion detection in mobile ad-hoc networks: Techniques, systems, and future challenges. *Secure Communications and Networks*, 9(14):2484–2556, 2016.

[25] A. Abduvaliyev, A.S.K. Pathan, Z. Jianying, R. Roman, and W. Wai-Choong. On the vital areas of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys*, 15(3):1223–1237, 2013.

[26] Ashfaq Hussain Farooqi and Farrukh Aslam Khan. Intrusion detection systems for wireless sensor networks: A survey. In *Communication and Networking*, pages 234–241, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[27] Christophe Kiennert, Ziad Ismail, Herve Debar, and Jean Leneutre. A survey on game-theoretic approaches for intrusion detection and response optimization. *ACM Comput. Surv.*, 51(5):90:1–90:31, August 2018.

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

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

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

[31] Linus Wallgren. Routing attacks and countermeasures in the rpl-based internet of things. *IJDSN*, 9, 2013.

[32] Hu Yih-Chun, Perrig Adrian, and B. Johnson David. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24:370–380, 2006.

[33] V. Mahajan, M. Natu, and A. Sethi. Analysis of wormhole intrusion attacks in manets. In *Proceedings of MILCOM 2008 - 2008 IEEE Military Communications Conference*, pages 1–7, 2008.

[34] Dang Nguyen Quan and Lamont Louise. A simple and efficient detection of wormhole attacks. *New Technologies, Mobility and Security*, pages 1–5, 2008.

[35] C Karlof and D Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1:293–315, 2003.

[36] J. Arshad, M. A. Azad, M. Mahmoud Abdellatif, , and K. Salah. An intrusion detection framework for energy constrained iot devices. *IET Networks*, 2019.

[37] René Hummen, Jens Hiller, Hanno Wirtz, Martin Henze, Hossein Shafagh, and Klaus Wehrle. 6lowpan fragmentation attacks and mitigation mechanisms. In *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '13, 2013.

[38] R. Graham. Mirai and iot botnet analysis. In *2017 RSA Conference*, 2017.

[39] L. O'Donnell. Partners warn against application layer ddos attacks targeting iot devices. *Available online at: http://www.crn.com/news/internet-of-things/300084491/partners-warn-against-application-layer-ddos-attacks-targeting-iot-devices.htm?itc=refresh*, 2017.

[40] L. Chen. Security management for the internet of things. *Electronic Theses and Dissertations*, 2017.

[41] K.N Mallikarjunan, K Muthupriya, and S.M Shalinie. A survey of distributed denial of service attack. In *Proceedings of IEEE International Conference on Intelligent System and Control*, 2016.

[42] A. Khairi M.U. Farooq, M. Waseem and S. Mazhar. A critical analysis on the security concerns of internet of things (iot). *International Journal of Computer Applications*, 111:1–6, 2015.

[43] M. Nobakht, V. Sivaraman, and R. Boreli. A host-based intrusion detection and mitigation framework for smart home iot using openflow. In *11th International Conference on Availability, Reliability and Security (ARES)*, 2016.

[44] Anita S. Chordia and S. Gupta. An effective model for anomaly ids to improve the efficiency. In *International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015.

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

[46] N. Thanigaivelan, E. Nigussie, R. Kanth, S. Virtanen, and J. Isoaho. Distributed internal anomaly detection system for internet-of-things. In *13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2016.

[47] Y. Zhang, L. Wang, W. Sun, R. Green II, and M Alam. Distributed intrusion detection system in a multi-layer network architecture of smart grids. In *IEEE Transactions on Smart Grid*, volume 2 of *4*, pages 796–808, 2011.

[48] D. Summerville, K. Zach, and Y. Chen. Ultra-lightweight deep packet anomaly detection for internet of things devices. In *IEEE 34th International Performance Computing and Communications Conference (IPCCC)*, 2015.

[49] N. Tamani and Y. Ghamri-Doudane. Towards a user privacy preservation system for iot environments: A habit-based approach. In *IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, 2016.

[50] L. Yang, C. Ding, M. Wu, and K. Wang. Robust detection of false data injection attacks for data aggregation in an internet of things-based environmental surveillance. *Computer Networks*, 129(2):410–428, 2017.

[51] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici. N-baiotnetwork-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, 17(3):12–22, Jul 2018.

[52] C. D. McDermott, F. Majdani, and A. V. Petrovski. Botnet detection in the internet of things using deep learning approaches. In *2018 International Joint Conference on Neural Networks (IJCNN)*, pages 1–8, July 2018.

[53] Vetrivelan Pandu, Jagannath Mohan, and Pradeep Kumar T S. *Network Intrusion Detection and Prevention Systems for Attacks in IoT Systems*, pages 128–141. 01 2019.

[54] P. Kasinathan, C. Pastrone, M. Spirito, and M. Vinkovits. Denial-of-service detection in 6lowpan based internet of things. In *IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).*, 2013.

[55] A. Sforzin, F. Marmol, M. Conti, and J. Bohli. Rpids: Raspberry pi ids ? a fruitful intrusion detection system for iot. In *Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld).*, 2016.

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

[57] K. Wang, M. Du, D. Yang, C. Zhu, and Y. Sun. Optimal active detection in machine-to-machine mobile networks: A repeated game approach. In *IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2016.

[58] Q. La, T. 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*, 3(6):1025–1035, 2016.

[59] X. Fu, W.and Xin, P. Guo, and Z. Zhou. A practical intrusion detection system for internet of vehicles. *China Communications*, 13(10):263–275, 2016.

[60] C. Jun and C. Chi. Design of complex event-processing ids in internet of things. In *Sixth International Conference on Measuring Technology and Mechatronics Automation*, 2014.

[61] J. Amaral, L. Oliveira, J. Rodrigues, G. Han, and L. Shu. Policy and network-based intrusion detection system for ipv6-enabled wireless sensor networks. In *IEEE International Conference on Communications (ICC)*, 2014.

[62] A. Le, J. Loo, Y. Luo, and A. Lasebae. Specification-based ids for securing rpl from topology attacks. In *IFIP Wireless Days (WD)*, 2011.

[63] G. Mulligan. The 6lowpan architecture. In *4th Workshop on Embedded Networked Sensors,*, 2007.

[64] J. Olsson. 6lowpan demystified. Technical report, Texas Instrument, 2018.

[65] Anand Mudgerikar, Puneet Sharma, and Elisa Bertino. E-spion: A system-level intrusion detection system for iot devices. In

Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, Asia CCS '19, pages 493–500, New York, NY, USA, 2019. ACM.

[66] V. Sharma, I. You, K. Yim, I. Chen, and J. Cho. Briot: Behavior rule specification-based misbehavior detection for iot-embedded cyber-physical systems. *IEEE Access*, 7:118556–118580, 2019.

[67] H. Sedjelmaci, S. Senouci, and T. Taleb. An accurate security game for low-resource iot devices. In *IEEE Transactions on Vehicular Technology*, 2017.

[68] A. Mayzaud, R. Badonnel, and I. Chrisment. A distributed monitoring strategy for detecting version number attacks in rpl-based networks. In *IEEE Transactions on Network and Service Management*, volume 14 of *2*, pages 472–486, 2017.

[69] J. Arshad, M. Abdellatif, M. Khan, and MA. Azad. A novel framework for collaborative intrusion detection for m2m networks. In *The 9th International Conference on Information and Communication Systems*, 2018.

[70] Daming Li, Lianbing Deng, Minchang Lee, and Haoxiang Wang. Iot data feature extraction and intrusion detection system for smart cities based on deep migration learning. *International Journal of Information Management*, 49:533 – 545, 2019.

[71] J. Bassey, D. Adesina, X. Li, L. Qian, A. Aved, and T. Kroecker. Intrusion detection for iot devices based on rf fingerprinting using deep learning. In *2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC)*, pages 98–104, June 2019.

[72] A. Gendreau. Situation awareness measurement enhanced for efficient monitoring in the internet of things. In *IEEE Region 10 Symposium*, 2015.

[73] A. Daramas, S. Pattarakitsophon, K. Eiumtrakul, T. Tantidham, and N. Tamkittikhun. Hive: Home automation system for intrusion detection. In *Fifth ICT International Student Project Conference (ICT-ISPC).*, 2016.

[74] M. Sheikhan and H. Bostani. A hybrid intrusion detection architecture for internet of things. In *8th International Symposium on Telecommunications (IST)*, 2016.

[75] M. Nogueira C. Cervantes, D. Poplade and A. Santos. Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things. In *IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2015.

[76] T. Golomb, Y. Mirsky, and Y. Elovici. Ciota: Collaborative iot anomaly detection via blockchain. In *Workshop on Decentralised IoT Security and Standards*, 2018.

[77] UK DCMS. Secure by design: Improving the cyber security of consumer internet of things report.

[78] I. Thomson. Forget mirai brickerbot malware will kill your crap iot devices. In *available at: https* : $//tinyurl.com/m5zm67v$, 2017.

[79] K. Townsend. Financial services ddos attacks tied to reaper botnet. In *available at: https://www.securityweek.com/financial-services-ddos-attacks-tied-reaper-botnet*, 2018.

[80] KDD Cup 1999. Kdd cup 1999 data. In *available at: kdd.ics.uci.edu/databases/kddcup99/kddcup99.html*, 1999.