A Survey on Recent Approaches in Intrusion Detection System in IoTs

Aliya Tabassum, Aiman Erbad, Mohsen Guizani
Computer Science and Engineering Department
Qatar University
Doha, Qatar
{at1700139, aerbad, mguizani}@qu.edu.qa

***Abstract*—Internet of Things (IoTs) are Internet-connected devices that integrate physical objects and internet in diverse areas of life like industries, home automation, hospitals and environment monitoring. Although IoTs ease daily activities benefiting human operations, they bring serious security challenges worth concerning. IoTs have become potentially vulnerable targets for cybercriminals, so companies are investing billions of dollars to find an appropriate mechanism to detect these kinds of malicious activities in IoT networks. Nowadays intelligent techniques using Machine Learning (ML) and Artificial Intelligence (AI) are being adopted to prevent or detect novel attacks with best accuracy. This survey classifies and categorizes the recent Intrusion Detection approaches for IoT networks, with more focus on hybrid and intelligent techniques. Moreover, it provides a comprehensive review on IoT layers, communication protocols and their security issues which confirm that IDS is required in both layered and protocol approaches. Finally, this survey discusses the limitations and advantages of each approach to identify future directions of potential IDS implementation.**

***Index Terms*—Internet of Things (IoTs), Intelligent Techniques, Deep Learning, Intrusion Detection System (IDS), Machine Learning.**

I. Introduction

IoTs are IP connected heterogeneous small objects in a hybrid network which sense and communicate with internal or external environments based on embedded technologies. It is a system of interconnected computer devices, humans and objects with unique identifiers making them capable of transferring information without human-to-human and human-to-computer interaction. IoTs include Radio-Frequency Identification (RFID), Machine-to-Machine (M2M) communication technologies, Wireless Sensor Networks (WSNs) and Low power Wireless Personal Area Networks (LoWPANs). The first machine controlled over the internet was invented at Carnegie Mellon University in 1980. It was a coke machine which displayed the status of the machine over internet for its users [1]. Kevin Ashton composed the phrase Internet of Things (IoTs) in 1999 [2] and now there are more than 7 billion IoT devices (not including laptops, smartphones, tablets) on the earth. Gartner predicts that in 2020 IoTs will generate a revenue of $1.9 trillion with its diverse sales and marketing. Moreover, it is predicted that by 2020 IoT products and service providers will produce more than 300 billion dollars [3]. A research, demonstrates the power of IoTs, anticipating a world with automatic commencement of things, such as the consequent unlocking of a door on the approach by an identified member whereas stays locked for unidentified individual [4]. Nowadays IoTs are embedded with Artificial Intelligence and Machine Learning techniques to ease the tasks of human, making non-living IoTs as intelligent robots for decision making and performing actions on their own. IoTs have become so sensible and discerning that they are capable to envision the life-cycle, capability and efficiency of any product in any field. These devices are conspicuous, locatable, addressable and controllable through the Internet. IoTs are capable to proctor heart impulse and report abnormal heart rate and can be used as an insulin pump to monitor the level of insulin in the body [5]. IoTs are also being adopted in automobile industries with built-in sensors to alert the drivers when the tyre (tire) pressure is low, to avoid unwelcome events.

These intelligent smart devices bring the risks from industrial control system space to real life, so it has gained significant attention of researchers and security specialists all over the world. The privacy and security in IoTs are concerned with confidentiality, integrity, and availability of the information and/or services. Meeting these security goals is very important for modern organizations to ensure trust and to guarantee the safety of data [6]. Financial, usability, resources and many other factors decide the degree of security mechanisms that are implemented in an IoT device. Every sector has to implement the security best practices appropriate to the needs. Moreover, IoT networks are vulnerable to cyber-attacks and various malicious intrusions. The security of IoTs is critical since the IoT networks are different from Cyber Physical Systems (CPS) and Wireless Sensor Networks (WSNs). The traditional mechanisms for cyber attacks, (especially for known attacks) are efficient in certain situations but cannot be applied to its variants or absolute unknown attacks. These conventional methods are difficult to be implemented in IoTs due to its complex structure of protocol stack, layers and technologies. Although, IoT systems are installed carefully by reviewing security requirements such as access control, data confidentiality, authentication and encryption, the IoT networks are facing devastating attacks, and this mandates a peripheral defense for IoT networks. Hence, Intrusion Detection Systems (IDSs) have become essential to regulate reliable and secure networking in IoT devices.

978-1-5386-7747-6/19/$31.00 ©2019 IEEE

This paper surveys the IoT architecture, communication protocols, their security issues and recent Intrusion Detection System (IDS) approaches to identify potential future directions of IDS implementations. The scope of the survey is illustrated in Fig. 1, where ML refers to Machine Learning and other intelligent techniques. The structure of the paper is as follows: The various layered architecture of IoTs and security requirements is illustrated in Section II, followed by section III which provides detailed information on popular communication protocols that support lossy and noisy communication networks, highlighting the security issues of each. The recent Intrusion Detection approaches are provided in Section IV and then the key challenges are enlisted in Section V. Finally, the work is concluded in Section VI by presenting a future direction of research.

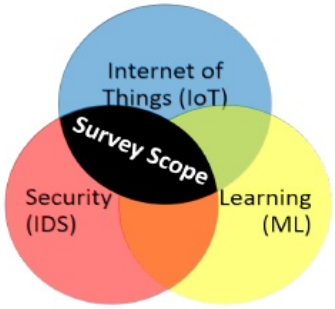

Fig. 1. Scope of the Survey

II. IoT Architecture

IoT provides various opportunistic features, however privacy and security management are equally challenging since these devices (i) are resource constrained, (ii) are globally accessible, (iii) use assorted recent protocols and (iv) are connected through internet, which is unreliable and untrusted. The key constraints of any IoT device are power, latency, integration and storage. All of these features are limited in IoTs and differ from device to device. Therefore, for this restraint nature of IoTs, it is worth investigating to provide a suitable security mechanism for its networks. Every IoT device must have 4 characteristics to deliver its service: receive information; collect and transmit; activate based on trigger and assistance during communication. These characteristics are provided by sensors, control units, communication modules and power sources [7]. This section provides detailed summary on IoT layered architecture and vulnerabilities of each layer.

The 3-layer architecture consists of Application, Network and Perception Layers. Due to the diversity of IoT devices, standardized architecture is not supported for all purposes. Other architectures also consist of 4-Layers and 5-Layers. Fig.2 shows 3 layer and 5 layer architecture of IoTs [8]. The 3-layer architecture is the most basic architecture with Application, Network and Perception Layers, but it is not sufficient to explain all aspects of IoTs so further enhancements were made to 5-layered architecture with Business, Application, Provcessing, Transport and Perception Layers.

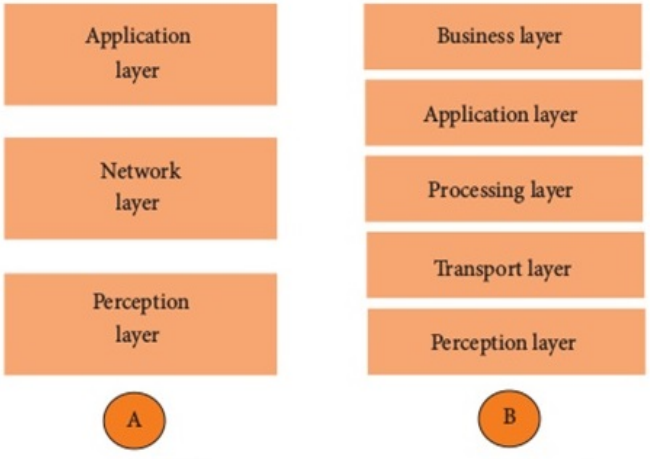

Fig. 2. Architecture of IoT (A: Three Layers) (B: Five Layers)

A. Perception Layer (Objects Layer)

It is the first layer consisting of the physical sensors and actuators of the IoT which senses environment and collects information. It is integrated with end components of IoT to sense and acquire information on the devices. The various functionalities like processing the collected information, querying location, reporting temperature, motion, acceleration, humidity, etc. are provided by this. The collected information is transferred to the above layers through secure channels [9]. However, nowadays there are hardware level (sensors/actuators) Trojans that can be triggered to overcome the security mechanisms and launch malicious activities. In a research done by Yang et al. [10], it was shown that analog time components can be used to inject malicious commands to exert a flip-flop which contains the processor privilege bit. The hardware-level attacks are increasing due to third-party manufacturers. The post-fabrication testing can be sometimes effective to detect the hardware level Trojans on a chip or any other hardware component of IoT devices. In some cases, the cryptographic keys are stored in the harware and isolation units are created for security purposes. But, these pose new challenges for the limited energy and resources of the IoT devices. In turn, the power and computational limitations create serious issues for higher layer security procedures [11]. It is worth investigating of how malicious software execution can be identified, prevented and removed from the hardware. Any malicious code execution can be detected by proper IDS system and hardware level Trojans can also be identified if testing is made on the devices before using it for real-time purposes.

B. Network Layer (Transport Layer)

It is also called the ”Backbone Layer” or ”Object Abstraction Layer”. This layer is responsible for communication among devices through internet and to transfer the

data collected by the objects to the processing layer. The infrastructure to support wireless or wired connections among IoTs is provided at this layer. Technologies such as RFID, 3G, GSM, UMTS, WiFi are used for transferring data. Unlike other internet-based devices, IoTs have numerous protocols and functions. Different protocols are used based on the device constraints and features. Take for example, powered devices can use short range protocols like Near Field Communication (NFC) or Bluetooth to conserve energy. However, they support only one-to-one communication unlike the multiple TCP connections. A single connection service is an overhead and time-consuming technique [12]. Another area of concern is the wireless communication technique that is adopted to transfer data. If Wifi is used for controlling the IoT devices in a home, then it poses serious security issues as Wifi was not originally designed for such purposes [13]. Access Control is the major security goal which prevents unauthorized access and untrusted code and is different for each domain. It requires diligent research to decide ACL prior to the usage of the device. If access control list (ACL) is compromised then no other technique can prevent execution of malicious code or flow of sensitive information in the network. Access Control and Information Flow Control can be monitored by the Intrusion Detection System.

C. Processing Layer (Service Management Layer)

This is also called the "Middleware" or "Pairing" or "Processing Layer" which pairs a specific service with its requester based on addresses and names, enabling heterogeneous objects on the same platform. In a 4 layer architecture, this layer is called the service layer and is present above the network layer which is used to provide and manage services required by users or applications. The System Software Layer is designed to isolate processes based on the hardware layer Memory Management Unit (MMU) so that bugs or security flaws in one process does not effect the other. In smaller IoT devices with small memory, isolation cannot be implemented. It is difficult to implement isolation of processes without MMU in small IoT devices [14], so security flaws have to be monitored by some internal or external tools to prevent compromising such a device.

D. Application layer

This layer customizes the services for users. The application layer has to make sure of transmission efficiency, power efficiency and complexity issues. IoTs are suitable for low-complexity application layer security schemes. The customer's or user's high-quality smart services are provided by this layer such as temperature and air humidity measurements. This layer consists of all interaction methods for users and applications [15]. Any attack on this layer causes operating system errors in the device and sometimes the attacker is able to bypass authorized access controls. Fernandes et al. [16] has shown that the access control design flaws can lead to security breaches and over-privilege exploits. The main reason for this kind of granularity flaw is the trade off between security and usability, mostly in hand held devices like mobile phones, tablets and laptops [17]. The stuxnet malware [18] modified the operation of Industrial Control System (ICS) by gaining privileged access control which destructed the Iranian Nuclear Plants. Similar to the previous layer, the application layer also needs monitoring of application and services in accordance with the security requirements.

E. Business Layer

The overall IoT system activities and services are managed here by creating business models, flowcharts and graphs. Various other activities like design, analysis, implementation, evaluation, and support decision-making processes are regulated and managed at this layer. Once a device is deployed, software updates are used to patch security patches and enhance features in a device. It is easy to update the OS or Software in PCs, tablets, smartphones and cloud services. However, updating software in physical IoT devices produces many challenges [19]. Updating the software requires the shutdown of complete physical processes which can have various impacts: economic, denial of service or life-threatening in hospitals and water or electric smart grid systems [20]. The incident that had devastating impact due to software update was the shutdown of a nuclear reactor of the business network [21]. In some cases, the manufacturers do not design the update channel which makes it impossible to fix the vulnerability patches or to enhance features, and the only option left will be replacing of that particular IoT device [22]. Alternatively, disposable IoT devices are small with limited computational capability which makes it harder to update software addressing the vulnerabilities after deployment. In such IoTs, regular monitoring is recommended to make sure that attackers does not exploit it.

III. IoT Communication Protocols

From the above section, it is understood that the Layered-Approach of IoT implementation requires appropriate monitoring mechanism as the attack can be triggered at any layer. This section describes the protocols that are popularly used in IoT networks. The protocols for IoT networks must support Internet enabled communication at lower power with reliability and high efficiency. The IoT nodes must be capable to operate at low power in a lossy and noisy communication network. The protocols significant for communication in IoT network are shown in Fig. 3 and detailed description of each is provided in the following subsections

A. IEEE 802.15.4

IEEE 802.15.4 was proposed as a standard for physical and medium access control by Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The devices with IEEE 802.15.4 technology operate in between 20kbps - 250 kbps with 10m - 100 m transmission range [23]. IEEE 802.15.4 is a low-power and low-data rate protocol with few meters coverage for the Personal Area Network (PAN). Based on IEEE 802.15.4, many standard organizations have developed various

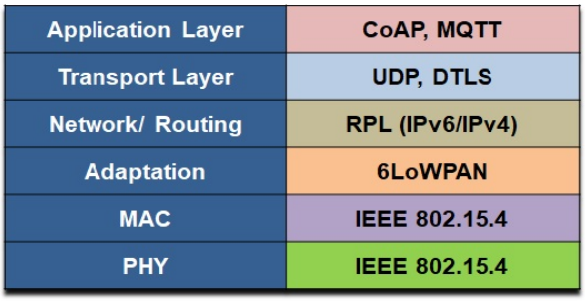

Fig. 3. IoT Stack: Layers and Protocols (TCP/IP Model)

low-power protocol stacks like WirelessHART and ZigBee. IEEE 802.15.4 supports a maximum data rate upto 250 kb/s, maximum packet size 127 bytes and a maximum output power of 1 mW. As the power consumption is critical in IoT devices, IEEE 802.15.4 protocol mechanism is managed intelligently where the power consumed by the transceiver when it is idle is lower than both the listen and transmit operation power consumption. The transceiver is turned off when there is no traffic and is switched on when communication is sensed [24]. IEEE 802.15.4 provides link layer security and is usually installed with other security mechanisms like IPsec and Lightweight Datagram Transport Layer Security (DTLS). Although it supports encryption and authentication of messages, the number attacks have disrupted networks [25] [26]. Hence, IDS is necessary for this protocol to ensure reliable networking.

B. 6LoWPAN

IPv6 technology has gained a lot of attention from the beginning of the research on IETF protocol stack. Due to the key characteristics such as universality, extensibility, and stability, IPv6 is expected to become the only choice for future wireless communication. Implementing IPv6 using IEEE 802.15.4 is not possible due to its two key challenges. First, in IEEE 802.15.4 the maximum frame size supported is only 127 bytes and the size of the payload at the application layer is very limited. Second, the minimum value of IPv6 Maximum Transmission Unit (MTU) is 1280 bytes (RFC 2460) where as the MTU supported by IEEE 802.15.4 is smaller than that. For which the data packets has to be fragmented and reassembled at the data link layer [24]. The 6LoWPAN protocol can be used to apply IPv6 to the PHY and MAC layers of IEEE 802.15.4 protocol. In order to address the issues of IEEE 802.15.4, 6LoWPAN provides an adaptation layer above the data link layer for the segmentation process of the IPv6 packets for the lower layers. Moreover, 6LoWPAN reduces the overhead of the IP header in IPv6 by specifying the stateless compression. Connection-less user datagram protocol (UDP) is used in these networks. Despite adopting IPv6 and 6LoWPAN, the Internet of Things (IoT) are exposed to attacks from within the 6LoWPAN network and outside, necessitating a favorable Intrusion Detection Systems (IDS). A real-time intrusion detection system named SVELTE was designed, implemented and evaluated in Contiki OS by Raza et al. [27] for routing attacks to identify spoofed or altered information, sinkhole attacks, and selective-forwarding in 6LoWPAN networks. This approach is able to detect the launched attacks with lesser true positive rate and is suitable to be deployed for constrained IoTs because the overhead it causes is much less. However, this approach was not able to detect other attacks.

C. RPL

RPL is an IPv6 Routing Protocol where the routers and nodes operate at a lower processing power, limited memory, and constrained energy (battery power). RPL is a versatile and robust protocol over lossy links and it supports simple and complex traffic models: Multipoint-to-Point, Point-to-Multipoint and Point-to-Point. Routing diagram of nodes is shown by Destination-Oriented Directed Acyclic Graph (DODAG) with a single root [9]. RPL routers support two modes of operation: uni-directional and bi-directional or Non-Storing mode and Storing mode. In Uni-directional (Non-Storing) mode, the traffic moves toward lower levels root between the constrained nodes and DODAG root (IP source routing to the 6BR). In Storing (bi-directional) mode, downward routing is based on destination IPv6 addresses (towards the DODAG root). Every node in this protocol has to know in advance if it has to forward the packets either to its parents or to the children. The best way to accomplish this is to follow the path of parent node routing. The routing table categorizes packets routing in forward direction and in downward direction [28]. This protocol is vulnerable to the routing attacks which can be detected by an IDS or IPS system.

D. CoAP

The Constrained Application Protocol (CoAP) is a web transfer protocol for resource constrained nodes and networks. CoAP is not a HTTP compression protocol but provides a part of HTTP functions and designed exclusively for constrained environments. Additionally it supports multicast routing and built-in resource discovery. This protocol adopts datagram-oriented transport protocols for providing reliable communication [24]. Fig. 4, illustrates the protocol stack and messages of CoAP. In this protocol, the end-to-end security in between two applications is provided by Datagram Transport Layer Security (DTLS), which also needs peripheral defense mechanism to completely secure its communication.

E. MQTT

Another popular protocol, Message Queue Telemetry Transport (MQTT) is an open messaging protocol, basically designed for constrained devices, and was standardized in 2013 at OASIS. It does not have specific routing techniques and relies on underlying the network for the delivery services of messages like TCP/IP. It is a topic-based protocol which uses various simple character strings for hierarchical topics and also supports multiple topics subscription. MQTT provides 3 levels of Quality of Service (QoS) for reliably delivering the messages to its receivers from the senders (end-to-end).

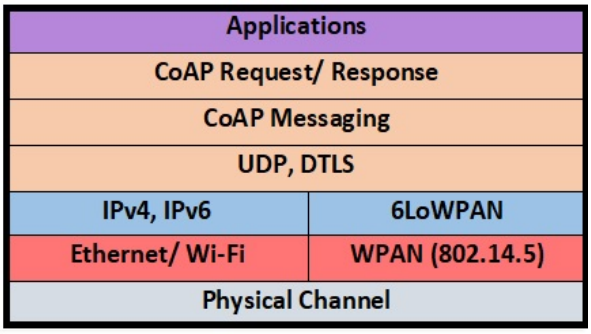

Fig. 4. CoAP Protocol Stack

The original MQTT protocol is customized for wireless sensor networks as MQTT-S [29].

From the above sections, it is clear that Intrusion detection system has become a necessary peripheral for protecting networks. Existing communication protocols lack security mechanisms and hence monitoring of malicious access and intrusions is the only desirable solution.

IV. Intrusion Detection in IoT Devices

The Intrusion Detection System (IDS) is a device or software application that monitors and protects a network from malicious activities or policy violation. Intrusion detection is the process of detecting unauthorized access and intrusions in the network and information systems [30]. Intruders can be internal or external, internal intruders are the legitimate users who try to escalate privileges in order to access unauthorized data or services. Whereas external intruders are those outside the network and attempt to gain access to network and/or information systems.

The principal challenge in IDS is identification of anomalous patterns in the network. Sometimes the benign behavior is detected as malicious and vice versa. The number of false positives and true negatives should be minimum to reduce the error rate in anomaly detection [27]. This challenge emerges due to complexity of the networks that are connected and numerous devices that interact and exchange information in IoT systems. These abundant distributed devices that are connected through internet also give ways to launch DDOS attacks making them unusable for a point in time or crashing the devices. The user-friendly internet infrastructure of ICT and limited power, battery life, memory resources, constrained network bandwidth make IoTs potentially vulnerable for disruptive distributed denial of service attacks (DDOS) [31].

Security Vulnerabilities or random bugs in IoT devices can cause user dissatisfaction and various unpredicted outcomes. Privacy violations like eavesdropping, denial of service attacks or ransomware can cause monetary loss and sometimes loss of life in vehicular IoT devices or Implanted Medical Devices [32]. There are 2 types of IDS: Network-based IDS (NIDS) and Host-based IDS (HIDS). Network-based IDS (NIDS) is connected to one or multiple network segments and monitors inbound and outbound traffic for malicious activities. Traditional NIDS mechanism is challenging and restrictive to be applied to IoTs due to heterogeneous connectivity, constrained resources and limited power. The nodes in traditional systems monitor inbound and outbound traffic without any resource or bandwidth constraints. In IoTs, many NIDS mechanisms have been developed using attack signatures but the False Positive rates were higher (false alarms) and unknown attacks were not identified [33]. Host-based IDS is connected to any component like computer device or node or a router to monitor the network traffic. Unlike NIDS, HIDS scans the operating system processes, file system modifications and system calls [34]. However, HIDS is not preferred due to its numerous limitations.

A. Intrusion Detection System (IDS) Approaches

IDS approaches are categorized as signature-based, anomaly-based, specification-based and hybrid depending on the detection approach [35].

1) Signature-based detection: This approach recognizes the bad patterns based on the signatures of the attacks stored in the internal database of IoTs [36]. Whenever an attack signature matches the existing one, an alert is triggered. This process is very effective and fast for identifying known attacks and it is difficult to detect new attacks or the attacks for which signatures are not stored or even variants of known attacks are undetectable [37]. Deploying any IDS mechanism in IoTs on the low capacity nodes and low power networks is highly difficult and challenging. In signature-based methods, both the cost of storing the signatures in the databases and the computational cost of running learning algorithms for checking each signature is high. A signature-based Intrusion Detection (IDS), Intrusion Prevention (IPS), Network Security Monitoring (NSM) method using Suricata Engine was adapted by authors for 6LoWPAN-based networks [38]. An improvement to this mechanism was implemented by [39] to reduce the computational cost of comparison between attack signatures and network packet payloads. The signature-based approach for current zero-day attack scenarios is unsuitable.

2) Anomaly-based detection: It detects unknown attacks and often relies on machine learning algorithms to create a model of trustworthy good traffic activity, and then compares anomalous network activities against this model. Sometimes, the previously unknown legitimate activity is also be classified as malicious (false positive). The machine learning techniques and statistical methods used for matching algorithms are heavy to be suitable for deploying on low capacity nodes, which is one of the challenges that needs to be considered. The authors in [40] proposed an anomaly-based method for detecting botnets based on the average of 3 metrics, TCP control fields sum, number of connections for each sensor and packet length to create the normal behavior. Author Lee and his group analyzed the nodes behavior for identifying anomalous activity, they considered energy consumption of the node as a parameter. They established models of conventional energy consumed by the nodes in normal routing and if any

node is abnormal in power consumption then it is removed from the 6LoWPAN routing table [41]. Another anomaly detection mechanism for resource constrained IoT devices was proposed by Summerville et al. [42]. The authors claim that the protocols in IoTs are simple which result in similar network payloads, so they performed feature selection using bit-pattern matching, but still the process was not efficient to detect various attacks. Another efficient method was devised in 2015 by Pongle et al. for detecting wormhole attacks in IoT networks which consumed very low power and energy [43]. The approach was based on the number of packets shared between nodes, if the packet exchange rate is high compared to a normal behavior then an alert is triggered. But, only specific attacks were being identified.

3) Specification-based detection: This method sets guidelines for the expected behavior for the network components like nodes, routing tables and protocols. The purpose is similar to anomaly detection, when the behavior is deviated from the specification then it is considered as an intrusion. However, unlike anomaly detection this approach needs some security expert to define the specifications for the elements and this procedure guarantees lower false positive rates. No learning algorithms are needed but the challenge is different specifications are required for different platforms or environment [44]. One such approach was implemented to tackle Denial of Service attack (DOS) in which the maximum capacity of each middle-ware layer is defined before hand and if the number of request matches or exceeds the capacity, an alert is triggered to the network administrator [45]. One of the specification-based approach was proposed for the RPL protocol where the behavior of the protocol was fed in finite state machine to monitor the network intrusions and malicious behavior. In an extension work by Le et.al, [46] simulation trace files were used to generate finite state machines. Most of the manually deciding specification approaches are highly dependent on the expertise of the security team and network administrator. Inappropriate specifications result in higher false positives and true negatives and in turn increase the risk of the network security.

B. IDS placement strategies

1) Centralized: In this approach the IDS is placed at any centralized component either at the border of the node or at any host. When the IDS is placed at the border router then it is able to analyze all the traffic between the node and the internet, while the traffic across the border router is left unmonitored. Moreover, when a part of the network is compromised then the centralized IDS may not monitor the nodes during the attack.

2) Distributed: In this mechanism, an optimized IDS is placed at each physical object meeting the resource constraints of the nodes in IoTs. A distributed lightweight IDS was proposed by [39] using the packet payloads and attack signatures in which the IDS was placed in various places to cover the whole network monitoring. To reduce the number of matches, they used auxiliary shifting and early decision. Another distributed lightweight method considering one node parameter to optimize the computation by the nodes proposed by Lee et al. is describe in previous subsection, Anomaly Based Detection.

C. Hybrid Approaches

This approach integrates the different IDS approaches with the placement strategy to maximize the advantages and minimize the limitations or impacts of the mechanisms all together. Hybrid IDS placement bolsters the performance when centralized and distributed schemes are combined together. From all the above methods, a hybrid approach which best suites the situation and network structure can be adopted. Designing a hybrid approach specifically for each criterion manually is impractical so intelligent techniques have to be used which customizes according to the requirements. Hence, researchers have focused on Machine Learning and Artificial Intelligence techniques, specifically on Deep Learning (DL) algorithms to design optimal IDS for IoT networks.

D. IDS using Machine Learning

The effectiveness of Machine learning techniques in fraud detection, image recognition and text classification has encouraged security researchers to employ these algorithms for anomalous pattern detection and to identify abnormal behaviors to enhance the security in IoT networks [47]. The machine learning algorithms rely on learning data sets taken as inputs. For this reason, Machine Learning is being applied even in conventional methods of attack detection such as signature-based and anomaly-based in traditional internet networks [48]. ML algorithms have been applied for data processing and management in IoTs in [49] to extract useful data from the voluminous, however, was not for Intrusion Detection due to huge complexity and computational requirements of ML algorithms. An ML based distributed attack detection method for IoTs in Fog networks is implemented using Extreme Learning Machine (ELM) classifier integrated with Semi-Supervised Fuzzy C-Means for efficient detection in lesser time [50]. This approach was tested using popular NSL KDD dataset. Shiven et al. [51] proposed a real-time Integrated Intrusion Detection system using ML and anomaly based detection approach. This method provides security-as-a-service incorporating different communication protocols and monitors inbound-outbound traffic. It easily adapts to different network topologies and does not require any specialized hardware for the setup in the network. However, this model is yet to be tested with different data sets and for the number of attacks it detects.

E. IDS using Deep Learning

Internet of Things support diverse protocol stack due to which numerous zero-day attacks are emerging. Its harder for traditional machine learning mechanisms to detect the small mutants of attacks over time. Deep Learning methods known for its success of high-level feature extraction capability in big data can be a resilient mechanism to detect small variants of the attacks. DL technique can identify hidden patterns

from the training data and completely rely on recognizing the true face (attack) of any variant. DL technique is a breakthrough approach of Artificial Intelligence, which is inspired by the ability of human brain to adapt to circumstances and deduce from past experiences. Compression capabilities and unsupervised pre-training are the key features of DL which makes it possible to be deployed on IoT constrained networks IDS. Deep learning approach is adopted by Sakurada et al. [52] by using AutoEncoders for anomaly detection, where the normal network behavior is self-learned by the auto-encoders. However, the approach has shown abnormal results for same datasets. Another distributed IDS approach using DL was proposed in [53] for intrusion detection in Social Internet of Things (SIoTs). The authors have shown that distributed Intrusion Detection Systems (IDS) in IoTs fog networks is more scalable than the IoTs centralized cloud. Deep networks are far better than the shallow machine learning methods in attack detection with best accuracy. This method can be evaluated by using various datasets, payload data and algorithms for comparisons and future enhancements using existing models.

V. Key Challenges

Unlike user-driven computer networks, IoT networks are object-driven which makes it difficult to apply conventional computer networks security mechanisms to IoT networks. Therefore, specialized tools are needed to secure, preserve and manage IoT devices and networks from evolving threats and vulnerabilities. The following are the key challenges and research directions that are deduced from this survey:

1) Designing an IDS based on one mechanism is inappropriate for current heterogeneous and complex IoT network. Proposing an advanced mechanism combining different approaches may give an optimal solution. Moreover, we can infer that Distributed attack detection approach is better than a centralized model.
2) The Rule-based / Specification-based method, in which the network administrator or specialist defines a set of rules for the benign network behavior has to be specialized for each topology and creates an overhead when the topology is frequently changed.
3) The Signature-based intrusion detection approach falls short for current emerging zero-day attacks for which the patterns or signatures are not defined in advance.
4) In contrast to rule-based and signature based approaches, Anomaly-based IDS using intelligent learning techniques can distinctively identify known and unknown intrusions with better accuracy and speed.
5) Applying Machine Learning and other intelligent techniques for IoTs is challenging due to its resource constraints. Very few approaches have been developed using these techniques for IoTs and it requires diligent validation of existing approaches using different data sets to prove effective for the real-time IoT scenarios.
6) Intelligent techniques like ML that require higher memory and processing power may affect the performance of IoT functioning and service delivery. Besides, ML techniques are unsuitable to detect mutants of various attacks. So Deep Learning and other advanced techniques such as Deep Belief Networks (DBN) and Deep Convolutional Neural Network (Deep CNN) are potential solutions.

VI. Conclusion

This article has identified the advantages and disadvantages of existing approaches of IDS, its placement strategies and the types of attacks that are being detected. The methods of IDSs using Machine Learning that are discussed in the literature so far have not been evaluated in real-time, specifically for IoTs. Most of these IDS using intelligent techniques are customized for Wireless Sensor Networks or for the traditional internet architecture. Artificial Intelligence and Deep Learning algorithms have the potential to develop an IDS mechanism that meets the requirements of IPv6 connected IoTs and is efficient in constrained environment of IoTs. In future, it is aimed to develop a secure and reliable Intrusion Detection System for heterogeneous IoT networks that is independent of protocols, network topology and known or unknown attacks. An intelligent IDS that monitors the network traffic invisibly and reports malicious behavior without creating overhead to the nodes. In addition, it provides mitigation steps when an intrusion is detected. The proposed mechanism must be seemingly adaptable to changing the network topology, threat landscape and various networks like Personal Area Network (PAN).

References

[1] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of things (iot): A literature review," *Journal of Computer and Communications*, vol. 3, no. 05, p. 164, 2015.

[2] K. Ashton, "That internet of things thing, june 2009," *Available at http*, 2016.

[3] "https://www.gartner.com/newsroom/id/2636073."

[4] P. V. Paul and R. Saraswathi, "The internet of thingsa comprehensive survey," in *Computation of Power, Energy Information and Commuincation (ICCPEIC), 2017 International Conference on*, pp. 421–426, IEEE, 2017.

[5] A. Tabasum, Z. Safi, W. AlKhater, and A. Shikfa, "Cybersecurity issues in implanted medical devices," in *2018 International Conference on Computer and Applications (ICCA)*, pp. 1–9, IEEE, 2018.

[6] M. Plachkinova and C. Maurer, "Teaching case security breach at target," *Journal of Information Systems Education*, vol. 29, no. 1, pp. 11–20, 2018.

[7] C. Doukas, *Building Internet of Things with the ARDUINO*. CreateSpace Independent Publishing Platform, 2012.

[8] P. Sethi and S. R. Sarangi, "Internet of things: architectures, protocols, and applications," *Journal of Electrical and Computer Engineering*, vol. 2017, 2017.

[9] 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, 2015.

[10] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "A2: Analog malicious hardware," in *Security and Privacy (SP), 2016 IEEE Symposium on*, pp. 18–37, IEEE, 2016.

[11] G. Hunt, G. Letey, and E. Nightingale, "The seven properties of highly secure devices," *tech. report MSR-TR-2017-16*, 2017.

[12] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of things (iot) communication protocols," in *Information Technology (ICIT), 2017 8th International Conference on*, pp. 685–690, IEEE, 2017.

[13] G. Lize, W. Jingpei, and S. Bin, "Trust management mechanism for internet of things," *China Communications*, vol. 11, no. 2, pp. 148–156, 2014.

[14] A. Levy, M. P. Andersen, B. Campbell, D. Culler, P. Dutta, B. Ghena, P. Levis, and P. Pannuto, "Ownership is theft: Experiences building an embedded os in rust," in *Proceedings of the 8th Workshop on Programming Languages and Operating Systems*, pp. 21–26, ACM, 2015.

[15] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[16] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 636–654, IEEE, 2016.

[17] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proceedings of the eighth symposium on usable privacy and security*, p. 3, ACM, 2012.

[18] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society*, pp. 4490–4494, IEEE, 2011.

[19] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma, "Iot sentinel: Automated device-type identification for security enforcement in iot," in *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*, pp. 2177–2184, IEEE, 2017.

[20] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry, *et al.*, "Challenges for securing cyber physical systems," in *Workshop on future directions in cyber-physical systems security*, vol. 5, 2009.

[21] B. Krebs, "Cyber incident blamed for nuclear power plant shutdown," *Washington Post, June*, vol. 5, p. 2008, 2008.

[22] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things," in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*, p. 5, ACM, 2015.

[23] I. . W. Group *et al.*, "Ieee standard for local and metropolitan area networkspart 15.4: Low-rate wireless personal area networks (lr-wpans)," *IEEE Std*, vol. 802, pp. 4–2011, 2011.

[24] Z. Sheng, S. Yang, Y. Yu, A. V. Vasilakos, J. A. McCann, and K. K. Leung, "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities," *IEEE Wireless Communications*, vol. 20, no. 6, pp. 91–98, 2013.

[25] S. Raza, S. Duquennoy, T. Voigt, and U. Roedig, "Demo abstract: Securing communication in 6lowpan with compressed ipsec," in *2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, pp. 1–2, IEEE, 2011.

[26] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the internet of thingsa comparison of link-layer security and ipsec for 6lowpan," *Security and Communication Networks*, vol. 7, no. 12, pp. 2654–2668, 2014.

[27] S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things," *Ad hoc networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[28] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki-a lightweight and flexible operating system for tiny networked sensors," in *29th annual IEEE international conference on local computer networks*, pp. 455–462, IEEE, 2004.

[29] U. Hunkeler, H. L. Truong, and A. Stanford-Clark, "Mqtt-sa publish/subscribe protocol for wireless sensor networks," in *Communication systems software and middleware and workshops, 2008. comsware 2008. 3rd international conference on*, pp. 791–798, IEEE, 2008.

[30] A. Riahi, E. Natalizio, Y. Challal, N. Mitton, and A. Iera, "A systemic and cognitive approach for iot security," in *Computing, Networking and Communications (ICNC), 2014 International Conference on*, pp. 183–188, IEEE, 2014.

[31] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[32] N. Davies, N. Taft, M. Satyanarayanan, S. Clinch, and B. Amos, "Privacy mediators: Helping iot cross the chasm," in *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*, pp. 39–44, ACM, 2016.

[33] Z. M. Fadlullah, F. Tang, B. Mao, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, "State-of-the-art deep learning: Evolving machine intelligence toward tomorrows intelligent network traffic control systems," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2432–2455, 2017.

[34] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.

[35] A. S. Ashoor and S. Gore, "Importance of intrusion detection system (ids)," *International Journal of Scientific and Engineering Research*, vol. 2, no. 1, pp. 1–4, 2011.

[36] J. Pacheco and S. Hariri, "Iot security framework for smart cyber infrastructures," in *Foundations and Applications of Self* Systems, IEEE International Workshops on*, pp. 242–247, IEEE, 2016.

[37] V. Vaidya, "Dynamic signature inspection-based network intrusion detection," Aug. 21 2001. US Patent 6,279,113.

[38] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6lowpan based internet of things," in *2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob)*, pp. 600–607, IEEE, 2013.

[39] 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. 24188–24211, 2014.

[40] E. J. Cho, J. H. Kim, and C. S. Hong, "Attack model and detection scheme for botnet on 6lowpan," in *Asia-Pacific Network Operations and Management Symposium*, pp. 515–518, Springer, 2009.

[41] T.-H. Lee, C.-H. Wen, L.-H. Chang, H.-S. Chiang, and M.-C. Hsieh, "A lightweight intrusion detection scheme based on energy consumption analysis in 6lowpan," in *Advanced Technologies, Embedded and Multimedia for Human-centric Computing*, pp. 1205–1213, Springer, 2014.

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

[43] P. Pongle and G. Chavan, "Real time intrusion and wormhole attack detection in internet of things," *International Journal of Computer Applications*, vol. 121, no. 9, 2015.

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

[45] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," *IEEE wireless communications*, vol. 11, no. 1, pp. 48–60, 2004.

[46] 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, p. 25, 2016.

[47] 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*, 2019.

[48] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 184–208, 2016.

[49] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for internet of things data analysis: A survey," *Digital Communications and Networks*, vol. 4, no. 3, pp. 161–175, 2018.

[50] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for iot," *Applied Soft Computing*, vol. 72, pp. 79–89, 2018.

[51] S. Chawla and G. Thamilarasu, "Security as a service: real-time intrusion detection in internet of things," in *Proceedings of the Fifth Cybersecurity Symposium*, p. 12, ACM, 2018.

[52] M. Sakurada and T. Yairi, "Anomaly detection using autoencoders with nonlinear dimensionality reduction," in *Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis*, p. 4, ACM, 2014.

[53] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for internet of things," *Future Generation Computer Systems*, vol. 82, pp. 761–768, 2018.