IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 7, 2021, accepted October 28, 2021, date of publication November 30, 2021,
date of current version December 13, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3131367

Secure and Reliable WSN for Internet of Things: Challenges and Enabling Technologies

SONAM LATA[1], SHABANA MEHFUZ[1], (Senior Member, IEEE), AND SHABANA UROOJ[2,3], (Senior Member, IEEE)

[1]Department of Electrical Engineering, Jamia Millia Islamia, New Delhi 110025, India
[2]Department of Electrical Engineering, College of Engineering, Princess Nourah Bint Abdulrahman University, Riyadh 84428, Saudi Arabia
[3]Department of Electrical Engineering, School of Engineering, Gautam Buddha University, Greater Noida, Uttar Pradesh 201312, India

Corresponding author: Shabana Urooj (shabanaurooj@ieee.org)

ABSTRACT Wireless Sensor Network (WSN) is an innovative technology with a broad range of applications and highly attractive benefits, such as low cost of implementation and data transmission, unmonitored access to the network, autonomous and long-term operation. With extensive demand for the advancement of related technologies (cloud computing, near-field communications and cellular mobile networks), the Internet of Things (IoT) is becoming a very exciting paradigm. By using communication technologies in sensors and sensing features in web devices, WSNs have begun interaction with the Iot devices. IoT provides access to a large amount of information gathered by WSNs. However, the security of WSN and IoT comes at a cost, mainly due to privacy management issues. Therefore, this paper offers a comprehensive analysis of security threats against WSN and IoT, along with the strategies for preventing, detecting and mitigating those threats. The related defense mechanisms can help in building a safe IoT expansion and widespread understanding by getting familiar with the details of these attacks. The aim of this paper is to address and demonstrate the impact of the security problems on WSNs from the viewpoint of the IoT and its applications. In the analysis carried out for this work, a classification of available attacks and threats against these requirements has also been included.

INDEX TERMS Attacks, Internet of Things (IoT), security, wireless sensor networks (WSN).

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are one of the major technologies required for the implementation of Internet of Things (IoT) architecture. WSNs are the networks used for communication between sensors and radio transceivers. The functional capability and energy of IoT depends on the network interaction, cost efficiency, reliability, stability and productive operation. IoT is emerging effortlessly from the Internet. Recent developments in Micro Electro Mechanical Systems (MEMS) for wireless communication technologies have made it possible to design WSNs by collecting data from their local environments and transmitting information wirelessly to a realistic sink. The things connected to the internet vary greatly in terms of features. These things include from very tiny and static devices (RFIDs) to large and mobile devices. IoT is emerging as a dynamic cyber-physical network that is enabling smart devices to sense and change the world. Further it will assist the humanity in functioning and living. The presence of large network of interconnected objects leads to serious issues about security that restricts the wider use of IoT. Incorporating expertise in various practical fields of operation provides the benefits of more effective action and quick responses to the required modifications. The protocols used for communication and messaging are one of the key requirements of an IoT system. IoT will integrate a variety of applications into the Internet, e.g., automation, weather sensing, and Smart Grids (SGs). The latter is one of the most promising IoT applications. In SGs, Wireless Sensors are used to measure and keep track of energy consumption and production in order to optimize energy usage. WSNs have started to merge with the Internet of Things (IoT) through the introduction of Internet access capability in sensor nodes and sensing ability in Internet-connected devices. Thereby, the IoT is providing access to huge amount of data, collected by the WSNs, over the Internet. However, owing to the absence of a physical line-of-defense, i.e. there is no dedicated infrastructure such as

The associate editor coordinating the review of this manuscript and approving it for publication was Paolo Giangrande.

gateways to watch and observe the flowing information in the network, security of WSNs along with IoT is of a big concern to the scientific community. More specifically, for the application areas in which CIA (confidentiality, integrity, and availability) has prime importance, WSNs and emerging IoT technology might constitute an open avenue for the attackers. Besides, recent integration and collaboration of WSNs with IoT has opened new challenges and problems in terms of security. Hence, this would be a nightmare for the individuals using these systems as well as the security administrators who are managing those networks. Therefore, a detailed review of security attacks towards WSNs and IoT, along with the techniques for prevention, detection, and mitigation of those attacks are provided in this paper.

A smart object network can access the cloud directly through a gateway via cloud services (Amazon Kinesis). One of the essential tasks of the IoT is to incorporate the WSN as the primary communication technology for the IoT. WSN has standards which enable the devices to communicate with each other and with the edge gateway. In addition, complex communication is enabled by WSN, which is typically based on the 802.15.4 standard. Low rate WPANs is among the 802.15.4 IEEE protocols that fit the specifications of the IoT system [1]. Some of the benefits of this protocol include scalability, unassisted operation, requirement of less resources and lower operating costs. Additionally, to meet the needs of IoT applications, Bluetooth, ZigBee, PLC, Wi-Fi, 4G and 5G can also be selected as the networking protocols.

WSN enabled IoTs have wide-ranging scientific applications due to its rapid and low-cost deployment features as shown in Fig.1. Some of which are monitoring environmental events, collecting human activity information and analyzing them (elderly care, nursing, health care), providing mission-critical details (military operation, highway traffic), tracking industrial sites (plant production, manufacturing efficiency) and so on [2]. From now on we can expect that, IoT in the near future will have a significant impact on our lives. In order to communicate with other nodes to collect data from their surroundings, WSNs will be integrated into the IoT and countless sensor nodes will join the network. In the near future, IoT will have interaction between humans and the world through the growing use of WSNs. The effect of an increased understanding of the environment would benefit our planet from this integration [3].

After integrating IoT and WSN, security if particularly commissioned for mission-critical applications like electric power grid systems, first responder communication systems and so on is an important matter. One more domain for which security cannot be compromised is health care. Authors have found that most of the existing processes have failed to incorporate robust security services that can protect the privacy of the patient. If their confidential health data are exposed to misbehaving nodes, it would be devastating [4].

IoT with WSNs are susceptible to a variety of attacks that could pose credible damage to the network security. Security-related attacks of WSNs can be categorized into two major categories: active and passive attacks. It is also possible to categorize passive attacks further as eavesdropping, interruption of the network, server failure, network degradation and traffic analysis. In active attacks an attacker compromises the roles and activities of the targeted network. The real intent of the attacker would be to provide apparent damage that cannot be easily detected by the security systems. Active attacks include jamming, flooding, denial-of-service (DoS), black hole, wormhole, sinkhole, and Sybil types. Relevant surveys and classifications of security issues and attacks have been subsequently published in [5]–[10].

Wireless Body Area Networks (WBAN) is also one of major technology that is a major area of research taken up by various researchers across the world. WBAN uses IoT to provide solutions for healthcare surveillance, and investigates the safety and security problems associated with IoT healthcare monitoring. The suggested method uses a cooperative communication and network coding strategy to reduce faults, bit error rate, and energy consumption by minimizing channel impairment and body fading. A case study for remote Sepsis monitoring was created based on the suggested method. To minimize hospital re-admissions and death rates, the system uses cooperative communication to identify tracking indicators. Reliable communication technologies are extensively utilized in WBANs to overcome concerns of trust and privacy. Given the objective, authors have offered a trust-based communication method to assure WBAN's dependability and privacy. A cooperative communication technique has been utilized to assure dependability, while a cryptography mechanism was used to protect privacy [11], [12].

We have recently witnessed the rapid growth in IoT technologies to enable smart living, smart houses, smart workplaces and smart city. For these applications also detailed investigation of WSN and IoT integration along with security requirements is essential. This study is extremely thorough and systematic as it covers all attacks on WSN, detection and preventive measures for WSN and IoT integration. Moreover, apart from the strategies discovered while learning to secure WSNs, this paper also provides a guide for defending IoT against such attacks.

This paper is organized as follows. First, we have presented an overview of security requirements for different layers in Section II and the motivation for this research in Section III. Then section IV presents a survey of existing challenges to reduce those security issues in IoT and WSNs. Analysis of possible attack and threats towards the WSNs and IoT is studied in section V. Then we provided the summary of mechanisms for security has been explained in section VI. Strategies for WSN and IoT interoperability have been discussed in section VII and applications of WSN and IoT integration through case studies are presented in section VIII. After that, few networking technologies to provide interoperability to WSN with IoT are presented in section IX. Survey on Machine learning approaches to combat security challenges in IoT and WSNs are presented in section X. Finally the observations and conclusion has been outlined.

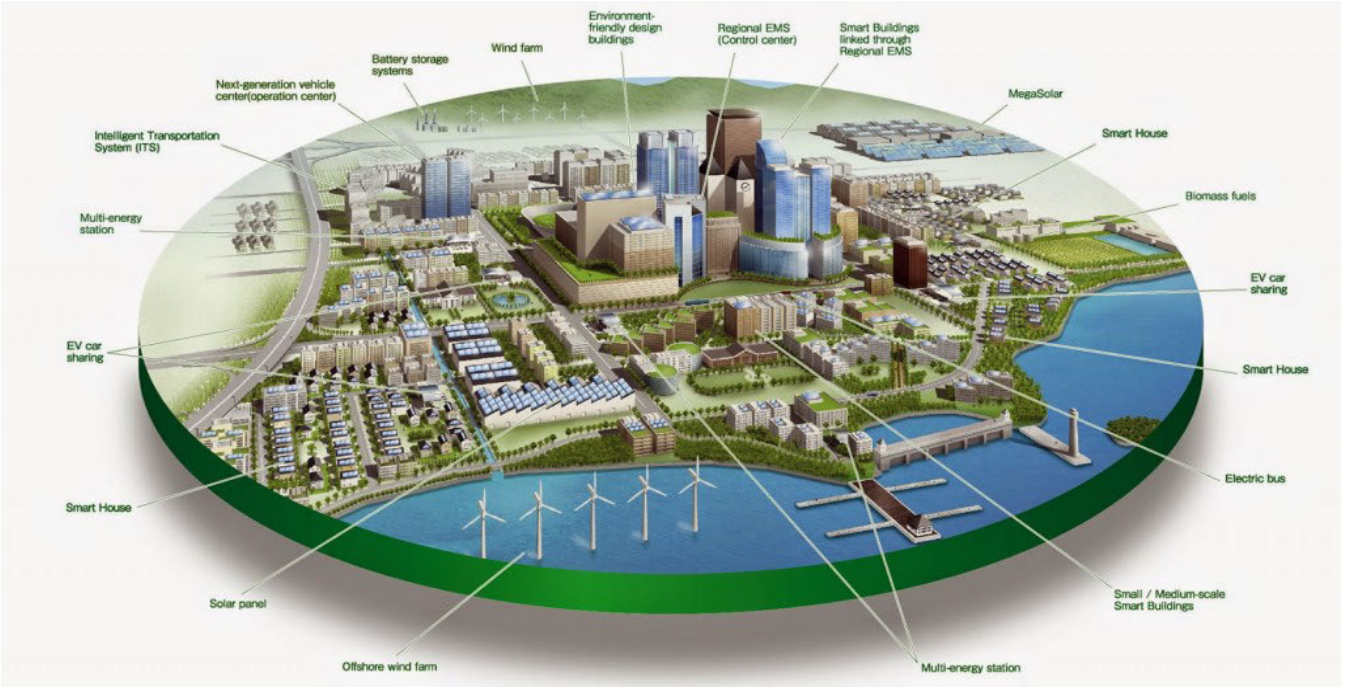

FIGURE 1. IoT integrated WSN practical applications [14].

II. SECURITY REQUIREMENTS FOR WSN AND IOT ARCHITECTURE

For Interoperability of IoT and WSN, study of security requirements is must. The IoT architecture has three layers (perception layer, network layer, and application layer). In securing IoT devices, hardware selection is particularly important. Authentication capabilities, end-to-end traffic encryption, secure boot-loading operation, compliance with digital signatures during firmware updates and transparent transactions are the IoT hardware problems. The introduction to IoT security threats as per the architecture of all IoT layers is shown in Fig. 2. Fig 2 shows the classification of security measures to be taken into consideration. Few of them have been discussed below.

In particular, confidentiality in a complex and dynamic environment is a mandatory aspect [13]. The ad-hoc enforcement of the WSN Offers lots of interesting advantages [15]. It can be seen as a potential key for IoT implementations, such as industrial surveillance, monitoring of the environment and health care [16]. The security requirements of WSNs and IoT can be classified into major and minor requirements [17], [18].

A. MAJOR REQUIREMENTS

The major requirements are as follows:

a) *Integrity of Data:* It ensures that the confidential information is never exposed to eavesdroppers and passive attackers, so that this information remains protected. Unauthorized parties should not be allowed to access the collected and transmitted sensory data. This is achieved by using data encryption in the data collection process with a hidden key, which is visible only to the desired recipients and receivers [19]. Data Integrity guarantees that malicious intermediate nodes due to the harsh communication environment of WSNs have never manipulated or compromised the gathered and communicated data within the WSNs.

b) *Source Authentication:* It is the process of ensuring the authenticity of the sensor data obtained and transmitted through the WSN by investigating the source and origin of the data. Source authentication is therefore very important for the decision-making and sharing of the WSN's control data [20].

c) *Availability:* This assures wireless communication and network resources are available for each sensor node, even in the existence of Denial-of-Service attacks. So, sensed information is gathered and communicated by the WSN because the availability of WSN is very critical to the IoT services and applications for survival.

B. MINOR REQUIREMENTS

a) *Data Freshness:* This is the freshness guarantee of each transmitted message that protects data communication mechanisms against repeated attacks. This is accomplished by ensuring that the old messages are not replayed again, so that the data transmission is updated, which can be achieved by adding a time-related counter to the transmitted packet.

b) *Self-Organization:* Depending on the organizational design of WSN, there is no fixed infrastructure that makes each sensor node autonomous and versatile to be self-organized in various circumstances.

c) *Time Synchronization:* In most WSN applications, it is necessary in order to achieve a power-efficient mechanism. The radio sensors could be switched off periodically.

d) *Secure Localization:* WSN's productivity also depends on its ability to detect all network sensors precisely and quickly. However, the threats have the ability to investigate false transmitted signal or to reuse signals of unsecured location information.

All the above mentioned security measures are supposed to be addressed while integrating IoT and WSN according to the demand of applications.

III. MOTIVATION

IoT will turn the entire planet into a smarter world. WSN and IoT devices are often installed in an unattended region where they cannot be physically monitored overnight in a day [20]. Intruders could take advantage of the weaknesses of external surveillance and can receive information from the planting site from certain IoT sensor nodes. By using data retrieved from the seized nodes, the opponent can assign nodes to adversaries and connect them to the existing infrastructure. These malicious nodes can then run a series of network attacks. These attempts can compromise network connectivity, quality and effectiveness. We may notice a decline in connection speeds, a rise in delay and also a decline in the packet forwarding ratio. Intrusion detection protocols are extremely important to avoid these kinds of activities. In this investigation, we have taken up a survey of existing network security protocols for both WSN and IoT applications. This survey work which has been conducted for WSN and IoT would benefit all the researchers working in this field.

IV. CHALLENGES TO OVERCOME SECURITY ISSUES REQUIRED FOR WSN INTEGRATED IoT

Major challenges worthy of focus for WSN to securely become an intrinsic part of the IoT have been provided in details in this section. These obstacles are closely related to WSN, but also relevant to IoT. Some of the most significant issues are as follows:

a) *Security:* Sensor nodes are critical part of WSNs for ensuring the data privacy, transparency, and authentication. By connecting WSNs to the internet, the proximity to the location requirement will not be needed anymore and attackers may threaten WSNs from anywhere. On top of this, because of diversity of locations, WSNs may need to counter new threats, including malware developed and emerging from internet connection. The majority of existing WSNs that are linked to the internet is secured by one strong and special gateway that guarantees successful security. Yet a simple reuse of these current protection measures is difficult due to lack of capacity, memory, and computational power of control nodes. Many internet services use cryptography with broad key lengths, which is not accepted by sensor nodes. Therefore, for power constrained WSN and IoT networks, new safety mechanisms have to be developed for new attacks emanating from the internet.

b) *Interoperability of Preventive Measures and Acknowledgement by Users:* IoT security is not only a collection of various problems, but also from a broader perspective, is an important field for research. We might have knowledge of few technologies to fulfill a limited range of safety requirements, but their integration with other technologies will lead to additional standards that have not been taken into account yet. As far as the user's point of view is concerned, the IoT should be able to accomplish their needs without relinquishing the security aspect.

c) *Data Privacy:* Data protection is a serious concern. The information about a specific user has personal data along with data produced by the objects accompanying the person. It is necessary to decide and be aware of who regulates the relevant information. And how well the person can be self-assured about the data security that it cannot be used without authorization. The data part also needs to be shared in order to provide security services in some cases. A person at times also has to let his or her health specifics easily

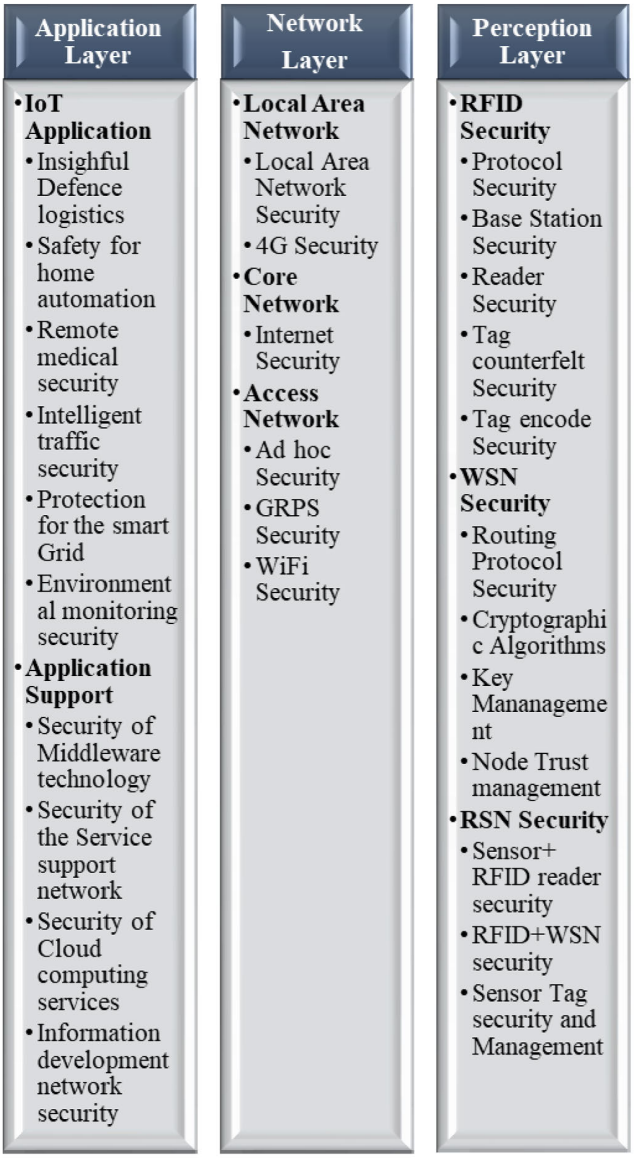

FIGURE 2. Typical IoT security architecture.

accessible to the hospital professionals in an emergency situation. Data protection is a matter of interest too for business scenarios similar to individual users. A large scale of data flow would be generated by any organization using the strategies offered by the IoT. All information should stay private and be accessible only when necessary.

d) *IoT Components:* One more critical factor that needs to be considered is the safety of components by utilizing suitable measures for security protocols at the network level. Given that IoT is a global and highly integrated infrastructure, it is critical that a variety of different technologies, standards and authentication models are implemented in order to provide adequate assistance. From a safety perspective, the fundamental properties and infrastructural facilities must be capable of managing a combination of recognition and security mechanisms in a consistent and scalable manner. Achieving an optimal solution for stable communications among the resources and products is one of the most significant issues in IoT.

e) *Quality of Service:* Sensor nodes contribute to the quality of service operations by optimizing the productive use of the energy of all heterogeneous sensors that would be a part of the future IoT, via gateways operating as repeaters and protocol translators. A huge amount of capital cost, including security mechanisms is needed to improve QoS. However, recent techniques for achieving QoS on the internet are not relevant for WSNs, as large variations exists in the properties of the route which results in a major restructuring of the WSN topology. It is indeed essential to find technological innovations to achieve delays and risk guarantees.

f) *Configuration:* Sensor nodes can help in controlling the WSN setup, such as addressing the administrator to verify networks adaptability and its ability to repair by finding and preventing node faults. However, on the World Wide Web, self-configurable nodes are not usually available. Instead, the user should install applications and the machine should recover from the crashes. Conversely, the unattended autonomous sensor nodes need new activity configuration for management of the network.

g) *Fault Tolerance:* Because of the harsh atmosphere, sensors could fail, but WSN should not be affected by this failure. Therefore, algorithm or protocol built for WSNs should have the capability to withstand faults. Different types of fault tolerance approaches have been correlated to the demands of the application. For household applications, there is less need for fault tolerance because sensors cannot be easily affected. However, for outdoor environments or harsh climate a high fault tolerance is necessary to prevent the risk of failure [21].

h) *Timing of Data Delivery:* Delay in WSNs and IoT based systems depends on the delay in the delivery time of data. For example, if healthcare professionals do not receive alert messages, patient lives would be at risk. While designing protocols, the total disparity between both the transmitter and the receiver should also be analyzed. It is necessary to consider the minimal permissible delay based on specific application demands [22].

i) *Scalability:* As hundreds of nodes are distributed on the basis of an application and the developer should be aware of the risks associated with the possibilities of expanding the network and large population of sensors must be used to cover as much ground as possible.

j) *Energy Consumption:* Rechargeable batteries cannot be used in some applications. Therefore, the life of the battery greatly influences the life of the node and the functioning of the existing network will be adversely affected resulting in compromise of the security of the entire network. Detection, encoding, sending and extracting are the key activities for which the sensors consume energy [23]. In addition, noise can increase the power consumption due to retransmission. Information transfer technologies for WSNs were explored to minimize energy consumption. The findings indicate that information transmission absorbs more energy than data analysis. Numerous power consuming communication operations are carried out in WSNs, such as propagation, interpretation, frequency synthesizers, voltage control.

k) *Gathering Data:* Depending on information analysis, WSN applications can be either Event Detection (ED) or Spatial Process Estimation (SPE). ED is used to predict a particular incident by the use of sensors and SPE estimates physical conditions. Both have different applications.

l) *Homogeneous vs. Heterogeneous:* WSNs with similar and different sensors are referred as homogeneous networks and heterogeneous networks respectively. Homogeneous networks are simple to handle, while heterogeneous networks can provide an effective solution because of different energy models for different sensors [24]. A heavy task is delegated to some nodes because they all have higher amount of energy than others. These are known as cluster heads which work as a path locator for cluster member nodes. So, heterogeneous networks would enhance the survival of the network. However, homogeneous networks are quickly implemented. In addition, cluster heads can be switched off to prevent the death of the nodes [25].

m) *Communication Architecture:* Sensing and routing of data to the sink are two of the sensor node's major tasks. The sink node and all nodes on the network follow the communication architecture or protocol stack [23].

In order to integrate WSN with IoT as per the demands of the application, all the above mentioned challenges are supposed to be addressed to overcome security issues.

V. ANALYSIS OF POSSIBLE ATTACK AND THREATS TOWARDS THE WSNS AND IoT

This section presents a classification of security attacks targeting higher-level WSNs and IoT systems on the basis of different parameters.

a) *Target-Based Attacks:* These types of attacks threaten secrecy of the target either actively or passively. Sensitive information (encryption keys) is provided to passive attackers without notification to authorized users. They use such information when weakly encrypted data is decrypted. Examples of passive threats are eavesdropping and traffic analysis.

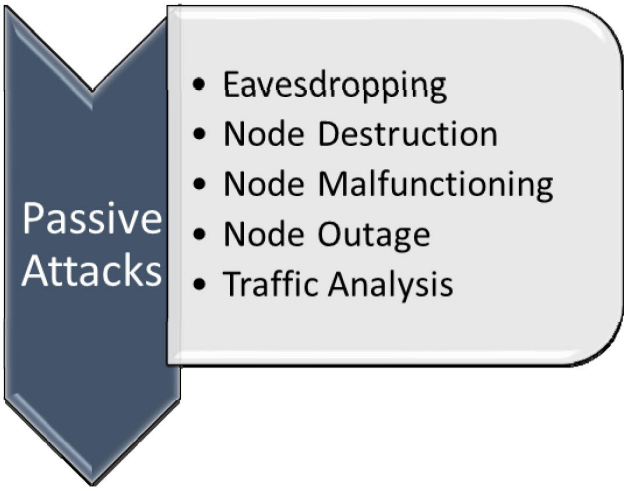

FIGURE 3. Passive attacks.

In the meantime, active attackers monitor the network and gather confidential data in order to control the network and modify the data.

b) *Location-Oriented Attacks:* These attacks are of two types (internal and external attacks) depending on the position of the attacker with reference to the network functioning. Through decryption keys, an attacker can access essential information. Hence, this form of attack is difficult to detect. Internal attacks can cause misrouting, dropped packets, eavesdropping and data modification. External attackers may cause network congestion by sending large quantities of data, such as DoS attacks.

c) *Attacks Based on Layers:* These attacks are classified according to the protocol stack layer on which attack is performed. Each stratum is vulnerable to various attacks. The data link layer can be attacked with the following:

1) Data attack flooding allows nodes to enter the channel using carrier sensing protocols and there is a high chance of collision.

2) Unfair attacks occur with malicious nodes transmitting data packets despite of waiting for a suitable period to enable other nodes to enter the platform.

3) Exhaustion attacks are the ones where malicious nodes transmit a high proportion of invitation signals to deplete other nodes batteries.

A. SECURITY ATTACKS IN IoT AND WSNS FOR DIFFERENT LAYERS

Network attack is an effort to attain the security, authentication, reliability or functionality of the network. WSNs are known to be part of the IoT network and are subjected to various attacks. Thus, we have considered the attackers (passive/active) behavior as the key categorization factor and the intended Open Systems Interconnection (OSI) model as a sub classification model which has been shown in Fig. 3 and Fig. 4.

B. PASSIVE ATTACKS

Passive attacks are not easy to be sensed by any means because of the lack of radio emissions produced by the adversaries. Passive threats are also against privacy. The attackers usually get camouflaged in passive attacks and break the communication channel to collect data. Eavesdropping, node malfunction, node tampering/destruction, node disruption and traffic analysis can be categorized as passive attacks (see Fig. 3). In some articles, node failure, node loss and node exploitation are treated as active attacks. In this paper, we have described them as passive attacks because they do not constitute a serious concern and the system will keep functioning without any engagement of damaged nodes within the network compared to other important active attacks.

1) PASSIVE DATA COLLECTION (EAVESDROPPING)

The compilation of passive knowledge is referred as eavesdropping. One can cause data loss the confidential data by tapping communication channels. WSNs employ short-range communications and this makes it easy for intruders to extract valuable information by eavesdropping.

Compared to other long-range wireless systems, WSNs are safe against tapping because they transmit signals for smaller distances. Significant data, such as the location of specific nodes, message IDs and almost all that is not secured, can be revealed by the interception of information transmitted via WSNs.

2) NODE DESTRUCTION AND MALFUNCTIONING

Destruction of nodes occurs because of electrical faults, brute force attack or by any means. While malfunctioning occurs because of various parameters arising from defective sensors, energy loss occurs due to faulty sensors and DoS attacks.

3) NODE OUTAGE

It occurs whenever the node does not work properly. To reduce node outages in the network, there is a need of efficient WSN protocols to replace new cluster head in place of an earlier one of a heterogeneous network which should be operating reliably and can follow alternate routes for data transmissions.

4) TRAFFIC ANALYSIS

Analysis of network traffic can be as important as the data packet material is for adversaries. An analysis of traffic patterns can help extract valuable knowledge about the topology of networking. Sink nodes are closest to the base station and they facilitate more transmissions than the other nodes. Therefore, base stations near cluster heads are at more risk of denial-of-service attack or eavesdropping of the packets. This kind of useful knowledge can be obtained by analyzing the traffic. In addition, traffic trends can include other confidential information, such as behavior. Silence may signify preparedness of an attack or a move and an increase in traffic rate may also signal the attack is going to occur.

C. ACTIVE ATTACKS

Suspicious actions are carried out during the attacks to affect the confidentiality of data and integrity. In the physical and/or network layer, an example of this is DoS (Denial of Service) attack that would cause packet loss for the network elements. DoS attack specifically attacks the network service availability. DoS are an attack that utilizes resources by minimizing the network performance and its desired functionality by blocking incoming and outgoing packets. In active attacks opponents cause detrimental impact on the operations of the attacked network or on the attacker's target. As a result of these attacks, the networking infrastructure could be compromised or can stop functioning. In order to gain access to the confidentiality of the network infrastructure, the adversary often seeks to remain undetected. WSNs active attacks are grouped into five key groups based on the OSI stack protocol layers as shown in Fig.4. We have discussed about the layer wise active attacks in the next section.

D. PHYSICAL LAYER ATTACKS

1) JAMMING DoS

It functions as a DoS attack on the physical layer. A signal can be jammed at the frequency of the transmitter by a malicious device. Noise gets added to the carrier signal because of the jamming signal and causes signal-to-noise ratio to reduce below the level with which the signals can be processed by the nodes using that channel. Jamming can be carried out continuously in an environment that prevents all the nodes from communicating in that area. Alternatively, jamming with random n time intervals can be achieved briefly, but can also affect the communications [26].

2) NODE CAPTURE (TAMPERING)

The attacker gets hold of the sensor through a physical attack by attaching cables to its circuit board and accessing the private information and also by a continuous transmission in the WSN [27]. The manipulating adversaries can modify the initial electronic board wiring or the node memory content and the captured slave node can be used by any other means. Capturing a node could reveal its sensitive data, especially the disclosure of cryptographic-related keys and could result in compromise of the entire WSN information security. Key management provides the creation, delivery, declaration, modification, storage, recovery, validation, and destruction of key. It also reduces interferences with nodes of the WSN and physically accesses nodes of the WSN for extracting their data (encryption keys and other confidential information) [10].

E. DATA LINK LAYER ATTACKS

Data link layer MAC algorithms give multiple opportunities for DoS attacks to be targeted and DoS attacks on MAC layers can continuously jam a channel. More nuanced DoS attacks can be conceived based on schemes addressing the MAC layer. Attacks on the data link layer are classified as follows: collision, sleep denial, de-synchronization, fatigue, flooding, jamming of the network layer, spoofing and unfairness. The collision occurs when the transmission of various nodes occurs at the same frequency range simultaneously. Collision attacks absorb all of the WSN nodes energy until these nodes are dead. The description of data link layer attacks is as follows:

a) *Collision:* An intruder proceeds to send the packet from the same channel of the authorized node in the system as soon as this node starts to transmit and causes a collision of transmitting packets. The destination node would not be able to collect the packet from the sender because of the transmission collision. The recovered packet is dropped and the transmitter requests for packet retransmission. The single byte inconsistency of message is sufficient to cause a CRC (Cyclic Redundancy Check) error and ultimately destroy the entire message. The collision attack is much more destructive than the jamming attack, since the propagation energy consumed is less (because of short use of the radio).

b) *Denial of Sleep (Sleep Deprivation Torture):* Prevention of a node sleeping to reduce exhaustion of the battery leads to energy depletion. This can be from attacks of collision or repetitive handshaking. A node is forced into depleting entire stored energy of its batteries in this attack.

c) *DE Synchronization:* A protocol for MAC layers implemented in IEEE 802.15.4e is Time Synchronized Channel Hopping (TSCH). This reduces accuracy and has short duty cycles. TSCH attacks occur when an attacker transmits messages in the time slots assigned to them, to other users. This enables packets to get misplaced and overlap with one another. An intruder may cause a number of such incidents after regularly evaluating the back-off times that would ultimately cause de synchronization of the neighboring nodes.

d) *Exhaustion:* This attack occurs if the collision attack persists until its energy is exhausted by the targeted node. This form of attack can be carried out using a normal node which is capable of transmitting radio signals in the same band as the rest of the sensors.

e) *Link Layer Flooding:* Through sending excessive MAC data packets or MAC control packets to their neighboring nodes, a malicious node in this type of attack violates the fairness of media access. Victim nodes eventually suffer from DoS or their battery power is exhausted. This attack can also consume channel bandwidth resources [28].

f) *Link Layer Jamming:* In order to jam the packets in this mode of attack, the most important data packets are targeted. It has been shown that this attack is successful against MAC protocols such as B-MAC, L-MAC, and S-MAC.

g) *Spoofing/ARP-Spoofing:* An intruder spoofs node MAC address and then produces a mix of additional valid identities from the victim node and uses them elsewhere in the network [8], while an attacker sends spoofed ARP (Address Resolution Protocol) messages to the device in an ARP spoofing. The objective is to connect the MAC address of the attacker with the physically stronger IP address of the node

such as in the default gateway allowing any traffic to be sent outside of that IP address.

h) *Unfairness:* Irregular attacks or MAC cooperative protocols could cause degradation in the network performance. Unlike the DoS attack, in this attack node does not get separated from the network. But few blackouts occur in which clients can transmit or receive delayed messages. The network quality degrades by this attack, so it is beneficial for less number of sensor nodes because the participating nodes in the MAC protocol configuration miss their transmission deadlines.

F. NETWORK LAYER ATTACKS

Network layer attacks cause data packet injected into the network and results in network traffic or congestion along with loss of power resources across the network. The overflow routing table attack causes a non-existent node to create routes [29]. Few network layer attacks are:

a) *HELLO-Flooding:* An attacker following a routing protocol with a usually large transmission range broadcasts a ''HELLO'' message for advertising to the existing network in order to convince other nodes that it is one of the neighboring nodes. Nodes that receive a ''HELLO'' message might assume that sender is located near them, which may result in ''HELLO'' flood attack. A malicious node could flood ''HELLO'' packets with processing power, high enough to convince nodes that they are located near them and causes packet loss. A number of network and MAC layer protocols ask nodes to send a ''HELLO'' message to announce their existence near them. Nodes that receive this message, presume that, although it is not correct, it is within the sender's normal radio range. ''Flooding'' is a spread of a signal throughout a multi-hop topology in the network.

b) *Hole Attacks:*

1) *Black Hole:* A corrupted node could lose many packets instead of forwarding them. These types of attacks will avoid all traffic data around the black hole. This attack is also referred to as ''selfishness.''

2) *Sinkhole:* By transmitting all the surrounding nodes, a malicious node will proclaim that it is the best next hop to send packets to their destination. Due to its location, a sinkhole acts as a hub and starts collecting all the packets going towards the base station. All network traffic is routed to this sensor point, but the sinkhole node does not drop any packets in this situation. This route believes the IDs to remain invisible for any subsequent attacks and creates a number of opportunities. Since all the network traffic passes through this particular node that essentially ''sinks'' all the information it receives, the attack is called a sinkhole attack.

3) *Selective Forwarding:* It is also known as a ''gray hole attack,'' since it is a black hole attack variant which drops the data packets of their choice and thereby data packet identity stays unnoticed. Similar to sinkhole attacks, as the malicious node is the part of several routes, all of them will be affected, but instead of dropping all packets, certain packets are dropped selectively while others are redirected to avoid detection. Packet forwarding is a big burden on a routing node. In case of Multi-hopped networks, it is assumed that the involved sensor nodes would transmit the information they receive. But, in a selective forwarding attack, opponent nodes have a choice to drop or refuse data packets. An attacker operating as a black hole attack does not send every packet it receives and suffers from the risk when neighboring nodes starts concluding that it has lost and changed its route.

4) *Wormhole:* Between two nodes, a passageway is generated, which can be used to transmit packets more speedily. Two different segments of the network are advertised to draw local traffic as neighbors [8]. Data packets can be received by a malicious node and transferred from the channel by another malicious node located in another part of the network. The packets are sent back to the second malicious server after that. It takes more time for packets following standard paths to enter the destination node than those sent through the wormhole and get dropped due to more hops.

c) *Node-Replication (Clone):* Node duplication (clone) attack is an alarming attack because replicas of damaged nodes can be intentionally located by an intruder to incur defects in the network [29]. They can allow attackers to subvert data aggregation, inappropriate behavior detection, and affect protocols by introducing corrupt data [30].

d) *Routing Attacks:*

Misdirection: Intentionally forwarding messages towards wrong paths is a misdirection attack. Main causes include false routing advertisements and forcing routing tables of adjacent node to get updated by false data. This attack is a DOS attack because the target nodes are absolutely blacked out and false routing information does not let them accept any additional packets.

1) *Routing Loop:* A routing loop exists in the direction of the route. It is developed by spoofing the routing changes. An attacker might assume that node A is not in the radio range of node B and would send a false routing update to a node by using the wrong source address by indicating that it was originated from node A. Node B after considering node A as its parent, forwards the data packet over the routing path suggested by A. After hearing the routing update from node B, node A will now consider node B as its parent. Loop messages sent from A or B and B to A may result in the energy depletion and the final collapse of the network.

2) *Rushing:* This attack affects ad hoc network routing protocols that results in DoS. For example: AODV, DSR, ARAN and SAODV are unable to discover longer routes because of this attack. Rush attacks are especially harmful to networks and most of the opponents can implement them [31]. Malicious nodes can change (Spoofed, Manipulated or Replayed Routing Information) the routing information shared between nodes in order to affect the routing scheme.

e) *RPL:* IoT is composed of limited resources such as battery operated nodes, memory, processing capabilities and so on. For this type of network, a new network routing protocol called RPL (Routing Protocol for Low Power and Lossy Networks) has been developed. RPL has been proposed,

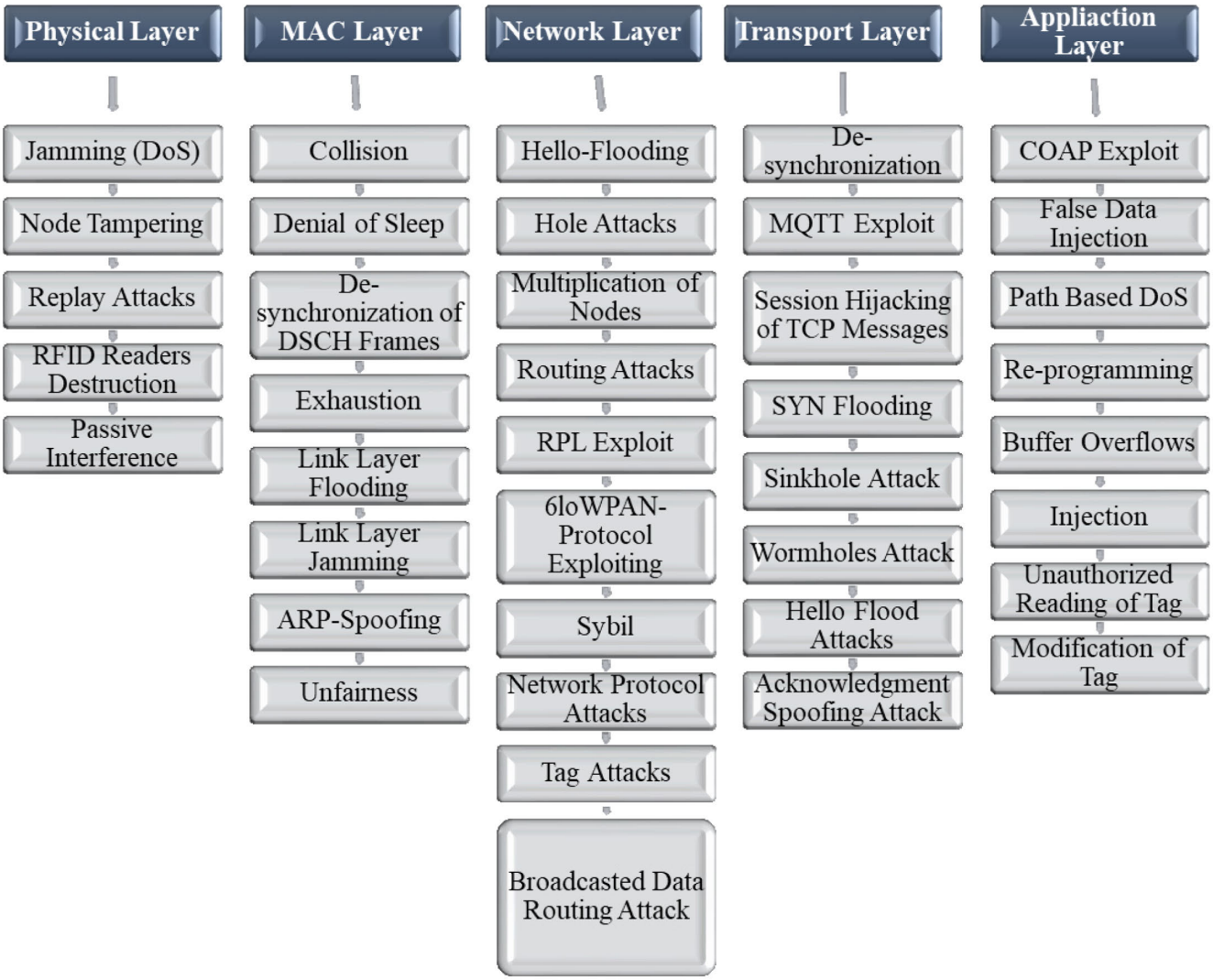

FIGURE 4. Active attacks.

specifically for multi-point to point communications data sinks. The analysis of various attacks on the IoT has been addressed in [32]. "Attacks against Routing Layer", have been presented in [33]. In this paper, few attacks directed against the RPL protocol have been explained. The various RPL protocol attacks include: local-repair attacks, Rank attack, DODAG version attack, DIS attack, and Neighbor attack. This causes the local repair loop to be followed by the surrounding nodes. These attacks affect the distribution ratio, produce a large number of control packets and increase the delay from end to end. By creating the loop-free topology, RPL produces the Destination Oriented Directed Acyclic Graph (DODAG).

f) *6LoWPAN Attack:* 6LoWPAN is an Internet protocol designed for IoT based systems. 6LoWPAN incorporates IP infrastructure and WSNs by defining how fragmentation and reassembly of data fields in IEEE 802.15.4 will route IPv6 packets. In a particular 6LoWPAN attack, for fragment replication the attacker positions his own fragments in the form of a chain of fragments. This attack occurs when the fragment source is similar to the received fragments of the IPv6 packet due to which the receiver is not able to find the 6LoWPAN layer. Therefore, a receiver can be easily fooled and cannot check spoofed fragments because of the lack of an authentication mechanism to verify the original or duplicate fragment. An appropriate process should be used to reduce more attacks like a DoS attack [33]–[35].

g) *Sybil Attack:* When node exhibits multiple identities, then network confusion arises, due to which nodes are forced to follow conflicting routing paths by the attacker. This places a serious challenge for fault tolerance schemes. The fusion and distributed storage may also be affected.

G. TRANSPORT LAYER ATTACKS

End to end communications between the two nodes are managed by the OSI protocol stack of the transport layer. Attacks

affect those protocols on the transport layer that hold connection information at the ends. The following are classified as causes of transport layer attacks:

- A corrupted node introduced for suitable communication with its neighboring nodes by supplying false routing information.
- Large number of false identities if being communicated to the WSN. Generally, protocols such as distributed storage and fault tolerant systems are easily affected by this attack.
- A link between two parts of the WSN affected by poor latency and capable of replaying an attacker's network message.
- A high-powered transmitter node can be used by the adversaries to cause Hello Flood attacks and could confuse multiple nodes into believing that they are neighbors and within their range.
- New connection requests are often created and when link resources are exhausted, valid requests get ignored. This can be achieved by consistently spoofing messages in the direction of the end host before retransmitting the missing frames.

1) DE-SYNCHRONIZATION

An attacker interrupts the real communication between the nodes by desynchronizing the rate of transmission. Transmission of misleading data and false packet transmission sequences with fake sequence numbers and desynchronizes endpoints for data retransmission. Thereby, continuously causing both sides of the negotiating parties to break their synchronization.

2) MQTT

Message Queue Telemetry Transport (MQTT) is a networking standard for the publication of devices that are resource-constrained, such as low-power embedded sensors. In the IoT domain, MQTT is commonly implemented using a publish-and-subscribe messaging system for communication. MQTT does not have a preset protective layer and the user has to handle security problems. MQTT and its variants need a scalable, lightweight and robust protection framework for deployment in IoT [36], [37].

3) SESSION HIJACKING

In order to gain access to the information on a computer, this attack causes manipulation and interference with a legitimate communication session can be called as a session key. Session hijacking of TCP messages as an extension of IP networks can also be a cause of trouble for IoT networks.

4) SYN-FLOODING

In a flooding attack, an attacker is able to drain a node's resources by flooding it with false messages. This is accomplished by sending several requests for connectivity, gradually overflowing the buffer and causing the node to die without the link being established.

H. APPLICATION LAYER ATTACKS

DoS attacks, including node localization, time synchronization, aggregation of information, collaboration, and fusion can affect application layer protocols. A malicious node by trying to impersonate a node, by providing false geolocation data will interrupt a node localization system. Since this form of attack reduces the network service associated with it, it can also be referred to as DoS attacks. The description and definition of attacks on application layer are as follows:

a) *CoAP Exploit:* Constrained Application Protocol (CoAP) is a protocol for providing interactive functionality to the rest of the internet as an HTTP replication for small IoT devices. Recently, CoAP has been used by many IoT implementations, which means it will play an important role in the future IoT applications. As stated by authors, the implementation of CoAP poses several security related challenges [38]. It does not translate completely HTTP features, which generates multicast messages with security issues.

b) *False Data Injection:* Captured nodes deliberately insert false data into the WSN to affect the overall result of a calculation.

c) *Path-Based DoS:* This DoS attack occurs within the application layer. An attacker overpowers nodes over a remote location by flooding an end-to-end communication route with either generated packets or broadcasted packets and impacts all nodes along the path from source to destination [39].

d) *Re-Programming:* Each network feature must be patched or re-programmed once in a while for version control, code creation, encoding-decoding, or when switching to a newly written application. If this reprogramming schedule is not kept secret, this vulnerable network time window can be used by opponents simply by sending false messages to the nodes and moving them to an unstable or dead state.

e) *Sensor Overwhelming:* It is an attack which changes the accuracy of the measurements by the sensor. The process consists of targeting sensors with artificial interference or blinding them entirely with bogus signals and flooding them with false stimuli.

VI. SUMMARY OF ATTACKS WITH SOLUTIONS FOR WSN AND IoT

All attacks against WSNs and IoT are listed along with possible defensive solutions associated with the respective attacks in Table 1. Being familiar with these attacks and their related security solutions would help researchers to securely build public trust and acceptance in the development of IoT integrated WSN algorithms, applications, and concepts.

Among all the attacks or security concerns, the counter measures for sinkhole and wormholes are necessary to be integrated with the design of the routing protocol. So that these attacks cannot affect the system security. In the same

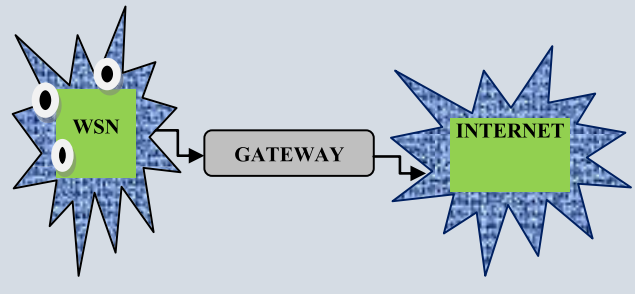

FIGURE 5. Independent network.

sense, the geographic routing protocol is one type of protocol that offers flexibility [40]. One important downside to the topology of multi-hop routing involving a collection of fixed base stations is that the base station nodes can be compressed into one or two hops. After a large number of such nodes are affected, the network is interrupted. This means that clustering protocols LEACH [41] and PCAC will destroy healthy nodes and will aim for those solutions where cluster heads interact with a base station directly [42].

VII. WIRELESS SENSOR NETWORKS AND THE INTERNET OF THINGS: INTEROPERABILITY

WSNs must be integrated into the ''IoT'' when sensor nodes access the internet and use it to connect and function more effectively. Although WSNs are integral part of the IoT, we need to carefully research and solve the associated challenges. Unlike desktop computers, IoT devices typically depend on the different short range wireless communication and networking [43]. Network level interoperability deals with the seamless sharing of messages for communication between systems across different networks. The system shares data through different networks with other systems in order to make the systems interoperable. Problems such as addressing, routing, resource use, protection, QoS and mobility should be addressed at the network interoperability level, due to the complex and heterogeneous network environment in IoT [44].

Among the three key approaches described, it is possible to link WSNs to the Internet, which varies from the degree of incorporation of WSNs to the Internet structure [45]. The first solution proposed was embraced by most WSNs for accessing the web and for providing the highest network abstraction (Fig. 5), which helps in linking of all independent WSNs and the web via a single gateway.

The second approach (Fig. 6) demonstrates the degree of WSN and IoT compatibility and generates a hybrid network that is still composed of separate networks and few dual sensor nodes are able to use the internet.

In Fig.7 the third solution is inspired by the current WLAN system and creates a dense 802.15.4 access point network that allows several sensor nodes to access the internet in one hop.

It is evident that because of the uniqueness of gateway, the first approach leads to a onetime failure. The link between both WSN and the internet networks would break down because of gateway instability. With multiple gateways and access points, such vulnerability is not present in the second and third scenarios.

As they ensure network robustness, they are favored. The option between each of the remaining integrative approaches is affected by the scenario of the WSN application. This attack will therefore be particularly suited to deployments of ''monitoring space'' and of ''monitoring interactions between objects and space''. By offering one-hop internet connectivity, WSN applications will follow the third approach. Generally following a star topology, the WSNs involved can sustain such an arrangement by accepting a central gateway without internet connection instead of a common base station. So, this third approach could be appropriate for tracking objects and human beings [96].

Both the second and third approaches for integration only promote static network configuration. A time-consuming gateway reprogramming is needed for each new computer wishing to connect to the Internet. Thus, in their present configuration, the versatility required by the future IoT cannot be achieved by both approaches. It may be necessary to take the ''IP to the Field'' paradigm to fulfill the versatility expectation. Sensor nodes are supposed to be intelligent network components in the model under consideration, which will no longer be restricted to sensing tasks. After switching the expertise to the sensor nodes, the gateway functionalities will be confined to redundancy and protocol translation. As a result, the dynamic network will no longer need gateway reprogramming operations.

From a network viewpoint, it is important to first investigate what sort of integration techniques should be used to link all infrastructures if we want to learn whether or not a WSN can be completely integrated with the Internet. One can describe the methods in two different ways: stack-based and topology-based [45], [98].

A. STACK BASED CLASSIFICATION

The degree of convergence in stack-based classification between the internet and the WSN focuses on the overlap between the two stacks on the network itself. A WSN may be completely independent of the internet in Front-End, can exchange data in Gateway or can share network layer in TCP/IP. Fig. 8 below shows interoperability approaches.

The first phase is the Front-End solution inside the stack-based classification.

1) FRONT-END SOLUTION

In this strategy, the external internet is the host and the sensor nodes are never in immediate contact with one another. Indeed, the WSN is entirely independent of the internet and can adopt its own set of protocols, such as Wireless HART for SCADA environments [99]. This handles all contact between the outside world and the centralized unit of the sensor network, such as the base station. The base station can store information from the WSN and provide them to external entities through well-known interfaces [100]. It is

TABLE 1. Security attacks for WSNS and IoT along with the suggested defence solutions.

Attack	Layer	Detection Solution	Prevention/Mitigation
Eavesdropping	All layers	N/A	• Multicast model of sensor Display communication [46], • Pre-distribution key [47] • Encryption link-layer [48], [49], [50]
Jamming-DoS	Physical Layer	JAM (mapping) [52], Swarm intelligence [53]	• Spread-spectrum contact usage [50], JAM (re-routing) [51], Wormhole technique [52]
Tampering	Physical Layer	Routinely conducting physical controls	• Tamper immune hardware, JTAG disabling and/or bootstrap loader protection [54], camouflaging
Denial of sleep and Flooding	MAC Layer	Anomaly detection on motes [66]	• N/A
De-Synchronization	MAC Layer	N/A	• 6TiSCH [55]
Unfairness	MAC Layer	N/A	• Usage of small frames [55]
Blackhole	Network Layer	Mote detection anomalies [56], REWARD [57], Active Trust [58], Packet count [60], TinyOS beaconing [91], Honeypot [61], Watchdog [62], Algorithm for pseudo clustering [63]	• REWARD routing [58], Multi-path routing [64], Topology of the mesh network [67], Routing of Active Trust [58], Isolation [59], BAMBi [60], MAODV [66]
HELLO flooding	Network Layer	Bidirectional verification technique [67]	• Protocol for identity verification [35], Multipath multi-base station routing [67], TESLA [48]
Node-Replication (Clone)	Network Layer	SET [68], Random pairwise main pre-distribution[69], Social fingerprinting [67], Speed test [71], Multilevel clustering [72] are Centralized solutions	• Public ID-based keys [73], Location-based key management [74], Multilevel clustering [72]
RPL DODAG version	Network Layer	SDC and P-MPC [75], RED [76], MEM [77], RDE [79], SDC and P-MPC [75], MEM [77], RDE [78]	• Integrity checks, VeRA [79]
RPL local repair	Network Layer	N/A	• Inclusion of timer in local link repair messages, VeRA [79]
RPL rank	Network Layer	N/A	• TRAIL [77], VeRA [79]
Selective forwarding (Grayhole)	Network Layer	N/A	• Multipath routing [81] , Usage of source authorization [51]
Sinkhole	Network Layer	Anomaly detection on motes [28], Acknowledgment monitoring [83], Neighbour knowledge [84], Packet drops were reported [85], System for failure detection [84]	• Secure routing algorithm [85]
6LoWPAN exploit	Network Layer	Network flow graph [87],Geo-statistical approach to sampling and distributed approach to monitoring [88], Redundancy mechanism [89]	• 6LowPSec [35], Content chaining scheme [81]

TABLE 1. ***(Continued.)*** **Security attacks for WSNS and IoT along with the suggested defence solutions.**

Sybil	Network Layer	N/A	• Indirect validation [81], Identity verification [49], Isolation [46], ID-based public keys [73]
Wormhole	Network Layer	Testing of radio tools, ID-based symmetric keys, registration, verification of location, attestation of code [51], RADS [46], Packet Leashes [29], Directional antennas [77]	• Location-based keys [73], Centralized computing [78], DAWWSEN [91]
De-Synchronization	Transport Layer	N/A	• Utilization of authentication, including protocol headers of the transport layer [56]
SYN-flooding	Transport Layer	N/A	• SYN-cookies [92], Client puzzles [93]
MQTT exploit	Transport Layer	N/A	• Enforcement of security policies [94], SMQTT [40]
Session hijacking	Transport Layer	N/A	• Lightweight user authentication algorithm for mobile network routing optimization [95]
CoAP exploit	Application Layer	N/A	• CoAPs, employment of DTLS [38]
False data injection	Application Layer	SET [96]	• Collective secret [96]
Path-based DoS	Application Layer	N/A	• One-way hash chains

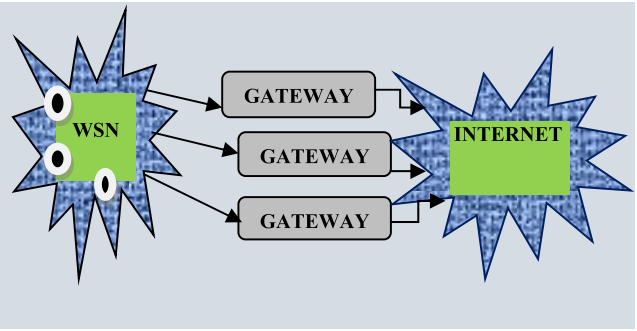

FIGURE 6. **Hybrid network.**

also important to forward any requests from internet hosts to the base station.

B. GATEWAY SOLUTION

It assumes that the base station is the gateway for the application layer, which is responsible for interpreting the layer below network layer and transferring the data from one point to another. As a consequence, web hosts and sensor nodes can address and exchange data without having a direct interface. The WSN remains independent of the internet in this method too, so all queries will need to pass through a gateway system.

C. TCP/IP SOLUTION

A TCP/IP stack is implemented by sensor nodes. In 802.15.4 networks, for example, 6LoWPAN will take all components of the internet into account. Any sort of host on the internet will connect to them directly, and vice versa. As a result of this approach, unique WSN protocols are no longer permitted to be used by the sensor nodes [101].

D. TOPOLOGY-BASED CLASSIFICATION

The degree of integration in a topology-based classification refers to the determination of the nodes location which provides internet access. There are few dual sensor nodes such as base station, located on the WSN root and form Hybrid solution and the nodes acquired in one hop by internet access point sensing form Access Point solution.

1) HYBRID SOLUTION

The Hybrid solution approach claims that within the WSN, there is a group of nodes which can have direct internet access. In addition, these would be the nodes that could be easily connected to base stations similar to those who need to be traversed to connect the central system and vice versa. Resilience and network intelligence are the essential features of such an approach.

2) ACCESS POINT SOLUTION

The method of increasing node capabilities that are part of the backbone network is one of the main features of the solution. Backbone nodes have more energy than standard nodes and

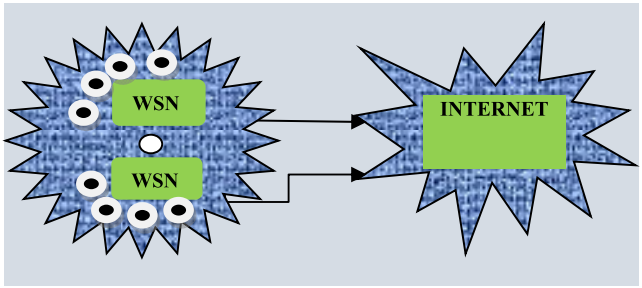

FIGURE 7. Access point network.

it is possible to add more accelerated network requirements as present in 802.11 and 802.15.4.

As per stack-based classification, the topology-based networks have been typically paired with methods previously. For example, internet driven nodes in a backbone type network will serve as a i) front end, in which the internet has completely isolated WSN sensors or (ii) as a gateway for direct data sharing among sensors and the center of the device. There is one exception though: integrating the TCP/IP is practically meaningless with hybrid and backbone solution, every node will be able to link to the internet.

After explaining various approaches for integration, the TCP/IP approach will appear to be the appropriate option for WSN and the IoTs effective integration. The information received directly from the nodes can be easily accessed by external devices, and the nodes can access all of its facilities using internet. Whereas, the nodes can control only those programs that has been introduced in the central setup of other solutions, such as the Front-End solution. There are some other considerations also that need to be considered before choosing an integration approach. This section shows the current issues with the integration. Moreover, as mentioned it is even much more difficult to ensure the protection of the WSN using the TCP/IP solution [45]. The key considerations in the following subsections have been summarized:

- *Resilience:* WSN used in outside organizations is quite susceptible to attacks. Because of the efficiency of the communication channel and the abilities of the sensor network, it might be very easy to execute a DoS attack. Protection mechanisms that improve their robustness against such attacks must be included in gateways and sensor nodes.
- *User Authentication and Authorization:* Security mechanisms that monitor their services are important for certain internet-enabled sensor node applications. For few applications, storing permissions inside the nodes may not be scalable. Therefore, it is important to consider the implementation of single sign-on systems, such as Kerberos [102].
- *Security of the Communication Channel:* IPsec may be too 'strong' for restricted WSN [103]. It is therefore important to examine how other frameworks may be used to provide a stable end-to-end channel. In fact, it is also important to investigate the multiple major exchange mechanisms which should be used in this context.
- *Functionality:* WSN does not need to contact any internet provider whose duties are limited for gathering data and responding to user queries.
- *Network Redundancy:* For redundancy purposes, a set of sensor nodes will provide the same functionality, but an external host in a TCP/IP environment can request services from unique nodes through their IP addresses. This implies that special mechanisms need to be established in TCP/IP environments to cope with unusual circumstances.
- *Protocol Optimizations:* Most protocols relevant to WSN are used to provide certain mechanisms that make it possible for a network to repair itself and optimize its actions. In 6LoWPAN networks, these optimizations are yet to be discovered.

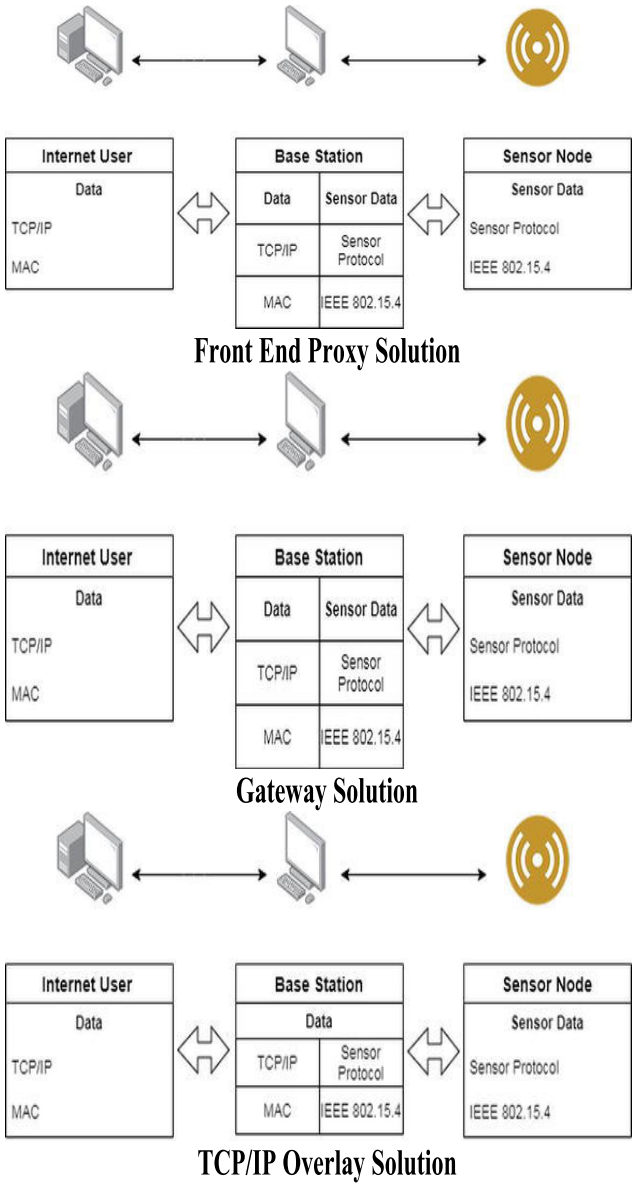

FIGURE 8. Interoperability approaches.

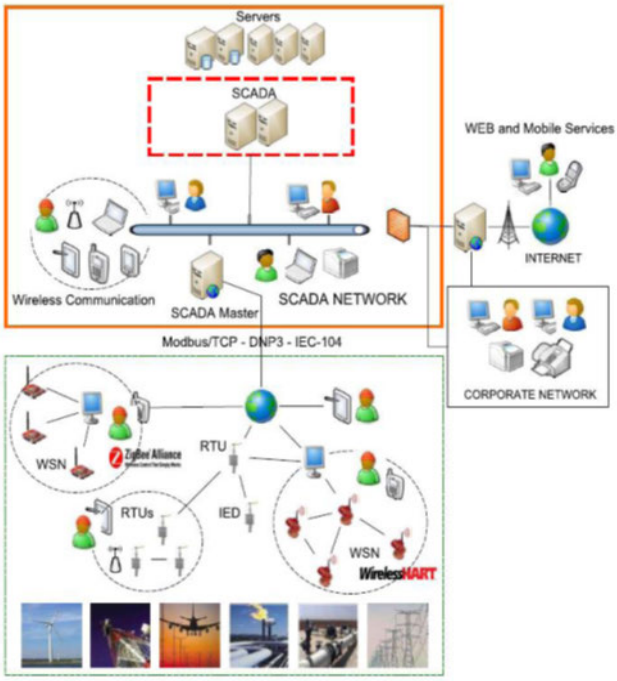

FIGURE 9. Network architecture of SCADA [45].

VIII. CASE STUDIES AND APPLICATIONS OF WSN AND IoT

It has been found that some disadvantages are present in the pure TCP/IP methodology, primarily in terms of security. However, the particular application criteria will eventually determine which form of integration solution is ideally suited. Two sensor network applications have been reviewed to test this statement: SCADA systems with WSN and First responder system.

SCADA (Supervisory Control and Data Acquisition) framework uses emerging technology to track many of the essential infrastructures that are implemented in the real world in real time (see Fig. 9). The central control systems, where human operators remotely control the different components of the essential infrastructure and the remote substations located within the communication networks themselves are indeed the primary components of the SCADA framework and would provide data streams created by the components of these systems. Mobile substations usually rely on Remote Terminal Units (RTUs) that use complex industrial protocols to gather physiological parameters from the network and relay sensor readings to the SCADA network.

In industrial environment, migration to IP monitoring and automation has become fairly important because real-time surveillance, peer-to-peer communication, multiple sessions, competition and security services are included in TCP/IP connections. However, the introduction of hybrid networks for remote control and wireless devices (e.g. Bluetooth, GSM, microwave or WSN) for local Web surveillance has been made possible by such a move. In particular, the internet can serve as a communication connection between control systems and substations while covering a wide range of important business and operational requirements. Wireless technology can provide low deployment and maintenance costs for mobility and interoperability [104].

For the sensing components of a remote substation, smart sensor nodes are capable of evaluating and transferring any data obtained from their sensors such as an RTU that serves as a data collection tool to the central network with significant hardware and software resources. Self-configuration capabilities, alarm generation and reporting of any life-threatening situation can be provided [105].

Currently, many sensor nodes are available in the market for critical and industrial applications. In order to detect faults and shorten the processing time, electrical power systems have realized the need for real-time large area monitoring, protection, control and implement solutions. In order to achieve real-time visualization and to provide real-time congestion management, wireless smart meters are commonly used.

It should be noted that the industrial sensor nodes currently have very similar capabilities to sensor nodes. Many of these standards for wireless networking are based on the IEEE 802.15.4-2006 specification, which sets out physical (PHY) wireless personal area networks (WPANs) and network access control layers (MAC) [106]. The key motive of these standards is to ensure safe communication by using a wireless mesh network to ensure energy savings, interoperability with other networks, and data reliability.

First Responders Systems are usually applied to the first individuals, such as fire fighters and emergency medical technicians, who arrive at a disaster scene. A variety of emergency response functions are performed by sensor networks in these cases, such as patient triage, physical environment control and position tracking [107]. In situations where other communication and support systems are not available, WSN's dynamic and autonomous architecture helps in building and maintaining a knowledge network. Integrating first responder systems based on WSN with the internet will offer many benefits. The network built at the disaster location allows individuals to visualize distant incidents and situations. In order to obtain a global view of the crisis situation, this information can also be accessed by centralizing decision-support structures [108]. In addition to this, in order to achieve optimal mission distribution, the network elements located at the scene of the disaster would communicate with the central networks. In less critical circumstances, first responders can act quickly to save lives. Table 2 summarizes the findings of this study, along with a general description of the benefits and drawbacks of each of the integration approach.

There are other aspects of the TCP/IP approach that need to be considered in addition to these security concerns. In particular, the basic optimizations of WSN protocols like ISA100.11a would not benefit from a TCP/IP-based WSN. There are many other security concerns that need to be resolved in the TCP/IP solution.

SCADA systems can use the Front-End solution and the Gateway solution for access. In addition, if a system is not operating, the gateway may apply different methods, such as wait until the device is running and access another device that monitors the same area. It can also be solved by using Hybrid and Access Point solutions, but these solutions have their own specific issues that need to be resolved.

The TCP/IP solution is actually very suitable for First Responder applications. Network elements can proactively interact with selected internet hosts being aware of the internet presence. Moreover, because these WSNs are short-lived, a few security protocols selected for a specific emergency situation (e.g. TLS/SSL) can be used, thus minimizing overhead on the sensor nodes. The fastest suitable support is delivered by the IP protocol, but different protocols get added at the transport or application level to improve the efficiency of the service. Besides this, network nodes are still vulnerable to external attacks, but due to the transient nature of the system, the risk is lower.

The Front-End solution and the Gateway solution can be used frequently, but in case of emergency, the advantages associated with these solutions are not sufficient always. For instance, most nodes play a unique position, like tracking the location. The only solution that can be used in the absence of a node is to store and forward. Additionally, there are other aspects that require careful consideration. Since the nodes cannot directly access the internet, they rely on the gateway presence. Given the complex nature of the application, multiple gateways are not feasible to boost the consistency of the network.

WSN and IoT-based technologies have profoundly changed people's lives, since they can easily promote and help people's daily activities. As a result, numerous WSN and IoT related applications have emerged. In the next section, we have presented some possible applications relevant to the IoT environment integrated with WSN.

A. HOME AUTOMATION SYSTEM

Almost all appliances are compliant with IoT-based technology. IoT has introduced smart home appliances. Users can monitor the home stuff from anywhere in the world using the IoT based automation system. In those nations that have more elderly people, such a project seems to be very beneficial. The children of these elderly people can support their parents through remote control of smart home appliances using smartphones [109].

B. MONITORING DEVICES FOR AIR POLLUTION

Certain harmful pollutants coming from various sources cause air pollution. This further degrades the air quality, especially in metro cities. Air pollution is responsible for many of the deadliest illnesses. It is possible to introduce a system to measure air pollution in an area. So, to solve the problem, the WSN and IoT domain researchers have come up with some ideas. Newly developed IoT devices can track the air quality and send data to servers (i.e. cloud servers).

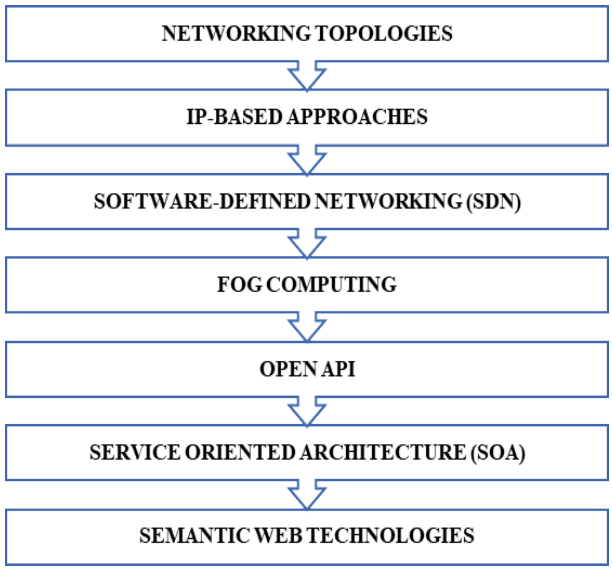

FIGURE 10. Networking architecture.

This information could be used to predict other issues associated with air quality and appropriate remedial action can be planned. For detecting air pollution in a city, these projects have been extremely helpful [110].

C. SMART HEALTH MONITORING SYSTEM

People's life these days are getting too stressful and they are not taking good care of their health and wellbeing. We do not usually go for usual routine check-ups. IoT projects can solve this problem through smart health surveillance systems. Security sensors are effective in monitoring the blood pressure levels, sugar level, and pulse in the body of the patient as well as healthy people and automatically warn the doctor if it is above the threshold value. In these cases, smart sensor-based devices regularly monitor person's health and send data to a cloud server that can be accessed by a concerned person via their smartphones. The physician can verify their patient's current health condition at anytime and from anywhere in the world by using such a communication environment [111], [112].

D. SMART TRAFFIC MANAGEMENT SYSTEM

There are traffic issues in nearly every metro city due to the growing number of vehicles in the towns. This problem can be solved by WSN and IoT related project. This system is made up of smart vehicles (integrated with a traffic sensor) that can communicate with each other. This data obtained from the vehicle can be submitted to a cloud server that can be used to further process and forecast and help in arriving at smart traffic management decisions.

Thus, in so many commercial sites, within that event of heavy traffic, a central authority can raise an alarm. For drivers that are in emergency circumstances, it would be extremely helpful. They can update their routes based on the information received and that too without wasting their

TABLE 2. Solutions and applications for integration.

	OVERVIEW	SCADA	FIRST RESPONDERS
TCP/IP	• Distributed processes • Overhead of device • Weak to foreign attackers • Resilient to failure of systems • Easy access to the computers	• Low lifetime: several protocols must be enabled. • Devices should not be Internet-conscious. • Critical climate • Protocols unique to SCADA • Provide additional attributes	• Limited lifetime: protocols unique to deployment • Devices will benefit from Internet awareness.
FRONT-END	• Centralized management • Single failure point • Store and Forward, Redundancy	• Increasing access points to enhance stability • Isolation of sensor equipment	• No redundancy requirement • There may not be extra access points available • Isolation of nodes may be detrimental.
GATEWAY	• Mixed Design • Single failure point • Application-Layer Control Access	• Enhance access points to enhance robustness. • Any intelligence must be passed to the computers.	• There may not be extra access points available

precious time. It can also track violators who violate the traffic rules while driving so that legal action can be initiated against them [111]–[113]. This would definitely improve the traffic management systems.

E. DETECTION AND PREVENTION OF EARLY FLOODS

Floods are an increasingly common seasonal concern in various countries. So to minimize the losses caused due to this natural disaster, we need an early warning system for floods. Such a scheme utilizes the humidity, temperature, and water and flow level to predict floods. The floating sensor is used to monitor water depth and water flow. It is composed of a water pump, a hall-effect sensor and a valve body made of plastic. So many controlling variables can be obtained via smart phone to determine the form of flood situation [115].

F. SMART ANTI-THEFT SYSTEM

Everyone needs to defend their home or business from physical theft of any sorts. Applications based on WSN and IoT can solve this problem. When a user leaves his/her home, they can switch on the anti-theft device that will track the floors and alert the warning system for any footsteps on the floor tiles. Then the microcontroller would convert it into a valid signal, allowing the camera to take an image and deliver this information to the house owner about the robbery. On his/her smartphone, the user can then view the images [116].

G. COAL MINE SAFETY SYSTEM

Despite all the safety measures, there is still a life-threatening danger in coal mines. To link the associated microcontroller with the gas sensor and temperature sensor for implementation, we need an Arduino device. A deployed device is configured to send a dangerous gas level warning message to the respective authorities if the gas sensor detects a gas rate above the target level. This can save the people employed in the coal mines in case of a mishap [116].

H. SMART FARMING

The population of the planet is rising day in and day out. Therefore, the farming industry must use modern technical

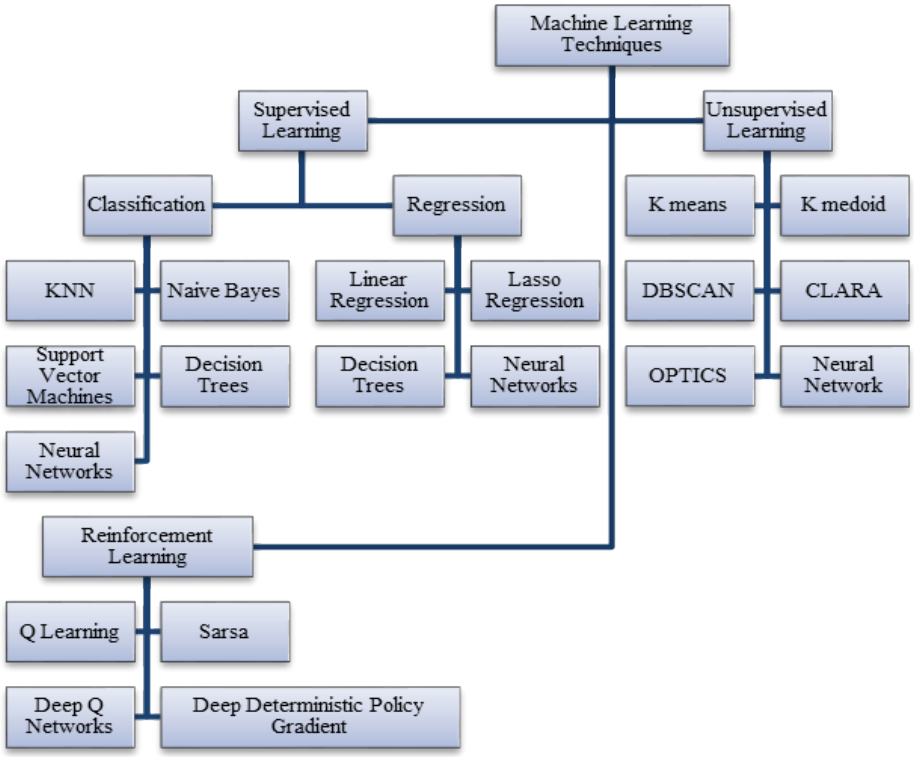

FIGURE 11. Machine Learning Techniques.

systems such as IoT to feed the increasing population. For example, agriculture suffers from other threats such as severe weather, rapid climate change and other environmental factors. IoT-related systems that help farmers minimize waste and maximize crops production is the objective of smart agriculture. Smart farming is a technology which is having low-cost, and uses high-tech devices for producing food for the masses cleanly and sustainably. In a smart farming based on WSN and IoT, a system is constructed to track the crop field using sensors and to automate the irrigation method. With such a device a farmer can track the conditions in the field from anywhere using a smartphone, which makes this approach efficient in contrast with the traditional approach. Smart agriculture can have various advantages such as effective water usage [117], [118].

IX. NETWORKING TECHNOLOGIES TO PROVIDE WSN INTEROPERABILITY WITH IoT

To provide WSN interoperability in IoT, various networking protocols and technologies were used as shown in Fig. 10. The following section is about primary technologies for network-level interoperability.

A. IP-BASED APPROACHES

The IP-based solutions incorporate the full TCP/IP stack on smart devices. In order to allow end-to-end communication between the sensor networks and the IP, the sensors and actuators are linked to the IP network. On sensor nodes such as Tiny TCP and lwIP, some researchers have attempted to implement a TCP/IP stack. The main benefit of introducing a TCP/IP stack on sensor nodes is that gateways and protocol translations are not needed. Nevertheless, the authors argue that because of its resource-constrained nature, sensor nodes cannot have an all-IP sensor network [119]–[121].

To address the resource-restricted problem of system connectivity, the IETF has developed network-based working groups (WGs) such as Routing over Low Power and Lossy Networks (ROLL), IPv6 over Low Power WPAN (6LoWPAN), UDP-based Constrained Application Protocol (CoAP) and Constrained Restful Setting. This method also uses gateways to switch between normal Internet protocols and proprietary protocols that are used in the sensor network, e.g. 6LoWPAN IPv6. Therefore, by using standard protocols, drawbacks of gateway-based methodologies can be reduced because the gateway and sensor nodes are not from the same manufacturer and this result in improving the interoperability of the device. IP as the internet de- facto standard provides a common open source platform for trillions of objects [122], [123].

B. SOFTWARE-DEFINED NETWORKING (SDN)

It is designed to make existing wireless and mobile networks smarter, more efficient, more stable and more flexible in order to manage the enormous amount of IoT information [124]. Separating control and data planes in network systems is one of SDN's major novelties for breaking IoT vertical

silos. To promote networking applications like heterogeneity, mobility management, QoS management and security [128], SDN has been extended to IoT [125]–[128].

Authors used SDN to enable different devices from multiple networks to connect with each other using IPv6, while improving the efficiency by adding an additional IoT controller over the SDN controller to control different object types [129]. It helps in connecting various devices to the Network. Another work has been discussed which demonstrate the need to address the heterogeneity of the most complex IoT systems and applications [130]. According to researchers, utilizing IPv6 to deal with the large number of connected devices would be an appropriate choice, but heterogeneity is still an active research topic. They use a very high-level IoT controller architecture to address this, which appears to be an appropriate mechanism for handling heterogeneous IoT flows to a specific level. Some researchers have suggested a new mobility service tailored to the SDN specification in order to solve the PMIPv6 protocol performance problems. The researchers have stated that they have not used the standard IPv4 protocol. In place of PMIPv6, their strategy would be to use mobility management. The results of the analysis show that the flow scheduling algorithm based on the genetic algorithm has improved efficiency in comparison with the approaches for the bin packaging and load balance. Network function virtualization, Network feature virtualization (NFV) is a complementary solution to SDN. NFV differs from the functions operating on the physical network hardware which includes network address translator and firewall. Some service providers would therefore create a number of independent virtual networks that would then be able to share the actual network equipment associated with network infrastructure providers. NFV has the capability to minimize operating expenditure (OPEX) and capital expenditure (CAPEX) costs.

They defined and combined the abstract IoT architecture developed by them with the SDN architecture to develop a particular SDN-IoT structure with an upper server layer that provides adequate IoT APIs for developers, a middle layer with a distributed network operating system, a few other physically distributed SDN controllers, a layer with SDN-enabled network switches, and an IoT gateway that connects them to the network's middle layer. With IoT applications in mind, this is essentially just the conventional SDN architecture. The researchers have stated that they are using virtualization technology to develop an IoT-optimized network based middle-layer OS. The network operating system needs to be implemented to take into account the variety of available IoTs and use cases. Details of the use of virtualization in the middle layer are missing, but the relationship of NFV techniques to the IoT network SDN logic is noteworthy.

C. FOG COMPUTING

As a technology [131], the cloud has been used to tackle interoperability, where computing, networking and storage resources are placed at the edge of the network rather than centralized cloud servers, i.e. as near as possible to end-user devices. This reduces network latency arising from the conversion of raw data generated by mobile devices and sensors that are limited by resources. The fog computing model adds importance to the data before making it available to the cloud and planning controlled data for interoperability in various applications, in order to facilitate interoperability in IoT, 5G, AI and network-intensive applications [132], [133].

D. OPEN API

The API exposes data or functionality to an application written in the highest standard language to a service provider. The range of common APIs is Google Maps, YouTube, and Amazon. In order to help developers access their services, almost every IoT system today has a public API. The APIs are usually based on Restful principles, and allow common operations such as PUT, GET, PUSH, or DELETE. However, in order to determine the syntax of the specific operations, they will use APIs that are platform-specific and proprietary relying on internal information models to define the syntax of specific operations to be used by their consumers.

For example, a smartphone application can provide control of your refrigerator connected to the Internet. It has features such as showing products in the fridge, notifying you of the ingredients' expiry date, or initiating/stopping operations. If more than one refrigerator vendor without a standard API is to be implemented in a mobile application, the application developers must write custom code to use another platform-specific API, which is a huge burden. However, a standard API allows the interoperability across platforms and existing implementations with minimal framework changes. ThingSpeak13 enable the development of widgets that can be provided to other platform users to explain the effect of the heterogeneity of the IoT API. HyperCat14 is a specification providing syntactic interoperability between different catalog-based APIs and services that can be tagged with metadata. The Interworking API acts as an interface that other systems can implement.

E. SERVICE ORIENTED ARCHITECTURE (SOA)

Service Oriented Architecture (SOA) has been proposed by researchers as a considerable technology in various aspects that can provide syntactic interoperability across heterogeneous devices [5]. In the network layer, the SOA was designed so that content and pattern recognition can be easily handled through various service components [134]. Exposing the functionality of each device as a standard service will greatly improve both network and application interoperability. In particular, the Web Service technology was proposed to provide complete data sharing, reuse, and interoperability on the SOA pledge [135]. The classic web service-oriented approach and the resource-oriented approach (REST web services) were used to address syntactic interoperability. In particular, the SOA pledge of full information exchange, redistribution, and integration with Web Service technology was proposed to be accomplished. For composing IoT services, event-oriented architecture (EDA) is combined with

the SOA [136], [137]. SOA divides the application into a number of independent services defined in the standard interface specification, while EDA uses event flows to handle independent services. The researchers have concentrated on creating a scalable EDSOA that can use resource data to assemble IoT services, run those services using separate and shared events and then use event sessions to organize them.

F. SEMANTIC WEB TECHNOLOGIES

Initially, W3C-developed Semantic Web technologies were used to describe Web resources. For the Semantic Web to converge with the WoT, the Semantic Web of Things (SWoT) paradigm is proposed for the realization of a mutual understanding of the different entities that form the IoT [138].

Current findings have suggested that semantic network technology is a powerful determinant of heterogeneous environment interoperability [139]. Using some standard data format and context agreements in a schematic form, by common vocabulary and by an ontology-led framework, the research utilizes semantic web technologies to achieve semantic interoperability. Ontologies are a collection of elements and connections used in IoT to describe a field of concerns. They operate as an intermediary among IoT applications and users and enhance their semantic matchmaking [140]. A research work of existing ontologies available that can be used in specific fields can be found in [141]. The authors reported that the SSN ontology had earned most of the attention. Although there is a global ontological norm for no specific domain. In order to boost semantic interoperability, many IoT research projects, such as the Semantic Sensor Network (SSW), OpenIoT, HYDRA17, SPITFIRE and SENSEI18, use the capabilities of the aforementioned ontologies or other semantic technologies [142], [143]. The SSW, widely known as Sensor Network and Semantic Web technology, is one of the original semantic representation studies of IoT/WoT. SensorML19, which is a semantic specification for web-enabled sensors (SWE) using XML-based protocols and APIs, has been developed by the Open Geospatial Consortium (OGC) without providing any semantic interoperability. Semantic interoperability around two layers is provided by Ubi ROAD: (1) data level and (2) functional protocol level. Serrano mentioned IoT semantic interoperability problems and also the SEG 3.0 solution for heterogeneous systems to provide semantic interoperability [144], [145]. The technology involves semantic web technology to implement heterogeneous IoT data, and also have attached context of the technology to help creators and IoT specialists to create IoT applications. The structure consists of twelve layers based on system heterogeneity, modes of communication, information and services. These standard service technologies were discussed by the authors of [146]. In this work, a series of semantic models were given IoT tools, entities, and services. Some semantic models for representation give interoperability at the data and service levels.

X. MACHINE LEARNING APPROACHES TO COMBAT SECURITY CHALLENGES IN IOT AND WSNS

Wireless Sensor Networks (WSNs) are the IoT's principal building blocks. Although, they are vulnerable to a couple of security threats. The protection of IoT and WSNs has become essential because of the limited resources. Machine learning inspires other security solutions for IoT and WSN.

Throughout this section, we survey various techniques of machine learning built to combat security challenges. Machine learning can be used to counter WSN and IoT security threats. As developing mathematical models is challenging for IoT and WSN systems, machine learning can be used which utilizes multiple intelligence techniques for preparing devices without explicit programming. Machine learning in WSNs and IoT, faces two major obstacles: node resources, processing limitation and the need for large sets of learning data.

A. OVERVIEW OF MACHINE LEARNING TECHNIQUES

Various types of approaches to machine learning are addressed shown in Fig. 11. Some of them have been explained below: [147].

1) SUPERVISED MACHINE LEARNING

In supervised machine learning, the machine model is based on a designated training set containing outputs and predefined inputs. The system model helps to determine the relationship between output and input and other parameters of the system. By using these learning methods for WSNs, localization and object targeting, query processing and event detection, medium access control, intrusion detection and protection, data integrity, service quality QoS and error detection can be accomplished.

The key supervised learning algorithms are:

1) *k-Nearest Neighbor:* Calculating the average of the closest k neighbors estimated from the Euclidean distance is the representation of an undefined node. For example, if a WSN node's reading is missing, it can be calculated from the neighboring nodes average readings for a given area. For wide training samples and higher dimensions, this could often give inaccurate outcomes.

2) *Support Vector Machine (SVM):* SVM is used to distinguish a hyper plane into two separate groups. For this, SVM aims to optimize the margin and distinguish with minimal errors between the two groups. In the absence of linear hyper plane, a kernel function is used by the SVM because of its high precision, and is also commonly used to fix security concerns in IoT and WSNs.

3) *Artificial Neural Network (ANN):* ANN uses neurons or processing and works quite similar to the human brain. It is composed of different layers. ANN can solve complex and nonlinear problems. It has complex calculations.

2) UNSUPERVISED (UN) MACHINE LEARNING

In unsupervised learning, the system model is not really based on input or output parameters. The layout of various classes of the sample set can be achieved by analyzing the similarities between a sample set and an unsupervised learning algorithm. Unmonitored learning algorithms can be used for WSN applications involving WSN node clustering or data collection in a sink code scenario. Since the system model is independent of labeled parameters, complex variable relationships are often found to be sufficient for attacks. Two main categories of learning algorithms are:

1) *Principal Component Analysis (PCA):* PCA collects and describes essential information from data formats as new orthogonal values for the identification of new coordinates. This method minimizes the level of data needed and translates large sets of data into smaller ones.

2) *k-Means Clustering:* A data set is grouped into k clusters in this algorithm and then cluster heads are selected randomly. The cluster head has been finding out with the help of each node present in the cluster.

3) REINFORCEMENT MACHINE LEARNING

In the reinforcement learning algorithm, the computer model learns by communicating with the environment. This sort of ML includes a reward mechanism for those sensor nodes that learn to work better by learning from their observations. One of the popular types of reinforcement learning is Q-learning, and it often tackles routing issues.

B. MACHINE LEARNING APPROACHES USED TO IDENTIFY VARIOUS ATTACKS IN IoT AND WSN

1) COUNTER DoS ATTACKS

In the WSN MAC layer, SVM and NN machine learning is used to estimate DoS attacks [148]. SVM and NN depend on two parameters to train their devices and to calculate DoS attack probability: the rate of collision and the rate of arrival. In NN, the node is the focus. Therefore, it goes into sleep mode and starts operating when the attack ends. For calculating the probability of a DoS attack by using SVM, two classes are designated as either Low or Strong. SVM accuracy has been said to be higher along with a smaller time to detect the attack. With four neuron layers, the authors used multi-layered deep learning [149]. They presumed there was two-layer network architecture: an IoT layer that included the sensor/actuator architecture and a fog layer that included computing and storage of the shared network. This architecture aims to elevate the burden of training and assault detection to the fog nodes to compensate for the limitations of the IoT edge node resource. Finally, a comparison is presented describing the different classification algorithms to classify the usual data in the Do's cases in [150].

2) COUNTER SELECTIVE FORWARDING ATTACKS

A one-class SVM was introduced by the authors to define selective forwarding and black hole attacks in [151]. To save memory and energy a simple intrusion detection device has been provided. SVM relies on two parameters for categorization: bandwidth and hop count. To accomplish security, this algorithm has assumed that more resources will not be consumed by nodes. Neither of the works mentioned in [152] detect selective forwarding attacks by applying machine learning.

TABLE 3. Machine learning to protect IoT and WSNs.

Paper	Attack	Learning Approach	Complexity	WSN/ IoT
Improvement in terms of Security [148]	DoS	SVM NN	Low Moderate	WSN
Determination of distributed attack [149]	DoS	NN	High	IoT
Selective forwarding attacks [151]	Selective Forwarding	SVM	Moderate	WSN
Machine Learning security for IoT [153]	Man in the Middle	ANN	High	IoT
Dynamic Watermarking [154]	Man in the Middle	RNN LSTM	High	IoT
IoT Sentinel [156]	Traffic Monitoring	Not Specified	Moderate	IoT
Unauthorized IoT Devices [157]	Traffic Monitoring	Supervised Learning	Moderate	IoT
ProfilIoT [158]	Traffic Monitoring	Supervised Learning	Moderate	IoT
Bio-Inspiration [159]	Malicious node	K-means & SVM	Moderate	WSN
Dynamic Access Facility and Policy of Control [160]	Different attacks	Blockchain	High	IoT

3) COUNTER MAN IN THE MIDDLE ATTACKS

Artificial NN has been used in [153]. The proposed NN tracks the node's health by using packages already available in the R programming language. If the value is different from the expected value, then it represents a man in the middle attack. The contact between an IoT system and the cloud can be protected by a watermark technique. It technically adds pseudo random noise to the IoT unit and calculates a bit of a stream [154]. The attack alert starts if the bit-stream retrieved by the receiver does not match. It can be cracked easily if the bit-stream stays unchanged. For the generation of dynamic bit-stream features such as spectral flatness, mean, variance, skew and kurtosis, a recurrent NN machine learning approach called Long Short Term Memory (LSTM) has been

suggested. To secure mobile edge caching and processing services for network users such as IoT, reinforcement learning was used [155].

4) IoT SYSTEM RECOGNITION BY MACHINE LEARNING

IoT SENTINEL characterizes recently installed machines at home or few developing organizations into devices which can be trusted, restricted devices [156]. The gateway tracks the traffic caused by these new devices and also collects fingerprints of the device being sent by the IoT service provider to identify the device according to its category and the traffic produced by the machine learning classification model. Machine learning technique, supervised by Random Forest was used for mapping traffic stream with a form of a framework designed to disregard emerging technologies in large enterprises [157]. If the mapping could not be matched to one of the forms, that system is not permitted. Based on data traffic, machine learning differentiates between IoT and non-IoT computers [158].

5) PROTECTION WITH MACHINE LEARNING USING BIO-INSPIRATION

The authors used machine learning with Bio-inspiration to remove the impact of malicious nodes [159]. Two clusters were created by the k-means algorithm: a regular cluster and a faulty cluster, and SVM were used to create a decision block comprising three regions: a normal zone, a fault region, and a border area. Statistics like the mean and standard deviation of the normal nodes given by the SVM data set are determined by an anomaly detection algorithm. After sensing, anomaly and immune system activation, digital antibodies are formed instead of biological systems, and after that malicious nodes are deactivated.

6) FOR PROTECTED IoT ACCESS CONTROL

To remove the single point of failure and improve privacy, the issue of IoT device access control has been altered from centralized to distributed [161]. A block chain scheme is used to allow communication between unknown participants without a trustworthy middleman.

The different machine learning methods used for IoT and WSN security have been summarized in Table 3. While many techniques lead to high accuracy, there are several challenges in securing IoT and WSNs because there should be a balance to suit the resource-limited IoT and WSN devices between strong security features and low computational complexity.

XI. CONCLUSION

At first we discussed about security requirements in WSN for IoT architecture from the perspective of different layers along with major and minor security requirements and challenges. Then we analyzed possible attacks and threats towards the WSNs and IoT for different layers. Steps to incorporate WSNs into the IoT have also been addressed. We have evaluated three approaches for integration and explained that they are not satisfactory for IoT to incorporate sensor nodes. We have highlighted a variety of tasks to illustrate the issues arising from the security, integration and network technology model used. And it was found that the solutions currently implemented are not sufficient for the limited resources of the sensor node. Networking technologies to provide WSN interoperability with IoT has been studied. This study examines the security problems associated with the integration of WSNs and IoT. It also seeks to assess whether the existing mechanisms of technology are relevant and applicable in a particular case. At last we have discussed about machine learning approaches to combat security challenges in IoT and WSNs. The study outlines possible strategies that can be used to link a WSN to the internet and to investigate the confidentiality issues raised because of interactions. It has been found that the network of sensors and the internet could communicate securely by delivering network services via a front-end proxy. The paper explores the relationships between sensor networks and IoT from a security perspective and also analyzes threats of both the technologies when integrated together.

REFERENCES

[1] N. Salman, I. Rasool, and A. H. Kemp, "Overview of the IEEE 802.15.4 standards family for low rate wireless personal area networks," in *Proc. 7th Int. Symp. Wireless Commun. Syst.*, Sep. 2010, pp. 701–705, doi: 10.1109/ISWCS.2010.5624516.

[2] 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 Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[3] S. Fang, L. Da Xu, Y. Zhu, J. Ahati, H. Pei, J. Yan, and Z. Liu, "An integrated system for regional environmental monitoring and management based on Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1596–1605, May 2014.

[4] P. Gope and T. Hwang, "BSN-Care: A secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors J.*, vol. 16, no. 5, pp. 1368–1376, Mar. 2016.

[5] S. Li, L. Xu, and S. Zhao, "The Internet of Things: A survey," *Inf. Syst. Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.

[6] A. Ghosal and S. Halder, "Intrusion detection in wireless sensor networks: Issues, challenges and approaches," in *Wireless Networks and Security* (Signals and Communication Technology), S. Khan and A. S. Pathan, Eds. Berlin, Germany: Springer, 2013, pp. 329–367.

[7] A. G. Finogeev and A. A. Finogeev, "Information attacks and security in wireless sensor networks of industrial SCADA systems," *J. Ind. Inf. Integr.*, vol. 5, pp. 6–16, Mar. 2017.

[8] K. Shabana, N. Fida, F. Khan, S. R. Jan, and M. U. Rehman, "Security issues and attacks in wireless sensor networks," *Int. J. Adv. Res. Comput. Sci. Electron. Eng. (IJARCSEE)*, vol. 5, no. 7, p. 81, 2016.

[9] S. Bartariya and A. Rastogi, "Security in wireless sensor networks: Attacks and solutions," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 5, no. 3, pp. 214–220, 2016.

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

[11] G. Mehmood, M. Z. Khan, S. Abbas, M. Faisal, and H. U. Rahman, "An energy-efficient and cooperative fault- tolerant communication approach for wireless body area network," *IEEE Access*, vol. 8, pp. 69134–69147, 2020, doi: 10.1109/ACCESS.2020.2986268.

[12] G. Mehmood, M. Z. Khan, A. Waheed, M. Zareei, and E. M. Mohamed, "A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks," *IEEE Access*, vol. 8, pp. 131397–131413, 2020, doi: 10.1109/ACCESS.2020.3007405.

[13] R. Rodrigo, Z. Jianying, and L. Javier, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, 2013.

[14] Development News. *How Can We Enable Smart and Sustainable Cities?* Accessed: Feb. 2021. [Online]. Available: http.//www.developmentnews.in/can-enable-smart-sustainable-cities/

[15] P. Tiwari, V. P. Saxena, R. G. Mishra, and D. Bhavsar, "Wireless sensor networks: Introduction, advantages, applications and research challenges," *HCTL Open Int. J. Technol. Innov. Res.*, vol. 14, pp. 1–11, Apr. 2015.

[16] R. Singh, J. Singh, and R. Singh, "Security challenges in wireless sensor networks," *IRACST-Int. J. Comput. Sci. Inf. Technol. Secur. (IJCSITS)*, vol. 6, no. 3, pp. 1–5, 2016.

[17] D. Padmavathi and M. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *Int. J. Comput. Sci. Inf. Secur.*, vol. 4, no. 2, pp. 1–9, 2009.

[18] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proc. IEEE Symp. Secur. Privacy*, May 2005, pp. 49–63.

[19] S. Jaydip, "A survey on wireless sensor networks security," *Int. J. Comput. Appl.*, vol. 1, no. 2, pp. 55–78, 2009.

[20] W. Yong, A. Garhan, and R. Byrav, "A survey of security issues in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2–23, 2nd Quart., 2006.

[21] V. B. A. Rajkumar, K. Jadhav, and S. Vidya, "Wireless sensor networks issues and applications," *Int. J. Comput. Technol. Appl.*, vol. 3, pp. 1667–1673, Sep. 2012.

[22] C. Buratti, A. Conti, D. Dardari, and R. Verdone, "An overview on wireless sensor networks technology and evolution," *Sensors*, vol. 9, no. 9, pp. 6869–6896, Aug. 2009.

[23] C. F. García-Hernández, P. H. Ibarguengoytia-Gonzalez, J. García-Hernández, and J. A. Pérez-Díaz, "Wireless sensor networks and applications: A survey," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 7, no. 3, pp. 264–273, 2007.

[24] N. Mehndiratta, M. M. Neha, and B. M. Harish, "Energy efficient homogeneous vs heterogeneous LEACH," *Int. J. Innov. Technol. Exploring Eng.*, vol. 2, pp. 280–283, Apr. 2013.

[25] A. A. Khan, N. Javaid, U. Qasim, Z. Lu, and Z. A. Khan, "HSEP: Heterogeneity-aware hierarchical stable election protocol for WSNs," in *Proc. 7th Int. Conf. Broadband, Wireless Comput., Commun. Appl.*, Nov. 2012, pp. 373–378.

[26] F. Hu and N. K. Sharma, "Security considerations in ad hoc sensor networks," *Ad Hoc Netw.*, vol. 3, no. 1, pp. 69–89, Jan. 2005.

[27] I. Butun, "Prevention and detection of intrusions in wireless sensor networks," Ph.D. dissertation, Dept. Elect. Eng., Univ. South Florida, Tampa, FL, USA, 2013.

[28] Y. Liu, Y. Li, and H. Man, "MAC layer anomaly detection in ad hoc networks," in *Proc. 6th Annu. IEEE Syst., Man Cybern. (SMC) Inf. Assurance Workshop*, Jun. 2005, pp. 402–409.

[29] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 38–47, Feb. 2004.

[30] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proc. IEEE 22nd Annu. Joint Conf. IEEE Comput. Commun. Societies (INFOCOM)*, vol. 3, Mar./Apr. 2003, pp. 1976–1986.

[31] M. Conti, R. Di Pietro, and A. Spognardi, "Clone wars: Distributed detection of clone attacks in mobile WSNs," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 654–669, 2014.

[32] T. Winter *et al.*, "RPL: IPv6 routing protocol for low-power and lossy networks," Internet Eng. Task Force, Stephen Dawson-Haggerty, UC Berkeley, CA, USA, Tech. Rep. draft-ietf-roll-rpl-13, 2012.

[33] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proc. ACM Workshop Wireless Secur. (WiSe)*, 2003, pp. 30–40.

[34] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, "6LoWPAN fragmentation attacks and mitigation mechanisms," in *Proc. 6th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*, 2013, pp. 55–66.

[35] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," in *Proc. Int. Conf. Pervasive Comput. (ICPC)*, Jan. 2015, pp. 1–6.

[36] M. Singh, M. A. Rajan, V. L. Shivraj, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," in *Proc. 5th Int. Conf. Commun. Syst. Netw. Technol.*, Apr. 2015, pp. 746–751.

[37] I. I. Technology, *Message Queuing Telemetry Transport (MQTT) V3.1.1*, International Organization for Standardization, Standard 20922-2016, 2016.

[38] B. Frank, Z. Shelby, K. Hartke, and C. Bormann, *Constrained Application Protocol (CoAP)*, document draft-ietf-core-coap-04, IETF-draft. IETF, 2011.

[39] J. Deng, R. Han, and S. Mishra, "Defending against path-based DoS attacks in wireless sensor networks," in *Proc. 3rd ACM Workshop Secur. Ad Hoc Sensor Netw. (SASN)*, 2005, pp. 89–96.

[40] H. P. Gupta, S. V. Rao, A. K. Yadav, and T. Dutta, "Geographic routing in clustered wireless sensor networks among obstacles," *IEEE Sensors J.*, vol. 15, no. 5, pp. 2984–2992, May 2015.

[41] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, 2000, p. 10.

[42] I. Butun, I.-H. Ra, and R. Sankar, "PCAC: Power-and connectivity-aware clustering for wireless sensor Networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, no. 1, p. 83, 2015.

[43] O. Hahm, E. Baccelli, H. Petersen, and N. Tsiftes, "Operating systems for low-end devices in the Internet of Things: A survey," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 720–734, Oct. 2016.

[44] O. Bello, S. Zeadally, and M. Badra, "Network layer inter-operation of device-to-device communication technologies in Internet of Things (IoT)," *Ad Hoc Netw.*, vol. 57, pp. 52–62, Mar. 2017.

[45] R. Roman and J. Lopez, "Integrating wireless sensor networks and the internet: A security analysis," *Internet Res.*, vol. 19, no. 2, pp. 246–259, Apr. 2009.

[46] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M. B. Srivastava, "On communication security in wireless ad-hoc sensor networks," in *Proc. 11th IEEE Int. Workshops Enabling Technol., Infrastruct. Collaborative Enterprises*, Jun. 2002, pp. 139–144.

[47] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 2, pp. 228–258, 2005.

[48] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," *Wireless Netw.*, vol. 8, no. 5, pp. 521–534, Sep. 2002.

[49] J. Deng, R. Han, and S. Mishra, "A performance evaluation of intrusion-tolerant routing in wireless sensor networks," in *Information Processing in Sensor Networks*. Berlin, Germany: Springer-Verlag, 2003, p. 552.

[50] M. Tubaishat, J. Yin, B. Panja, and S. Madria, "A secure hierarchical model for sensor network," *ACM SIGMOD Rec.*, vol. 33, no. 1, pp. 7–13, Mar. 2004.

[51] A. Agah and S. K. Das, "Preventing DoS attacks in wireless sensor networks: A repeated game theory approach," *Int. J. Netw. Secur.*, vol. 5, no. 2, pp. 145–153, Sep. 2007.

[52] A. D. Wood, J. A. Stankovic, and S. H. Son, "JAM: A jammed-area mapping service for sensor networks," in *Proc. 24th IEEE Real-Time Syst. Symp. (RTSS)*, Dec. 2003, pp. 286–297.

[53] R. Muraleedharan and L. Osadciw, "Cross layer denial of service attacks in wireless sensor network using swarm intelligence," in *Proc. 40th Annu. Conf. Inf. Sci. Syst.*, Mar. 2006, pp. 1653–1658.

[54] W. Znaidi, M. Minier, and J.-P. Babau, "An ontology for attacks in wireless sensor networks," Ph.D. dissertation, INRIA, Le Chesnay-Rocquencourt, France, 2008.

[55] N. Accettura and G. Piro, "Optimal and secure protocols in the IETF 6TiSCH communication stack," in *Proc. IEEE 23rd Int. Symp. Ind. Electron. (ISIE)*, Jun. 2014, pp. 1469–1474.

[56] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[57] Z. Karakehayov, "Using REWARD to detect team black-hole attacks in wireless sensor networks," in *Proc. Workshop Real-World Wireless Sensor Netw.*, 2005, pp. 20–21.

[58] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: Secure and trustable routing in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2013–2027, Sep. 2016.

[59] M. Wazid, A. Katal, R. Singh Sachan, R. H. Goudar, and D. P. Singh, "Detection and prevention mechanism for blackhole attack in wireless sensor network," in *Proc. Int. Conf. Commun. Signal Process.*, Apr. 2013, pp. 576–581.

[60] S. Misra, K. Bhattarai, and G. Xue, "BAMBi: Blackhole attacks mitigation with multiple base stations in wireless sensor networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2011, pp. 1–5.

[61] A. Prathapani, L. Santhanam, and D. P. Agrawal, "Intelligent honeypot agent for blackhole attack detection in wireless mesh networks," in *Proc. IEEE 6th Int. Conf. Mobile Adhoc Sensor Syst.*, Oct. 2009, pp. 753–758.

[62] M. Tiwari, K. V. Arya, R. Choudhari, and K. S. Choudhary, "Designing intrusion detection to detect black hole and selective forwarding attack in WSN based on local information," in *Proc. 4th Int. Conf. Comput. Sci. Converg. Inf. Technol.*, 2009, pp. 824–828.
[63] A. Amouri, L. G. Jaimes, R. Manthena, S. D. Morgera, and I. J. Vergara-Laurens, "A simple scheme for pseudo clustering algorithm for cross layer intrusion detection in MANET," in *Proc. 7th IEEE Latin-American Conf. Commun. (LATINCOM)*, Nov. 2015, pp. 1–6.
[64] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 5, no. 4, pp. 11–25, 2001.
[65] S. S. Nagamuthu Krishnan and P. Srinivasan, "A QOS parameter based solution for black hole denial of service attack in wireless sensor networks," *Indian J. Sci. Technol.*, vol. 9, no. 38, Oct. 2016.
[66] M. Medadian, M. H. Yektaie, and A. M. Rahmani, "Combat with black hole attack in AODV routing protocol in MANET," in *Proc. 1st Asian Himalayas Int. Conf. Internet*, Nov. 2009, pp. 1–5.
[67] M. A. Hamid, M. Rashid, and C. S. Hong, "Routing security in sensor network: Hello flood attack and defense," in *Proc. IEEE ICNEWS*, Jan. 2006, pp. 2–4.
[68] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in *Proc. 3rd Int. Conf. Secur. Privacy Commun. Netw. Workshops (SecureComm)*, 2007, pp. 341–350.
[69] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," *IEEE Trans. Syst., Man, Cybern., C (Appl. Rev.)*, vol. 37, no. 6, pp. 1246–1258, Nov. 2007.
[70] K. Xing, F. Liu, X. Cheng, and D. H. C. Du, "Real-time detection of clone attacks in wireless sensor networks," in *Proc. 28th Int. Conf. Distrib. Comput. Syst.*, Jun. 2008, pp. 3–10.
[71] J.-W. Ho, M. Wright, and S. K. Das, "Fast detection of replica node attacks in mobile sensor networks using sequential analysis," in *Proc. IEEE 28th Conf. Comput. Commun. (INFOCOM)*, Apr. 2009, pp. 1773–1781.
[72] I. Butun, I.-H. Ra, and R. Sankar, "An intrusion detection system based on multi-level clustering for hierarchical wireless sensor networks," *Sensors*, vol. 15, no. 11, p. 28960–28978, 2015.
[73] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 247–260, Feb. 2006.
[74] M.-J. Duan and J. Xu, "An efficient location-based compromise-tolerant key management scheme for sensor networks," *Inf. Process. Lett.*, vol. 111, no. 11, pp. 503–507, 2011.
[75] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis & defenses," in *Proc. 3rd Int. Symp. Inf. Process. Sensor Netw.*, Apr. 2004, pp. 259–268.
[76] P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information," *Expert Syst. Appl.*, vol. 42, no. 21, pp. 7560–7572, 2015.
[77] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *Proc. NDSS*, 2004, pp. 241–245.
[78] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in *Proc. ACM Workshop Wireless Secur. (WiSe)*, 2004, pp. 51–60.
[79] A. Dvir and L. Buttyan, "VeRA-version number and rank authentication in RPL," in *Proc. IEEE 8th Int. Conf. Mobile Ad-Hoc Sensor Syst.*, Oct. 2011, pp. 709–714.
[80] H. Perrey, M. Landsmann, O. Ugus, T. C. Schmidt, and M. Wählisch, "TRAIL: Topology authentication in RPL," 2013, *arXiv:1312.0984*.
[81] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Netw.*, vol. 1, nos. 2–3, pp. 293–315, Sep. 2003.
[82] L. Teng and Y. Zhang, "SeRA: A secure routing algorithm against sinkhole attacks for mobile wireless sensor networks," in *Proc. 2nd Int. Conf. Comput. Modeling Simulation*, Jan. 2010, pp. 79–82.
[83] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," in *Proc. 20th IEEE Int. Parallel Distrib. Process. Symp.*, Apr. 2006, p. 8.
[84] T. H. Hai and E.-N. Huh, "Detecting selective forwarding attacks in wireless sensor networks using two-hops neighbor knowledge," in *Proc. 7th IEEE Int. Symp. Netw. Comput. Appl.*, Jul. 2008, pp. 325–331.
[85] J. Brown and X. Du, "Detection of selective forwarding attacks in heterogeneous sensor networks," in *Proc. IEEE Int. Conf. Commun.*, 2008, pp. 1583–1587.
[86] G. Wang, W. Zhang, G. Cao, and T. La Porta, "On supporting distributed collaboration in sensor networks," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2003, pp. 752–757.
[87] E. H. Ngai, J. Liu, and M. Lyu, "On the intruder detection for sinkhole attack in wireless sensor networks," in *Proc. IEEE Int. Conf. Commun.*, vol. 8, Jun. 2006, pp. 3383–3389.
[88] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 644–653, 2014.
[89] F.-J. Zhang, L.-D. Zhai, J.-C. Yang, and X. Cui, "Sinkhole attack detection based on redundancy mechanism in wireless sensor networks," *Proc. Comput. Sci.*, vol. 31, pp. 711–720, Jan. 2014.
[90] G. Glissa and A. Meddeb, "6LowPSec: An end-to-end security protocol for 6LoWPAN," *Ad Hoc Netw.*, vol. 82, pp. 100–112, Jan. 2019.
[91] R. Z. El Kaissi, A. Kayssi, A. Chehab, and Z. Dawy, "Dawwsen: A defense mechanism against wormhole attacks in wireless sensor networks," Ph.D. dissertation, Dept. Elect. Comput. Eng., Amer. Univ. Beirut, Beirut, Lebanon, 2005.
[92] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 74–81, Jan. 2008.
[93] T. Aura, P. Nikander, and J. Leiwo, "DOS-resistant authentication with client puzzles," in *Proc. Int. Workshop Secur. Protocols*. Berlin, Germany: Springer-Verlag, 2000, pp. 170–177.
[94] R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the Internet of Things," in *Proc. IEEE 10th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2014, pp. 165–172.
[95] S. Song, H.-K. Choi, and J.-Y. Kim, "A secure and lightweight approach for routing optimization in mobile IPv6," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, Dec. 2009, Art. no. 957690.
[96] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 4, pp. 839–850, Apr. 2005.
[97] H. Al Zaid, E. Foo, and J. G. Nieto, "Secure data aggregation in wireless sensor network: A survey," *Int. J. Eng. Sci. Technol. (IJEST)*, vol. 5, no. 3, pp. 93–105, 2011.
[98] D. Christin, A. Reinhardt, P. S. Mogre, and R. Steinmetz, "Wireless sensor networks and the Internet of Things: Selected challenges," in *Proc. 8th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze*, 2009, pp. 1–3.
[99] *HART Communication Foundation*. Accessed: Oct. 2010. [Online]. Available: http://www.hartcomm.org/
[100] A. Kansal, S. Nath, J. Liu, and F. Zhao, "Senseweb: An infrastructure for shared sensing," *IEEE MultiMedia*, vol. 14, no. 4, pp. 8–13, Oct./Dec. 2007.
[101] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, *Transmission of IPv6 Packets over IEEE 802.15.4 Networks*, document RFC 4944, 2007.
[102] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, *The Kerberos Network Authentication Service*, document RFC 4129, 2005.
[103] N. Kushalnagar, G. Montenegro, and C. Schumacher, *IPv6 Over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*, document RFC 4919, 2007.
[104] G. W. Irwin, J. Colandairaj, and W. G. Scanlon, "An overview of wireless networks in control and monitoring," in *Proc. ICIC* (Lecture Notes in Computer Science), vol. 4114. Berlin, Germany: Springer-Verlag, 2006, pp. 1061–1072.
[105] J. Lopez, R. Roman, and C. Alcaraz, "Analysis of security threats, requirements, technologies and standards in wireless sensor networks," in *Foundations of Security Analysis and Design V* (Lecture Notes in Computer Science), vol. 5705. Berlin, Germany: Springer-Verlag, 2009, pp. 289–338.
[106] *Wireless Medium Access Control and Physical Layer Specifications for Low-Rate Wireless Personal Area Networks*, IEEE Standard 802.15.4-2006, 2006.
[107] K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, and M. Welsh, "Sensor networks for emergency response: Challenges and opportunities," *IEEE Pervasive Comput.*, vol. 3, no. 4, pp. 16–23, Oct./Dec. 2004.
[108] G. Misuraca, "Futuring e-government: Governance and policy implications for designing an ICT-enabled knowledge society," in *Proc. 3rd Int. Conf. Theory Pract. Electron. Governance*, 2009, pp. 83–90.
[109] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 2, pp. 391–406, Mar. 2020.

[110] *Air Pollution Diseases*. Accessed: Oct. 2020. [Online]. Available: https://www.environmentalpollutioncenters.org/air/diseases/
[111] S. Challa, M. Wazid, A. K. Das, and M. K. Khan, "Authentication protocols for implantable medical devices: Taxonomy, analysis and future directions," *IEEE Consum. Electron. Mag.*, vol. 7, no. 1, pp. 57–65, Jan. 2018.
[112] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.
[113] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "AKM-IoV: Authenticated key management protocol in fog computing-based internet of vehicles deployment," *IEEE Internet of Things J.*, vol. 6, no. 5, pp. 8804–8817, Oct. 2019, doi: 10.1109/jiot.2019.2923611.
[114] M. Wazid, A. K. Das, N. Kumar, V. Odelu, A. G. Reddy, K. Park, and Y. Park, "Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks," *IEEE Access*, vol. 5, pp. 14966–14980, 2017.
[115] H. Larthani, A. Zrelli, and T. Ezzedine, "On the detection of disasters: Optical sensors and IoT technologies," in *Proc. Int. Conf. Internet Things, Embedded Syst. Commun. (IINTEC)*, Hammamet, Tunisia, Dec. 2018, p. 142.
[116] M. Hasan. *Top 20 Most Remarkable IoT Applications in Today's World*. Accessed: Oct. 2020. [Online]. Available: https://www.ubuntupit.com/most-remarkable-iot-applications-in-todays-world/
[117] S. Ravindra (2018). *IoT Applications in Agriculture*. Accessed: Oct. 2020. [Online]. Available: https://www.iotforall.com/iot-applications-in-agriculture
[118] F.-H. Tseng, H.-H. Cho, and H.-T. Wu, "Applying big data for intelligent agriculture-based crop selection analysis," *IEEE Access*, vol. 7, pp. 116965–116974, 2019.
[119] G. Han and M. Ma, "Connecting sensor networks with IP using a configurable tiny TCP/IP protocol stack," in *Proc. 6th Int. Conf. Inf., Commun. Signal Process.*, 2007, pp. 1–5.
[120] A. Dunkels, "Design and implementation of the lwIP TCP/IP stack," *Swedish Inst. Comput. Sci.*, vol. 2, p. 77, Feb. 2001.
[121] M. Zúniga and B. Krishnamachari, "Integrating future large-scale wireless sensor networks with the internet," USC, Comput. Sci., Los Angeles, CA, USA, Tech. Rep. 14860572, 2003.
[122] P. Thubert, "Objective function zero for the routing protocol for low power and lossy networks (RPL)," Cisco Syst., Moulineaux, France, Tech. Rep. draft-ietf-roll-of0-20, 2012.
[123] D. Chasaki and C. Mansour, "Security challenges in the Internet of Things," *Int. J. Space-Based Situated Comput.*, vol. 5, no. 3, p. 141, 2015.
[124] N. Bizanis and F. A. Kuipers, "SDN and virtualization solutions for the Internet of Things: A survey," *IEEE Access*, vol. 4, pp. 5591–5606, 2016.
[125] Y. Jararweh, M. Al-Ayyoub, A. Darabseh, E. Benkhelifa, M. Vouk, and A. Rindos, "SDIoT: A software defined based Internet of Things framework," *J. Ambient Intell. Humanized Comput.*, vol. 6, no. 4, pp. 453–461, Aug. 2015.
[126] T.-T. Nguyen, C. Bonnet, and J. Harri, "SDN-based distributed mobility management for 5G networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–7.
[127] P. Thubert, M. R. Palattella, and T. Engel, "6TiSCH centralized scheduling: When SDN meet IoT," in *Proc. IEEE Conf. Standards for Commun. Netw. (CSCN)*, Oct. 2015, pp. 42–47.
[128] O. Flauzac, C. González, A. Hachani, and F. Nolot, "SDN based architecture for IoT and improvement of the security," in *Proc. IEEE 29th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, Mar. 2015, pp. 688–693.
[129] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 236–262, 1st Quart., 2016.
[130] J. Li, E. Altman, and C. Touati, "A general SDN-based IoT framework with NVF implementation," *ZTE Commun.*, vol. 13, no. 3, pp. 42–45, 2015.
[131] C. Prazeres and M. Serrano, "SOFT-IoT: Self-organizing FOG of things," in *Proc. 30th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Mar. 2016, pp. 803–808.
[132] Y. Ai, M. Peng, and K. Zhang, "Edge computing technologies for Internet of Things: A primer," *Digit. Commun. Netw.*, vol. 4, no. 2, pp. 77–86, 2018.
[133] A. Gyrard, M. Serrano, and P. Patel, "Building interoperable and cross-domain semantic web of things applications," in *Managing the Web of Things*. Ithaca, NY, USA: Cornell Univ., 2017, pp. 305–324.
[134] S. Li, G. Oikonomou, T. Tryfonas, T. M. Chen, and L. Da Xu, "A distributed consensus algorithm for decision making in service-oriented Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1461–1468, May 2014.
[135] M. P. Papazoglou and W.-J. van den Heuvel, "Service oriented architectures: Approaches, technologies and research issues," *VLDB J.*, vol. 16, no. 3, pp. 389–415, 2007, doi: 10.1007/s00778-007-0044-3.
[136] S. Alam and J. Noll, "A semantic enhanced service proxy framework for Internet of Things," in *Proc. IEEE/ACM Int. Conf. Green Comput. Commun. Int. Conf. Cyber, Phys. Social Comput.*, Dec. 2010, pp. 488–495, doi: 10.1109/GreenCom-CPSCom.2010.116.
[137] P Varga, F. Blomstedt, L. L. Ferreira, J. Eliasson, M. Johansson, J. Delsing, and I. M. de Soria, "Making system of systems interoperable–The core components of the arrowhead framework," *J. Netw. Comput. Appl.*, vol. 81, pp. 85–95, Mar. 2017.
[138] F. Scioscia and M. Ruta, "Building a semantic web of things: Issues and perspectives in information compression," in *Proc. IEEE Int. Conf. Semantic Comput.*, Sep. 2009, pp. 589–594.
[139] A. J. Jara, A. C. Olivieri, Y. Bocchi, M. Jung, W. Kastner, and A. F. Skarmeta, "Semantic web of things: An analysis of the application semantics for the IoT moving towards the IoT convergence," *Int. J. Web Grid Services*, vol. 10, nos. 2–3, pp. 244–272, 2014.
[140] M. Sheng, Y. Qin, L. Yao, and B. Benatallah, *Managing the Web of Things: Linking the Real World to the web*. San Mateo, CA, USA: Morgan Kaufmann, 2017.
[141] M. Ganzha, M. Paprzycki, W. Pawłowski, P. Szmeja, and K. Wasielewska, "Semantic interoperability in the Internet of Things: An overview from the INTER-IoT perspective," *J. Netw. Comput. Appl.*, vol. 81, pp. 111–124, Mar. 2017.
[142] A. Sheth, C. Henson, and S. S. Sahoo, "Semantic sensor web," *IEEE Internet Comput.*, vol. 12, no. 4, pp. 78–83, Jul./Aug. 2008.
[143] D. Pfisterer, K. Romer, D. Bimschas, O. Kleine, R. Mietz, C. Truong, H. Hasemann, A. Kröller, M. Pagel, M. Hauswirth, M. Karnstedt, M. Leggieri, A. Passant, and R. Richardson, "SPITFIRE: Toward a semantic web of things," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 40–48, Nov. 2011.
[144] V. Terziyan, O. Kaykova, and D. Zhovtobryukh, "UbiRoad: Semantic middleware for context-aware smart road environments," in *Proc. 5th Int. Conf. Internet Web Appl. Services*, 2010, pp. 295–302.
[145] A. Gyrard and M. Serrano, "Connected smart cities: Interoperability with seg 3.0 for the Internet of Things," in *Proc. 30th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Mar. 2016, pp. 796–802.
[146] S. De, P. Barnaghi, M. Bauer, and S. Meissner, "Service modelling for the Internet of Things," in *Proc. Federated Conf. Comput. Sci. Inf. Syst. (FedCSIS)*, Sep. 2011, pp. 949–955.
[147] S. Lata and S. Mehfuz, "Machine learning based energy efficient wireless sensor network," in *Proc. Int. Conf. Power Electron., Control Autom. (ICPECA)*, Nov. 2019, pp. 1–5, doi: 10.1109/ICPECA47973.2019.8975526.
[148] A. B. Raj, M. V. Ramesh, R. V. Kulkarni, and T. Hemalatha, "Security enhancement in wireless sensor networks using machine learning," in *Proc. IEEE 14th Int. Conf. High Perform. Comput. Commun. IEEE 9th Int. Conf. Embedded Softw. Syst.*, Jun. 2012, pp. 1264–1269.
[149] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Gener. Comput. Syst.*, vol. 82, pp. 761–768, May 2018.
[150] V. Singh, S. Puthran, and A. Tiwari, "Intrusion detection using data mining with correlation," in *Proc. 2nd Int. Conf. for Converg. Technol. (I2CT)*, Apr. 2017, pp. 620–625.
[151] S. Kaplantzis, A. Shilton, N. Mani, and Y. A. Sekercioglu, "Detecting selective forwarding attacks in wireless sensor networks using support vector machines," in *Proc. 3rd Int. Conf. Intell. Sensors, Sensor Netw. Inf.*, 2007, pp. 335–340.
[152] N. M. Alajmi and K. M. Elleithy, "Comparative analysis of selective forwarding attacks over wireless sensor networks," *Int. J. Comput. Appl.*, vol. 111, no. 14, pp. 27–38, Feb. 2015.
[153] J. Canedo and A. Skjellum, "Using machine learning to secure IoT systems," in *Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST)*, Dec. 2016, pp. 219–222.
[154] A. Ferdowsi and W. Saad, "Deep learning-based dynamic watermarking for secure signal authentication in the Internet of Things," 2017, *arXiv:1711.01306*.

[155] L. Xiao, X. Wan, C. Dai, X. Du, X. Chen, and M. Guizani, "Security in mobile edge caching with reinforcement learning," 2018, *arXiv:1801.05915*.
[156] 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 *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 2177–2184.
[157] Y. Meidan, M. Bohadana, A. Shabtai, M. Ochoa, N. Ole Tippenhauer, J. Davis Guarnizo, and Y. Elovici, "Detection of unauthorized IoT devices using machine learning techniques," 2017, *arXiv:1709.04647*.
[158] Y. Meidan, M. Bohadana, A. Shabtai, J. D. Guarnizo, M. Ochoa, N. O. Tippenhauer, and Y. Elovici, "ProfilIoT: A machine learning approach for IoT device identification based on network traffic analysis," in *Proc. Symp. Appl. Comput.*, 2017, pp. 506–509.
[159] H. Rathore, V. Badarla, S. Jha, and A. Gupta, "Novel approach for security in wireless sensor network using bio-inspirations," in *Proc. 6th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2014, pp. 1–8.
[160] A. Outchakoucht, E.-S. Hamza, and J. P. Leroy, "Dynamic access control policy based on blockchain and machine learning for the Internet of Things," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 7, pp. 417–424, 2017.
[161] G. O. Young, "Synthetic structure of industrial plastics," in *Plastics*, 2nd ed., vol. 3, J. Peters, Ed. New York, NY, USA: McGraw-Hill, 1964, pp. 15–64.

SONAM LATA was born in India, in 1991. She received the B.Tech. degree in electronics and communication engineering from Uttar Pradesh Technical University (UPTU), Lucknow, in 2013, and the M.Tech. degree in instrumentation engineering from NIT Kurukshetra, in 2016. She is currently pursuing the Ph.D. degree in electrical engineering with Jamia Millia Islamia, India. She has coauthored 12 papers in SCIE indexed journals and conferences.

SHABANA MEHFUZ (Senior Member, IEEE) received the B.Tech. degree in electrical engineering from Jamia Millia Islamia, New Delhi, India, in 1996, the M.Tech. degree in computer technology from IIT Delhi, in 2003, and the Ph.D. degree in computer engineering from Jamia Millia Islamia, in 2008.

She has been working at the Department of Electrical Engineering, Jamia Millia Islamia, for the past 22 years. She has guided seven Ph.D. candidates and is supervising six other candidates. She has published more than 70 papers in international journals and conferences. Her research interests include computer networks and computational intelligence. She is a Life Member of ISTE, a member of the Institution of Engineers, and a Life Member of the Computer Society of India. She has received grants for research projects from agencies, like AICTE and UGC. She has been awarded the International Inspirational Women Award 2020 for Best Performer in Government Award by the GISR Foundation. She has acted as the track chair for two flagship International IEEE conferences held in 2015 and 2019. Her research interest includes Computer Networks and Computational Intelligence.

SHABANA UROOJ (Senior Member, IEEE) received the B.E. degree in electrical engineering and the M.Tech. degree in instrumentation and control from Aligarh Muslim University, Aligarh, India, in 1998 and 2003, respectively, and the Ph.D. degree from the Department of Electrical Engineering, Jamia Millia Islamia (A Central University), Delhi, India, in 2011. She has nearly three years of industry experience and over 19 years of teaching experience. She is currently working as an Associate Professor with the Department of Electrical Engineering, College of Engineering, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia. She has guided several Ph.D. and master's thesis and dissertations. She has authored and coauthored more than 140 research papers which are published in high quality international journals and conference proceedings. She was a recipient of the Research Excellence Award from PNU, the Springer's Excellence in Teaching and Research Award, the American Ceramic Society's Young Professional Award, the IEEE Region 10 Award for outstanding contribution in Educational Activities, and several best paper presentation awards. Recently, she has received the Badge of IEEE STEM Ambassador-Region 8 for her volunteering and efforts in STEM promotional activities and involvement. She is holding the responsibility of the Vice Chair of the IEEE Saudi Arabia Section.