Security Issues and Challenges in Wireless Sensor Networks: A Survey

Yawar Abbas Bangash, Qamar ud Din Abid, Alshreef Abed Ali A, Yahya E. A. Al-Salhi

***Abstract*—Wireless Sensor Networks (WSNs) have facilitated human life in different fields: medical, engineering, agriculture, environment, traffic, and military. WSNs are extensively used in monitoring, tracking, and controlling applications; however, their resource constraint nature faces new challenges. These are: centralized management, device heterogeneity, routing protocols, node's mobility, information privacy, and limited computational-power. WSN spans over a large geographical area; therefore, they must address the issue of routing-protocols, scalability, communication, and security. This survey highlights WSNs' applications, security requirements, different attacks and defenses, and contemporary issues and challenges. In addition, the integration of virtualization, cloud computing, and Software Defined Networking (SDN) in WSNs is also explained with a new set of challenges. We believe, this paper provides a deep insight and a valuable blue print for interested readers and researchers in WSN, and its related technologies.**

***Index Terms*—Wireless Sensor Network, Security Attacks, Security Challenges, Defenses, Software Defined Networking.**

I. Introduction

Wireless Sensor Networks (WSNs) are defined as a large number of low-cost, low memories, self-organizing, unattended, low processing capable, and distributed embedded [1] small sensor nodes; they communicate through a channel (air) to collect data from the surrounding interest, process it, and report to the sink. WSNs are used in commercial, and military applications, such as, inventory control, traffic monitoring, and tactical surveillance. They also provide border security to prevent terrorism, and illegal movement of drugs and weapons[2]. These networks provide socio-economic benefits, e.g., weather prediction, mission-critical systems, target field imaging, precision agriculture, and patient monitoring; they provide a communication way in disaster-hit area [3]. A brief explanation about WSNs applications can be found in Section III.

Designing a secure, a scalable, a robust, and a reliable WSN needs sufficient knowledge to overcome the inherited limitations of storage capacity, processing power, and communication range. According to [4], cryptographic techniques and key management tools bring computational and space challenges for resource constraint hardwares. Developing and building a robust WSN operating system faces the complications of memory management, processes scheduling, and energy-efficient processing. WSNs need to address the technology trend, the integration of: cloud computing, Software Defined Networking (SDN), and virtualization technologies. A hostile environment—enemy vicinity—poses challenges of security and protection against tampering and physical attacks. Considering these issues, we aim to provide a comprehensive and state of the art literature review.

Our contributions are: a comprehensive overview surrounding security issues and challenges in WSNs, explanations of different terminologies common in WSNs security, a rigorous analysis of different techniques used in WSNs, and introduction of new challenges of SDN, cloud computing, and virtualization technologies. Section II discusses the basic model of WSNs and its background knowledge. In Section III, we briefly explain WSNs applications. Section IV is about WSNs requirements; Section V discuses common attacks in WSNs. Section VI elaborates defenses/solutions; and Section VII describes key challenges in WSNs. A brief summary in Section VIII concludes the survey.

II. Wireless Sensor Network Background

The basic building block of a WSN is the sensor node; the reference diagram is shown in Figure 1. A sensor node consists of different units: memory, processor, power, sensor, transceiver, position finding system, and/or a mobilizer. All these units are not mandatory; it depends on the context and situation. For example, a GPS capable WSN should have a mobilizer or position finding system for tracking.

An important unit of a sensor node is the transceiver; it can send and receive data/signals. In a sensor node, transceiver unit consumes more power compared to other units, because the packet transmission process includes signal amplification. To improve the sensor node's battery power, it is advised that transceiver unit should be designed properly to consume less amount of energy when sending and receiving data/signals.

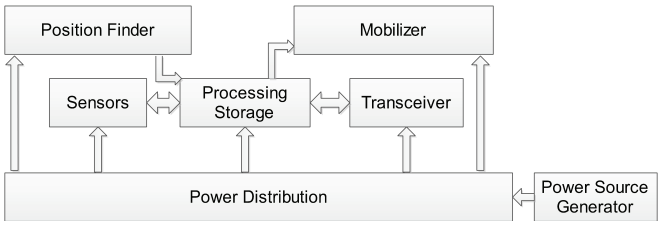

Fig. 1: Reference Diagram of a Wireless Sensor Node: The power generating unit provides power to the main power unit, which further distributes power to all sub-units. All sub-units work together to perform sensing activities.

Manuscript submitted on 2016-04-08, revised on 2017-02-21. This work is supported in part by the National 973 Program of China under grant 2011CB302301, the Fundamental Research Funds for the Central Universities (HUST:2014QN009), Natural Science Foundation of Hubei Province (2013CFB150), and Higher Education Commission Pakistan (HEC).

Mr. Yawar Abbas Bangash (yawarabbas@hust.edu.cn, yawar.parachinar2003@gmail.com), and Mr. Yahya E. A. Al-Salhi (yahya_alsalhi@yahoo.com) are with the School of Computer Science, Huazhong University of Science and Technology, China.

Mr. Qamar ud Din Abid (qabid@hust.edu.cn) is with the school of Mechanical Science and Engineering, Huazhong University of Science and Technology, China.

Mr. Alshreef Abed Ali A (alshreefabed@whut.edu.cn) is with the School of Computer Science and Technology, Wuhan University of Technology, China.

Different sensor nodes are available in the market e.g., mica2 and mica2dot, and Tmote Sky, etc. These sensors have a small memory space (10KB, 16KB, 32KB), and a limited processing power (8MHz, 16MHz) that can handle node's operations. In addition, a small flash ROM (24K, 48K) is available to store important processing-data.

Reference architecture for a WSN node [1] is shown in Figure 2. The physical infrastructure includes sensor nodes and related hardwares. OS governs overall node's operations; different OSs are in practice for low power wireless devices. One of the most popular OS is TinyOS [5]; it is an open source, event-based operating system designed for low-power wireless devices, and optimized for memory limitations. System services provide core functionalities: storage management, localization, time synchronization, and reprogramming. Programming abstraction provides APIs to the application layer. An application developer can build applications to operate the desired WSN.

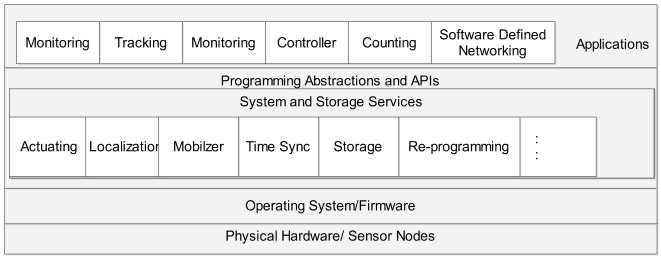

Fig. 2: WSN Reference Architecture: A general reference architecture defines the core functionalities, standards, and APIs; APIs facilitate an application developer to interact with the system services.

A WSN consists of different nodes: base station, sensor nodes, and aggregator nodes as shown in Figure 3. This proposed model provides minimum delay, prolonged network life, and sink-node location privacy [6]. Base station is highly equipped system both in software and hardware; it has more processing capabilities, more memory, and more energy.

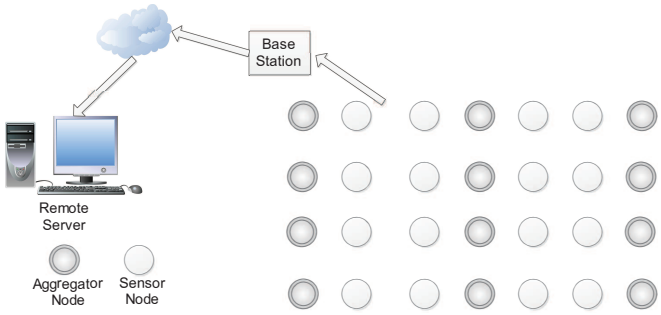

Fig. 3: Basic Diagram of WSN with Aggregator Node: Sensor nodes sense the events, which are collected by aggregator-nodes. Aggregator nodes forward all events to the Base Station, which is further forwarded to a remote server via the Internet or directly.

Base station is responsible for topology generation and taking on the spot action against any malfunctioning in the network [6]. It collects critical data (military applications); its location should be protected from outside and inside attackers. If an adversary knows about the base station location, he can launch different attacks via traffic monitoring [7] or traffic tracing techniques [8]. In WSNs, aggregator node reduces delay, increases network life, and above-all hides base station location from adversaries very efficiently [6].

III. Wireless Sensor Networks Applications

WSNs are resource constraints devices; however, due to their diversity, they are used in: university campuses, buildings, road traffic monitoring, vehicle tracking systems, mission-critical systems, and atomic reactors. Sensors are embedded in a physical object for different purposes, e.g., field monitoring, picture/video capturing, and task performing in a high or cold temperature (automation industry). These interconnected sensor devices produce a huge amount of data, which can be used to analyze and understand the collective behavior of some geographically populated area. Materials for Section III can be found at [9], [1]. This section briefly overviews important applications, which further explains the importance of security in WSNs.

A. Wireless Sensor Networks in Industry

Different sensors combinations are used to form WSNs to monitor machine structural health; the network timely informs the control room for any structural flaw in a material.

1) Environmental Wireless Sensor Networks: Sensors include in this category are: temperature, humidity, soil moisture, wind, and pressure; the network of these sensors facilitates precision agriculture, which monitor temperature, humidity of soil and leaf, and the speed of wind and direction.
2) Physical Wireless Sensor Networks: Sensors combination of accelerometer, presence, vibration, power, ultrasound, water, sound, bend, flex, strain, and stress can establish a cooperative WSN to control motion, vibration, and presence of different objects.
3) Wireless Sensor Networks in Gas Sector: Different sensors combination of CO_2, CO, CH_4, O_2, NH_3, SH_2, NO_2, and pollution sensors can build a WSN to monitor the organic gases like CO_2, CH_4, NH_3, and SH_2.
4) Wireless Sensor Networks in Optics: Different sensors in optics are: infrared, sunlight, radiation, ultraviolet, and color. These networks are used in agriculture to monitor the sunlight, radiation, and ultraviolet rays; the result is analyzed to measure the amount of energy and light used by plants.

B. Wireless Sensor Networks for Society

WSNs facilitate society in health care and traffic monitoring systems [10]; they provide a new paradigm of smart cities where everything is connected to each other. The distributed connectivity provides the following advantages.

1) Intelligent Buildings/Homes and Bridges: In intelligent buildings, WSNs are used to reduce energy wastage by proper ventilation, and air-conditioning system; in homes, smart metering solves traditional metering system issues: installation, cost, and management. Intelligent bridges use WSNs to monitor the stress, number of allowed vehicles, and any leakage or crack

in the bridges. Structural Health Monitoring (SHM) is a sensor based approach to monitor the reliability or health of structural materials used in bridges.

2) Smart Parking and Cities: An efficient traffic system uses smart parking; WSNs monitor the flow and exit of vehicles, and inform the control room about the congestion if any. In addition, smart cities exploit WSNs advantages to monitor noise pollution, which can prevent environmental problems, e.g., loud noise.
3) Wireless Body Area Networks: A body area network monitors the human body temperature, sugar level, blood pressure, and stress level [11]; this helps doctors to diagnose a disease on a scientific approach.

C. Wireless Sensor Networks in Agriculture and Wild Life

WSNs are used to monitor wild life; information is collected about animal behavior, their interaction, and their different habits.

1) Wireless Sensor Networks in Precision Agriculture: Wikipedia defines precision agriculture (PA) as —a satellite farming, or site specific crop management (SSCM) is a farming management concept based on observing, measuring, and responding to inter and intra-field variability in crops. Different crops have different properties. For these diverse properties, WSNs provide a scientific approach to collect data and analyze it. They [12] have shown that it is possible to build a fully robust, solar powered, and low cost Irrigation Management System (IMS) to suit the socio-economic conditions of small-scale farmers in developing countries. The smart irrigation system reduces wastage of water; these networks timely inform farmers about water level and plant diseases.
   WSNs are useful in controlling nursery's conditions, and closely monitoring high-performance crops, such as, tropical fruits. The monitored parameters can vary from location to location; however, different soil types, temperature and wind level, water quality, and humidity and sunlight intensity can affect the smart agriculture systems.
2) Wireless Sensor Networks in Animal Rearing: WSNs are used in animal rearing; the installed network monitors the room temperature and keeps it on a suitable level. Live stocks emit different gases: Methane, Ammonia, Hydrogen, and Sulphide; WSNs monitor different gas levels for taking livestock health care.

D. Wireless Sensor Network for Environment Protection

In a disaster quick relief emergency situation, sensor nodes are dropped from a helicopter to the affected area, e.g., fire, to monitor the temperature and send back the data to the server. A pre-installed sensor network in wild life timely inform control room about any fire case.

1) Wireless Sensor Networks in Atomic Reactors: For the state-level policy, an installed WSN in the atomic reactor needs a crucial importance [9]. These networks monitor highly radiated zones without sacrificing the life of the reactor's staff. In case of radiation leakage, catastrophic situation (station blackout), natural calamity, and earthquake, these networks facilitate governments and states. However, these networks should be highly equipped to cope with high temperature and un-predictable catastrophic situations.
2) Wireless Sensor Networks in Pollution Monitoring: WSNs provide data about the pollutant, resulted from vehicle emission, industrial application, coal trains, glass and steel factories, and coal-fired power plants. These emissions are dangerous to both health and physical environment. According to world health organization (WHO), this problem kills 2.4 million people each year [13]. Some important diseases caused by pollution are: asthma, cancer, heart disease, respiratory problems, emphysema, weak immunity system, and birth defects.
3) Volcano Monitoring: Volcanos are natural events where monitoring must consider technical, scientific, and social aspects [14]; the main goal is to provide public safety on time. Figure 4 shows a bird-view of different applications.

IV. Security Requirements in Wireless Sensor Networks

Security requirements are the basic roots of any WSN; fulfilling security requirements ensure network stability and operations. The basic security requirements of WSNs definitely surround Confidentiality, Integrity and Authentication (CIA) triangle, but it is not only limited to cryptography. Cryptography can help to protect the system as much as secure; however, cryptography is not the solution of all security measures. A secure network should consider authorization and authentication as too. Some requirements are related to application-specific environment [15]. We grouped security requirements into: data level security, node level security, code/program level security, and network level security.

A. Data Level Security

Data security ensures safety from unauthorized access, and protects it from alteration and corruption. In the context of WSNs, a transit data can be captured, and altered by a malicious user, who can resend the modified data [16].

1) Authentication: One of the core requirements for WSNs is authentication—ensuring that the data is from the intended right source. Any bad guy/adversary can claim as a true source [17], [18]. It is the mechanism to verify the identity of a node who wants to communicate with other nodes. In general authentication, multiple ways are used to provide identity, e.g., typing a username and password, swiping a smart card, waving a token device, using a digital certificate, using voice recognition, and using retina and finger prints [19]. For WSNs, biometrics, retina, or finger prints will not be applicable; however, in future IT, WSNs may incorporate these technologies.
2) Confidentiality: Confidentiality refers to limiting information access and disclosure only to user/nodes, who are authorized; and preventing it from those who are unauthorized [20]. Authorized people and authorized nodes can access data, while unauthorized people and unauthorized nodes cannot access data. It ensures the

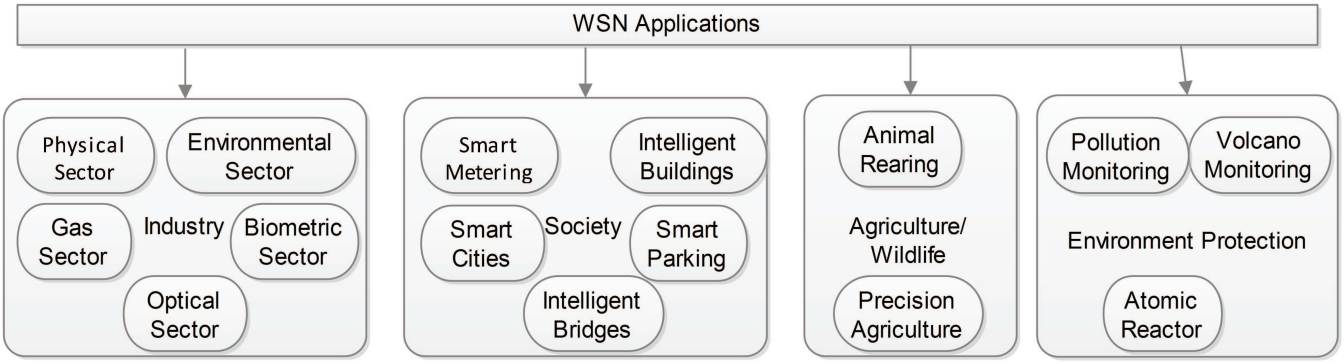

Fig. 4: WSN Applications: Applications are categorized according to their scope; they are used at a big scale in industry. Applications' list presented in this section is not the final–it is growing.

privacy of contents, and protects the contents to be meaningless for any bad guy [17]. Confidentiality consists of two parts, access authorization, and privacy [21]. Access authorization allows data access only to legitimate users, while privacy protects the sensitive data from all those who are un-authorized.

3) Integrity: Integrity refers to the accuracy, authenticity, completeness, and trustworthiness of information resources [22], [23]. Integrity is concerned with data, that haven't been changed inappropriately, accidentally, or deliberately; integrity of data cannot be justified without detection [23]. Integrity also includes source/origin integrity–the sending node is the trusted node to receive data from. Integrity involves the entire life cycle of data maintenance, consistency, accuracy, and trustworthiness. It is the preservation of information, whether wrong or right that are being sent by a source. All information is valid if sent by the right trustworthy source, and the received data is same as sent data.
4) Freshness: Data must be recent, and no old messages should have been replayed. Data freshness is the message received, but not a replayed message sent by the adversary [15]. If the receiver gets out-of order packets, such freshness is called a weak freshness; and if the receiver gets all packets in-order, such freshness is called a strong freshness [22].

B. Node Level Security

Some WSNs are designed to work in a hostile environment; it is not feasible for a human being visit those sites, and performs an attended operation, for instance, fire in wild-life, cold temperature zones, atomic reactors, and military operations. In a hostile environment, attended access to nodes is much difficult or impossible–in some ways. These situations demand for more security. All nodes must be properly placed and protected from malicious users. Every node in the deployed field carries information, e.g., node ID, cryptographic key, and the underlined designed secure protocol. Proper node level security measures prevent attackers to access a node and extract cryptographic keys.

1) Availability: Availability is the guarantee that a network responsible for delivering, storing, maintaining, and processing information must be accessible whenever needed by those entities who need them with authorization [20]. WSNs should ensure that all nodes and gateways must be available all the times; network should be protected from bad guys, who can flood sensor nodes with a lot of packets. According to [20] network is called useless network, until its availability, no matter how strong it is. Technical and catastrophic phenomenon affects the security aspects of WSNs—availability is not different in this case. Some phenomena are: node failure, communication link failure, power drain, high temperature, wind storm, and water flood.
2) Authorization: Authorization surrounds users' rights access; it defines services that they can avail. Network administrator assigns different service policies for different users; some users are assigned modification access, while some users have only read access. In WSNs, different rules and policies are assigned to different sensor nodes; policies and rules dictate, which sensor node can read data from the surroundings, and which sensor node can send data to base station.
3) Non-repudiation: Non-repudiation is an attribute in communication technology, specifically in digital communication, used to prevent future false denial of what is being sent or done. ITU-T Recommendation X.805 security dimension states preventing the ability to deny that an activity/action on the network occurred. In WSNs, non-repudiation is to prevent any node that in later stages deny of not sending that data. It ensures the digital evidence of that node, which is involved in the communication; it is a service that provides proof of the integrity and origin of data; it is the guaranty that someone who has sent something or done some action cannot deny his or her action at later stages. In a real-world example, if a legal document is signed without witnesses, that person at later stages can deny of his own signature. The purpose of non-repudiation is to prevent such a denial.
4) Secure Localization: Often, the use of a sensor network relies on its ability to accurately and automatically locates sensor node in the network [24]. A sensor network designed to locate faults and errors needs accurate location information to pinpoint the fault. If any adversary identifies the location of a deployed sensor node, he can destroy it.

C. Network Level Security

Network security is a broad term comprising of policies and rules assigned by the network administrator to prevent unauthorized data or system access. It includes activities related to reliability, integrity, scalability, and safety of network data and hardwares.

1) Self-Organizing: In a WSN, due to its open media vulnerable nature, eavesdropping is very easy for an adversary. Adversary can monitor and analyze wireless signals by the spectrum analyzer; adversary can launch man in the middle or denial of service attack on the sensor network. Self-organizing is the solution to such problems [25]. All sensor nodes in a WSN are distributed; a centralized sensor node/base station is responsible to communicate with all other sensor nodes. These distributed sensor devices send data in-directly–hop by hop communication. If self-organization is lacking in a sensor network, the damage resulting from an attack can lead to unavailability of a network [18].
2) Time Synchronization: In a distributed WSN, events and communication must be synchronized to carry out network operations; it is a way to synchronize local clock of the sensor node with the communicating entities [26]. The knowledge of timing among sensor nodes is essential that detects events: movement, humidity, and temperature. These events should be synchronized to get in-oder information. Different synchronization protocols are used for single hop and multi hop communication [27]. Time synchronization is also important for data freshness, where the communication entities ensure the real-time data—not a replayed packet.
3) Scalability: Hundreds of thousands of nodes are deployed in a network carrying out distributed operations. Because of this explosive proliferation of sensor nodes, scalability is becoming an important topic in WSN; it is the fundamental concern in WSN, that dictates the system performance measure. Generally, scalability refers to the ability of a system to perform useful work when the size of the system increases or input to system increases. WSN must be scalable to provide capacity for additional nodes. New nodes insertion and old nodes removal should be easy with no bad impact over the network operations. Moreover, as new sensors are deployed and old sensors are failed, it is suggested that forward and backward secrecy should also be considered–leaving sensor must not be able to read any future messages, and the incoming sensor must not be able to read any past message [18].
4) Surrounding Security: The deployed WSN environment must be secured and protected from outside world. A proper surveillance cameras mechanism helps monitoring any malicious activity. Deploying surrounding security may not be practical in some mission-critical applications, e.g., monitoring enemy vicinity; however, such a system can be deployed in security systems for instance, in medical fields, wild life monitoring, and industrial applications.
5) Less Energy Consumption and Maximum Performance: The most important parameter in a WSN is power/energy. Insufficient energy leads to a catastrophic situation, e.g., unavailability and message drop. All nodes in the network must use some protocols/methods to conserve the provided less amount of energy. It is the trade-off between energy consumption and performance of the network. On one side, demand for high processing application such as, complex cryptography methods sacrifice the battery power. On the other side, to conserve more energy, low processing involved operations are suggested. for instance, humidity checking, temperate measurement, and object's movement.

D. Operating System and Tools for WSNs

OS governs all operations in a computing system. For WSN, the OS must be robust enough to cope with normal routines; it must address the issues of security holes in OS [28]. Memory protection, privilege mode, and file access permissions are some key-points where OS provides system-level security. The limited resource constraint behavior of WSNs faces additional challenges in OS design. These constraints affect the whole operations if not properly configured. They [28] have shown extensive explanation of OS architecture, programming model, scheduling, memory management and protection, communication protocols, resource sharing, and support for real-time applications.

1) Re-Programming: Re-programming provides flexibility; it removes the hardware burnt firmware modification limitations; [1] have provided a comprehensive survey about WSNs programming. Re-programming determines the system flexibility and adaptability to cope with new changes that are occurring in the deployed network e.g., changing the code for some specific node. To maintain a network, the administrator intervention is of crucial importance. In the software fault, an update and up-grade activity are necessary, either physically or remotely. The deployed network should have OTA programming feature [29] for insertion/removal of some code remotely; OTA programming provides global access to remote nodes. Re-programming can change the static behavior of a system to a dynamic behavior.
2) Tools for Wireless Networks: Tools play an important role to operate the system. For WSNs, proper tools are necessary to configure, manage, and update the underlined sensor node. Different command line tools and graphical user interface (GUI) come with specific vendors. These tools help in programing and examining the wireless media, and analyzing its characteristics; they also help troubleshooting the network. Different stakeholders, in WSNs, provide services ranging from device vendors to application programmers and end users. They use APIs to perform tasks: code modification, firmware upgradation, and software maintenance; these devices must go through the standardization agency to remove any future incompatibility. WSN requirements and their relation are shown in Figure 5.

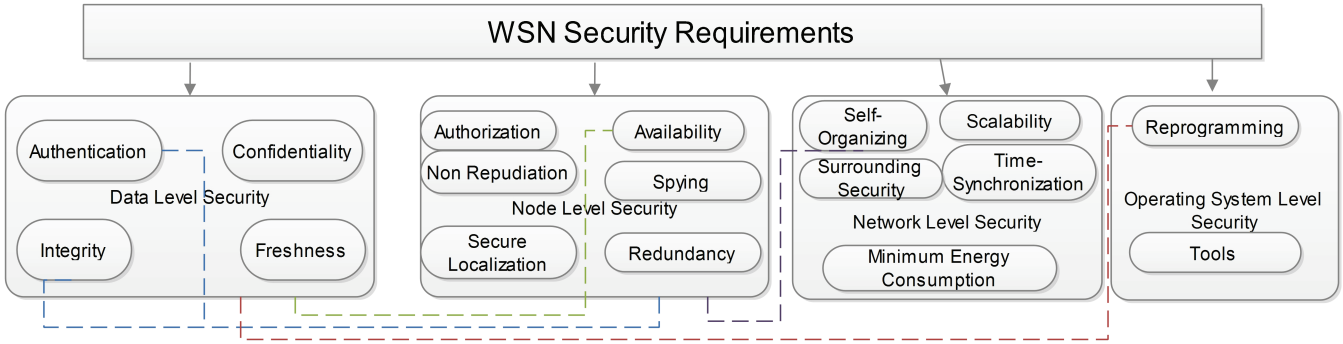

Fig. 5: WSNs Security Requirements and their Relation: WSNs requirements are directly related to the specific application area. These requirements are not only limited to as stated. These requirements have dependency as shown in dotted lines. For example, authentication and integrity also depend on node level security.

V. Attacks on Wireless Sensor Networks

Applications discussed in Section III, face their own specific challenges and security issues such as, data protection and sensor node protection. Because of the diverse set of applications, WSNs face a big list of attacks: traffic analysis, traffic tracing, node stealing, node tampering, and data alteration. When data is at rest, policies to secure it are different when data is in transit. A large number of sensor nodes communicate with each other, carrying-out an operation, involves a substantial amount of processing and communications. This communication can be monitored by an adversary; he can steal sensitive information [7].

A. Physical Attack

In a physical attack, the aim is to destroy the sensor physically, or steal it from its vicinity [30]. The attacker even does more harm; he can study and analyze the internal code; he can extract the secret cryptography key; he can modify it and, later, inject the replicated node in the network. This attack leads future communication towards the attacker's side. In this attack, the injected node sends data to both attacker and base station, at the same time, to hide its identity.

1) New Node Injection Attack: In this attack, an attacker introduces his malicious node [18]. His own designed injected new node, if successful, works with the deployed network to steal useful information; he also disrupts the proper operation of network, e.g., randomly bombarding fake packets to drain node's energy. The new malicious node can behave like a legitimate nodes and, thus, can violate the security of a system. Furthermore, if the attacker intention is to read the sensitive information, the injected new node forwards data to him to analyze the network traffic.
2) Sybil Attack: Redundancy provides availability and system maintainability. An attacker exploits this functionality by making a node to have multiple identities [31]; an insecure node is hijacked to have multiple identities. A node having multiple identities at different times disrupts routing and lead to false results. It is difficult to know the legitimate node; Sybil attack creates the confusion of a real node and a fake node.
3) Reverse Engineering Attack: Reverse engineering is the process to dissemble something in order to know its internal circuitry or functionality; it is not the process to copy or re-produce something, but the main goal is to analyze the system and know about its working mechanism. In this attack, the outside/inside attackers extract very useful information: software code, cryptography key, and node architecture.

B. Communication Attacks

In this paper, a physical attack refers to the physical access, while the logical attack refers to the changing or damaging the node remotely —without physically touching it. An extensive attacks' list can be found at [18].

1) Jamming: Jamming attack is directly launched on the physical layer of the WSN protocol architecture. In jamming attack, the attacker jams or block the communication signals [18]. He uses special devices to block signals, for instance, frequency jammers. Blocking the communication signals lead to unavailability.
2) DoS and Collision Attack: An attacker may flood the network with a large number of fake packets; in this attack, sensors' resources are used to process fake packets automatically [32]. Entertaining sufficient number of packets drain nodes' energy quickly. In addition, the attacker drains the node's energy by collision. In a collision attack [33], he sends continues packets in all directions to collide with the legitimate packets, and, thus the retransmission will occur for other packets. Retransmission causes delay, and drain nodes' energy. In these attacks, no service is available to the legitimate nodes.

C. Code Attack

Poor programming and ill-practiced code developing behavior lead to a weak software; a malicious user can exploit poor programming vulnerabilities. The OS must be well designed, tested, and implemented to cope with software bugs, e.g., overflow attack and exceptions. According to the [34], 90% of all vulnerabilities are related to the application level. This is the reason, that attackers have turned their attentions towards application.

1) Overflow Attack: An attacker exploits a weak software code, and launches overflow attack in the application layer [35]. In this attack, the victim node is unable to accept any further legitimate attempts for a new connection. Buffer overflow attack overflows the buffer,

and all future connections to that node are blocked. Overflow attack leads to node's unavailability.

2) Changing the Existing Node Remotely by Re-Programming: An expert attacker changes the code after accessing it; he can re-program the affected node and miss-route all the consequent communication. In tempering the existing node attack, he first gains access to the node, then reads the internal of a node remotely. After thoroughly investigating the node's code, he tries to change the behavior of a node, e.g., all future information will be sent to both attacker and other nodes. This attack is different from physical-tempering attack; in physical tempering attack, he captures a node and tempers/changes its code, and again injects into the network. In a remote tempering attack, attacker tempers the node functionality remotely.

D. Base Station Attack

In a WSN, base station or sink-node gathers data from surrounding nodes and reports to outside world via the Internet as shown in Figure 3. If base station is attacked and compromised, the critical mission is considered to be a failed one. Traffic tracing, and traffic monitoring attack [6] are very common attacks that are launched on base station. All the deployment cost will be compromised if the base station location is compromised.

1) Source Location Attack: In a source location attack, the attacker searches for the data/signal generated by a node and traces it [36]; he uses advance techniques, e.g., packet tracing [6], [37]. In a packet tracing technique, an attacker finds one packets while in transit, and follows the source address of that packet; the repeats the same method, and finally, reaches to the source via reverse packet tracing. He uses the node's source location information for any malicious activity, e.g., DoS attack on that particular source node.
2) Destination Location Attack: In this attack, attacker goal is to find the sink/destination node. Most of the cases, he aims to find the base station. He also aims to reach some other aggregator nodes or sensor nodes. For destination attack, the attacker uses traffic analysis [7] and traffic tracing [8] techniques. He analyzes traffic density around any node, and thus, wherever he observes a huge traffic density pattern, he deduces the destination node location.
3) Traffic Analysis Attack: An attacker analyzes the traffic volume without being aware of the contents of data, and ultimately, deducts the location of a base station. This attack exploits base station location information without being an expert in the WSN knowledge. In this attack, the attacker is not even interested to know what protocol is used, and which cryptography techniques are used. He only monitors the traffic volume over the entire network; wherever he sees huge traffic volume, he deducts the base station location, and launches other attacks to destroy base station or damage its operation.
4) Traffic Tracing Attack: In traffic tracing attack [8], attacker captures packets and studies the destination or source field; following the destination/source fields of all packets, he successfully traces a particular node. He can bombard the victim with fake packets and causes un-availability. Packet tracing attack is used to attack both the source node and the destination node.
5) Content Analysis Attack: In a content analysis attack, attacker captures packets and deeply studies it. His goal is to find useful information out of the packet, e.g., source address, destination address, and payload [38]. He can also alter the packet contents, and destination address so that all subsequent communications will be towards him. In content analysis attack, the attacker is interested in the actual contents to know about the real happening in the WSNs.

E. Routing Protocol Attacks

A strong OS provides a security for all its operations. A vulnerable OS can give a privileged mode access to an attacker; routing protocol exhibits the same phenomenon. Routing protocols in WSNs govern all the communication. Weak routing protocols exploits vulnerabilities; additionally, if the underline protocol is unable to cope with dynamics of surroundings, an attacker can exploit other weaknesses in it, e.g., large latency.

1) Black Hole Attack: In this attack, an attacker creates multiple nodes, where all traffic is forwarded, drowned, and dropped. This attack exploits the routing algorithm/protocol's weakness; a black hole node shows itself as the nearest and zero cost node. The surrounding nodes think of it as the nearest legal one and, thus, all traffic goes through it and doing nothing [17]. This attack makes fool the real sensor nodes to believe the injected node as a true node.
2) Hello Flood Attack: An attacker uses high power radio transmission to betray the legal nodes. Legal nodes consider the high transmission node as the shortest path node. In this attack, the real node follows the attacker's node, which leads to traffic congestion [17], [18] and packets drop. All subsequent communications are forwarded to the attacker node; he monitors and reads the whole network traffic to carry out malicious activity/operations.

VI. Defenses in Wireless Sensor Networks

Different techniques are used to protect WSNs from adversaries; these techniques prevent: jamming attack, black hole attacks, and DoS attacks; they also provide source, destination, and data privacy. Figure 6 shows the taxonomy of different WSNs attacks, causes, and their defenses.

A. Defenses for Cryptography Triangle

Business needs information integrity, authenticity, and privacy. The goal of WSNs deployment is to monitor some area, and collect information for future the purpose. Cryptography techniques must be used to ensure business privacy and integrity; it is difficult to apply traditional passwords techniques in WSNs, e.g., two-factor authentication. However, in WSNs, we suggest to use light weight protocols, while implementing cryptography techniques.

1) Confidentiality: Confidentiality, integrity, and availability are used to validate the proper entity—to provide

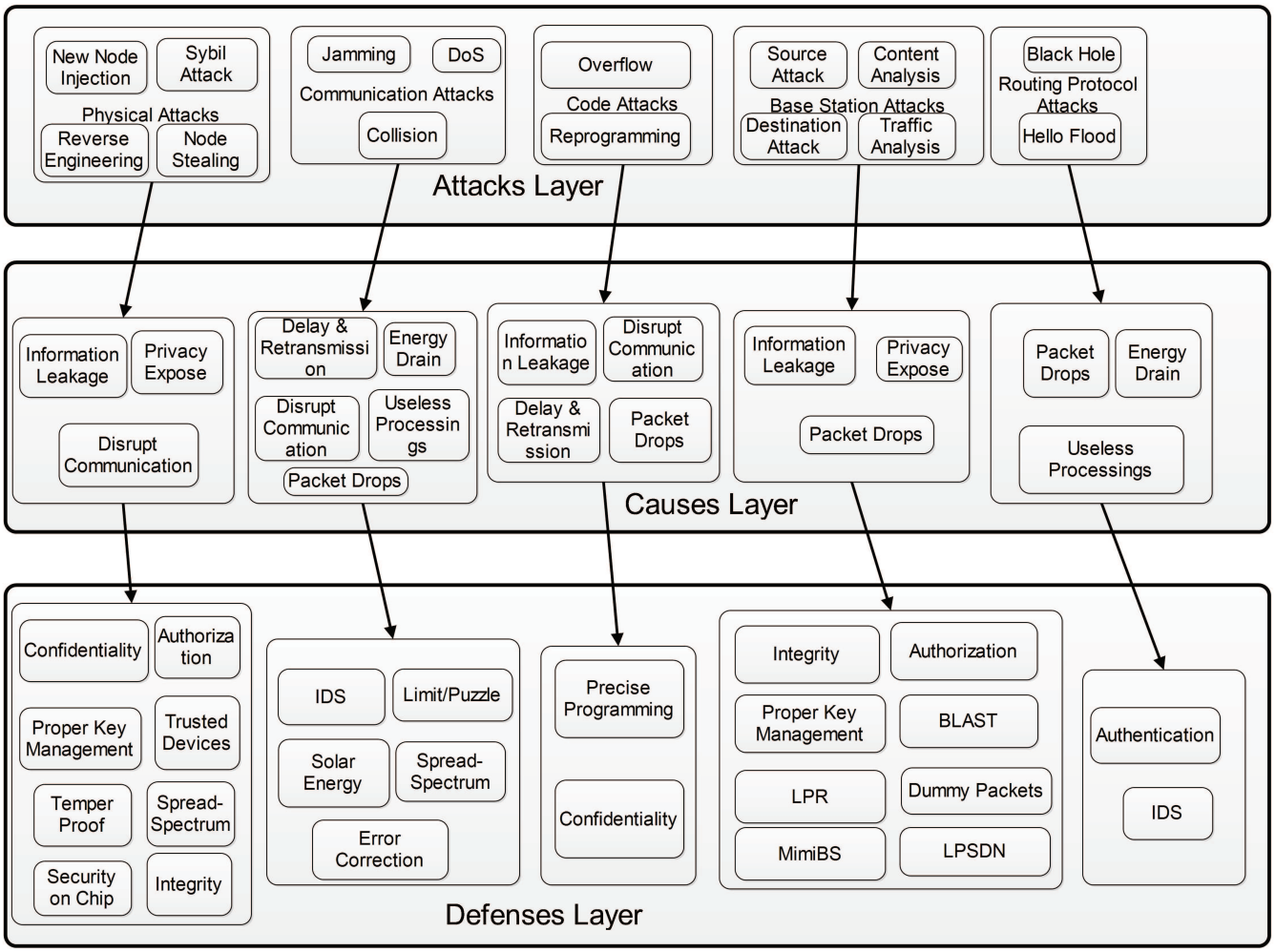

Fig. 6: Taxonomy of Different WSNs Attacks, Causes and Their Defenses: The upper layer consists of WSN attacks, and their causes are presented in second layer; defenses are shown in the bottom layer. Arrows represent attack's relation with causes and defenses. For example, Node injection attack causes information leakage, and privacy-expose; and the solution is provided via authorization, key management, and security on chips.

privacy/secrecy, and to prove the unaltered data. Confidentiality provides content privacy by encryption-mechanism–translation of data into secret code so that only authorized users can access it. When nodes are communicating with each other, the flow of data is encrypted in the network; a bad guy cannot extract information from the intercepted message. Care must be taken to apply energy-efficient encryption techniques in resource constraint devices.

2) Integrity: It ensures the validity of data and node [17]. An attacker captures a packet and changes its contents; he replays those packets. In addition, a malicious node may add some fragments or manipulate the data within a packet. Integrity differentiates between the true data and modified data; it validates the true data, and identifies the intercepted changes in it. Integrity provides solutions to node injection attack and data fabrication attack.
3) Authentication: Authentication is used to truly identify the node in a sensor network [17]. An adversary can inject his node if no authentication is incorporated. For node injection attack, the attacker must authenticate his node to the network; authentication prevents malicious node injection. It prevents outside nodes to be the part of a deployed network. Authentication-techniques for WSNs must be well-designed and should address the resource constraint nature. New node injection and tempering attack can be prevented by authentication.
4) Authorization: Real nodes in a WSNs are entitled to access rights; rights range from accessing node's data to modification of data, etc. Authorization always comes after authentication; therefor, strong authentication reduces attacks related to authorization. If authorization is not implied in the deployed network, an adversary's node can access useful data from any node. Authorization prevents data fabrication or modification attack.
5) Replay and Alteration: Communication in WSNs yields useful data: routing information, sensitive data, patients' records. Packets carry information, e.g., destination and sender node address. These messages, when exchanged, carry information about payload/routing in packets; an adversary can monitor it, and intercept it. At later stages, he alters or replays messages, which leads to false messages or misroute the information. Integrity and encryption prevent attacks in these sit-

uations. Encryption provides contents privacy, while integrity validates the received messages. Techniques to counter this attack are MAC, and time stamping [39]. In case of a shared key, data freshness must be ensured to prevent replay attacks.

6) Proper Key Management: Key management is used to identify the legal node in WSNs; it plays an important role in determining the security performance, and system operations. Secure and efficient key distribution system provides a simple key establishment for a large-scale sensor networks [40]. Key-management helps to counter new node injection attack.
7) Digital Certificates and Digital Signatures: Digital signature, and digital certificates prevent non-repudiation. Digital certificates assert the digital origin of the data; digital origin of the sensor node verifies that the signed data can be trusted by all sensor nodes.

B. Defenses for Wireless Link

The open nature of a wireless media (signal) is a big hurdle to provide an efficient security mechanism. Wireless signals are all around a device; it is impossible to prevent signals' propagation. Noise can affect the signal strength; it is advised to deploy WSNs in a non-susceptible noise area.

1) Defense Against Jamming: Jamming attack directly affects the physical layer of WSN protocol architecture. Variations of spread-spectrum communication [41], e.g., frequency hopping and code spreading can guard against jamming attacks. Communication protocols must be well designed to cope with jamming attack [42]. However, because of the low power and low processing capabilities, WSNs are only limited to using single frequency, and, thus, susceptible to jamming attacks. Building a secured information sensitive environment can prevent an attacker to access the place and install devices to block communication.
2) Defense Against Collision Attack: An enemy can exploit the inherited nature of wireless media–open nature. Authors [33] proposed a new scheme to detect a collision attack through histograms study at the sender side. A proper physical secure environment can prevent this problem; however, for hostile environment, error correction code is used [43].

C. Defense for Availability

WSNs must be available all the times; proper techniques should be incorporated to ensure availability; it can be best ensured by proper and thorough maintaining all sensor nodes' energy and their sub-units. Authors in [44] proposed a battery-aware multiple route constructions with path-overlap avoidance method to provide a prolonged network life. Availability is the performance measure for any network/system, and it dictates the uptime of that network/system. For mission critical system, availability must be high compared to non-critical system; there should not be an energy drain issue. Information must be available whenever needed. Different techniques to support network availability are: providing redundancy for backup and failure, efficient energy aware routing protocols, emergency power backup, and guarding against malicious actions such as denial-of-service (DOS) attacks.

1) Defense Against Node Stealing Attack: Proper physical security measures can protect WSNs environment from outside attacks. Most of the times, attacks are not predicted; a situation can arise where an adversary can steal a node physically. When an enemy steals a node, a tempered proof property ensures node protection–as soon as adversary opens the sensor node's hardware, the internal logic of a node must be useless [41]–; however, due to its high cost, it is not practical. It depends on the situation, whether it is needed or not.
2) Defense against Exhaustion: Repeated-packet transmission to a node drains energy quickly [41]; consequently, leads to un-availability. A technique is suggested to watch the maximum number of requests not exceeding a threshold. When any node crossed the threshold value in the specific time interval, those nodes will not entertain further packets.
3) Solar Energy to Maintain Power/Generate Power: Renewable energy always provides socio-economic benefits. The use of renewable energy decreases power outage issue; however, it adds an extra design cost. Running the network for a long time, solar-energy feature is an added value [45]; it is free and come with the only capital cost at first.
4) Redundancy: In WSNs, predicting the future events are not 100% accurate. In most cases, it is unknown in advance which node will get down (power failure, hardware failure, software failure). To counter this, redundant nodes are deployed; if any node fails, it will not affect the network communication. Redundancy incurs an extra cost of more nodes; however, it supports the system availability. In a hop by hop communication, e.g., one node works as a bridge for two other nodes; if the bridge node fails, communication will be interrupted. Furthermore, network protocols should identify failed neighbors in a real time and adjust according to the updated topology [24].
5) Defense Against Black Hole Attack: Proper key management, and authentication can protect black hole attack; the adversary's node will be unable to authenticate itself.
6) Defense Against Sybil Attack: Trust certification is a tool to prevent multiple identities for a single node; however, it uses up a large amount of resources–a big bottleneck over the network traffic. Verification system can block the outsider node to be the part of a system/network. In addition, trusted devices, similar to trusted certification, associate special identities with each device, that prevent any non-associated node to be added to system/network. Sybil attack can exploit node's redundancy used for reliability. Proper authentication can prevent Sybil attack [41].
7) Defense Against Flooding, Hello Flood Attack: WSN must be well-engineered to counter flood attacks [17] and DoS attacks [18]. In addition, it is desired to figure out which node utilizes more energy; such identification eases the troubleshooting process. Flooding can be prevented by the cryptography principle–authentication. If a node receives any packets,

the receiver must authenticate the packet before giving a reply to the sender. Another solution is to solve a puzzle; when a node receives too many packets from other nodes, it challenges a puzzle to that node; the puzzle is some pre-defined problem–only the legal nodes can interpret it. In case of failure, nodes will entertain future generated packets from that node anylonger.

8) Defense for Data Backup: It is a good habit to have the backup of all useful data. If data is compromised, at later stages, it will rescue the operations immediately.

D. Application Level Defense

Implementing Intrusion Detection System (IDS) or Firewall (FW) in WSNs is not like implementing it in LAN or WAN; these resource-intensive applications need greater deployment considerations. For the resource constraints device, code must be compact. Application level security focuses on software and hardware.

1) IDS: Providing more Security beyond Cryptography: IDS is a full fledge system aimed to provide detection of malicious behavior in a network—traffic pattern. Attackers may intrude into the network and steal useful data. Intrusion detection system can be employed in WSNs to provide maximum security. Only cryptography cannot provide all the solution for all security issues; there must be an IDS to know the current state of a network, and detect and prevent any anomaly [46].
2) Defense against Buffer over Flow Attack: An attacker tries to find any vulnerability in the software code to exploit it; buffer overflow is the solid example. He exploits overflow vulnerability by bombarding many packets beyond the buffer capacity. This attack can be prevented by proper programming code, precise programming practices, and the proper use of data type initialization.
3) Defense for Code Attacks: Cryptography and strong deployed infrastructure prevent direct attacks. It is necessary to consider all well standard methods to write a code–test it accordingly, and deploy it in the enterprise. Code security can be implemented by software engineering principles; software development life cycle (SDLC) must be incorporated. Installing and deploying software for WSNs, detailed security code analysis, and reviews must be done to provide better and controlled code security.
4) Security via Security on Chip (SoC): Providing security in software systems demands high processing capabilities and memory usages. Security in software systems reduces the repetition of the hardwired key burning process (process that involves connecting circuits permanently). However, it brings disadvantages of demanding processing capabilities—WSN lacks it. The solution is to embed the security key at manufacturing process; hardware embedded security is faster than software defined security. Cryptography key is preinstalled on sensor chips; it prevents the key management overhead, and reduces the risk associated with it.

E. Defenses against Eavesdropping

Eavesdropping is secretly listening to other conversations without their consent. In WSNs, when information is exchanged among nodes, any malicious user can monitor those signals. As wireless media is open, an adversary can monitor the communication easily; he can analyze the traffic density for base station attack; he can analyze the packet contents to know about the exchanged information; and he can also analyze the path followed by packet to know about the sender or receiver location.

1) Defense against Traffic Analysis/Tracing and Contents Analysis Attack: Traffic analysis attack can be prevented by introducing fake packets generation techniques as discussed by [47], [6], [37]. Techniques to counter traffic analysis attack are generating fake packets, and creating fake hotspot locations (hotspots are those locations where traffic density is more than other locations). The drawback of fake packets is more overhead and extra energy. To guard against traffic tracing and content analysis attack, strong cryptography techniques, e.g., encryption is used. If an attacker traces some particular packets, he cannot read its contents—contents privacy. A random fake packet creation can also prevent tracing attack.
2) Defense against Base Station Attack:
Securing location information plays an important role in WSN; it guarantees that no one knows the exact location of a node. A recent attempt is done by [6], [37]; they provided base station anonymity via aggregator node integration and fine-tuning TTL value (MimiBS), and through software-defined way (LPSDN).

VII. Challenges for Wireless Sensor Networks

WSNs application's diameter poses many challenges; used in many sectors as discussed in Section III, WSNs should address performance, scalability, reliability, cloud computing, SDN integration, and virtualization.

A. Strong Routing Protocols

A strong routing protocol can protect the network from malicious activities. Traditional matured routing protocol (TCP/IP, BGBP, OSPF, and ISIS) cannot be used in WSNs resource constraint environment. WSN must have the richest set of different protocols to carryout application requirements; a WSN protocol must handle a hostile environment. Routing protocol should provide a high throughput, and a decrease packet loss ratio. Routing algorithm should handle mobility and dynamic changing behavior in WSNs [48]. Unreliable wireless media can drop packets; routing protocols should prevent packet loss. Designing a new routing protocol for WSN should consider security and privacy issues.

1) Node's Mobility: A strong routing protocol must handle nodes' mobility–mobility of source and sink node; sink mobility is used to collect data from all sensors. A static sink node collects data from all sensors without changing its constant position. A mobile sink node has its own effects on the network, e.g., performance and dynamic change behavior. An adaptive routing scheme has been presented in [25]. Routing protocols

must provide better connectivity, an efficient energy consumption, a controlled flooding mechanism, utility based fair usage, and on demand swarm intelligence [25]. Routing protocol must have good topology management scheme to handle any failure; topology can be managed by node adaption, link adaption, and through mobility [25].

2) Trust Relations: Authors in [49], and [50] have introduced a new way for building a strong routing protocol; establishing a trust relation among nodes can minimize the cryptography overhead. The higher is the rate of trust, the lower will be cryptographic key usage; this technique preserves more energy and provides better network performance. For resource constraint devices, routing protocol must be designed according to the application requirement: it should balance processing, memory, and energy for an efficient operation.
3) Base Station Location Privacy: Research community [7], [51], [52], [53] [54], [47], and [6], [37] has already done an extensive work to protect base station location privacy from malicious users. All these methods use fake packets to hide base station location privacy; fake packets consume extra energy. The main challenge is to hide base station location without fake packets.

B. Wireless Media Challenges

Wireless signals are open; they are easy to monitor compared to wired signals; an attacker exploits the open nature of wireless media. Ad-hoc infrastructure reduces the capital expenditure (CapEx) and operational expenditure (OpEx); however, ad-hoc infrastructure needs to address maintenance, management, and security. Ad-hoc infrastructure provides: enhanced-mobility, productivity, deployment, expandability, convenience, low-cost, and remote access control; however, it faces problems of: security, reliability, range, and speed. World Health Organization (WHO) says excessive exposure to wireless signals has an adverse health effect. According to SANS organization, all forms of networking and transmitting data come with security vulnerability—wireless media is the most compromised among them.

Another key challenge is to cope with the dynamics of environment [25]. On the average, node's mobility in WSNs is lower than other ad-hoc networks, e.g., Mobile Ad-Hoc Networks (MANETs), and Vehicular Ad-Hoc Networks (VANETs). For some WSNs, productivity, convenience, and enhanced mobility are not important; however, reliability, deployment, scalability, security, and cost are driving factors.

1) Coverage problem: Coverage is an important performance metric in WSNs; it reflects how well the environment is monitored [55]. The surrounding vicinity should be monitored all times to collect data; a dead nod cannot forward any packets; consequently, it degrades network services; connectivity should be ensured for communication. A network wide coverage area demonstrates Quality of Service (QoS) for specific geographical location. Coverage spans over the entire life of WSNs–at the initial placement time, and operational time. It ought to be guaranteed that all sensor nodes must report to base station.
   Coverage is well defined for a uniform distributed deployment. Nodes dropped from air faces the coverage problem; different coverage models, e.g., Boolean Sector Coverage Model, Boolean Disk Coverage Model, Attenuated Disk Coverage Model, Truncated Attenuated Disk Model, Detection Coverage Model, and Estimation Coverage Model are explained in [55]. This problem also occurs when the network runs in an energy-saving mode; in this mode, some nodes save energy for future use. The real question, what will happen, if at this time, some useful event occurs? Network misses this event at all; the issue should be addressed.
2) Quality of Service: QoS is the function of its application; proper congestion control provides better QoS. In WSNs, there is a minimum chance of congestion outside the base station area. Congestion near the base station results into: channel occupancy, buffer overflow, packet collision, channel contention, high data rate, and minimum node's life. For better services, minimum congestion in the network is necessary. Congestion avoidance ensures high throughput, better link utilization, minimum delay, energy efficiency, and minimum data rate error [56]. Control packets are used to prevent congestion. Different QoS parameters are: reliability, better data rate/sufficient bandwidth, strong wireless signals, better coverage area, minimum delay, collision avoidance, and minimum packet loss. An extensive survey can be found about different congestion control protocols at [56].
3) Unattended Operations: Controlling a massive amount of distributed sensor nodes—with unattended operations—is a big challenge. OTA programming facilitates adding any module on-line to the node [29]. Unattended operations need extra care in a hostile environment, e.g., military, monitoring, and controlling application. In unattended WSNs, a mobile sink node provides dynamic authentication. Authors [50] have shown the collaborative authentication scheme for mobile sink to authenticate data; however, this scheme did not discuss how to deal with other problems, e.g., node failure and OTA.

C. Application Challenges

Deploying WSNs in a hostile environment (where we are fully dependent on nature) is a big challenge. Weather condition, e.g., rain, snow-fall, cold, and hot can affect the performance and life of WSNs. Humidity can destroy a node; rain-drop may corrupt the whole WSNs security on chip services. There is no security scheme that is 100% secure; it needs innovations. In case of non-repudiation, experts warn that a digital signature alone cannot be used to prevent non-repudiation.

1) Intrusion Detection System Integration: Nodes send special IDS messages to IDS server [57]; this IDS message brings an extra overhead in the network: it can drain energy; it also utilizes nodes' resources. Another work is done by [58]; they claimed their system could handle unknown attacks based on the anomalies' behavior. They have assumed majority of neighbor nodes are honest to the base station—this assumption is not true in practical applications.

IDS integration in WSNs brings extra cost of data rate and packet overhead. Authors [46] claimed that their system provides an energy-efficient IDS system to detect and prevent anomalies. IDS solution should not drain the power; better IDS integration must not decrease the overall network life; however, IDS brings delay to network. Authors [59] have shown the effects of IDS on the life of WSNs. An increased number of nodes consume more energy in an IDS integrated sensor network. For maximum security, IDS solutions should be incorporated.

2) Sensor Classification: Different vendors' equipment use vendor's specific firmware. Integrating heterogeneous nodes lead to the proprietary firmwares compatibility problem. Different applications use different sensor nodes; agricultural sensor nodes are different from medical or health care systems nodes. These different classifications bring challenges of: scalability, maintainability, integration, synchronization, and cost.
3) Long Distance Wireless Sensor Networks: Simulation results have shown that long distance WSNs are possible [60]. Such networks will be very useful for long-distance communication. Farming, agriculture, and monitoring the water quality are some applications for long distance WSNs. A typical WSN supports 100 meters range communication [60]. Authors [60] have simulated the link quality; for this purpose, objects are placed in line of sight with interference-free environment. They claimed that only lower frequencies delivered long-distance communication, e.g., 868 MHz and 900 MHz; 2.4 GHz is only feasible for short-distance communication. They supported their claim by practical experiments and claimed that link margin must be greater than 10 dB to achieve 1239-meter-long distance communication. Only 1239 meters distance is shown in their experiments. Further research is needed to increase the distance range at some other frequencies. Long-distance communication should address power consumption, link quality, routing protocol, and security measures.
4) Programming Wireless Sensor Networks: Programming a large network of highly resource-constraint devices that are self-organized and globally consistent, with a robust behavior and a dynamically changing environment, is a big challenge. Programming in a hostile or un-secure environment, to monitor the surroundings, is a daunting task. Programming WSNs must be equipped with proper software engineering principles; it must be well coded, tested, debugged, and should provide a flawed free design. An easy domain-specific language for WSNs application description is introduced by [58]; they claimed their designed language help those novice programmers who lack good programming skills.
   According to the best of our knowledge, a comprehensive survey about WSN programming can be found at [1]. Authors have clearly mentioned state of the art programming concepts, trends, and challenges. They have shown different programming approaches, e.g., code snap shots. When updating only a small portion of a sensor node, it requires only few joules of energy and minimum management overhead. However, reconfiguration of a wireless sensor node is not like a general hardware. There must be a way of re-configuration of small changes or full image installation. Authors [61] introduced how to re-configure, re-install, or update a very small portion of a sensor node code; this leads to save more energy.
5) Wireless Sensor Networks and Market Gap: WSNs are used in different applications as discussed in Section III; however, there is still a market gap while adapting WSNs. All hard works made by labs, industries, and researchers seem not being enough to get WSNs out of its resource constraint environment. WSN still needs time to populate in a dense market. This gap is caused because of the poor integration of different technologies. To decrease the market gap, better application platform is needed. Work done in class rooms or in labs do not grow in scale, and are not economical. Some materials for this section are added from [62].
   Different hardware vendors, e.g., sensor and wireless modules manufacturers need proper coordination and integration mechanism. Software developers also pose the gap cause. Different code writers, algorithm designers, developer, and system integrators all pose significant gap, while adapting WSNs. WSN demands are *plug and play*. These plug and play nodes need to be self-aware, auto-configurable, and auto-diagnosable. To reduce the communication overhead and enhance reliability, these WSNs must store data locally. Building a universal framework to integrate all these different applications, the ecosystem will facilitate improving efficiency, performance, scalability, and interoperability.

D. Key Management and New Paradigm Challenges

Key management and distribution [40] is the most important challenge. A centralized base station having maximum capability (computation) can be used; however, it raises communication overhead issue when nodes try to authenticate themselves. Symmetric key cryptography, and asymmetric key cryptography are the current research areas for low power sensors. Author [57] has shown secure and efficient key management protocol for WSNs. He adapted asymmetric cryptography. His scheme used only one public key for a sink node, and a single private key is used for all sensor nodes. Although, this scheme simplifies the key management issue by using only one private key; however, if an attacker finds the private key, the whole network will be compromised.

An extensive survey has been done by [59]; they showed a symmetric key management system for WSNs. In a symmetric key cryptography, the key is always shared among the communication nodes/entities. A secret key cryptography used in low power motes faces key distribution issue [41]. Public key cryptography brings computational challenges; it is a trade-off among cryptography, sensor's processing capability, and application requirements.

1) Wireless Sensor Network and Software Defined Networking: A recent challenge for WSNs is to adapt the SDN architecture—the decoupled architecture. In SDN, a central controller called SDN controller is

responsible for managing and controlling the whole network, while implementing routing, load balancing, traffic shaping, traffic engineering, and firewall policy [63]. In the resource constraint environment, SDN integration brings whole new challenges of routing and forwarding.

Merging SDN with WSN eases the management burden, key distribution problem, battery drain issue, limited processing and memory issue, and controlling issue. The introduction of new technology in WSNs brings many advantages; however, new problems of security, key management, load sharing, and existing routing techniques should be re-engineered to work with traditional WSNs.

A very brief and first step in WSN to work with SDN, as claimed by [64], has shown advantages of versatility, flexibility, and easy management; However, traffic between controller and sensor nodes can lead to traffic overhead. Overhead problem mainly occurs because of sharing the same channel for data and control traffic together [65]; this problem reduces the reliability of a control channel. Centralized controller leads to single point of failure; multiple controllers provide backup. Multiple controllers increase management and configuration/installation overhead, and cost. The integration of WSN and SDN raises backward compatibility and interoperability issues to legacy WSNs. WE suggest a centralized management policy WSNs; all devices will be visible to a network administrator via graphical user interface (GUI) or a console. Network operators will see the bird-eye view of the whole network. We strongly encourage industry to step-in integration WSN with SDN.

2) Wireless Sensor Network Virtualization: Virtualized WSN is originated to provide a common platform and architecture for experiments and evaluations while integrating with legacy WSNs [49]. The separation of services and infrastructures introduce new ways of providing different services to the end users. In traditional WSNs, the whole physical sensor network is dedicated to some specific task. In WSN virtualization, some geographical areas are divided into parts: north, and south; different tasks care assigned to different areas. To the best of our knowledge, sensor hardwares are not virtualized yet.
3) Wireless Sensor Network and Cloud Computing: In the era of IT and the Internet of Things (IoT), the distributed connectivity provides different new platforms: cloud computing is the new trend for WSN. These platforms are designed for more general-purpose hardware where computational capacity and memory space is not limited. In case of WSNs, designing and integrating cloud concepts in WSNs must not introduce new issues and negative-impact. A framework of cloud-sensor integration is elaborated by [48]. Data collected from different applications are processed in pub/sub broker, which then served as software application as a service (SaaS). In this framework, end user can see the interested data on a graphical interface; it supports health department, and urban traffic monitoring.

VIII. Conclusion

WSNs are application specific; however, their application spectrum is very broad. To develop a secured environment, we should consider the capacities of resources (memory, processor, and power supply). Encryption provides privacy; however, it consumes more energy. Experimental results show that the encryption algorithms using 64-bit keys for data privacy can be broken in 3.5 months with super computers, which can process 10^{12} passwords in one second. This value is $5.4 * 10^{18}$ years for the one using $128 - bit$ encryption algorithms [15]. It is an open challenge, whether to use such a big key in resource constrained sensor nodes or not. Security may not be important in some situation (e.g., monitoring animals); however, it is the top priority in military and information sensitive environment.

Increasing demand in sensor network promising applications is emerging. Better techniques are needed for security, privacy, power, computational-capability, and scalability. Full-fledged WSN system that covers all security requirements, e.g., data privacy, data integrity, data freshness, identity authentication, and availability, is the demanded application for industries and organizations. A versatile WSN architecture should address: security requirements, QoS, attacks, and encryption algorithms. Software defined networking integration in WSN is reshaping the whole architecture of legacy WSN. Benefits and challenges of cloud services and virtualization technology also need attention. We believe, reading and understanding, this paper provides a comprehensive one place exploration for WSN and its related knowledge.

Acknowledgments

We are indebted to the anonymous reviewers whose insightful-comments, suggestions, and directions noticeably improved the quality of the paper.

References

[1] L. Mottola and G. P. Picco, "Programming wireless sensor networks: Fundamental concepts and state of the art," *ACM Computing Surveys (CSUR)*, vol. 43, no. 3, pp. 19:1–19:51, 2011.

[2] M. Hammoudeh, "Putting the lab on the map: A wireless sensor network system for border security and surveillance," in *Proceedings of the International Conference on Internet of Things and Cloud Computing*, ser. ICC '16, New York, NY, USA, 2016, pp. 4:1–4:1.

[3] J. Wang, Y. Yonamine, E. Kodama, and T. Takata, "Supporting user communication in disaster-hit area using mobile ad hoc networks," *IAENG International Journal of Computer Science*, vol. 42, no. 2, pp. 152–159, 2015.

[4] J. Lopez, "Unleashing public-key cryptography in wireless sensor networks," *Journal of Computer Security*, vol. 14, no. 5, pp. 469–482, 2006.

[5] TinyOS.net, "TinyOS," 2015. [Online]. Available: http://tinyos.net/

[6] Y. Bangash, L. Zeng, and D. Feng, "MimiBS: Mimicking base-station to provide location privacy protection in wireless sensor networks," in *Proceedings of the 10th IEEE International Conference on Networking, Architecture and Storage (NAS'15)*, 2015, pp. 158–166.

[7] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," in *Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05).*, 2005, pp. 113–126.

[8] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)*, 2005, pp. 599–608.

[9] A. Bagula, "Applications of wireless sensor networks," 2012. [Online]. Available: http://wireless.ictp.it/wp-content/uploads/2012/02/WSN-Applications.pdf

[10] A. Bounceur, "Cupcarbon: A new platform for designing and simulating smart-city and iot wireless sensor networks (sci-wsn)," in *Proceedings of the International Conference on Internet of Things and Cloud Computing*, ser. ICC '16, New York, NY, USA, 2016, pp. 1:1–1:1.

[11] S. Adhikary, S. Choudhury, and S. Chattopadhyay, "A new routing protocol for wban to enhance energy consumption and network lifetime," in *Proceedings of the 17th International Conference on Distributed Computing and Networking*, ser. ICDCN '16, New York, NY, USA, 2016, pp. 40:1–40:6.

[12] M. Mafuta, M. Zennaro, A. Bagula, G. Ault, H. Gombachika, and T. Chadza, "Successful deployment of a wireless sensor network for precision agriculture in malawi," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, 2013.

[13] A. Bagula, M. Zennaro, G. Inggs, S. Scott, and D. Gascon, "Ubiquitous sensor networking for development (usn4d): An application to pollution monitoring," *Sensors*, vol. 12, no. 1, pp. 391–414, 2012.

[14] G. Liu, R. Tan, R. Zhou, G. Xing, W.-Z. Song, and J. M. Lees, "Volcanic earthquake timing using wireless sensor networks," in *Proceedings of the 12th International Conference on Information Processing in Sensor Networks*, ser. IPSN '13, New York, NY, USA, 2013, pp. 91–102.

[15] M. Dener, "Security analysis in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 10, 2014.

[16] C. V. Samundre and P. A. D. Bijwe, "LEDS - an innovative corridor of data security in WSN," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 3, no. 2, pp. 707–711, 2015.

[17] V. C. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in wireless sensor networks: Research article," *Wireless Communications and Mobile Computing*, vol. 8, no. 1, pp. 1–24, 2008.

[18] A. Singla and R. Sachdeva, "Review on security issues and attacks in wireless sensor networks," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 4, pp. 529–534, 2013.

[19] J. M. Kizza, *Guide to computer network security*, 3rd ed. Springer, 2015.

[20] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," in *Proceedings of the Security in Distributed, Grid, Mobile, and Pervasive Computing*. CRC Press, Boca Raton, FL, USA, 2007.

[21] T. Winkler and B. Rinner, "Security and privacy protection in visual sensor networks: A survey," *ACM Computing Surveys (CSUR)*, vol. 47, no. 1, 2014.

[22] W. Min, C. Ruixiang, and H. Shunbin, "A secure data aggregation approach in hierarchical wireless sensor networks," in *Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication*, ser. IMCOM '16, 2016, pp. 89:1–89:7.

[23] S. Saha, R. Das, S. Datta, and S. Neogy, "A cloud security framework for a data centric wsn application," in *Proceedings of the 17th International Conference on Distributed Computing and Networking*, ser. ICDCN '16, New York, NY, USA, 2016, pp. 39:1–39:6.

[24] M. Elleuchi, A. M. Obeid, M. Abid *et al.*, "An efficient secure scheme for wireless sensor networks," in *Proceedings of the 9th International Conference on Security of Information and Networks*, 2016, pp. 129–132.

[25] C. Sengul, A. C. Viana, and A. Ziviani, "A survey of adaptive services to cope with dynamics in wireless self-organizing networks," *ACM Computing Surveys (CSUR)*, vol. 44, no. 4, pp. 23:1–23:35, 2012.

[26] M. Xu, W. Xu, T. Han, and Z. Lin, "Energy-efficient time synchronization in wireless sensor networks via temperature-aware compensation," *ACM Trans. Sen. Netw.*, vol. 12, no. 2, pp. 12:1–12:29, 2016.

[27] M. Sarvghadi and T.-C. Wan, "Overview of time synchronization protocols in wireless sensor networks," in *Proceedings of the 2nd International Conference on Electronic Design (ICED'14)*, 2014, pp. 204–209.

[28] T. V. Chien, H. N. Chan, and T. N. Huu, "A comparative study on operating system for wireless sensor networks," in *Proceedings of the International Conference on Advanced Computer Science and Information System (ICACSIS'11)*, 2011, pp. 73–78.

[29] Y.-S. Chen, M.-T. Sung, S.-H. Fang, and K.-L. Lin, "8051 netisp: Internet-based remote programmable embedded micro-controller system." *Engineering Letters*, vol. 23, no. 1, pp. 1–7, 2015.

[30] C. Rong, S. Eggen, and H. bing Cheng, "A novel intrusion detection algorithm for wireless sensor networks," in *Proceedings of the 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE'11)*, 2011, pp. 1–7.

[31] G. Schoenebeck, A. Snook, and F.-Y. Yu, "Sybil detection using latent network structure," in *Proceedings of the 2016 ACM Conference on Economics and Computation*, ser. EC '16, New York, NY, USA, 2016, pp. 739–756.

[32] D. Mansouri, L. Mokdad, J. Ben-Othman, and M. Ioualalen, "Detecting dos attacks in wsn based on clustering technique," in *Proceedings of the IEEE Conference on Wireless Communications and Networking (WCNC'13)*, 2013, pp. 2214–2219.

[33] F. Alassery, W. K. Ahmed, M. Sarraf, and V. Lawrence, "A low computational complexity statistical discrimination algorithm for collision detection in wireless sensor networks," *IAENG International Journal of Computer Science*, vol. 41, no. 3, pp. 204–211, 2014.

[34] Gartner, "Code security," 2016. [Online]. Available: http://www.gartner.com/technology/home.jsp

[35] A. Kundu and E. Bertino, "A new class of buffer overflow attacks," in *Proceedings of the 31st International Conference on Distributed Computing Systems (ICDCS'11)*, 2011, pp. 730–739.

[36] L. Yao, L. Kang, F. Deng, J. Deng, and G. Wu, "Protecting source-location privacy based on multirings in wireless sensor networks," *Concurrency and Computation: Practice and Experience*, 2013.

[37] Y. Bangash, L. Zeng, S. Deng, and D. Feng, "LPSDN: Sink-node location privacy in wsns via SDN approach," in *Proceedings of the 11th IEEE International Conference on Networking, Architecture and Storage (NAS'16)*, 2016, pp. 1–10.

[38] L. Zhou, C. Wan, J. Huang, B. Pei, and C. Chen, "The location privacy of wireless sensor networks: Attacks and countermeasures," in *Proceedings of the 9th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*, 2014, pp. 64–71.

[39] A. Bhatia, S. H. Talawar, and R. C. Hansdah, "Umac: A universal mac protocol for wireless networks," in *Proceedings of the 6th IBM Collaborative Academia Research Exchange Conference (I-CARE) on I-CARE 2014*, ser. I-CARE 2014, 2014, pp. 8:1–8:4.

[40] A. Laouid, M.-L. Messai, A. Bounceur, R. Euler, A. Dahmani, and A. Tari, "A dynamic and distributed key management scheme for wireless sensor networks," in *Proceedings of the International Conference on Internet of Things and Cloud Computing*, ser. ICC '16, New York, NY, USA, 2016, pp. 70:1–70:6.

[41] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.

[42] M. Klonowski and D. Pajak, "Electing a leader in wireless networks quickly despite jamming," in *Proceedings of the 27th ACM Symposium on Parallelism in Algorithms and Architectures*, ser. SPAA '15, New York, NY, USA, 2015, pp. 304–312.

[43] M. R. Islam, "Error correction codes in wireless sensor network: An energy aware approach," *International Journal of Computer and Information Engineering*, vol. 4, no. 1, pp. 59–64, 2010.

[44] Y. A. Yudo, N. Shigei, and H. Miyajima, "Multiple route construction with path-overlap avoidance for mobile relay on wsn." *Engineering Letters*, vol. 23, no. 4, pp. 299–306, 2015.

[45] T. Wu, Y. Liu, H. Li, C. J. Xue, H. G. Lee, and H. Yang, "Sats: An ultra-low power time synchronization for solar energy harvesting wsns," in *Proceedings of the 2016 International Symposium on Low Power Electronics and Design*, ser. ISLPED '16, New York, NY, USA, 2016, pp. 106–111.

[46] Yassine MALEH, and Abdellah Ezzati, "Lightweight intrusion detection scheme for wireless sensor networks," *IAENG International Journal of Computer Science*, vol. 42, no. 4, pp. 347–354, 2015.

[47] V. Gottumukkala, V. Pandit, H. Li, and D. Agrawal, "Base-station location anonymity and security technique (blast) for wireless sensor networks," in *Proceedings of the International Conference on Communications (ICC'12)*, 2012, pp. 6705–6709.

[48] K. Tripathi, M. Pandey, and S. Verma, "Comparison of reactive and proactive routing protocols for different mobility conditions in wsn," in *Proceedings of the International Conference on Computing, Communication and Security (ICCCS '11)*, 2011, pp. 156–161.

[49] M. Almasri, K. Elleithy, A. Bushang, and R. Alshinina, "Terp: A trusted and energy efficient routing protocol for wireless sensor networks (wsns)," in *Proceedings of the17th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications (DS-RT'13)*, 2013, pp. 207–214.

[50] L. Mengyao, Y. Zhang, and X. Li, "Ring-based security energy-efficient routing protocol for wsn," in *Proceedings of the 26th Chinese Control and Decision Conference (CCDC)*, 2014, pp. 1892–1897.

[51] X. Luo, X. Ji, and M.-S. Park, "Location privacy against traffic analysis attacks in wireless sensor networks," in *Proceedings of the International Conference on Information Science and Applications (ICISA'10)*, 2010, pp. 1–6.

[52] K. Mehta, D. Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper," *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 320–336, 2012.

[53] B. Ying, J. R. Gallardo, D. Makrakis, and H. T. Mouftah, "Concealing of the sink location in wsns by artificially homogenizing traffic intensity," in *Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS'11)*, 2011, pp. 988–993.

[54] Y. Ebrahimi and M. Younis, "Using deceptive packets to increase base-station anonymity in wireless sensor network," in *Proceedings of 7th International Conference on Wireless Communications and Mobile Computing (IWCMC'11)*, 2011, pp. 842–847.

[55] B. Wang, "Coverage problems in sensor networks: A survey," *ACM Computing Surveys (CSUR)*, vol. 43, no. 4, pp. 32:1–32:53, 2011.

[56] R. A. Uthra and S. V. K. Raja, "Qos routing in wireless sensor networks: A survey," *ACM Computing Surveys (CSUR)*, vol. 45, no. 1, pp. 9:1–9:12, 2012.

[57] M. Alshammari and K. Elleithy, "Secure and efficient key management protocol (sekmp) for wireless sensor networks," in *Proceedings of the 10th ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS '14)*, 2014, pp. 253–254.

[58] A. Elsts and L. Selavo, "A user-centric approach to wireless sensor network programming languages," in *Proceedings of the 3rd International Workshop on Software Engineering for Sensor Network Applications (SESENA)*, 2012, pp. 29–30.

[59] S. Bala, G. Sharma, and A. K. Verma, "A survey and taxonomy of symmetric key management schemes for wireless sensor networks," in *Proceedings of the Conference on International Information Technology (CUBE'12)*, 2012, pp. 585–592.

[60] M. Zennaro, A. Bagula, D. Gascon, and A. B. Noveleta, "Long distance wireless sensor networks: Simulation vs reality," in *Proceedings of the 4th ACM Workshop on Networked Systems for Developing Regions*, 2010, pp. 12:1–12:2.

[61] A. Taherkordi, F. Loiret, R. Rouvoy, and F. Eliassen, "Optimizing sensor network reprogramming via in situ reconfigurable components," *ACM Transactions on Sensor Networks*, vol. 9, no. 2, pp. 14:1–14:33, 2013.

[62] A. Borse, "Wsn market gap," 2015. [Online]. Available: http://wireless.ictp.it/wpcontent/uploads/2012/02/WSN-vs-Market2012.pdf

[63] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: Enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.

[64] T. Luo, H.-P. Tan, and T. Quek, "Sensor openflow: Enabling software-defined wireless sensor networks," *IEEE Communications Letters*, vol. 16, no. 11, pp. 1896–1899, 2012.

[65] N. A. Jagadeesan and B. Krishnamachari, "Software-defined networking paradigms in wireless networks: A survey," *ACM Computing Surveys (CSUR)*, vol. 47, no. 2, pp. 27:1–27:11, 2014.

Yawar Abbas Bangash Yawar Abbas Bangash has received BS degree in Software engineering from NWFP University of Engineering And Technology Peshawar, Mardan Campus in 2008. From 2008 to 2012, he has worked in Huawei Organization Pakistan Ltd, Higher Education Commission project (HEC) PERN2, and Baluchistan Education Foundation (BEF) on different positions in the networking sector. In 2014, he got MS degree in Computer Engineering from Wuhan University of Technology, Wuhan, China. Right now, he is a PhD scholar in Wuhan National Laboratory for Optoelectronics (WNLO), Huazhong University of Science and Technology (HUST).

Qamar ud Din Abid Qamar ud Din Abid is a mechanical engineer by profession. After graduation in 2007 from University of Engineering and Technology Peshawar (Pakistan), he served a government organization as a project engineer for almost four years. From the beginning, he was interested in the profession of teaching and therefore, he joined the national university of emerging sciences (Pakistan) as a Lecturer. To build his career as a teacher, he needed to pursue further education and came to China for his higher studies. He completed his Master degree from Wuhan University of Technology and is currently enrolled as a PhD scholar in Huazhong University of Science and Technology, China.

Alshreef Abed Ali A Alshreef Abed has received his master degree from the School of Computer Science and Technology, Wuhan University of Technology, China in 2014. He was a research member at the Center of Excellence in Information Assurance (CoEIA)-King Saud University, Kingdom of Saudi Arabia. Currently, he is a PhD candidate at the School of Computer Science and Technology, Wuhan University of Technology, China. His main research interests include network security, cloud computing, and data mining.

YAHYA E. A. ALSALHI YAHYA E. A. ALSALHI is a Ph.D student in school of computer science, Huazhong University of Science and Technology, Wuhan, Hubei, P.R. china. He has completed M.Sc from the Department of Computer Science in B.A.M.U University, Aurangabad, Maharashtra, India in 2012. His research area includes data and information security, digital image processing, neural networks, quantum computing and algorithm design.