Wireless Pers Commun (2018) 98:2037–2077
https://doi.org/10.1007/s11277-017-4962-0

Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks

Bharat Bhushan[1] · Gadadhar Sahoo[1]

Published online: 8 September 2017

Abstract Advances in hardware manufacturing technology, wireless communications, micro electro-mechanical devices and information processing technologies enabled the development of WSNs. These consist of numerous, low cost, small sensor nodes powered by energy constrained batteries. WSNs have attracted much interest from both industry and academia due to its wide range of applications such as environment monitoring, battlefield awareness, medical healthcare, military investigation and home appliances management. Thus information in sensor network needs to be protected against various attacks. Attackers may employ various security threats making the WSN systems vulnerable and unstable. This paper examines the security threats and vulnerabilities imposed by the distinctive open nature of WSNs. We first summarize the requirements in WSNs that includes both the survivality and security issues. Next, a comprehensive survey of various routing and middleware challenges for wireless networks is presented. Next, paper explores the potential security threats at different protocol layers. Here various security attacks are identified along with their countermeasures that were investigated by different researchers in recent years. We also provide a detailed survey of data aggregation and the energy-efficient routing protocols for WSNS. And finally, few unsolved technical challenges and the future scope for WSN security has been outlined.

Keywords Wireless sensor networks (WSNs) · Security · Survivality · Middleware · MAC protocols · Sybil attack · Wormhole attack · Jamming attack · DoS attack · Security threats · Data aggregation and routing protocol

✉ Bharat Bhushan
bharat_bhushan1989@yahoo.com

Gadadhar Sahoo
gsahoo@bitmesra.ac.in

[1] Department of Computer Science, Birla Institute of Technology, Mesra, Ranchi, Jharkhand, India

1 Introduction

Advances in hardware manufacturing technology, wireless communications, micro electromechanical devices and information processing technologies enabled the development of WSNs [1]. These consist of numerous, low cost, small sensor nodes powered by energy constrained batteries. WSN proves to be a useful network for various applications such as health-care monitoring, environment monitoring, home appliance management, and military investigations [2]. These are even more useful for homeland security and battlefield surveillance scenarios as these can be easily deployed for such applications [3]. Sensor nodes (SNs) are generally static while sometimes mobile nodes can also be deployed based on the application requirements. Base stations (BSs) are introduced in the network which can either be mobile or static. A sensor node monitors the network area after deployment, detect any event of interest and generate a report. These transmit the report to the base station via multi-hop wireless channel. BS processes the report and sends it to the external world through a high quality wired or wireless links. BS serves as gateway between external world and the WSN [4, 5].

In a sensor node, energy consumption has significant impact on WSNs lifetime. Several energy saving technologies are proposed for WSNs such as energy-efficient MAC [6], cycle scheduling, node replacement, energy replenishment, energy harvesting, cycle scheduling and energy balance. The communication in sensor network consumes maximum power, thus an efficient routing protocols are required to balance the energy consumption among sensor nodes [7]. It needs to prolong the WSN lifetime as well as provide means for better data transmission.

With an increase in decentralized distributed system, the malicious behavior presence is no more an exception as it becomes normal. Most designs, in order to counter the malicious behavior assume that only a fraction of SNs are honest. To make WSNs usable for several applications, simple protocols for topology management, security and communications are required. Though security is the foremost issue in WSN, not much work is available for securing a WSN [8]. WSNs have several characteristics that make them vulnerable to various attacks in diverse and hostile environments.

- Sensor nodes in the WSNs are resource constrained. They have limited memory, energy, computing power, bandwidth and communication range.
- Ad hoc deployment of nodes in the sensor network facilitates attackers to launch various kinds of attacks ranging from active interfering to passive eavesdropping.
- WSNs topology is dynamic. It is deployed in hostile environment lacking any fixed infrastructure. Thus continuous surveillance of the network is difficult. Therefore WSN may face several types of attacks.
- Strong security protocols can degrade the applications performance as it costs more resources on SNs. Thus a trade-off must be set between performance and the security. However, attackers can easily break weak security protocols.
- A wireless network channel is open to all. Anyone can participate or monitor the channel communications with a radio configured at similar frequency band. Thus attackers can conveniently break into the WSNs.

In this paper, the security threats and vulnerabilities imposed by the distinctive open nature of WSNs are examined. We first summarize the requirements in WSNs that includes both the survivality and security issues. Next, a comprehensive survey of various routing and middleware challenges for wireless networks is presented. Next, paper explores the potential security threats at different protocol layers. Here various security attacks are identified along with their countermeasures that were investigated by different researchers in recent years. We also provide a detailed survey of data aggregation and the energy-efficient routing protocols for WSNS. And finally, few unsolved technical challenges and the future scope for WSN security has been outlined.

The remainder of the paper is organized as follows. Section 2 presents the security requirements of wireless sensor networks, where the confidentiality, authentication, integrity and secure management services are discussed. It also presents the survivality requirements of WSNs, where the reliability, availability, and energy efficiency is discussed. It also presents the various requirements related attacks. In Sect. 3, we discuss the routing challenges in WSNs. Next, in Sect. 4, middleware's and middleware challenges in WSNs are explored. Various types of MAC protocols are discussed in Sect. 5. Layers and specific attacks in WSNs are explored in Sect. 6. Prominent attacks and countermeasures such as Sybil attack, denial of service attack, wormhole attack, jamming attack, selective forwarding attack and sinkhole attacks in WSNs are explored in Sect. 7. Next, Sect. 8 discusses the various types of data aggregation protocols. Structured, structure-free and hybrid data aggregation protocols are discussed in this section. Section 9 discusses the energy efficient routing protocols in WSNs. various routing protocols for homogeneous and heterogeneous WSNs are explored in this section. Finally, Sect. 10 provides some of the open challenges, summary and future trends in wireless sensor networks security.

2 Requirements in WSNs

The wireless networks require exchanging information among legitimate users. Due to the broadcast nature of wireless medium, this information exchange is vulnerable to attacks. In order to protect wireless transmissions from different types of attacks, there exist two basic requirements in the WSNs: security and survivality requirements for WSNs. The various aspects of these requirements are reviewed in the table below (Table 1).

2.1 Security Requirements for WSNs

There are several security requirements specified for protecting wireless transmissions against attacks such as DoS attack, node compromise attack, eavesdropping attack and so on. The various types of security requirements for WSNs are explored as follows.

2.1.1 *Confidentiality*

This ensures the protection of sensitive information so that unauthorized users do not get access to the sensitive information. Confidentiality protects the disclosure of information in

Table 1 Requirements in WSNs

Requirements in WSN	
Security requirements for WSN	Survivality requirements for WSNs
Confidentiality Authentication Integrity Secure management	Reliability Availability Energy efficiency

the sensor environment when packets are being transferred among the sensor nodes or between a base station and the sensor nodes. This also prevents eavesdropping type of attack. The biggest threat for confidentiality is the existence of compromised nodes as these nodes can be exploited by the attacker to steal critical data such as cryptographic keys. These keys may be used to decrypt the messages and gain sensitive information. The data part of the transmitted packets is encrypted and sometimes the packet header is also encrypted. This is basically to protect the node identities.

2.1.2 Authentication

This technique is for identity verification of the participants and mainly distinguishes malicious users and the legitimate traffic. In case of wireless sensor networks, every base station and the sensor node must have capability to identify whether the received packet is sent by an attacker node or legitimate node. This is because an attacker can trick the legitimate node and force them to accept false data packets. If false data is injected in the sensor network, it may result in unexpected outcome. MAC appended with the message can be used to authenticate the origin of such false information.

2.1.3 Integrity

This prevents the information from being altered during data transmission process in the sensor network. The use of inaccurate or wrong information can lead to disastrous consequences, thus lack of integrity is a serious concern. Some sensor networks applications like healthcare or environmental monitoring relies heavily on the integrity issue thus protection of information being sent in the network from being modified or intercepted is of utmost importance.

2.1.4 Secure Management

Management of multiple components in the entire network is required to handle sensitive information. Secure management at the base station level is required in the wireless sensor networks as the communication from the sensor nodes end at the base station. Several key distribution management techniques are required to establish encryption as well as maintain the routing information. In clustering technique, each node group or cluster consists of large number of nodes, thus secure management is required for secure data exchange.

2.2 Survivality Requirements for WSNs

There are three basic survivality requirements in WSNs: Reliability, Availability and Energy Efficiency. These survivality requirements are described below.

2.2.1 Reliability

Many applications of wireless sensor networks operate in uncontrolled environments thus reliability in the sensor network is an important aspect. Some sensor nodes may cause unwanted problems or may affect the entire network operation if they are subjected to the failure. Reliability deals with the capability of the network to continue its functionality even if few of the nodes fail.

2.2.2 Availability

It enables the information and the services being accessible at any time if required. Denial of service attacks or node compromise may lead to several services being unavailable, which may lead to disastrous consequences for some real time applications. The WSN protocols employed must be robust, so that any outages could be encountered by providing alternate and more secure routes.

2.2.3 Energy Efficiency

WSNs consists of sensor nodes that are mainly battery operated with data processing, computing and communicating components. These batteries have limited life energy thus energy conservation is an important aspect for the sensor networks. The better battery life also enhances both the availability and the reliability related to the sensor networks. The routing protocols used must be energy efficient.

The various requirements related attacks in WSNs can be summarized as below. The table below provides description of attacks in WSNs that can affect different security and survivality requirements of WSNs (Table 2).

3 Routing Challenges in WSNs

Routing in WSN is a challenge mainly because of varying characteristics of mobile ad-hoc networks and sensor networks. Many obstacles influence the performance of routing protocols. The various routing challenges in WSNs that affect the design of efficient routing protocols are described below.

3.1 Node Distribution

Based on their applications, SNs in the WSNs are deployed [9]. There exist two types of deployment strategies namely deterministic and non-deterministic deployment techniques. Sensor nodes are placed manually and the data transmission takes place through the precompiled routes in the case of deterministic deployment approach. Whereas sensor nodes are scattered randomly in non deterministic deployment technique without any pre-computed paths. In the case of non uniform distribution of nodes, routing protocol must be able to perform optimal clustering to increase the energy efficiency of the wireless network and also to solve the connectivity issue.

3.2 Data Reporting Model

Data reporting as well as data sensing in WSNs is application based [10]. There can be three basic types of data reporting models namely query driven, event driven and time driven models. Data monitoring as well as transmission is done periodically after fixed time interval in time driven models. In the case of query or event driven models data is reported only when an event or query is generated by the base station. These models

Table 2 Requirements related attacks in WSNs

Attacks	Description
Data confidentiality and integrity related attacks	
(i) Denial of service on sensing attack (DoSS)	Adversary modifies the data, resulting in falsified readings which may lead to wrong decisions Targets physical layer where the SNs are located
(ii) Node capture attack	Adversary captures the SN physically leading to manipulated or inaccurate readings Attacker may extract the cryptographic keys or the group keys
(iii) Eavesdropping attack [142]	Adversary eavesdrops on the ongoing communication between nodes This leads to leakage of information on cryptography (session key material) or connection (MAC addresses)
Power or energy consumption related attacks	
(i) Denial of sleep attack [143–146]	Adversary drains the limited power supply of the wireless device leading to significantly shortened lifetime of sensor nodes
Bandwidth consumption and service availability related attacks	
(i) Flooding attack [40]	Adversary sends numerous packets to the victim node preventing the entire network from establishing communication
(ii) Jamming attack [40, 41]	Adversary continuously transmits radio signals thereby cuts off connectivity among sensor nodes Authorized users are unable to use a particular frequency channel
(iii) Replay attacks	Adversary copies a packet and the copy is sent repeatedly to the compromised node leading to exhaustion of victim's power supply and thereby degrading the networks performance
(iv) Selective forwarding attack	Compromised node selectively drops relevant packets and forwards irrelevant packets
Routing related attacks [147]	
(i) Routing update attacks [23, 148]	Adversary updates routing information to fabricate the routing table. This may lead to several problems such as partitioned network, messages being dropped after the TTL expires, few nodes isolated from the BS or messages forwarded to unauthorized nodes
(ii) Wormhole attacks [149]	Adversary intercepts the sender's communications, copies data packets, and sends the copy through a wormhole tunnel Poses a threat to geographic location aware routing protocols
(iii) Sinkhole attacks [93–95]	Adversary attracts all SNs to send transmissions through colluding nodes Sinkhole node is made attractive having higher trust level and shorter distance to the base station

Table 2 continued

Attacks	Description
Identity related attacks	
(i) Impersonate attacks [150]	Adversary impersonates other node's identity (either IP address or MAC) to launch attacks
(ii) Sybil attack [23, 26]	Adversary impersonates other nodes identities and creates multiple identities in the network layer Packets being transmitted on the route having fake identities are modified or selectively dropped Threshold-based signature technique is corrupted
Privacy related attacks [151]	
(i) Traffic analysis attack [152, 153]	Adversary tries to gain knowledge of traffic, network and nodes behaviour It includes examining message pattern, message length, and duration for which the message stays in the router Adversary can perversely link two nodes with untrusted connections

influence the performance of routing protocols from route stability and energy consumption point of view.

3.3 Defect Resistance

Environmental interferences, physical damage or insufficient power supply may cause nodes to die out in WSNs. Such nodes that have died or failed must not damage the overall functioning of the wireless sensor networks [11]. In case of node failure or any other interruptions, routing protocols must have capability to generate alternative routes destined towards the base station [12].

3.4 Extensibility and Connectivity

Routing scheme must be capable of dealing with multiple SNs scattered in the sensing region. With an increase in the number of nodes, the routing protocols must be extensible enough to cover the entire range of nodes. The routing protocols must be aware of such change in topology and should be capable of dealing with it.

3.5 Network Dynamics

Sensor nodes in a wireless sensor networks can be either mobile or stationary. Message routing in case of mobile nodes is more challenging than in stationary nodes because of the route stability issues. Routing protocols must take into account the route stability issue for delivering data securely to the mobile nodes.

3.6 Unattended Locations

Sensor nodes after deployment in majority of the applications have no human control. In case of any kind of change in requirements, nodes must reconfigure themselves accordingly. Thus routing protocols according to the requirements of the application, must allow the sensor nodes to be self-configurable.

3.7 Physical Resources

Primary reason behind the limited applications of WSNs is the limited battery supply. Thus a major design issue in protocol designing is energy wastage. Also, the sensor nodes have limited processing capabilities and memory.

4 Middleware

The application areas of wireless sensor networks had increased drastically in the recent past and these includes shipping, pollution monitoring, infrastructure security, disaster prevention and health care monitoring. These applications require several heterogeneous devices like RFID components, high end servers, storage devices, mobile devices, robots and sensors. Many software components developed using several programming models is required for controlling these devices. These software components are non-trivial in nature and consider scalability, security, reliability and usability along with certain other operational issues. To meet the implementation and design issues of WSN, it requires a middleware that may perform some important functions like data aggregation or software installation in an efficient manner [13].

The software infrastructure for stitching together the operating system, sensor network hardware, and the applications is called a WSN middleware. A complete middleware must incorporate runtime environment supporting system services and multiple applications like data aggregation and other management and control policies [14]. It must include secure, efficient and adaptive mechanism for efficient resource utilization to prolong sensor networks lifetime. The complexity of the network is hidden by the WSN middleware by isolating the hardware and communication details from the application [15].

4.1 Middleware Challenges in WSN

The various types of middleware challenges in WSNs are described below.

4.1.1 Hardware Resources

Sensor nodes are tiny devices deployed in large numbers in hostile environments. These have limited resources and energy. Thus the WSN middleware must entertain low power communications by providing mechanisms for efficient use of memory and processor. There are three basic operations performed by the sensor nodes namely data sensing, data processing and data communication. In order to avoid resource exhaustion and to minimize resource utilization, the device components and the radio must be turned off when not needed and should be activated only when the application needs.

4.1.2 Network Topology Changes

Due to device mobility, device failures, interferences, and many other aspects, the network topology changes frequently. If the sensing area and the number of nodes increase, then the network must be flexible enough to facilitate the node integration without degrading network performance. The middleware must also report failure in case any link or node fails. In addition to reporting of failure activity, the middleware must also incorporate automatic corrective measure for continued network operations. Middleware must also support self-maintenance and self-configuration of SNs. To adjust any change in the network topology, the middleware must incorporate adjusting of sleep periods and transmission ranges.

4.1.3 Heterogeneity

In a WSN, links, devices and software components require programming models and other software tools to integrate and utilize them for various applications as these components are heterogeneous in nature. Thus the middleware considered, must bridge the gap between required hardware technology and the applications.

4.1.4 Network Organization

Sensor networks need to deal with processing power, bandwidth and energy resources that change dynamically. Also efficient routing protocols design is required for long running applications to facilitate the running of applications for as long as possible. Since network knowledge is required for proper network operation, middleware must facilitate resource discovery mechanisms. In addition to the entire network topology, the sensor nodes must also know their own location in the sensing environment. Thus a middleware must also be responsible for providing robust sensor operation.

4.1.5 Security

Wireless sensor networks deal with sensitive information as they are deployed for critical applications such as healthcare, military and rescue services. Secure communication, service availability and service execution is of utmost importance in a WSN. Deployment in harsh and hostile environment increases the exposure of WSN to huge number of attacks like eavesdropping, denial of service attacks, node capture and many other threats. Strong access control and authentication policies are required for proper WSN functionality. Strong security mechanisms are not suitable as they consume lots of resources and energy and the sensor nodes are energy and resources constrained. Middleware must incorporate security functions to achieve security principles like authentication, confidentiality, data freshness, integrity and availability.

4.1.6 Quality of Service (QoS)

In wireless sensor networks there are two types of QoS. Firstly, application specific QoS that includes measurement, coverage and deployment of sensor nodes. Secondly, network specific QOS that includes bandwidth, power consumption and other network resources. Middleware's, to maintain QoS, must provide new mechanisms and should adjust itself when application changes. Thus the middleware must incorporate the performance metrics such as throughput, energy consumption and packet delivery ratio.

5 MAC Protocol

For deployment of long term wireless sensor network, MAC plays a vital role in the context of bandwidth utilization and energy consumption. A better MAC protocol ensures energy efficiency for low sensing WSN ranges. There are different MAC protocols proposed with various objectives and each of these MAC protocols account for energy management and also minimize energy wastage of wireless systems. Sensors are energy constrained, as the only source of power for the device is battery and there exists energy limit for the batteries as these batteries are not replaceable or rechargeable. The main objective of designing MAC protocol was to extend networks lifetime by setting an energy efficient routing of information from the SN to sink [6, 16]. Two basic reasons for energy wastage in WSN are:

- Idle listening (listening to an idle channel to get the traffic)
- Collision (if nodes receive more number of packets at the same time then these results in collision)

To remove these energy wastage sources, following energy efficient MAC protocols are considered.

5.1 S-MAC

Sensor MAC involves two different states namely rest and the dynamic state. S-MAC through periodic resting and listening, tackles the problem of energy wastage. When SN is static or not receiving any traffic, MAC will be in rest state thereby decreasing the overall listening time [17]. Moreover, the S-MAC does not require synchronization with the neighbouring nodes.
Advantages:

- Energy wastage is diminished because of the existence of rest state.
- Avoidance of overall related to synchronization of global time.
- Low energy usage under low traffic.

Disadvantage:

- Sleep latency issue.
- Listen and sleep periods diminish the efficiency under variable traffic load.
- Costly long listening interim.

5.2 B-MAC

It is designed for ad hoc system consisting of N sender and one receiver. It implies low power listening technique while using rest/listen cycles. B-MAC is not synced and the rest time varies from each other. While sending information, SNs switches the radio mode and sends a declaration which must be long enough so that the receiving end notices it [18]. Another technique for reduction of energy consumption is CCA (clear channel appraisal). B-MAC requires 4700 bytes of memory instead of 6400 bytes required by the S-MAC.
Advantages:

- Low overhead under ideal network.
- Lesser energy consumption compared to S-MAC.

- Provides higher data rate.

Disadvantages:

- Performance degrades in high traffic.
- Overhearing.

5.3 LWT-MAC

It is an advancement of B-MAC protocol [19]. B-MAC serves for energy consumption under low load only and as the load increases, it results in collision thereby leading to energy wastage. LWT-MAC under low load involves low energy utilization and also has the capacity to counter any immediate increase in the network load. It involves lesser energy wastage than B-MAC [19, 20].
Advantages:

- When network is ideal, involves lesser overhead.

Disadvantages:

- Lesser throughput than other MAC protocols.

5.4 X-MAC

It is a low power MAC protocol where every packet contains the destination address as well as the remaining preambles. A node sends these preambles after a sufficiently long time interval to get back the recipient reaction. Upon receiving an affirmation, sender stops sending the preambles and sends the data promptly. This introduces latency but reduces energy consumption at both the sender and receiver ends.
Advantages:

- Energy efficient.
- Decoupling and ease of rest schedule for transmitter and the receiver.

Disadvantages:

- Data is sometimes transmitted to the receiver by mistake.

5.5 T-MAC

It is a protocol in which rest and non-rest periods are settled. It is an extension of S-MAC protocol where the SN enters the rest period when there is no traffic movement for some time period. This time period is referred to as Tact Time. As compared to S-MAC, it decreases the sensors inactive time. T-MAC under variable load provides better performance.
Advantages:

- Because of resting schedule, it can handle variable burden.
- Adaptive active time

Disadvantages:

- Early sleeping issue causing loss of longer messages.

5.6 U-MAC

It enhances the performance in terms of energy utilization for various sensor systems. It is an enhancement of S-MAC protocol on three fundamental grounds. Firstly, use of different duty cycles. Secondly, it involves resting after transmission. Thirdly, diverse nodes are allocated different duty cycles.
Advantages:

- Enhances energy productivity.
- Enhances end to end latency [21].

Disadvantages:

- Less rest time.

5.7 Spare-MAC

It is TDMA based protocol for data dissemination in wireless sensor networks. It uses scheduling arrangement called reception schedules. It spreads the data allocated to the neighbouring nodes and the RS thereby making the node dynamic with respect to reception schedule of its receiver [22].
Advantages:

- Minimum collision
- Minimum idle listening

Disadvantages:

- High data end to end delay
- Greater delivery overhead

5.8 Z-MAC

The main design motive of Z-MAC is to characterize transmission control. Every node maintains a list of two best neighbors with the help of neighbor revelation method. It does not support global frame utilization and is exceptionally costly in case of frequent topology changes. Z-MAC uses both TDMA and CSMA methods. TDMA enhances the contention resolution and CSMA is the standard MAC plan. The node is given holder's slot in TDMA style or it can have access to different slots using contention based in CDMA style. This lessens the energy utilization and collision. Z-MAC consists of two phases: neighbor revelation phase and neighbor synchronization phase.
Advantages:

- Low collision rate

Disadvantages:

- Involves clock synchronization.

6 Layers and Specific Attacks in WSNs

In this section, a systematic review of security threats encountered in wireless networks is presented. Attacks in WSNs can be classified as either *passive or active attack*. The goal of the attacker in passive attack is to obtain transmitted information passively without being detected. Attackers collect large amount of data and performs data analysis to extract some secret information. In active attack, adversary launches various attacks such as injection, replaying or packet modification by exploiting security holes in the wireless protocol stack. Passive attack is less severe than active attack but at the same time, it is difficult to detect passive attack as attacker is hidden and does not leave any evidence. Attacks in WSNs can also be classified as *external and internal attacks*. In external attack, adversary can launch attacks from outside the network and it has limited impact. Adversary in internal attack gains authorization for network access and cause severe damage by compromising secrets of legitimate nodes or even by deploying attacker nodes.

Every layer in OSI reference model has its own security issues and challenges. Since various layers rely on various protocols, hence exhibits different security vulnerabilities. In the table below, various security threats and their solutions in different OSI layers are summarized (Table 3).

7 Prominent Attacks and Their Countermeasures in WSNs

The most prominent attacks in WSNs such as Sybil attack, denial of service attack, wormhole attack, jamming attack, selective forwarding attack and sinkhole attacks are explored as follows.

7.1 Sybil Attack

This was primarily encountered in peer-to-peer networking context [23]. It was observed as a resource exhaustion attack, and furthermore analyzed in the area of wireless sensor networks [24, 25]. Then the same kind of attack was detected as a serious threat to wireless sensor networks [26]. A malicious node takes on multiple identities illegitimately in the Sybil attack [26], it was also shown that this attack can cause several severe consequences to some applications in WSNs like fair resource allocation, data aggregation and misbehavior detection. Sybil attack pose a very serious threat to routing protocols and also the distributed storage and this has been shown in [23]. Most designs against malicious behavior basically rely on the assumed fact that some nodes in the wireless system are not malicious or honest. This makes the routing protocols vulnerable to Sybil attacks [23], in which an adversary takes on multiple identities and even pretends to be distinct nodes in the system. Such nodes are called Sybil identities or Sybil nodes. Series of negative results was proved in the first investigation into Sybil attacks [23], showing that prevention of Sybil attack is impossible without making certain special assumptions. The adversaries have potentially more resources and power than a general user. Also the puzzles that need human efforts, like CAPTHAs [27], could not prevent the Sybil attack. Another recent research proposal [28], suggests network coordinates usage [29] for identifying whether the multiple identities is of the same user.

A malicious node in Sybil attack claims numerous client identities either by claiming false identities or by impersonating other legal nodes. A Sybil node sometimes send large number of request messages for association to an access point, utilizing randomized MAC

Table 3 Security threats and their solutions in different OSI layers

Layers and specific attacks	Threats	Solutions
1. Physical layer		
(i) Jamming	Adversary interferes with communication radio frequencies of SNs in the sensor network. Adversary randomly selects jamming nodes and applies jamming simultaneously	Different forms of spread spectrum, can be used to prevent jamming. The most widely used spread spectrum for preventing jamming is frequency hopping. Cost involved in this process is high, so not suitable, as SN are power and energy constrained
(ii) Tampering	For reduced cost estimate of the sensor network, nodes are not provided with temper resistant hardware. Thus adversary can physically access the SN and also adversaries can introduce few duplicate SNs in the network	Self-destruction: whenever SN is physically accessed, the nodes vaporize their content and thereby preventing leakage of information Fault-tolerant protocols
(iii) Sybil attack	Adversary compromise any legitimate node and obtains new identities by fabricating or stealing others identities Also called classical attack	Originates in physical layer but can be tackled at higher layers of the stack by fixing the total number of SNs in the sensor network
2. Link layer		
(i) Collision	Adversary includes collision in a small area. The negligible change in packets data portion may lead to checksum error forcing retransmissions	Error correcting codes can be used but it may lead to increased energy consumption as well as complex computation
(ii) Exhaustion	Continuously disturbing the communication leads to continuous retransmissions. This also leads to quick decline in the SNs energy level	If a sensor node transmits same message, and when this count exceeds the threshold value, it assumes itself to be under attack and switches itself to sleep mode
(iii) Interrogation attack	Malicious nodes send request to send (RTS) packets continuously without taking into account the control to send (CTS) reply packets. This floods the targeted nodes network link	Nodes must limit itself to not accept many connections from the same node or identity
(iv) Sybil attack	Data aggregation: Induces negative reinforcements Voting: Attacker may determine the voting outcome	Radio resource testing: this may lead to extra communication overhead
3. Network layer		
(i) Misdirection	Malicious node In the routing path sends packets to falsified direction making the destination unreachable	If the nodes link gets flooded with unwanted information, it may switch itself to sleep mode
(ii) Neglect and Greed	A node in the routing path drops the message or can assign arbitrary priorities to packets passing through them	Use of multipath routing paths
(iii) Black hole attack	Malicious nodes advertise zero cost routes and affect the routing protocols that select the malicious nodes as intermediate node in the routing path	Defended by accepting route reply from legitimate nodes only

Table 3 continued

Layers and specific attacks	Threats	Solutions
(iv) Sybil attack	Adversary can fool the routing protocols giving an impression of existence of multiple paths to the destination. It greatly affects the geographic routing protocols	There is very less effective defense mechanism against such attack in network layer
(v) Wormhole attack [60]	Adversary creates a well-placed wormhole to completely disrupt the routing. Adversary can convince the nodes to be only few hops away from the base station	Check the bi-directionality of the link during the process of path selection
(vi) Altering and Spoofing attack	Adversary can create routing loops, shorten or extend source routes, repel or attract network traffic or may generate falsified error messages	Efficient authentication and encryption mechanism can be employed. Encryption of header may be applied in order to conserve energy. TESLA provides strong authentication
4. Transport layer		
(i) Flooding attack	Adversary continuously transmits connection requests leading to flooding of network link of the target nodes—TCP SYN flood attack	Enabling limited number of connections for any node. The upper limit needs to be fixed
(ii) De-synchronization	This leads to energy wastage of nodes	To authenticate all the exchanged packets, a secure and efficient authentication mechanism must be employed. This enables the end nodes to detect malicious packets

values to influence huge number of clients. Once the Sybil node has occupied an access point channel slots or association slots, the legal clients are denied access. As a special case of denial of service attacks, this Sybil attack severely endangers the network services availability for the wireless systems [25].

For Sybil attack detection two major methods were discussed in [26]. First method was radio resource testing where each node to each of its neighbors, assigns a unique channel and then tests whether their neighbors could communicate with them through the channels assigned to them. Since radio of the sensor platform is not capable of receiving or sending on more than one channel, at the same time, it would be the sign of Sybil attack if there is failure of communication via one channel. The use of ID-based symmetric keys is the other method of Sybil attack detection.

In absence of a trusted central authority defending against the Sybil attack is much harder. But adversary can readily steal the IP addresses. Spammers steal a variety of IP addresses by advertising BGP routes [30].

Defending and detection of Sybil attack: A traditional approach for addressing different network attacks is secret key based encryption and authentication technique. Several key management techniques have been proposed based on probability related key sharing for authentication in wireless sensor networks, [31–34]. The performance was even improved by exploring the location information of SN in wireless sensor networks [35]. To prevent Sybil attacks, the use of pair wise keys was briefly described in [23]. The problem with these key management techniques is that these usually involve a large amount of system overhead with the process of key management, which is sometimes undesirable. The usage of physical layer information to reduce the system overhead has been proposed in wireless sensor networks for security enhancement. Another work focuses on received signal strength (RSS) in [36, 37]. This had certain limitations. Firstly, the monitor network must be deployed in such a way that each client should be measured by varying landmarks. Secondly the RSS information may be spoofed or eavesdropped [38]. To address such type of problems and also to enhance wireless security, the spatial variability in multipath propagation is used. A channel based strategy for detecting Sybil attacks in wireless sensor networks have been proposed in rich scattering environments [39]. It has proposed a cross layered approach for detection of Sybil attack in WSNs.

7.2 Denial of Service Attack

In wireless sensor networks, all the components including software protocols and hardware architecture integrate themselves to perform various tasks cooperatively. The capability of the entire system may degrade if any of the components malfunctions. Due to this the adversary may launch attacks that are capable of bringing down the capability of the entire network leading to denial of service attacks [40]. DoS is a type of active attack where the adversary participates in the network operation like jamming or packet dropping rather than the passive attacks where the adversary performs network operations from outside the network that may include eavesdropping. One of the most prominent techniques to trigger a DoS attack is the use of radio jamming [41]. Random or constant interferences can be affected by adversaries to disrupt the normal communications [41]. It was also identified that using carrier sensing time, signal strength or packet delivery ration (PDR) is not enough for detection of jamming attacks individually. By exploitation of the link layer semantics, even effective and efficient jamming attack could be implemented [42].

An alternative way to launch denial of service attack is to launch protocol defects. Aad et al. [43] presented a particular type of DoS attack and named it a jellyfish, where the relay nodes delay, reorder or periodically drop packets that must be forwarded, leading to congestion control astray. This shows high impact on the throughput. However in this attack all resources are provided one hop flows that increases the capacity of the networks.

A recent survey over 70 internet operations demonstrated DoS attacks to be more evolving and individual attacks to be more sophisticated and stronger [44]. Such attacks are basically aimed at degrading and denying the QoS for legitimate users. To protect resource rich servers, numerous approaches have been proposed [45–48]. These approaches could be classified into three basic criteria's. First, victim based approaches that mitigate the impact of DoS attack through resource multiplication from the victim end [49]. Second is the attacker based defense approaches that protect the victims from the attacker end. Prominent examples that fall in this category are MULTOPS and D-WARD [50, 51]. D-WARD operates between the internet and a private network on a router preventing private network machines from sending corrupted packets. Third is hybrid defense approaches that mitigate the effect of DoS attacks from both the source end and the victim end of attacks. Prominent examples that fall in this category are dynamic en route filtering [52], distributed packet filtering [53], aggregate congestion control [54], and multi power level transmission [55]. The existing DoS defense approaches detect the primary stage of DoS attacks and distinguish between network traffic from a DoS attack and legitimate network traffic. The primary problem in dealing with the DoS attack is the differentiation between network traffic from DoS and the legitimate network traffic.

In [56], McCune et al. have presented the DoS attack in broadcast. They have proposed an algorithm; namely, secure implicit sampling (SIS). Primary goal of SIS focus to increase the chances of attacker detection with raise in splitting of broadcasts. This goal is achieved by acknowledging each broadcast by subset of recipients, where the subset is measured in a way hidden from the adversary. It is tedious to counter against dos attacks as compared to DoS detection. Adversaries have the potential of projecting many different attacks resulting in DoS attacks and thus rectifying every possible attack in never an easy job. Generally we avoid the affected region through establishment of new routes. DoS resistance mechanisms must be addressed during network designing phase thereby reducing the total number of loopholes.

In [57], Deng et al. presented a distinct type of DoS attack named permanent DoS attack (PDoS), where adversary overwhelms SNs, a long distance away by flooding communication path with either injected spurious packets or replayed packets. A solution that used OHCs was proposed to protect end to end communication from PDoS. Every node is configured using OHC, enabling intermediate nodes for PDoS detection and prevention of the propagation of replayed or spurious packets. Here, each packet incorporates a new OHC number. Only if OHC number is new, intermediate node forwards a packet. Use of OHC number prevents adversaries from flooding the path with replayed packets.

In [58], a path identification mechanism was introduced to defend against DDoS attack. Various approaches for protection against DoS attacks are summarized in the table below. The table also summarizes the operations and the percentage of DoS attacks removed by various approaches (Table 4).

7.3 Wormhole Attack

In sensor and ad hoc networks the most severe threat is the wormhole attack. In such attacks the adversary tunnels the packet through out of band or in band channel between two distant locations. Such wormhole tunnels give two distant nodes an illusion that they

Table 4 Approaches against DoS attacks

Approaches for protection against DoS attacks		
Approaches	Percentage of DoS attacks removed	Operations
(i) Victim-based approach		Reduces the impact of DoS attack from the victim end
(ii) Attacker-based approach	MULTOPS [93%] D-WARD [99.4%]	Reduces the impact of DoS attack from the attacker end Typical examples are MULTOPS (Multi-Level Tree for Online Packet Statistics) [50] D-Ward (Dos Network Attack Recognition and Defence) [51] D-WARD operates on router between the internet and a private network. It analyzes incoming traffic and prevents private network machines from sending DoS packets
(iii) Hybrid-based approach	ACC [64%]	It reduces DoS attacks from both the source-end as well as victim-end of attacks Typical examples are Dynamic en-route filtering [52], Distributed packet filtering [53], Multiple power transmission levels [54], ACC (Aggregate Congestion Control) [55].

are very much closer than it actually is to each other. The adversary can manipulate and collect network traffic as the wormhole can bypass and attract huge amount of traffic. Thus adversary can derive these benefits to launch a wide range of attacks such as dropping or delaying relayed packets. These significantly jeopardize a large number of network protocol like localization [59] or routing protocols [60, 61]. The attacker does not possess any valid network identity and is an outsider and can forward the communication stream along the wormholes without directly looking into the packets content. Using such wormhole links, adversary can launch protocol reverse engineering, man-in-middle attacks, cipher breaking, etc. Thus wormhole attacks can pose serious threat to sensor and wireless ad hoc networks. Many corrective measures have been proposed for detection of wormholes in sensor and wireless ad hoc networks. That solution frequently encounters the attacks by exposing the partial symptoms induced by wormholes. Some wormhole preventive approaches include specialized hardware device like GPS [62] or radio transceiver modules [5], or directional antennas [63]. Other approaches are based on some ideal assumptions like incorporation of special guard nodes [64], global tight clock synchronization [60], or attack free environments [65].

Hu et al. [60], presented geographic packet leash in which they determine the possibility of hop by hop by attaching the location information in each packet of the sending nodes and thereby detecting the wormholes. Wang et al. [66], Considered the end to end distance between the destination and the source nodes for wormhole detection. Zhang et al. [62], presented neighborhood authentication scheme that was location based for the detection and locating of wormholes. These methods however needs pre-knowledge of location of the nodes to detect the distance mismatch. Some methods observed time mismatch instead of distance mismatch in packet forwarding. Hu et al. [60], presented temporal packet leash assuming global clock synchronization for wormhole detection. Capkun et al. [5], proposed SECTOR that measures the round trip time of the transmitted packet for detection of extraordinary wormholes. This eliminates clock synchronization but requires special hardware for sending fast messages without involvement of CPU utilization. Some other approaches observed neighborhood mismatch that may cause physical infeasibility. Hu et al. [63], Found infeasible communicating links by adopting directional antennas using the directionality aspect of the communication antennas. Khalil et al. [65], proposed the concept of Liteworp which assumes that there exists a attack free sensor environment before launching of the wormhole attack. Each node in the deployment phase collects its two hop neighbors and by eavesdropping on the non neighboring nodes selects the guard nodes. Some approaches considered graph mismatch in network model graphs under special assumptions. Poovendran et al. [67], to tackle wormholes introduced a graph based framework. The assumption taken in this was under high communication range, there exists, guard nodes for detection of wormholes. Wang et al. [68], presented a graphical visualization of the wormhole presence. By centralized multidimensional scaling they reconstructed the networks layout for wormhole detection. Song et al. [69], observed abnormally high frequency at the wormhole links and thus wormhole links could be identified by comparison with the normal links. Buttyan et al. [70], proposed another statistical approach that focused on increased number of neighbours and reduction in shortest path links which may be caused by wormhole attacks.

Taheri et al. [71], introduced leash with enhanced packet distributor system for reduction in measurement costs for TESLA using TIK protocol. Tran, lee and hung brothers [72], introduced a method in which while transmitting RREQ messages collecting of time frames and RREP packets is also important. Singh and Vaisla [73], presented an improvement of this by switching receptor and sender against manipulating proposal packet and response time rate. Hu and evans [63], presented a method in which the details of the neighbors can be checked by locating antennas by HELLO message locations analysis and neighbor detection by the verifiers.

7.4 Jamming Attack

It can be viewed as a special type of DoS attack. Stankovic and wood [40], presented DoS attack as "an event that eliminates or diminishes a networks capability". Through flooding DoS prevents the normal use of communications in a network. Jammer emits radio frequency signals which are useless or unwanted information for the sensor nodes. This signal may resemble network traffic or may be white noise. The act of directing electromagnetic energy intentionally towards a communication system is called jamming to disrupt signal transmission [74]. WSNs attack that plays with radio frequencies of the nodes is referred to as jamming [8]. The first instance of jamming attack was recorded in the start of twentieth century in the field of military radio telegraphs. The jamming signals consisted of co-channel characters. Russia and Germany were the first to implement jamming. The first jamming activities during wartime were recorded during World War II. It was used to mislead pilots by the ground radio operators by sending false instructions to them. This is considered as deceptive jamming [75].

The most important aspect in jamming technique is the signal to noise ratio. Undesirable change in electromagnetic spectrum is call noise which is recorded by the antenna. For an effective jamming the SNR must be less than unity. There are many types of existing jamming techniques. Firstly, spot jamming, in which the attacker targets single frequency that victim uses with much power to overwrite the original signal. It can be avoided as spot jamming jams only a single frequency, by simply switching to another frequency. Secondly, Sweep jamming, in which the full power of the jammer switches to different frequencies rapidly. This can in quick succession jam multiple frequencies but all of them is not affected by this at the same time. Thirdly, Barrage jamming, in which at the same time range of frequencies could be affected by jamming. As the jammed frequencies range grows, the jamming power gets reduced. There are several countermeasures proposed against the jamming techniques which are explained below.

7.4.1 Frequency Hopping Spread Spectrum

It is a spread spectrum method for radio signal transmission by switching a carrier rapidly among many different frequency channels [76, 77]. It uses a shared algorithm that is known both to receiver and the transmitter. It reduces jamming and the interception of radio transmissions between SN. In FHSS, without leading to interference problems in the same area multiple WSNs can coexist. The overall bandwidth requirement is much more than to transmit the same data with single carrier frequency and this is the major drawback of the use of FHSS.

7.4.2 Direct Sequence Spread Spectrum

It is performed by multiplying the pseudo noise signal and the data being transmitted (RF Carrier). The pseudorandom sequence of 1 and −1 at much higher frequency than original signal is called pseudo noise signal (PN). This replaces Rf signal with wide bandwidth signal, however at the receiving end the noise could be filtered to gain the original data [77, 78].

Table 5 Countermeasures against jamming attacks

Countermeasures against jamming attacks [154]	
(i) FHSS [155]	Uses a shared algorithm that is known both to receiver and the transmitter Overall bandwidth requirement is more
(ii) DSSS	Performed by multiplying the pseudo noise signal and the data being transmitted
(iii) UWBS	Transmitting short pulses on very large frequency band spectrum
(iv) Antenna polarization	If nodes sense interference, they can change the polarization of their antenna
(v) Directional transmission	Provides better resistant to detection, eavesdropping and jamming

7.4.3 Ultra Wide Band Spectrum

It is a modulation technique that relies on transmitting short pulses on very large frequency band spectrum [79]. This makes it difficult for the transmitted signal to be jammed or intercepted and also makes it resistant from effects caused by multipath. Opperman et al. [80], presented low cost and low power deployment of sensor networks. UWB also guarantees prolonged battery lifetime and accurate localisation.

7.4.4 Antenna Polarization

With respect to earths, the orientation of electric field from the radio wave is called antenna polarisation. Antennas physical structure and its orientation determine the polarisation of the antenna. For LOS communications polarization can cause much difference in the quality of the signal as the receiver and the transmitter use the same polarization. Right circular polarization antenna is unable to receive left polarized signals. Hence if the nodes sense inference and they can change the polarization of their antenna then the nodes may defend jamming. Thus antenna polarization plays an important role in defence of jamming [81].

7.4.5 Directional Transmission

Sensor nodes use Omni directional antenna. To improve jamming tolerance, directional antenna is used in WSNs [81]. Directional transmission as compared to Omni directional antenna provides better resistant to detection, eavesdropping and jamming attacks [82–84]. Directional antenna receives or transmits radio waves in only one direction as opposed to Omni directional antenna that does so in all directions. This use of directional antenna increases the transmission power and also reduces interference from other sources. There are two major problems related to directional transmissions. Firstly, they require a sophisticated MAC protocol [85, 86]. Secondly, they involve more complex multipath routing [87, 88].

The various types of countermeasures against jamming attacks are summarized in the table below (Table 5).

7.5 Selective Forwarding Attack

It is a network layer attack in which the malicious node refuses some packets legitimately and drops them [1]. A node acting as a black hole is a simpler form of this attack in which such node drops all the packets that pass through them. However in such type of attack it is possible for the nodes to detect the attack and thereby exclude the adversary from routing.

Thus a complex form of similar attack was launched where the nodes drop packets selectively making it harder to be detected. The most effective selective forwarding attack is when the adversary is explicitly included in the data flow path. Selective forwarding can be implemented in two different ways with respect to the packets being dropped. Firstly, dropping of packets of specified type and secondly, dropping of packets originating or destined for some specified nodes.

Different countermeasures and detection schemes were proposed for counteracting against selective forwarding attacks. These countermeasures are explored as follows.

7.5.1 Detection Using Acknowledgments

Yu and Xaio [89], presented multihop acknowledgement scheme which on obtaining responses from other nodes launches an alarm. Every node that falls in the forwarding path has malicious node detection capability. Intermediate nodes on detecting malicious nodes sends a alarm message to the base station via multihops. There are two detection processes. Firstly, downstream signifies that data transmission towards base station from the source nodes and secondly, upstream that signifies data transmission towards source node from the base station. It involves three types of packets for attack detection namely, acknowledgement packet, report packet and the alarm packet.

7.5.2 Neighbour Node Light Weight Detection

Xin et al. [90], proposed a scheme for selective forwarding detection in which the neighbouring nodes behave as monitoring nodes. The packet drops are monitored by the neighbouring nodes and also the dropped packets are resent by the neighbour nodes.
Advantages:

- Detection of malicious nodes does not involve any traffic overhead.
- Energy utilization is efficient as only one node at a time is active.
- Shared key is not needed between every node thereby reducing the storage overhead.

Disadvantages:

- Probability based routing is not always optimal.
- Requirement of GPS makes them costly.
- Resource utilisation is not efficient.

7.5.3 Multi Data Flow Detection Scheme

Sun et al. [91], proposed a scheme that uses multi flow topologies for detection of selective dropping attacks. In such techniques the entire network is divided into specific data topologies such that nodes in one topology can communicate with only the nodes in that particular topology. Such divisions are done only during the deployment time. Base station by utilizing the location information detects the malicious node.
Advantages:

- Additional software or hardware is not required to detect the attack.
- Results in higher packet delivery ratio.

Table 6 Security threats and countermeasures

Secure routing protocols and countermeasures to attacks

Security threats	Countermeasures
(i) Injection, modification	Enable link layer authentication [1, 156–158]
(ii) Eavesdropping	Enable link layer encryption [1, 156, 157]
(iii) Selective forwarding	Multipath routing [1] Local monitoring [159]
(iv) Node replication	Location-based key [160] Location verification by nodes [161]
(v) Node impersonation	BS authentication [156]
(vi) DoS	Prevent broadcasts from SNs [157]
(vii) Wormhole	Directional antennas [63] Packet leashes [60] Topology checking by servers [68]
(viii) False routing information	Topology checking by base station [157] Authenticated broadcast [1]
(ix) Rushing	ROUTE REQUEST [162]

Disadvantages:

- High network cost.
- Low network lifetime because of multi data transmission.

7.5.4 Detection in Heterogeneous Networks

Brown and Jiang [92], presented heterogeneous sensor network (HSN) model for selective forwarding detection. HSN model consists of two types of sensors. Firstly, H-sensors that is a powerful high-end sensor. Secondly, L-sensors that is numerous low end sensors.

7.6 Sinkhole Attack

In this, the compromised node is made attractive with respect to the routing algorithms. As it is difficult to verify the routing information of the node, sinkholes are difficult to detect and counter. A sinkhole detection technique using network flow information and data inconsistency is discussed in [93]. It determines the suspected nodes and also estimates the attacked area and finally identifies the intruders with the help of network flow graph. Daniel et al. [94] proposed sinkhole detection mechanism using hop-count monitoring and presented an Anomaly Detection System for analysing the hop-counts magnitude in the routing table. Chanatip et al. [95], presented a concept of extra monitor nodes with high antenna gain and RSSI value which will receive the message every time the SN sends a message. Min et al. [96], presented a technique to calculate the CPU utilization difference for each node by monitoring the CPU utilization in a fixed time interval for each node. Using this difference, the base station decides whether a node is legitimate or malicious. For information collection of every node, some routing algorithms make use of mobile agents. These mobile agents communicate with the nodes in the entire network to share information about the malicious nodes and the legitimate nodes such that normal nodes do not send packets to the malicious node [97].

The various security threats and their countermeasures are summarized in the table below (Table 6).

8 Data Aggregation

As the sensor nodes have limited energy and computation capability, the basic method in which the intermediate nodes facilitate the forwarding of sensed information's from the SN to the base stations is not appropriate. Also this method involves computation overhead and increases the energy consumption. For this reason the in-network aggregation is performed that involves combining of partial readings at the intermediate nodes. This reduces the communication overhead as well as the energy consumption of the sensing environment. Many data acquisition systems construct spanning tree with base station serving as the root and perform in-network aggregation [98, 99]. Sum and Count are the most prominent aggregates in the research community. This is because the Sum algorithm can be extended for computing average, statistical moment or statistical deviation. Tree-based aggregation leads to communication loss from nodes or failure in transmissions. To solve this problem, synopsis diffusion, a scalable and robust aggregation framework, was proposed in [100, 101]. This uses ring topology in which a node might have multiple parents and each sensed value is indicated by duplicate bitmap called synopsis. However, there is no provision for security in most of the data aggregation schemes. An attacker might launch several attacks through compromised nodes like jamming, eavesdropping, or message fabrication. Several problems were studied by researchers in the field of data aggregation.

Different data aggregation techniques can be classified into two subdivisions on the basis of security considerations. These subdivisions are explored as follows.

- Data aggregation without security

Tiny aggregation service (TAG) was proposed that uses tree-based aggregation techniques to compute aggregates like Sum and Count. Tree-based aggregation leads to communication loss from nodes or failure in transmissions. To solve these problems, multi-path routing was proposed for forwarding sub aggregates. But, this multi-path routing may sometimes lead to duplicity of sensor readings. To solve this problem, synopsis diffusion, a scalable and robust aggregation framework, was proposed in [100, 101]. This technique is useful for computation of duplicate sensitive aggregates like Sum and Count. These techniques use duplicate-insensitive techniques for aggregates computation in a multi-set.

- Secure data aggregation techniques

Base station is the only point of aggregation in several proposed secure data aggregation algorithms [102, 103]. Next concept proposed a tree based verification technique in which the base station can detect the falsified final aggregated value [104, 105]. Synopsis computation is insensitive to duplicacy. An attack-resilient computation algorithm was designed so that the base station could filter out the false readings that might be sent by some compromised nodes, from the final aggregated value. The first such hierarchical attack-resilient data aggregation algorithm was proposed in [106]. This scheme however works securely only when there is a single compromised node in the entire network. A sampling attack-resilient data aggregation technique was proposed for computation of aggregates like count and sum [107].

Data aggregation protocols can be classified into three basic types namely structured, structure-free and hybrid data aggregation protocols. These protocols are explored as follows.

8.1 Structured Data Aggregation Protocol

LEACH, the first structured protocol for data aggregation. It used CDMA scheme for communication among the cluster heads and the base stations and TDMA for communication among the cluster members and the cluster heads. The structured aggregation protocol is the best choice, if it is to be deployed in a stable environment. This is because there is no need to select cluster head so reduces the energy wastage in doing so. Here in this section some of the protocols that are structured are reviewed.

8.1.1 EECDA: Energy Efficient Clustering Data Aggregation

This protocol was a result of combination of both the routing protocols and the energy efficient techniques for heterogeneous WSNs [108]. This protocol proposed a novel aggregation path and cluster head election approaches. Once CH is elected, selection of aggregation path is based on residual energy level.
Advantages:

- It has longer stability period as compared to other protocols.

Disadvantages:

- It involves high mathematical computation.
- In case of heterogeneous networks, the communication cost increases.

8.1.2 YEAST: dYnamic and scalablE tree Aware of Spatial correlaTion

It is based on the concept of correlation region. This refers to the region where nodes sense the similar kind of information. The representative node that performs aggregation is selected using spatial correlation. The represented nodes elected are dynamically adjusted. To ensure aggregation and sensing accuracy the sensing region is also dynamically adjusted.
Advantage:

- Maximize the aggregation gain.
- Minimize the cost for route discovery.
- It is efficient in terms of communication overhead.

Disadvantage:

- For large and dense WSNs, it increases the complexity of the protocol.

8.1.3 EEBCDA: Energy Efficient and Balanced Cluster-based Data Aggregation Algorithm

It overcomes the unbalanced energy issues and the network is fragmented into unequal sized rectangular grids. The cluster head is elected based on residual energy level and it keeps moving around in each cluster. This ensures energy efficiency in each grid and in turn in the complete network.
Advantage:

- Prolong the lifetime of the network.

- Minimize unbalanced energy dissipation.

Disadvantage:

- Difficult to identify the cluster sizes.

8.1.4 Delay Aware Network Structure for WSN

This was proposed for in-network data fusion in a delay efficient manner [109]. This involves clusters of varying sizes to communicate with the base station in an interleaved manner. To guarantee reduced aggregation delay, it uses a tree based network model. Clusters of varying sizes are designed in a multiple single layered model.
Advantages:

- In case of partially fusible or non fusible data, the delay is minimised.

Disadvantages:

- Static in nature.
- Not suited for fully fusible data.

8.1.5 DMLDA: Dynamic Message List Based Data Aggregation

It is clustering based real time protocol that uses dynamic message list instead of delayed transmission for improvement of aggregation efficiency [110]. Data redundancy is detected immediately so it reduces the delay involved.
Advantages:

- It performs better for large scale WSNs with respect to the filtering ratio.
- It adjusts the length as well as content of the message dynamically.
- Efficient performance for real time applications

Disadvantages:

- With increase in network size, the memory cost increases.
- Extensive memory requirements.

8.2 Structure Free Data Aggregation Protocols

To minimize the communication cost, queuing delay and maintenance overhead, these protocols were proposed for real time applications. The performance of structured protocols is not suited for dynamic scenarios and this lead to development of structure free protocols. Data Aware Any cast and Randomized Waiting (DAARW) Protocol, was the first proposed structure free protocol for data aggregation [111]. In this the nodes send an RTS for one hop neighbour discovery. To make the aggregation efficient, random waiting was considered in DAARW. The network structure maintenance is not required in DAARW making it more efficient and the protocols discussed here are DAARW different variants. Here in this section some of the protocols that are structure free are reviewed.

8.2.1 RAG: Real-time data AGgregation protocol

It uses both the mechanisms, temporal and spatial convergence to achieve data aggregation. This was designed to lower the communication overhead for real-time applications and to enable the WSN to fulfil its mission without causing any loss of sensitive data. Packets are delayed when they are being transmitted to the base station and their lifetime period is enhanced to facilitate the process of data aggregation and make the entire process more efficient.

8.2.2 Ant Colony Algorithm

This performs data aggregation in WSN at the network layer. SNs are assumed as artificial ants for solving optimization problems. The next hop node selection is done dynamically based on the energy estimates of the neighbouring nodes. It improves the WSN performance in terms of networks lifetime and energy [112].
Advantages:

- Prolongs network lifetime
- Energy efficient.

Disadvantages:

- Higher complexity for multi-hop WSNs.

8.2.3 ADA: Attribute aware Data Aggregation scheme

Static routing cannot aggregate data of homogeneous sensors. Thus ADA was proposed for the purpose of aggregating data of homogeneous sensors. It introduces packet attribute concept for identifying the packet type. It uses packet driven algorithm and dynamic routing protocol [113]. Every node maintains a timer for the packets in its queue.
Advantages:

- Energy and delay efficient aggregation of heterogeneous data.

Disadvantages:

- High complexity.

8.2.4 DA-MAC

It is combination of dynamic and robust technique for aggregation of event-triggered data. It is a cross-layer solution that works at the application layer. In order to decide the place and time of data aggregation dynamically, it also retrieves information from the MAC layer. It uses virtual overlay concept that results in minimization of packet losses as in this single packet is forwarded to several nodes. It is asynchronous protocol and relies on preamble transmissions [114].
Advantages:

- Efficient data aggregation protocol for event-driven applications.

Disadvantages:

- Hidden terminal problem.
- Cross-layer communication is complex

8.3 Hybrid Data Aggregation Protocols

It is proposed for performing data aggregation for a huge range of WSN applications with low energy requirements and lower computation overhead. This protocol combines the advantages of both the structure free and structured aggregation mechanisms.

8.3.1 HEAP: Hybrid Energy-efficient Aggregation Protocol

It is designed for various large-scale WSNs applications such as periodic monitoring, event detection and on-demand data transmission. It uses both temporal as well as spatial correlation for data aggregation. The SNs are divided into clusters and each cluster is governed by a cluster-head [115]. If data from all the nodes is to be aggregated then tree structure and static aggregation is used. If only some nodes detect events and data from few nodes only is to be aggregated, it uses dynamic aggregation.

Advantages:

- Energy-efficient aggregation for large scale WSNs.

Disadvantages:

- Not suited for busty data.

A comparison of various data aggregation protocols are reviewed in the table below on the basis of Category, Approach, Discovery and Design objective of these protocols (Table 7).

9 Energy Efficient Routing Protocols in WSNs

There is significant impact of energy consumption on WSNs lifetime. The energy problem of WSN can be countered using several techniques such as energy-efficient MAC [116], cycle scheduling [117], node replacement [118], energy replenishment [119], energy-efficient routing [120], energy balance [121] etc. The maximum power utilized by the SNs is in the process of communication. The communication module involves four states: *idle, sleep, send and receive*. Sending and receiving compromise two-thirds of the entire energy consumption. Thus an efficient protocol is necessary to balance the energy consumption among nodes in the WSN. This may prolong the WSN lifetime and also may improve the data transmission quality. Low Energy Adaptive Cluster Hierarchy (LEACH), an energy efficient cluster-based routing protocol is studied and cited by all the survey papers [2, 122, 123]. It is more secure and scalable as compared with flat routing protocols [124]. It groups nodes into clusters and elects a cluster head for each cluster. It operates in two phases that is set-up and the steady phase. Clusters are formed and CHs are elected in the set-up phase. In the steady phase, the nodes transmit data. The CHs performs aggregation and sends data directly to the BS. Thus for large scale WSNs, it is not suitable. Routing protocols can be classified into two types*: homogeneous and heterogeneous WSNs*. The table provides a review of routing protocols classifications (Table 8).

Table 7 Data aggregation protocols

Comparison of various data aggregation protocols

Protocol	Discovery	Category	Approach	Design objective
EECDA	2011	Structured	CH election Routing path selection	Minimize energy consumption Prolong network lifetime
YEAST	2011	Structured	Scalable and dynamic routing structure	Minimize redundant data transmission
EEBCDA	2012	Structured	CH rotation	Minimize node's energy dissipation
DMLDA	2015	Structured	Inter-leaved node and sink communication	Reduce delay
RAG	2011	Structure-free	Temporal and spatial convergence	Timely data delivery
DAACA	2012	Structure-free	Ant colony algorithm	Minimize energy consumption Prolong network lifetime
ADA	2012	Structure-free	Dynamic routing	Heterogeneous data aggregation
DA-MAC	2013	Structure-free	Cross-layer solution	Combines dynamic and robust aggregation
HEAP	2013	Hybrid	Temporal and spatial correlation	Energy efficient aggregation of data for large scale WSNs

9.1 Homogeneous WSNs

In case of homogeneous WSNs, routing protocols needs to address identical nodes. These can be subdivided as mobile and static ones. These homogeneous WSNs can be classified into static and mobile homogeneous WSNs routing protocols as explored below.

9.1.1 Static Homogeneous WSNs

The various types of static homogeneous WSN routing protocols can be classified as follows.

9.1.1.1 Cross-Layer Routing In contrary to the layered protocols, it facilitates interaction among non-adjacent layers. It provides flexibility along with delivering higher energy efficiency and increased network lifetime.

Hu et al. [125], proposed Joint Routing Power and Random Access (JRPRA) algorithm. Joint optimal design is performed at physical, routing and MAC layers to maximize the network lifetime. It adopts correlated dat gathering method to minimize energy consumption of the network. It adopts link capacity adjusting technique to increase the network lifetime. LMCRTA is introduced in [126]. It is the result of combination of the physical layer, automatic repeat request involved at the data link layer and routing strategies at the network layer. It optimise the network lifetime and decreases the energy consumption. It utilizes CRC as the metric for determining the received signals correctness.

LMCRTA and JRPRA algorithm is compared on several parameters in the table below (Table 9).

Table 8 Routing protocols classification

Routing protocols			
Homogeneous WSNs		Heterogeneous WSNs	
Static	Mobile	Static	Mobile
Opportunistic routing: MORE EEOR [127], EER [128]. Cross-layered routing: JRPRA [125], LMCRTA [126]. Co-operative routing: RBCR [129, 163], EBCR [130].	Mobile sink: Termite-Hill [132]. Mobile source: TARS [131, 164]. Multiple mobile sinks: MobiCluster [134].	Energy heterogeneity: ECDC [136], EEMHR [137], LEMHR [165]. Transmission range and cost heterogeneity: CSLRP [166].	Energy heterogeneity: HARP [140], RAHMoN [141]. Transmission range and cost heterogeneity: HSN [139].

9.1.1.2 Opportunistic Routing (OR) It was proposed to reduce unnecessary retransmissions and solve link problems. It improves transmission reliability and energy efficiency. MAC-Independent OR and Encoding (MORE) protocol is a famous opportunistic routing protocol [127]. These do not consider energy consumption issue.

An Energy-Efficient OR protocol is proposed to reduce energy cost and increase network lifetime [127]. It is a multi-path routing protocol and the Expected Energy Cost is the primary metric. It consists of two power models, namely, adjustable and non-adjustable models. It has better efficiency than MORE in terms of packet delivery loss ratio, energy consumption and throughput.

Energy-Efficient Routing (EER) protocol is proposed in [128]. It was a forwarder self-selection technique during the data delivery phase. During the route discovery phase, greedy forwarding algorithm is used in order to decrease the control message overhead.

EER and EEOR algorithm is compared on several parameters in the table below (Table 10).

9.1.1.3 Co-operative Routing This enables channel fading mitigation, achieving better spectral efficiency and better transmission capacity [4]. It is developed using MIMO techniques to reduce power transmission and extend coverage. It allows multiple nodes to share their resources and antennas.

Table 9 Comparision of cross layer routing protocols

Parameters	LMCRTA [126]	JRPRA [125]
Integrated technology	Cooperative diversity	Correlated data gathering
Congestion control	No	Yes
Assumption	QoS requirement	Lossless transmission
Relay-selection	Residual energy	Total data rate flow
Applications	High quality channel WSN	High stability WSN

Relay Based Co-Operative Routing (RBCR), is introduced in [129]. It considers channel quality as well as consumed energy. It uses minimum cost path technique to model the problem and formulates the problem using multi-objective optimization technique. It utilizes cooperative diversity and selects best optimal path in terms of consumed energy for enhancing energy efficiency. EBCR is introduced in [130], ensures higher energy efficiency. EBCR uses one hop neighborhoods instead of two hop neighborhoods used in RBCR. It determines multiple-relay strategy and the selected neighboring nodes behave as multiple receiving and transmitting antennas. It provides higher throughput but does not consider the fading problem. Thus it is suitable for only those applications that do not consider network reliability.

EBCR and RBCR algorithm is compared on several parameters in the table below (Table 11).

9.1.2 Mobile Homogeneous WSNs

The various types of mobile homogeneous WSN routing protocols can be classified as follows.

9.1.2.1 Mobile Source Chi and Chang introduced Trace-Announcing Routing Scheme (TARS) [131]. These focus on applications that require support of both targets and mobile sinks. It captures the mobile objects path by sending a broadcast of trace-announcing packets. TARS maintain both tracking and routing information tables.

9.1.2.2 Mobile Sink In order to balance the energy consumption of the sensor network and avoids energy hole emergence, Termite-Hill is introduced in [132]. It avoids energy-hole creation in static WSN at nodes near the sink. It is considered as an intelligent algorithm and its performance is evaluated by implementing on WSN hardware and

Table 10 Comparision of opportunistic routing protocols

Parameters	EER [128]	EEOR [127]
Forwarder list generator	Relay-node	Source
Forwarder list selection	Self-selection	Pre-selection
Co-ordination	Back-off time	ACK-based
Applications	Large scale WSNs	Unicast cases
Data communications	No	No

Table 11 Comparision of cooperative routing protocols

Parameters	EBCR [130]	RBCR [129]
Cooperative strategy	Adaptive	Fixed
Relaying node count	Multiple	Single
Scope cooperative relay	One-hop	Two-hop
Relay selection	Residual energy	Channel state
On-line computation	Yes	Yes
Applications	Low SNR-WSN	Better channel quality WSN

stimulating in mobile and static sink scenarios. It achieves higher success rate throughput and energy efficiency with respect to AODV [133].

9.1.2.3 Multiple Mobile Sink An energy-efficient clustering protocol, Mobicluster is introduced in [134]. It deals with "sensor islands" where nodes are immobile. The CHs communicate with "rendezvous nodes" located near sinks trajectory. The selection of such rendezvous nodes reduces the collision and energy consumption along with increased throughput. To increase the network lifetime, rendezvous nodes or CHs can be replaced when the energy level is low.

Mobicluster, TARS and Termite-hill algorithms are compared on several parameters in the table below (Table 12).

9.2 Heterogeneous WSNs

In case of heterogeneous WSNs, routing protocols deals with energy and heterogeneity issues [7, 135]. The heterogeneity can be reflected via computation, energy and links. These heterogeneous WSNs can be classified into static and mobile homogeneous WSNs routing protocols as explored below.

9.2.1 Static Heterogeneous WSN

The various types of static homogeneous WSN routing protocols can be classified as follows.

9.2.1.1 Transmission Range and Cost Heterogeneity To address major design issues of sensor network: sink location, sensor deployment and data routing, CSLRP (Coverage Sink Location and Routing Problem) is proposed for heterogeneous WSNs. All sensors are subdivided into "types" with each ty[pe having different transmission and sensing range. It is suitable for small-sized networks with less than 49 nodes in total. It considers coverage threshold as QoS metric.

9.2.1.2 Energy Heterogeneity For point and area coverage in heterogeneous WSNs, an Energy and Coverage Aware Distributed Clustering (ECDC) protocol is proposed in [136]. It prolongs the sensor network lifetime and divides SN into three categories: cluster member, cluster head and plain nodes. It elects cluster head based on coverage and residual energy. Energy-Efficient Multilevel (EEMHR) protocol is introduced in [137]. It partitions all nodes into two levels. Level 1 consists of normal nodes and level 2 consists of advanced nodes. EEMHR is better than other routing protocols in terms of stability and lifetime

Table 12 Comparision of Mobile homogeneous WSNs routing protocols

Parameters	Mobicluster [181]	TARS [131]	Termite-hill [132]
Mobile elements	Sinks	Targets and sinks	Sinks
Solution methods	Clustering-based	Virtual grid-based	Intelligent algorithm
Moving trajectory	Fixed	Random	Random
Applications	WSN with fixed mobile sinks	Location-aware WSN	WSN with single mobile sink
Speed considered	No	Yes	Yes

[138]. Lifetime Extended Multi-Level (LEMHR) HR protocol is introduced in [137] for EEMHR enhancement. LEMHR doubles the network lifetime if compared with EEMHR.

EEMHR, LEMHR, ECDC and CSLRP algorithms are compared on several parameters in the table below (Table 13).

9.2.2 Mobile Heterogeneous WSNs

The various types of mobile heterogeneous WSN routing protocols can be classified as follows.

9.2.2.1 Data Rate and Transmission Range Heterogeneity A heterogeneous sensor network (HSN) is proposed in [139] with a mobile sink. The nodes are divided into three levels: H-nodes, L-nodes and the sink having infinite energy. H-nodes stand for high energy level nodes and provide higher data rate and longer transmission range than the L-nodes. Simulation results proved it to be more efficient and also there occurs data loss with increase in speed of mobile sink.

9.2.2.2 Energy Heterogeneity Hierarchical Adaptive and Reliable (HARP) protocol was introduced in [140]. It divides nodes into normal nodes and cluster nodes based on their residual energy capacities. Further CH is elected based on residual energy of the SNs. It builds a hierarchical tree with three layers: inter cluster and intra cluster. HARP introduces mobility management and local recovery mechanism to counter the link failures. Routing algorithm for heterogeneous mobile network (RAHMON) was introduced in [141]. It divides all nodes into mobile and static ones. The former can be sink nodes or cluster heads. It works under assumption that all sensor nodes can be a CH. CH election depends on energy, mobility level and distance to the sink.

HSN, HARP and RAHMON algorithms are compared on several parameters in the table below (Table 14).

Table 13 Comparision of static heterogeneous WSNs routing protocols

Parameters	EEMHR [138]	LEMHR [137]	ECDC [136]	CSLRP
Heterogeneity	Energy	Energy	Energy	Cost and transmission range
CH selection	Weighted election probabilities	Weighted election probabilities	Residual energy	–
Inter-clustering routing	Multiple-hop	Multiple-hop	Multiple-hop	–
Intra-clustering routing	Single-hop	Single-hop	Single-hop	–
Cluster sizes	Uneven	Uneven	Even	–
Applications	Vertical energy heterogeneity	Horizontal energy heterogeneity	Uniform or non-uniform node deployment	Varying cost nodes

Table 14 Comparision of mobile heterogeneous WSNs protocols

Parameters	HSN [139]	HARP [140]	RAHMON [141]
Heterogeneity	Energy, data rate and transmission range	Energy	Energy
Mobile elements	Sink	Sinks	CHs and sinks
Node types	H-nodes, L-nodes and sink	CH and normal nodes	Static and mobile nodes
CH selection	Predetermined	Residual energy	Mobility level, energy and sink distance
Data transmission	Single-hop	Multiple-hop	Multiple-hop
Applications	Large scale WSNs	Reliable WSN	Hydropower plants

10 Summary and Future Works

Because of wide range of security-critical applications, security is of utmost concern for WSNs. In this paper, we presented a detailed survey of security challenges as well as defense strategies conceived for protection of confidentiality, authentication, integrity, energy efficiency and availability of transmissions against malicious attacks. Range of wireless security threats and attacks potentially experienced at various protocol layers are discussed in this paper. We have discussed detection and prevention techniques along with countermeasures for some prominent attacks in WSNs such as Sybil attack, DoS attack, wormhole attack, jamming attack, selective forwarding attack and sinkhole attack. The various data aggregation as well as energy efficient routing protocols is reviewed in the context of various widely deployed WSNs.

In this article, general security problems and their corresponding solutions are discussed. However, there are still several open issues. These open challenges that needs to be addressed are detailed below.

- Techniques and new theories needs to be developed for jointly defending mixed wireless attacks in WSNs.
- An efficient transmission technique needs to be developed for enhancing the security performance by joint optimization of reliability, throughput and security.
- Various applications may require varied security requirements and thus effective prevention of attacks at the application layer is required. Thus security resilience needs to be incorporated into the application layer before WSNs deployment.
- A framework for cross-layer security needs to be investigated for wireless security improvement along with reduced latency and security overhead as compared to conventional mechanisms.
- Efficiency of physical layer security techniques needs to be verified and tested in real-time WSN systems even in presence of eavesdropping and jamming attacks.

The WSNs features makes designing security protocols, a challenging task at the same time maintaining low overheads. Hence, security for WSNs is a very fruitful research domain and needs to be explored.

References

1. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. In *Proceedings of 1st IEEE international workshop sensor network protocols and applications (SNPA'03)*.
2. Kumar, A. A. S., Ovsthus, K., & Kristensen, L. M. (2014). An industrial perspective on wireless sensor networks—A survey of requirements, protocols, and challenges. *IEEE Communications Surveys & Tutorials, 16*(3), 1391–1412.
3. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Elsevier Ad Hoc Networks Journal, 1,* 293–315.
4. Nosratinia, A., Hunter, T. E., & Hedayat, A. (2004). Cooperative communication in wireless networks. *IEEE communications Magazine, 42*(10), 74–80.
5. Capkun, S., Buttyan, L., & Hubaux, J.-P. (2003). Sector: Secure tracking of node encounters in multihop wireless networks. In *Proceedings ACM SASN*, pp. 21–32.
6. Ye, W., Heidemann, J., & Estrin, D. (2002). An energy-efficient MAC protocol for wireless sensor networks. *IEEE INFOCOM, 2,* 1567–1576.
7. Tanwar, S., Kumar, N., & Rodrigues, J. J. P. C. (2015). A systematic review on heterogeneous routing protocols for wireless sensor networks. *Journal of Network and Computer Applications, 53,* 39–56.
8. Shi, E., & Perrig, A. (2004). Designing secure sensor networks. *Wireless Communications Magazine, 11*(6), 38–43.
9. Raghunandan, G. H., & Lakshmi, B. N. (2011). A comparative analysis of routing techniques for wireless sensor networks. In *2011 national conference on innovations in emerging technology*.
10. Rashvand, H. F. (2012). Smart sensing architectures. In *Distributed sensor systems practice and applications*.
11. Ye, W., & Yarvis, M. (2004). Tiered architectures in sensor networks. In *Handbook of sensor networks compact wireless and wired sensing systems*.
12. Tilak, S., et al. (2002). A taxonomy of wireless micro sensor network models. *Mobile Computing and Communications Review, 6*(2), 28–36.
13. Hadim, S. (2006). Middleware challenges and approaches for wireless sensor networks. *IEEE Distributed Systems Online, 7,* 1–23.
14. Mohamed, N., & Al-Jaroodi, J. (2011). A survey on service-oriented middleware for wireless sensor networks. *Service Oriented Computing and Applications, 5,* 71–85.
15. Wang, M. M., Cao, J. N., Li, J., & Dasi, S. K. (2008). Middleware for wireless sensor networks: A survey. *Journal of Computer Science and Technology, 23,* 305–326.
16. Charri, L., & Kamoun, L. (2010). Wireless sensors networks MAC protocols analysis. *Journal of Telecommunications, 2,* 42–48.
17. Vikas, & Nand, P. (2015). Contention based energy efficient wireless sensor network—A survey (Vol. 10). In *IEEE international conference on computing, communication and automation (ICCCA2015)*, pp. 546–551.
18. Polastre, J., Hill, J., & Culler, D. (2004). Versatile low power media access for wireless sensor networks. In *ACM-SenSys '04 proceedings of the 2nd international conference on embedded networked sensor systems*.
19. Cano, C., Bellalta, B., Barcel´o, J., Oliver, M., & Sfairopoulou, A. (2009). Analytical model of the LPL with wake up after transmissions MAC protocol for WSNs (Vol. 10). In *IEEE (ISWCS)*, pp. 146–159.
20. Cano, C., Bellalta, B., Barcel´o, J., Oliver, M., & Sfairopoulou, A. (2011). *Taking advantage of overhearing in low power listening WSNS: A performance analysis of the LWT-MAC protocol mobile networks and applications* (Vol. 16, pp. 613–628). Berlin: Springer.
21. Zareei, M., Budiarto, R., & Wan, T. (2011). Study of mobility effect on energy efficiency in medium access control protocols. *IEEE Symposium on Computers & Informatics, 10,* 759–763.
22. Turati, F., Cesana, M., & Campelli, L. (2009). SPARE MAC enhanced: A dynamic TDMA protocol for wireless sensor networks. *IEEE (GLOBCOM), 10,* 1–6.
23. Douceur, J. R. (2002). The sybil attack. In *Proceedings 1st ACM international workshop peer-to-peer systems (IPTPS'02)*.
24. Faria, D., & Cheriton, D. (2006). Detecting identity-based attacks in wireless networks using signalprints. In *Proceedings ACM workshop on wireless security*, pp. 43–52.
25. Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). The Sybil attack in sensor networks: Analysis and defenses. In *Proceedings of international symposium on information processing in sensor networks (IPSN)*, pp. 259–268.

26. Newsome, J., et al. (2004). The Sybil attack in sensor networks: Analysis and defenses. In *Proceedings of 3rd IEEE international symposium on information processing in sensor networks (IPSN'04)*, Berkeley, CA.
27. von Ahn, L., Blum, M., Hopper, N. J., & Langford, J. (2003). CAPTCHA: Using hard AI problems for security. In *Proceedings Eurocrypt 2003*, Warsaw, Poland, pp. 294–311.
28. Bazzi, R., & Konjevod, G. (2005). On the establishment of distinct identities in overlay networks. In *Proceedings of 24th ACM symposium on principles of distributed computing (PODC 2005)*, Las Vegas, NV, pp. 312–320.
29. Ng, T. S. E., & Zhang, H. (2002). Predicting internet network distance with coordinates-based approaches. In *Proceedings IEEE INFOCOM 2002*, New York, NY, pp. 170–179.
30. Ramachandran, A., & Feamster, N. (2006). Understanding the network-level behavior of spammers. In *Proceedings of ACM SIGCOMM 2006*, Pisa, Italy, pp. 291–302.
31. Chan, H., Perrig, A., & Song, D. (2003). Random key predistribution schemes for sensor networks. In *Proceedings of IEEE symposium on security and privacy*, pp. 197–213.
32. Liu, D., & Ning, P. (2003). Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. In *Proceedings of ACM conference on computer and communications security*, pp. 263–276.
33. Du, W., Deng, J., Han, Y., Chen, S., & Varshney, P. (2004). A key management scheme for wireless sensor networks using deployment knowledge. In *Proceedings of IEEE INFOCOM'04*, Hongkong, China, pp. 586–597.
34. Jajodia, S., Zhu, S., & Setia, S. (2003). Efficient security mechanisms for large-scale distributed sensor networks. In *Proceedings of ACM conference on computer and communications security*, pp. 62–72.
35. Yang, H., Ye, F., Yuan, Y., Liu, S., & Arbaugh, W. (2005). Toward resilient security in wireless sensor networks. In *Proceedings of ACM Mobihoc'05*, pp. 34–44.
36. Demirbas, M., & Song, Y. (2006). An RSSI-based scheme for Sybil attack detection in wireless sensor networks. In *Proceedings of IEEE international symposium on world of wireless, mobile and multimedia networks (WoWMoM).*
37. Chen, Y., Trappe, W., & Martin, R. (2007). Detecting and localizing wireless spoofing attacks. In *Proceedings of sensor, mesh and ad hoc communications and networks*, pp. 193–202.
38. Patwari, N., & Kasera, S. (2007). Robust location distinction using temporal link signatures. In *Proceedings of ACM international conference mobile computing and networking*, pp. 111–122.
39. Xiao, L., Greenstein, L. J., Mandayam, N. B., & Trappe, W. (2009). Channel based detection of Sybil attacks in wireless networks. *IEEE Transactions on Information Forensics and Security, 4*(3), 492–503.
40. Wood, A., & Stankovic, J. (2002). Denial of service in sensor networks. *IEEE Computer Magazine, 35* (10), 54–62.
41. Xu, W., et al. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of 6th ACM international symposium on mobile ad hoc networking and computing (Mobi-Hoc'05)*, Urbana-Champaign, IL.
42. Law, Y. W. (2005). Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols. In *Proceedings of 3rd ACM workshop on security of ad hoc and sensor networks (SASN'05)*, Alexandria, VA.
43. Aad, I., Hubaux, J., & Knightly, E. (2004). Denial of service resilience in ad hoc networks. In *Proceedings of 10th annual ACM international conference on mobile computing and networking (MobiCom'04)*, Philadelphia, PA.
44. Arbor Networks: 'IP flow-based technology'. http://www.arbornetworks.com. Accessed May 2010.
45. Ricciato, F., Coluccia, A., & D'Alconzo, A. (2010). A review of DoS attack models for 3G cellular networks from a system-design perspective. *Computer Communications, 33*(5), 551–558.
46. Wang, H. D., & Li, Q. (2010). Achieving robust message authentication in sensor networks: A public-key based approach. *Wireless Networks, 16*(4), 999–1099.
47. Lee, P., Bu, T., & Woo, T. (2009). On the detection of signaling DoS attacks on 3G/WiMax wireless networks. *Computer Networks, 53*(15), 2601–2616.
48. Zhou, Y., Zhu, X. Y., & Fang, Y. G. (2010). MABS: Multicast authentication based on batch signature. *IEEE Transactions on Mobile Computing, 9*(7), 982–993.
49. Chiba, T., Katoh, T., Bista, B.B., & Takata, T. (2006). DoS packet filter using DNS information. In *Proceedings 20th international conference on advanced information networking and applications*, Vienna, Austria, pp. 6–11.
50. Thomer, M. G., & Massimiliano, P. (2001). MULTOPS: A data-structure for bandwidth attack detection. In *Proceedings of tenth usenix security symposium*, Washington, DC, USA, pp. 23–29.
51. Mirkovic, J., Prier, G., & Reiher, P. (2003). Source-end DDoS defense. In *Proceedings of second IEEE international symposium on network computing and applications*, Cambridge, MA, USA, pp. 171–178.

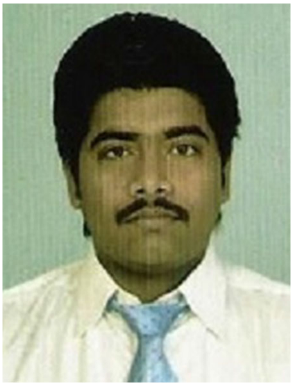
52. Yu, Z., & Guan, Y. (2010). A dynamic en-route filtering scheme for data reporting in wireless sensor networks. *IEEE/ACM Transactions on Networking, 18*(1), 150–163.
53. Kihong, P., & Heejo, L. (2001). On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets (Vol. 31, no. 4). In *ACM SIGCOMM computer communication review—Proceedings 2001 SIGCOMM conference*, San Diego, CA, USA, pp. 15–26.
54. Ratul, M., Steven, M. B., Sally, F., John, I., Vern, P., & Shenker, S. (2002). Controlling high bandwidth aggregates in the network. *ACM SIGCOMM Computer Communication Review, 32*(3), 62–73.
55. Sarker, J. H., & Mouftah, H. T. (2010). Throughput and stability improvements of slotted ALOHA based wireless networks under the random packet destruction DoS attack. In *Proceedings of IEEE international conference on communications*, Cape Town, South Africa, pp. 1–6.
56. McCune, J. M. (2005). Detection of denial-of-message attacks on sensor network broadcasts. In *Proceedings of 2005 IEEE symposium on security and privacy (SP'05)*, Oakland, CA.
57. Deng, J., Han, R., & Mishra, S. (2005). Defending against path-based DoS attacks in wireless sensor networks. In *Proceedings of 3rd ACM workshop on security of ad hoc and sensor networks (SASN'05)*, Alexandria, VA.
58. Yaar, A., Perrig, A., & Song, D. (2003). Pi: A path identification mechanism to defend against DDoS attack. In *Symposium on security and privacy*, pp. 93–107.
59. Akan, Ö. B., & Akyildiz, I. F. (2005). Event-to-sink reliable transport in wireless sensor networks. *IEEE/ACM Transactions on Networking, 13*(5), 1003–1016.
60. Hu, Y.-C., Perrig, A., & Johnson, D. (2003). Packet leashes: Adefense against wormhole attacks in wireless networks (Vol. 3). In *Proceedings of IEEE INFOCOM*, pp. 1976–1986.
61. Eriksson, J., Krishnamurthy, S. V., & Faloutsos, M. (2006). Truelink: A practical countermeasure to the wormhole attack in wireless networks. In *Proceedings of IEEE ICNP*, pp. 75–84.
62. Wang, W., Bhargava, B., Lu, Y., & Wu, X. (2006). Defending against wormhole attacks in mobile ad hoc networks. *Wireless Communications and Mobile Computing, 6,* 483–503.
63. Hu, L., & Evans, D. (2004). Using directional antennas to prevent wormhole attacks. In *Presented at the NDSS*.
64. Poovendran, R., & Lazos, L. (2007). A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. *Wireless Networks, 13,* 27–59.
65. Khalil, I., Bagchi, S., & Shroff, N. B. (2005). Liteworp: A light-weight countermeasure for the wormhole attack in multi-hop wireless networks. In *Proceedings of DSN*, pp. 612–621.
66. Zhang, Y., Liu, W., Lou, W., & Fang, Y. (2006). Location-based compromise tolerant security mechanisms for wireless sensor networks. *IEEE Journal on Selected Areas in Communications, 24*(2), 247–260.
67. Poovendran, R., & Lazos, L. (2007). A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. *Wireless Networks, 13,* 27–59.
68. Wang, W., & Bhargava, B. (2004). Visualization of wormholes in sensor networks. In *Proceedings of ACM WiSe*, pp. 51–60.
69. Song, N., Qian, L., & Li, X. (2005). Wormhole attack detection in wireless ad hoc networks: A statistical analysis approach. In *Proceedings of IEEE IPDPS*.
70. Buttyan, L., Dora, L., & Vajda, I. (2005). Statistical wormhole detection in sensor networks. In *Proceedings of IEEE ESAS*, pp. 128–141.
71. Taheri, M., Naderi, M., & Barekatain, M. (2001). New approach for detection and defending the wormhole attacks in wireless ad hoc networks (Vol. 10). In *Proceedings of IEEE international conference on communications*, pp. 3201–3205.
72. Tran, P. V., Hung, L. X., Lee, Y. K., Lee, S. Y., & Lee, H. (2007). TTM: An efficient mechanism to detect wormhole attacks in wireless ad hoc networks. In *4th IEEE conference on consumer communications and networking conference*, pp. 593–598.
73. Singh, A., & Vaisla, K. S. (2010). A mechanism for detecting wormhole attacks on wireless ad hoc network. *International Journal of Computer and Network Security, 2*(9), 27–31.
74. Adamy, D. L., & Adamy, D. (2004). *EW 102: A second course in electronic warfare*. Norwood, MA: Artech House Publishers.
75. Radio Jamming—wikipedia. http://en.wikipedia.org/wiki/Radiojamming.
76. Pickholtz, R. L., Schilling, D. L., & Milstein, L. B. (1982). Theory of spread spectrum communications—A tutorial. *IEEE Transactions on Communications, 20*(5), 855–884.
77. FHSS-wikipedia. http://en.wikipedia.org/wiki/Frequency-hoppingspread-spectrum.
78. DSSS-wikipedia. http://en.wikipedia.org/wiki/Direct-sequence-spreadspectrum.
79. UWB-wikipedia. http://en.wikipedia.org/wiki/Ultrawideband.
80. Oppermann, I., Stoica, L., Rabbachin, A., Shelby, Z., & Haapola, J. (2004). UWB wireless sensor networks: UWEN-a practical example. *IEEE Communications Magazine, 42*(12), 27–32.

81. Stutzman, W., & Thiele, G. (1997). *Antenna theory and design* (2nd ed.). New York: Wiley.
82. Murthy, C. S. R., & Manoj, B. S. (2004). Transport layer and security protocols for ad hoc wireless networks. In *Ad hoc wireless networks: Architectures and protocols*. Prentice Hall, Upper Saddle River.
83. Ramanathan, R. (2001). On the performance of ad hoc networks with beamforming antennas. In *ACM international symposium on mobile ad hoc networking and computing (MobiHoc'01)*, Long Beach, California, USA.
84. Spyropoulos, A., & Raghavendra, C. S. (2002). Energy efficient communications in ad hoc networks using directional antennas. In *IEEE conference on computer communications (INFOCOM'02)*, NY, USA.
85. Bandyopadhyay, S., Hasuike, K., Horisawa, S., & Tawara, S. (2001). An adaptive MAC and directional routing protocol for ad hoc wireless network using directional ESPAR antenna. In *Proceedings ACM symposium on mobile ad hoc networking and computing 2001 (MOBIHOC 2001)*, Long Beach, California, USA.
86. Ko, Y. B., Shankarkumar, V., & Vaidya, N. H. (2000). Medium access control protocols using directional antennas in ad hoc networks. In *Proceedings of the IEEE INFOCOM 2000.*
87. Li, Y., & Man, H. (2004). Analysis of multipath routing for ad hoc networks using directional antennas (Vol. 4). In *IEEE 60th vehicular technology conference*, pp. 2759–2763.
88. Roy, S., Bandyopadhyay, S., Ueda, T., & Hasuike, K. (2002). Multipath routing in ad hoc wireless networks with omni directional and directional antenna: A comparative study. In *Proceedings of 4th international workshop of distributed computing, mobile and wireless computing, IWDC 2002*, Calcutta, India, pp 184–191.
89. Yu, B., & Xiao, B. (2006). Detecting selective forwarding attacks in wireless sensor networks. In *Parallel and distributed processing symposium, 2006. IPDPS 2006. 20th international*, p. 8.
90. Xin-Sheng, W., Yong-Zhao, Z., Shu-Ming, X., & Liangmin, W. (2009). Lightweight defence scheme against selective forwarding attacks in wireless sensor networks, pp. 226–232.
91. Sun, H.-M., Chen, C.-M., & Hsiao, Y.-C. (2007). An efficient countermeasure to the selective forwarding attack in wireless sensor networks, pp. 1–4.
92. Brown, J., & Du, X. (2008). Detection of selective forwarding attacks in heterogeneous sensor networks. In *ICC*, pp. 1583–1587.
93. Ngai, E. C. H., Liu, J., & Lyu, M. R. (2006). On the intruder detection for sinkhole attack in wireless sensor networks (Vol. 8). In *IEEE international conference on communications, 2006*, pp. 3383–3389.
94. Dallas, D., Leckie, C., & Ramamohanarao, K. (2007). Hop-count monitoring: Detecting sinkhole attacks in wireless sensor networks. In *15th IEEE international conference on networks, 2007, ICON 2007,* pp. 176–181.
95. Tumrongwittayapak, C., & Varakulsiripunth, R. (2009). Detecting sinkhole attacks in wireless sensor networks. In *ICROS-SICE international joint conference 2009,* pp. 1966–1971.
96. Chen, C., Song, M., & Hsieh, G. (2010). Intrusion detection of sinkhole attacks in large-scale wireless sensor networks. In *IEEE international conference on wireless communications, networking and information security (WCNIS), 2010*, pp. 711–716.
97. Sheela, D., Kumar, C. N., & Mahadevan, G. (2011). A non cryptographic method of sinkhole attack detection in wireless sensor networks. In *IEEE international conference on recent trends in information technology, ICRTIT 2011*, pp. 527–532.
98. Madden, S., Franklin, M. J., Hellerstein, J. M., & Hong, W. (2002). TAG: A tiny aggregation service for ad hoc sensor networks. In *Proceedings of 5th USENIX symposium on operating systems design and implementation (OSDI).*
99. Zhao, J., Govindan, R., & Estrin, D. (2003). Computing aggregates for monitoring sensor networks. In *Proceedings of 2nd international workshop on sensor network protocols applications.*
100. Considine, J., Li, F., Kollios, G., & Byers, J. (2004). Approximate aggregation techniques for sensor databases. In *Proceedings of 20th international conference on data engineering (ICDE)*, April 2004 (pp. 449–460).
101. Nath, S., Gibbons, P. B., Seshan, S., & Anderson, Z. (2008). Synopsis diffusion for robust aggregation in sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, *4*(2), 7.
102. Wagner, D. (2004). Resilient aggregation in sensor networks. In *Proceedings of ACM workshop security of sensor and adhoc networks (SASN).*
103. Buttyan, L., Schaffer, P., & Vajda, I. (2006). Resilient aggregation with attack detection in sensor networks. In *Proceedings of 2nd IEEE workshop sensor networks and systems for pervasive computing.*
104. Chan, H., Perrig, A., & Song, D. (2006). Secure hierarchical in-network aggregation in sensor networks. In *Proceedings of ACM conference on computer and communications security (CCS).*
105. Frikken, K. B., & Dougherty, J. A. (2008). An efficient integrity-preserving scheme for hierarchical sensor aggregation. In *Proceedings of 1st ACM conference on wireless network security (WiSec).*

106. Hu, L., & Evans, D. (2003). Secure aggregation for wireless networks. In *Proceedings of workshop security and assurance in ad hoc networks*.
107. Yu, H. (2009). Secure and highly-available aggregation queries in large-scale sensor networks via set sampling. In *Proceedings of international conference on information processing in sensor networks*.
108. Kumar, D., Aseri, T., & Patel, R. (2011). EECDA: Energy efficient clustering and data aggregation protocol for heterogeneous wireless sensor networks. *International Journal of Computers, Communications & Control, 6*(1), 113–124.
109. Cheng, C.-T., Leung, H., & Maupin, P. (2013). Delay-aware network structure for wireless sensor networks with in-network data fusion. *IEEE Sensors Journal, 13*(5), 1622–1631.
110. Du, T., Qu, Z., Guo, Q., & Qu, S. (2015). A high efficient and real time data aggregation scheme for WSNs. *International Journal of Distributed Sensor Networks, 2015,* 1–11.
111. Fan, K. W., Liu, S., & Sinha, P. (2007). Structure-free data aggregation in sensor networks. *IEEE Transactions on Mobile Computing, 6*(8), 929–942.
112. Lin, C., Wu, G., Xia, F., Li, M., Yao, L., & Pei, Z. (2012). Energy Efficient ant colony algorithms for data aggregation in wireless sensor networks. *Journal of Computer and System Sciences, 78*(6), 1686–1702.
113. Ren, F., Zhang, J., Wu, Y., He, T., Chen, C., & Lin, C. (2013). Attribute-aware data aggregation using potential-based dynamic routing in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems, 24*(5), 881–892.
114. Wu, W., Cao, J., Wu, H., & Li, J. (2013). Robust and dynamic data aggregation in wireless sensor networks: A cross-layer approach. *Computer Networks, 57*(18), 3929–3940.
115. Simon, S., & Jacob, K. P. (2013). HEAP: Hybrid energy-efficient aggregation protocol for large scale wireless sensor networks. *International Journal of Computers & Technology, 4*(2), 713–721.
116. Shaullah, G. M., Azad, S. A., & Ali, A. S. (2013). Energy-efficient wireless MAC protocols for railway monitoring applications. *IEEE Transactions on Intelligent Transport System, 14*(2), 649–659.
117. Yoo, H., Shim, M., & Kim, D. (2012). Dynamic duty-cycle scheduling schemes for energy-harvesting wireless sensor networks. *IEEE Communications Letters, 16*(2), 202–204.
118. Parikh, S., Vokkarane, V. M., Xing, L., & Kasilingam, D. (2007). Node replacement policies to maintain threshold-coverage in wireless sensor networks. In *Proceedings of IEEE conference on computer communications and networks*, pp. 760–765.
119. Tong, B., Wang, G., Zhang, W., & Wang, C. (2011). Node reclamation and replacement for long-lived sensor networks. *IEEE Transactions on Parallel and Distributed Systems, 22*(9), 1550–1563.
120. Wei, C., Zhi, C., Fan, P., & Letaief, K. B. (2009). AsOR: An energy efficient multi-hop opportunistic routing protocol for wireless sensor networks over Rayleigh fading channels. *IEEE Transactions on Wireless Communications, 8*(5), 2452–2463.
121. Han, Z., Wu, J., Zhang, J., Liu, L., & Tian, K. (2014). A general self-organized tree-based energy-balance routing protocol for wireless sensor network. *IEEE Transactions on Nuclear Science, 61*(2), 732–740.
122. Pantazis, N. A., Nikolidakis, S. A., & Vergados, D. D. (2013). Energy-efficient routing protocols in wireless sensor networks: A survey. *IEEE Communications Surveys & Tutorials, 15*(2), 551–591.
123. Sudevalayam, S., & Kulkarni, P. (2011). Energy harvesting sensor nodes: Survey and implications. *IEEE Communications Surveys & Tutorials, 13*(3), 443–461.
124. Chachulski, S., Jennings, M., Katti, S., & Katabi, D. (2007). Trading structure for randomness in wireless opportunistic routing. *ACM SIGCOMM Computer Communication Review, 37*(4), 169–180.
125. He, S., Chen, J., Yau, D. K. Y., & Sun, Y. (2012). Cross-layer optimization of correlated data gathering in wireless sensor networks. *IEEE Transactions on Mobile Computing, 11*(11), 1678–1691.
126. Zhai, C., Liu, J., Zheng, L., Xu, H., & Chen, H. (2012). Maximize lifetime of wireless sensor networks via a distributed cooperative routing algorithm. *Transactions on Emerging Telecommunications Technologies, 23*(5), 414–428.
127. Mao, X., Tang, S., Xu, X., Li, X.-Y., & Ma, H. (2011). Energy-efficient opportunistic routing in wireless sensor networks. *IEEE Transactions on Parallel Distributed Systems, 22*(11), 1934–1942.
128. Zhu, T., & Towsley, D. (2011). E2R: Energy efficient routing for multi-hop green wireless networks. In *Proceedings of IEEE INFOCOM*, pp. 265–270.
129. Nacef, A. B., Senouci, S.-M., Ghamri-Doudane, Y., & Beylot, A.-L. (2012). A combined relay-selection and routing protocol for cooperative wireless sensor networks. In *Proceedings of IEEE conference on wireless communications mobile computing*, pp. 293–298.
130. Chen, S., Li, Y., Huang, M., Zhu, Y., & Wang, Y. (2013). Energy-balanced cooperative routing in multihop wireless networks. *Wireless Networks, 19*(6), 1087–1099.

131. Chi, Y.-P., & Chang, H.-P. (2012). TARS: An energy-efficient routing scheme for wireless sensor networks with mobile sinks and targets. In *Proceedings of IEEE international conference advanced information networking and applications*, pp. 128–135.
132. Zungeru, A. M., Ang, L.-M., & Seng, K. P. (2012). Termite-hill: Routing towards a mobile sink for improving network lifetime in wireless sensor networks. In *Proceedings of international conference on intelligent systems, modelling simulation*, pp. 622–627.
133. Perkins, C. E., & Royer, E. M. (1999). Ad hoc on-demand distance vector routing. In *Proceedings of IEEE WMCSA*, pp. 90–100.
134. Konstantopoulos, C., Pantziou, G., Gavalas, D., Mpitziopoulos, A., & Mamalis, B. (2012). A rendezvous-based approach enabling energy-efficient sensory data collection with mobile sinks. *IEEE Transactions on Parallel and Distributed Systems, 23*(5), 809–817.
135. Tyagi, S., Tanwar, S., Gupta, S. K., Kumar, N., & Rodrigues, J. J. P. C. A lifetime extended multi-levels heterogeneous routing protocols for wireless sensor networks, pp. 43–62.
136. Gu, X., Yu, J., Yu, D., Wang, G., & Lv, Y. (2014). ECDC: An energy and coverage aware distributed clustering protocol for wireless sensor networks. *Computers & Electrical Engineering, 40*(2), 384–398.
137. Tanwar, S., Kumar, N., & Niu, J.-W. (2014). EEMHR: Energy-efficient multilevel heterogeneous routing protocol for wireless sensor networks. *International Journal of Communication Systems, 27*(9), 1289–1318.
138. Kumar, D., Aseri, T. C., & Patel, R. B. (2011). Multi-hop communication routing (MCR) protocol for heterogeneous wireless sensor networks. *International Journal of Information Technology, Communications and Convergence, 1*(2), 130–145.
139. Sudarmani, R., & Kumar, K. R. S. (2013). Particle swarm optimization-based routing protocol for clustered heterogeneous sensor networks with mobile sink. *American Journal of Applied Sciences, 10* (3), 259–269.
140. Atero, F. J., Vinagre, J. J., Ramiro, J., & Wilby, M. (2011). A low energy and adaptive routing architecture for efficient field monitoring in heterogeneous wireless sensor networks. In *Proceedings of IEEE international conference on high performance computing and simulation*, pp. 449–455.
141. Vilela, M. A., & Araujo, R. B. (2012). RAHMoN: Routing algorithm for heterogeneous mobile networks. In *Proceedings of 2nd Brazilian conference on critical embedded systems (CBSEC)*, pp. 24–29.
142. Deng, J., & Han, Y. S. (2013). Cooperative secret delivery in wireless sensor networks. *International Journal of Ad Hoc and Ubiquitous Computing, 14*(4), 226–237.
143. Wang, C., Feng, T., Kim, J., Wang, G., & Zhang, W. (2011). Catching packet droppers and modifiers in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems, 22*(9), 1550–1563.
144. Raymond, D., et al. (2006). Effects of denial of sleep attacks on wireless sensor network MAC protocols. In *Proceedings of 7th annual IEEE systems, man, and cybernetics (SMC) information assurance workshop (IAW)*, IEEE Press, pp. 297–304.
145. Stajano, F., & Anderson, R. (1999). The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Proceedings of 7th international workshop security protocols*, Springer, pp. 172–194.
146. Sohrabi, K., et al. (2000). Protocols for self-organization of a wireless sensor network. *IEEE Personal Communications, 7*(5), 16–27.
147. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks : Attacks and countermeasures. In *Proceedings of the first international workshop on sensor network and protocols and applications*.
148. Deng, J., Han, R., & Mishra, S. (2004). Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks. In *Proceedings of international conference on dependable systems and networks*, IEEE CS Press, pp. 637–656.
149. Yu, Y., Govindan, R., & Estrin, D. (2001). *Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks*, technical report UCLA/CSD-tr-01-0023, Computer Science Department, University of California, Los Angeles.
150. Tanabe, N., Kohno, E., Kakuda, Y. (2013). A path authentication method using bloom filters against impersonation attacks on relaying nodes in wireless sensor networks. In *IEEE 33rd international conference on distributed computing systems workshops*, pp. 357–361.
151. Yao, L., Kang, L., Deng, F., Deng, J., & Wu, G. (2013). Protecting source-location privacy based on multi-rings in wireless sensor networks. In *Wiley's concurrency and computation: Practice and experience, special issue on trust and security in wireless sensor networks*.
152. Ward, J., Younis, M. (2016). A cross-layer traffic analysis countermeasures against adaptive attackers of wireless sensor networks. In *MILCOM 2016*, pp. 271–276.

153. Alsemairi, S., & Younis, M. (2015). Adaptive packet combining to counter traffic analysis in wireless sensor networks. In *IWCMC 2015*, pp. 337–342.
154. Xu, W. Y., Ma, K., Trappe, W., & Zhang, Y. (2006). Jamming sensor networks: Attacks and defense strategies. *IEEE Network, 20*(3), 41–47.
155. Min, J. (1995). *Analysis and design of a frequency-hopped spread-spectrum transceiver for wireless personal communications*, University of California.
156. Perrig, A., et al. (2002). SPINS: Security protocols for sensor networks. *ACM Wireless Networks, 8*(5), 521–534.
157. Deng, J., Han, R., & Mishra, S. (2003). A performance evaluation of intrusion-tolerant routing in wireless sensor networks. In *Proceedings 2nd IEEE international workshop on information processing in sensor networks (IPSN'03)*, Palo Alto, CA.
158. Pietro, R. D., et al. (2003). LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks. In *Proceedings of 2003 IEEE international. conference on parallel processing workshops (ICPP'03).*
159. Wang, G., et al. (2003). On supporting distributed collaboration in sensor networks. In *Proceedings of 2003 IEEE military communication conference (MILCOM'03)*, Boston, MA.
160. Zhang, Y., et al. (2006). Location-based compromise-tolerant security mechanisms for wireless sensor networks. *IEEE JSAC, 24*(2), 247–260.
161. Parno, B., Perrig, A., & Gligor, V. (2005). Distributed detection of node replication attacks in sensor networks. In *Proceedings of 2005 IEEE symposium on security and privacy (SP'05)*, Oakland, CA.
162. Hu, Y., Perrig, A., & Johnson, D. (2003). Rushing attacks and defense in wireless ad hoc network routing protocols. In *Proceedings 2003 ACM workshop. wireless security (WiSe'03)*, San Diego, CA.
163. Laporte, G., & Pascoal, M. M. B. (2011). Minimum cost path problems with relays. *Computers & Operations Research, 38*(1), 165–173.
164. Chi, Y.-P., & Chang, H.-P. (2009). TRENS: A tracking-assisted routing scheme for wireless sensor networks. In *Proceedings of IEEE international symposium on pervasive system algorithms and networks*, pp. 190–195.
165. Tyagi, S., Tanwar, S., Gupta, S. K., Kumar, N., & Rodrigues, J. J. P. C. (2015). A lifetime extended multi-levels heterogeneous routing protocol for wireless sensor networks. *Telecommunication Systems, 59*(1), 43–62.
166. Güney, E., Aras, N., Altınel, İ. K., & Ersoy, C. (2012). Efficient solution techniques for the integrated coverage, sink location and routing problem in wireless sensor networks. *Computers & Operations Research, 39*(7), 1530–1539.



Bharat Bhushan received the B.Tech. degree in computer science and engineering from SHIATS, Allahabad, India in 2012, and the M.Tech degree in information security from Birla Institute of Technology, Mesra, Jharkhand, India in 2015, and is currently working toward the Ph.D. degree at Birla Institute of Technology, Mesra, Jharkhand, India. From 2012 through 2013, he worked as a network engineer at HCL Infosystems Ltd., Noida, India. He is IEEE student member. His research interests includes the security and attacks in wireless sensor networks, performance analysis of wireless sensor network communications and security in networking systems.

Gadadhar Sahoo received his Ph.D. degree from IIT Kharagpur. He is currently working as professor (Department of Computer Science and Engineering) and Dean (Admissions and Academic Coordination) of Birla Institute of Technology, Mesra, Jharkhand, India. He has teaching and research experience of 26 years with Birla Institute of Technology, Mesra, Jharkhand, India. His research interests includes Soft Computing, Clustering, Cloud Computing, Cryptography, Bio-Informatics and security in wireless sensor networks.