Security Implementations in Smart Sensor Networks

Mohamed Fazil Mohamed Firdhous

Abstract Wireless sensor networks have become one of the widely deployed networking technologies in the recent times due to the capabilities and advantages of them. The applications of wireless sensor networks include many civilian and industrial applications to military applications. Due to the distributed nature of these networks, deployment in remote and open areas and many constraints in individual nodes, these networks are vulnerable to several security threats. Many security mechanisms and algorithms proposed for the implementation in the traditional networks cannot be implemented in wireless sensor networks due to the unique nature of these networks and nodes. Many active research programmes have been carried out throughout the world for making wireless sensor networks more secure and user friendly. This chapter takes an in-depth look at some of the prominent mechanisms, schemes, algorithms and protocols published in the literature.

1 Introduction

Smart sensor networks have found a place in many popular application domains especially for monitoring, tracking and control purposes [1]. A sensor network is an array of sensors and other nodes interconnected by a network for the purpose of transmitting the data captured and other information between these nodes. In these networks, the sensors occupy the main position as they play the important role of capturing the information that is considered to be of value when processed. With the advancement of semiconductor and sensor technologies, smart sensors have been developed that can carry out many more tasks than just capturing the data. Smart sensors are required to have seven major elements in them. They are namely sensor, signal conditioner, analog to digital converter, application algorithms, data storage area, user interface and communication interface [2]. These additional elements make these sensors to be more versatile, reliable and secure while requiring less

M.F.M. Firdhous (✉)
Faculty of Information Technology, University of Moratuwa, Katubedda, Sri Lanka
e-mail: Mohamed.Firdhous@uom.lk

K.K. Ravulakollu et al. (eds.), *Trends in Ambient Intelligent Systems*,
Studies in Computational Intelligence 633, DOI 10.1007/978-3-319-30184-6_8

maintenance compared to normal sensors. Smart sensors can be setup fast and have the capability of reprogrammed to suit the changes in requirements. Also these sensors can be monitored remotely, this eases the administration of these networks to a very great extent [3].

With the increased deployments and applications of sensor networks, many issues that demand immediate and special attention have also come to the fore. One such major issue demand the critical attention of the implementers as well as researchers is security [4]. Security in smart sensor networks not only need to be enhanced but also made to be more rugged in the face of increased security threats and new methods of attacks. The security in sensor networks must be addressed from multiple directions requiring a multi-pronged approach. The areas that require special attention can be summarized as: security of the sensor nodes, security of the information transferred and security of the information path. Implementing security in sensor networks is a challenging task due to inherent constraints in the wireless sensor networks such as remoteness of implementation, limitations in processing power, instability of the network and shortage of energy supplies [4–8].

This chapter presents an in-depth evaluation of security implementations in smart sensor networks, specifically on three main areas. They are namely: security of smart sensor nodes, security of data transferred and security of routing in smart sensor networks. The evaluation primarily concentrates on the present security implementations with special reference to their principles, strengths and weaknesses along with the future directions of research in these specific aspects.

2 Smart Sensor Networks

A sensor network is an array of sensors possibly of different kinds and processors that are interconnected by a communication network for the purpose of transferring data and control information between them [9]. A sensor can be of single modal or multi modal depending the requirement and the complexity of the sensor itself. A single modal sensor can carry out only one sensing function and made of a single technology. On the other hand, multi-modal sensors are multifunctional and may be composed of many sensing hardware created using optical, acoustic, chemical, infrared, magnetic, seismic, tactile, temperature, gravity, pressure, electric, semiconductor etc. In recent times, semiconductor sensors have become more popular due to their functionality and versatility [10]. For example, modern semiconductor gas sensors can detect more than 150 gases making them the most preferred choice in many industries like automotive, consumer, commercial, industrial, indoor and outdoor air quality monitoring and environmental monitoring [11]. Also, semiconductor sensors have special characteristics such as better sensitivity, faster response time, long term stability and longer life time compared to other sensors.

Smart sensor networks can be created installing intelligence into the sensors or closer to them [9]. When the processing capability along with sensing and other

required units such as signal conditioner, analog to digital converter, application algorithms, memory for data and application storage, user interface and communication interfaces are built into a single module, it is known as a smart sensor [2]. When intelligence is integrated into an aggregator node that receives raw data from neighbouring not so smart sensor nodes and processes them before sharing it with other aggregator nodes in the network or a central processing unit, the intelligence or smartness is located closer to the nodes. Thus the aggregator nodes are considered to be more capable and powerful compared to the other simple nodes in the network. Simple nodes just broadcast the data they collect while the smart nodes process them for the purpose of extracting information through various operations such as validating, deriving, integrating etc., before transmitting. Since the data is validated and processed closer the source itself, it saves the valuable network bandwidth and in sometimes energy by not transmitting invalid or partial information.

Smart sensor networks can be deployed for various purposes such as monitoring the environment, functions and operations of machinery or the human body itself or movement of objects within certain premises or operations [12]. Depending on the type of application and the type of nodes deployed, these networks will have various capabilities and limitations. Depending on the type of connection between the nodes, sensor networks can be divided to two categories known as wireless sensor networks and wired sensor networks. Wireless sensor networks suffer from many limitations compared to wired sensor networks due to their inherent nature. The main limitations of wireless sensor networks include limited power, limited processing capabilities within nodes and unstable communication between nodes. Generally wireless sensor networks are also implemented far away from the final processing centres in remote locations making the management of these sensor nodes a difficult task.

2.1 Sensor Node Placement

Sensor node placement is an important aspect that must be given proper consideration for the successful implementation of sensor network [13]. Sensor nodes can be either placed deterministically or randomly depending on the type of application, size of deployment, number of nodes to be placed and the geographical area to be covered. In industrial applications, sensors are placed deterministically at strategic points for collecting the right information. Generally in industrial settings, it is the operation and functions of machineries and related equipment are monitored. When the health of a machine is monitored in an industrial setting, the sensors are placed at various points within the machine or closer to the machine for monitoring the temperature, flow of coolants, properties of coolants etc. When indoor environments or outdoor environments are monitored in a limited fashion like traffic monitoring system or the monitoring of pollutants in a certain area, the sensors are placed in a deterministic manner.

When sensors are placed for monitoring a large area for environmental changes, aftermath of natural disasters or military operations, it is not possible to place them

deterministically due to the large number of nodes to be placed or the accessibility issues in these areas [14]. Generally during large scale sensor deployment in a geographically distributed manner, sensors are placed randomly by dropping them off from an airplane or some other method [15]. This kind of placements have many shortcomings including coverage and communication problems. When sensors are dropped randomly, certain areas may have been deployed with many nodes resulting in coverage overlaps and wasting of resources. On the other hand the areas, where there are insufficient nodes, would have coverage holes and connectivity problems resulting in inefficient monitoring and isolation of sensor nodes. Hence nodes must be placed in an efficient and effective manner to reduce the problems arising from coverage overlaps, holes and communication. In many situations, redundant nodes are deployed in order to overcome the problems of shortage of coverage and communications in random node deployments [16].

2.2 Sensing and Data Acquisition

The set of nodes deployed in a particular application can be either homogeneous or heterogeneous. When all the nodes deployed are of the same type and have similar capabilities, it is known as a homogeneous deployment. In a heterogeneous deployment, certain nodes may have different capabilities compared to other nodes used. One of the main attribute that is used for categorising nodes in a deployment is their sensing range. The sensing range is the area across which a node is capable of detecting the presence or absence of an object or phenomenon. Certain types of nodes may have different sensing ranges and can choose a specific range out of all the available ranges as its working range depending in the requirements. A general assumption is that when a large sensing range is used by a sensor node, it consumes more energy. In heterogeneous deployment, the nodes with larger sensing ranges are generally used as cluster heads due to their advanced capabilities [17]. In remote deployments of wireless sensor networks, the total amount of energy available in nodes will determine the life of the networks. Hence it is recommended to use the minimum amount of energy for all sensor operations including sensing, processing and communication in order to prolong the life of sensor networks. Ranjan and Kar [18] have provided a method for determining the optimal number of cluster heads for homogeneous sensor networks using reasonable energy consumption model.

2.3 Connectivity in Wireless Sensor Networks

The other important parameter that affects the performance of a sensor network is communication range. In a multi-hop sensor network, communication nodes are linked by a wireless medium such as radio, infrared, or optical media [19]. Once the data has been collected, that data needs to be transmitted to the processing centre.

Connectivity between nodes is important to ensure that every sensor node can communicate with the processing centre [20]. In a multi-hop wireless sensor network, the network is said to be fully connected if every pair of nodes is able to communicate with each other, either directly or via intermediate relay nodes.

A sensors network is considered to be connected, only if there is at least one path between each pair of nodes through which successful communication can take place. Hence for the successful transfer of data from any given node to the processing centre, there must be a communication path from that node to the processing centre. Connectivity between nodes depends primarily on the existence of paths and affected by changes in topology due to mobility, failure of nodes and attacks that cause loss of links, isolation of nodes or partitioning of the network [21]. Though the cost of individual sensor is relatively low, the total cost of implementing a sensor network could be high due to the large number of sensor nodes required to setup a network. Therefore, it is important to find the minimum number of nodes required for a wireless sensor network to achieve full connectivity while optimizing coverage at the same time.

Since nodes in wireless sensor network are connected to other nodes via radio, infrared or optical media, the communication range of the nodes will determine whether the nodes still are part of the network or have become isolated from other nodes. When a sensor node needs to communicate with other nodes, it must be within the communication ranges of both transmitting as well as receiving nodes. The communication range of a sensor node is generally determined by the transmit power, receiver sensitivity and the total attenuation introduced by the transmission path. The relationship between the communication range and sensing range of sensor nodes for maintaining communication and proper coverage is given by Formula 1 [22].

$$R_c \leq R_s^1 + R_s^2 \tag{1}$$

where R_c is the communication range of the nodes and R_s^1 and R_s^2 are sensing ranges of node 1 and node 2 respectively.

The relationship given in Formula 1 can be better explained graphically as shown in Fig. 1.

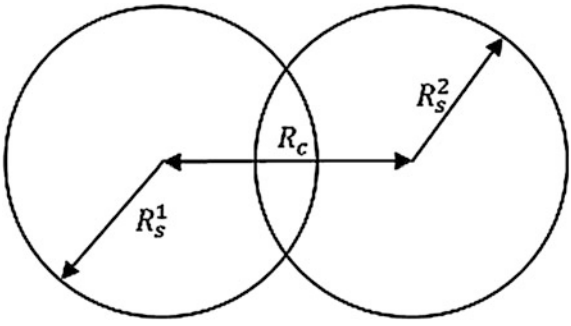

Fig. 1 Relationshipe between communication range and sensing ranges

It must also be noted that maintaining larger communication range require more energy. Hence when deciding an optimum distribution of sensor nodes in a large network, many things including connectivity, coverage, energy consumption, cost and flexibility need to be taken into account.

2.4 Communication Protocols

The successful operation of a wireless sensor network largely depends on the communication protocol chosen for the implementation [7]. The communication protocol chosen every aspect of the wireless sensor network including architecture, data rate, network size, span, power management and security. One factor that is common to all the available communication protocols is that they all are low power communication protocols. Currently there are three communication protocols that can be chosen for the implementation in wireless sensor networks. They are namely Bluetooth, IEEE 802.15.4 and ZigBee [23–25]. The following subsections briefly discuss these protocols with special reference to their suitability for the implementations in wireless sensor networks when security is the main concern.

2.4.1 Bluetooth

Bluetooth that has been standardized by IEEE 802.15.1 has been initially developed and standardized for the low power wireless devices [23]. The design of Bluetooth requires all nodes within its piconet to be synchronized within a few microseconds. This requirement cannot be met by many wireless sensor networks as they have large network latencies due to several constraints within them [26]. With typical Bluetooth configuration, it would take around 2.4 microseconds to establish a connection. Also typical Bluetooth radios consume hundreds of milliwatts power just for monitoring the channel. All these shortcomings makes Bluetooth unsuitable for implementation in wireless sensor networks.

2.4.2 IEEE 802.15.4

The IEEE 802.15.4 was developed for low rate wireless personal are networks [24]. Wireless personal area networks require little or no infrastructure at all for successful implementation and operation. IEEE 802.15.4 allows the implementation of small, power efficient and inexpensive solutions using a wide range of devices. The features of IEEE 802.15.4 allows the realization of the objectives of personal area networks, that are ease of installation, reliable data transfer, short range operation, low cost of implementation and maintenance and reasonable battery life. These are the main objectives of wireless sensor networks as well, hence IEEE 802.15.4 is

very suitable for the implementation in wireless sensor networks. IEEE 802.15.4 standard defines both physical and media access control layers along with component devices and supported network topologies. There are many security suits defined in this standard.

At the basic level, it is possible to either enable or disable security. Security can be disabled by enabling the unsecured mode, which selects the null security suit. An application can select the appropriate security level by entering the required parameters in the radio stack. If no parameter is entered then, no security is enabled by default.

A link layer protocol provides four basic security services. These are access control, message integrity, message confidentiality and replay protection. Access control is enabled through an access control list. The access control list enables message filtering for accepting messages only from selected nodes in the list. Message integrity and authentication is achieved through a message authentication code appended to every frame of data transmitted. Message authentication code is computed using a secret cryptographic code shared by both sender and receiver. When a data frame is received, the receiver recomputes the message authentication code using the cryptographic key in its memory and checks it against the message authentication code received with the frame. If the message authentication codes match with each other, then the data is accepted as genuine, otherwise it is discarded. Without compromising the secret key, it is impossible for an adversary to change valid messages or introduce phoney message into the network. Sequential freshness checks carried out on each received frame enables the detection of replay attacks. The receiver maintains a received frame counter for every message sequence received. When a frame with a counter value equal to or less than the sequence counter value stored in the memory, it is discarded as a duplicate or replay frame.

The access control and message integrity checks can effectively eliminate the unauthorised parties from sending messages and participating in network activities. The authorised nodes can easily detect the messages from rogue nodes initially by filtering messages by the access control list. Even when a rogue node fakes the identity of a genuine node, the message authentication code will help the authorized node to detect the phoney or compromised message frame and discard it.

There are eight different security suites defined within the IEEE 802.15.4 standards. Based on the type of functionality provided, these suites can be broadly categorised into four different groups as shown in Table 1. The broad categories are namely, no security, encryption only, authentication only and encryption and authentication.

Encryption is performed by Advanced Encryption Standard (AES) algorithm. The united States government has accepted AES algorithm as its official standards for its organizations to protect sensitive information [7]. Counter mode cryptographic operation with AES (AES-CTR) uses AES as the block cipher providing access control and encryption along with optional sequential freshness.

Table 1 Security suites defined in IEEE 802.15.4 [7]

Name	Description
Null	No security
AES-CTR	Encryption only—CTR mode
AES-CBC-MAC-128	128 bit MAC
AES-CBC-MAC-64	64-bit MAC
AES-CBC-MAC-32	32-bit MAC
AES-CCM-128	Encryption and 128 bit MAC
AES-CCM-64	Encryption and 64 bit MAC
AES-CCM-32	Encryption and 32 bit MAC

Message authentication is carried out by cipher block chaining with message authentication code (CBC-MAC). Message authentication code is created using block cipher in CBC mode over the entire data packet including the length of the authenticated data. The detailed description of this process is included with the IEEE 802.15.4 standard itself. Depending on the level of security required, it is possible to select 128, 64 or 32 bit message authentication codes within this mode.

AES-CCM mode provides both authentication and encryption for better security. This mode of operation requires three inputs. They are namely; the data payload to be encrypted and authenticated, the associated data along with the headers to be authenticated only and nonce to be assigned to the payload and associated data.

2.4.3 ZigBee

ZigBee is an industrial consortium setup for the purpose of developing a standard data link communication layer for ultra low power wireless communications [25]. Instead of building from scratch, ZigBee standard has been built on top of IEEE 802.15.4. ZigBee network layer has been designed to work above the physical and media access control layers defined under IEEE 802.15.4 standard. The ZigBee network layer functions include mechanisms for joining and leaving a network, apply security to frames, routing the frames to the intended destination and extra security services including key exchange mechanisms and authentication beyond IEEE 802.15.4.

ZigBee specification introduces a new concept known as “trust centre” played by the ZigBee coordinator. The trust centre controls and administers other devices that are willing to join the network and distributes the appropriate key information among them. The trust centre is entrusted to play three specific roles with respect to managing security in the network. They are namely, trust manager, network manager and configuration manager. The trust manager authenticates the devices that apply to join the network. The network manager maintains and distributes the keys among the members of the network. The configuration manager’s task is to enable end-to-end security between devices.

A ZigBee enabled network can work in distinguished modes known as residential mode and commercial mode. In the residential mode, where low security application are run, only device authentication is carried out prior to joining the network. No keys are distributed in the residential mode operation persevering much of the memory for data processing operations. On the other hand, the commercial mode is intended for use in high security environments that require not only the authentication of devices but also managing the integrity of information transferred. In commercial mode, the trust centre first authenticates the devices, distributes the keys among them and maintains freshness counter for every device in the network. This enables centralized control and management of keys. Central management with a single trust centre may not scale well with large networks with hundreds or thousands of devices as the memory requirements for managing large number of keys and updating them regularly will be prohibitively high. This shortcoming can be easily overcome by dividing the network into small clusters and managing the keys locally.

ZigBee security services use three types of keys known as master keys, link keys and network keys. The master key that is installed first in the factory or out of band is responsible for long term security between devices. on the other hand link keys and network keys are basis for security between devices and the entire network respectively. The link and network keys employ symmetrical key-key exchange handshake between devices.

3 Security Challenges in Smart Sensor Networks

The nodes deployed in large wireless sensor networks are characterized by their low cost, small size and resource constraints [8]. These nodes have limited processing capability, storage capacity, communication bandwidth and range, energy and sensing range. Due to these constraints, it is not possible to employ conventional security mechanisms and algorithms in a wireless sensor network. Hence when conventional security algorithms and mechanisms are to be employed in a wireless sensor network, they must be optimized to suit the demands, limitations and the environment in which they are deployed [27]. The main limitations of sensor networks with respect to security are explained in Sect. 3.1.

3.1 Constraints in Wireless Sensor Networks

One of the main constraints in a sensor node is the limited energy available for its operations. Generally sensor nodes are powered by small cells (batteries) of limited capacity that can be exhausted in a short time, if not used wisely [7, 10]. The problem of energy consumption is exaggerated due to the fact these batteries cannot

be recharged or replaced once they have been deployed [7]. The energy in a sensor node is consumed in three main parts. They are namely the transducer, transmitter and the microprocessor. It has been found that the amount of energy consumed for transmitting one bit of information is equal to about executing 800–1000 lines of codes in the microprocessor [28]. Hence it can be seen that transmission is much more expensive than processing in a sensor node. When security mechanisms are implemented in traditional manner, they result in the expansion of the messages due to the redundant bit added by the security mechanism. This is very costly for implementation in sensor networks in terms of energy consumption.

Limited storage and memory capacity of sensor nodes is another constraint in wireless sensor networks. The storage area in a sensor node generally consists of flash memory and volatile Random Access Memory (RAM) [29]. The flash memory is used for storing permanent information such as operating system and programme codes, while the RAM can hold the programme codes currently in use, data and intermediate results. Hence the memory of a sensor node hardly has any space in its memory for holding and executing complex security algorithms and applications.

Since the sensor nodes and communication paths are affected by various environmental conditions, the communication in a wireless sensor network may not be as reliable as in a wired network. Due to the less overhead associated with connectionless communication protocols, they are commonly employed in wireless sensor networks [30]. The connectionless communication protocols are inherently less reliable. This reduced reliability in communication provides a haven of opportunity for attacks like sink attack, denial of service attack etc. Packet errors and loss will also play a big role in reduced reliability of these communication paths. Due to the higher error rates and employment of connectionless protocols will further demand error detection and correction mechanisms embedding additional bits further reducing the amount of space available for security implementations.

The other major issue confronting the communication in wireless sensor networks in large latencies from source to destination [26]. Higher latencies in communication path is the result of low bandwidth connections, network congestion, multi-hop communication and processing in intermediate nodes. Higher latencies result in loss of synchronization that is essential in many security implementations such as distribution of cryptographic keys, critical event reports etc. Loss of synchronization may also help attackers engaged in replay attacks where time stamping and timely delivery play an important role in containing these attacks.

Sensor networks use broadcasting as the common mode of transmission instead of directed communication [6]. Broadcasting helps nodes transmit the data to all the neighbours enabling the nodes to find the available end to end path even in the case of unavailability of some nodes on the way. Broadcasting can be easily exploited by adversaries for eavesdropping sensitive information with relative ease. Broadcasting can be used by adversaries to transmit commands and data to nodes by capturing a single node in the network, even if the transmission is secured by a pre-deployed global key.

Many wireless sensor networks are deployed in remote areas where the nodes are left unattended and managed remotely [31]. This increases the likelihood of physical tampering by attackers. Such physical tampering is more difficult detect as well almost impossible to stop due to the remoteness of the implementations. This type of node capture attacks are very serious in nature as compromising the security of a single node can pollute the entire sensor network [6].

Every node in a network must be installed with complete security as any node can be the target of an attack [7]. This demands that the security must pervade every aspect of the design of wireless sensor network design as any component left without security will be easily exploited by an adversary. This is high level of security implementation compared to traditional security implementations in conventional networks [32]. High level of security implementation requires more resources and time to implement making the deployment of wireless sensor network more expensive.

Wireless sensor network protocols heavily depend on application scenarios [33]. Hence generic security mechanisms need to be customized to suit each and every application domain. This puts a heavy burden on application developers and increases the application development cost. If the customizing operation is not carried out taking all the aspects into account or any aspect was overlooked, it may create security threats. Also this kind of mass customization makes it difficult to identify the bugs that can be exploited by the adversary as every implementation is different from each other.

3.2 Types of Attacks

This section briefly describe the possible security threats to wireless sensor networks. With the increase of popularity and development of wireless sensor networks, the number and types of threats and attacks carried out on these networks have also increased [7]. Many of the attacks have been identified and described in [34]. These attacks can be broadly categorized into four main groups. They are namely, attacks against the privacy of network, denial of service attacks, impersonation or replication attacks and physical attacks [7].

Some of the most common attack types are described below:

Selective forwarding: Selecting forwarding involves a malicious node dropping certain messages intentionally, while forwarding only a subset of messages it receives. The malicious node that carries out this kind of attack becomes a preferred intermediate node for unsuspecting source nodes as the forwarded messages undergo low latencies faking a shorter route. The impact of this attack depends on two main factors such as the location of the adversary and the number of packets dropped. When the adversary is closer to the base station, it will attract many more frames that it would normally do, if located far away. More the packets dropped higher the energy saved, as the transmission of packets requires a lot of energy. Hence the malicious node can stay alive longer than a normal node perpetuating its attack.

Sinkhole attack: Also known as black hole attack is where a malicious node attracts the traffic towards a compromised node. Generally this kind of attack is carried out faking a base station by a malicious node. A network with a single base station is more susceptible to this kind of attack.

Sybil attack: In this kind of attack, a malicious node presents multiple illegitimate identities to unsuspecting nodes. The identities presented by a node could be either fabricated ones or stolen from legitimate nodes or both. Once a node assumes many identities, it can launch many different types of attacks such as negative reinforcement, stuffing ballot boxes of a voting scheme such as trust computing etc. Sybil attacks are generally carried out against routing algorithms and topology maintenance.

Wormhole: In wormhole attacks, an adversary placed close to a base station channels the traffic over a low latency link. This effectively creates a sink hole completely disrupting the traffic.

HELLO flood attack: In this attack, the malicious node broadcasts a HELLO message with strong transmission power pretending to be coming from the base station. The nodes receiving this HELLO message would respond to them effectively wasting their energy. The other effect of this kind of attack is that the unsuspecting nodes would forward their messages to this malicious node falsely assuming it to the base station.

DoS attack: Denial of service attacks on a wireless sensor networks can be carried out using various techniques. At physical level, radio jamming by transmitting a more powerful signal on the same frequency or exhausting the battery power are common methods. At other level, the legitimate traffic can be diverted from the intended node or illegitimate traffic diverted towards a genuine node effectively making it unavailable for legitimate traffic.

Traffic analysis attack: It is possible to identify the location of the base station by closely monitoring the network traffic patterns. If an adversary can compromise the security of the base station, the entire network would be affected.

Node replication attack: This attack is carried out by copying the identity of a legitimate network node by a malicious attacker node. The results of this attack would be corrupted, misrouted or deleted packets.

Eavesdropping: Since wireless sensor networks generally employs broadcasting as the mode of communication, it is possible for a malicious node to gather all the information transmitted in the network, if they are not encrypted. Eavesdropping could also be the first step in a more powerful and serious attack such as wormhole or sink hole attack.

Tampering: Since the wireless sensor nodes are generally left unattended in remote locations, it is possible for adversaries to physically tamper them compromising all the security implementations.

Table 2 summarizes and classifies the attacks discussed above into different layers of a communication stack based on where they can possibly be effected.

Table 2 Senor network attack classification

Layer	Type of attack
Physical layer	DoS—jamming, tampering
	Sybil
Data link layer	DoS—collision, exhaustion, unfairness
	Interrogation
	Sybil—data aggregation, ballot stuffing
	Node replication
	HELLO message flood
Network layer	DoS—flooding, spoofing, sink holes
	Sybil
	Wormhole
	Traffic analysis
	Selective forwarding
	Node replication
	HELLO message flood
Transport layer	DoS—flooding, desynchronization
Application layer	DoS—flooding, diversion
	Eavesdropping

4 Security of Smart Sensor Nodes

Generally wireless sensor networks are implemented in remote locations for monitoring various things including the environment, enemy movements in military applications etc. [35]. Compared to conventional network devices, wireless sensor nodes are more susceptible to attack as they are physically accessible by adversaries [7, 8, 34]. Once a sensor node is physically tampered with, the entire security implementation in the node including the cryptographic keys can be compromised. Hence physical security of sensor nodes is of utmost important. Since it is nearly impossible to protect the nodes from physical tampering by adversaries, many schemes have been developed for detecting malicious or tampered nodes and isolating them. This section takes an in depth look at some of the prominent malicious node detection schemes reported in the literature.

4.1 Threats to Wireless Sensor Nodes

Compared traditional network nodes, wireless sensor network nodes face several additional threats due to the very nature of their implementations. Generally, wireless sensor network nodes are located in open space that can be considered as insecure and hostile [8]. When an environment is considered to be insecure or hostile, generally the physical security in the area is beefed up with various special

mechanisms such as perimeter security through the implementation of security cameras, personnel and policies. But, due to the open nature of the wireless sensor network implementation, the above mechanism cannot be implemented as it is.

The main threats faced by the wireless sensor nodes deployed in the open area are tampering, theft and physical destruction [8]. These attacks can cause irreversible attacks to the nodes and sometimes to the entire network if not handled properly and curtailed at the beginning itself.

Tampering involves the modification of the sensor from its normal operation. An adversary can get hold of the cryptographic keys installed in the nodes, when he gets physical access to the nodes easily compared to attacking the nodes remotely or through data analysis. Also the attacker can now alter the physical hardware including circuitry and wiring or modify the program code as he wants. In the worst case, the entire sensor node can be replaced with malicious sensor node itself.

Theft and physical destruction of sensor node make them totally unavailable for use by authorised users. Both these attacks fall under the denial of service attacks as they deny the genuine user from using these nodes and getting the intended services from them.

4.2 Security Schemes for Protecting Wireless Sensor Nodes

Since wireless sensor nodes have been installed outdoors open to both genuine and malicious users on the whole, it is difficult or many a time impossible to protect them from the physical damages caused by malicious attackers. Installing the sensor nodes more densely than needed may reduce the impact of theft or physical destruction to the nodes [6, 7]. On the other hand, when a node is tampered with, it must be detected, identified and isolated from the network. Many schemes, mechanisms and protocols have been proposed in the literature for identifying misbehaving nodes. This section takes in detailed look at some of the important mechanisms for identifying and isolating them reported in the literature.

Zia and Zomaya [34] have presented a malicious node detection mechanism based on monitoring its own message retransmitted by a neighbouring node in transit. In this mechanism, the source node first forwards the message to one of its neighbours for the purpose of routing it towards the base station. Once the transmission is completed, the source node converts itself to monitoring node actively observing the retransmitted message by the neighbour. If the retransmitted message resembles the original message, the monitor terminates its task and continues with its normal operations. If the retransmitted message differs from the original message, it updates the locally maintained node suspicious table. Once the number of entries for a node in its suspicious table goes beyond a predefined threshold, it informs its neighbours about the suspicious node. The neighbours then respond back to this message with their own opinion based on their observations. When the suspicious entry for a given node increases beyond a threshold, it is then informed to the cluster head. Cluster head will then isolate the suspicious node as malicious

barring all the members from communicating with it and dropping all the messages from the identified malicious node in the future. This mechanism looks robust as node monitors its own message being retransmitted for identifying a malicious node. This mechanism has two main drawbacks. First all the nodes must use the same "link key" for encrypting the message. If different node pairs use different link keys for encrypting the message, it is not possible to identify the modification of the message just by observing the retransmitted message. In such a situation, this mechanism totally fails. Second, this mechanism is prone to collusion attacks, as the opinion of neighbours about a suspected node are taken in without any further inquiry or clarification, the neighbours may collude to promote or demote a neighbouring node as a genuine one or malicious one. Hence robustness of this mechanism is questionable.

In Baburajan and Prajapati [36] have proposed a watchdog mechanism to identify malicious nodes in a wireless sensor networks. Similar to the node detection mechanism proposed in [34], the watchdog mechanism also depends on the broadcast nature of communication in wireless sensor networks. As opposed to the mechanism proposed in [34] where the transmitter itself acts as the monitor listening to the transmission from the intermediate node, in the watchdog mechanism all the nodes who can hear both transmissions can act as the monitors. The identified limitations of the watchdog mechanism include; ambiguous collision, receiver collision, limited transmission power, false misbehaviour and partial dropping. Some of the shortcomings of the watchdog algorithm has been solved by improved algorithms. By creating a cluster head and making it the first level watch dogs can help solve impartial removal, false malicious node, limited power and node conspiracy. Receiver collision problem can be solved by enabling a collision detection mechanism. But this mechanism may not solve the ambiguous collision problem.

Nakul [37] has reviewed several intrusion detection mechanisms that can effectively identify the misbehaving nodes in wireless sensor network. Node misbehaviour in a network may indicate the presence of compromised nodes or malicious nodes introduced by the adversaries or corrupted nodes due to external factors. Irrespective of the reason for misbehaviour, the misbehaving node must be identified and removed from the network. The methods reviewed in [37] include weighted trust evaluation approach, ant colony based approach, data mining based approach, agent based approach, trust based approach, weak hidden Markov model based approach neighbour based approach, game theory based approach and hybrid approach. Details of some of the important approaches are discussed below.

In weighted trust evaluation the sender node assigns trust scores to other nodes in the cluster based on its experience with those nodes. When an intermediate node forwards the frame correctly, its trust score is enhanced. On the other hand, when the forwarded frame does not match the original frame, its trust score is decremented. This algorithm is simple to implement and based on two strong assumptions. They are the base station is honest or not compromised and the majority of nodes in a network are well behaved. This algorithm would fail, if any of these assumption is violated.

In data mining approach applied to the detection of anomalous behaviour of nodes checks all the data packets transmitted in the network. This method has very good detection rate but suffers from the limitation that it requires a lot of processing power and energy to run the data mining algorithms in real time. The main advantages of this method are its ability to detect the anomalous packet before it reaches the access point, to start the detection process immediately without needing any prior training and higher detection rates.

The agent based anomaly detection mechanism employs a combination of both rule based scheme and naive Bayesian technique. This mechanism shows good performance in large distributed sensor networks using common anomaly detection framework with agent learning and distributed data mining techniques.

The trust based approach combines social trust and QoS trust for computing the trust worthiness of a node. Honesty has been used as the parameter for social trust while energy and cooperativeness are the attributes used for computing QoS trust. The final trust score is used for identifying the malicious nodes in the network. The cluster head assigns the trust scores to all the members within the cluster and the cluster heads are similarly evaluated by the base station.

In the weak hidden Markov model based anomaly detection mechanism, state transition probabilities are reduced to rules of reachability. This is a two stage mechanism where in the first stage, the training and learning takes place and in the second stage real time detection of intrusion is carried out. The scoring scheme and deviation detection mechanism introduced as enhancements improves the detection accuracy.

The neighbour based approach exploits the similarity of behaviour in a given community. It is assumed that all the neighbouring nodes in a sensor network would behave similarly due to the fact that they all face similar conditions and limitations. If any node deviates from the common behaviour of its nodes, then it is identified as a malicious node. This approach has better detection rates when the neighbours cooperate with each other with very low false positives and negatives.

The game theory based intrusion detection scheme makes use of a signalling game to model the interaction between nodes in a wireless sensor network. In this mechanism, the interaction between an attacker and a normal has been modelled as a Bayesian game with incomplete information.

In Li et al. [38] have presented survey on methods for detecting node replication attacks in wireless sensor networks. When a sensor node is physically captured by an intruder, it is possible to capture all the information stored within the node. Then he duplicates this node along with inserting his malicious code and then plants them in many strategic locations within the network. The methods presented in [38] include Node to node broadcasting (N2NB), Deterministic Multicast (DM), Randomized Multicast, Randomized, Efficient, Distributed mechanism (RED), Memory Efficient Multicast (MEM), Randomly Directed Exploration (RDE), Distributed detection of node capture attacks, Zone and based Replica Detection, Out of these schemes, some of the important mechanisms are described below.

In node to node broadcasting, every node broadcasts an authenticated message claiming its own location throughout the network. Each node stores the location claim of its neighbours. When a conflict was detected in location claim, the malicious node is revoked immediately. Since the messages from every node in the entire network needs to be processed by every other node, the storage, message and communication cost are high in this scheme. The directed multicast is an improved version of N2NB. In directed multicast, claimer-reporter-witness framework is fully exploited to detect the malicious node efficiently. The claimer shares its location claim to its neighbours and the neighbours act as the reporters. The reporters select a witness using claimer's ID and a function. Then the reporter forwards the claimer's location claim to the witness. If a witness receives multiple claims for the same location, it would then trigger the duplicate node revocation mechanism. This mechanism suffers from one main shortcoming. When an adversary knows the claimer's ID, then it can compute the location of the witness. Hence the adversary can compromise both the claimer and the witness before deploying the malicious node in the network.

Distributed detection of node capture attacks exploits the fact that when a node has been physically captured by an adversary, it will be dormant for a period of time. This protocol measures absence time period of nodes and compares it with a predefined threshold. If the period of absence is more than the threshold value, then it is declared as a compromised node. The effectiveness of this protocol depends on the threshold value.

In Virmani et al. [39] have proposed an exponential trust based mechanism to detect black hole attack in wireless sensor networks. In this mechanism every node maintains a tables and a streak counter in its memory. The table maintains the trust factor of other nodes and the streak counter measures the number of consecutive packets dropped by that node. The trust factor starts with 100 and the streak counter with zero (0) incremented by 1 for every consecutive drop. The streak counter is reset to zero (0) whenever it forwards a packet to the next node. The trust factor for each consecutive drop is computed using the formula $100 * x^i$ where x is a factor less than 1 and i the number of consecutive packets dropped. Since black holes (sinkholes) would be continuously dropping all the packets they receive, their trust value would fall drastically with few packets dropped. This would help identify the sinkholes very fast.

Lim and Choi have proposed malicious node detection mechanism using dual threshold method [40]. In this mechanism two different threshold values are maintained, one for event detection accuracy and the other one for false alarm rate along with trust values for each neighbour in the network. This helps improve the detection of malicious nodes without increasing the overhead.

In Atakli et al. [41] have proposed a weighted trust evaluation to identify malicious nodes by monitoring the reported data. In this work, initially the network is divided into three main groups creating a hierarchical architecture. At the top of the network there are access points or base stations followed by the middle layer occupied by the high powered forwarding nodes. At the lowest level are the low

powered sensor nodes with limited functionality. The sensor nodes re organized around high powered forwarding nodes as cluster heads and communicate only with those cluster heads. Only the forwarding nodes have the multi-hop routing capability and assumed to be trustworthy and cannot be compromised. The sensor nodes within the control of a forwarding node are given a weight with 0 and 1 based on its prior behaviour. The forwarding node computes an aggregation results from weighted average of the information received from the sensor nodes within its control. Whenever the reported information of a sensor node deviates from the aggregation results, its trust value is decremented. When the trust value of a given node falls below a pre-decided threshold, it is identified malicious and removed from the network.

In Junior et al. [42] have proposed a malicious node detection scheme through traffic monitoring. In this scheme, all the nodes are considered equal in every sense and communication between the nodes is symmetrical. Every node in the network transmits its node id and the location coordinates obtained from the GPS system. Every node could compute the theoretical received signal power given the identical nature of nodes and the inter-node distance obtained from the location coordinates using the two-ray signal model. When the received signal power is different from the computed theoretical value, the suspicious count maintained in the memory is incremented, otherwise, unsuspicious count would be incremented. When a suspicious message is detected by a node, it transmits the message of suspicion with the id of the suspicious node. Whoever has received this message of suspicion and the original transmission may reply back their opinion based on their own calculations. Then all the nodes within the reach of these nodes updates their opinion (suspicious and unsuspicious) tables based on the opinion received. When the ratio between the suspicious to unsuspicious messages received increases beyond a preset threshold value, it is named malicious and removed from the network.

5 Security of Data in Smart Sensor Networks

Similar to any other network, the data transmitted over a wireless sensor network must also be protected [8]. For any data to be considered as secure, it must satisfy the three security primitives known as confidentiality, integrity and availability. When any of the above security primitive is breached then the security of the data is considered as breached. The confidentiality ensures that only the intended recipient has access to the data and no one else. When data is transmitted over a large network, it may go through many intermediaries before it reaches the final recipient. All the intermediaries must only forward the data towards the recipient but should not be able to read or understand what is in it. Eavesdropping is an attack confidentiality of data. Data integrity assures the recipient that the data received has not been modified or tampered with en-route. In addition to data security, it is also important to ensure source integrity. Source integrity means the data must really be originated by the node where it is claimed to be originated. Impersonation is an attack on source integrity.

Availability is the capability to access the data on a timely fashion, when required to the authorised user. Denial of service is an attack on the availability of data as it prevents the authorised user from accessing the data. This section takes an in depth look at data security in wireless sensor networks. This section takes a detailed look at the prominent work carried out for protecting data in wireless sensor networks.

5.1 Threats to Data in Wireless Sensor Networks

The threats to data collected and transferred in wireless sensor network are not uniform and depends on the type of application [6]. For example, the data collected in a agriculture farm with the aid of a wireless sensor network only requires integrity checking against intentional or unintentional modification. On the other hand, in a military application, the data must be protected for all the three types of security requirements. Namely, confidentiality, integrity and availability [7].

The information transmitted over the wireless channels of a sensor network could be monitored [7]. This is commonly known as eavesdropping. Eavesdropping is a passive attack on the data and can be carried out very easily on a wireless sensor network as the common mode of communication employed in a sensor network is broadcasting. Eavesdropping may not be considered a big issue for many applications such as environmental monitoring or machine health check monitoring in industrial applications. On the other hand, military and medical application require higher security implementation against disclosure of information to unauthorised persons [7]. In military surveillance applications, the information on enemy movements and others of strategic importance are captured and transmitted via a wireless sensor network. If this information falls into the enemy's hand, the consequences would be very serious. Hence it must be protected with the highest level of security available. Similarly, in remote health monitoring applications, the patient information is required to be protected by law. Thus, healthcare applications also require high level security ensuring confidentiality of data. The data confidentiality can be assured by implementing the proper encryption depending on the requirements.

Data injection is another type of attack that can be carried out in a wireless sensor network [7]. Data injection is wrong information introduced into a network by malicious or compromised nodes. Data injection is an active attack where the malicious node actively participates in the network activities. Data injection is more dangerous than eavesdropping as it can affect all types of sensor network applications. Solutions to the issue of data injection is the identification of the malicious node and removing it from the network.

Data modification or corruption is an attack on the integrity of data [7]. Data corruption can happen due to activities of malicious nodes or due to external interferences such as noise. Irrespective of the reason, data corruption must be detected and corrected. Data corruption can be detected using simple hash functions appended to the data or through complicated double encryption techniques [6]. The corrupted packet is generally recovered through retransmission.

Packet deletion in a wireless sensor network may happen due to unintentional dropping of packets as a result of a shortage of resources such as buffer space in a node or a malicious attack such as sinkhole attack and selective packet forwarding [7]. The loss of packets are detected using sequence numbers added to the headers. Unintentionally dropped packets can be recovered through retransmission and if there is a malicious attack on the network, the rogue nodes responsible for the attack must be removed.

Misrouting of packets happen when packet headers get corrupted or due to an active attack on the routing process [7]. If an active attack takes place, the nodes responsible for the attack must be detected and removed. Both packet deletion and misrouting are attacks on the availability of network resources.

5.2 *Mechanisms for Protecting Data in Wireless Sensor Networks*

Data security in a wireless sensor network is carried out through implementing the right level of encryption of data based on the requirement [6]. For the encryption to be successful, proper distribution and management of keys is a critical requirement [34]. Due to the resource constraints in sensor networks, the conventional key management schemes used in traditional networks cannot be used in wireless sensor networks due to their high overhead and the involvement of external parties [8, 34]. Hence the cryptographic schemes employed in a wireless sensor network must be evaluated to meet the constraints in terms of code size, data size, processing time and power consumption [8].

As public key cryptography has been found to be too expensive to be implemented in a wireless sensor network, many researchers have focussed their attention on secret (symmetric) key cryptography for implementing security in such a constrained environments [8]. When symmetric key cryptography is used, the key management in an open environment becomes a critical issue. In symmetric key cryptographic mechanisms use the same key for encryption as well as decryption. Hence it is essential to transfer the key to the receiver confidentially without the knowledge of the adversary. Also the key management scheme must be capable of handling the addition of new nodes and the removal of existing nodes from the network [8].

Key management schemes can be broadly divided into centralized and distributed key management schemes [8]. In centralized key management, a single node probably the base station carries out all the tasks pertaining to key management including generation, regeneration, distribution and revocation. This single node is known as the key distribution centre. The main shortcomings of this scheme are single point of failure and scalability. On the other hand, in distributed key management schemes, the responsibility of the administration of key is distributed among multiple nodes effectively eliminating the single point of failure and providing better scalability. The distributed key management schemes may use either deterministic or probabilistic distribution algorithms [8].

A key distribution issue can be decomposed into the following steps [34]:

- Key pre-distribution—installing the key in a node prior to deployment.
- Neighbour discovery—discovering the nodes that are just one hop away.
- End to end path key establishment—end to end communication with nodes that are not directly connected.
- Isolating misbehaving nodes—identifying and isolating damaged or malicious nodes.
- Key establishment latency—reducing the latency resulting from communication and power consumption.

Perrig et al. proposed a suit of security protocols for wireless sensor networks in 2002 called SPINS [43]. Within this suite is a secure network encryption protocol (SNEP) that provides confidentiality, integrity and freshness of data through the use of encryption and authentication. The main features of this protocol include the low overhead per message, managing state at every node eliminating the need for transmitting counter values and semantic security. The SNEP also enhances the security of encryption by preceding the data to be encrypted by a random sequence effectively countering the known plain text attack that can be carried out by an attacker. SNEP communicating nodes derive their keys from a shared master key using pseudorandom function. A secure authenticated message using SNEP would be as given in Eq. (2).

$$A \rightarrow B : \{D\}\{K_{AB}, C_A\}, MAC\left(K'_{AB} C_A \parallel \{D\}\{K_{AB}, C_A\}\right) \tag{2}$$

where A and B are the communicating nodes, D is the data encrypted with derived key K_{AB} and counter value of A; $A; C_A . MAC\left(K'_{AB} C_A \parallel E\right)$ is the message authentication code computed using K'_{AB} the derived key for MAC operation and E the encrypted message.

TinySec is an improved version of SNEP where access control and message integrity are provided through authentication, confidentiality through encryption and semantic security through the use of a unique initialization vector for each invocation of the encryption algorithm [44]. TinySec comes in two specific variants; TinySec-Auth and TinySec-AE. TinySec-Auth provides only authentication using a message authentication code and the payload is left unencrypted. TinySec-AE provides both authentication through the message authentication and encryption of the payload. In TinySec replay protection is not included, hence it must be carried out by a higher layer protocol, if necessary.

Security manager is a method of authenticated key agreement based on public key infrastructure and elliptic cryptography for low rate wireless personal area networks [45]. The security manager gives the static domain parameters such as the base point and elliptic curve coefficients to prospective nodes which use them to establish permanent and ephemeral public keys. Every node in the network computes its own public key and sends it to the security manager which maintains them in its memory. Elliptic curve algorithms provides reasonable computational loads and smaller key

sizes for equivalent security compared to RSA the traditional method for public key cryptography. The authenticated key agreement is achieved via security manager based on RC-MQV algorithm that is more advanced than Diffie-Hellman algorithm. RC-MQV is resistant to man in the middle attack, hence security manager is a very robust technique against all known attacks on data in wireless sensor networks as long as the security manager is not attacked and compromised.

In [46], Soroush, Salajegheh and Dimitriou have proposed a strong post deployment key management protocol that is flexible, scalable and robust against node capture attacks. This is a triple key mechanism consisting of pair-wise key, broadcast key and node-base key. Pair-wise key that is established between two neighbours protects their direct one-to-one communication, broadcast key secures the messages sent between neighbours and node-base key protects the communication between a node and the base station. The first step in the operation of this mechanism is the node discovery. Node discovery is carried out through a ping-pong handshake message exchange between neighbours. Once all the neighbours have been discovered, a node will compute its own node-base key and its pair-wise keys and broadcast keys as given in Eq. 3.

$$\left.\begin{aligned} NB_i &= F(i \parallel \textit{base station address} \parallel K) \\ PW_{i,j} &= F(min(i,j) \parallel max(i,j) \parallel K) \\ BC_i &= F(i \parallel K) \end{aligned}\right\} \tag{3}$$

where i, $\parallel$, F and K are the node id, concatenation operator, secure pseudo random function and pre-installed global master key respectively.

Secure pseudo random function is implemented using a hash function SHA-1 or MD5. The global master key (K) can be deleted from the memory of nodes later protecting them from falling into enemy hands in times of node capture attacks. Once the calculations are over, node i would be having a complete set of keys for node j. But, node j does not have any information about node i, as it must be sent from i. Node i would then create a message M containing the pair-wise and broadcast keys and encrypt that message with a node-base key derived as follows.

$$NB_j = F(j \parallel \textit{base station address} \parallel K)$$

After sending this message, node i will delete the node-base key of node j from its memory leaving only node j capable of decrypting this message. Then global master key K will also be deleted from the memory of node i. The above steps can be followed by a new node when getting added to the network if comes with the pre-installed global master key K. This makes the network resilient to node capture attacks or introduction of malicious nodes by an intruder as he will not have access to K.

The Distributed ANGEL Key Agreement (DAKE) is a direct distributed key establishment based on keying material stored on the nodes [47]. This is an α-Secure Key Establishment process, where α-secure refers to the system that resists the collision up to α entities. Some α-secure keying material KM_{root} stored at a secure

location is used to generate an α-secure keying material share KM_i for each entity i in the system. In a typical system, a single symmetric bivariate polynomial $f(x, y)$ of degree α over a finite field $GF(q)$ where q is large enough to accommodate a cryptographic key can be used as KM_{root}. Each entity in the network receives its polynomial share $f(i, y)$ generated by evaluating the original symmetric bivariate polynomial in $x = i$. Two entities in the network (i, j) can agree on a pairwise key by evaluating their respective polynomial shares in the identity of other party as shown in Eq. 4.

$$K_{i,j} = f(i,y)|_{y=j} = f(j,y)|_{y=i} \tag{4}$$

In DAKE, key segmentation and Horner's rule are used to break the large into multiple sub-polynomials and reduce the number of multiplications by factoring out.

The Modular Architecture for the Security of Sensor Networks (MArSSeNs) is a complete framework of security tools that can provide transparent security individually to all the data streams and network layers of applications in a wireless sensor network [48]. The advantages of MArSSeNs include the implicit and transparent security at any layer of network stack and data stream without requiring changes to application code, elimination code complexity and reduction of errors compared to hard-coded security and facilitation of configuration at both compile as well as run time. MArSSeNs provides in-depth key management and allows distinction between session keys (short term) and encryption keys (long term), using different keys for every service in a data stream policy, controlling maximum key

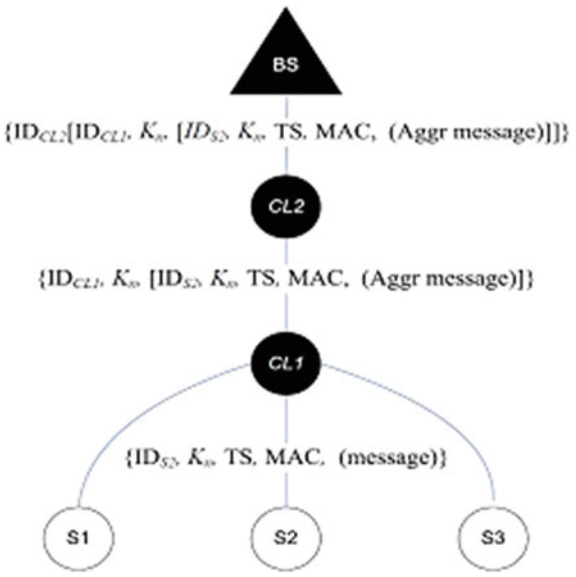

Fig. 2 Key calculation for sensor node S2 up to base station BS [34]

usage and facilities for key establishment, renewal, derivation and revocation. The MArSSeNs key manager administers the key database, key life cycle and key management protocols where needed. MArSSeNs supports third party protocols through a set of interfaces. For non supported key types, it is possible to implement a sub key manager to handle all the tasks.

The secure triple key management scheme proposed in [34] consists of three keys. Two of these keys namely the network key and sensor key are pre-installed in all nodes and the other key is the network generated cluster key addressing the hierarchical nature of the network. The network key is used for encrypting data and pass it to the next hop, the sensor key is used by the base station to decrypt and process it while the cluster leader uses it for decrypting and passing the data to the base station and the cluster key is used for decrypting data and passing it to the cluster leader. Figure 2 shows the key calculation process at different levels.

6 Routing Security in Smart Sensor Networks

Wireless sensor network is a infrastructureless multi-hop network, where the transfer of data takes place by forward from one node to another. In such a network, routing plays an important role in carrying the information from the source to destination [49]. The routing protocols employed determines the best route to transfer the data from the source to destination possibly the base station.

The routing protocols in wireless sensor networks can be grouped into three main categories according to the network structures [8]. There are namely (i) flat-based routing, (ii) hierarchical-based routing and (iii) location-based routing. In flat-based routing, all nodes are considered equal and assigned similar roles, in hierarchical routing, nodes are assigned different role and in location based routing, the geographical location of the nodes are used for routing data in the network.

Many parameters of a wireless sensor network including the end-to-end delay, packet delivery ratio, life time of the network etc., depends on the performance of the routing protocol [49]. Due to the nature of wireless sensor networks, the routing protocols may employ different criteria for selecting best path such as low energy consumption path or least hostile path compared to traditional network where the shortest path or the least congested path is generally selected as the best path [50].

The routing protocols in a wireless sensor network is also vulnerable to several attacks [49]. The attacks carried out on routing protocols have severe consequences due to the self contained and self configuring nature of the network itself. In order to overcome these threats, several secure routing protocols have been proposed in the literature [49]. This section takes an in depth look at the security threats for routing and the mechanism proposed for overcoming them.

6.1 Threats that Affect Routing in Wireless Sensor Networks

There are several attacks that directly target the routing protocols for disrupting the traffic in a network [8]. The attacks on a routing protocol may create routing loops, attracting or repelling traffic from a selected set of nodes, extend or shorten source routes, generate fake error messages, partition the network or extend the end to end delay. Some of the most common attacks on the routing process are described below.

Spoofed routing information: This is direct attack against a routing protocol targeting the routing information. Routing protocols require exchanging routing information between nodes for building a routing table with the most current status of the network. The routing table must be up-to-date with the status of nodes as this information is used by nodes to identify the best path to the destination. An attacker may spoof, alter or replay routing information effectively disrupting the traffic flow in a network. This attack may lead to many problems such as routing loops, increased end to end latency and even network partitioning [50].

Sinkhole attack: In this attack, a malicious node has been shown as the most attractive next hop node to forward the packet towards the destination. Once a packet reaches the malicious node, it is dropped instead being forwarded.

Sybil attack: A single node presents itself with multiple identities which are either stolen ones or fabricated ones. When a Sybil attack has been carried on routing, it makes multiple routes to go through a single compromised node effectively delaying or dropping packets en-route.

HELLO flood: Many routing protocols assume that the HELLO messages come only from a neighbouring node. A malicious node with a high powered transmitter may fool many nodes as it is within their neighbourhood effectively announcing a false shorter route to the base station. All the nodes receiving this HELLO message would try to forward the packets to this malicious node though it is outside their range.

Acknowledgement spoofing: Some routing algorithms require the transmission of acknowledgement messages for proper operation. A malicious node eavesdropping on the conversation of other nodes may spoof their acknowledgement packets. This disseminate wrong information about nodes.

6.2 Secure Routing Protocols

In order to overcome the threats and attacks on routing, many researchers have proposed secure routing protocols that can withstand these attacks. Many of these protocols make use of cryptographic primitives and authentication mechanisms to minimize the effects of attacks, while others make use of trust between nodes identify the malicious or compromised nodes.

In Duan et al. [49] have proposed a lightweight and secure routing scheme. This scheme makes use of trust computed between nodes to identify the best path to the destination. The routing algorithm and the operation of the scheme is as follows:

Step 1: When the node v_0 wants to send a packet to v_{11}, which is not its neighbour, it sends a trust request packet to its neighbours. A trust request is a 6-ary tuple and is denoted by $TR = s_{id}, t_{id}, t(p)_{th}, ts, s, hl$, where $s_{id}, t_{id}, t(p)_{th}$, ts, s *and* hl are source and destination node ids, threshold of path trust, timestamp, sequence number and hop limit of trust request packet respectively.

Step 2: A neighbouring node receiving this request will check, if the destination node v_{11} is in its neighbour list. if yes, it replies to the request with the trust value of the destination hop, else it broadcasts the requests to all its neighbours. All the neighbours who initiated the process would process this request.

Step3: This process continues until the request reaches a node in whose neighbour list the destination is found. Then the reverse process initiated through the selected path (through which the request came) with the trust value of path until the original requester node v_0.

Step 4: The originator evaluates the paths received, if more than one is received and selects the path with the highest trust.

Step 5: v_0 forwards the data packet through the selected path.

The routing algorithm and operation of the scheme are shown in Figs. 3 and 4 respectively.

The lightweight secure routing scheme may not be as secure as it has been claimed to be and come under many attacks when there are malicious nodes in the networks. The best path selected purely depends on the trust scores transmitted by intermediate nodes. This can be exploited by the adversary to mislead the requester to select non optimal paths, worse sometimes towards sinkholes. If the malicious nodes collude, the effect would be worse.

Ambient Trust Sensor Routing (ATSR) proposed by Zahariadis et al. [51] follows the geographical approach. The main criteria of the next hop selection in this mechanism is the geographical coordinates along with the remaining energy and trust value of the node. The combination of the multiple input parameters make the protocol more rugged and help lengthen the life of the network by not exploiting the best (having highest score) node as it might drain their battery very soon. The trust computation process takes many criteria including packet forwarding efficiency, network layer acknowledgements, message integrity, node authentication, confidentiality, reputation response and reputation validation as inputs making it a very comprehensive process and less vulnerable to attacks by an intruder that provides false information. The energy computation mechanism is the weakest link in the process. Since the remaining energy is expressed as a percentage of original energy, if all the nodes are not of the same capacity, this information may mislead the nodes to select a node with lower level of absolute energy when better nodes with large energy levels are present in the network.

Secure routing mechanism proposed in [34] uses only the cluster heads to forward the encrypted data towards the base station. The routing protocol is divided

(1) Process Initialization
(2) $G_R^*(V, E_R, r) = v_n$, v_n is the destination node
(3) Add v_n to V^*, V^* represents the set of nodes that have optimal routes to v_n
(4) **while** $V \neq V^*$ **do**
(5) **for all** node $v_i \in V - V^*$ **do**
(6) Sort $r(p(v_i, v_n))$
(7) Obtain $\vec{r}(p(v_i, v_n)) \triangleq (q_0, q_1, \ldots, q_m)$
(8) where $q_0 = t(p(v_i, v_n))$
(9) **for all** $v_k \in \Gamma(v_i)$ **do**
(10) **if** $t(v_i, v_k) \otimes_T t(p(v_k, v_n)) \succeq t(p(v_i, v_n))_{\text{th}}$ **then**
(11) Add $(v_i, p(v_k, v_n))$ to $P_{Q_0}^*(v_i, v_n)$
(12) **end if**
(13) **end for**
(14) **if** $P_{Q_0}^*(v_i, v_n) = \emptyset$ **then**
(15) v_i is disconnected from the network
(16) Continue;
(17) **end if**
(18) **for** $j = 1; j < m; j++$ **do**
(19) $P_{Q_j}^*(v_i, v_n) = \oplus_{Q_j} p_{Q_{j-1}}^*(v_i, v_n)$
(20) where $p_{Q_{j-1}}^*(v_i, v_n) \subseteq P_{Q_{j-1}}^*(v_i, v_n)$
(21) **end for**
(22) **if** $P_{Q_m}^*(v_i, v_n) = \emptyset$ **then**
(23) v_i is disconnected from the network
(24) Continue;
(25) **else**
(26) Add v_i to V^*
(27) Add $P_{Q_m}^*(v_i, v_n)$ to $G_R^*(V, E_R, r)$
(28) **return** $p_R^*(v_i, v_n), p_R^*(v_i, v_n) \subseteq P_{Q_m}^*(v_i, v_n)$
(29) **end if**
(30) **end for**
(31) **end while**
(32) END Process

Fig. 3 Lightweight secure routing algorithm

into two categories; one for sending data from a sensor node to the base station and the one for sending information from the base station to the sensor nodes.

The algorithm for sending data from a sensor node to the base station is as follows:

Step 1: Request the cluster key K_c from cluster leader.
Step 2: Use K_c and its own key K_n to compute the encryption key K_{cn}.
Step 3: Encrypt the data with K_{cn} and append its node ID and current time stamp TS and forward the packet to the cluster head.
Step 4: The cluster head upon receiving the encrypted data packet, appends its ID and forwards it to the base station, if directly connected, otherwise forwards it to another cluster head.

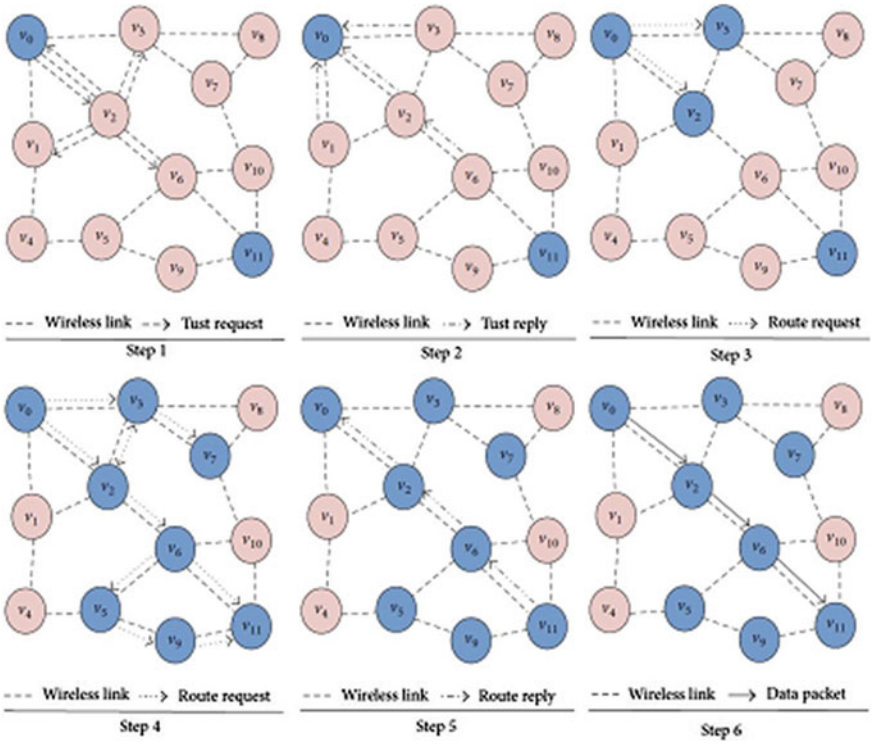

Fig. 4 Operation of lightweight and secure routing scheme

Figure 5 shows the node algorithm in detail.

When the base station wants to broadcast any data to sensor nodes, it just encrypts the data packet with sensor key K_s and forwards it to the directly connected cluster heads.

In this scheme, the cluster heads are assumed to be non-compromisable, this may not be 100 % correct. When a cluster head is compromised, the entire security of the system may fail.

Intrusion-tolerant routing mechanism in wireless sensor networks (INSENS) proposed in [52] builds routing tables in each node bypassing the malicious nodes in the network. Control information pertaining to routing is authenticated by the base station for the purpose of preventing injection of false routing data. The base station computes and disseminates the routing tables to all the nodes helping the nodes saving their energy. Redundant multi-path routing enables the nodes to overcome the sinkhole and wormhole attacks carried out by malicious nodes.

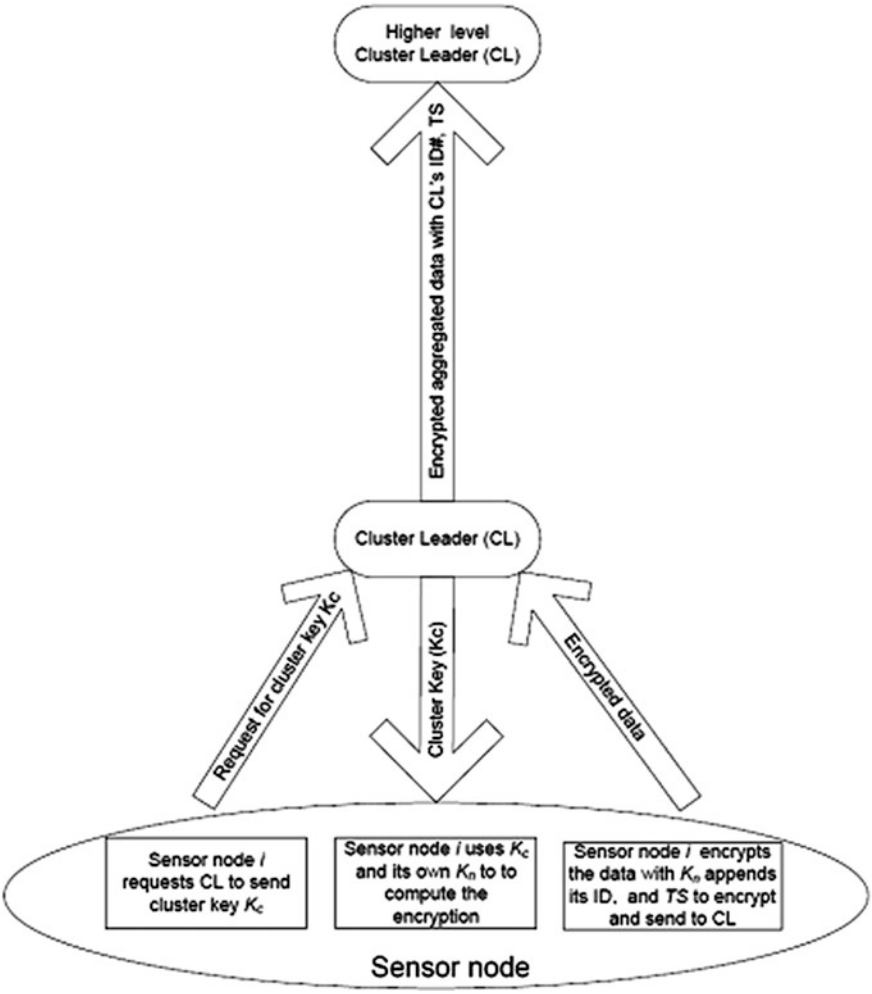

Fig. 5 Node routing algorithm [34]

The route discovery mechanism of INSENS is as follows:

Step 1: Base station sends a request message to all nodes through multi-hop forwarding.

Step 2: Nodes receiving the request message, records the identity of the sender and forwards it to their neighbours for the first time (repeated flooding not allowed).

Step 3: Nodes respond with their local topology by sending feedback messages.

Step 4: Base station calculates forwarding tables for all nodes with two independent paths for each node and disseminates them.

In this communication, the integrity of all the messages including requests and feedbacks are protected using encryption by a shared key mechanism. In this protocol, when a malicious node does not forward the message, it can reach the destination through another path. Hence the effect of the sinkhole attack is minimised, if not eliminated. The malicious nodes may also send spurious messages to drain the battery power in the downstream nodes.

Trust routing for location aware sensor networks (TRANS) proposed in [53] is a location aware routing protocol. TRANS makes use of a loose-time synchronization asymmetric cryptographic scheme to ensure message confidentiality. The operation of the protocol is as follows:

Step 1: The base station broadcasts an encrypted message to all its neighbours.
Step 2: Neighbours receiving this message, decrypt it add their locations encrypt and forwards it to its neighbours closer to the destination.

The security of this protocol is ensured by encryption. Only the trusted nodes can decrypt the messages as only they possess the shared key. The destination node authenticate the received message using the message authentication code added by the base station.

The acknowledgements and replies from the sensor nodes to the base station just traverse the reverse path through which the message arrived.

The secure route discovery protocol proposed in [54] guarantees correct topology discovery in an ad hoc sensor networks. This protocol ensures security of messages through message authentication code and accumulation of node identities along the route traversed by the message. Each node in the network discovers every other node using the node identities appended to the messages finally discovering the entire network topology. The verification of the message authentication protocol at both source and destination ensures the integrity of the messages.

The ant colony-based routing protocol proposed in [55] consists of four distinct stages in setting up a secure route to destination. In stage 1, clusters are formed based on their geographical regions. Within each region a node N and a parameter L are chosen randomly where L indicates the level of neighbours in the cluster. Using limited HELLO floods, the neighbour list exchange process starts from node N to L levels. In stage 2, cluster heads are chosen. Within each cluster formed, three nodes H_1, H_2 and H_3 are chosen randomly and their resource levels are computed. The node with the highest resource level is selected as the cluster head. In stage 3, the routing process starts. The node with data to be sent forwards its message to the cluster head. Then the cluster head sends HELLO messages along with pheromone request to its neighbouring cluster heads. The entire neighbour cluster heads reply to the request with their current pheromone values. This process is repeated until a optimum path is found to the destination. The elimination of malicious nodes in this protocol is achieved through conformity checks carried out at the end of cluster formations.

7 Future Directions in Smart Sensor Network Security

Though extensive work has been carried out in various aspects of wireless sensor networks security, there are still many open problems that need to be addressed. This section takes a brief look at the some of the open areas.

Currently security in wireless sensor network research is carried out in a fragmented manner each group concentrating on specific problems and aspects. It is necessary to have a more unified approach towards various aspects of the security in wireless sensor networks. Hence it is necessary to produce a uniform application independent security framework for wireless sensor networks.

Generally the implementation and enhancement of security affects the other aspects of sensor networks such as user friendliness and quality of service. This would normally affect the usefulness and usability of these networks. It is necessary to have security implementations that have minimal impacts on other aspects of wireless sensor networks.

hough some research has already been carried out and obtained some promising results on the use of public key cryptography in wireless sensor networks, it is still an open area. The code size, processing time and power consumption are still high for the deployment of them widely. Hence an active look into this area would be a worthwhile effort. The specific areas that can be looked at include code optimization, energy efficient computation, and optimization of private key operations.

Wireless sensor nodes are deployed in an open area that is not only harsh but also hostile. Hence the sensor nodes face several threats from natural as well as manmade sources. Hence the security of the sensor nodes must be increased. The improvement of sensor node security requires a multi-pronged approach including physical, logical and technological aspects.

In wireless sensor network secure routing arena, the following areas need further investigations.

- Energy optimized routing protocols: In any network, though routing is an essential requirement, the operation of routing protocols is an overhead. Hence the overhead incurred in the operation of routing protocols must be reduced as much as possible.
- Faster convergence: The scale of operation of wireless sensor networks is large with thousands of nodes. Also the topology is also dynamic compared to conventional networks. Under these circumstances, the routing table would also constantly undergo rapid changes. Thus routing protocols with faster convergence times is an immediate requirement.
- The routing protocols and information face attacks by various threats and these would increase in the future with the popularity of wireless sensor networks. Hence it is necessary to have more secure routing protocols that are robust and resilient in the face of increased attacks in the future.

8 Conclusions

Sensor nodes have become more intelligent in recent times due to the developments in many fields including VLSI design, computing and communication. With the increased intelligence incorporated into the sensor nodes, the application areas where these nodes can be used has also increased. Along with the increased popularity and deployments of wireless sensor networks, the threats and attacks on these networks have also become a major issue demanding immediate attention to them. Several research groups are working on enhancing the security of these networks and proposed many mechanisms, techniques and algorithms. This chapter took an in depth look at the security implementations in wireless smart sensor networks from three specific angles; namely sensor node security, data security and routing security. Though tremendous work has already been done in the area of wireless sensor network security, still there is a lot room for future work in this area.

References

1. Mohamed, M.I., Wu, W.Y., Moniri, M.: Power harvesting for smart sensor networks in monitoring water distribution system. IEEE International Conference on Networking, Sensing and Control, pp. 393–398, Delft, The Netherlands (2011)
2. Zhang, Y., Gu, Y., Vlatkovic, V., et al.: Progress of smart sensor and smart sensor networks. 5th World Congress on Intelligent Control and Automation, pp. 3600–3606, Hangzhou, China (2004)
3. Lyle, A.C., Naish, M.D.: A software architecture for adaptive modular sensing systems. Sensors **10**(8), 7514–7560 (2010)
4. Kizza, J.M.: Implementing security in wireless sensor networks. 4th Annual International Conference on Computing and ICT Research, pp. 296–311, Kampala, Uganda (2008)
5. Razzak, M.I., Elmogy, B.A., Khan, M.K., et al.: Efficient distributed face recognition in wireless sensor network. Int. J. Innovative Comput. Inf. Control **8**(4), 2811–2822 (2012)
6. Sharma, K., Ghose, M.K., Kuldeep, : Complete security framework for wireless sensor networks. Int. J. Comput. Sci. Inf. Secur. **3**(1), 1–7 (2009)
7. Boyle, D., Newe, T.: Securing wireless sensor networks security architectures. J. Netw. **3**(1), 65–77 (2008)
8. Sen, J.: A survey on wireless sensor network security. Int. J. Commun. Netw. Inf. Secur. **1**(2), 55–78 (2009)
9. Hecker, M., Karol, A., Stanton, C., et al.: Smart sensor networks: communication, collaboration and business decision making in distributed complex environments. International Conference on Mobile Business, pp. 242–248, Sydney, Australia (2005)
10. Herrera-Quintero, L.F., Macia-Perez, F., Ramos-Morillo, H., et al.: Wireless smart sensors networks, systems, trends and its impact in environmental monitoring. IEEE Latin-American Conference on Communications, pp. 1–6, Medellin, Colombia (2009)
11. Fine, G.F., Cavanagh, L.M., Afonja, A., et al.: Metal oxide semi conductor gas sensors in environmental monitoring. Sensors **10**(6), 5469–5502 (2010)
12. Hancke, G.P., Silva, B.C., Hancke, G.P.: The role of advanced sensing in smart cities. Sensors (Basel) **13**(1), 393–425 (2013)
13. Fan, G., Wang, R., Huang, H., et al.: Coverage-guaranteed sensor node deployment strategies for wireless sensor networks. Sensors (Basel) **10**(3), 2064–2087 (2010)

14. Singh, A., Sharma, T.P.: A survey on area coverage in wireless sensor networks. International Conference on Control, Instrumentation, Communication and Computational Technologies, pp. 900–907, Kumaracoil, Thuckalay, TN, India (2014)
15. Taniguchi, Y., Kitani, T., Leibnitz, K.: A uniform airdrop deployment method for large-scale wireless sensor networks. Int. J. Sens. Netw. **9**, 182–191 (2011)
16. Filippou, A., Karras, D.A., Papademetriou, R.C.: Coverage problem for sensor networks: an overview of solution strategies. 17th Telecommunications Forum, pp. 134–136, Serbia, Belgrade (2009)
17. Sheikhpour, R., Jabbehdari, S., Khadem-Zadeh, A.: Comparison of Energy efficient clustering protocols in heterogeneous wireless sensor networks. Int. J. Adv. Sci. Technol. **36**, 27–40 (2014)
18. Ranjan, R., Kar, S.: A novel approach for finding optimal number of cluster head in wireless sensor network. National Communications Conference, pp. 1–5, Bangalore, India (2011)
19. Ghosh, A., Das, K.S.: Coverage and connectivity issues in wireless sensor networks. In: Shorey, R., Ananda, A.L., Chan, M.C., et al. (eds.) Mobile, wireless and sensor networks: Technology, applications, and future directions. Wiley, New York (2006)
20. Li, J., Andrew, L.L.H., Foh, C.H., Zukerman, M., et al.: Connectivity, coverage and placement in wireless sensor networks. Sensors **9**, 7664–7693 (2009)
21. Khelifa, B., Haffaf, H., Madjid, M., et al.: Monitoring connectivity in wireless sensor networks. Int. J. Future Gener. Commun. Networking **2**(2), 1–10 (2009)
22. Zhang, H., Hou, J.C.: Maintaining sensing coverage and connectivity in large sensor networks. Ad Hoc Sens. Wireless Netw. **1**, 89–124 (2005)
23. McDermott-Wells, P.: What is bluetooth? IEEE Potentials **23**(5), 33–35 (2005)
24. Ting, K.S., Ee, G.K., Ng, C.K., et al.: The performance evaluation of IEEE 802.11 against IEEE 802.15.4 with low transmission power. 17th Asia-Pacific Conference on Communications, pp. 850–855, Kota Kinabalu, Sabah, Malaysia (2011)
25. Liu, T., Liu, J., Liu, B.: Design of intelligent warehouse measure and control system based on Zigbee WSN. International Conference on Mechatronics and Automation, pp. 888–893, Xi'an, China (2010)
26. Teng, Z., Kim, K.I.: A survey on real-time MAC protocols in wireless sensor networks. Commun. Netw. **2**(2), 104–112 (2010)
27. Carman, D.W., Krus, P.S., Matt, B.J.: Constraints and approaches for distributed sensor network security. Technical Report 00-010, Network Associates Inc., Glenwood, MD, USA (2000)
28. Hill, J., Szewezyk, R., Woo, A., et al.: System architecture directions for networked sensors. 9th International Conference on Architectural Support for Programming Languages and Operating systems, pp. 93–104, Cambridge, MA, USA (2000)
29. Tsiftes, N., Dunkels, A., He, Z., et al.: Enabling large-scale storage in sensor networks with the coffee file system. International Conference on Information Processing in Sensor Networks, pp. 349–360, San Francisco, CA, USA (2009)
30. Marigowda, C.K., Shingadi, M.: security vulnerability issues in wireless sensor networks: A short survey. Int. J. Adv. Res. Comput. Commun. Eng. **2**, 2765–2770 (2013)
31. Kumar, Y., Munjal, R., Kumar, K.: Wireless sensor networks and security challenges. Int. J. Comput. Appl. RTMC **9**, 17–21 (2012)
32. Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. Commun. ACM **47**(6), 53–57 (2004)
33. Raman, B., Chebrolu, K.: Censor networks: A critique of sensor networks from a systems perspective. ACM SIGCOMM Comput. Commun. Rev. **38**(3), 75–78 (2008)
34. Zia, T.A., Zomaya, A.Y.: A lightweight security framework for wireless sensor networks. J. Wireless Mobile Netw., Ubiquitous Comput. Dependable Appl. **2**(3), 53–73 (2011)
35. Tsitsigkos, A., Entezami, F., Ramrekha, T.A., et al.: A case study of internet of things based on wireless sensor networks and smart phones. 28th Wireless World Research Forum Meeting, pp. 1–10, Athens, Greece (2012)

36. Baburajan, J., Prajapati, J.: A review paper on watchdog mechanism in wireless sensor network to eliminate false malicious node detection. Int. J. Res. Eng. Technol. **3**(1), 381–384 (2014)
37. Nakul, P.: A survey on malicious node detection in wireless sensor networks. Int. J. Sci. Res. **2** (1), 691–694 (2013)
38. Li, W.T., Feng, T.H., Hwang, M.S.: Distributed detecting node replication attacks in wireless sensor networks: a survey. Int. J. Netw. Secur. **16**(5), 323–330 (2014)
39. Virmani, D., Hemrajani, M., Chandel, S.: Exponential trust based mechanism to detect black hole attack in wireless sensor network. Int. J. Soft Comput. Eng. **4**(1), 14–16 (2014)
40. Lim, S.Y., Choi, Y.H.: Malicious node detection using dual threshold in wireless sensor networks. J. Sens. Actuator Netw. **2**, 70–84 (2013)
41. Atakli, I.M., Hu, H., Chen, Y., et al.: Malicious node detection in wireless sensor networks using weighted trust evaluation. Symposium on Simulation of System Security, pp. 836–843, Ottawa, Canada (2008)
42. Junior, W.R.P., Figueiredo, T.H.P., Wong, H.C., et al.: Malicious node detection in wireless sensor networks. 18th International Parallel and Distributed Processing Symposium, Santa Fe, NM, USA (2004)
43. Perrig, A., Szewczyk, R., Tygar, J.D., et al.: SPINS: security protocols for sensor networks. Wireless Netw. **8**(5), 521–534 (2002)
44. Karlof, C., Sastry, N., Wagner, D.: TinySec: a link layer security architecture for wireless sensor networks. 2nd International Conference on Embedded Networked Sensor Systems, pp. 162–175, Baltimore MD, USA (2004)
45. Heo, J., Hong, C.S.: Efficient and authenticated key agreement mechanism in low rate WPAN environment. International Symposium on Wireless Pervasive Computing, pp. 1–5, Phuket, Thailand (2006)
46. Soroush, H., Salajegheh, M., Dimitriou, T.: Providing transparent security services to sensor networks. IEEE International Conference on Communication, pp. 3431–3436, Glasgow, Scotland (2007)
47. Garcia-Morchon, O., Baldus, H.: The ANGEL WSN Security Architecture. Third International Conference on Sensor Technologies and Applications, pp. 430–435, Athens, Greece (2009)
48. Cionca, V., Newe, T., Dadarlat, V.: MArSSeNs: a modular architecture for the security of sensor networks. IEEE Sensors, pp. 1209–1212, Limerick, Ireland (2011)
49. Duan, J., Yang, D., Zhu, H., et al.: TSRF: a trust aware secure routing framework in wireless sensor networks. Int. J. Distrib. Sens. Netw. 1–14 (2014)
50. Xiangyu, J., Chao, W.: The security routing research for WSN in the application of intelligent transport system. IEEE International Conference on Mechatronics and Automation, pp. 2318–2323, Luoyang, Henan, China (2006)
51. Zahariadis, T., Leligou, H.C., Voliotis, S., et al.: Energy-aware secure routing for large wireless sensor networks. WSEAS Trans. on Commun. **9**(8), 981–991 (2009)
52. Deng, J., Han, R., Mishra, S.: INSENS: intrusion-tolerant routing in wireless sensor networks. Technical report CU-CS-939-02, Department of Computer Science, University of Colorado, Boulder, CO, USA (2002)
53. Tanachaiwiwat, S., Dave, P., Bhindwale, R.: Routing on trust and isolating compromised sensors in location-aware sensor networks. 1st International Conference on Embedded Networked Sensor Systems, pp. 324–325, Los Angeles, CA, USA (2003)
54. Papadimitratos, P., Haas, Z.J.: Secure routing for mobile ad hoc networks. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, pp. 1–13, San Antonio, TX, USA (2002)
55. Arolkar, H.A., Sheth, S.P., Tamhane, V.P.: Ant colony based approach for intrusion detection on cluster heads in wireless sensor networks. International Conference on Communication, Computing and Security, pp. 523–526, Rourkela, Odisha, India (2011)

Author Biography

Mohamed Fazil Mohamed Firdhous Mohamed Fazil Mohamed Firdhous is a Senior Lecturer and the Director of Postgraduate Studies at the Faculty of Information Technology, University of Moratwua, Sri Lanka. He is engaged in undergraduate and postgraduate teaching along with cutting edge research in the areas of trust and trust management for cloud computing, Internet of Things, mobile adhoc networks, vehicular networks, computer security and rural ICT development. He has teaching, research and industry experience in many countries including Sri Lanka, Singapore, United States of America and Malaysia. In addition to his teaching and research activities at the University, he is a highly sought after ICT consultant to the government and private institutions in Sri Lanka.