International Journal of Future Generation Communication and Networking
Vol.6, No.5 (2013), pp.97-116
http://dx.doi.org/10.14257/ijfgcn.2013.6.5.10

Security Issues in Wireless Sensor Networks: A Survey

Mahfuzulhoq Chowdhury[1], Md Fazlul Kader[2] and Asaduzzaman[1]

[1]*Department of Computer Science & Engineering, Chittagong University of Engineering & Technology, Chittagong, Bangladesh.*
[2]*Department of Applied Physics, Electronics and Communication Engineering, University of Chittagong, Chittagong, Bangladesh.*
[E-mail: mahfuz_csecuet@yahoo.com, f.kader@cu.ac.bd,asadcuet@cuet.ac.bd]

Abstract

Due to a wide range of applications, wireless sensor networks (WSNs) have recently attracted a lot of interest to the researchers. Limited computational capacity and power usage are two major challenges to ensure security in WSNs. Recently, more secure communication or data aggregation techniques have discovered. So, familiarity with the current research in WSN security will benefit researchers greatly. In this paper, security related issues and challenges in WSNs are investigated. We identify the security threats and review proposed security mechanisms for WSNs. Moreover, we provide a brief discussion on the future research direction in WSN security.

Keywords: *Wireless Sensor Network, Security, Threats, Attacks, Security Mechanism*

1. Introduction

WSNs are quickly gaining popularity due to the fact that they provide potentially low cost solutions to a variety of real world challenges [1]. Unfortunately, conventional security approaches with high overhead are not feasible for resource constrained sensor nodes. Economically feasible sensor nodes provide a means to deploy large sensor arrays in a variety of conditions capable of performing both military and civilian tasks. Lack of data storage and power are two major obstacles to the implementation of traditional computer security techniques in a WSN [2]. The main challenges in sensor network security are as follows:

- The trade-off between resource consumption minimization and security maximization.
- The capabilities and constraints of sensor node hardware will influence the type of security mechanisms that can be hosted on a sensor node platform.
- Link attacks on WSNs, ranging from passive eavesdropping to active interfering causes due to the ad-hoc networking topology.
- Traditional wired-based security schemes may become impractical because of the wireless communication characteristics of WSN.

A number of secure and efficient routing protocols [3, 4], secure data aggregation protocols [5, 6] have been proposed by several researchers in WSN security. Traditional security issues in WSNs should involve collaborations among the nodes due to the decentralized nature of the networks and the absence of any infrastructure. Therefore, researchers have focused on building a sensor trust model to solve the problems which are beyond the capabilities of traditional cryptographic mechanisms [7, 8]. In most cases, a trade-off has to be made between security and performance. However, weak security protocols may

ISSN: 2233-7857 IJFGCN

be easily broken by attackers. Since in most cases, sensor nodes are insecure, so vulnerability to attack is an important issue. In this paper, we explore various security issues in WSNs and try to give a comparative note of various existing security approaches. Our contribution is therefore to provide a detailed yet concise analysis of various existing techniques which will enable the WSN implementers to approach security in an organized way. In this paper, we have reviewed possible attacks on WSN in general as well as existing security mechanism.

The rest of the paper is organized as follows. Section 2 gives a general overview of different security constraints. Section 3 elaborates possible attacks against WSN in general. Section 4 presents the numerous countermeasures for all possible attacks on WSNs. Finally, in Section 5, we conclude the paper highlighting some future research directions in WSN security.

2. Overview of Security Constraints in WSN

A WSN is a special network which has many constraints compared to a traditional computer network. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints first [2].

- Memory and power limitations: A sensor is a tiny device with only a small amount of memory and storage space for the code. It is necessary to limit the code size of the security algorithm to build an effective security mechanism,. Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced or recharged because of high operating cost.
- Unreliable Communication: It is one of the major threats to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication. The major parameters are unreliable transfer, latency and conflicts.
- Security Requirements: The security requirements [9, 10] of a wireless sensor network can be classified as follows:
    - Authentication: In any decision making process, the receiving nodes need to ensure that the data originates from the reliable source. Similarly, authentication is necessary during an exchange of control information in the network. Data authenticity is an assurance of the identities of communicating nodes.
    - Integrity: Data in transit can be changed by the adversaries. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Data integrity ensures that the information is not changed in transit, either due to malicious intent or by accident. Use of message integrity code is a standard approach for ensuring data integrity.
    - Data confidentiality: Applications like surveillance of information, industrial secrets and key distribution need to rely on confidentiality. The standard approach for keeping confidentiality is through the use of encryption. The major problem is that radio spectrum is an open resource and can be used by anyone equipped with proper radio transceivers. An attacker can eavesdrop on the packets transmitted in the air as long as he is able to keep track of the radio channels used in the communication. The attacker can also discover the secrets in a node without capturing it, which can be done by analyzing the secret data collected from other compromised nodes and/or packet protocol data units (PDUs). Under the attacker's control, the new compromised node can be used to launch more malicious attacks.

- Data freshness: Data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when the WSN nodes use shared keys for message communication, where a potential adversary can launch a replay attack using the old key as the new key is being refreshed and propagated to all the nodes in the WSN. The out-dated information contained in the packet can cause many problems to the applications deployed in the network. An example is the wormhole attack in WSNs [11].
- Availability: Sensor nodes may run out of battery power due to excess computation or communication and become unavailable. It may happen that an attacker may jam communication to make sensor(s) unavailable. The requirement of security not only affects the operation of the network, but is also highly important in maintaining the availability of the network.
- Self-Organization: In WSN, every sensor node is independent and flexible enough to be self-organizing and self-healing according to different hassle environments. Due to the random deployment of nodes no fixed infrastructure is available for WSN network management. Distributed sensor networks must be self-organize to support multi-hop routing. They must also be self-organize to conduct key management and building trust relation among sensors. A number of key pre-distribution schemes have been proposed in the context of symmetric encryption [12, 13].
- Time Synchronization: In order to conserve power, an individual sensor node may be turned off periodically. Any security mechanism for WSN should also be time-synchronized.
- Secure Localization: The sensor network often needs location information accurately and automatically. However, an attacker can easily manipulate non secured location information by reporting false signal strengths and replaying signals, *etc*.

3. Security Threats and Attacks in WSN

Attackers may devise different types of security threats to make the WSN system unstable. Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium.

3.1. Security Threats

According to capability of attacker [14], threats in WSNs can be classified into the following categories:

- External versus internal attacks: The external attacks come from nodes which do not belong to a WSN. An external attacker or outsider has no access to most cryptographic materials in sensor network. External attacks may cause passive eavesdropping on data transmissions as well as can extend to inject bogus data into the network to consume network resources and raise denial of service (DoS) attack. On the contrary, the internal attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways. Internal attacker or insider is an authorized participant in the sensor network who seeks to disrupt operations or exploit organizational assets.
- Passive versus active attacks: Passive attacks include eavesdropping or monitoring packets exchanged within a WSN whereas active attacks involve some modifications of the data stream or the creation of a false stream.

- Mote-class versus laptop-class attacks: In mote class (sensor-class) attacks, an adversary attacks a WSN by using a few nodes with similar capabilities as that of network nodes. In laptop-class attacks, an adversary can use more powerful devices like laptop, *etc.* and can do much more harm to a network than a malicious sensor node. These devices have a greater transmission range, processing power, and energy reserve than the network nodes.

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be attacked to provide wrong information to the base stations or sinks. The weakness in a system security design, implementation, configuration or limitations that could be exploited by attackers is known as vulnerability or flaw.

3.2. Security Attacks

Attacks on the computer system or network can be broadly classified [15] as interruption, interception, modification and fabrication.

- Interruption: Interruption is an attack on the availability of the network, for example physical capturing of the nodes, message corruption, insertion of malicious code etc. The main purpose is to launch DoS attacks.
- Interception: Interception is an attack on confidentiality. The sensor network can be compromised by an adversary to gain unauthorized access to sensor node or data stored within it.
- Modification: Modification is an attack on integrity. Modification means an unauthorized party not only accesses the data but also tampers it. For example, by modifying the data packets being transmitted or causing a DoS attack such as flooding the network with bogus data. The main purpose is to confuse or mislead the parties involved in the communication protocol. This is usually aimed at the network layer and the application layer, because of the richer semantics of these layers.
- Fabrication: Fabrication is an attack on authentication. In fabrication, an adversary injects false data and compromises the trustworthiness of the information relayed. This threatens the message authenticity. This operation can also facilitate DoS attacks by flooding the network.

Attacks can also be classified as host-based and network-based attacks.

- Host-based attacks: It is further divided into three types: software compromise, hardware compromise and user compromise. Software compromise involves breaking the software running on the sensor nodes (buffer overflows). Hardware compromise involves tampering with the hardware to extract the program code, data and keys stored within a sensor node. User compromise involves compromising the users of a WSN, *e.g.*, by cheating the users into revealing information such as passwords or keys about the sensor nodes.
- Network-based attacks: It has two perspectives: layer-specific compromises and protocol-specific compromises. This includes all the attacks on information in transit. Apart from that it also includes deviating from protocols. Attacker gains an unfair advantage for itself in the usage of the network. In addition, the attacker manifests selfish behaviors *i.e.*, behaviors that deviate from the intended functioning of the protocol.

3.3. Layering based Attacks

Though there is no such standard layered architecture of the communication protocol for WSN, here, we have summarized possible attacks and their security solution approaches in different layers with respect to ISO-OSI layer in the Table-1 [16, 17].

Table 1. Layering based Attacks and Possible Security Approach

Layer	Attacks	Security Approach
Physical layer	Jamming and Tampering	Use spread spectrum techniques and medium access control (MAC) layer admission control mechanisms
Data link layer	Jamming and Collision	Use error correcting codes and spread spectrum techniques
Network layer	Sinkhole	Redundancy checking
	Sybil	Authentication, monitoring
	Wormhole	Authentication, probing
	Hello flood	Authentication, packet leashes by geographical and temporal info.
	Ack. flooding	Authentication, bidirectional link authentication, verification
Transport layer	Injects false messages and energy drain attacks	Authentication
	Flooding	Client puzzles
	De-synchronization	Authentication
Application layer	Attacks on reliability	Cryptographic approach

Most of the routing protocols proposed for ad hoc and sensor network are not designed to handle security related issues. Therefore, there is a lot of scope for attacks on them. Different possible attacks on the flow of data and control information can be categorized as in [18]. Two types of attacks in physical layer are (i) jamming and (ii) tampering.

- Jamming: This is one of the DoS attacks in which the adversary attempts to disrupt the operation of the network by broadcasting a high-energy signal. To defense against this attack, use spread-spectrum techniques for radio communication.
- Tampering: Sensor networks typically operate in outdoor environments. Due to unattended and distributed nature, the nodes in a WSN are highly susceptible to physical attacks [19]. The physical attacks may cause irreversible damage to the nodes. The adversary can extract cryptographic keys from the captured node, tamper with its circuitry, modify the program codes or even replace it with a malicious sensor.

The link layer is responsible for multiplexing of data streams, data frame detection, MAC, and error control [20]. Attacks at this layer include purposefully created collisions, resource exhaustion, and unfairness in allocation.

- Continuous Channel Access (Exhaustion): A malicious node disrupts the MAC protocol, by continuously requesting or transmitting over the channel. This eventually leads a starvation for other nodes in the network with respect to channel access. One of the countermeasures to such an attack is rate limiting to the MAC admission control

such that the network can ignore excessive requests. The second technique is to use time division multiplexing.

- Collision: This is very much similar to the continuous channel attack. A collision occurs when two nodes attempt to transmit on the same frequency simultaneously. When packets collide, a change will likely occur in the data portion, causing a checksum mismatch at the receiving end. The packet will then be discarded as invalid.
- Unfairness: Repeated application of these exhaustion or collision based MAC layer attacks or an abusive use of cooperative MAC layer priority mechanisms, can lead into unfairness. This kind of attack is a partial DOS attack, but results in marginal performance degradation. One major defensive measure against such attacks is the usage of small frames, so that any individual node seizes the channel for a smaller duration only.
- Denial of Service (DoS): Denial of Service (DoS) [21, 22] is produced by the unintentional failure of nodes or malicious action. This attack is a pervasive threat to most networks. Sensor networks being very energy-sensitive and resource-limitations are very vulnerable to DoS attacks. Wood and Stankovic [23] explored various DoS attacks that may happen in every network layer of sensor networks. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In WSNs, several types of DoS attacks in different layers might be performed. At the physical layer, DoS attacks could be jamming and tampering. At the link layer, DoS attacks are colliding, exhaustion, unfairness whereas at the network layer, attacks are neglect and greed, homing, misdirection and black holes. Moreover, at the transport layer, this attack could be performed by malicious flooding and de-synchronization.

The network layer of WSNs is vulnerable to the different types of attacks such as: spoofed routing information, selective packet forwarding, sinkhole, sybil, wormhole, hello flood, acknowledgment spoofing *etc*.

- Spoofed, altered, or replayed routing information: This is the most common direct attack against a routing protocol. This attack targets the routing information exchanged between the nodes. Adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, and increase end-to-end latency. The standard solution for this attack is authentication. *i.e.*, routers will only accept routing information from valid routers.
- Selective forwarding: In a multi-hop network like a WSN, all the nodes need to forward messages accurately. An attacker may compromise a node in such a way that it selectively forwards some messages and drops others [24].
- Sybil Attack: In this attack, a single node presents multiple identities to all other nodes in the WSN. This may mislead other nodes. Hence, routes believed to be used by disjoint nodes with respect to node that can have the same adversary node. A countermeasure to Sybil attack is the use of a unique shared symmetric key for each node with the base station. Sybil attack is defined as a malicious device illegitimately taking on multiple identities. In Sybil attack [25], an adversary can appear to be in multiple places at the same time. In other words, a single node presents multiple identities to other nodes in the sensor network either by fabricating or stealing the identities of legitimate nodes.

- Sinkhole attack: By sinkhole attack, the adversary tries to attract nearly all the traffic from a particular area through a compromised node. A compromised node which is placed at the centre of some area creates a large “sphere of influence”, attracting all traffic destined for a base station from the sensor nodes. The attacker targets a place to create sinkhole where it can attract the most traffic, possibly closer to the base station so that the malicious node could be perceived as a base station.
- HELLO flood attack: Many protocols require nodes to broadcast HELLO packets for neighbor discovery, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. A laptop-class attacker with large transmission power could convince every node in the network that the adversary is its neighbor, so that all the nodes will respond to the HELLO message and waste their energy. We can prevent this attack by verifying the bi-directionality of local. Another way to prevent the HELLO flood attack is the use of authenticated broadcast protocols.
- Wormhole: A wormhole is low latency link between two portions of a network over which an attacker replays network messages [24]. This link may be established either by a single node forwarding messages between two adjacent but otherwise non-neighboring nodes or by a pair of nodes in different parts of the network communicating with each other. The latter case is closely related to sinkhole attack as an attacking node near the base station can provide a one hop link to that base station via the other attacking node in a distant part of the network.
- Acknowledgement spoofing: Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements. Due to the inherent broadcast medium, an adversary can spoof link layer acknowledgments for “overheard” packets addressed to neighboring nodes. Protocols that choose the next hop based on reliability issues are susceptible to acknowledgments spoofing. This results in packets being lost when travelling along such links
- Sniffing attack: Sniffing attack is a good example of interception or listen-in channel attack. In this attack an adversary node is placed in the proximity of the sensor grid to capture data. The collected data is transferred to the intruder by some means for further processing. Sniffing attacks can be prevented by using proper encryption techniques for communication.

The attacks that can be launched on the transport layer in a WSN are flooding attack and de-synchronization attack.

- Flooding: An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes. One proposed solution to this problem is to require that each connecting client demonstrates its commitment to the connection by solving a puzzle. As a defense against this class of attack, a limit can be put on the number of connections from a particular node.
- De-synchronization: De-synchronization refers to the disruption of an existing connection [23]. An attacker may, for example, repeatedly spoof messages to an end host causing the host to request the retransmission of missed frames.

There are also other attacks like energy drain attack, black hole attack, homing and node replication attacks.

- Energy drain attacks: is battery powered and dynamically organized. It is difficult or impossible to replace/recharge sensor node batteries. Because there is a limited

amount of energy available, attackers may use compromised nodes to inject fabricated reports into the network or generate a large amount of traffic in the network.

- Black-hole attack: The black hole attack positions a node in range of the sink and attracts the entire traffic to be routed through it by advertising itself as the shortest route.
- Homing: Another interesting type of attack is homing. In a homing attack, the attacker looks at network traffic to deduce the geographic location of critical nodes, such as cluster heads or neighbors of the base station. The attacker can then physically disable these nodes.
- Node replication attacks: This is an attack where the attacker tries to mount several nodes with the same identity at different places of the existing network. There are two methods for mounting this attack. In the first method, the attacker captures one node from the network, creates clones of a captured node and mounts in different places of the network. In the second method, an attacker may generate a false identification of a node then makes a clone out of this node and mounts in different places of the network.

Depending on the network architecture and information used while taking routing decision, routing protocol in WSNs can be classified into flat-based routing, hierarchical-based routing, location-based routing, and network flow or quality of service (QoS) aware routing. In Table 2, we summarize the class of routing protocols and possible attacks.

4. Security Solutions for WSN and Future Research Area

In this section, defense mechanisms for combating various types of attacks on WSNs will be discussed.

4.1. Cryptography

To achieve security in WSNs, it is important to be able to perform various cryptographic operations, including encryption, authentication, and so on. Selecting the appropriate cryptographic method for sensor nodes is fundamental to provide security services in WSNs and communication capability of the sensor nodes. Since, sensor nodes usually have severely constrained, asymmetric cryptography is often too expensive for many applications. Thus, a promising approach is to use more efficient symmetric cryptographic alternatives. Security protocols for sensor networks (SPIN) was proposed by Adrian Perrig *et al.*,[34]. SPINs has two secure building blocks: (a) sensor network encryption protocol (SNEP) and (b) μTESLA. SNEP provides data confidentiality, two-party data authentication, and data freshness. μTESLA provides authenticated broadcast for severely resource-constrained environments. Recent studies on public key cryptography have demonstrated that public key operations may be practical in sensor networks. Most current symmetric key schemes for WSNs aim at link layer security for one-hop communications, but not the transport layer security for multi hop communications. It is unlikely for each node to store a transport layer key for each of the other nodes in a network due to the huge number of nodes. Proving the authenticity of public keys is another important problem.

Table 2. Class of Routing Protocols and Possible Attacks

Protocols	Spoofed, altered, or replayed routing information	Selective forward	Sink hole	Sybil	Worm hole	HELLO flood	Acknowledgement spoofing	Sniffing	Data integrity	Energy drain	Black hole	Node replication
Network flow & QoS-aware [26][27]	no	yes	yes	no	yes	yes	yes	yes	yes	yes	yes	yes
Location Based [28][29]	no	yes	no	yes	yes	yes	yes	yes	no	yes	yes	no
Hierarchi-cal [30][31]	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Flat Based [32][33]	no	no	yes	yes	yes	yes	no	yes	yes	yes	yes	yes

Public key algorithms such as RSA are computationally intensive and usually execute thousands or even millions of multiplication instructions to perform a single-security operation. Brown et al found that a public key algorithm such as RSA, which exposes a vulnerability to DoS attacks [35]. Recent studies have shown that it is feasible to apply public key cryptography to sensor networks by using the right selection of algorithms and associated parameters, optimization, and low power techniques [36]. The investigated public key algorithms include Rabin's Scheme [37], RSA [38], and Elliptic Curve Cryptography (ECC) [39, 40]. The limitation of private key operation occurring only at a base station makes many security services using public key algorithms not available under these schemes. Such services include peer-to-peer authentication and secure data aggregation. Most of the public key cryptographic mechanisms are computationally expensive. So, most of the research studies for WSNs focus on use of symmetric key cryptographic techniques. Symmetric key cryptographic mechanisms use a single shared key between the two communicating hosts which is used both for encryption and decryption. However, one major challenge for deployment of symmetric key cryptography is how to securely distribute the shared key between the two communicating hosts. This is a non-trivial problem since pre-distributing the key may not always be feasible. Selecting the appropriate cryptographic method for sensor nodes is fundamental to provide security services in WSNs. However, the decision depends on the computation and communication capability of the sensor nodes. Five popular encryption schemes such as RC4 [41], RC5 [42], IDEA [41], SHA-1 [43] and MD5 [41, 44] were evaluated on six different microprocessors ranging in word size from 8-bit to 32-bit widths in [45]. Symmetric key cryptography is superior to public key cryptography in terms

of speed and low energy cost. However, the key distribution schemes based on symmetric key cryptography are not perfect. Efficient and flexible key distribution schemes need to be designed.

4.2. Key Management Protocols

The area that has received maximum attention of the researchers in WSN security is key management. Key management is a core mechanism to ensure security in network services and applications in WSNs. The goal of key management is to establish the keys among the nodes in a secure and reliable manner. Depending on the underlying network structure, the key management protocols in WSNs may be centralized or distributed. In a centralized key management scheme, there is only one entity that controls the generation, re-generation, and distribution of keys. This entity is called key distribution center (KDC). Generally speaking, the problem of key management in WSN can be decomposed into the following sub-problems:(1) Key pre-distribution, (2) Neighbor discovery, (3) End-to-end path-key establishment, (4) Isolating aberrant nodes, (5) Re-keying, (6) Key-establishment latency. In Table 3, we summarize the classification of key management protocols.

In key pre-distribution, a big issue is how to load a set of keys (called key ring) into the limited memory of each sensor. The key management protocols for WSNs may be classified on the probability of key sharing between a pair of sensor nodes. Depending of this probability the key management schemes may be either deterministic or probabilistic. Localized encryption and authentication protocol (LEAP) [46] is a key management protocol for sensor networks. It is designed to support in-network processing and secure communications in sensor networks. LEAP provides the basic security services such as confidentiality and authentication. Four types of keys are established for each node: (i) an individual key shared with the base station (pre-distributed), (ii) a group of key shared by all the nodes in the network (pre-distributed), (iii) pair-wise key shared with immediate neighbor nodes, and (iv)a cluster key shared with multiple neighbor nodes. The pair-wise keys shared with immediate neighbor nodes are used to protect peer-to-peer communication and the cluster key is used for local broadcast. Most of the key management protocols for WSNs are probabilistic and distributed schemes. In Table 4, we summarize the security schemes for wireless sensor WSNs with major features.

Eschenauer and Gligor have proposed a random key pre-distribution scheme for WSNs that relies on probabilistic key sharing among nodes of a random graph [32]. The mechanism has three phases: key pre-distribution, shared key discovery, and path key establishment. Hwang and Kim in [33], improved the basic random key management protocol [32] by reducing the amount of key-related materials required to be stored in each node, while guaranteeing a certain probability of sharing a key between two nodes. Hwang *et al.*, extended the basic random key management scheme and proposed a cluster key grouping scheme [50]. They further analyzed the trade-offs involved between energy, memory, and security robustness. In the location-based key pre-distribution (LBKP) scheme [51], the entire WSN is divided into many square cells. After deployment, any two neighbor nodes can establish a pair wise key if they have shares of the same polynomial.

Table 3. Classification of Key Management Protocols

Type	Protocol Name	Lit. Ref	Storage load	Comm. load	Robustness	Scalability	Cluster key	Path key	Pairwise key
Deterministic	Leap	[46]	low	low	low	good	yes	yes	yes
	LKHW	[47]	low	low	low	limited	yes	no	yes
	IOS& DMBS	[48]	high	medium	good	good	no	no	yes
	BROSK	[49]	low	low	low	good	no	no	yes
Probabilistic	Cluster key grouping	[50]	high	medium	good	good	no	no	yes
	Location based	[51]	medium	medium	good	good	no	no	yes
	Polynomial based	[13]	high	medium	good	good	no	no	yes
	Basic	[14]	high	medium	good	good	no	yes	yes

4.3. Defense against DoS Attacks

Various types of DoS attacks in WSNs have been discussed in Section 3. Jamming attack may be defended by employing variations of spread-spectrum communication such as frequency hopping and code spreading [23]. A typical defense against collision attack is the use of error correcting codes [23]. Most of the codes work best with low levels of collisions such as those caused by environmental or probabilistic errors. A possible solution for energy exhaustion attack is to apply a rate limiting MAC admission control. This would allow the network to ignore those requests that intend to exhaust the energy reserves of a node. A second technique is to use time division multiplexing. A possible defense against de-synchronization attack on the transport layer is to enforce a mandatory requirement of authentication of all packets communicated between nodes.

Table 4. Security Schemes for WSNs with Major Features

Security Schemes	Attacks Type	Network Model	Features
Radio resource testing, random key pre-distribution	Sybil attack	Traditional WSN	Uses radio resource, random key pre-distribution, registration procedure, position verification and code attestation for detecting sybil entity
Random key pre-distribution	Data and information spoofing	Traditional WSN	Provide resilience of the network, protect the network even if part of the network is compromised, provide authentication

			measures for sensor nodes
Wormhole based	DoS attack (Jamming)	Hybrid sensor network	Use wormholes to avoid jamming
Jamming based	DoS attack (Jamming)	Traditional WSN	Avoidance of the jammed region by using coalesced neighbor nodes.
Bidirectional verification, Multipath, Multibase station routing	Hello flood attack	Traditional WSN	Adopts probabilistic secret sharing, uses bidirectional verification and multi-path multi-base station routing
SNEP & μTESLA	Data or information spoofing, Message replay attack	Traditional WSN	Semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead
Reward	Black-hole attacks	Traditional WSN	Uses geographic routing. Takes advantage of the broadcast inter-radio behavior to watch neighbor transmission and detect black hole attacks
On communication security	Information or Data Spoofing	Traditional WSN	Efficient resource management, Provide the network even if part of the network is compromised

4.4. Secure Data Aggregation

Since WSNs are energy constrained and bandwidth limited, reducing communications between sensors and base stations has a significant effect on power conservation and bandwidth utilization. Aggregated sensor networks serve this purpose. Data aggregation (or data fusion) is a process in which intermediary nodes called “aggregators” collect the raw sensed information form sensor nodes, process it locally, and forward only the result to the end-user. This important operation essentially reduces the amount of transmitted data on the network and thus prolongs its overall lifetime [52]. An active adversary can forge, the home server to accept false aggregation results (Stealthy attacks), which are very much different from the actual results determined by the measured values [16]. Multicasting and broadcasting techniques are used primarily to reduce the communication and management overhead of sending a single message to multiple receivers. In order to ensure that only legitimate group members receive the multicast and broadcast communication, appropriate authentication and encryption mechanisms must be in place.

4.5. Intrusion Detection

The problem of intrusion detection is very important in the case of WSNs. Traditional approaches which do an anomaly analysis of the network at a few concentration points, are expensive in terms of network's memory and energy consumption. So, there is a need for decentralized intrusion detection [53]. Wang *et al.*, proposed a scheme to detect whether a node is faulty or malicious with the collaboration of neighbor nodes [54]. It is very difficult to integrate intrusion detection techniques into a uniform hardware platform due to cost and implementation considerations [55]. Zhu *et al.*, proposed an interleaved hop-by-hop

authentication (IHOP) scheme in [56]. Many techniques have been used to design intrusion detection schemes (IDS) for WSN. Here we give a comparison between most popular IDS schemes [57].

4.6. Secure Routing

In Table 5, we compare the different intrusion detection system with their relative advantages and disadvantages. There are a lot of approaches to ensure routing security [14, 15]. The goal of a secure routing protocol for a WSN is to ensure the integrity, authentication, and availability of messages. Secure routing is vital to the acceptance and use of sensor networks for many applications. In [58], the authors define the security attributes of routing protocols in WSNs so that the attackers cannot achieve their goals. Security attributes are the mechanisms that allow the routing protocols to defend against the possible threats in the whole network. The authors in [14], proposed security goals for routing in sensor networks and presents the detailed security analysis of all the major routing protocols as well as energy conserving topology maintenance algorithms for sensor networks. Most current proposals are suitable for static WSNs. Though some secure routing algorithms are proposed based on hierarchical sensor networks, most of these studies did not show the different effects such as energy consumption, security for different cluster size.

4.7. Secure Localization

In a WSN, sensors can be randomly distributed in order to collect data from a site. Knowledge of the position of the sensing nodes in a WSN is an essential part of many sensor network operations and applications. Sensors reporting monitored data need to also report the location where the information is sensed, and hence, sensors need to be aware of their position. The authors in [64], have described a technique called verifiable multilateration (VM). In multilateration, the position of a device is accurately computed from a series of known reference points. The authors have used authenticated ranging and distance bounding to ensure accurate location of a node. In [65], the authors have described a scheme called secure range-independent localization (SeRLoC). The scheme is a decentralized range independent localization scheme.

Table 5. Comparison of Intrusion Detection System

Intrusion detection system(IDS)	Advantage	Shortcomings	Example
Rule based IDS	1. Fast detection 2. Low computational complexity 3. Higher detection accuracy	1. Voting mechanism may increase the communication overhead 2. Absence of standardized evaluation metrics	[59][60]
Data mining and Computational Intelligence (DM/CI) techniques	1. Less communication overhead. 2. Generality is guaranteed 3. Scalability is also guaranteed	1. Slow detection 2. High computational complexity 3. High false alarms	[61]
Game theory based	1. The game theory-	1. The scope of the	[62]

IDS schemes	based IDS schemes do not need extra data to build the model 2. The techniques used in these kinds of schemes are lightweight since no training is involved	game theory-based schemes is limited to some layers information like the routing and application layers information	
Statistical based schemes	1. Mathematically proven and can be used effectively only if the accurate probability distribution model for normal or abnormal traffic is obtained.	1. The process of acquiring the correct probability distribution is not easy. The dynamic streaming of network data makes it difficult to keep the probability distribution model up to date	[63]

4.8. Trust Management System

A key aspect for WSN is the trust on the behavior of the elements of the network. In [66], the authors present a classification of trust methods for ad-hoc and sensor networks. Trust evaluation mechanisms in distributed networks, such as MANETs and sensor networks, have been investigated in [67]. It is clear that any trust management system has to be specially designed and prepared for reacting against the particular issues, such as autonomy, decentralization and initialization that can be found in WSN environments. The trust valued of a node is computed based on the cryptographic suite being applied, availability statistics and the packet forwarding information about the node. If computed trust associated with a node falls below a threshold, the node's location is considered insecure and it is avoided in the routing process.

Table 6. Different trust model with major features

Trust model	Properties	Limitations
Agent based approach-ATSN[68]	1.Runs at middle-ware of every agent node. Applied for multi hop WSN communication topology. Every node monitors the behavior of the neighbor node like forwarding data time and control frame time and processing time for algorithms.	1. ATSN uses agent nodes with more power, long radio range and large storage space than normal sensor node to perform operations. 2. ATSN work with fixed window and aging is specified by considering the positive outcome from the current window.
Weight based trust model[69]	1.The trust is used to eliminate data from malicious node, during data aggregation. 2.The every node is capable enough to compare the	1. The model highly based on synchronism phenomenon.

	receive data with sensed data duration and develop a weight trust model on it.	
Beacon based trust model[70]	1. The system was developed on the location information of the node. Quite slow process for huge node network.	1. The beacon Trust model depends on the neighbor reputation table that highly vulnerable to attacks. Different threshold value to develop trust.

In [71], the authors have proposed a personalized trust model called PET for nodes in a WSN. In [7], for aggregation of various ratings received from its peer sensor nodes, a comprehensive analytical and inference model of trust has been presented. In Table 6, we summarize different trust models with major features.

4.9. Future Research Area

Although research efforts have been made on cryptography, key management, secure routing, secure data aggregation and intrusion detection in WSNs, there are still some challenges to be addressed. The current cryptography mechanisms, such as authentication, identification, etc. may detect and defend against node compromise in some extent. However, most compromise activities cannot be detected immediately. Designing secure routing that can defend against undetected node compromise is a promising research area. Currently, most proposals only consider security metrics and only a few of them evaluate other metrics. So, metrics, such as QoS (quality of service) need to be considered in addition of security. More elaborate studies are needed to be done in the future for some other security issues including security-energy assessment, data assurance, survivability, trust, end to end security, security & privacy support for data centric sensor networks (DCS) and node compromise distribution. It is very important to study these areas due to a sensor network's special characteristics, such as battery limitation, high failure probability nodes, easier compromised nodes, unreliable transmission media, etc. Until now, there have been only a few approaches available. Therefore, more studies are needed in these areas. Although there are some existing architectures for WSN that partially solve these problems, it is still possible to point out the neglected aspects that can be considered crucial for creating a satisfactory trust system.

5. Conclusion

We have described the four main aspects of WSN security: obstacles, requirements, attacks and defenses. In this article, we summarize the typical attacks as well as surveyed the literatures on several important security issues relevant to the sensor networks. Our aim is to provide a general overview of the existing WSNs security approaches. Many security issues in WSNs remain open and we expect to see more research activities on these exciting topics in the future.

References

[1] J. S. Perrig and D. Wagner, "Security in wireless sensor networks", Comm. of the ACM, vol. 47, no. 6, **(2004)**, pp. 53-57.
[2] M. K. Jain, "Wireless sensor networks: security issues & challenges", IJCIT, vol. 2, no. 1, **(2011)**, pp. 62-67.

[3] J. Deng, R. Han and S. Mishra, "INSENS: Intrusion-tolerant routing in wireless sensor networks", Technical Report CUCS- 939-02, Department of Computer Science, University of Colorado at Boulder, **(2002)** November.
[4] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks", Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, ACM Press, **(2000)**, pp. 243-254.
[5] L. Hu and D. Evans, "Secure aggregation for wireless networks", Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), **(2003)**, pp. 384.
[6] B. Przydatek, D. Song and A. Perrig, "SIA: secure information aggregation in sensor networks", Proceedings of the 1st International Conference on Embedded Networked Systems (SenSys'03), New York, ACM Press, **(2003)**, pp. 255- 265.
[7] Z. Liang and W. Shi, "Analysis of ratings on trust inference in the open environment", Technical report MIST-TR-2005-002, Department of computer Science, Wayne State University, **(2005)** February.
[8] Z. Liang and W. Shi, "Enforcing cooperative resource sharing in untrusted peer-to-peer environment", ACM Journal of Mobile Networks and Applications (MONET), vol. 10, no. 6, **(2005)**, pp. 771-783.
[9] G. Bianchi, "A comparative study of the various security approaches used in wireless sensor networks," International journal of advanced science and technology, vol. 17, **(2010)** April, pp. 31-44.
[10] T. A. Zia, "A Security Framework for Wireless Sensor Networks", http://ses.library.usyd.edu.au/ bitstream/2123/2258/4/02whole.pdf, **(2008)**.
[11] Y. C. Hu, A. Perrig and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks", Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '03), San Francisco, CA, March, vol. 3, **(2003)**, pp. 1976-1986.
[12] H. Chan, A. Perrig and D. Song, "Random key pre distribution schemes for sensor networks", Proceedings of the IEEE Symposium on Security and Privacy, IEEE Computer Society, **(2003)** May, pp. 197.
[13] D. Liu, P. Ning and R. Li, "Establishing pair-wise keys in distributed sensor networks", ACM Transactions on Information Systems Security, vol. 8, no. 1,**(2005)**, pp. 41-77.
[14] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures", Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network (SNPA), **(2003)** September, pp. 293-315.
[15] X. Chen, K. Makki, K. Yen and N. Pissinou, "Sensor Network Security: A Survey", IEEE Communications Surveys & Tutorials, vol. 11, no. 2, Second Quarter **(2009)**, pp. 52-73.
[16] M. Saxena, "Security in Wireless Sensor Networks-A Layer based classification", Technical Report, Center for Education and Research in Information Assurance and Security-CERIAS, Purdue University. pages.cs.wisc.edu/~msaxena/papers/2007-04-cerias.pdf, **(2007)**.
[17] J. Sen, "A Survey on Wireless Sensor network Security", International Journal of Communications Network and Information Security", vol. 1, no. 2, **(2009)** August, pp. 59-82.
[18] P. Mohanty, S. Panigrahi, N. Sarma and S. S. Satapathy, "Security issues in wireless data gathering protocols", Journal of theoretical and applied information technology, vol. 13, no. 1, **(2010)**, pp. 14-27.
[19] X. Wang, W. Gu, K. Schosek, S. Chellappan and D. Xuan, "Sensor network configuration under physical attacks", Technical report (OSU-CISRC-7/04-TR45), Department of Computer Science and Engineering, Ohio State University, **(2004)** July.
[20] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, vol. 40, no. 8, **(2002)** August, pp. 102-114.
[21] M. Sharifnejad, M. Shari, M. Ghiasabadi and S. Beheshti, "A Survey on Wireless Sensor Networks Security", SETIT, **(2007)**.
[22] B. T. Wang and H. Schulzrinne, "An IP traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, vol. 2, **(2004)** May 2-5, pp. 901-904.
[23] A. D. Wood and J. Stankovic, "Denial of service in sensor network", IEEE Computer Magazine, vol. 35, no. 10, **(2002)** October, pp. 54-62.
[24] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, **(2003)** May, pp. 113-127.
[25] J. R. Douceur, "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), LNCS, vol. 2429, **(2002)** March, pp. 251-260.
[26] R. Sivakumar, P. Sinha and V. Bharghavan, "Core extraction distributed ad hoc routing (CEDAR) specification", IETF Internet draft draft-ietf-manet-cedar-spec-00.txt, **(1998)**.
[27] S. Sharma, D. Kumar and R. Kumar, "QOS-Based Routing Protocol in WSN", Advances in Wireless and Mobile Communications, vol. 1, no. 1-3, **(2008)**, pp. 51-57.
[28] V. Rodoplu and T. H. Ming, "Minimum energy mobile wireless networks", IEEE Journal of Selected Areas in Communications, vol. 17, no. 8, **(1999)**, pp. 1333-1344.

[29] Y. Xu, J. Heidemann and D. Estrin, "Geography-informed energy conservation for ad hoc routing", The Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom_01), Rome, Italy, **(2001)**, pp. 70-84.
[30] S. Lindsey and C. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems", IEEE Aerospace Conference Proceedings, vol. 3, **(2002)**, pp. 1125-1130.
[31] F. Ye, H. Luo, J. Cheng, S. Lu and L. Zhang, "A Two-tier data dissemination model for large-scale wireless sensor networks", The proceedings of ACM/IEEE MOBICOM, **(2002)**, pp. 148-159.
[32] W. Heinzelman, J. Kulik and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks", The Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom_99), Seattle, WA, **(1999)**, pp. 174-185.
[33] K. Anipindi, "Routing in Sensor Networks", University of Texas at Arlington, Arlington, http://crystal.uta.edu/~kumar/cse6392/termpapers/Kalyani_paper.pdf, **(2002)**.
[34] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no. 5, **(2002)**, pp. 521-534.
[35] M. Brown, D. Cheung, D. Hankerson, J. L. Hernandez, M. Kirkup and A. Menezes, "PGP in constrained wireless devices", Proceedings of the 9th USENIX Security Symposium, **(2000)** August.
[36] A. S. Wander, N. Gura, H. Eberle, V. Gupta and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks", Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communication, **(2005)** March.
[37] M. O. Rabin, "Digitalized Signatures and Public-Key Functions as Intractable as Factorization", Cambridge, MA, Technical Report, **(1979)**.
[38] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol. 26, no. 1, **(1983)**, pp. 96-99.
[39] V. S. Miller, "Use of elliptic curves in cryptography", Lecture Notes in Computer Sciences: 218 on Advances in Cryptology- CRYPTO 85, New York, Springer-Verlag, **(1986)**, pp. 417-426.
[40] N. Kobiltz, "Elliptic curve cryptosystems", Mathematics of Computation, vol. 48, **(1987)**, pp. 203-209.
[41] A. J. Menezes, S. A. Vanstone and P. C. V. Oorschot, "Handbook of Applied Cryptography", CRC Press, Boca Raton, FL, **(1996)**.
[42] R. L. Rivest, "The RC5 encryption algorithm", Fast Software Encryption, B. Preneel, Ed. Springer, **(1995)**, pp. 86-96.
[43] D. Eastlake and P. Jones, "U.S. Secure Hash algorithm 1 (SHA1)", RFC 3174 (Informational), **(2001)** September.
[44] R. L. Rivest, "The MD5 Message-Digest Algorithm", RFC 1321, **(1992)** April.
[45] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes", Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications, New York, ACM Press, **(2003)**, pp. 151-159.
[46] S. Zhu, S. Setia and S. Jajodia. "Leap: efficient security mechanisms for large scale distributed sensor networks", CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, New York, USA, **(2003)**, pp. 62-72.
[47] R. Di Pietro, L.V. Mancini, Y. W. Law, S. Etalle and P. Havinga, "LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks", Proceedings of the 32nd International Conference on Parallel Processing Workshops (ICPPW'03), IEEE Computer Society Press, **(2003)**, pp. 397- 406.
[48] J. Lee and D. R. Stinson, "Deterministic key pre-distribution schemes for distributed sensor networks", Proceedings of Selected Areas in Cryptography, **(2004)**, pp. 294-307.
[49] B. Lai, S. Kim and I. Verbauwhede, "Scalable session key construction protocols for wireless sensor networks", IEEE Workshop on Large Scale Real Time and Embedded Systems, **(2002)**.
[50] D. D. Hwang, B. Lai and I. Verbauwhede, "Energy-memory security tradeoffs in distributed sensor networks", Proceedings of the 3rd International Conference on Ad-hoc Networks and Wireless, **(2004)** July, pp. 70-81.
[51] D. Liu and P. Ning, "Location-based pair-wise key establishments for static sensor networks", Proceedings of the ACM Workshop on Security in Ad hoc and Sensor Networks, **(2003)** October.
[52] D. Djenouri, L. Khelladi and A. Nadjib Badache, "A Survey Of Security Issues In Mobile Ad Hoc And Sensor Networks", IEEE Communications Surveys & Tutorials, vol. 7, no. 4 ,Fourth Quarter **(2005)**.
[53] E. J. Palomo, E. Domínguez, R. M. Luque and J. Muñoz, "An Intrusion Detection System based on Hierarchical Self-Organization", Journal of Information Assurance and Security, vol 4, no. 3, **(2009)**, pp. 209-216.
[54] S. Zhu, S. Setia, S. Jajodia and P. Ning, "An interleaved hopby- hop authentication scheme for filtering of injected false data in sensor networks", Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA, **(2004)** May, pp. 259-271.

[55] Y. Zhou, Y. Fang and Y. Zhang, "Securing Wireless Sensor Networks: A Survey", IEEE Communications Surveys & Tutorials, vol. 10, no. 3, Third Quarter **(2008)**, pp. 6-28.
[56] G. Wang, W. Zhang, C. Cao and T. L. Porta, "On supporting distributed collaboration in sensor networks", Proceedings of MILCOM, **(2003)**.
[57] M. A. Rassam, M. A. Maarof and A. Zainal, "A survey of Intrusion Detection Schemes in Wireless Sensor Networks", vol. 9, no. 10, **(2012)**, pp. 1636-1652.
[58] M. Nikjoo, A. S. Tehrani and P. Kumarawadu, "Secure Routing in Sensor Networks", IEEE, **(2007)**, pp. 978-981.
[59] M. V. D. S. Lemos, L.B. Leal and R. H. Filho, "A new collaborative approach for intrusion detection system on wireless sensor networks", Novel Algorithms Techniques Telecommu,Netw. DOI:10.1007/978-90-481-3662-9_41, **(2010)**.
[60] Y. A. Ponomarchuk and D. W. Seo, "Intrusion detection based on traffic analysis and fuzzy inference system in wireless sensor networks", J. Convergence, vol. 1, **(2010)**, pp. 35-42.
[61] R. Muraleedharan and L. A. Osadciw, "An intrusion detection framework for sensor networks using ant colony", Proceedings of the 43rd Asilomar Conference on Signals, Systems and Computers, IEEE Xplore Press, Pacific Grove, California,USA, DOI:10.1109/ACSSC.2009.5470103, **(2009)**, pp. 275-278.
[62] Y. B. Reddy and S. Srivathsan, "Game theory model for selective forward attacks in wireless sensor networks", Proceedings of the 17th Mediterranean Conference on Control and Automation, IEEE Xplore Press, Thessaloniki, pp. 458-463. DOI:10.1109/MED.2009.5164584, **(2009)** June 24-26
[63] G. Li, J. He and Y. Fu, "Group-based intrusion detection system in wireless sensor networks", Comput. Commun., DOI: 10.1016/j.comcom.2008.06.020, vol. 31, **(2008)**, pp. 4324-4332.
[64] S. Capkun and J.-P. Hubaux, "Secure positioning in wireless networks", IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, **(2006)**, pp. 221-232.
[65] L. Lazos and R. Poovendran, "SERLOC: Robust localization for wireless sensor networks", ACM Transactions on Sensor Networks, vol. 1, no. 1, **(2005)**, pp. 73-100.
[66] E. Aivaloglou, S. Gritzalis and C. Skianis, "Trust Establishment in Ad Hoc and Sensor Networks", Proc. of 1st International Workshop on Critical Information Infrastructure Security, CRITIS'06, Lectures Notes in Computer Science, LNCS, Samos, Greece, Springer, vol. 4347, **(2006)**, pp. 179-194.
[67] Y. Sun, Z. Han and K. J. Ray Liu, "Defense of Trust Management Vulnerabilities in Distributed Networks", IEEE Communications Magazine, **(2008)** February, pp. 112-119.
[68] H. Chen, H. Wu and X. Zhou, "Reputation-based Trust in Wireless Sensor Network", IEEE International Conference on Multimedia and Ubiquitous Engineering, (MUE'07), Shanghai, **(2007)** April 26-27, pp. 603-607.
[69] P. Lapsiwala and R. Kshirsagar, "Authentication and Intrusion Detection Topology for Wireless Sensor Network", International Conference on Electronics, Information and Communication System Engineering (ICEICE), Jodhpur, India, **(2010)**.
[70] D. Liu, P. Ning and W. Du, "Detecting Malicious Beacon node for Secure Location Recovery in Wireless Sensor Networks", 25th IEEE International Conference on Distributed Computing Systems (ICDCS '05), **(2005)**.
[71] Z. Liang and W. Shi, "PET: A Personalized Trust model with reputation and risk evaluation for P2P resource sharing", Proceedings of the HICSS-38, Hilton Waikoloa Village Big Island, Hawaii, **(2005)** January.

Authors

Mahfuzulhoq Chowdhury received the B. Sc. Engineering Degree in computer science and engineering from Chittagong University of Engineering and Technology, Bangladesh, in 2010. From September 2010 onwards he has been serving as a faculty member in the Department of Computer Science and Engg., Chittagong University of Engineering and Technology (CUET), Chittagong, Bangladesh. He is currently working toward the M.Sc. Engineering degree in the Department of CSE, CUET, Bangladesh. His major researches include cognitive radio networks, cryptography, wireless sensor networks etc.

Md Fazlul Kader received the B. Sc. Engineering Degree in Computer Science and engineering (CSE) from Chittagong University of Engineering and Technology (CUET), Bangladesh, in 2005. From 2007 onwards he has been serving as a faculty member in the Dept. of Applied Physics, Electronics and Communication Engineering, University of Chittagong, Bangladesh. He is currently working toward the M.Sc. Engineering degree in the Department of CSE, CUET, Bangladesh. His major research interests include cognitive radio networks, cooperative communications, wireless sensor networks, computer network, pattern recognition etc.

Asaduzzaman received the B. Sc. Engineering Degree in electrical and electronics engineering from Chittagong University of Engineering and Technology, Bangladesh, in 2001. From 2001 onwards he has been serving as a faculty member in the Department of Computer Science and Engg., Chittagong University of Engineering and Technology (CUET), Chittagong, Bangladesh. He received his Ph.D. from the Department of Electrical Engineering, University of Ulsan, Korea in 2010. His major research interests include wireless communication systems with emphasis on cooperative communications and MIMO systems, wireless sensor networks, modulation and coding techniques, cognitive radio, etc.