Journal of Information Assurance and Security 5 (2010) 031-044

Security Vulnerabilities In Wireless Sensor Networks: A Survey

T.Kavitha[1], D.Sridharan[2]

[1] Department of Electronics and Communication Engineering
College of Engineering Guindy
Anna University – Chennai, India
haikavi18@yahoo.co.in

[2] Department of Electronics and Communication Engineering
College of Engineering Guindy
Anna University – Chennai, India
sridhar@annauniv.edu

Abstract: The significant advances of hardware manufacturing technology and the development of efficient software algorithms make technically and economically feasible a network composed of numerous, small, low-cost sensors using wireless communications, that is, a wireless sensor network (WSN). Security is becoming a major concern for WSN protocol designers because of the wide security-critical applications of WSNs. In this article, how WSN differs from wired network and other wireless network and also basic information about the WSN and its security issues compared with wired network and other wireless networks is discoursed. Summarization of typical attacks on sensor networks and survey about the literatures on several important security issues relevant to the sensor networks are also dissertated.

Keywords: Wireless Sensor Network, Security, Vulnerabilities, Security Mechanism.

1. Introduction

One of the key issues rising from switching to wireless communication lies in security; while an air gap is among the most effective security measures in wired networks, wireless communication is not as easy to isolate from attack. The security issues in MANETs are more challenging than those in traditional wired computer networks and the Internet. Providing security in sensor networks is even more difficult than in MANETs due to the resource limitations of sensor nodes and security concerns remain a serious impediment to widespread adoption of these WSNs [27].

1.1 Wired & Wireless Networks

Wireless networks have offered attractive flexibility to both network operators and users. Ubiquitous network coverage, for both local and wide areas, is provided without the cost of deploying and maintaining the wires. This fact is extremely useful in several situation like network deployment in difficult to wire areas, prohibition of cable deployment and deployment of a temporary network. Mobility support is another salient feature of wireless networks.

Although most, if not all, security threats against the TCP/IP stack in a wired network are equally applicable to an IP-based wireless network, the latter possesses a number of additional vulnerabilities; wireless medium unreliability, spectrum use, power management, security, limited bandwidth, system complexity, routing, Interfacing with wired networks and health concern make it more challenging to secure [19], [17].

1.2 WSN vs. MANET

WSNs are used in many interesting applications. Realization of these applications requires wireless ad hoc networking techniques. Although many protocols and algorithms have been proposed for traditional wireless ad hoc networks, they are not well suited to the unique features and application requirements of sensor networks. To illustrate this point, the differences between sensor networks and ad hoc networks are given below [9]:

1. The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
2. Sensor nodes are densely deployed.
3. Sensor nodes are prone to failures.
4. The topology of a sensor network changes very frequently.
5. Sensor nodes mainly use a broadcast communication paradigm, whereas most ad hoc networks are based on point-to-point communications.
6. Sensor nodes are limited in power, computational capacities, and memory. Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.

1.3 The Organization of This Article

Though there are varieties of challenges in sensor networks, here we focus on different security issues and possible remedies of those. Though security is a very important issue in WSN, due to various resource limitations and the salient features of a WSN, the security design for such networks is significantly challenging. In this paper, we explore the security issues and challenges for next generation WSNs and discuss the crucial parameters that require extensive investigations. This article is structured as follows. In the next section some basic information about the WSNs is given. Section 3 reports on Security aspect of WSNs. Section 4 emphasizes taxonomy of different types of attacks. Lastly, section 5 covers security issues and possible future directions in this area.

Received June 23, 2009

2 Wireless Sensor Network

2.1 Operation

A WSN is a large network of resource-constrained sensor nodes with multiple preset functions, such as sensing and processing, to fulfill different application objectives. The major elements of WSN are the sensor nodes and the base stations. In fact, they can be abstracted as the “sensing cells” and the “brain” of the network, respectively.

Usually, sensor nodes are deployed in a designated area by an authority and then, automatically form a network through wireless communications. Sensor nodes of homogeneous or heterogeneous type can be deployed randomly or at pre-determined locations using a deterministic scheme. Sensor nodes are static most of the time, whereas mobile nodes can be deployed according to application requirements. One or several, static or mobile[10] base stations (BSs) are deployed together with the network.

Sensor nodes keep monitoring the network area after being deployed. After an event of interest occurs, one of the surrounding sensor nodes can detect it, generate a report, and transmit the report to a BS through multi hop wireless links. Collaboration can be carried out if multiple surrounding nodes detect the same event. In this case, one of them generates a final report after collaborating with the other nodes. The BS can process the report and then forward it through either high-quality wireless or wired links to the external world for further processing. The WSN authority can send commands or queries to a BS, which spreads those commands or queries into the network. Hence, a BS acts as a gateway between the WSN and the external world. An example is illustrated in Figure. 1.

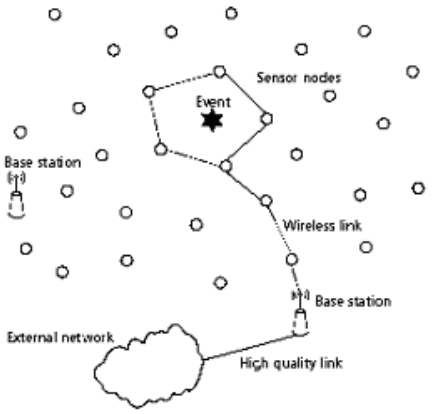

Figure 1. A wireless sensor network.

2.2 Hardware Components of Sensor Node

When choosing the hardware components for a wireless sensor node, evidently the application’s requirements play a decisive factor. A sensor node integrates hardware and software for sensing, data processing, and communication. They rely on wireless channels for transmitting data to and receiving data from other nodes. Figure 2 illustrates the basic structure of a sensor node. The lifetime of a sensor node depends to a large extent on the battery lifetime; hence it is extremely important to adopt energy-efficient strategies for information processing [9],[7].

A sensor node is made up of a sensing unit, a processing unit, a transceiver unit, and a power unit as shown in Figure 2. They may also have additional application-dependent components such as a location finding system, power generator, and mobilizer. Sensors, the actual interface to the physical world: devices that can observe or control physical parameters of the environment is converted to digital signals by the ADC, and then fed into the processing unit. The processing unit, which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to the network. Power units may be supported by power scavenging units such as solar cells.

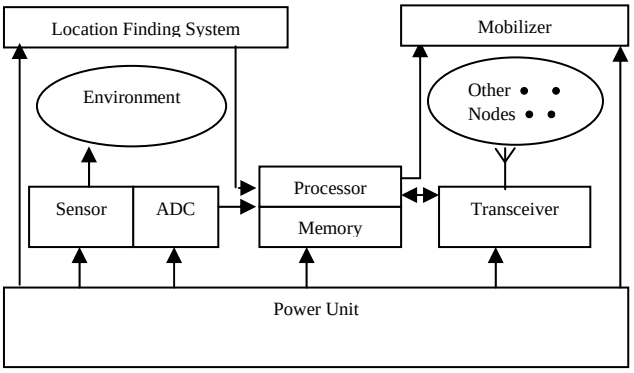

Figure 2. Sensor node architecture

Most of the sensor network routing techniques and sensing tasks require knowledge of location with high accuracy. Thus, it is common that a sensor node has a location finding system. A mobilizer may sometimes be needed to move sensor nodes when it is required to carry out the assigned tasks.

2.3 Software Components of Sensor Node

2.3.1 Operating System/Software

Traditional OS are not suitable for wireless sensor networks because WSNs have constrained resources and diverse data-centric applications, in addition to a variable topology. WSNs need a new type of operating system, considering their special characteristics.

Sensor operating systems (SOS) should embody the following functions, bearing in mind the limited resource of sensor nodes [14], [15]:

- Should be compact and small in size
- Should provide real-time support
- Should provide efficient resource management mechanisms.
- Should support reliable and efficient code distribution
- Should support power management
- Should provide a generic programming interface up to sensor middleware or application software
- Should support parallel processing along with threading when a sensor is deployed for multiple purposes.

2.3.2 Querying Sensor Network

For the placement, management, and processing of the sensor data, a data storage, management and query processing policy is necessary. A sensor database is needed that can store dynamic information. A web accessible query processing system is needed to provide replies to high-level user queries. Unfortunately, the resource constraints related to sensor nodes such as computation, communication, power consumption, uncertainty in sensor readings have posed a numerous challenges in query processing for sensor networks [20].

2.4 Sensor Node Types

Desirable functionality of sensor nodes in a WSN include: ease of installation, self-indication, self-diagnosis, reliability, time awareness for coordination with other nodes, some software functions and DSP, and standard control protocols and network interfaces.

There are many sensor manufacturers and it is too costly for them to make special transducers for every network on the market. Different components made by different manufacturers should be compatible. Therefore, in 1993, the IEEE and the National Institute of Standards and Technology (NIST) began work on a standard for smart sensor networks. IEEE 1451, the standard for smart sensor networks was the result 13]. Commercially available sensors of many types [18] are suitable for wireless network applications.

2.5 Protocol Stack

The protocol stack used by the sink and sensor nodes shown in Figure 1 is given in Figure 3**.** This protocol stack combines power and routing awareness, integrates data with networking protocols, communicates power efficiently through the wireless medium, and promotes cooperative efforts of sensor nodes [2].

The physical layer addresses the needs of simple but robust modulation, transmission, and receiving techniques. It is responsible for frequency selection, carrier frequency generation, signal detection, and signal processing and data encryption.

The data link layer is responsible for the multiplexing of data streams, data frame detection, medium access flow control and error control. It ensures reliable point-to-point and point-to-multipoint connections in a communication network.

The network layer takes care of routing the data supplied by the transport layer. It is responsible for specifying the assignment of addresses and how packets are forwarded – Routing.

The transport layer helps to maintain the flow of data if the sensor networks application requires it. This layer is especially needed when the system is planned to be accessed through the Internet or other external networks.

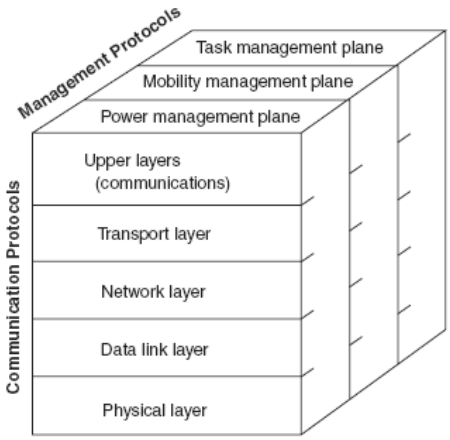

Figure 3. Generic protocol stack for sensor networks

Application layer Depending on the sensing tasks, different types of application software can be built and used.

The power management plane manages how a sensor node uses its power. The mobility management plane detects and registers the movement of sensor nodes, so a route back to the user is always maintained, and the sensor nodes can keep track of who their neighbor sensor nodes are. By knowing who the neighbor sensor nodes are, the sensor nodes can balance their power and task usage. The task management plane balances and schedules the sensing tasks given to a specific region.

These management planes are needed so that sensor nodes can work together in a power efficient way, route data in a mobile sensor network, and share resources between sensor nodes.

2.6 Constraints

Individual sensor nodes in a WSN have the inherent limitations in resources, which make the design of security procedures more complicated. A typical sensor node processor is of 4-8 MHz, having 4KB of RAM, 128KB flash and ideally 916 MHz of radio frequency. Each of these limitations is due in part to the two greatest constraints — limited energy and physical size.

Energy: Sensor nodes typically have a small form factor with a limited amount of battery power. Therefore, protocols designed for sensor networks should utilize only a few control messages. Sensor transducer, communication among sensor nodes and microprocessor computation consumes energy in sensor nodes. In that communication consumes more energy in WSNs. Any message expansion caused by security mechanisms comes at a significant cost. Further, higher security levels in WSNs usually correspond to more energy consumption for cryptographic functions.

Memory: Sensor nodes usually have a small amount of memory. Hence, sensor network protocols should not require the storage of a large amount of information at the sensor node. There is usually not enough space to run complicated algorithms after loading OS and application code. This makes it impractical to use the majority of current security algorithms.

Transmission range: the communication range of sensor nodes is limited both technically and by the need to conserve energy.

Fault Tolerance: Sensor nodes are prone to failure. This may be due to a variety of reasons. Loss of battery power may lead to failure of the sensor nodes. Thus, protocols designers should build fault tolerance into their algorithms for improving the utility of sensor networks.

Self-Organization: Sensor nodes are often air-dropped in hostile or harmful environments. It is not possible for humans to reach these sensor nodes. Besides, it is not possible for humans to repair each sensor node, as often the number of sensor nodes is quite large. Hence, self-organization of sensor nodes to form a connected network is an essential requirement.

Scalability: The number of sensor nodes in a sensor network can be in the order of hundreds or even thousands. Hence, protocols designed for sensor networks should be highly scalable.

2.7 Performance Metrics of Sensor Network

It is necessary to examine a list of metrics that determine the performance of a sensor network [17],[12]:

Energy efficiency/system lifetime: The sensors are battery operated, rendering energy a very scarce resource that must be wisely managed in order to extend the lifetime of the network.

Coverage: It is always advantageous to have the ability to deploy a network over a larger physical area. Multi-hop communication techniques can extend the coverage of the network; but increase the power consumption of the nodes, which may decrease the network lifetime. Additionally, they require a minimal node density, which may increase the deployment cost.

Cost and ease of deployment: For system deployments to be successful, the WSNs must configure itself for any possible physical node placement. In the long term, the total cost of ownership for a system may have more to do with the maintenance cost than the initial deployment cost.

Response Time/Latency: Many sensor applications require delay-guaranteed service. Protocols must ensure that sensed data will be delivered to the user within a certain delay. The ability to have low response time conflicts with many of the techniques used to increase network lifetime.

Accuracy: Obtaining accurate information is the primary objective; accuracy can be improved through joint detection and estimation.

Fault tolerance: Robustness to sensor and link failures must be achieved through redundancy and collaborative processing and communication.

Scalability: Because a sensor network may contain thousands of nodes, scalability is a critical factor that guarantees that the network performance does not significantly degrade as the network size increases.

Transport capacity/throughput: Because most sensor data must be delivered to a single base station or fusion center, a critical area in the sensor network exists, whose sensor nodes must relay the data generated by virtually all nodes in the network. Apparently, this area has a paramount influence on system lifetime, packet end-to-end delay, and scalability.

Security: WSNs must be capable of keeping the information they are collecting private from eavesdropping. Use of encryption and cryptographic authentication costs both power and network bandwidth. This impacts application performance by decreasing the number of samples than can be extracted from a given network and the expected network lifetime.

Effective Sample Rate It is the sample rate that sensor data can be taken at each individual sensor and communicated to a collection point in a data collection network. In-network processing can increase the effective sample rate.

2.8 Individual Node Evaluation Metrics

It can be linked that the system performance metrics down to the individual node characteristics that support them. The end goal is to understand how changes to the low-level system architecture impact application performance [12].

Power: To meet the multi-year application requirements individual sensor nodes must be incredibly low power. This can be achieved by combining both low-power hardware components and low duty-cycle operation techniques.

Flexibility: Each application scenario will demand a slightly different mix of lifetime, sample rate, response time and in-network processing. WSN architecture must be flexible enough to accommodate a wide range of application behaviors.

Robustness: In order to support the lifetime requirements demanded, each node must be constructed to be as robust as possible. System modularity is a powerful tool that can be used to develop a robust system.

Security: In order to meet the application level security requirements, the individual nodes must be capable of performing complex encrypting and authentication algorithms. In addition to securing all data transmission, the nodes themselves must secure the data that they contain.

Communication: A key evaluation metric for any WSN is its communication rate, power consumption, and range. Higher communication rates translate into the ability to achieve higher effective sampling rates and lower network power consumption. As bit rates increase, transmissions takes less time and therefore potentially require less energy.

Computation: The two most computationally intensive operations for a wireless sensor node are the in-network data processing and the management of the low-level wireless communication protocols. Higher communication rates required faster computation. The same is true for processing being performed on sensor data.

Time Synchronization: In order to support time correlated sensor readings and low-duty cycle operation of our data collection application scenario; nodes must be able to maintain precise time synchronization with other members of the network. Errors in the timing mechanism will create inefficiencies that result in increased duty cycles.

Size & Cost: The physical size and cost of each individual sensor node has a significant and direct impact on the ease and cost of deployment. Total cost of ownership and initial deployment cost are two key factors that will drive the adoption of WSN technologies. Physical size also impacts the ease of network deployment. Smaller nodes can be placed in more locations and used in more scenarios.

2.9 Application

Regarding the services offered by a WSN, they could be classified into three major categories: monitoring, alerting, and provisioning of information “on demand”. Traditionally, sensor networks have been used in the context of high-end applications. More recently, interest has focusing on networked biological and chemical sensors for national security applications.

3. Security

3.1 Why Need Security?

Wireless mobile ad hoc networks (MANETs) and sensor networks have many applications in military, homeland security, and other areas. In that many sensor networks have mission-critical tasks. Security is critical for such networks deployed in hostile environments, and security concerns remain a serious impediment to widespread adoption of these wireless networks. The security issues in MANETs are more challenging than those in traditional wired computer networks and the Internet. Providing security in sensor networks is even more difficult than in MANETs due to the resource limitations of sensor nodes. Most sensor networks actively monitor their surroundings, and it is often easy to deduce information other than the data monitored. Such unwanted information leakage often results in privacy breaches of the people in the environment. Moreover, the wireless communication employed by sensor networks facilitates eavesdropping and packet injection by an adversary. The combination of these factors demands security for sensor networks at design time to ensure operation safety, secrecy of sensitive data, and privacy for people in sensor environments [6]. Significant efforts and

research have been undertaken to enhance security levels of wireless networks. Currently, there are three levels of security available in wireless networking environments [25].

3.2 Why Security Complicated In WSN?

Security in sensor networks is complicated by the constrained capabilities of sensor node hardware and the properties of the deployment [6],[4] and [10].

- The overall cost of the WSN should be as low as possible.
- Sensor nodes are susceptible to physical capture, but because of their targeted low cost, tamper-resistant hardware are unlikely to prevail. Sensor nodes use wireless communication, which is particularly easy to eavesdrop on.
- Similarly, an attacker can easily inject malicious messages into the wireless network.
- Advanced anti-jamming techniques such as frequency-hopping spread spectrum and physical tamper proofing of nodes are generally impossible in a sensor network due to the requirements of greater design complexity and higher energy consumption.
- The use of radio transmission, along with the constraints of small size, low cost, and limited energy, make WSNs more susceptible to denial-of-service attacks.
- Ad-hoc networking topology of WSN facilitates attackers for different types of link attacks ranging from passive eavesdropping to active interfering. Attacks on a WSN can come from all directions and target at any node leading to leaking of secret information, interfering message, impersonating nodes etc.
- Security also needs to scale to large-scale deployments. Most current standard security protocols were designed for two-party settings and do not scale to a large number of participants.
- There is a conflicting interest between minimization of resource consumption and maximization of security level. A better solution actually gives a good compromise between these two.
- 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.
- Instead, most security schemes make use of symmetric key cryptography. One thing required in either case is the use of keys for secure communication. Managing key distribution is not unique to WSNs, but again constraints such as small memory capacity make centralized keying techniques impossible.

3.3 Security Requirements

In short, the goal of security is to provide security services to defend against all the kinds of threat explained in this chapter. The paper [46] provides the analysis of security and survivability requirements concern with the design goals of scalability, efficiency, key connectivity, resilience and reliability. Security services include the following**:** [11], [47]

Authentication ensures that the other end of a connection or the originator of a packet is the node that is claimed. *Access-control* prevents unauthorized access to a resource. *Confidentiality* protects overall content or a field in a message. Confidentiality can also be required to prevent an adversary from undertaking traffic analysis. *Privacy* prevents adversaries from obtaining information that may have private content. The private information may be obtained through the analysis of traffic patterns, i.e. frequency, source node, routes, etc. Ensures that a packet is not modified during transmission is known as *Integrity. Authorization:* authorizes another node to update information (import authorization) or to receive information (export authorization). *Anonymity* hides the source of a packet or frame. It is a service that can help with data confidentiality and privacy. *Non-repudiation* proves the source of a packet. In authentication the source proves its identity. Non-repudiation prevents the source from denying that it sent a packet. *Freshness* ensures that a malicious node does not resend previously captured packets. *Availability* mainly targets DoS attacks and is the ability to sustain the networking functionalities without any interruption due to security threats. *Resilience to attacks* required to sustain the network functionalities when a portion of nodes is compromised or destroyed. In *Forward secrecy* a sensor should not be able to read any future messages after it leaves the network. In *Backward secrecy* a joining sensor should not be able to read any previously transmitted message. *Survivability* is the ability to provide a minimum level of service in the presence of power loss, failures or attacks. Ability to change security level as resource availability changes is the *Degradation of security services.*

3.4 Guiding Principles for Securing WSN

As an initial contribution towards developing a paradigm for securing sensor networks based on a holistic approach to securing multiple layers in the protocol stack. Wang [24] proposed a set of principles for addressing the problem of securing wireless sensor networks. A solution in the context of these principles supports a differential security service that can be dynamically configured to cope with changing network state.

- Security of a network is determined by the security over all layers.
- In a massively distributed network, security measures should be amenable to dynamic reconfiguration and decentralized management.
- In a given network, at any given time, the cost incurred due to the security measures should not exceed the cost assessed due to the security risks at that time.
- If physical security of nodes in a network is not guaranteed, the security measures must be resilient to physical tampering with nodes in the field of operation.

3.5 Holistic Security in WSN

A holistic approach [23] aims at improving the performance of WSNs with respect to security, longevity and connectivity under changing environmental conditions. The holistic approach of security concerns about involving all the layers for ensuring overall security in a network. For such a network, a single security solution for a single layer might not be an efficient solution rather security is to be ensured for all the layers of the protocol stack that is employing a holistic approach could be the best option.

3.6 Cross Layer Design for Secure WSN

Because sensor networks pose unique challenges, traditional security techniques used in traditional networks cannot be applied directly. Because of various constraints in WSN the following aspects should be carefully considered when designing a security scheme: Power efficiency, Node Density and Reliability, Adaptive security, Self configurability, Simplicity and local ID. To effectively

address the above issues, it may be advantageous to break with the conventional layering rules for networking software.

Layered security schemes have been shown to be inadequate and/or inefficient because of the following limitations [49].

i. Redundant Security Provisioning: without a systematic view, individual security protocols developed for different individual protocol layers might provide redundant security services, and hence consume more WSN resource than necessary.

ii. Non-adaptive Security Services: Because attacks on a WSN come from any layers any protocols, a counterattack scheme in some protocol layer is unlikely to guarantee security all the time.

iii. Power Inefficiency: In designing a sensor network, a very important problem we must consider is energy efficiency. The power efficiency design cannot be addressed completely at any single layer in the networking stack.

The point one in section 3.4 is actually on cross-layer security design. Owing to its extreme vulnerability, satisfactory security provisioning in WSN is crucial. However, as discussed in the previous sections, security based on layered design is often inadequate. Moreover, a highly secure mechanism inevitably often consumes a rather large amount of system resources, which in turn may unintentionally cause a security service Denial of Service attack. As a result, the cross-layer design is believed to provide a better security solution.

3.7 Security by Wireless – Using Wireless Properties to Increase Security

Every cryptographic design is based on the principles of confusion and diffusion, as identified in Shannon's landmark paper "Communication Theory of Secrecy Systems" [21]. Confusion refers to a relationship between a secret key and a cipher text; such a relationship should be kept as complex and as possible. Diffusion aims to reduce any statistical relationship between the plaintext and the cipher text as far as possible.

Interestingly, such a diffuse relationship between input and output may also be found in wireless communication. It is well investigated that even a small change in physical position, antenna orientation or subtle changes of the physical environment strongly affect the signal strength measured at a receiver, especially in transmissions lacking Line-Of-Sight (LOS). Rather than using substitution and transposition to induce chaotic properties, physical phenomena of wave propagation such as reflection, diffraction, scattering and fading account for properties similar to confusion and diffusion. In a security context, this means that determining the exact physical configuration that produces a specific set of signal properties at the receiver may equal an exhaustive brute-force attack on a search space defined by the available physical positions, frequencies, transmission power levels, etc. The idea of security by wireless [26] is to use wireless properties offered by the communication itself to design lightweight security mechanisms.

3.8 Evaluation Metrics to Security Scheme

In [9],[23], following metrics are suggested to evaluate whether a security scheme is appropriate for WSNs .

• Security: a security scheme has to meet the requirements discussed above.

• Resiliency: in case a few nodes are compromised, a security scheme should still protect against the attacks.

• Energy efficiency: a security scheme must be energy efficient so as to maximize node and network lifetime.

• Flexibility: key management needs to be flexible so as to allow for different network deployment methods, such as random node scattering and predetermined node placement.

• Scalability: a security scheme should be able to scale without compromising the security requirements.

• Fault-tolerance: a security scheme should continue to provide security services in the presence of faults such as failed nodes.

• Self-healing: sensors may fail or run out of energy. The remaining sensors may need to be reorganized to maintain a set level of security.

• Assurance: assurance is the ability to disseminate different information at different levels to end-users. A security scheme should offer choices with regard to desired reliability, latency, and so on.

4 Taxonomy of Attacks

Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, WSNs have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. For a large-scale sensor network, it is impractical to monitor and protect each individual sensor from physical or logical attack. Attackers may device different types of security threats to make the WSN system unstable. Here in this section we present a layer-based classification of WSN security threats and also based on the capability of the attacker and defenses proposed in the literature.

4.1 Based On the Capability of the Attacker

4.1.1 Outsider versus insider (Node Compromise) attacks

Outside attacks [6], [9] are defined as attacks from nodes, which do not belong to a WSN; insider attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways. To overcome these attacks [6], we require robustness against Outsider Attacks, Resilience to Insider Attacks, Graceful Degradation with Respect to Node Compromise and Realistic Levels of Security.

4.1.2 Passive versus active attacks

Passive attacks include eavesdropping on or monitoring packets exchanged within a WSN; active attacks involve some modifications of the data steam or the creation of a false stream.

4.1.3 Mote-class versus laptop-class attacks

In mote-class attacks, an adversary attacks a WSN by using a few nodes with similar capabilities to the network nodes; in laptop-class attacks, an adversary can use more powerful devices (e.g., a laptop) to attack a WSN. These devices have greater transmission range, processing power, and energy reserves than the network nodes.

4.2 Attacks on Information in Transit

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 attacks are [9],[7]:

4.2.1 Interruption

Communication link in sensor networks becomes lost or unavailable. This operation threatens service availability. The main purpose is to launch denial-of-service (DoS) attacks. From the layer-specific perspective, this is aimed at all layers.

4.2.2 Interception

Sensor network has been compromised by an adversary where the attacker gains unauthorized access to sensor node or data in it. Example of this type of attacks is node capture attacks. This threatens message confidentiality. The main purpose is to eavesdrop on the information carried in the messages. From the layer-specific perspective, this operation is usually aimed at the application layer.

4.2.3 Modification

Unauthorized party not only accesses the data but also tampers with it. This threatens message integrity. 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.

4.2.4 Fabrication

An adversary injects false data and compromises the trustworthiness of information. This threatens message authenticity. The main purpose is to confuse or mislead the parties involved in the communication protocol. This operation can also facilitate DOS attacks, by flooding the network.

4.2.5 Replaying existing messages

This operation threatens message freshness. The main purpose of this operation is to confuse or mislead the parties involved in the communication protocol that is not time-aware.

4.3 Host Based Vs Network Based

4.3.1 Host-based attacks

It is further broken down in to [22]:

User compromise: This 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.

Hardware compromise: This involves tampering with the hardware to extract the program code, data and keys stored within a sensor node. The attacker might also attempt to load its program in the compromised node.

Software compromise: This involves breaking the software running on the sensor nodes. Chances are the operating system and/or the applications running in a sensor node are vulnerable to popular exploits such as buffer overflows.

4.3.2 Network-based attacks

It has two orthogonal perspectives [22]: layer-specific compromises, and protocol-specific compromises. This includes all the attacks on information in transit. Apart from that it also includes

Deviating from protocol: When the attacker is, or becomes an insider of the network, and the attacker's purpose is not to threaten the service availability, message confidentiality, integrity and authenticity of the network, but to gain an unfair advantage for itself in the usage of the network, the attacker manifests selfish behaviors, behaviors that deviate from the intended functioning of the protocol.

4.4 Based On Protocol Stack

This section discusses about the WSN layer wise attack. The article [45], [48] provides the layer wise issues.

4.4.1 Physical Layer

(a) Jamming: This is one of the Denial of Service Attacks in which the adversary attempts to disrupt the operation of the network by broadcasting a high-energy signal. Jamming attacks in WSNs, classifying [5] them as constant (corrupts packets as they are transmitted), deceptive (sends a constant stream of bytes into the network to make it look like legitimate traffic), random (randomly alternates between sleep and jamming to save energy), and reactive (transmits a jam signal when it senses traffic).

To defense against this attack, use spread-spectrum techniques for radio communication. Handling jamming over the MAC layer requires Admission Control Mechanisms. Network layer deals with it, by mapping the jammed area in the network and routing around the area. Algorithms that combine statistically analyzing the received signal strength indicator (RSSI) values, the average time required to sense an idle channel (carrier sense time), and the packet delivery ratio (PDR) techniques can reliably identify all four types of jamming.

(b) Radio interference: In which the adversary either produces large amounts of interference intermittently or persistently. To handle this issue [16], use of symmetric key algorithms in which the disclosure of the keys is delayed by some time interval.

(c) Tampering or destruction: Given physical access to a node, an attacker can extract sensitive information such as cryptographic keys or other data on the node [9].

One defense to this attack involves tamper-proofing the node's physical package. Self Destruction (tamper-proofing packages) – whenever somebody accesses the sensor nodes physically the nodes vaporize their memory contents and this prevents any leakage of information. Second - Fault Tolerant Protocols – the protocols designed for a WSN should be resilient to this type of attacks.

4.4.2 Data Link Layer

(a)Continuous Channel Access (Exhaustion): A malicious node disrupts the Media Access Control 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, thus preventing the energy drain caused by repeated transmissions. A second technique is to use time-division multiplexing where each node is allotted a time slot in which it can transmit [16],[9].

(b) 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. A typical defense against collisions is the use of error-correcting codes [16],[9].

(c)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 [16], [9].

(d)Interrogation: Exploits the two-way request-to-send/clear to send (RTS/CTS) handshake that many MAC protocols use to mitigate the hidden-node problem. An attacker can exhaust a node's resources by repeatedly sending RTS messages to elicit CTS responses from a targeted neighbor node. To put a defense against such type of attacks a node can limit itself in accepting connections from same identity or use Anti replay protection and strong link-layer authentication [4],[5].

(e)Sybil Attack: This type of attack is very much prominent in Link Layer. First type of link layer Sybil Attack is Data Aggregation in which single malicious node is act as different Sybil Nodes and then this may many negative reinforcements to make the aggregate message a false one.

Second type is Voting. Many MAC protocols may go for voting for finding the better link for transmission from a pool of available links. Here the Sybil Attack could be used to stuff the ballot box. An attacker may be able to determine the outcome of any voting and off course it depends on the number of identities the attacker owns [5].

4.4.3 Network Layer

(a)Sinkhole: Depending on the routing algorithm technique, a sinkhole attack tries to lure almost all the traffic toward the compromised node, creating a metaphorical sinkhole with the adversary at the center. Geo-routing protocols are known as one of the routing protocol classes that are resistant to sinkhole attacks, because that topology is constructed using only localized information, and traffic is naturally routed through the physical location of the sink node, which makes it difficult to lure it elsewhere to create a sinkhole. [3],[9],[7] and [23]

(b)Hello Flood: This attack exploits Hello packets that are required in many protocols to announce nodes to their neighbors. A node receiving such packets may assume that it is in radio range of the sender. A laptop-class adversary can send this kind of packet to all sensor nodes in the network so that they believe the compromised node belongs to their neighbors. This causes a large number of nodes sending packets to this imaginary neighbor and thus into oblivion. Authentication is the key solution to such attacks. Such attacks can easily be avoided by verify bi-directionality of a link before taking action based on the information received over that link. [3],[9],[7] and [23]

(c) Node Capture: It is observed and analyzed that even a single node capture is sufficient for an attacker to take over the entire network. Good solution to this problem would definitely constitute a groundbreaking work in WSN. [16],[9] and [7]

(d) Selective Forwarding/ Black Hole Attack (Neglect And Greed): WSNs are usually multi-hop networks and hence based on the assumption that the participating nodes will forward the messages faithfully. Malicious or attacking nodes can however refuse to route certain messages and drop them. If they drop all the packets through them, then it is called a Black Hole Attack. However if they selectively forward the packets, then it is called selective forwarding. To overcome this, Multi path routing can be used in combination with random selection of paths to destination, or braided paths can be used which represent paths which have no common link or which do not have two consecutive common nodes, or use implicit acknowledgments, which ensure that packets are forwarded as they were sent [16],[9] and [7].

(e)Sybil Attack: In this attack, a single node presents multiple identities to all other nodes in the WSN. This may mislead other nodes, and hence routes believed to be disjoint with respect to node can have the same adversary node. A countermeasure to Sybil Attack is by using a unique shared symmetric key for each node with the base station. [16],[9] and [7]

(f)Wormhole Attacks: An adversary can tunnel messages received in one part of the network over a low latency link and replay them in another part of the network. This is usually done with the coordination of two adversary nodes, where the nodes try to understate their distance from each other, by broadcasting packets along an out-of-bound channel available only to the attacker. To overcome this, the traffic is routed to the base station along a path, which is always geographically shortest or use very tight time synchronization among the nodes, which is infeasible in practical environments. [16],[9] and [7]

(g) Spoofed, Altered, or Replayed Routing Information: The most direct attack against a routing protocol in any network is to target the routing information itself while it is being exchanged between nodes. An attacker may spoof, alter, or replay routing information in order to disrupt traffic in the network. These disruptions include the creation of routing loops, attracting or repelling network traffic from select nodes, extending and shortening source routes, generating fake error messages, partitioning the network, and increasing end-to-end latency. A countermeasure against spoofing and alteration is to append a message authentication code (MAC) after the message. Efficient encryption and authentication techniques can defend spoofing attacks. [9]

(h) Acknowledgment Spoofing: Routing algorithms used in sensor networks sometimes require Acknowledgments to be used. An attacking node can spoof the Acknowledgments of overheard packets destined for neighboring nodes in order to provide false information to those neighboring nodes. The most obvious solution to this problem would be authentication via encryption of all sent packets and also packet headers. [9]

(i) Misdirection: This is a more active attack in which a malicious node present in the routing path can send the packets in wrong direction through which the destination is unreachable. In place of sending the packets in correct direction the attacker misdirects those and that too towards one node and thus this node may be victimized. If it gets observed that a node's network link is getting flooded without any useful information then the victim node can be scheduled into sleep mode for some time to over come this. [4]

(j) Internet Smurf Attack: In this type of attack the adversary can flood the victim node's network link. The attacker forges the victim's address and broadcasts echoes in the network and also routes all the replies to the victim node. This way the attacker can flood the network link of the victim. If it gets observed that a node's network link is getting flooded without any useful information then the victim node can be scheduled into sleep mode for some time to over come this**.** [4]

(k) Homing: uses traffic pattern analysis to identify and target nodes that have special responsibilities, such as cluster

heads or cryptographic- key managers. An attacker then achieves DoS by jamming or destroying these key network nodes. Header encryption is a common prevention technique. Using "dummy packets" throughout the network to equalize traffic volume and thus prevent traffic analysis. Unfortunately, this wastes significant sensor node energy, so use it only when preventing traffic analysis is of utmost importance [5].

4.4.4 Transport Layer

(a) 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 demonstrate 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 [16],[9].

(b) De-synchronization Attacks: In this attack, the adversary repeatedly forges messages to one or both end points which request transmission of missed frames. Hence, these messages are again transmitted and if the adversary maintains a proper timing, it can prevent the end points from exchanging any useful information. This will cause a considerable drainage of energy of legitimate nodes in the network in an end less synchronization-recovery protocol. A possible solution to this type of attack is to require authentication of all packets including control fields communicated between hosts [16],[9]. Header or full packet authentication can defeat such an attack [5].

4.4.5 Application Layer

(a) Overwhelm attack: An attacker might attempt to overwhelm network nodes with sensor stimuli, causing the network to forward large volumes of traffic to a base station. This attack consumes network bandwidth and drains node energy. We can mitigate this attack by carefully tuning sensors so that only the specifically desired stimulus, such as vehicular movement, as opposed to any movement, triggers them. Rate-limiting and efficient data-aggregation algorithms can also reduce these attacks' effects [5].

(b) Path-based DOS attack: It involves injecting spurious or replayed packets into the network at leaf nodes. This attack can starve the network of legitimate traffic, because it consumes resources on the path to the base station, thus preventing other nodes from sending data to the base station. Combining packet authentication and anti replay protection prevents these attacks [5].

(c) Deluge (reprogram) attack: Network-programming system let you remotely reprogram nodes in deployed networks If the reprogramming process isn't secure, an intruder can hijack this process and take control of large portions of a network. It can use authentication streams to secure the reprogramming process [5].

5 Issues with High-Level Security Mechanisms

5.1 Cryptography & Key Management

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 cryptography method for sensor nodes is fundamental to providing security services in WSNs. However, the decision depends on the computation 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. However, symmetric cryptography is not as versatile as public key cryptographic techniques, which complicates the design of secure applications. Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power, which are very important resources for the sensors' longevity. Applying the security mechanisms such as encryption could also increase delay, jitter and packet loss in WSNs.

The process by which public key and symmetric key cryptography schemes should be selected is based on the following criteria [31]:

1. Energy: how much energy is required to execute the encrypt/decryption functions
2. Program memory: the memory required to store the encryption/decryption program
3. Temporary memory: the required RAM size or number of registers required temporarily when the encryption/decryption code is being executed
4. Execution time: the time required to execute the encryption/decryption code.
5. Program parameters memory: the required memory size to save the required number of keys used by the encryption/decryption function.

The security of a cryptographic system relies mainly on the secrecy of the key it uses. Keys for these cryptographic operations must be set up by communicating nodes before they can exchange information securely. Key management schemes are mechanisms used to establish and distribute various kinds of cryptographic keys in the network, such as individual keys, pair wise keys, and group keys. Key management is an essential cryptographic primitive upon which other security primitives are built. If an attacker can find the key, the entire system is broken. In fact, a secure key management scheme is the prerequisite for the security of these primitives, and thus essential to achieving secure infrastructure in sensor networks.

In Sensor networks end-to-end encryption is impractical because of large number of communicating nodes and each node is incapable of storing large number of encryption keys. Therefore hop-by-hop encryption mechanism is usually used in which each sensor node stores only encryption keys shared with its immediate neighbors.

Open research issues range from cryptography algorithms to hardware design [6],[9] and [29] and the design of key management protocol's open research [3],[16],[9],[10] and [32] issues are described below:

1. Recent studies on public key cryptography have demonstrated that public key operations may be practical in sensor networks. However, private key operations are still too expensive in terms of computation and energy cost to accomplish in a sensor node. The application of private key operations to sensor nodes needs to be studied further.
2. 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.
3. 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, because usually, 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. A more promising approach is to combine both symmetric and asymmetric cryptography techniques.

4. Proving the authenticity of public keys is another important problem. Identity-based cryptography is a shortcut to avoid the problem.
5. Key revocation is another un-addressed problem. It is very difficult to design a universal key revocation scheme. It is still an open problem for resource constrained WSNs.
6. Current proposed key management schemes assume that the base station is trustworthy. However, there may be situations (e.g., in the battlefield) where the security of a base station needs to be considered.
7. All key management protocols discussed in literature so far are based on symmetric key cryptography. Key management schemes based on public key cryptography need to be designed. A typical WSN may contain from hundreds to thousands of sensor nodes. Any protocol used for key management and distribution must be adaptable to such scales.
8. For any pair of nodes that do not share a key and are connected by multiple hops, there needs to be assigned a path-key to guarantee end-to-end secure communication. Such a path key establishment needs to be improved
9. Another challenging issue is that each node needs to discover a neighbor in wireless communication range with which it shares at least one key. A good-shared key discovery approach should not permit an attacker to know shared keys between every two nodes.
10. Most key management schemes discussed in literature so far are suitable for static WSNs. Following technique advance, key management and security mechanisms for mobile WSNs should be considered and become a focus of attention.
11. Though many key management approaches consider defending against node compromise, the efficiency and security performance is not high when their mechanisms are deployed in some special application environment. Thus, the study of node compromise distribution and integrating it in key management is a promising research area.

5.2 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 [3].

This operation cannot be efficiently done without being secured. Because of deployment environment, the physical compromise of aggregators and some of the sensor nodes is possible. An active adversary can forge [16], the home server to accept false aggregation results (Stealthy attacks), which are very much different from the actual results determined by the measured values. The first line of defense against threats is cryptographic mechanisms: integrity and confidentiality can be achieved using cryptographic schemes. Open research issues include the following [9],[30] and [32]:

1. To prevent this type of attack, techniques are needed to ensure that the user can still be confident of the (approximate) accuracy of the aggregated data even when the aggregator and a small subset of the sensor nodes are under the control of an adversary.
2. No comparisons have been conducted on existing secure data aggregation protocols. So performance comparison are required in terms of matrices such as security, processing overhead, communication overhead, energy consumption, and data compression rate.
3. New data aggregation protocols need to be developed to address higher scalability and higher reliability against aggregator and sensor node cheating.
4. The field of cryptography within in-network data processing (what we call secure data processing) is a very promising research field, and introduces many interesting challenges.
5. Need to design and implement secure, yet very efficient and cost-effective, data aggregation mechanisms. Very promising results have been recently achieved in this area based on advanced cryptographic concepts, such as privacy homomorphism, bilinear pairings, and elliptic curve cryptography.
6. Another important issue is related to assessment of trustworthiness and reliability of the data provided by WSNs, especially when this data is preprocessed in the network and received by the application in an aggregated form.
7. Currently, most studies assume aggregators as big nodes. It is desirable to design a secure data aggregation scheme in the environments without big nodes.
8. Since data aggregation can save system energy and introduces security issues, is it possible to design a scheme based on the different security and energy requirement?
9. Most of current schemes are only suitable for static WSNs. Designing new secure data aggregation schemes for mobile WSNs including mobile aggregators or normal nodes still needs further studies.

5.3 Secure Group Management

In-network processing of the raw data is performed in WSNs by dividing the network into small groups and analyzing the data aggregated at the group leaders. So the group leader has to authenticate the data it is receiving from other nodes in the group. This requires group key management. However, addition or deletion of nodes from the group leads to more problems. Consequently, secure protocols for group management are required [16].

5.4 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 [16],[41]. Intrusion detection in WSNs is still largely open to research. Key research issues are [9]

1. Due to the constraints in WSNs, intrusion detection has many aspects that are not of concern in other network types. 2. The problem of intrusion detection needs to be well defined in WSNs. 3. The proposed IDS protocols in literature focus on filtering injected false information only. 4. These protocols need to be improved so as to address scalability issues. 5. It is very difficult to integrate intrusion

detection techniques into a uniform hardware platform due to cost and implementation considerations [10].

5.5 Secure Time Synchronization

Due to the collaborative nature of sensor nodes, time synchronization is very important for many sensor network operations, such as coordinated sensing tasks, sensor scheduling (sleep and wake), mobile object tracking, time-division multiple access (TDMA) medium access control, data aggregation, and multicast source authentication protocol. However, none of the aforementioned time synchronization schemes were designed with security in mind. Hence, they are not suitable for applications in hostile environments (e.g., military battlefields) where security is critical. Most existing time synchronization schemes are vulnerable to several attacks [8] which include Masquerade attack, Replay attack, Message manipulation attack, Delay attack and Denial of service (DoS).

5.6 Secure Location Discovery

As mentioned earlier, sensor locations play a critical role in many sensor network applications, such as environment monitoring and target tracking. Without protection, an attacker may easily mislead the location estimation at sensor nodes and subvert the normal operation of sensor networks. For example, an attacker may provide incorrect location references by replaying the beacon packets intercepted in different locations. Moreover, an attacker may compromise a beacon node and distribute malicious location references by lying about the location or manipulating the beacon signals. In either case, non-beacon nodes will determine their locations incorrectly. Two approaches to deal with malicious attacks against location discovery in WSNs are based on minimum mean square estimation (MMSE) and use a voting-based location estimation technique and iteratively refine voting to tolerate malicious location references sent by attackers [8].

5.7 Code Attestation

Sensors that operate in an unattended, harsh or hostile environment often suffer from break-in compromises, because their low costs do not allow the use of expensive tamper-resistant hardware. Besides the exposure of secret information (e.g., cryptographic keys), compromised sensors may be reprogrammed with malicious code to launch all kinds of insider attacks. Very desirably, if we can identify and further revoke those corrupted nodes in a timely manner, the potential damages caused by them could be minimized. To address this problem, a promising direction is to use code attestation to validate the code running on each sensor node. Because the code running on a malicious node must be different from that on a legitimate node, we can detect compromised nodes by verifying their memory content. Code attestation may be achieved through either hardware or software. So far little research has been done in this aspect, and we believe it is a promising research direction [28],[6].

5.8 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. In addition, many network protocols such as routing require location information in order to provide the specific protocol service. Localization systems can be divided into three distinct components as Distance/angle estimation, Position computation and Localization algorithm and attacks on these three different areas are discussed in [1]. Currently, most of current proposals are suitable for static WSNs. Secure location algorithms for mobile WSNs in different environments need to be investigated [32].

5.9 Secure Routing

Secure routing is vital to the acceptance and use of sensor networks for many applications, but many sensor network routing protocols have been proposed, but none of them have been designed with security as a goal. WSNs use multi-hop routing and wireless communication to transfer data, thus incur more routing attacks. The paper [36] define the security attributes of routing protocols in WSNs which with them the attackers can not achieve their goals. Security attributes are the mechanisms that allow the routing protocols to defend against the possible threats in the whole network. These attributes consist of identity verification, bi-directionality confirmation, topology structure restriction, base station decentralization and braided and multi-path transmission. The article [37] proposed security goals for routing in sensor networks and presents the detailed security analysis of all the major routing protocols and energy conserving topology maintenance algorithms for sensor networks. It also describes practical attacks against all of them that would defeat any reasonable security goals and discuss countermeasures and design considerations for secure routing protocols in sensor networks. There are a lot of approaches to ease routing security [32],[38] and [42].

1. Most current proposals are suitable for static WSNs. Designing secure routing algorithms for mobile WSNs is complex and current secure routing algorithms will meet issues when they are applied in mobile environments.
2. Undetected node compromise issues: 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.
3. Currently most proposals only consider security metrics and only a few of them evaluate other metrics. More metrics, such as QoS (quality of service) need to be considered in addition of security.
4. 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 consummations, security, etc. due to different cluster size. What's more, though these algorithms may ease secure routing issues, they bring complex cluster management issues and costs. More elaborate studies need to be done in the future.
5. Routing maintenance: During the lifetime of a sensor network, the network topology changes frequently, and routing error messages are normally produced. Preventing unauthorized nodes from being producing this type of message is important and needs more studies.

5.10 Trust Management System

Trust, or the trust on the behavior of the elements of the network, is a key aspect for WSN. A trust management

system can be useful for detecting a node which is not behaving as expected (either faulty or maliciously) or it can assist in the decision-making process, for instance, if a node needs a partner in order to achieve a common goal. Even though trust is an important feature for WSN few systems have considered it. However, more efforts have been made on the fields of Ad-hoc and P2P networks, which are somehow similar to WSN.

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 work in paper [34] presents a classification of trust methods for Ad-Hoc and sensor networks. The article [35] describes trust evaluation mechanisms in distributed networks such as MANETs and sensor networks. In particular, the benefits of introducing trust into distributed networks, the vulnerabilities in trust establishment methods, and the defense mechanisms. It identified five attacks against trust establishment methods, and developed defense techniques

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.

1. 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. 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.
2. It should be necessary to deduce different trust values for every distinct behavior of the nodes.
3. Sensor nodes should also be aware of the trust history of their neighborhood. The consistence in the trust readings is also significant.
4. Note that all the important decisions taken by the nodes, such as node exclusion, should be notified to the base station for logging, monitoring and maintenance purposes.
5. As a final matter, one of the biggest constraints regarding trust management for sensor networks is the overhead that the existence of this system may impose over the constrained elements of the network.

5.11 Other Security Issues

Other security issues include [32] security-energy assessment, data assurance, survivability, Trust, end to end security, Security and Privacy Support for data centric sensor networks (DCS) and node compromise distribution. It's very important to study these areas due to a sensor network's special character, 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, and more studies are needed in these areas.

6. Conclusions

Security concerns constitute a potential stumbling block to the impending wide deployment of sensor networks. WSNs are still under development, and many protocols designed so far for WSNs have not taken security into consideration. On the other hand, the salient features of WSNs make it very challenging to design strong security protocols while still maintaining low overheads. In this article, we summarize typical attacks on sensor networks and surveyed the literatures on several important security issues relevant to the sensor networks, including key management, secure time synchronization, secure location discovery and etc. Many security issues in WSNs remain open and we expect to see more research activities on these exciting topics in the future.

References

[1] A. Boukerche, Horacio A. B. F. Oliveira, Eduardo F. Nakamura, Antonio A. F. Loureiro, "Secure Localization Algorithms for Wireless Sensor Networks", IEEE Communications Magazine, Security In Mobile Ad Hoc And Sensor Networks, pp: 96 –101, April 2008.

[2] I. F. Akyildiz W. Su, Y. Sankarasubramaniam, "A Survey on Sensor Setworks," IEEE Commun.Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.

[3] D. Djenouri And L. Khelladi, 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

[4] Hiren Kumar Deva Sarma, Avijit Kar, "Security Threats in Wireless Sensor Networks", IEEE 2006.

[5] Raymond D.R. Midkiff.S.F, "Denial of Service in Wireless Sensor Network: Attacks and Defenses", IEEE Pervasive Computing, Vol:7, Issue 1, PP: 74 – 81, March 2008.

[6] E. Shi and A. Perrig, "Designing Secure Sensor Networks," Wireless Commun. Mag., vol. 11, no. 6, pp. 38–43, Dec. 2004.

[7] Tanveer Zia and Albert Zomaya, "Security Issues in Wireless Sensor Networks", IEEE.

[8] Xiaojiang Du; Hsiano-Hwa Chen; " Security in wireless sensor networks**",** Wireless Communications, IEEE, Vol: 15, Issue 4, pp: 60 –66, Aug 2008.

[9] Yong Wang, Garhan Attebury, And Byrav Ramamurthy, "A Survey Of Security Issues In Wireless Sensor Networks" , IEEE Communications Surveys & Tutorials, Volume 8, No. 2, 2nd Quarter 2006.

[10] Yun Zhou; Yuguang Fang; Yanchao Zhang, "Securing Wireless Sensor Networks: A Survey", IEEE Communications Surveys & Tutorials, Vol:10, Issue 3, PP: 6 –28, Third Quarter 2008.

[11] Erdal Çayırcı, Chunming Rong, "Security in Wireless Ad Hoc and Sensor Networks", A John Wiley and Sons, Ltd, Publication, 2009.

[12] Jason Lester Hill, "System Architecture for Wireless Sensor Networks", Ph.D.-Thesis, spring 2003.

[13] Jagannathan Sarangapani, "Wireless Ad Hoc and Sensor Networks Protocols, Performance, and Control, CRC Press, 2007.

[14] Javier Lopez, Jianying Zhou, "Wireless Sensor Network Security", IOS Press, 2008.

[15] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Auerbach Publications, CRC Press, 2006.

[16] Mohit Saxena, "Security In Wireless Sensor Networks - A Layer Based Classification", Cerias Tech Report 2007-04.

[17] Mohammad Ilyas And Imad Mahgoub, "Handbook Of Sensor Networks: Compact Wireless And Wired Sensing Systems", CRC Press LLC, 2005.
[18] F. L. LEWIS, "Wireless Sensor Networks", Technologies, Protocols, and Applications ed. D.J. Cook and S.K. Das, John Wiley, New York, 2004.
[19] Robert M. Crovella, "Sensor Networks and Communication", CRC Press LLC, 2000.
[20] Sayed Ahmed, "Current Researches on Sensor Networks", TRLabs Report, May 30, 2004.
[21] C. E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, vol. 28, no. 2, pp. 656–715, 1949.
[22] Yee Wei Law, "Key Management And Link-Layer Security Of Wireless Sensor Networks", Ctit Ph.D.-Thesis Series, Series Number: 1381-3617, Ctit Number: 05-75, 2005.
[23] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", ICACT, pp: 1043 – 1048, 2006.
[24] Hongfa Wang, "A Robust Mechanism for Wireless Sensor Network Security", 4th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM '08), PP 1 –4, Oct 2008.
[25] A. Karnik, K. Passerini ,"Wireless network security - A discussion from a business perspective", IEEE Wireless Telecommunications Symposium, pp:261 – 267, 2005.
[26] Martinovic.I, Gollan.N, Schmitt.J.B, "Firewalling Wireless Sesor Networks: Security by Wireless", 33rd IEEE Conference on Local Computer Networks (LCN 2008), pp:770 – 777, Oct 2008.
[27] Yang, H; Ricciato, F.;Lu, S.;Zhang.L, "Securing a Wireless World", Proceedings of the IEEE, Vol:94, Issue 2, PP: 442 –454, Feb 2006.
[28] Yi Yang, Xinran Wang, Sencun Zhu, and Guohong Cao, "Distributed Software-based Attestation for Node Compromise Detection in Sensor Networks", 26th IEEE International Symposium on Reliable Distributed Systems, IEEE Computer Society, PP: 219 – 228, 2007.
[29] Riaz A. Shaikh, Sungyoung Lee, Young Jae Song, Yonil Zhung, "Securing Distributed Wireless Sensor Networks: Issues and Guidelines", Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), 2006.
[30] Alessandro Sorniotti, Laurent Gomez, Konrad Wrona and Lorenzo Odorico, "Secure and Trusted in-network Data Processing in Wireless Sensor Networks: a Survey", Journal of Information Assurance and Security, Vol 2, Issue 3, pp. 189 -199, 2007.
[31] Mohammad AL-Rousan, A. Rjoub and Ahmad Baset, "A Low-Energy Security Algorithm for Exchanging Information in Wireless Sensor Networks", Journal of Information Assurance and Security, Vol 4, pp.48-59, 2009.
[32] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, "Sensor Network Security: A Survey", IEEE Communications Surveys & Tutorials, Vol. 11, No. 2, Pp. 52 – 73, Second Quarter 2009.
[33] M. Carmen Fern´andez-Gago, Rodrigo Rom´an, Javier Lopez, "A Survey on the Applicability of Trust Management Systems for Wireless Sensor Networks", Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2007. SECPerU 2007. Third International Workshop on, pp 25 -30, July 2007.
[34] E. Aivaloglou, S. Gritzalis, and C. Skianis. Trust Establishment in Ad Hoc and Sensor Networks. In J. L´opez, editor, *1st International Workshop on Critical Information Infrastructure Security, CRITIS'06*, volume 4347 of *Lectures Notes in Computer Science, LNCS*, pages 179–194, Samos, Greece, 2006. Springer.
[35] Yan (Lindsay) Sun, Zhu Han and K. J. Ray Liu, "Defense of Trust Management Vulnerabilities in Distributed Networks", IEEE Communications Magazine, pp. 112 – 119, February 2008.
[36] Mohammad Nikjoo S., Arash Saber Tehrani and Priyantha Kumarawadu, "Secure Routing in Sensor Networks", IEEE, pp. 978 – 981, 2007.
[37] Chris Karlof, David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", Ad Hoc Networks, Elsevier Publications, Vol.1, pp.293–315, 2003.
[38] C. Karlof and D. Wagner, "Summary of "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Seminar on Theoretical Computer Science. 27.4.2005
[39] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, Special Issue: Wireless sensor networks, vol. 47, pp. 53–57, 2004.
[40] Y. W. Law, S. Etalle, and P. H. Hartel, "Assessing security in energy efficient sensor networks," in *Proc. 18th IFIP TC11 Int. Conf. Information Security Privacy Age Uncertainty (SEC)*, 2003, pp. 459–463.
[41] Esteban J. Palomo, Enrique Domínguez, Rafael M. Luque and José Muñoz, "An Intrusion Detection System based on Hierarchical Self-Organization", Journal of Information Assurance and Security, Vol 4, Issue 3, pp.209-216, 2009.
[42] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Ad Hoc Networks*, vol. 1, 2003, pp. 293–315.
[43] Jamal N. Al-Karaki And Ahmed E. Kamal, "Routing Techniques In Wireless Sensor Networks: A Survey", Ieee Wireless Communications, pp. 06 – 28, December 2004.
[44] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato, "A Survey Of Routing Attacks In Mobile Ad Hoc Networks", Ieee Wireless Communications, pp. 85 -91, October 2007.
[45] I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey", Computer Networks, Published by Elsevier Science, 38, pp. 393–422, 2002.
[46] Yi Qian, Kejie Lu, and David Tipper, "Towards Survivable and Secure Wireless Sensor Networks", IEEE, pp.442 – 448, 2007.
[47] Yi Qian And Kejie Lu And David Tipper, "A Design For Secure And Survivable Wireless Sensor Networks", IEEE Wireless Communications , Pp. 30 - 37, October 2007.
[48] Riaz A. Shaikh, Sungyoung Lee, Young Jae Song, Yonil Zhung," Securing Distributed Wireless Sensor Networks: Issues and Guidelines", Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), 2006.

[49] Mingbo Xiao; Xudong Wang and Guangsong Yang, **“**Cross-Layer Design for the Security of Wireless Sensor Networks”, The Sixth World Congress on Intelligent Control and Automation 2006 (WCICA ’06), IEEE, Vol 1, pp. 104 – 108, 2006.

Author Biographies

T.Kavitha received Bachelor of Engineering in Electronics and Communication Engineering from Bharathidasan University in the year 2000 and Master of Engineering in Systems Engineering and Operations Research from College of Engineering Guindy, Anna University Chennai in the year 2006. Presently she is a research scholar in Anna University Chennai, India. Her area of interest includes Network security and wireless sensor networks.

D.Sridharan received B.Tech and M.E in Electronics Engineering in the year 1991 & 1993 respectively from Madras Institute of Technology, Anna University and Ph.D degree in the department of Faculty of Information and Communication Engineering from Anna University in the year 2005. He was awarded Young Scientist Research Fellowship by SERC of Department of Science and Technology, Government of India.

He is currently working as an Assistant Professor, Department of Electronics and Communication Engineering, at College of Engineering Guindy, Anna University – Chennai, India. His research interest includes Internet Technology, Network Security, Distributed Computing, and VLSI for Wireless Communication.

He has published more than 25 papers in National/ International conferences and journals. He has visited USA, Italy, Germany, Singapore, Hong Hong and Dubai to participate and present research papers and he has also attended number of workshops sponsored by UNEFCO. He is a life member of Institute of Electronics and Telecommunication Engineers (IETE), Indian Society for Technical Education (ISTE), and Computer Society of India (CSI). Presently he is working on research project on Wireless Sensor Network sponsored by Department of Atomic Energy.