Volume 2, Issue 10, October 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Analysis of Threat's in Wireless Sensor Networks

Dr.G.Murugaboopathi
Associate Prof. & Head – R & D Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering college Avadi Chennai

V.Geta
Assistant Professor Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering college Avadi Chennai

V.Sujathabai
Asistant Prof. Dept of MCA Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering college Avadi Chennai

T.K.S.Rathish babu
Assistant Prof. Dept of CSE Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering college Avadi Chennai

S.Hariharasitaraman
A P-II Dept of IT Kalasalingam university, Krishnankoil, Srivilluputur Virudhunagar dt

Abstract—Wireless sensor networks are a networked systems, characterized by several energy resources, and the security mechanisms are actually used to detect, prevent and recover from the security attacks. In this security concerns must be addressed from the beginning of the system design. Securely communication among sensor nodes is a fundamental challenge for providing security services in WSNs. There is currently enormous research in the field of wireless sensor network security. Thus, the current research in this field will benefit the researchers. Many researchers have tried to provide security by using symmetric key cryptography, but thinking that public key steganography are feasible to implement in these networks because they are provided with more resources. This paper tends to investigate the security related issues and challenges in wireless sensor networks. We identify the security threats, discuss the proposed security mechanisms for wireless sensor networks and also present the obstacles and the requirements in the sensor security, classify many of the current attacks, and finally list their corresponding defensive measures.

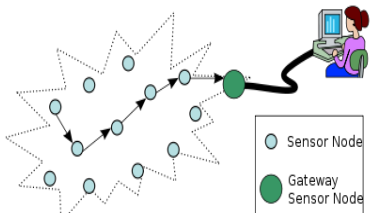
keywords—Wireless sensor networks, sensor security, attacks of wsn, Holistic Security in Wireless Sensor Networks, Challenge of wsn.

I INTRODUCTION

Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements. A typical multi-hop wireless sensor network architecture will consist of hundreds or thousands of self-organizing, low-power, low cost wireless nodes deployed en masse to monitor and affect the environment. Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real world challenges. Their low cost provides a means to deploy large sensor arrays in a variety of conditions capable of performing both military and civilian tasks. But sensor networks also introduce severe resource constraints due to their lack of data storage and power. Both of these represent major obstacles to the implementation of traditional computer security techniques in a wireless sensor network. To address the critical security issues in wireless sensor networks we talk about cryptography, steganography and other basics of network security and their applicability . We also explore various types of threats and attacks against wireless sensor network and proposed schemes concerning security in WSN and also introduces the view of holistic security in WSN. Issued need to be addressed in future research are also identified, which provide a vital information for future researchers. Finally we concludes the paper delineating the research challenges and future trends toward the research in wireless sensor network security.

II BASIC SECURITY SCHEMES IN WIRELESS SENSOR NETWORKS

Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, nonrepudiation, and anti-playback . The more the dependency on the information provided by the networks has been increased, the more the risk of secure transmission of information over the networks has increased. For the secure transmission of various types of information over networks, several cryptographic, steganographic and other techniques are used which are well known[1]. In this section, we discuss the network security fundamentals and how the techniques are meant for wireless sensor networks.



TYPICAL MULTIHOP WIRELESS SENSOR NETWORK ARCHITECHTURE

A. Cryptography

The encryption-decryption techniques devised for the traditional wired networks are not feasible to be applied directly for the wireless networks and in particular for wireless sensor networks. WSNs consist of tiny sensors which really suffer from the lack of processing, memory and battery power . 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 wireless sensor networks [1]. Moreover, some critical questions arise when applying encryption schemes to WSNs like, how the keys are generated or disseminated. As minimal (or no) human interaction for the sensors, is a fundamental feature of wireless sensor networks, it becomes an important issue how the keys could be modified time to time for encryption. Adoption of pre-loaded keys or embedded keys could not be an efficient solution.

B. Steganography

While cryptography aims at hiding the content of a message, steganography aims at hiding the existence of the message. Steganography is the art of covert communication by embedding a message into the multimedia data (image, sound, video, etc.) . The main objective of steganography is to modify the carrier in a way that is not perceptible and hence, it looks just like ordinary. It hides the existence of the covert channel, and furthermore, in the case that we want to send a secret data without sender information or when we want to distribute secret data publicly, it is very useful. However, securing wireless sensor networks is not directly related to steganography and processing multimedia data (like audio, video) with the inadequate resources of the sensors is difficult and an open research issue[1].

III OBSTACLE TO SENSOR SECURITY

A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Because sensor networks pose unique challenges, traditional security techniques used in traditional networks cannot be applied directly. First, to make sensor networks economically viable, sensor devices are limited in their energy, computation, and communication capabilities. Second, unlike traditional networks, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack[3]. And third, sensor networks interact closely with their physical environments and with people, posing new security problems. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. 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.

A. Very Limited Resources

All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor.

The major parameters are:

1)Limited Memory and Storage Space:

A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm. For example, one common sensor type (TelosB) has an 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage. With such a limitation, the software built for the sensor must also be quite small.

2)Power Limitation:

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 (high operating cost) or recharged (high cost of sensors). Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network.

B. Unreliable Communication

Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication. The major parameters are:

1)Unreliable Transfer:
Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. Furthermore, the unreliable wireless communication channel also results in damaged packets[1].
2)Conflicts:
Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network. If packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail. In a crowded (high density) sensor network, this can be a major problem. More details about the effect of wireless communication can be found.

3)Latency:
The multi-hop routing, network congestion, and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes. The synchronization issues can be critical to sensor security where the security mechanism relies on critical event reports and cryptographic key distribution[1].

C. Unattended Operations

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main caveats to unattended sensor nodes:

1)Exposure to Physical Attacks:
The sensor may be deployed in an environment open to adversaries, bad weather, and so on. The likelihood that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network[3].

2) Managed Remotely:
Remote management of a sensor network makes it virtually impossible to detect physical tampering (i.e., through tamperproof seals) and physical maintenance issues (e.g., battery replacement). Perhaps the most extreme example of this is a sensor node used for remote reconnaissance missions behind enemy lines. In such a case, the node may not have any physical contact with friendly forces once deployed.

3)No Central Management Point:
A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile.

IV SECURITY REQUIREMENTS

A sensor network is a special type of network. It shares some commonalities with a typical computer network, but also poses unique requirements of its own. Therefore, we can think of the requirements of a wireless sensor network as encompassing both the typical network requirements and the unique requirements suited solely to wireless sensor networks.

A. *Data Confidentiality*

Data confidentiality is the most important issue in network security. Confidentiality means keeping information secret from unauthorized parties. The confidentiality relates to the following:

1) A sensor network should not leak sensor readings toits neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.
2) In many applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.
3) Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

B. *Data Integrity*

With the implementation of confidentiality, an adversary may be unable to steal information. Data integrity ensures the receiver that the received data is not altered in transit by an adversary. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or

damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit. Note that Data Authentication can provide Data Integrity also.

C. *Data Freshness*

Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages. Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design. A common defense is to include a monotonically increasing counter with every message and reject messages with old counter values. With this policy, every recipient must maintain a table of the last value from every sender it receives.Assuming nodes devote only a small fraction of their RAM for this neighbour table, an adversary replaying broadcast messages from many different senders can fill up the table. At this point, the recipient has one of two options: ignore any messages from senders not in its neighbor table, or purge entries from the table. Neither is acceptable; the first creates a DoS attack and the second permits replay attacks. In the authors contend that protection against the replay of data packets should be provided at the application layer and not by a secure routing protocol as only the application can fully and accurately detect the replay of data packets (as opposed to retransmissions ,for example). In the authors reason that by using information about the network's topology and communication patterns, the application and routing layers can properly and efficiently manage a limited amount of memory devoted to replay detection. In the authors have identified two types of freshness: weak freshness, which provides partial message ordering, but carries no delay information, and strong freshness, which provides a total order on a request response pair, and allows for delay estimation. Weak freshness is required by sensor measurements, while strong freshness is useful for time synchronization within the network. To solve this problem a once, or another time-related counter, can be added into the packet to ensure data freshness.

D. Availability

Adjusting the traditional encryption algorithms to fit within the wireless sensor network is not free, and will introduce some extra costs. Some approaches choose to modify the code to reuse as much code as possible. Some approaches try to make use of additional communication to achieve the same goal. What's more, some approaches force strict limitations on the data access, or propose an unsuitable scheme (such as a central point scheme) in order to simplify the algorithm. But all these approaches weaken the availability of a sensor and sensor network for the following reasons:

1) Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.
2) Additional communication also consumes more energy. What's more, as communication increases so too does the chance of incurring a communication conflict.
3) A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network.

E. Self Organization

A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security as well.

F. Time Synchronization

Most sensor network applications reply on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair-wise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc.

G. Secure Localization

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals. This Section has discussed about the security goals that are widely available for wireless sensor networks and the next section explains about the attacks that commonly occur on wireless sensor networks.

H. Authentication

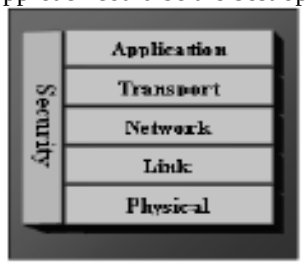
In a sensor network, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision making process originates from the correct source. Data authentication prevents unauthorized parties from participating in the network and legitimate nodes should be able to detect messages from unauthorized nodes and reject them. In the two party communication case, data authentication can be achieved through a purely symmetric mechanism: The sender and the receiver share a secret key to compute a message authentication code (MAC) of all communicated data. When a message with a correct MAC arrives, the receiver knows that it must have been sent by the sender. However, authentication for broadcast messages requires stronger trust assumptions on the
network nodes. The creators of SPINS contend that if one sender wants to send authentic data to mutually untrusted receivers, using a symmetric MAC is insecure since any one of the receivers know the MAC key, and hence could impersonate the sender and forget messages to other receivers. SPINS constructs authenticated broadcast from symmetric primitives, but introduces asymmetry with delayed key disclosure and one-way function key chains. LEAP uses a globally shared symmetric key for broadcast messages to the whole group. However, since the group key is shared among all the nodes in the network, an efficient rekeying mechanism is defined for updating this key after a compromised node is revoked. This means that LEAP has also defined an efficient mechanism to verify whether a node has been compromised.

V PROPOSED SECURITY SCHEMES

In the recent years, wireless sensor network security has been able to attract the attentions of a number of researchers around the world. In this section we review about the security schemes proposed or implemented so far for wireless sensor networks[3].

A. *Holistic Security in Wireless Sensor Networks*

A holistic approach aims at improving the performance of wireless sensor networks 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 employing a holistic approach could be the best option.



Holistic view of Security in WNS

The holistic approach has some basic principles like, in a given network; security is to be ensured for all the layers of the protocol stack, the cost for ensuring security should not surpass the assessed security risk at a specific time, if there is no physical security ensured for the sensors, the security measures must be able to exhibit a graceful degradation if some of the sensors in the network are compromised, out of order or captured by the enemy and the security measures should be developed to work in a decentralized fashion. If security is not considered for all of the security layers, for example; if a sensor is somehow captured or jammed in the physical layer, the security for the overall network breaks despite the fact that, there are some efficient security mechanisms working in other layers. By building security layers as in the holistic approach, protection could be established for the overall network.

VI ATTACKS

Sensor networks are particularly vulnerable to several key types of attacks. Attacks can be performed in a variety of ways, most notably as denial of service attacks, but also through traffic analysis, privacy violation, physical attacks, and so on. Denial of service attacks on wireless sensor networks can range from simply jamming the sensor's communication channel to more sophisticated attacks designed to violate the 802.11 MAC protocol or any other layer of the wireless sensor network. Due to the potential asymmetry in power and computational constraints, guarding against a well orchestrated denial of service attack on a wireless sensor network can be nearly impossible. A more powerful node can easily jam a sensor node and effectively prevent the sensor network from performing its intended duty. We note that attacks on wireless sensor networks are not limited to simply denial of service attacks, but rather encompass a variety of techniques including node takeovers, attacks on the routing protocols, and attacks on a node's physical security. In this section, we first address some common denial of service attacks and then describe additional attacking, including those on the routing protocols as well as an identity based attack known as the Sybil attack[1].

1)Passive Attacks:
The monitoring and listening of the communication
channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature.

2)Active Attacks:
The unauthorized attackers monitors, listens to and
modifies the data stream in the communication channel are known as active attack.

The most popular types of attacks are:
1) Denial of Service Attacks
2) The Sybil Attack
3) Traffic Analysis Attack
4) Node Replication Attack
5) Attacks against Privacy
6) Physical Attacks

A. *Denial of Service Attacks*
Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. 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 wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at
link layer, collision, exhaustion and unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

B. *the Sybil Attack*

A single node duplicates itself and presented in the
multiple locations. The Sybil attack targets fault tolerant schemes such as distributed storage, multipath routing and topology maintenance. In a Sybil attack, a single node presents multiple identities to other nodes in the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network.

A. Traffic Analysis Attack
Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns. Sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network.

B. Node Replication Attack
Conceptually, a node replication attack is quite simple; an attacker seeks to add a node to an existing sensor network by copying the nodeID of an existing sensor node. A node replicated in this approach can severely disrupt a sensor network's performance. Packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc. If an attacker can gain physical access to the entire network he can copy cryptographic keys to the replicated sensor nodes. By inserting the replicated nodes at specific network points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether.

C. Attacks against Privacy
The main privacy problem is not that sensor networks
enable the collection of information. In fact, much
information from sensor networks could probably be
collected through direct site surveillance. Rather, sensor networks intensify the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information at low-risk in anonymous manner.

D. Physical Attacks
Sensor networks typically operate in hostile outdoor
environments. In such environments, the small form factor of the sensors, coupled with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks, i.e., threats due to physical node destructions. Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses
are irreversible. For instance, attackers can extract

cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.

VII DEFENSE MEASURES

The security mechanisms are actually used to detect,
prevent and recover from the security attacks. A wide variety of security schemes can be invented to counter malicious attacks and these can be categorized as highlevel and low-level.

A. Low-Level Mechanism

Low-level security primitives for securing sensornetworks includes,

1)Key establishment and trust setup:

The primary requirement of setting up the sensor network is the establishment ofcryptographic keys. Generally the sensor devices have limited computational power and the public key cryptographic primitives are too expensive to follow. Key-establishment techniques need to scale to networks with hundreds or thousands of nodes. In addition, the communication patterns of sensor networks differ from traditional networks; sensor nodes may need to set up keys with their neighbors and with data aggregation nodes. The disadvantage of this approach is that attackers who compromised sufficiently and many nodes could also reconstruct the complete key pool and break the scheme.

2)Secrecy and authentication:

Most of the sensor network applications require
protection against eavesdropping, injection, and modification of packets. Cryptography is the standard defense. Remarkable system trade-offs arise when incorporating cryptography into sensor networks. For point-to-point communication, end-to-end cryptography achieves a high level of security but requires that keys be set up among all end points and be incompatible with passive participation and local broadcast. Link-layer cryptography with a network wide shared key simplifies key setup and supports passive participation and local broadcast, but intermediate nodes might eavesdrop or alter messages. The earliest sensor networks are likely to use link layer cryptography, because this approach provides the greatest ease of deployment among currently available network cryptographic approaches.

3)Privacy:

Like other traditional networks, the sensor networks have also force privacy concerns. Initially the sensor networks are deployed for legitimate purpose might subsequently be used in unanticipated ways. Providing awareness of the presence of sensor nodes and data acquisition is particularly important.

4)Robustness to communication denial of service:

An adversary attempts to disrupt the network's operation by broadcasting a high-energy signal. If the transmission is powerful enough, the entire system's communication could be jammed. More sophisticated attacks are also possible; the adversary might inhibit communication by violating the 802.11 medium access control (MAC) protocol by, say, transmitting while a neighbor is also transmitting or by continuously requesting channel access with a request-tosend signal.

5)Secure routing:

Routing and data forwarding is a crucial service for
enabling communication in sensor networks. Unfortunately, current routing protocols suffer from many security vulnerabilities. For example, an attacker might launch denialof-service attacks on the routing protocol, preventing communication. The simplest attacks involve injecting malicious routing information into the network, resulting in routing inconsistencies. Simple authentication might guard against injection attacks, but some routing protocols are susceptible to replay by the attacker of legitimate routing messages.

6)Resilience to node capture:

One of the most challenging issues in sensor networks is resiliency against node capture attacks. In most applications, sensor nodes are likely to be placed in locations easily accessible to attackers. Such exposure raises the possibility that an attacker might capture sensor nodes, extract cryptographic secrets, modify their programming, or replace
them with malicious nodes under the control of the attacker. Tamper-resistant packaging may be one defense, but it's expensive, since current technology does not provide a high level of security.Algorithmic solutions to the problem of node capture are preferable.

B. High-Level Mechanism

High-level security mechanisms for securing sensor networks, includes,

1)Secure group management:
Each and every node in a wireless sensor network is limited in its computing and communication capabilities. However, interesting in-network data aggregation and analysis can be performed by groups of nodes. For example, a group of nodes might be responsible for jointly tracking a vehicle through the network. The actual nodes comprising the group may change continuously and quickly. Many other key services in wireless sensor networks are also performed by groups. Consequently, secure protocols for group management are required, securely admitting new group members and supporting secure group communication. The outcome of the group key computation is normally transmitted to a base station. The output must be authenticated to ensure it comes from a valid group.

2)Intrusion detection:
Wireless sensor networks are susceptible to many forms of intrusion. Wireless sensor networks require a solution that is fully distributed and inexpensive in terms of communication, energy, and memory requirements. The use of secure groups may be a promising approach for decentralized intrusion detection.

3) Secure data aggregation:
One advantage of a wireless sensor network is the finegrain sensing that large and dense sets of nodes can provide. The sensed values must be aggregated to avoid overwhelming amounts of traffic back to the base station. For example, the system may average the temperature of a geographic region, combine sensor values to compute the location and velocity of a moving object, or aggregate data to avoid false alarms in real-world event detection. Depending
on the architecture of the wireless sensor network,
aggregation may take place in many places in the network. All aggregation locations must be secured.

VIII CHALLENGES OF SENSOR NETWORKS

The nature of large, ad-hoc, wireless sensor networks presents significant challenges in designing security schemes. A wireless sensor network is a special network which has many constraint compared to a traditional computer network[2].

A. Wireless Medium

The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Although this problem is not unique to sensor networks, traditional solutions must be adapted to efficiently
execute on sensor networks.

B. Ad-Hoc Deployment

The ad-hoc nature of sensor networks means no structure can be statically defined. The network topology is always subject to changes due to node failure, addition, or mobility. Nodes may be deployed by airdrop, so nothing is known of the topology prior to deployment. Since nodes may fail or be replaced the network must support self-configuration.
Security schemes must be able to operate within this
dynamic environment.

C. Hostile Environment

The next challenging factor is the hostile environment in which sensor nodes function. Motes face the possibility of destruction or capture by attackers. Since nodes may be in a hostile environment, attackers can easily gain physical access to the devices. Attackers may capture a node, physically disassemble it, and extract from it valuable information (e.g. cryptographic keys). The highly hostile environment represents a serious challenge for security researchers.

D. Resource Scarcity

The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity, and memory. This is no trivial task. Energy is the most precious resource for sensor networks. Communication is especially expensive in terms of
power. Clearly, security mechanisms must give special effort to be communication efficient in order to be energy efficient.

E. Immense Scale

The proposed scale of sensor networks poses a significant challenge for security mechanisms. Simply networking tens to hundreds of thousands of nodes has proven to be a substantial task. Providing security over such a network is equally

challenging. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency.

F. Unreliable Communication

Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication.

1)Unreliable Transfer:

Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable.

2) Conflicts:

Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network.

3) Latency:

The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes.

G. Unattended Operation

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main cautions to unattended sensor nodes.

1)Exposure to Physical Attacks:

The sensor may be deployed in an environment open to adversaries, bad weather, and so on. The probability that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network.

2)Managed Remotely:

Remote management of a sensor network makes it virtually impossible to detect physical tampering and physical maintenance issues.

3)No Central Management Point:

A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile. Perhaps most importantly, the longer that a sensor is left unattended the more likely that an adversary has compromised the node.

IX CONCLUSION

In this paper, we have described the four main aspects of wireless sensor network security: obstacles, requirements, attacks, and defenses. Within each of those categories we have also sub-categorized the major topics including routing, trust, denial of service, and so on.Wireless Sensor Networks, are self organising, self healing networks of small "nodes" have huge potential across industrial, military and many other sectors. While appreciable sales have now been established, major progress depends on standards and achieving twenty year life.

REFERENCES

1) Kumar, P.; Cho, S.; Lee, D.S.; Lee, Y.D.; Lee, H.J. TriSec: A secure data framework for wireless sensor networks using authenticated encryption. Int. J. Marit. Inf. Commun. Sci. (2010), 129-135.

2) Hadim, Salem, Nader Mohamed (2006). "Middleware Challenges and Approaches for Wireless Sensor Networks". IEEE Distributed Systems Online **7** (3). art. no. 0603-o3001.

3) Protocols and Architectures for Wireless Sensor Networks, Holger Karl, Andreas Willig, ISBN 0-470-09511-3, 526 pages, January 2006.

4) H. Mohamed and B. Majid, "Forest Fire Modeling and Early Detection using Wireless Sensor Network" in *Ad Hoc & Sensor Wireless Networks*, Vol 7, Philadelphia: Old City Publishing, 2009.

