ISSN:0975-9646

Review of Threats in Wireless Sensor Networks

Monika roopak,Tushank bhardwaj, Sumit soni, Gunjan batra

Ansal Institute of Technology, Gurgaon
(Department Of Computer Science Engineering)

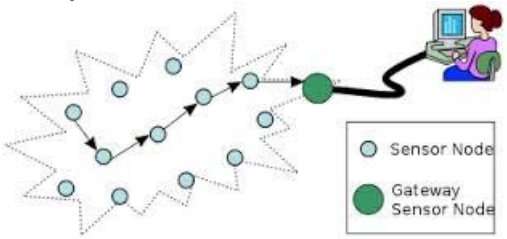
Abstract—Wireless sensor networks are networked systems, characterized by several energy resources, and the security mechanisms are actually used to detect, prevent and recover from the security attacks. In this security concerns must be addressed from the beginning of the system design. Securely communication 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 for wireless sensor networks and also present the obstacles and the requirements in the sensor security, classify many of the current attacks.

….

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

INTRODUCTION

Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements. 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 is also identified, which provide vital information for future researchers. Finally we conclude the paper delineating the research challenges and future trends toward the research in WSN security.



BASIC SECURITY SCHEMES IN WIRELESS SENSOR NETWORKS:

A. Cryptography-

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.

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.

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.

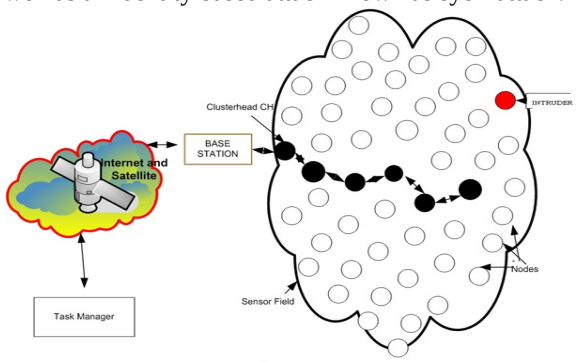
A. Holistic Security in Wireless Sensor Networks

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.

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.

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 sybil attack.



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

Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Further more, 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.

A. **Based On the Capability of the Attacker**

***1*. Outsider versus insider (node compromise) attacks**

Outside attacks 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, we require robustness against Outsider Attacks, Resilience to Insider Attacks, Graceful Degradation with Respect to Node Compromise and Realistic Levels of Security.

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.

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.

B. Attacks on Information in Transit

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink stored within a sensor node. The attacker might also attempt to load its program in the compromised node.

1 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.

2. Network-based attacks

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

D. Based On Protocol Stack

This section discusses about the WSN layer wise attack.

1. Physical Layer

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 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.

Radio interference

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

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. 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.

2. Data Link Layer

(a) Continuous Channel Access (Exhaustion):

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.

(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 .

(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.

(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.

(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.

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.

(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.

(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.

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.

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.

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.

(d) 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.

(e) Homing:

It 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.

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.

(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 . Header or full packet authentication can defeat such an attack.

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.

(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.

(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.

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.

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.

SECURITY REQUIREMENTS FOR SENSOR NETWORKS:

As the sensor networks can also operate in an ad hoc manner the security goals cover both those of the traditional networks and goals suited to the unique constraints of ad hoc sensor networks. Setting security goals for sensor networks will depend on knowing what it is that needs protecting. Sensor networks share some of the features of mobile ad hoc networks. Therefore the security goals encompass both those of the traditional networks and goals suited to the unique constraints of sensor networks. The security goals are classified as primary and secondary. The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA). The secondary goals are Data Freshness, Self-Organization, Time Synchronization and Secure Localization. The four security goals for sensor networks are determined as Confidentiality, Integrity, Authentication and Availability (CIAA).

A. Confidentiality

Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security. Carman et al. and Perrig et al. have the following to say regarding confidentiality in sensor networks:

- A sensor node should not reveal its data to the neighbors. For example, in a sensitive military application where an adversary has injected some malicious nodes into the network, confidentiality will preclude them from gaining access to information regarding other nodes.
- Establishing and maintaining confidentiality is extremely important when node identities and keys are being distributed to establish a secure communication channel among sensor nodes.

B. Integrity

Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed while on the network. Even if the network has confidentiality measures in place, there is still a possibility that the data's

integrity has been compromised by alterations. The integrity of the network will be in question if:

- A malicious node present in the network injects some bogus data.
- Turbulent conditions due to wireless channel cause damage or loss of data.

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.

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.
5)http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.94.3415&rep=rep1&type=pdf
6)https://www.nics.uma.es/system/files/papers/Lopez2009.pdf
7)http://wwwusers.cs.york.ac.uk/~jac/PublishedPapers/ThreatModellingInMANETs.pdf
8)http://bioinfo.in/uploadfiles/13111289031_1_2_IJN.pdf
9)http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.94.3415&rep= rep1&type=pdf