International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161
©2014 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

Review Article

Security in Wireless Sensor Networks: Issues and Security Mechanisms

Sachin Lalar[Â*]

[Â]Department of Computer Science & Engg., TERI, Kurukshetra

Accepted 10 January 2014, Available online 01 February 2014, **Vol.4, No.1 (February 2014)**

Abstract

Wireless sensor networks are a new type of networked systems, characterized by severely constrained computational and energy resources, and an ad hoc operational environment. Wireless sensor network is highly vulnerable to attacks because it consists of various resources constrained devices with their low battery power, less memory, and associated low energy. Sensor nodes communicate among themselves via wireless links. However, there are still a lot of unresolved issues in wireless sensor networks of which security is one of the hottest research issues. This paper is an attempt to present a survey on the major topics in wireless sensor network security, 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.

Keyword: *Wireless sensor networks, network security, attacks, defensive measures*

1. Introduction

Recently, wireless sensor networks (WSN) have gained great popularity, mainly because they provide a low cost alternative to solving a great variety of real-world problems. Their low cost enables the deployment of large amounts of sensor nodes (in the order of thousands, and in the future perhaps millions), which most of the time operate under harsh environments. WSN present extreme resource limitations, mainly in available memory space and energy source. Both limitations represent great obstacles for the integration of traditional security techniques. The highly unreliable communication channels that are used in WSN and the fact that they operate unattended make the integration of security techniques even harder. The advancement in wireless communications and integration of electronics technology have enabled the development of low cost, low-power, multifunctional sensor nodes. These nodes small in size and communicate among themselves in short distances. These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks [Culler and Hung, 2004]. Sensor networks represent a significant improvement over traditional sensors. A sensor network is composed of a large number of tiny sensor nodes that are densely deployed either inside the phenomenon or very close to each other. The position of these sensor nodes are adhoc and may change according to the requirement. This allows nodes suitable for random deployment in inaccessible terrains or disaster relief operations. As sensor nodes are adhoc in nature there is need of sensor network protocols and algorithms which allows nodes with self-organizing capabilities [Pathan,Islam,Sayeed,Ahme and Hong, 2006]. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an onboard processor. Instead of sending the raw data to the nodes responsible for the fusion, they use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.

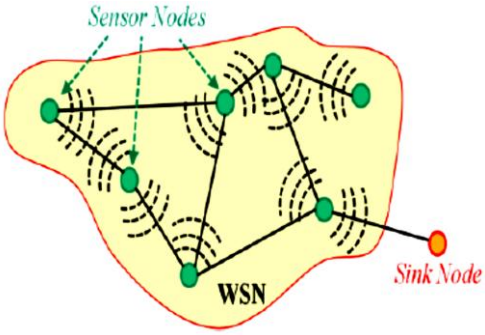

Figure 1: Scenario of Wireless Sensor Network

Sensor networks are being used in a wide range of application areas. The major application domains are, home and office, control and automation, logistics and transportation, environmental monitoring, healthcare, security and surveillance, tourism and leisure, education and training and entertainment. Sensor devices that can be used to monitor human activities have garnered great research interest in recent years. Some of the application areas are health, military, and home. In military, for example, the rapid deployment, self organization, and fault tolerance characteristics of sensor networks make them a very promising sensing technique for military command,

*Corresponding author: **Sachin Lalar**

control, communications, computing, intelligence, surveillance, reconnaissance, and targeting systems. In health, sensor nodes can also be deployed to monitor patients and assist disabled patients. Some other commercial applications include managing inventory, monitoring product quality, and monitoring disaster areas. Such networks have substantial data acquisition and data processing capabilities and for this reason is deployed densely throughout the area where they will monitor specific phenomena [Akyildiz et al ,2002] [Dai et al ,2005].

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:

- The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are densely deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network changes very frequently.
- Sensor nodes mainly use a broadcast communication paradigm, whereas most ad hoc networks are based on point-to point communications.
- 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 [Pathan,Islam,Sayeed,Ahme and Hong, 2006].

However, due to the lack of tamper-resistant packaging and the insecure nature of wireless communication channels, these networks are vulnerable to internal and external attacks [Undercoffer et al 2002] [Blackert et al 2003] [Wood et al,2003]. Adversary can physically capture and get the information contained in the sensor node, eavesdrop and inject new messages, modify messages. Hence there must be some sort of mechanism for node to node securely data transmission. We discuss these issues and challenges in this paper. To address the critical security issues in wireless sensor networks we talk about basics of network security and their applicability in Section 2. We explore various types of threats and attacks against wireless sensor network in Section 3. Section 4 reviews the security mechanisms in WSN. Finally Section 5 concludes the paper delineating the research challenges and future trends toward the research in wireless sensor network security.

2. Security Requirement in WSN

Security is one of the most important aspects of any system. Since sensor networks are used for many applications where security is crucial. It is essential to ensure secure communication among the nodes. It is not possible to use general secure communication techniques for WSNs because of resource-constraints and communication overheads involved [Carman et al ,2000]. The security requirement of wireless sensor network can be classified as follows:

- **Data Confidentiality**

Data confidentiality is the biggest problem in network security. Every network with any security approach would probably address this issue before any other. In sensor networks, confidentiality relates to the following:

- A sensor node must not filter sensor readings to its neighbors; particularly on military applications where the stored data in a node can be highly confidential.
- On many applications, the nodes need to communicate highly confidential data (i.e., key distribution), thus, it is very important to build a secure communication channel in WSN.
- The nodes' public information, such as their identity and their public keys, can be encrypted to a certain extent for protecting against traffic analysis attacks.

The traditional approach for keeping confidential information secret is to encrypt it using a secret key that only the destination node knows, thus, resulting in confidentiality [Carman et al ,2000].

- **Data Integrity**

Data in transit can be changed by the adversaries. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Data integrity is to ensure that information is not changed in transit, either due to malicious intent or by accident [Undercoffer et al 2002].

- **Availability**

Availability ensures that the desired network services are available even in the presence of denial-of-service attacks require configuring the initial duty cycle carefully [Dai et al ,2005].

- **Authorization**

Authorization ensures that only authorized sensors can be involved in providing information to network services [Dai et al ,2005].

- **Privacy**

Privacy prevents adversaries from obtaining information that may have private content [Dai et al ,2005.

- **Authentication**

Authentication which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node [Dai et al ,2005].

- **Anonymity**

Anonymity hides the source of the data. It is a service that

can help with data confidentiality and privacy [Akyildiz et al ,2002].

- **Resilience**

Resilience sustains the network functionalities when a portion of nodes are compromised by the attacks [Carman et al ,2000].

- **Time Synchronization**

Most sensor network applications rely on some form of time synchronization. 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 [Undercoffer et al 2002, Carman et al ,2000].

- **Secure Localization**

In WSN each sensor node is required to locate itself in the network accurately and automatically to identify the location of the fault [Undercoffer et al 2002].

- **Flexibility**

Sensor networks will be used in dynamic battlefield scenarios where environmental conditions, threat, and mission may change rapidly. Changing mission goals may require sensors to be removed from or added to an established sensor node. Furthermore, two or more sensor networks may be fused into one, or a single network may be split in two Key establishment protocols must be flexible enough to provide keying for all potential scenarios a sensor network may encounter [Yan et al ,2010][Undercoffer et al 2002].

- **Freshness**

Freshness implies that the data is recent and ensures that no adversary can replay old messages [Dai et al ,2005]. To make sure that no old messages replayed a timestamp can be added to the packet [Undercoffer et al 2002].

3. Attacks in WSNs

The nature of the WSN makes them vulnerable to several types of attacks. Such attacks can be perpetrated in a variety of ways, most notably are the denial or service attacks (DoS), but there are also traffic analysis attacks, eavesdropping, physical attacks, and others. DoS attacks in wireless sensor networks go from simple communication channel saturation techniques to more sophisticated designed to tamper with the message authentication code (MAC) layer protocol. Due to the great differences in available energy and computational power, protecting against a well designed denial-of-service attack is practically impossible [Wood et al,2002][Blackert et al 2003][Wan et al ,2004]. A more powerful node could easily block any other normal node, and consequently, prevent the sensor network from performing its function.

WSN attacks categorized at different layers

A. Physical layer: Attacks at the physical layer include jamming and tampering. These two attacks are discussed in this subsection.

1. Jamming

Jamming is a type of attack which interferes with the radio frequencies. 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). An attacker sends some radio waves at the same frequency that it is used by wireless sensor networks [Wood et al,2003][Cagalj et al]. A jamming source may either be powerful enough to disrupt the entire network or less powerful and only able to disrupt a smaller portion of the network.

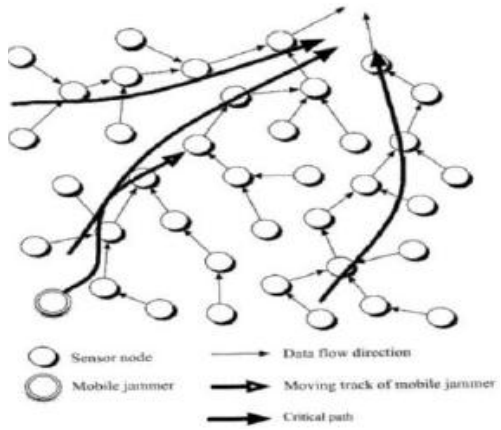

Figure 2: Jamming Attack

2. Tampering

Another physical layer attack is tampering [Cagalj et al]. Given physical access to a node, an attacker can extract sensitive information such as cryptographic keys or other data on the node. The node may also be altered or replaced to create a compromised node which the attacker controls.

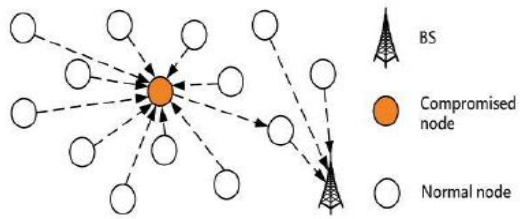

Figure 3: Tampering Attack

B. Data link layer: Attacks at the link layer include collisions, resource exhaustion, and unfairness. This subsection looks at each of these three link-layer attack categories.

1. *Collisions:* A collision results when two nodes trying to send data on same frequency. 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. An adversary may strategically cause collisions in specific packets such as ACK control messages. A possible result of such collisions is the costly exponential back-off. The adversary may simply violate the communication protocol and continuously transmit messages in an attempt to generate collisions [Wagner et al , 2004].

2. *Exhaustion:* Repeated collisions can also be used by an attacker to cause resource exhaustion [Wagner et al , 2004][Wagner et al ,2003]. For example, a naive link-layer implementation may continuously attempt to retransmit the corrupted packets. Unless these hopeless retransmissions are discovered or prevented, the energy reserves of the transmitting node and those surrounding it will be quickly depleted [Wagner et al , 2004][Wagner et al ,2003].

3. *Unfairness:* Unfairness can be considered a weak form of a DoS attack. An attacker may cause unfairness in a network by intermittently using the above link-layer attacks. Instead of preventing access to a service outright, an attacker can degrade it in order to gain an advantage such as causing other nodes in a real-time MAC protocol to miss their transmission deadline [Wagner et al , 2004][Wagner et al ,2003].

C. Network layer: The network and routing layer of sensor networks is usually designed according to the following principles [Wagner et al ,2003] [Smith et al 2003].

• Power efficiency is an important consideration.
• Sensor networks are mostly data-centric.
• An ideal sensor network has attribute-based addressing and location awareness.

The attacks in the network layer include the following:

1. Spoofed, Altered, or Replayed Routing Information: The most direct attack against a routing protocol in any network is to target the routing information

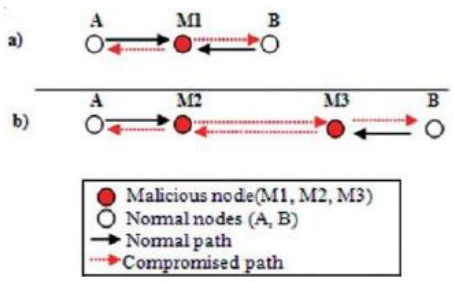

Figure 4: Replay Attack

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 [Wood et al 2002][Mayank Saraogi,2004]. 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.

2. Sybil: The Sybil attack is a case where one node presents more than one identity to the network [Douceur,2002]. It was originally described as an attack intended to defeat the objective of redundancy mechanisms in distributed data storage systems in peer-to-peer networks [Newsome et al 2002]. A Sybil attack is attack in which an attacker destabilizes the reputation scheme of a peer-to-peer network by creating a huge number of pseudonymous entities, using them to gain a disproportionately big influence [Douceur,2002].

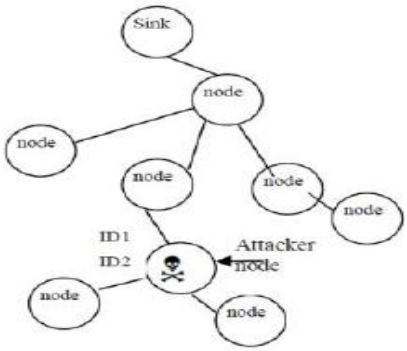

Figure 5: Sybil Attack

3. Selective Forwarding: A significant assumption made in multihop networks is that all nodes in the network will accurately forward receive messages. An attacker may create malicious nodes which selectively forward only certain messages and simply drop others [Wagner et al ,2003] [Yang et al ,2004]. One form of this attack is Black hole. A simple approach is that malicious nodes refuse to forward any packets through it, which is like a black hole attack [Karakehayov,2005].

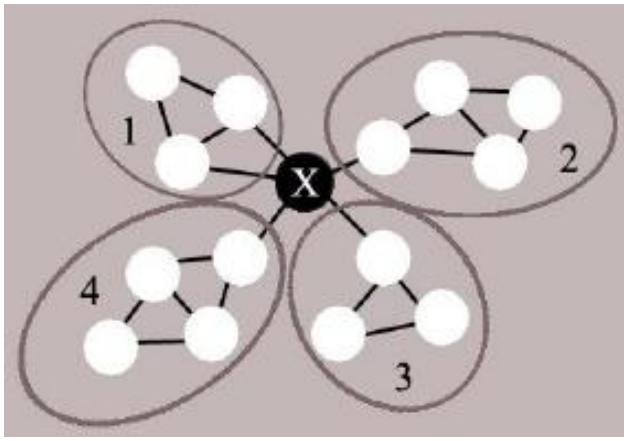

Figure 6: An Example of Black Hole Attack

4. Wormhole attack: Wormhole attack needs to insert at least two malicious nodes in the network and these nodes

are connected by a powerful connection. A wormhole is low latency link between two portions of a network over which an attacker replays network messages [Cagalj et al] [Perrig and Johnson,2003]. This link may be established either by a single node forwarding messages between two adjacent but otherwise non-neighboring nodes or by a pair of nodes in different parts of the network communicating with each other.

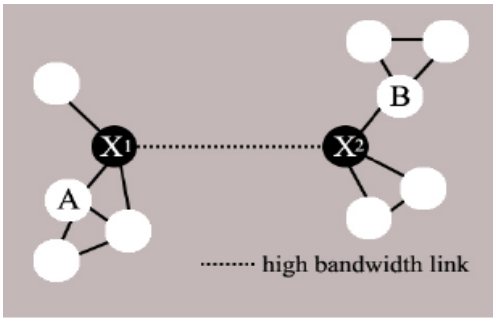

Figure 7: Wormhole Attack

5. Sinkhole: In a sinkhole attack, an attacker makes a compromised node look more attractive to surrounding nodes by forging routing information. The end result is that surrounding nodes will choose the compromised node as the next node to route their data through. This type of attack makes selective forwarding very simple, as all traffic from a large area in the network will flow through the adversary's node [Culpepper et al 2004].

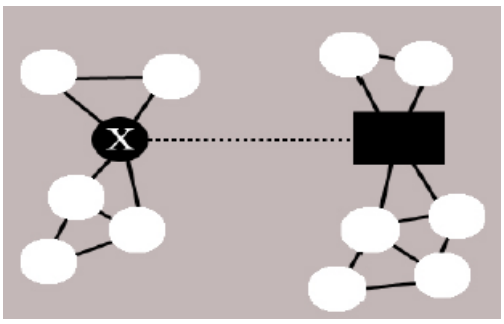

Figure 7: Sinkhole Attack

6. Hello Flood Attacks: An attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within a WSN. The sensors are thus influenced that the adversary is their neighbor. As a result, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker [Hamid et al , 2006].

7. Acknowledgment Spoofing: Routing algorithms used in sensor networks sometimes require acknowledgments to be used. Attacking node spoof the routing information and send false information to the receiving node. An example of such false information is claiming that a node is alive when in fact it is dead [Karlof et al ,2004].

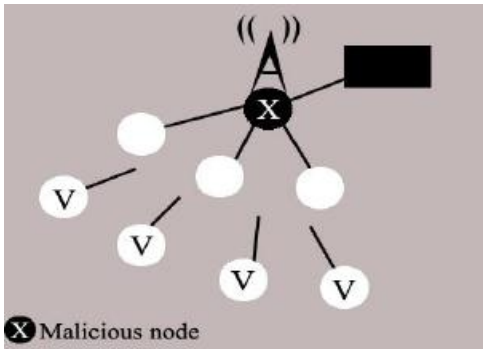

Figure 8: A Hello Flood Attack

D. Transport layer: Two possible attacks in this layer, flooding and desynchronization, are discussed in this subsection.

1. *Flooding:* Whenever a protocol is required to maintain state at either end of a connection it becomes vulnerable to memory exhaustion through flooding [Wood et al,2002] [Karlof et al ,2004]. An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored.

2. *Desynchronization:* Desynchronization refers to the disruption of an existing connection [Wood et al,2002] [Karlof et al ,2004]. An attacker may, for example, repeatedly spoof messages to an end host, causing that host to request the retransmission of missed frames. If timed correctly, an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data, thus causing them to instead waste energy by attempting to recover from errors which never really existed.

4. Security Schemes for Wireless Sensor Networks

C. Karlof and D. Wagner give an analysis of secure routing in wireless sensor networks [Karlof et al ,2004]. L. Yuan and G Qu studies how to design secure distributed sensor networks with multiple supply voltages to reduce the energy consumption on computation and therefore to extend the network's life time [Yuan and Qu,2002]. Younis et. al. aim at increasing energy efficiency for key management in wireless sensor networks and uses Younis et. al. network model for its application [Younis et. Al,2003]. Wood et al. studies DoS attacks against different layers of sensor protocol stack [Wood and Stankovic, 2002]. JAM presents a mapping protocol which detects a jammed region in the sensor network and helps to avoid the faulty region to continue routing within the network, thus handles DoS attacks caused by jamming [Wood et al 2003].

Cagalj et. Al. show that wormholes those are so far considered harmful for WSN could effectively be used as a reactive defense mechanism for preventing jamming DoS attacks. Ye et. al. present a statistical en-route

filtering (SEF) mechanism to detect injected false data in sensor network and focus mainly on how to filter false data using collective secret and thus preventing any single compromised node from breaking the entire system [Zhang et al ,2005]. SNEP & μTESLA [Perrig et al ,2002] are two secure building blocks for providing data confidentiality, data freshness and broadcast authentication.

In Table 1 summarize various security schemes along with their main properties proposed so far for wireless sensor networks.

Table 1: Summary of various security schemes for wireless sensor networks

Attacks Derived	Security Schemes	Major Features
DoS Attack (Jamming)	JAM	Avoidance of jammed region by using coalesced neighbor nodes
DoS Attack (Jamming)	Wormhole based	Uses wormholes to avoid jamming
Information Spoofing	Statistical En-Route Filtering	Deletes and Drops false reports during forwarding process
Sybil Attack	Radio Resources Testing , Random Key Pre-distribution etc.	Uses radio resources, Random key pre-distribution, Registration procedure, Position verification and Code attestation for detecting sybil entity
Hello Flood Attack	Bidirectional Verification Multi-path multi-base station routing	Adopts probabilistic secret sharing, Uses bidirectional verification and multi-path multi-base station routing
Information or Data Spoofing	On Communication Security	Efficient resource management. Protects the network even if part of the network is compromised
Wormhole Attack, Information or Data Spoofing	TIK	Based on symmetric cryptography, Requires accurate time synchronization between all communicating parties, implements temporal leashes
Blackholes Attacks	REWARD	Uses geographic routing. Take advantage of the broadcast inter-radio behavior to watch neighbor transmissions and detect blackhole attacks
Data and information spoofing, Message Replay Attack	TinySec	Focuses on providing message authenticity, integrity and confidentiality, Works in the Link Layer
Data and information spoofing, Message Replay Attack	SNEP & µTESLA	Semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead

TinySec proposes a link layer security mechanism for sensor networks which uses an efficient symmetric key encryption protocol [Karlof et al 2004]. Newsome et. al. proposes some defense mechanisms against sybil attack in sensor networks. Hamid et. al. presents a probabilistic secret sharing protocol to defend Hello flood attacks. The scheme uses a bidirectional verification technique and also introduces multi-path multi-base station routing if bidirectional verification is not sufficient to defend the attack. REWARD is a routing algorithm which fights against blackholes in the network [Karakehayov,2005]. Johnson et. al. implement symmetric key cryptographic algorithms with delayed key disclosure on motes to establish secure communication channels between a base station and sensors within its range.

Conclusion

Wireless Sensor Networks often operate in a resource constrained environment. Optimal resource utilization is main objective of WSN. But Wireless Sensor Networks are equally vulnerable to security attacks. Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. However, developing such a detection mechanism and making it efficient represents a great research challenge. Many of today's proposed security schemes are based on specific network models. As there is a lack of combined effort to take a common model to ensure security for each layer, in future though the security mechanisms become well-established for each individual layer, combining all the mechanisms together for making them work in collaboration with each other will incur a hard research challenge. This paper motivates future researchers to come up with smarter and more robust security mechanisms and make their network safer.

References

Culler, D. E and Hong, W. (June 2004),Wireless Sensor Networks, *Communication of the ACM*, Vol. 47, No. 6, pp. 30-33.

Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S.(2006),A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks, *IEEE ICNEWS*.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E. (2002), Wireless Sensor Networks: A Survey, Computer Networks, 38, pp. 393-422.

Dai, S, Jing, X, and Li, L.(May 2005),Research and analysis on routing protocols for wireless sensor networks, *Proc. International Conference on Communications, Circuits and Systems*, Volume 1, pp. 407-411.

Zhou, L. and Haas, Z. J.(Dec 1999),Securing ad hoc networks, *IEEE Network*, Volume 13, Issue 6, pp. 24 – 30.

Yan-Xiao Li, Lian-Qin and Qian-Liang (2010), Research On Wireless Sensor Network Security, 2010 International Conference on Computational Intelligence and Security

Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J.(2002), Security for Sensor Networks, CADIP Research Symposium,

available at,http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf

D. W. Carman, P. S. Krus, and B. J. Matt. (2000), Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood,MD.

Wood, A. D. and Stankovic, J. A.(Oct 2002),Denial of Service in Sensor Networks , *Computer*, Volume 35, Issue 10, pp. 54 - 62.

Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M.(April 2003),Analyzing interaction between distributed denial of service attacks and mitigation technologies, *Proc. DARPA Information Survivability Conference and Exposition*, Volume 1, pp. 26 – 36

Wang, B-T. and Schulzrinne, H.(May 2004),An IP traceback mechanism for reflective DoS attacks, *Canadian Conference on Electrical and Computer Engineering*, Volume 2, pp. 901 – 904.

Wood, A.D., Stankovic, J.A., and Son, S.H.(2003), JAM: A Jammed-Area Mapping Service for Sensor Networks, 24th *IEEE Real-Time Systems Symposium*, pp. 286-297.

Cagalj, M., Capkun, S., and Hubaux, J-P., Wormhole-baseAnti-Jamming Techniques in Sensor Networks from http://lcawww.epfl.ch/Publications/Cagalj/CagaljCH05-worm.pdf

C. Karlof, N. Sastry, and D. Wagner (November 2004), Tinysec: A link layer security architecture for wireless sensor networks. In *Second ACM Conference on Embedded Networked Sensor Systems (SensSys 2004)*, pages 162–175.

C. Karlof and D. Wagner (September 2003), Secure routing in wireless sensor networks: Attacks and countermeasures. *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, 1(2–3):293–315.

Strulo, B., Farr, J., and Smith, A. (2003), Securing Mobile Ad hoc Networks — A Motivational Approach, BT Technology Journal, Volume 21, Issue 3, pp. 81 – 89.

A. D. Wood and J. A. Stankovic (2002),Denial of service in sensor networks ,*Computer*, 35(10):54–62

Mayank Saraogi (2004), Security in Wireless Sensor Networks, In *ACM SenSys*.

Douceur, J. (2002), The Sybil Attack, 1st International Workshop on Peer-to-Peer Systems.

Newsome, J., Shi, E., Song, D, and Perrig, A (2004), The sybil attack in sensor networks: analysis & defenses , Proc. of the third international symposium on Information processing in sensor networks, *ACM*, pp. 259 – 268.

Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L. (February 2004),Security in Mobile Ad Hoc Networks: Challenges and Solutions, *IEEE Wireless Communications*, Volume 11, Issue 1, pp. 38 – 47.

Karakehayov, Z (June 2005), Using REWARD to detect team black-hole attacks in wireless sensor networks, in Workshop on Real-World Wireless Sensor Networks (REALWSN'05),Stockholm, Sweden.

Hu, Y.-C., Perrig, A., and Johnson, D.B. (April 2003), Packet leashes: a defense against wormhole attacks in wireless networks, Twenty-Second Annual Joint Conference of the *IEEE Computer and Communications Societies. IEEE INFOCOM* 2003, Vol. 3, pp. 1976 – 1986.

Culpepper, B.J. and Tseng, H.C. (2004), Sinkhole intrusion indicators in DSR MANETs, Proc. First International Conference on Broad band Networks, pp. 681 – 688.

Hamid, M. A., Rashid, M-O., and Hong, C. S. (January 2006), Routing Security in Sensor Network: Hello Flood Attack and Defense, to appear in *IEEE ICNEWS*, Dhaka.

Karlof, C., Sastry, N., and Wagner, D.(2004), TinySec: a link layer security architecture for wireless sensor networks, Proc. of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, pp. 162 – 175.

Yuan, L. and Qu, G. (July 2002), Design space exploration for energy-efficient secure sensor network, Proc. The IEEE International Conference on Application-Specific Systems, *Architectures and Processors*, 2002, pp. 88 – 97.

Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., A Low-Energy Key Management Protocol for Wireless Sensor Networks, *Proc. Eighth IEEE International Symposium on Computers and Communication*, 2003.(ISCC 2003). vol.1,pp. 335 - 340.

Ye, F., Luo, H., Lu, S, and Zhang, L (April 2005), Statistical en-route filtering of injected false data in sensor networks, *IEEE Journal on Selected Areas in Communications*, Volume 23, Issue 4, pp. 839 – 850.

Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D. (2002), SPINS: Security Protocols for Sensor Networks, *Wireless Networks*, vol. 8, no. 5, pp. 521-534.