Rajkumar, Sunitha K R, Dr.H.G.Chandrakanth, / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue4, July-August 2012, pp.1684-1691

A Survey on Security Attacks in Wireless Sensor Network

Rajkumar
Assistant Professor, Dept. of ISE, Sambhram Institute of Technology Bangalore

Sunitha K R
Lecturer, Dept. of ISE, Sambhram Institute of Technology Bangalore

Dr.H.G.Chandrakanth
Sri Krishna Institute of Technology, Bangalore

Abstract

A wireless sensor network (WSN) has important applications such as remote environmental monitoring and target tracking. This has been enabled by the availability, particularly inrecent years, of sensors that are smaller, cheaper, and intelligent. These sensors are equipped with wireless interfaces with which they can communicate with one another to form a network. In this paper we deal with the security of the wireless sensor networks. Staring with a brief overview of the sensor networks, and discusses the current state of the security attacks in WSNs. Various types of attacks are discussed and their countermeasures presented. A brief discussion on the future direction of research in WSN security is also included

Keywords: Wireless Sensor Networks (WSNs), Attacks, Security, Threats.

1 INTRODUCTION

Wireless sensor networks (WSNs) are innovative large-scale wireless networks that consist of distributed, autonomous, low-power, low-cost, small-size devices using sensors to cooperatively collect information through infrastructureless ad-hoc wireless network. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control. Security plays a fundamental role in many wireless sensor network applications. Because sensor networks pose unique challenges, security techniques used in conventional networks cannot be directly applied to WSNs because of its unique characteristics. First, sensor nodes are very sensitive of production cost since sensor networks consist of a large number of sensor nodes. [1] argued that the cost of a sensor node should be much less than one dollar in order for sensor networks to be feasible. Therefore, most sensor nodes are resource restrained in terms of energy, memory, computation, and communication capabilities. Normally sensor nodes are powered by batteries, and recharging batteries are infeasible in many circumstances. Energy consumption becomes a key consideration for most sensor network protocols. Second, Sensor nodes may be deployed in public hostile locations, which make sensor nodes vulnerable to physical attacks by adversaries. Generally, adversaries are assumed to be able to undetectably take control of a sensor node and extract all secret data in the node. Furthermore, the scale of sensor networks is considerably large, and the network topology is dynamically adjusted, because some nodes may die out of running out of energy or failure, and new nodes may join the network to maintain desirable functionality. At last, sensor networks use insecure wireless communication channel and lack infrastructure. As a result, existing security mechanisms are inadequate, and new approaches are desired.

Since large number of sensor nodes are densely deployed, neighbor nodes may be very close to each other. Hence, multihop communication in sensor networks is expected to consume less power than the traditional single hop communication. Furthermore, the transmission power levels can be kept low, which is highly desired in covert operations. Multihop communication can also effectively overcome some of the signal propagation effects experienced in long-distance wireless communication. One of the most important constraints on sensor nodes is the low power consumption requirement. Sensor nodes carry limited, generally irreplaceable, power sources. Therefore, while traditional networks aim to achieve high quality of service (QoS) provisions, sensor network protocols must focus primarily on power conservation. They must have inbuilt trade-off mechanisms that give the end user the option of prolonging network lifetime at the cost of lower throughput or higher transmission delay. Many researchers are currently engaged in developing schemes that fulfill these requirements. In this paper, we present a survey of protocols and algorithms proposed thus far for sensor networks. Our aim is to provide a better understanding of the current research issues in this field. We also attempt an investigation into pertaining design constraints and outline the use of certain tools to meet the design objectives [2].

WSNs are intelligent compared with traditional sensors, and some WSNs are designed to use in-network processing, where sensed data can be gathered in situ and transformed to more abstract and aggregated high-level data before transmission. The combination of processing power, storage and wireless communication also means that data can be assimilated and disseminated using smart algorithms. The vast number of sensor nodes planned for many applications also implies a major portion of these networks would have to acquire self organization capability. Intuitively, a denser infrastructure would create a more effective sensor network. It can provide higher accuracy and has more energy available for aggregation. If not properly handled, a denser network can also lead to collisions during transmission, and network congestion. This will no doubt increase latency and reduce efficiency in terms of energy consumption. One distinguishing characteristic of WSNs is their lack of strong boundaries between sensing, communication and computation. Unlike the Internet, where data generation is mostly the province of end points, in sensor networks every node is both a router and a data source[30].

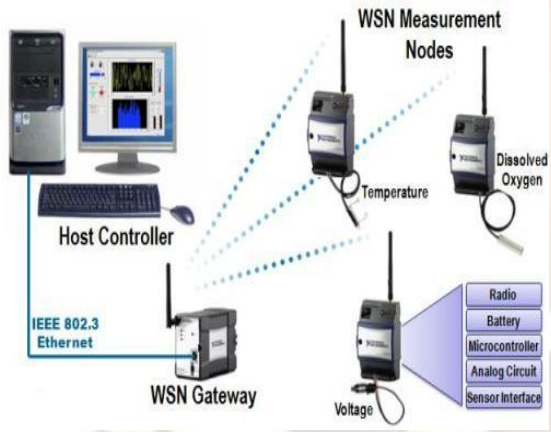

Figure 1: *Common Wireless Sensor Network Architecture*

2. Constraints in Wireless Sensor Networks

A wireless sensor network consists of a large number of sensor nodes which are inherently resource-constrained. These nodes have limited processing capability, very low storage capacity, and constrained communication bandwidth. These limitations are due to limited energy and physical size of the sensor nodes. Due to these constraints, it is difficult to directly employ the conventional security mechanisms in WSNs. In order to optimize the conventional security algorithms for WSNs, it is necessary to be aware about the constraints of sensor nodes [3]. Some of the major constraints of a WSN are listed below. *Energy constraints*: Energy is the biggest constraint for a WSN. In general, energy consumption in sensor nodes can be categorized in three parts: (i) energy for the sensor transducer, (ii) energy for communication among sensor nodes, and (iii) energy for microprocessor computation. The study in [4] found that each bit transmitted in WSNs consumes about as much power as executing 800 to 1000 instructions. Thus, communication is more costly than computation in WSNs. Any message expansion caused by security mechanisms comes at a significant cost. Further, higher security levels in WSNs usually correspond to more energy consumption for cryptographic functions. Thus, WSNs could be divided into different security levels depending on energy cost [5, 6]. *Memory limitations:* A sensor is a tiny device with only a small amount of memory and storage space. Memory is a sensor node usually includes flash memory and RAM. Flash memory is used for storing downloaded application code and RAM is used for storing application programs, sensor data, and intermediate results of computations. There is usually not enough space to run complicated algorithms after loading the OS and application code. In the SmartDust project, for example, TinyOS consumes about 4K bytes of instructions, leaving only 4500 bytes for security and applications [4]. A common sensor type- TelosB- has a 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage [7]. The current security algorithms are therefore, infeasible in these sensors [8].

Unreliable communication*:* Unreliable communication is another serious threat to sensor security. Normally the packet-based routing of sensor networks is based on connectionless protocols and thus inherently unreliable. Packets may get damaged due to channel errors or may get dropped at highly congested nodes. Furthermore, the unreliable wireless communication channel may also lead to damaged or corrupted packets. Higher error rate also mandates robust error handling schemes to be implemented leading to higher overhead. In certain situation even if the channel is reliable, the communication may not be so. This is due to the broadcast nature of wireless communication, as the packets may collide in transit and may need retransmission [1].

Higher latency in communication*:* In a WSN, multi-hop routing, network congestion and processing in the intermediate nodes may lead to higher latency in packet transmission. This makes synchronization very difficult to achieve. The synchronization issues may sometimes be very critical in security as some security mechanisms may rely on critical event reports and cryptographic key distribution [9]. *Unattended operation of networks:* In most cases, the nodes in a WSN are deployed in remote regions and are left unattended. The likelihood that a sensor encounters a physical attack in such an environment is therefore, very high. Remote management of a WSN makes it virtually

impossible to detect physical tampering. This makes security in WSNs a particularly difficult task.

3 SECURITY REQUIREMENTS

The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior. The security requirements in WSNs include:

• Availability, which ensures that the desired network services are available even in the presence of denial-of-service attacks

• Authorization, which ensures that only authorized sensors can be involved in providing information to network services

• 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

• Confidentiality, which ensures that a given message cannot be understood by anyone other than the desired recipients

• Integrity, which ensures that a message sent from one node to another is not modified by malicious intermediate nodes

• No repudiation, which denotes that a node cannot deny sending a message it has previously sent

• Freshness, which implies that the data is recent and ensures that no adversary can replay old messages Moreover, as new sensors are deployed and old sensors fail, we suggest that forward and backward secrecy should also be considered:

• Forward secrecy: a sensor should not be able to read any future messages after it leaves the network.

• Backward secrecy: a joining sensor should not be able to read any previously transmitted message. The security services in WSNs are usually centered on cryptography. However, due to the constraints in WSNs, many already existing secure algorithms are not practical for use.

4. Security Goals

Wireless sensor networks are vulnerable to many attacks because of broadcast nature of transmission medium, resource limitation on sensor nodes and uncontrolled environments where they are left unattended. Similar to other communication systems, WSNs have the following general security goals:

- Confidentiality: protecting secret information from unauthorized entities
- Integrity: ensuring message has not been altered by malicious nodes
- Data Origin Authentication: authenticating the source of message;
-Entity Authentication: authenticating the user / node / base - station is indeed the entity
whom it claims to be
- Access control : restricting access to resources to privileged entities
- Availability: ensuring desired service may be available whenever required

In addition, WSNs have following specific security objects:

- Forward secrecy: preventing a node from decrypting any future secret messages after it leaves the network
- Backward secrecy: preventing a joining node from decrypting any previously transmitted secret message
- Survivability: providing a certain level of service in the presence of failures and/or attacks
- Freshness: ensuring that the data is recent and no adversary can replay old messages
- Scalability: supporting a great number of nodes
-Efficiency: storage, processing and communication limitations on sensor nodes must be considered

5. CHALLENGES

Providing efficient data aggregation while preserving data privacy and integrity is a challenging problem in wireless sensor networks due to the following factors:

1. Trust management in WSN is very challenging. Users in the wireless sensor networks can be very curious to learn others' private information, and the communication is over public accessible wireless links, hence the data collection is vulnerable to attacks which threaten the privacy. Without proper protection of privacy, the communication of privacy-sensitive data over civilian wireless sensor networks is considered impractical.
2. During in-network aggregation, adversaries can easily alter the intermediate aggregation result and make the final aggregation result deviate from the true value greatly. Without protection of data integrity, the data aggregation result is not trustworthy.
3. Data collection over wireless sensor networks does not rely on dedicated infrastructure. In many cases, the number of nodes answering a query is unknown before the data aggregation is conducted.
4. Resource limited portable devices cannot afford heavy computation and communication load.
5. The requirement on accuracy of information collection (i.e., aggregated result) makes the existing randomized privacy-preserving algorithms not suitable. Besides the above mentioned factors, it is very challenging to protect privacy and integrity of data aggregation simultaneously, because usually privacy-preserving schemes disable traffic peer monitoring mechanisms, which reduces the availability of information in a neighborhood to verify data integrity.

6. Security Vulnerabilities in WSNs

Wireless Sensor Networks are vulnerable to various types of attacks. These attacks are mainly of three types [87]: *Attacks on secrecy and authentication*: standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks, and

modification or spoofing of packets. *Attacks on network availability*: attacks on availability of WSN are often referred to as denial-of-service (DoS) attacks. *Stealthy attack against service integrity*: in a stealthy attack, the goal of the attacker is to make the network accept a false data value. For example, an attacker compromises a sensor node and injects a false data value through that sensor node. In these attacks, keeping the sensor network available for its intended use is essential. DoS attacks against WSNs may permit real-world damage to the health and safety of people [11]. The DoS attack usually refers to an adversary's attempt to disrupt, subvert, or destroy a network. However, a DoS attack can be any event that diminishes or eliminates a network's capacity to perform its expected functions [29].

6.1 Denial of Service (DoS) attacks

Wood and Stankovic have defined a DoS attack as an event that diminishes or attempts to reduce a network's capacity to perform its expected function [81]. There are several standard techniques existing in the literature to cope with some of the more common denial of service attacks, although in a broader sense, development of a generic defense mechanism against DoS attacks is still an open problem. Moreover, most of the defense mechanisms require high computational overhead and hence not suitable for resource constrained WSNs. Since DoS attacks in WSNs can sometimes prove very costly, researchers have spent a great deal of effort in identifying various types of such attacks, and devising strategies to defend against them. Some of the important types of DoS attacks in WSNs are discussed below.

6.1.1 Physical layer attacks

The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption [12]**.** As with any radio-based medium, the possibility of jamming is there. In addition, nodes in WSNs may be deployed in hostile or insecure environments where an attacker has the physical access.

Two types of attacks in physical layer are (i) jamming and (ii) tampering.

Jamming: it is a type of attack which interferes with the radio frequencies that the nodes use in a WSN for communication [11,24]. A jamming source may be powerful enough to disrupt the entire network. Even with less powerful jamming sources, an adversary can potentially disrupt communication in the entire network by strategically distributing the jamming sources. Even an intermittent jamming may prove detrimental as the message communication in a WSN may be extremely time-sensitive [11].

Tampering: sensor networks typically operate in outdoor environments. Due to unattended and distributed nature, the nodes in a WSN are highly susceptible to physical attacks **[65**]. The physical attacks may cause irreversible damage to the nodes. The adversary can extract cryptographic keys from the captured node, tamper with its circuitry, modify the program codes or even replace it with a malicious sensor [15]. It has been shown that sensor nodes such as MICA2 motes can be compromised in less than one minute time [14].

6.1.2 Link layer attacks

The link layer is responsible for multiplexing of data-streams, data frame detection, medium access control, and error control [12]. Attacks at this layer include purposefully created collisions, resource exhaustion, and unfairness in allocation.

A collision occurs when two nodes attempt to transmit on the same frequency simultaneously [11]. When packets collide, they are discarded and need to re-transmitted. 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. Repeated collisions can also be used by an attacker to cause resource exhaustion [11]. For example, a naïve link layer implementation may continuously attempt to retransmit the corrupted packets. Unless these retransmissions are detected early, the energy levels of the nodes would be exhausted quickly. Unfairness is a weak form of DoS attack [11]. An attacker may cause unfairness by intermittently using the above link layer attacks. In this case, the adversary causes degradation of real-time applications running on other nodes by intermittently disrupting their frame transmissions.

6.1.3 Network layer attacks

The network layer of WSNs is vulnerable to the different types of attacks such as: (i) spoofed routing information , (ii) selective packet forwarding, (iii) sinkhole, (iv) Sybil, (v) wormhole, (vi) hello flood, (vii) acknowledgment spoofing etc[25, 26, 27]. These attacks are described briefly in the following: *Spoofed routing information*: the most direct attack against a routing protocol is to target the routing information in the network. An attacker may spoof, alter, or replay routing information to disrupt traffic in the network [12]. These disruptions include creation of routing loops, attracting or repelling network traffic from selected nodes, extending or shortening source routes, generating fake error messages, causing network partitioning, and increasing end-to-end latency.

Selective forwarding: in a multi-hop network like a WSN, for message communication all the nodes need to forward messages accurately. An attacker may

compromise a node in such a way that it selectively forwards some messages and drops others [43].

Sinkhole: In a sinkhole attack, an attacker makes a compromised node look more attractive to its neighbors by forging the routing information [13,12,11]. The result is that the neighbor nodes choose the compromised node as the next-hop 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 would flow through the compromised node.

Sybil attack: it is an attack where one node presents more that one identity in a network. It was originally described as an attack intended to defeat the objective of redundancy mechanisms in distributed data storage systems in peer-topeer networks [11]. Newsome et al describe this attack from the perspective of a WSN [13]. In addition to defeating distributed data storage systems, the Sybil attack is also effective against routing algorithms, data aggregation, voting, fair resource allocation, and foiling misbehavior detection. Regardless of the target (voting, routing, aggregation), the Sybil algorithm functions similarly. All of the techniques involve utilizing multiple identities. For instance, in a sensor network voting scheme, the Sybil attack might utilize multiple identities to generate additional "votes". Similarly, to attack the routing protocol, the Sybil attack would rely on a malicious node taking on the identity of multiple nodes, and thus routing multiple paths through a single malicious node.

Wormhole: a wormhole is low latency link between two portions of a network over which an attacker replays network messages [12]. This link may be established either by a single node forwarding messages between two adjacent but otherwise non-neighboring nodes or by a pair of nodes in different parts of the network communicating with each other. The latter case is closely related to sinkhole attack as an attacking node near the base station can provide a one-hop link to that base station via the other attacking node in a distant part of the network.

Hello flood: most of the protocols that use Hello packets make the naïve assumption that receiving such a packet implies that the sender is within the radio range of the receiver. An attacker may use a high-powered transmitter to fool a large number of nodes and make them believe that they are within its neighborhood [12]. Subsequently, the attacker node falsely broadcasts a shorter route to the base station, and all the nodes which received the Hello packets, attempt to transmit to the attacker node. However, these nodes are out of the radio range of the attacker.

Acknowledgment spoofing: some routing algorithms for WSNs require transmission of acknowledgment packets. An attacking node may overhear packet transmissions from its neighboring nodes and spoof the acknowledgments thereby providing false information to the nodes [12]. In this way, the attacker is able to disseminate wrong information about the status of the nodes.

6.1.4 Transport layer attacks

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

Flooding: Whenever a protocol is required to maintain state at either end of a connection, it becomes vulnerable to memory exhaustion through flooding [81]. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored.

De-synchronization: De-synchronization refers to the disruption of an existing connection [81]. An attacker may, for example, repeatedly spoof messages to an end host causing the 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 causing them instead to waste energy attempting to recover from errors which never really exist. The possible DoS attacks and the corresponding countermeasures are listed in **Table 1.**

Table 1. Attacks on WSNs and countermeasures

Layer	Attacks	Defense
Physical	Jamming	Spread-spectrum, riority messages, lower duty cycle,region mapping, modechange
Link	Collision	Error-correction code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network	Spoofed routing information & selective forwarding	Egress filtering, authentication, monitoring
	Sinkhole	Redundancy checking
	Sybil	Authentication, monitoring,redundanc y
	Wormhole	Authentication, probing
	Hello Flood	Authentication, packet leashes by using geographic and temporal info
	Ack. flooding	Authentication, bi-directional link authentication verification
Transpor t	Flooding De-synchronizatio	Client puzzles Authentication

	n	

6.2 Attacks on secrecy and authentication

There are different types of attacks under this category as discussed below.

6.2.1 Node replication attack

In a node replication attack, an attacker attempts to add a node to an existing WSN by replication (i.e. copying) the node identifier of an already existing node in the network [17]. A node replicated and joined in the network in this manner can potentially cause severe disruption in message communication in the WSN by corrupting and forwarding the packets in wrong routes. This may also lead to network partitioning, communication of false sensor readings. In addition, if the attacker gains physical access to the entire network, it is possible for him to copy the cryptographic keys and use these keys for message communication from the replicated node. The attacker can also place the replicated node in strategic locations in the network so that he could easily manipulate a specific segment of the network, possibly causing a network partitioning.

6.2.2 Attacks on privacy

Since WSNs are capable of automatic data collection through efficient and strategic deployment of sensors, these networks are also vulnerable to potential abuse of these vast data sources. Privacy preservation of sensitive data in a WSN is particularly difficult challenge [18]. Moreover, an adversary may gather seemingly innocuous data to derive sensitive information if he knows how to aggregate data collected from multiple sensor nodes. This is analogous to the panda hunter problem, where the hunter can accurately estimate the location of the panda by monitoring the traffic [19].

The privacy preservation in WSNs is even more challenging since these networks make large volumes of information easily available through remote access mechanisms. Since the adversary need not be physically present to carryout the surveillance, the information gathering process can be done anonymously with a very low risk. In addition, remote access allows a single adversary to monitor multiple sites simultaneously [20]. Following are some of the common attacks on sensor data privacy [18,20]:

Eavesdropping and passive monitoring: This is most common and easiest form of attack on data privacy. If the messages are not protected by cryptographic mechanisms, the adversary could easily understand the contents. Packets containing control information in a WSN convey more information than accessible through the location server, Eavesdropping on these messages prove more effective for an adversary.

Traffic analysis: In order to make an effective attack on privacy, eavesdropping should be combined with a traffic analysis. Through an effective analysis of traffic, an adversary can identify some sensor nodes with special roles and activities in a WSN. For example, a sudden increase in message communication between certain nodes signifies that those nodes have some specific activities and events to monitor. Deng et al have demonstrated two types of attacks that can identify the base station in a WSN without even underrating the contents of the packets being analyzed in traffic analysis [21].

Camouflage: An adversary may compromise a sensor node in a WSN and later on use that node to masquerade a normal node in the network. This camouflaged node then may advertise false routing information and attract packets from other nodes for further forwarding. After the packets start arriving at the compromised node, it starts forwarding them to strategic nodes where privacy analysis on the packets may be carried out systematically.

It may be noted from the above discussion that WSNs are vulnerable to a number of attacks at all layers of the TCP/IP protocol stack. However, as pointed out by authors in [22], there may be other types of attacks possible which are not yet identified. Securing a WSN against all these attacks may be a quite challenging task.

7 FUTURE TRENDS

Though significant research in WSNs and mobile computing continues, issues concerning the enablement of seamless and transparent interaction between each domain need to be resolved. A number of issues are now identified. Communication protocol issues: In order for a PDA (Personal Digital Assistants) to communicate with a sensor network, it is necessary that both PDAs and WSNs use the same communication protocol. At present, off the shelf PDAs have the Bluetooth protocol for short range communication provided. Unfortunately, studies of the Bluetooth architecture (Leopold, 2003) showed the unsuitability of such a protocol for wireless sensor networks. On the other hand, although recent advances propose a vast number of protocols tailored to WSNs, the communication compatibility between the two technologies is still an open issue. Ontology issues: Such kinds of issues arise after PDAs and sensors agree which communication protocol to use. In the context of knowledge sharing between PDAs and sensors at the application layer, they should agree with the specification of a conceptualization, also known as an ontology. Although some research propose the study of semantic techniques for wireless sensor networks (Whitehouse, 2006), a comprehensive methodology of PDA/sensor interaction is still an open issue to be addressed. Trust management issues: Requests of m-commerce-

related information from sensors to PDAs and vice versa raises issues of trust management. In fact, sensors should trust the quality of service offered by the PDA protocol. On the other side, PDAs should trust sensors when, for example, product availability or machinery condition are sent to a PDA. While the latter case can be considered as an instance of internet trust management, the former case needs to consider the issue of memory capability constraints of sensors. Procedures for realizing trust management on individual sensors, for example, through intelligent agent technologies, need further research. The big "umbrella" of trust management also includes more specific issues of security. In fact, the multi-hop routing of WSNs together with the relatively simple architecture of sensors pose an inherent risk, as an attacker may only need to compromise one device to compromise the security of the entire network. This concern is amplified in applications like m-commerce where private credentials must be fully safely encoded.

8 CONCLUSIONS

Security is becoming a major concern for energy constrained wireless sensor network because of the broad security-critical applications of WSNs. Thus, security in WSNs has attracted a lot of attention in the recent years. The salient features of WSNs make it very challenging to design strong security protocols while still maintaining low overheads.

In this paper, we introduce sensor networks, its related security problems, threats, risks and characteristics. Network security for WSNs is still a very fruitful research direction to be further explored.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, 2002.

[2] Wireless sensor networks: a survey I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci

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

[4] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D.E. Culler, and K. Pister, "System architecture directions for networked sensors", In *Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems*, New York, ACM Press, 2000, pp. 93-104.

[5] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M.B. Srivastava, "On communication security in wireless ad-hoc sensor networks", In *Proceedings of 11th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02),* 2002, pp. 139-144.

[6] L. Yuan and G. Qu, "Design space exploration for energy-efficient secure sensor networks", In *Proceedings of IEEE International Conference on Application-Specific Systems, Architectures, and Processors*, July 2002, pp. 88-100.

[7] http://www.xbow.com/wireless_home.aspx, 2006.

[8] A. Perrig, R. Szewczyk, V. Wen, D.E. Culler, and J.D. Tygar,"SPINS: Security protocols for sensor networks", *WirelessNetworks*, Vol.8 , No. 5, pp. 521-534, September 2002.

[9] J.A. Stankovic et al, "Real-time communication and coordination in embedded sensor networks", *In Proceedings of the IEEE,* Vol. 91,No. 7, , pp. 1002-1022, July 2003.

[10] E. Shi and A. Perrig, "Designing secure sensor networks", *Wireless Communication Magazine*, Vol. 11, No. 6, pp. 38-43, December 2004

[11] A.D. Wood and J.A. Stankovic, "Denial of service in sensor networks", *IEEE Computer*, Vol. 35, No. 10, pp. 54-62, 2002.

[12] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, May 2003, pp. 113-127.

[13] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses", In *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, pp. 259-268, ACM Press 2004.

[14] C. Hartung, J. Balasalle, and R. Han, "Node compromise in sensor networks: The need for secure systems", Technical Report CU-CS-988-04, Department of Computer Science, University of Colorado at Boulder, 2004.

[15] X. Wang, W. Gu, S. Chellappan, Dong Xuan, and Ten H. Laii, "Search-based physical attacks in sensor networks: Modeling and defense, Technical report, Department of Computer Science and Engineering, Ohio State University, February 2005.

[16] J. Douceur, "The Sybil attack", In *Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02),*February 2002.

[17] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks", In *Proceedings of IEEESymposium on Security and Privacy*, May 2005.

[18] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald, "Privacy-aware location sensor networks", In *Proceedings of the 9th USENIX Workshop on Hot Topics in Operating Systems, (HotOS IX)*, 2003.

[19] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing ", In *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2004.

[20] H. Chan and A. Perrig, "Security and privacy in sensor networks", *IEEE Computer Magazine*, pp. 103-105, 2003.

[21] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis in wireless sensor networks", Technical Report CU-CS-987-04, University of Colorado at Boulder, 2004.

[22] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks", *Communications of ACM* , Vol 47, No. 6, pp. 53-57, 2004

[23] X. Wang, W. Gu, K. Schosek, S. Chellappan, and D. Xuan, "Sensornetwork configuration under physical attacks,", Technical report (OSU-CISRC-7/04-TR45), Department of Computer Science and Engineering, Ohio State University, July 2004.

[24] E. Shi and A. Perrig, "Designing secure sensor networks", *Wireless Communication Magazine*, Vol. 11, No. 6, pp. 38-43, December 2004.

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

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

[27] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315

[28] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks", *In 2nd ACM Conference on Embedded Networked Sensor Systems (SensSys'04),* Baltimore, MD, November 2004, pp. 162-175.

[29] N. Xu, S. Rangwala, K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, and D. Estrin, "A Wireless Sensor Network for Structural Monitoring," *Proceedings of the ACM Conference on Embedded Networked Sensor Systems, Baltimore, MD*, November 2004.

[30] D. Culler, D. Estrin, and M. Srivastava, "Overview of Sensor Networks," *IEEE Computer*,August 2004.