Global Journal of Computer Science and Technology
Volume 11 Issue 16 Version 1.0 September 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Study & Analysis of Security Issues in Wireless Sensor Networks

By Payal Jain, Sameer verma
Maharishi Markandeshwar University, Mullana, Ambala Haryana

Abstract - Wireless sensor networks are successfully used in the conditions of war as well as natural calamities like earthquake, flood, volcanoes etc. Rapid technological advances in the area of micro electro-mechanical systems have spurred the development of small inexpensive sensors capable of intelligent sensing. A significant amount of research has been done in the area of connecting large numbers of these sensors to create robust and scalable Wireless Sensor Networks (WSNs). Proposed applications for WSNs include habitat monitoring, battlefield surveillance, and security systems. WSNs aim to be energy efficient, self-organizing, scalable, and robust. Relatively little work has been done on security issues related to sensor networks. The resource scarcity, ad-hoc deployment, and immense scale of WSNs make secure communication a particularly challenging problem. The primary consideration for sensor networks is energy efficiency, security schemes must balance their security features against the communication and computational overhead required to implement them. This paper will describe the fundamental challenges in the emergent field of sensor network security and the initial approaches to solving them.

Keywords : *Sensor network, Seismic, Message authentication code, Hopping, Spread spectrum etc.*

GJCST Classification : *H.2.8, D.2.9*

Strictly as per the compliance and regulations of:

Study & Analysis of Security Issues in Wireless Sensor Networks

Payal Jain[α], Sameer verma[Ω]

Abstract - Wireless sensor networks are successfully used in the conditions of war as well as natural calamities like earthquake, flood, volcanoes etc. Rapid technological advances in the area of micro electro-mechanical systems have spurred the development of small inexpensive sensors capable of intelligent sensing. A significant amount of research has been done in the area of connecting large numbers of these sensors to create robust and scalable Wireless Sensor Networks (WSNs). Proposed applications for WSNs include habitat monitoring, battlefield surveillance, and security systems. WSNs aim to be energy efficient, self-organizing, scalable, and robust. Relatively little work has been done on security issues related to sensor networks. The resource scarcity, ad-hoc deployment, and immense scale of WSNs make secure communication a particularly challenging problem. The primary consideration for sensor networks is energy efficiency, security schemes must balance their security features against the communication and computational overhead required to implement them. This paper will describe the fundamental challenges in the emergent field of sensor network security and the initial approaches to solving them.

Keywords: Sensor network, Seismic, Message authentication code, Hopping, Spread spectrum etc.

I. Introduction

Wireless Sensor Networks is composed of hundreds or thousands of inexpensive, low-powered sensing devices with limited computational and communication resources, provide a useful interface to the real world with their data acquisition and processing capabilities. Applications include burglar alarms, inventory control, medical monitoring and emergency response monitoring remote or inhospitable habitats, target tracking in battle fields, disaster relief networks early fire detections in forest and environmental monitoring. Sensor devices, also called motes or nodes, typically consist of a sensing unit, a transceiver unit, a processing unit, and a power source unit. Depending on the application, the sensing unit may monitor various types of data including acoustic, seismic, visual, and temperature data. The transceiver unit is a low-power radio capable of short range communication (tens of meters). The processing unit contains memory and a processor with severely limited size and speed. Wireless sensor motes are powered by a battery energy source which is not intended to be recharged. Communication usually consists of source nodes which sense the data and return it to sink nodes over multiple hops. Sink nodes may be ordinary sensor nodes or specialized base stations with greater resources.

In the future thousands to millions of sensor devices will be embedded in almost every aspect of life. The main aim is create an intelligent environment which is capable of collecting massive amounts of information, recognizing significant events automatically and responding appropriately. Sensor networks facilitate "large-scale, real-time data processing in complex environments" [Wood and Stankovic 2002].

Although two of the most security-orientated applications of WANs are military and medical solutions. Sensor networks can be applied to a large number of areas and its applications are continuously growing. Sensor networks are extremely vulnerable against any type of internal or external attacks, due to resource constraints, lack of tamper-resistant packaging, and the nature of its communication channels.

If sensor networks are to attain their potential, however, secure communication techniques must be developed in order to protect the system and its users. WSNs are ideal for detecting chemical, biological, or environmental threats over large areas, but maliciously induced false alarms could completely negate the value of the system. As [1] point out, if security is weak, sensor networks "will only be suitable for limited, controlled environments – falling far short of their promise." The widespread deployment and overall success of sensor networks will be directly related to their security strength.

II. Security Issues and Goals

a) Data confidentiality

Confidentiality means keeping information secret from unauthorized parties. A sensor network should not leak sensor readings to neighboring networks. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality. Most of the proposed protocols use symmetric key encryption methods.

Author α : Lecturer, Department of Information and Technology, Maharishi Markandeshwar College of Engineering Maharishi Markandeshwar University, Mullana, Ambala Haryana.
E-mail : payaljain2006@gmail.comb, Mobile No: 91-9466742552.
Author Ω : Lecturer, Department of Information and Technology, Maharishi Markandeshwar College of Engineering Maharishi Markandeshwar University, Mullana, Ambala, Haryana.
E-mail : sameer. verma1986@gmail.com, Mobile no: +919416320512.

b) Data authenticity

In a sensor network, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. Data authentication prevents unauthorized parties from participating in the network and legitimate nodes should be able to detect messages from unauthorized nodes and reject them. In Data authentication can be achieved through a purely symmetric mechanism: The sender and the receiver share a secret key to compute a message authentication code (MAC) of all communicated data. When a message with a correct MAC arrives, the receiver knows that it must have been sent by the sender. However, authentication for broadcast messages requires stronger trust assumptions on the network nodes.

c) Data integrity

Data integrity ensures the receiver that the received data is not altered in transit by an adversary.

d) Data freshness

Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages. 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. For RAM constrained sensor nodes, this defense becomes problematic for even modestly sized networks. Assuming nodes devote only a small fraction of their RAM for this neighbor 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.

The 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). The 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.

There are two types of freshness identified: 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.

e) Robustness and Survivability

The sensor network should be robust against various security attacks, and if an attack succeeds, its impact should be minimized. The compromise of a single node should not break the security of the entire network.

III. Threats to WSNS

There are a large and increasing number of threats and attacks to which WSNs are susceptible. They can be broadly classified as attacks against the privacy of the network data, denial of service (DOS) attacks, impersonation or replication attacks and physical attacks. A denial of service (DoS) attack aims to deny access to legitimate users to shared services or resources. Attacks can be launched at any point in the network. This implies that certain attacks may be more effective at different layers of the communication protocol,

Table I : sensor network layer and attack

Layer	Attack
Physical Layer	DOS – Jamming, Tampering
Data-link Layer	DOS – Collision, Exhaustion, Unfairness
Network Layer	DOS – Neglect & Greed, Homing, Misdirection (Spoofing), Black Holes, Flooding Sybil Wormhole Attack

a) Physical layer

Attacks at the physical level include radio signal jamming and tampering with physical devices.

i. *Jamming*

Jamming is interference with the radio frequencies used by a device's transceiver. It represents an attack on the availability of a network. Jamming is only different from normal radio propagation in that it is unwanted and disruptive, thus creating a denial-of-service condition **[4]**. The degree of the jamming is determined by physical properties such as the available power, antenna design, obstacles, and height above ground **[4]**. This attack is extremely effective against single frequency networks.

Defense against jamming involves the use of spread-spectrum or frequency hopping techniques. Spread-spectrum communication uses a wider band for radio transmission. Frequency hopping is a type of spread-spectrum in which a pseudorandom sequence is used to change the frequency of transmission. The receiver, who also knows the hopping sequence, can "dehop" the signal to reconstruct the original message **[2]**. Frequency hopping also protects against unintentional jamming, i.e., interference. Spread-

spectrum techniques provide protection in high noise environments in which sensor networks will certainly be deployed. The inherent complexity involved in spread-spectrum systems is particularly costly for sensor motes. Frequency hopping requires greater power and financial cost, two scarce resources in sensor networks.

Prevention of denial of service attacks is a difficult task. Since most sensor networks currently use single frequency communication, [4] have proposed a Jammed Area Mapping (JAM) service which emphasizes detection and adaptation in response to jamming. They assume that only a portion of the network is being jammed and attempt to map this area so it can be avoided. Nodes in the affected area switch to low power mode. Information about jammed areas is passed to the network layer so it can successfully route packets around the dead areas. If spread spectrum techniques cannot be incorporated into motes, then detection algorithms such as JAM may be important in defending against jamming attacks.

ii. *Tampering*

A second problematic issue at the physical layer is the relative ease and potential harm of device tampering. This problem is exacerbated by the large-scale, ad-hoc, pervasive nature of sensor networks. Access to thousands of nodes spread over several kilometers cannot be completely controlled [4]. Attackers may very well have greater physical access to nodes than the network administrator. Nodes may be captured, interrogated, and compromised without difficulty.

One defense involves physically tamper-proofing the devices. Nodes should react to tampering by erasing sensitive cryptographic information [Wood and Stankovic 2002]. However, tamper-resistant packaging increases the cost of the devices, thus reducing their economic viability. The preferred solution is algorithmic: algorithms that reduce the effect a single key compromise has on the security of the entire network. The tampering is "one of the most vexing problems in sensor network security",[5].

b) LInk layer

The link and media access control (MAC) layer handles neighbor-to-neighbor communication and channel arbitration. Like the physical layer, the link layer is particularly susceptible to denial of service attacks.

i. *Collision*

If an adversary can generate a collision of even part of a transmission, he can disrupt the entire packet [[15], Stankovic, and Wagner 2004]. A single bit error will cause a CRC mismatch and possibly require retransmission. In some MAC protocols, a corrupted ACK may cause exponential back-off and unnecessarily increase latency. Although error-correcting codes protect against some level of packet corruption, intentional corruption can occur at levels which are beyond the encoding scheme's ability to correct. The advantage, to the adversary, of this MAC level jamming over physical layer jamming is that much less energy is required to achieve the same effect: preventing devices from successfully transmitting packets.

ii. *Exhaustion*

Another malicious goal is the exhaustion of a network's battery power. In addition to the previous types of attacks, exhaustion may also be induced by an interrogation attack. In the IEEE 802.11-based protocols, for example, Request To Send (RTS) and Clear To Send (CTS) packets are used to reserve bandwidth before data transmission. A compromised node could repeatedly send RTS packets in order to elicit CTS packets from a targeted neighbor, eventually consuming the battery power of both nodes.

iii. *Unfairness*

A more subtle goal of the previously described attacks may be unfairness in the MAC layer [3]. A compromised node can be altered to intermittently attack the network in such a way that induces unfairness in the priorities for granting medium access. This weak form of denial of service might, for example, increase latency so that real-time protocols miss their deadlines, [3]. Another form of this attack could target one particular flow of data in order to suppress detection of some event. The use of small frames which prevent a node from capturing the channel for a long period of time has been proposed as a defense against this sort of attack [1].

c) Network Layer

The network layer is responsible for routing packets across multiple nodes. Due to the ad-hoc nature of sensor networks, every node must assume routing responsibilities. WSNs are particularly vulnerable to routing attacks because every node is essentially a router. [3] have identified a variety of routing attacks and have shown them to be effective against every major sensor network routing protocol. Their classifications of attacks are summarized below and are followed by a general discussion of secure routing techniques.

i. *False Routing Information*

The most direct attack on routing is to spoof, alter, or replay routing information. This false information may allow adversaries to create routing loops, attract or repel traffic, shorten or extend route lengths, increase latency, and even partition the network [3]. Clearly, the falsification of routing information can cripple a network. The standard solution is to require authentication for routing information, i.e., routers only accept routing information from valid routers. Not surprisingly, authentication is an important element in the security systems proposed for sensor networks.

ii. *Selective Forwarding*

Selective forwarding is a more subtle attack in which some packets are correctly forwarded but others are silently dropped. A compromised node could be configured to drop all packets, creating a so-called black hole. Since the network is capable of handling node failure it may conclude that the compromised node has failed and find another route. If the compromised node selectively forwards packets, the neighboring nodes will believe that the malicious node is still functioning correctly and continue to route packets to the node. This vulnerability is due to the assumption that nodes will faithfully forward received messages. If an attacker can get in the path of a desired data flow, he can selectively drop packets from that flow.

iii. *Sinkhole Attack*

The adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. For instance, an adversary could spoof or replay an advertisement for an extremely high quality route to a base station. Due to either the real or imagined high quality route through the compromised node, it is likely each neighboring node of the adversary will forward packets destined for a base station through the adversary, and also propagate the attractiveness of the route to its neighbors. Effectively, the adversary creates a large "*sphere of influence*", attracting all traffic destined for a base station from nodes several hops away from the compromised node.

iv. *The Sybil Attack*

In a Sybil attack, a single node presents multiple identities to other nodes in the network. They pose a significant threat to geographic routing protocols, where location aware routing requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network. However, an insider cannot be prevented from participating in the network, but (s)he should only be able to do so using the identities of the nodes (s)he has compromised. Using globally shared keys allows an insider to masquerade as any (possibly even nonexistent) node. Public key cryptography can prevent such an insider attack, but it is too expensive to be used in the resource constrained sensor networks. One solution is to have every node share a unique symmetric key with a trusted base station. Two nodes can then use a Needham-Schroeder like protocol to verify each other's identity and establish a shared key. A pair of neighboring nodes can use the resulting key to implement an authenticated, encrypted link between them. An example of a protocol which uses such a scheme is LEAP, which supports the establishment of four types of keys.

v. *Wormhole Attack*

The wormhole attack is used to convince two possibly distant nodes that they are neighbors so that the attacker can place himself on the route between them. Basically, the adversary tunnels messages from one part of the network to another through an out-of-bound channel available only to the attacker. Wormholes typically involve two colluding nodes. This sort of attack is likely to be used in combination with selective forwarding or eavesdropping.

vi. *Hello Flood Attack*

The Hello flood attack, a novel attack proposed by Karlof and Wagner, exploits routing protocols that require periodic HELLO packets be transmitted to announce the presence of a node. Nodes which receive a HELLO packet assume they are within radio range of the sender, i.e., the sender is a neighboring node. This assumption may be false in the case of a laptop-class attacker. An adversary with a powerful transmitter may be able to transmit a single HELLO packet to every node in the network and convince every node that it is a one-hop neighbor. As a result, the network is left in a state of confusion. If, for example, the attacker advertises a very quick route to a base station in the HELLO packet, many non-neighbor nodes will attempt to route packets through the malicious node. In actuality, however, they will be sending packets into oblivion. [3] point out that this attack is actually a "one-way, broadcast wormhole." The simplest solution for this attack is to verify the bidirectionality of a link before acting on its information. Essentially, routing messages from one-way links are ignored. Karlof and Wagner propose an identity verification protocol to defend against the HELLO flood attack.

vii. *Acknowledgement Spoofing*

The last routing attack [3] identify is the acknowledgement spoofing attack. Several routing protocols rely on link layer acknowledgements for determining next-hop reliability. If an adversary can respond for weak or dead nodes, he can deceive the sender about the strength of the link and effectively mount a selective forwarding attack. The artificial reinforcement allows the attacker to manipulate the routing through the weak or dead node.

There have been several approaches to defend against network layer attacks. Authentication and encryption are a first step, but more proactive techniques such as monitoring, probing, and transmitting redundant packets have also been suggested. Secure routing methods protect against some of previous attacks. Proposed techniques are described below.

viii. *Authentication & Encryption*

Link layer authentication and encryption protect against most outsider attacks on a sensor network routing protocol. Even a simple scheme which uses a globally shared key will prevent unauthorized nodes from joining the topology of the network. In addition to preventing selective forwarding and sinkhole attacks, authentication and encryption also make the Sybil attack impossible because nodes will not accept even one identity from the malicious node **[3]**. SPINS and TinySec are two proposed solutions for link level encryption and authentication. They are discussed in greater detail in the next section.

ix. *Monitoring*

A more active strategy for secure routing is for nodes to monitor their neighbors and watch for suspicious behavior **[1].** In this approach, nodes act as "watchdogs" to monitor the next hop transmission of the packet. In the event that misbehavior is detected, nodes will update routing information to avoid the compromised node.

x. *Probing*

Another proactive defense against malicious routers is probing **[1].** This method periodically sends probing packets across the network to detect blackout regions. Since geographic routing protocols have knowledge of the physical topology of the network, probing is especially well-suited to their use. Probes must appear to be normal traffic, however, so that compromised nodes do not intentionally route them correctly in order to escape detection.

xi. *Redundancy*

Redundancy is another strategy for secure routing [**1**]. An inelegant approach, redundancy simply transmits a packet multiple times over different routes. Hopefully, at least one route is uncompromised and will correctly deliver the message to the destination. Despite its inefficiency, this method does increase the difficulty for an attacker to stop a data flow.

IV. Conclusion

While the majority of the research in sensor networks has focused on making them feasible and useful, a few researchers have proposed solutions to the security issues discussed previously. Sensor network security mechanisms can be divided into two categories: communication protocols and key management architectures. Communication protocols deal with the cryptographic algorithms used to achieve availability, confidentiality, integrity, and authentication. Key management architectures handle the complexities of creating and distributing keys used by communication protocols.

References References Referencias

1. A.D. Wood and J.A. Stankovik, (2002) "Denial of service in Sensor Networks", Computer, Vol. 35, No. 10, 2002, pp 54-62.
2. H. Chen, Q-A. Zeng, and D. P. Agrawal, "A Novel Optimal Channel Partitioning Algorithm for Integrated Wireless and Mobile Networks," accepted for the Journal of Mobile Communication, Computation and Information.
3. Karlof and Wagner, Secure Routing in Wireless Sensor Networks, "Attacks and Countermeasures", (SNPA 2003), pages 113-127, May-2003.
4. A.Wood, J. Stankovik, S.Son, "Jam : A mapping service for jammed regionsnin sensor networks, RTTS, Mexico, Dec, 2003.
5. Adrian Perrig, John Stankovik and David Wagner (2004), "Security in wireless Sensor Networks", Communication. ACM, 47(6): 53-57.

This page is intentionally left blank