A Comparative Study of Attacks, Security Mechanisms, Preventive Measures, and Challenges in Wireless Sensor Networks

Kamaljit I Lakhtaria
Sir Padampat Singhania University, India

INTRODUCTION

Research on Wireless Sensor Networks (WSNs) initiated during the Distributed Sensor Networks (DSN) program at the Defense Advanced Research Projects Agency (DARPA) at around 1980. During this tenure the ARPANET (Advanced Research Projects Agency Network) had been functional with more than 200 Universities and Research Institutes (Chong & Kumar, 2003). DSNs were assumed to have many spatially distributed low-cost sensing nodes that collaborated with each other but operated autonomously, with information being routed to whichever node was best able to use the information. The processing was mainly performed on minicomputers and the Ethernet was used for DSNs. The Potential of Sensor Network was identified in a Distributed Sensor Nets workshop in 1978 organized by DARPA (Wang & Balasingham, 2010).

DARPA launched research program called SensIT (Kumar & Shepherd, 2001) which provided the present sensor networks with new capabilities such as ad hoc networking, dynamic querying and tasking, reprogramming and multitasking. The IEEE defined ZigBee (IEEE 802.15.4) standard for low expense and high capabilities sensor network with having low data rates. The ZigBee standard specifies a suite of high level communication protocols for WSNs.

BACKGROUND

WSNs are primarily designed for real time collection and analysis of low level data in hostile environments. WSNs are suitable for substantial amount of surveillance and monitoring. WSNs have been widely deployed in broad spectrum of civil and military applications. In future there would be millions of small sensors which are forming self organizing wireless networks. Security is one of the major challenges for creating WSNs a reality. Serious privacy questions arise if third parties can read or tamper with sensor data. Modification of information is easily possible because of the nature of the wireless channels and uncontrolled node environment. Security attacks on information flow can be widespread. An opponent can use natural impairments to modify information and also render the information unavailable.

WSNs continue to grow and needs more effective security mechanism for long survival in any system. As sensor networks may interact with sensitive data and/or operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the system design. However, due to inherent resource and computing constraints, security in sensor networks poses different challenges than traditional network or computer security.

Majority of the current secure algorithms designed for powerful workstations are not suitable for sensors for example, the working memory of a sensor node is insufficient to even hold the variables of sufficient length to ensure security that are required in asymmetric cryptographic algorithms (Othman et al., 2013). Ultimately WSN security requirement is to provide confidentiality, integrity, authenticity and availability of all messages in the presence of resourceful adversaries. To provide secure communications for the WSNs, all messages must be encrypted and authenticated.

SECURITY GOALS FOR WIRELESS SENSOR NETWORKS

A wireless sensor network is an ad hoc network, which requires every sensor node be independent and flexible

DOI: 10.4018/978-1-4666-5888-2.ch601

enough to be self-organizing and self-healing according to different situations (Chan & Castelluccia, 2011). This inherent feature brings a great challenge to wireless sensor network security. Security goals for WSNs can be classified as primary and secondary (Table 1).

Table 1. Security Goals for WSNs

Primary Goals	Secondary Goals
Data Confidentiality	Data Freshness
Data Integrity	Time Synchronization
Data Authentication	Secure Localization
Data Availability	Self-Organization

Primary Goals

Data Confidentiality

Data Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remain confidential. A sensor network should not leak sensor readings to neighboring networks. In many applications (e.g. key distribution) nodes communicate highly sensitive data. 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. Network administrator can set up secure channels between nodes and base stations and later bootstrap other secure channels as necessary (Liu et al., 2013).

Data Integrity

For WSNs data integrity ensures the receiver that the received data is not altered in transit by an adversary. Data integrity is achieved through data authentication; this is vital property of WSN security. Data integrity in sensor networks ensures reliability of data and refers to ability to confirm message & that it has not been tampered with, altered or changed (Yoon et al., 2013). Even if the network has confidentiality measures, It may be possible that data integrity has been compromised by alterations. The integrity of the network will be in trouble when any malicious node present in the network injects false data. Unstable conditions due to wireless channel cause damage or loss of data

Data Authentication

In both formative and functioning phase, wireless network sensors authentication is necessary for administrative tasks like network reprogramming or controlling sensor node duty cycle. An adversary can easily inject messages; the receiver needs to make sure that the data used in any decision-making process originates from the correct source (Shi et al., 2013).

Data authentication verifies the identity of the senders and receivers; it is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys. Due to the wireless nature of the media and the unattended nature of sensor networks, it is extremely challenging to ensure authentication.

Data Availability

The need of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network. Failure of the base station or cluster leader's availability will eventually threaten the entire sensor network (Ozdemir & Xiao, 2009). If no energy exists, the data will no longer be available; as communication increases so too does the chance of incurring a communication conflict. A single point failure will greatly threatens the availability of the network. Thus availability is of primary importance for maintaining an operational network.

Secondary Goals

Data Freshness

As all sensor networks stream some forms of time varying measurements. Therefore guarantying confidentiality and authentication is not the sole purpose, ensuring the freshness of each message is also very important. Informally, data freshness implies that the data is recent, and it ensures that no adversary replayed old stored messages (Jose et. al., 2013). There are two types of freshness: weak freshness, which provides partial message ordering, but carries no delay information, and strong freshness, which provides a total order on a request-response pair, and allows for delay estimation. Weak freshness is required by sensor measurements, while strong freshness is useful for time synchronization within the network.