Security Challenges and Efficient Security Solutions for Ad-Hoc Wireless Sensor Network

Manju Kumari[1]
Lecturer,
Polytechnic College, Bikaner
manjusunia08@gmail.com

Abstract: Wireless sensor networks sense the information, process them locally and communicate it to the outside world via satellite or Internet. Wireless Sensor Networks (WSNs) use tiny, inexpensive

sensor nodes with several distinguishing characteristics: they have very low processing power and radio ranges, permit very low energy consumption and perform limited and specific

monitoring and sensing functions. Wireless sensor networks (WSN) are widely used for applications such as environment monitoring, habitat monitoring, forest fire control, border surveillance and health monitoring due to their capability of establishing communications among peer nodes in a self-organizing and adapting manner, without any infrastructure. Sensor networks use radio frequencies as a communication medium, which is vulnerable of all active and passive attacks from adversaries. The sensor net-work must be protected to avoid attacks from external parties. This protection is provided by the security primitives.

This paper mainly concerns with problems associated in developing security protocols for wireless sensor networks, their requirements, and different types of attacks on sensor networks.

This paper describes secure solutions for collecting and processing data in Wireless Sensor Networks (WSNs). Adequate security

capabilities for medium and large scale WSNs are a hard but necessary goal to achieve to prepare these networks for the market. The paper also includes security and reliability challenges and also security solution for WSNs.

Keywords- *central processing centers (CPCs), MAC (Message Authentication Code).*

*****

I. Introduction

A sensor network is a network of such sensors that can (a) sense specified parameters relating to their environment, (b) process them either locally or in a distributed manner, and (c) communicate the processed information to Base station which in turns one or more central processing centers (CPCs). The CPCs are expected to analyze the information and respond suitably. Sensor networks are an emerging wireless computing technology for monitoring a

Variety of environments in scientific, military, medical, and other critical applications. Such networks comprise collections of wireless micro-sensors.

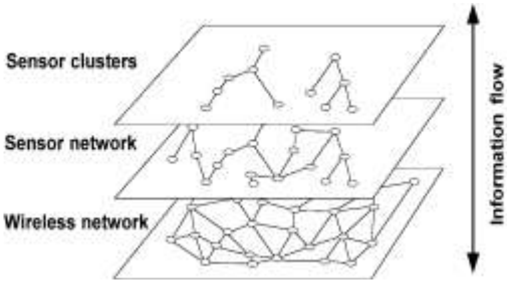

Fig1: layers in a wireless sensor network.

These sensors are deployed within a predetermined geographical area to self-organize into an ad hoc wireless network to gather and aggregate data. These sensor nodes are characterized by severely limited resources in terms of memory size, computational power, and bandwidth, and even energy. The ad hoc nature of sensor networks makes them particularly vulnerable to interception, intrusion and service deprivation.

Without encryption and integrity checking, the content of a broadcast message is subject to eavesdropping and tampering. Without authentication, an attacker can easily inject malicious code or false data into the network by either subverting a good node or inserting a bad node. Still worse, the attacker can inflict sleep torture on an energy constrained node by engaging it in unnecessary communication work to quickly drain its battery power. The effects of these attacks can be dramatic: a compromised node in an airport surveillance system may pose serious threats to flight safety.

The implication of security in sensor networks is mainly quadruple, i.e. confidentiality (privacy of communication), authenticity (trustworthiness of a source), integrity (non-modification in transit), and freshness (no replay able messages)

II. Security Challenges in fixed and Ad Hoc Sensor Networks

Providing adequate security measures for ad hoc networks is a challenging task.
1. Wireless communications are easy to intercept and difficult to contain.
2. In many situations the nodes may be left unattended in a hostile environment.
3. The dynamic topology and the absence of a supporting infrastructure render most of the existing cryptographic protocols useless as they were not developed for this dynamic environment
4. Many wireless nodes will have a limited energy resource for example battery, solar panel etc.
5. Security mechanisms should be scalable to handle such a large network.

III. Performance issue for wireless sensor networks

There are certain critical features that can determine the efficiency and effectiveness of an ad hoc network.

- Network join time: the time required for an entering node or group of nodes to become integrated into the ad hoc network.
- Network depart time: the time required for the network to recognize the loss of one or more nodes, and reorganize itself to route around the departed nodes.
- Network recovery time: the time required for a collapsed portion of the network, due to traffic overload or node failures, to become functional again once the load is reduced or the nodes become operational.
- Memory requirement: the storage space requirements in bytes, including routing tables and other management tables.
- Network scalability: the number of nodes that the ad hoc network can scale to and reliably preserve communication.
- Knowledge of nodal locations: Does the routing algorithm require local or global knowledge of the network?
- Effect of topology changes: Does the routing algorithm need complete restructuring or only incremental updates?
- Power consciousness: Does the network employ routing mechanisms that consider the remaining battery life of a node?
- Single or multichannel: Does the routing algorithm utilize a separate control channel? In some applications, multichannel execution may make the network vulnerable to countermeasures.
- QoS routing and handling of priority messages: Does the routing algorithm support priority messaging and reduction of latency for delay sensitive real-time traffic? Can the network send priority messages/voice even when it is overloaded with routine traffic levels?
- Real-time voice and video services: Can the network support simultaneous real-time multicast voice or video while supporting traffic loads associated with situation awareness, and other routine services?

IV. Security Goals

4.1 Data Confidentiality

Data confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first. In sensor networks, the confidentiality relates to the following:
• A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.
• In many applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.
• Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

4.4 Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data Integrity ensures that any received data has not been altered in transit.

4.2 Availability

Adjusting the traditional encryption algorithms to fit within the wireless sensor network is not free, and will introduce some extra costs. Some approaches choose to modify the code to reuse as much code as possible. Some approaches try to make use of additional communication to achieve the same goal. What's more, some approaches force strict limitations on the data access, or propose an unsuitable scheme (such as a central point scheme) in order to simplify the algorithm. But all these approaches weaken the availability of a sensor and sensor network for the following reasons:

• Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.

•Additional communication also consumes more energy. What's more, as communication increases so too does the chance of incurring a communication conflict.

• A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network.

The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network.

4.3 Authentication

An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). From the above, we can see that message authentication is important for many applications in sensor networks. Informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

4.4 Time Synchronization

Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc. The authors propose a set of secure synchronization protocols for sender-receiver (pair wise), multihop sender-receiver (for use when the pair of nodes are not within single-hop range), and group synchronization.

V. Security solution for Confidentiality, Integrity, and Authenticity

Data can be encrypted to support the confidentiality. To support data integrity and authenticity, the sender can compute the MAC (Message Authentication Code) on the message to be transmitted using a keyed one-way hash function. Upon receiving the message, the receiver can verify the MAC by applying the publicly known one-way hash function to the received data using the key. If the verification is successful, the receiver knows that the message has not been altered during the transit and the message is actually sent by the sender. This is because only the sender and receiver share the key unless the key is exposed to a third party. Replay attacks, in which an adversary replays old messages, can also be avoided by including the counter value (or sequence number) when the sender computes the MAC. SPINS and TinySec can support message confidentiality, integrity, and authenticity in WSNs. µTESLA can support authenticated broadcast in which only the base station can securely broadcast legitimate messages. Notably, most existing work including are based on the secret key system in which the sender and receiver share a secret key. Although a public key system simplifies the difficult task of key distribution, it is several orders of magnitude more expensive than a secret key system in terms of computational complexity. For example, ecTinyOS takes several minutes to run in the worst case. Also, end-to-end encryption is often ineffective due to a strong need for in-network data processing prevalent in WSNs. The simplest approach for encryption, message authentication, and in-network data processing is using a network-wide global key. However, this

Approach could be dangerous, because an adversary can get access to the entire network by compromising a single node. Better solutions involve the use of pair-wise shared keys between neighbors and/or cluster-based shared keys. To this end, many approaches for key distribution in WSNs are developed to support link-layer secret key solutions.

VI. Conclusion

In this paper, we introduce sensor networks,

its related security challenges in fixed and ad-hoc network, performance issue for wireless sensor network and security solution for wireless sensor network. In this paper we specify different security challenges and its solution like data confidentiality, data integrity, availability and time synchronization and a brief introduction toSPINS, TinySec and LEAP.

References

[1] Adrian Perrig, Ran Canetti, J. D. Tygar, Dawn Xiaodong Song (2000): "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," IEEE Symposium on Security and Privacy, May 2000.

[2] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler (2001): "SPINS: Security Protocols for Sensor Networks," Proceedings of Seventh Annual International Conference on Mobile Computing and Networks MOBICOM 2001, July 2001.

[3] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler (2002): "SPINS: Security Protocols for Sensor Networks," Wireless Networks, Vol.8, 521-534, 2002.

[4] Kris S. J. Pister, Joe M. Kahn, Bernhard E. Boser (1999): "Smart Dust: Wireless Networks of Millimeter-Scale Sensor Nodes," Highlight Article in 1999 Electronics Research Laboratory Research Summary, 1999.

[5] Sasha Slijepcevic, Miodrag Potkonjak, Vlasios Tsiatsis, Scott Zimbeck, Mani B. Srivastava (2002): "On Communication Security in Wireless Ad-Hoc Sensor Networks," Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), 139-144, 2002.

[6] Jeffery Undercoffer, Sasikanth Avancha, Anupam Joshi, John Pinkston (2002): "Security for Sensor Networks," CADIP Research Symposium, 2002