RESEARCH ARTICLE OPEN ACCESS

Protocols for Wireless Sensor Networks and Its Security

Dr. Adil Jamil Zaru
Ph.D. in Computer Science and Engineering

ABSTRACT
This paper proposes a protocol for Wireless Sensor Networks and its security which are characterized by severely constrained computational and energy resources, and an ad hoc operational environment. The paper first introduces sensor networks, and discusses security issues and goals along with security problems, threats, and risks in sensor networks. It describes crippling attacks against all of them and suggests countermeasures and design considerations. It gives a brief introduction of proposed security protocol SPINS whose building blocks are SNEP and µTESLA which overcome all the important security threats and problems and achieves security goals like data confidentiality, freshness, authentication in order to provide a secure Wireless Sensor Network.

Keywords: Wireless Sensor Network, Security, Routing, Key Management

I. INTRODUCTION

1.1.Wireless Sensor Networks are new type of networked systems characterized by severely constrained computational and energy resources. These networks will consist of hundreds or thousands of self-organizing, low power, low cost wireless nodes.

Sensor networks often have one or more points of centralized control called base stations. A base station (sink) is typically a gateway to another network, a powerful data processing or storage center, or an access point for human interface which are used as a nexus to disseminate control information into the network or extract data from it. They have enough battery power to surpass the lifetime of all sensor nodes, sufficient memory to store cryptographic keys, stronger processors, and means for communicating with outside networks. The sensor nodes establish a routing forest, with a base station at the root of every tree.

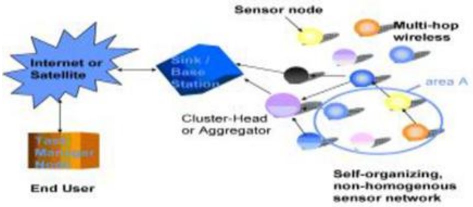
Base stations are many orders of magnitude more powerful than sensor nodes.

1.2. Applications for WSNs are many and varied. They are used in commercial and

industrial applications to monitor data that would be difficult or expensive to monitor using wired sensors

. Some of the typical applications are:

a) Habitat monitoring
b) Environmental monitoring.
c) Inventory tracking
d) Medical monitoring
e) Process Monitoring
f) Acoustic detection
g) Seismic Detection
h) Military surveillance



II. SECURITY ISSUES AND GOALS:

Sensor networks are used in a number of domains that handle sensitive information. Due to this, there are many considerations that should be investigated and are related with protecting sensitive information traveling between nodes from been disclosure to unauthorized parties.

2.1 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 the two-party communication, data authentication can be achieved through a purely symmetric mechanism where, 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 the sender must have sent it. Authentication requires stronger trust assumptions on the network nodes.

2.2 Confidentiality:

Confidentiality means keeping information secret from unauthorized parties. 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. Since public-key cryptography is too expensive to be used in the resource constrained sensor networks, most of the proposed protocols use symmetric key encryption methods.

2.3 Integrity:

Moving on to the integrity objective, there is the danger that information could be altered when exchanged over insecure networks. Lack of integrity could result in many problems since the consequences of using inaccurate information could be disastrous, for example for the healthcare sector where lives are endangered. Integrity controls must be implemented to ensure that information will not be altered in any unexpected way there is urgent need to make sure that information is traveling from one end to the other without being intercepted and modified in the process.

2.4 Secure Management:

Management is required in every system that is constituted from multi components and handles sensitive information. In the case of sensor networks, we need secure management on base station level; since sensor nodes communication ends up at the base station, issues like key distribution to sensor nodes in order to establish encryption and routing information need secure management. Furthermore, clustering requires secure management as well, since each group of nodes may include a large number of nodes that need to be authenticated with each other and exchange data in a secure manner. In addition, clustering in each sensor network can change dynamically and rapidly. Therefore, secure protocols for group management are required for adding and removing members, and authenticating data from groups of nodes.

2.5 Availability:

Availability ensures that services and information can be accessed at the time that they are required. In sensor networks there are many risks that could result in loss of availability such as sensor node capturing and denial of service attacks. Lack of availability may affect the operation of many critical real time applications like those in the healthcare sector that require a 24 * 7 operation that could even result in the loss of life. Therefore, it is critical to ensure

2.6 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. SECURITY THREATS

Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected.

3.1 Passive Information Gathering:

An intruder with an appropriately powerful receiver and well-designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields. To minimize the threats of passive information gathering, strong encryption techniques needs to be used.

3.2 Subversion of a Node:

A particular sensor might be captured, and information stored on it (such as the key) might be obtained by an adversary. If a node has been compromised then how to exclude that node, and that node only, from the sensor network is at issue some network protocol applications are designed to do so.

3.3 False Node and malicious data:

An intruder might add a node to the system that feeds false data or prevents the passage of true data. Such messages also consume the scarce energy resources of the nodes. This type of attack is called “sleep deprivation torture”. Insertion of malicious code is one of the most dangerous attacks that can occur. Malicious code injected in the network could spread to all nodes, potentially destroying the whole network, or even worse, taking over the network on behalf of an adversary. A seized sensor network can either send false observations about the environment to a legitimate user or send observations about the monitored area to a malicious user. By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc. Strong authentication techniques can prevent an adversary from impersonating as a valid node in the sensor network.

IV. SECURITY PROTOCOL SPINS

SPINS is a suite of security building blocks proposed by Perig et all. It is optimized for resource constrained environments and wireless communication.

The building blocks of SPINS are:

SNEP which provides data confidentiality, two-party data authentication, and data freshness

μTESLA which provides authenticated broadcast for severely resource-constrained environments

4.1 SNEP: security network encryption protocol:

SNEP uses encryption to achieve confidentiality and message authentication code (MAC) to achieve two-party authentication and data integrity. This ensures that an eavesdropper has no information about the plaintext, even if it sees multiple encryptions of the same plaintext .The basic technique to achieve this is randomization i.e. before encrypting the message with a chaining encryption function the sender precedes the message with a random bit string .This prevents the attacker from inferring the plaintext of encrypted messages if it knows plaintext-cipher text pairs encrypted with the same key. To avoid adding the additional transmission overhead of these extra bits, SNEP uses a shared counter between the sender and the receiver for the block cipher in counter mode (CTR). The communicating parties share the counter and increment it after each block.

SNEP offers the following properties:

4.1.1 Semantic security: Since the counter value is incremented after each message, the same message is encrypted differently each time. The counter value is long enough that it never repeats within the lifetime of the node.

4.1.2 Replay protection: The counter value in the MAC prevents replaying old messages. If the counter were not present in the MAC, an adversary could easily replay messages.

4.1.3 Data freshness: If the message verified correctly, a receiver knows that the message must have been sent after the previous message it received correctly (that had a lower counter value). This enforces a message ordering and yields weak freshness.

4.2 □TESLA:

Most of the proposals for authenticated broadcast are impractical for sensor networks, as they rely on asymmetric digital signatures for the authentication. The TESLA protocol provides efficient authenticated broadcast. μTESLA uses symmetric authentication but introduces asymmetry through a delayed disclosure of the symmetric keys, which results in an efficient broadcast authentication scheme.

μTESLA requires the base station and nodes to be loosely time synchronized, and each node knows an upper bound on the maximum synchronization error. While sending an authenticated packet, the base station simply computes an AC on the packet with a key that will be secret at that point of time. When a node receives a packet, it can verify the corresponding MAC key based on its loosely synchronized clock, its maximum synchronization error, and the time schedule at which keys are disclosed. Initially receiver node stores the packet in a buffer assuming the packet was disclosed by a base station .As MAC key is known only by the base station it broadcasts verification key to all receivers during the time of key discloser based on which receiver node can easily verify the correctness of the key. If the key is correct, the node can now use it to authenticate the packet stored in its buffer. Each node can easily perform time synchronization and retrieve an authenticated key of the key chain for the commitment in a secure and authenticated manner, using the SNEP building block.

The keys are calculated using a one-way hash function (F) and are disclosed in the reverse order that they are generated. Once a node receives a key, it can apply the same hash function to calculate the keys for previous epochs and decrypt buffered packets. Figure 1 illustrates this process.

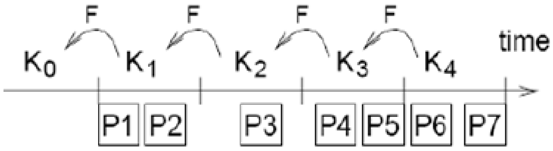


Figure 1: μTELSA key disclosure and computation. Each hash mark denotes an epoch. P1, P2…P7 represent packets

V. CONCLUSION

Thus, Combination of these two building blocks SNEP and μTESLA can fulfill the security goals and threats in the wireless sensor networks which are the most important challenges faced by current wireless communicational systems. Therefore, we conclude that security in Wireless Sensor Networks can be achieved by implementing our proposed security protocol SPINS.

REFERENCES

[1]. Agrawal, Dharma P.; Qing-An Zeng. 2003. Introduction to Wireless and Mobile Systems. Brooks/Cole – Thompson, Pacific Grove, CA.

[2]. Chan, H., A. Perrig, and D. Song. Random Key Predistribution Schemes for Sensor Networks. IEEE Symposium on Security and Privacy (SP)

[3]. M. chen, W. Cui, and V. Wen. Security and Deployment Issues in a Sensor Network (http://www.cs.berkeley.edu/~wdc/classes/cs294-1-report.pdf), 2000.

[4]. A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar. SPINS: Security Protocols for Sensor Networks. In Seventh Annual ACM International Conference on Mobile Computing and Networks (MobiCom 2001), July 2001.

[5]. A. Perrig, R. Canetti, D. Song and J.D. Tygar. Efficient and secure source authentication for multicast. Network and Distributed System Security Symposium (NDSS). 2001.

[6]. A. Fiat and M. Naor. Broadcast encryption. Advances in Cryptology - CRYPTO'93, volume 773 of Lecture Notes in Computer Science, 1994.