
Submitted by

ISMAIL BUTUN

Department of Electrical Engineering
University of South Florida

A report submitted in partial fulfillment of the requirements for the course
EEL 6935 – Wireless Network Architectures and Protocols
(Instructor: Prof. Ravi SANKAR)

Spring-2008

Ismail Butun

Department of Electrical Engineering at USF, Email: ibutun@mail.usf.edu

Abstract—Wireless sensor networks are new extension area for wireless technology in which physical environment monitoring and sensing is achieved. Hence those sensors have limited computational and power capacity, they set up network as an ad-hoc manner. The mentioned paper [23] issues the communication security aspects of those networks. Owing to the lack of resources brings the need of customized security measures. The authors classify the data flowing through the sensor networks, and identify the security threats regarding to that data classification. They propose a security scheme, where they issue different techniques for different types of data. They claim that their multi-step security scheme manages the limited resources efficiently, which is essential for wireless sensor network architecture.


I. INTRODUCTION

Wireless sensor networks are new extension area for wireless technology, a combination of both wireless communications and integrated computing technologies, in which physical environment monitoring and sensing is achieved.

Sensor nodes are low energy consumption devices equipped with sensors. They consist of DSP circuits, microcontrollers and wireless transiver. Their mission is to convert some real physical environment data to intended data format. As a result the data belonging to physical world are used for computing and again these data are used to conclude a decision where the physical world may be affected through actuators. Hundred or more of those sensor nodes come together to build up a Sensor Network and used for monitoring remote locations, target tracking in battlefields, disaster relief networks, early fire warning in forests and environmental monitoring.

Till the year of paper publishing, the main focus of the researchers was on network protocols, distributed databases and power efficiency of the sensor networks excluding the security side. In some applications security is as important as the other issues. Furthermore some applications require more attention on security such as battlefield applications. The limited energy and computational sources differs sensor networks from the others. In the design of security network security those differences must be considered.

The authors [23] state their contribution as:

- Evaluation of communication security threats of sensor networks
- Different security measures for data according to their sensitivity level.
- Local protection schemes.

As stated in [18], data items have to be protected to a degree regarding to their value. In their architecture, authors propose a communication security scheme, differentiating between three types of data sent through the network:

1. Mobile code
2. Sensor nodes locations
3. Application specific data

According to this categorization, they specify the main security threats and according security mechanisms:

- If a faulty manufactured sensor node inserted in a sensor network, it can affect the network flow unpredictably
- Requesting sensor mode locations can ease the work of an attacker to discover the locations of the nodes
- Securing the application specific data is dependent on the security requirements of peculiar application.

The author’s aim was to minimize the energy consumption for security. They offer several layered architecture according to required data protection.

II. SENSOR NETWORK ARCHITECTURE

The aspects of the sensor network architecture that affect the design of the security scheme are: localized algorithms, local communication broadcast model and mobile code.
A. Localized Algorithms

Sensor networks have a unique feature in which limited power is provided to sensor nodes. As a result, efficient power consumption becomes a fundamental design issue. Hence communication between nodes is the main power consumption way, and the main target of the overall system must be to minimize the network traffic load while achieving a specific task. In the authors’ SensorWare architecture, localized algorithms build up the applications where nodes are stimulated with messages coming from the neighbor nodes. One node has a key mission of collecting overall sensor readings and forwarding them to the gateway node. The gateway node serves as a proxy between the network and the user.

B. Local Broadcast

Local broadcast is a fundamental communication primitive, necessary to construct and maintain sensor network architectures and to support the data exchange through sensed events. Any node can be either a sender or a receiver of broadcast messages in the network. These properties determine the structure of the security scheme. In the authors’ proposed scheme, for encryption they use shared symmetric keys. By this way they simplify the key management and ensure the power efficiency of local broadcast, but they don’t present strict authentication process.

C. Code Mobility

Code mobility pattern is very important for sensor networks, because,

- It is impossible for the nodes to keep all application data at all times because of the limited storage.
- After network deployment, new applications should be introduced to the network.

After network deployment, manual reconfiguration of sensor nodes is not achievable. Thus mobile code support becomes more essential.

III. SECURITY THREATS

Owing to the broadcast nature of the transmission medium, wireless networks are more vulnerable to security attacks compared to wired networks. Hence nodes are generally placed in dangerous foreign environments, which are physically insecure, which also increases the vulnerability. For instance, in target tracking applications, the nodes detecting a target in a field exchange messages with timestamp, sensing node location, and other information specific to the application. Whenever the target location is determined, the node informs the location to the user. Just like exchange of application messages in the network, mobile code is sent from node to node. The security of this mobile code is the core part of the author’s security scheme. Possible threats to a network in case of weak communication security are:

1. Malicious code can be injected in the network, spreading to all nodes, potential destruction of the network or capturing network administration. This way the network can be used to send intentionally wrong sensed values to the users or it can be used just for monitoring the sensed data.
2. If the attackers capture the messages including the physical locations of the sensor nodes, this will give an opportunity of destroying the nodes to the attackers.
3. The attackers can also capture some messages including important data such as message IDs and time stamps. Although these data are also important, they are not so critical with respect to location information.
4. There is an attack type, called sleep deprivation torture [24], where an attacker injects false messages including wrong information about the environment to the user.

IV. COMMUNICATION SECURITY SCHEME

The proposed security scheme consists of three security levels based on private key cryptography issuing group keys. The content of all messages in the network is encrypted to guarantee confidentiality.

Hence the main focus of the authors is communication security; they assume that all sensor nodes of the network are allowed to access any message. Authors did not account the protection of data inside the nodes.

Hence execution of security algorithms increases the power consumption of the nodes, authors propose a multilevel encryption scheme in which more critical data handled more carefully. Meaning that encryption applied at level 1 is stronger than the level 2 encryption and so on. The scheme has three security levels as shown in the table below:

<table>
<thead>
<tr>
<th>Level</th>
<th>Security Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Mobile code security, where the most sensitive data sent through the network</td>
</tr>
<tr>
<td>Level 2</td>
<td>Security of messages containing location information</td>
</tr>
<tr>
<td>Level 3</td>
<td>Security of application specific information</td>
</tr>
</tbody>
</table>

Implementing different security levels can be done in two ways:

- Using various algorithms
- Using same algorithm but with adjustable parameters, such as key length

The second way occupies the less memory space.
In their scheme authors use RC6 encryption algorithm [22], because its parameter, the number of rounds, directly affects the security strength of the algorithm. The SensorWare communication multicast model that authors propose, suggests group key deployment. By this way, the number of messages between the nodes decreased considerably. The utilization of the group keys does not require overall change of the sensor network.

The scheme is deployed as follows: All of the sensor network nodes share an initial set of master keys. The longer the lifetime of the network, the more keys are required to expose less data for known ciphertext attack. At any instance, one of the master keys in the list is active. The selection is made in pseudorandom manner, in which each node uses the same seed for randomization. Randomly selected number is matched to the master keys list to determine the active master key. The keys for the three layer security architecture are derived from the active master key.

A. Security Level 1

The messages including mobile code are less frequent compared to messages in which different nodes exchange application instances. As a result strong encryption can be used for this level, resulting processing overhead. The data that have to be protected in this level are: master keys, pseudorandom number generator and the random seed. If an attacker, using “brute force” technique breaks the encryption of this level, he can insert whatever he want in the network (harmful code).

B. Security Level 2

The messages including the sensor node locations, authors propose area based security approach in which a lack of security in one area does not affect the rest of the network. Most of the applications can require the locations of the nodes in a sensor network, so encrypting those messages with higher encryption level should increase the network overhead drastically. As a result medium encryption level is chosen here. To increase the overall security of the network, authors propose a location based security scheme: Level 2 employs location-based keys, in which the nodes in the separated areas use different keys. The overall network area is divided into small cells just like as GSM cell architecture. Nodes in one cell share a location based key. This key is a function of active master key and the location of the node in the cell. Cell shape is not pointed out but diamond cells used in the GSM can also be used here. It has the advantage that the gateway nodes have at most three possible keys (that is the minimum achievable one). Whatever the shape of the cells, the coverage must contain the entire network.

The dimensions of the cells should be kept large enough to maintain the cell based traffic low compared to network traffic.

The nodes in the border of the cells contain the keys of the cells in the neighborhood, see Figure 1.

C. Security Level 3

The messages containing the application specific data has the lowest encryption level, thus having the lowest computational overhead and security level as well.

The Level 3 key is derived from the active master key. The derivation process uses MD5 hash function, which generates Level 3 key from the active master key. As a result refreshing the master key will also refresh the Level 3 key.

For all of the levels mentioned above, it is assumed that sensor nodes have perfect time synchronization and know exactly where their location is.

V. IMPLEMENTATION

The authors implemented their scheme as follows: they used Rockwell WINS sensor nodes, where they can inject the encryption routines of RC6. The nodes have 100Kbps transmitting radios, with three different power levels, namely 1mW, 10 mW and 100mW. They have measured their algorithms for 128 bit data transmission with 128 bit long keys. The measurement criterion was based on the clock cycles required for encryption and decryption processes.

For an algorithm, it is shown [15] that the security is related to the number of rounds required to process the data. Authors assign $R_{\text{min}}$ as the minimum required number of rounds to ensure the security. They also define security margin $(M_s)$ as the percentage deviation of the actual number of rounds $(R)$ from the $R_{\text{min}}$:

$$M_s = \frac{(R - R_{\text{min}})}{R_{\text{min}}}$$

It is clear that increasing the number of rounds, will also cause the security margin to increase. But this also gives a rise to the processing overhead.

They have used 1mW radio transmitting power option first. They have set $R_{\text{min}}$ as 32 rounds for Level 1 and 22 rounds for Level 3 security. 3.9 µJ is consumed for Level 1 encryption and 2.7 µJ is consumed for Level 3 encryption, which is 23% less power consuming than the Level 1. In the system Level 2 and Level 3 encryption will be dominant, compared to Level 1 encryption. So as a result by issuing multilevel encryption scheme at least 23% power efficiency should be achieved.
VI. RELATED WORK

Authors claim that there was not much work done on the sensor network security, maybe it was like that at the time of publishing (2002) but now it is not.

As stated in [27] many researchers started to focus on challenges of maximizing the processing capabilities and energy reserves of wireless sensor nodes while also securing them against attackers. All aspects of the wireless sensor network are being examined including secure and efficient routing [2, 8, 16, 25], data aggregation [3, 7, 14, 19, 29], group formation [1, 9, 20] and sensor trust model [5, 13, 11, 12, 21, 26, 28, 4].

Authors believed that, there should be much more attention to the security in wireless sensor networks. [17] was the only work in this area, in which the authors proposed a security protocol called µTesla. This protocol can be used on the existing infrastructure of the base stations to communicate with the sensor nodes. Authenticated broadcast from the base station through the sensor nodes is provided meaning that a message sending node needs the support of the base station.

As discussed in [6] and [10], key management is the main problem for assuring security in wired and wireless network multicasting. It is the rekeying overhead occurring through the entering and exiting the group. In the sensor network case, the group membership does not change often; the goal is to exclude the attackers out of the group while providing power and computational efficiency as well.

VII. CONCLUSION

In their paper, authors propose a communication security scheme for sensor networks. According to their approach, different levels of security measure are applied for different data types. By this way, they try to achieve maximum efficient resource management. Their scheme identifies the data type included in the message and uses related encryption scheme according to its level based categorization. They left the system level security for sensor networks as a future study.

ACKNOWLEDGMENT

This report is prepared to fulfill the midterm requirement of Wireless Network Architectures and Protocol course (EEL6597), and submitted as it is.

REFERENCES


Ismail Butun (ibutun@mail.usf.edu) received his BS degree in Electrical and Electronics Engineering in 2003 and his MSc in Electrical and Electronics Engineering in 2006 from Hacettepe University, Ankara, Turkey. He is currently pursuing his Ph.D. degree in Electrical Engineering at University of South Florida. His research interests are digital signatures, wireless communication network security, and neural networks. His web site is: http://www.eng.usf.edu/~ibutun/