International Journal of Advanced Trends in Engineering, Science and Technology(IJATEST)Volume.4,Special Issue.1Dec.2016

COMMUNICATION SECURITY IN WIRELESS SENSOR NETWORKS

S.Arif Hussain
Dept. of ECE,S.V.R Engineering College,Nandyal

Abstract:
Networks of wireless micro sensors for monitoring physical environments have emerged as an important new application area for wireless technology. Key attributes of these new types of networked systems are the severely constrained computational and energy resources, and anad hoc operational environment. This paper is a study of the communication security aspects of these networks. Resource limitations and specific architecture of sensor networks call for customized security mechanisms. Our approach is to classify the types of data existing in sensor networks, and identify possible communication security threats according to that classification. We propose a communication security scheme where for each type of data we define a corresponding security mechanism. By employing this multitiered security architecture where each mechanism has different resource requirements, we allow for efficient resource management, which is essential for wireless sensor networks.
Keywords:wireless, sensor, networks, communication.

1.Introduction

Now a day's wireless sensor networks are emerged as an one of the important applications of wireless communications. These sensors networks are resulted as a combination of embedded computing technologies and wireless communications. [1][3].

Sensor networks are low power networks consisting of several hundreds of sensor nodes. Typically, each sensor node consists of micro controllers, signal processing circuits, wireless transmitter/receiver. Sensor networks are computed by coupling with physical world where the information about the physical world is fed into existing infrastructure information. Various important applications of the the wireless sensors networks are target tracking in battlefields, early fire detection in forests, disaster relief networks and environmental monitoring.

With the Wireless sensor networks are gaining importance in day to day life, the relevant research has been focused on distributed data bases, network protocols and energy efficiency. Apart from the focused research areas, security aspects are major concern in critical systems application like hospitals, airports etc. Distinctive features like computational resources and constrained energy are the important aspects of wireless sensor networks. By accommodating existing security mechanisms, a new mechanism is created.

The most important contributions of our work are:

- Security threats are assessed in sensor networks.
- Security mechanisms for efficient data resource management.

In the architecture [4], for which our communication security scheme is being developed differentiates types of data being sent through the network:

1. Mobile code
2. Locations of sensor nodes
3. Application specific data

Moreover, the appropriate security threats and the security mechanisms are listed as follows:

- Malicious mobile code introduced into a sensor network can change the functionality of the network in unpredictable ways.
- Acquiring sensor nodes locations may help an adversary to discover locations of sensor nodes easier than using radio location techniques.
- Protection of application specific data depends on the security requirements of a particular application.

In this brief the main goal is to reduce the security related energy consumption. Here we ensure that scarce resources of sensor nodes are as per the protection levels. There are many other important issues for security in sensor networks, e.g. physical protection of the sensitive data in sensor nodes, and the system-level security.

In Section 2, the Sensor Ware network architecture for communication security scheme is discussed. Section 3 categorizes the

threats to a sensor network. In Section 4, communication security mechanisms and its corresponding types of data are proposed. In Section 5, the implementation environment is discussed. While Section 6 concludes the paper.

2.Sensor Network Architecture

In this section, the Sensor Ware network architecture is described based on the research at Rockwell Science Centre and UCLA [15]. Here the aspects of the architecture are pointed that has impact on the design of the security scheme. The most important elements of the architecture are: local broadcast, localized algorithms, model of communication, and mobile code[2].

2.1.Localized Algorithms

The most important feature of sensor networks is its limited energy available to sensor nodes. Consequently, careful budgeting of the available energy becomes a fundamental design principle. Keeping in mind that communication between nodes consumes a significant amount of the energy resources, applications and system software are expected to achieve a required level of performance while minimizing the amount of traffic in the network. In the Sensor Ware architecture, the applications are designed based on localized algorithms, where nodes triggered by an event exchange messages within an immediate neighbourhood. Only one node aggregates all the sensor readings and sends the combined data to a gateway node, which is one of the sensor nodes in a network capable of serving as a proxy between the network and the user[4].

2.2.Local broadcast

In sensor networks, local broadcast is a fundamental communication primitive. Local broadcast is necessary to build and maintain sensor networks architectures, and to support the exchange of the data about detected events. Any node in the network can be a sender or a receiver of a broadcast message. These properties of sensor networks have a significant impact on the security. In our security scheme, we use shared symmetric keys for encryption. Such a solution simplifies the key management and retains the energy efficiency of local broadcast, but does not offer strong authentication.

2.3Code Mobility

The code mobility paradigm is essential in sensor networks for two reasons:

Limited storage available to nodes does not allow keeping all application on a node at all times.

Applications that a network should run may not be known at the time of deployment of the network.

Since manual reconfiguration of sensor nodes after deployment is not feasible, the support for mobile code is additionally important.

3.Security Threats

Wireless networks, in general, are more vulnerable to security attacks than wired networks, due to the broadcast nature of the transmission medium. To demonstrate, on an example, some of the security threats and our corresponding protection mechanisms, we simulated and implemented a target tracking application. The nodes that detect a target in an area exchange messages containing a timestamp, the location of the sending node and other application-specific information. When one of the nodes acquires a certain number of messages such that the location of the target can be approximately determined, the node sends the location of the target to the user.

Not only the application messages are exchanged through the network, but also mobile code is sent from Node to node.

we list the possible threats to a network if communication security is compromised:

1. Insertion of malicious code is the most dangerous attack that can occur. Malicious code injected in the network could spread to all nodes, potentially destroyingthe whole network, or even worse, taking over the network on behalf of an adversary.
2. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them.
3. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields.
4. An adversary can inject false messages that give incorrect information about the environment to the user.Such messages also consume the scarce energy resources of the nodes. This type of attack is called *sleep deprivation torture* in [14].

4. Communication Security Scheme

After we defined the three types of data in the Sensor Ware network, and the possible threats to thenetwork, in this section we define the elements of the security scheme. The three security levels described here are based on private key cryptography utilizing group keys. Applications and system software access the security API as a part of the middleware defined by the Sensor Ware architecture. Since all three types of data contain more or less confidential information, the content of all messages in the network is encrypted[5].

We assume that all sensor nodes in the network are allowed to access the content of any message. As we said before, we only deal with communication security. Protection of data within a node is not discussed here.

The deployment of security mechanisms in a sensor network creates additional overhead. Not only does latency increases due to the execution of the security related procedures, but also the consumed energy directly decreases the lifetime of the network. To minimize the security related costs we propose that the security overhead, and consequently the energy consumption, should correspond to sensitivity of the encrypted information. Following the taxonomy of the types of data in the network, we define three security levels:

• Security level I is reserved for mobile code, the most sensitive information sent through the network,

• Security level II is dedicated to the location information conveyed in messages,

• The security level III mechanism is applied to the application specific information.

The strength of the encryption for each of security levels corresponds to the sensitivity of the encrypted information. Therefore, the encryption applied at level I is stronger than the encryption applied at level II, while the encryption on level II is stronger than the one applied at level III[6].

Different security levels are implemented either by using various algorithms or by using the same algorithm with adjustable parameters that change its strength and corresponding computational overhead. Using one algorithm with adjustable parameters has the advantage of occupying less memory space

Our implementation results

presented in Section 5 also demonstrate that property. The multicast model of communication inherent for the Sensor Ware architecture suggests deployment of group keys. Otherwise, if each pair of nodes would require a key or a pair of keys, communication between the nodes would have to be unicast based. This would significantly increase the number of messages. Since the addition of security in a sensor network must not require the change of the whole sensor network architecture, group keys are utilized. The keys for three levels of security corresponding to the three types of data are then derived from the active master key[7].

4.1. Security Level I

The messages that contain mobile code are less frequent than the messages that the application instances on different nodes exchange. It allows us to use a strong encryption in spite of the resulting overhead. For information protected at this security level, nodes use the current master key. The set of master keys, the corresponding pseudorandom number generator, and a seed are credentials that a potential user must have in order to access the network[13].

` 4.2. Security Level II

For data that contains locations of sensor nodes, we provide a novel security mechanism that isolates parts of the network, so that breach of security in one part of the network does not affect the rest of the network. `

4.3. Security Level III

We encrypt the application specific data using a weaker encryption than the one used for the two aforementioned types of data. The weaker encryption requires lower computational overhead for application specific data. Additionally, the high frequency of messages with application specific data prevents using stronger and resource consuming encryption. Therefore, we apply an encryption algorithm that demands less computational resources with a corresponding decrease in the strength of security.

5. Implementation

As a part of a proof of concept implementation, we ported the encryption routines of RC6 on the Rockwell WINS sensor nodes. Each operates with an Intel Strong ARM 1100 processor running at 133 MHz, 128KBSRAM, 1MB Flash Memory, a Conexant DCT RDSSS9Mradio[8], a Mark IV geophone and RS232 external interface. The

radios transmit at 100Kbps with the transmission power of 1mW, 10mW, or 100mW[9]. Using the ARM System Developers Kit profiling tools, we measured the clock cycles spend for encryption and decryption of a single 128-bit block with a key of length 128, versus the number of algorithmic rounds. In the AES candidate report [10] the number of rounds, determines the security
strength of an algorithm. In this report for each algorithm minimum number of rounds for which the algorithm is considered to be secure (Rmin) is presented. Based on this quantity, the security margin of an encryption algorithm is defined as the percentage of deviation of the actual number of rounds from Rmin:

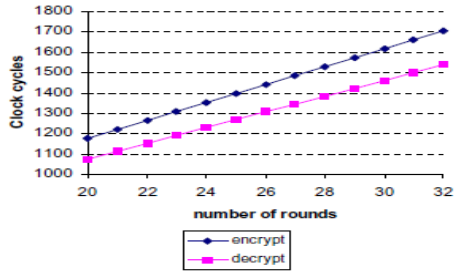

Figure 2. Encryption and decryption clock cycles versus the number of rounds for RC6

Fig.1:depicts the total clock cycles for encryption and decryption of a single 128-bit block with a 128-bit key versus the number of rounds.

As the figure shows, there is a linear relationship between the clock cycles and the number of rounds[12]. As also shown from the equation above, increasing the number of rounds, increases the security margin but the overhead for each block is also increased.

6.Conclusion

In this paper, we propose a communication security scheme for sensor networks. The straightforward approach to the secure communication in sensor networks could Bethe application of a single security mechanism for all detain the network. However, if the mechanism is chosen according to the most sensitive data in the network, security related resource consumption might be unacceptable. On the other hand, a less consuming mechanism could allow for serious security threats. Therefore, the solution lies in the identification of appropriate security requirements for various types of data and the application of suitable security mechanisms. Using the target tracking application as an example, and the sensor Ware architecture as a target platform, we define here some security challenges in sensor networks, identify different types of data, and propose and implement elements of a communication security scheme.

REFERENCES

[1] H. Abelson et. al., "Amorphous Computing", Communicationof ACM, vol.43, vol. 5, May 2000, pp. 74-82.

[2] R. Anderson, M. Kuhn, "Tamper resistance—a CautionaryNote", In Proceedings of the Second USENIX Workshop onElectronic Commerce, 1996.

[3] G. Borriello, R. Want, "Embedding the Internet: EmbeddedComputation Meets the World Wide Web", Communication ofACM, vol.43, no.5, May 2000, pp. 59-66.

[4] DARPA SensIT program. http://dtsn.darpa.mil/ixo/sensit.asp

[5] J. Elson, D. Estrin, "Time Synchronization for Wireless SensorNetworks", In Proceedings of the 2001 IPDPS, Workshop onParallel and Distributed Computing Issues in Wireless Networks
and Mobile Computing, San Francisco, CA, April 2001.

[6] D. Estrin, R. Govindan, J. Heidemann, "Embedding theInternet: Introduction", Communications of the ACM, vol.43,no.5, May 2000, pp. 38-41.

[7] L. Gong, N. Shacham, "Multicast Security and its Extension toa Mobile Environment", Wireless Networks, vol.1, (no.3), 1995,pp. 281-295.

[8] P. Kruus, J. Macker, "Techniques and Issues in MulticastSecurity", MILCOM 98, vol.3, Boston, MA, USA, 1998, pp.1028-32.

[9] J. Agre, L. Clare, G. Pottie, N. Romanov, "DevelopmentPlatform for Self-Organizing Wireless Sensor Networks",Proceedings of SPIE AeroSense'99 Conference on Digital WirelessCommunication, Orlando, FL, USA, April 1999.

[10] J. Nechvatal, E. Barker, D. Dodson, M. Dworkin, J. Foti, E.Roback, "Status Report on the First Round of the Development ofthe Advanced Encryption Standard", http://csrc.nist.gov/encryption/aes/round1/r1report.htm.

[11] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar,"SPINS: Security Protocols for Sensor Networks", MOBICOM2001, Rome, Italy, June 2001.

[12] C. P. Pfleeger, "Security in Computing", Second Edition,Prentice Hall, 1997.

[13] G. J. Pottie, W. J. Kaiser, "Embedding the Internet: WirelessIntegrated Network Sensors", Communications of ACM, vol.43,no.5, May 2000, pp.51-58.

[14] J. Rabaey, J. Ammer, J. L. da Silva, D. Patel, "PicoRadio: AdhocWireless Networking of Ubiquitous Low-EnergySensor/Monitor Nodes", Workshop on VLSI, April 2000.

[15] R. L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin, "TheRC6 Block Cipher", AES submission, Jun 1998.http://theory.lcs.mit.edu/~rivest/rc6.pdf.