IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661 Volume 3, Issue 2 (July-Aug. 2012), PP 01-05
www.iosrjournals.org

Secure Dispatch of Mobile Sensors in a Hybrid Wireless Sensor Networks

Shalini Kumari H. A.[1], R Aparna[2]
[1]*Department of Computer Science and Engineering, Shridevi Institute of Engineering and Technology, Tumkur,*
[2]*Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur,*

Abstract*: A Hybrid Wireless Sensor network (HWSN) with static and mobile nodes is considered. Static sensors monitor the environment and report events occurring in the sensing field. Mobile sensors are then dispatched to visit these event locations to conduct more advanced analysis. Mobile sensor will collect the information about the event and in turn will send it to the base station. As WSN is vulnerable to attacks, a big challenge is to provide security for the communication that takes place between the base station and mobile sensor. Therefore the goal of the paper is to provide security for the data that is transferred between the base station and mobile sensor. In this paper data security will be provided using Sensor Network Encryption Protocol (SNEP) which is one of the building block of SPINS. This paper contributes in defining a suitable data security mechanism.*

Keywords: *Wireless Sensor Network (WSN), Hybrid Wireless Sensor Networks (HWSN), Symmetric Mechanism, Asymmetric Mechanism.*

I. Introduction

Wireless sensor networks (WSNs) are based on physically small-sized sensor nodes exchanging mainly environment-related information with each other [1]. WSNs have a very wide application area including home control, military applications, environmental monitoring etc [2], [3]. Sensors typically have very limited power, memory and processing resources. Therefore interactions between sensors are limited to short distances and low data-rates.

The sensor node may be static sensor node or mobile sensor node, the combination of both static sensor nodes and the mobile sensor nodes is called Hybrid Wireless Sensor network (HWSN). Static sensors support environmental sensing and network communication. They serve as the backbone to identify where suspicious events may appear and report such events to mobile sensors. These Mobile sensors are more resource-rich in sensing [4] and computing capabilities and can move to particular locations to conduct more complicated missions such as providing in-depth analysis, repairing the network etc. Once static sensors collect the sensed information about the event, mobile sensors are then dispatched to visit these event locations to conduct more in depth analysis about the events. Applications of wireless sensor networks have been studied in [2], [3], [4].

The WSN increasingly becoming more practicable solution to many challenging applications. The sensor networks depend upon the sensed data, which may depend upon the application. One of the major applications of the sensor networks is in military. With the rapid growth of the WSN, designing a scalable secure sensor network is a challenging issue. The implementation of security mechanism is a complex and challenging issue because sensors will have limited processing power, storage, bandwidth, and energy.

Communication security is essential to the success of WSN applications, especially for those mission-critical applications working in unattended and even hostile environments. However, providing satisfactory security protection in WSNs has ever been a challenging task due to various network & resource constraints and malicious attacks. This motivates the research on communication security for WSNs.

In this paper, we are providing security for the communications that takes place between base station and sensor nodes. If any event occurs in the network, static sensor node will collect the information about the event and that data will be sent to the base station. In turn that data will be sent to the mobile sensor node to do more in depth analysis about the event. This sensed data that is transferring between the static sensor and the base station should be secured. Therefore providing security is important task.

The data that is transferred between the sensor nodes and the base station should be secured. This data security will be provided using one of the most energy efficient mechanism such as Sensor Network Encryption Protocol (SNEP) which is one of the building block of Security Protocols for Sensor Networks (SPINS).

The rest of the paper is organized as follows: Section II reviews related work. Section III gives security mechanism. Section IV gives the proposed scheme. Conclusions and future research topics are drawn in Section V.

II. Related Work

The work in [1], [2], [3] gives the working of the sensor network as well as Hybrid wireless sensor networks. The working of mobile sensors, how these mobile sensors are dispatched to the event location. how they collect the information about the event.

The work in [5] addresses how to dispatch mobile sensors to the event locations in energy balanced way, where dispatch problem is considered for a single round. In that we mainly considered centralized dispatch algorithm, where there is a communication between base station and the sensor nodes. But they do not considered security for the data transfer between base station and sensor nodes. The studies [6], [7] also address the sensor dispatch problem, but they do not consider energy balance and only optimize energy consumption in one round.

The work in [8] addresses the security challenges in WSN. The studies in [9], [10] addresses the various security mechanisms for WSN. Work in [11] shows various security issues in WSN with full explanation and diagrams.

In this paper based on the requirements and data type transformations we are going to select the security mechanism. The mechanism using for the data security between base station and the sensor nodes is SNEP. Which is one of the building block of SPINS, another one is μTESLA, which is not considered, because it mainly gives security for data broadcasting, but there is no concept of broadcast in dispatching mobile sensor to the event location.

III. Security Mechanism

The field of security for sensor networks is very much in its infancy. The only one algorithm that is written specifically for Dynamic Sensor Networks (DSNs) is called SPINS. The work in [12] gives the detailed information about the working of SPINS.

A. Requirements for Sensor Network Security

This section formalizes the security properties required by sensor networks.

1) Data Confidentiality

Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security.

A sensor node should not reveal its data to the neighbors'. For example, in a sensitive military application where an adversary has injected some malicious nodes into the network, confidentiality will preclude them from gaining access to information regarding other nodes [17]. 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.

2) Data Authentication

Authentication ensures the reliability of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets, adversaries can also inject additional bogus packets. Therefore, the receiving node needs to be able to confirm that a packet received does in fact stem from the node claiming to have sent it [17]. In other words, data authentication allows a receiver to verify that the data really was sent by the claimed sender. Message authentication is important for many applications in sensor networks.

In the two-party communication case, data authentication can be achieved through a purely symmetric mechanism: The 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 it must have been sent by the sender.

3) Data Integrity

Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed while on the networks [17]. In SPINS, data integrity is achieved through data authentication by using MAC, which is a stronger property.

4) Data Freshness

Sensor networks send measurements over time, so it is not enough to guarantee confidentiality and authentication, it must ensure each message is fresh. Informally, data freshness implies that the data is recent, and it ensures that no adversary replayed old messages.

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 useful for sensor measurements, while strong freshness is useful for time synchronization within the network.

In SPINS to achieve the security requirements, two security building blocks are established: SNEP and μTESLA. SNEP provides data confidentiality, two-party data authentication, integrity, and freshness. μTESLA provides authentication for data broadcast. As we are not using μTESLA for the security, so we are not going in depth analysis about this.

IV. Proposed Scheme

Once the static sensor collects information about the event, the data will be sending to the base station. In turn base station will send that data to the mobile sensor. Then the mobile sensor will be dispatched to the event location to conduct more in-depth analysis about the event. WSN is vulnerable to attaches, data that is transferred between base station and mobile sensor should be secured.

In this paper, data security is provided using SPINS, the assumption that are made in the SPINS are as follows:

1. Communications fall into three different categories:

- Node to base station, e.g. sensor readings.
- Base station to node, e.g. specific requests.
- Base station broadcasting to all nodes, e.g. routing beacons, queries or reprogramming of the entire network.

For the first two, SNEP is used, and for the third, µTESLA is used.

Note that it is possible to send a message from one node to another node, but this would involve hopping through the base station.

2. All nodes trust the base station.

This is a reasonable assumption since the base station is at a secure location.

3. The nodes mutually mistrust each other.

It is important because if a node is compromised then its loss would hopefully not compromise the whole network.

4. Each node M_i has a master key K_i which it shares with only the base station.

This master key can be installed when the node is created, or prior to deploying it in the network.

A. Notations

Table 1 list out the symbols used in the security protocols and cryptographic operations.

B. Communication Security

In the proposed data security mechanism, independent keys will be derived for encryption and MAC operations. The two communicating parties Base station B and mobile sensor M share a master secret key X_{BM}, and they derive independent keys using the pseudo-random function *F*: encryption keys $K_{BM} = FX$ (1) and $KM_B = FX$ (3) for each direction of communication, and MAC keys $K'_{BM} = FX$ (2) and $K_{MB} = FX$ (4) for each direction of communication. The combinations of these mechanisms form Sensor Network Encryption Protocol SNEP. The encrypted data has the following format: $E = \{D\}_{<K, C>}$, where *D* is the data, the encryption key is *K*, and the counter is *C*. The MAC is $M = \text{MAC}(K', C||E)$. The complete message that Base station *B* sends to mobile sensor M is:

$B \rightarrow M: \{D\}_{<KBM,CB>}, \text{MAC}(K'_{BM}, C_B || \{D\}K_{BM}, C_B)$

C. Counter Exchange Protocol

The communicating parties B and M know each other's counter values C_B and C_M and so the counter does not need to be added to each encrypted message. However, messages might get lost and the shared counter state can become inconsistent. Fig 1 shows counter exchange protocol in SNEP. The messages sent are marked with the number of the step given below.

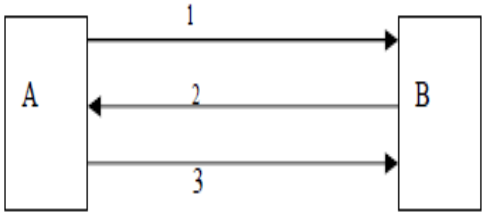

Fig.1. Counter exchange protocol in SNEP.

1) $B \rightarrow M: C_B$

2) $M \rightarrow B: C_M, \text{MAC}(K'_{MB}, C_B || C_M)$

3) $B \rightarrow M: \text{MAC}(K'_{BM}, C_B || C_M)$

B ,M	Principals, such as communicating nodes. Where B is the base station and M is the mobile sensor.
N_B	A nonce generated by *B* (a nonce is an unpredictable bit string, usually used to achieve freshness)
X_{BM}	Master secret (symmetric) key which is shared between *A* and *B*. No direction information is stored in this key, so we have $X_{BM} = X_{MB}$
K_{BM} , K_{MB}	Secret encryption keys shared between B and M
K'_{BM} , K'_{MB}	Secret MAC keys shared between B and M
$\{M\}K_{BM}$	Encryption of message *M* with the encryption key K_{BM}
$\{M\}_{<KBM;IV>}$	Encryption of message *M*, with key K_{BM}, and the initialization vector *IV*
MAC(K'_{BM}; *M*)	Computation of the message authentication code (MAC) of message *M*, with MAC key K'_{BM}.

Table 1: List of Symbols

We now present protocols to synchronize the counter state. To bootstrap the counter values initially, the following protocol is used: This protocol needs strong freshness, so both parties use their counters as a nonce (assuming that the protocol never runs twice with the same counter values, hence incrementing the counters if necessary). Also note that the MAC does not need to include the names of B or M, since the MAC keys K'_{BM} and K'_{MB} implicitly bind the message to the parties, and ensure the direction of the message.

If party *A* realizes that the counter C_M of party M is not synchronized any more, B can request the current counter of M using a nonce N_B to ensure strong freshness of the reply:

$B \rightarrow M: N_M$

$M \rightarrow B: C_M$, MAC (K'_{MA}, $N_B \parallel C_M$)

D. Random-Number Generation

The node has its own sensors, wireless receiver, and scheduling process, from which random digits can be derived. But to minimize power requirements, a MAC function is used as our pseudorandom number generator (PRG), with the secret pseudo-random number generator key X_{rand}. A counter C is used that will be incremented after generating each pseudo-random block. C^{th} pseudo-random output block computed using MAC(X_{rand} ,C). If C wraps around (which should never happen because the node will run out of energy first), new PRG key is generated from the master secret key and the current PRG key using our MAC as a pseudo-random function (PRF): X_{rand} = MAC(X, X_{rand}). Key derivation procedure is given in [12].

E. Encryption Function

To save code space, SNEP uses the same function for both encryption and decryption. The counter (CTR) mode of block ciphers (Fig 2) has this property. CTR mode is a stream cipher. Therefore the size of the ciphertext is exactly the size of the plaintext and not a multiple of the block size. This property is particularly desirable.

Message sending and receiving consume a lot of energy. Also, longer messages have a higher probability of data corruption. Therefore, block cipher message expansion is undesirable. CTR mode requires a counter for proper operation. Reusing a counter value severely degrades security.

In addition, CTR-mode offers semantic security: the same plaintext sent at different times is encrypted into different ciphertext since the encryption pads are generated from different counters. To an adversary who does not know the key, these messages will appear as two unrelated random strings.

Since the sender and the receiver share the counter, we do not need to include it in the message. If the two nodes lose the synchronization of the counter, they can simply transmit the counter explicitly to resynchronize using SNEP with strong freshness. Fig 2 shows counter mode encryption and decryption. The encryption function is applied to a monotonically increasing counter to generate a onetime pad. This pad is then XORed with the plaintext. The decryption operation is identical.

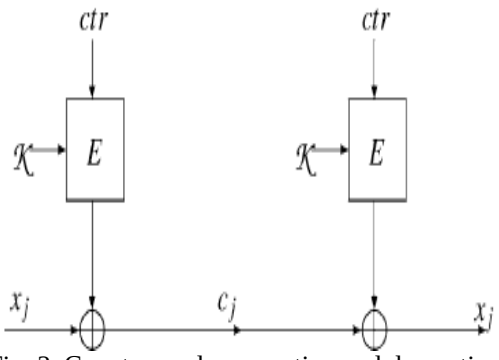

Fig. 2. Counter mode encryption and decryption.

V. Conclusion

In this paper, a mechanism to provide security for the communication that takes place between base station and the mobile sensor is presented. Here we are providing data security using SNEP, which is the most suitable and the easiest mechanism for Wireless Sensor Network. This mechanism provides all the security properties such as Data authentication, freshness, confidentiality and integrity. As sensor nodes will have less energy minimization is also important. This mechanism optimizes energy consumption to provide data security.

In this work there are many assumptions about the working of SNEP. As a future research, we extend our work to relax these assumptions.

References

[1] Yong Wang, Garhan Attebury and Byrav Ramamurthy "A Survey Of Security Issues In Wireless Sensor Networks" IEEE Communications surveys, *The Electrinoc Magazine of Original Peer-Reviewed Survey Articles*, Volume 8, No. 2, 2006.

[2] M.A. Batalin, M. Rahimi, Y. Yu, D. Liu, A. Kansal, G.S. Sukhatme, W.J. Kaiser, M. Hansen, G.J. Pottie, M. Srivastava, and D. Estrin, "Call and Response: Experiments in Sampling the Environment," Proc. *ACM Int'l Conf. Embedded Networked Sensor Systems*, pp. 25- 38, 2004.

[3] T. Wark, P. Corke, P. Sikka, L. Klingbeil, G. Ying, C. Crossman, P. Valencia, D. Swain, and G. Bishop-Hurley, "Transforming Agriculture through Pervasive Wireless Sensor Networks," *IEEEPervasive Computing*, vol. 6, no. 2, pp. 50-57, Apr.-June 2007.

[4] Y.C. Tseng, Y.C. Wang, K.Y. Cheng, and Y.Y. Hsieh, "iMouse: An Integrated Mobile Surveillance and Wireless Sensor System," Computer, vol. 40, no. 6, pp. 60-66, June 2007.

[5] You chiun wang, Wen chih peng, Yu chee tseng "Energy-Balanced Dispatch of Mobile Sensors in a Hybrid Wireless Sensor Networks", *IEE Transactions on parallel and distributed systems*, Vol. 21, No.12, December 2010.

[6] Y.C. Wang, C.C. Hu, and Y.C. Tseng, "Efficient Placement and Dispatch of Sensors in a Wireless Sensor Network," *IEEE Trans. Mobile Computing*, vol. 7, no. 2, pp. 262-274, Feb. 2008.

[7] Y.C. Wang and Y.C. Tseng, "Distributed Deployment Schemes for Mobile Wireless Sensor Networks to Ensure Multilevel Coverage," *IEEE Trans. Parallel and Distributed Systems*, vol. 19, no. 9, pp. 1280-1294, Sept. 2008.

[8] Kuthadi Venu Madhav, Rajendra.C and Raja Lakshmi Selvaraj "A Study of Security Challenges in Wireless Sensor Networks" *Journal of Theoretocal and applied information technology* 2005.

[9] David Boyle, Thomas Newe," Securing Wireless Networks: Security Architectures", *journal of Networks*, Vol. 3 No.1, January 2008.

[10] Ritu Sharma, Yogesh Chaba, Yudhvir Singh, "Analysis of Security Protocols in Wireless Sensor Network", *Int.J. Advanced Networing and Applications*, Vol.02, Issue.03, Pages 707-713, 2010.

[11] Prabhudatta Mohanty, Sangram Panigrahi, Nityananda Sarma and Siddhartha Sankar Satapathy, "Security Issues In Wireless Sensor Network Data Gathering Protocols: A Survey", *journal of Theretical and Applied Information Technology*, 2010.

[12] A.Perrig, R.Szewczyk, J. D. Tygar, V. Wen and D. E. Culler, "SPINS: Security Protocol for Sensor Networks", *ACM Journal of WSN*, pp. 521-534, September, 2002.