ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

The Three – Tier security Scheme in Wireless Sensor Networks with Mobile Sinks

Ranganath Kulkarni[1] , Patil Deogonda[2]

Assistance Professor, Department of Computer Engineering, J.S.P.M's BIT. Engineering College, BARSHI, India[1]

Assistance Professor, Department of Mechanical Engineering, J.S.P.M's BIT. Engineering College, BARSHI, India[2]

ABSTRACT: Mobile sinks (MSs) are vital in many wireless sensor network (WSN) applications for efficient data accumulation, localized sensor reprogramming, and for distinguishing and revoking compromised sensors. However, in sensor networks that make use of the existing key predistribution schemes for pairwise key establishment and authentication between sensor nodes and mobile sinks, the employment of mobile sinks for data collection elevates a new security challenge: in the basic probabilistic and q-composite key predistribution schemes, an attacker can easily obtain a large number of keys by capturing a small fraction of nodes, and hence, can gain control of the network by deploying a replicated mobile sink preloaded with some compromised keys. This paper describes a three-tier general framework that permits the use of any pairwise key predistribution scheme as its basic component. The new framework requires two separate key pools, one for the mobile sink to access the network, and one for pairwise key establishment between the sensors. To further reduce the damages caused by stationary access node replication attacks, authentication mechanism between the sensor and the stationary access node is strengthened in the proposed framework.

KEYWORDS*:* Distributed, security, wireless sensor networks.

I. INTRODUCTION

In recent advances in electronic technology have path the way for the development of a new generation of wireless sensor networks consisting of a large number of low-power, low-cost sensor nodes that communicate wirelessly [1]. Such sensor networks can be used in a wide range of applications, such as, military sensing and tracking, health monitoring [2], data acquisition in hazardous environments. The sensed data often need to be sent back to the base station for analysis. When the sensing field is too far from the base station, transmitting the data over long distances using multi hop may weaken the security strength and increasing the energy consumption at nodes near the base station, reducing the lifetime of the network. Therefore, mobile sinks (MSs) are essential components in the operation of many sensor network applications, including data collection in hazardous environments [3], [4] localized reprogramming, and military navigation.

In many of these applications, sensor nodes transmit critical information over the network; therefore, security services, such as, authentication and pairwise key establishment between sensor nodes and mobile sinks, are important. However, the resource constraints of the sensors and their nature of communication over a wireless medium make data confidentiality and integrity a nontrivial task. Traditional schemes in ad hoc networks using asymmetric keys are expensive due of their storage and computation cost. These limitations [5], [7], [9], [13] make key predistribution schemes provide low cost, secure communication between sensor nodes and mobile sinks. The problem of authentication and pairwise key establishment in sensor networks with Mobile Sinks is still not solved in the face of mobile sink replication attacks. For the basic probabilistic [5] and q-composite [7] key predistribution schemes, an attacker can easily obtain a large number of keys by capturing a small fraction of the network sensor nodes, making it possible for the attacker to take control of the entire network by deploying a replicated mobile sink, preloaded with some compromised keys to authenticate and then initiate data communication with any sensor node.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

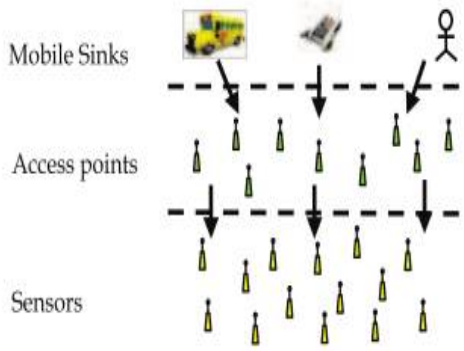


Figure 1: - The three-tier security scheme in wsn with mobile sinks

To address the above-mentioned problem, a general framework developed that permits the use of any pairwise key predistribution scheme as its basic component, to provide authentication and pairwise key establishment between sensor nodes and Mobile Sinks. To facilitate the study of a new Security technique, we first cultivated a general three-tier security framework for authentication and pairwise key establishment, based on the polynomial pool-based key predistribution scheme [8]. The proposed technique will substantially improve network resilience to mobile sink replication attacks compared to the single polynomial pool-based key predistribution approach (see fig 1).

Using two separate key pools and having few sensor nodes that carry keys from the mobile key pool will make it more difficult for the attacker to launch a mobile sink replication attack on the sensor network by capturing only a few arbitrary sensor nodes. Rather, the attacker would also have to capture sensor nodes that carry keys from the mobile key pool. Keys from the mobile key pool are used mainly for mobile sink authentication, and thus, to gain access to the network for data gathering.

Although the above security approach makes the network more resilient to mobile sink replication attacks compared to the single polynomial pool-based key predistribution scheme [8], it is still vulnerable to stationary access node replication attacks. In these types of attacks, the attacker is able to launch a replication attack similar to the mobile sink replication attack. After a fraction of sensor nodes have been compromised by an adversary, captured static polynomials can be loaded into a replicated stationary access node that transmits the recorded mobile sink's data request messages to trigger sensor nodes to send their aggregated data.

II. RELATED WORK

The key management problem is an active research area in wireless sensor networks. Eschenauer and Gilgor [5] proposed a probabilistic key predistribution scheme to bootstrap the initial trust between the sensor nodes. The main idea was to let each sensor node randomly pick a set of keys from a key pool before deployment, so that any two sensor nodes had a certain probability of sharing at least one common key. Chan et al. [7] further extended this idea and developed two key predistribution schemes: the q-composite key predistribution scheme and the random pairwise keys scheme. The q-composite key predistribution scheme also used a key pool, but required two sensor nodes to compute a pairwise key from at least q predistributed keys that they shared. The random pairwise keys scheme randomly picked pairs of sensor nodes and assigned each pair a unique random key. Both schemes improved the security over the basic probabilistic key predistribution scheme.
The pairwise key establishment problem, however, is still not solved. For the basic probabilistic [5] and the qcomposite [7] key predistribution schemes, as the number of compromised nodes increases, the fraction of affected pairwise keys also increases quickly. As a result, a small number of compromised nodes may affect a large fraction of pairwise keys. Although, the random pairwise key does not suffer from the above-mentioned problem, given a memory constraint, the

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

network size is strictly limited by the desired probability that two sensor nodes share a pairwise key, as also by the number of neighbor nodes with which a sensor can communicate. An enhanced scheme using the t-degree bivariate key polynomial was proposed by Liu et al. [8]. They developed a general framework for pairwise key establishment using the polynomial-based key predistribution protocol [10] and the probabilistic key distribution in [5] and [7]. Their scheme could tolerate no more than t compromised nodes, where the value of t was limited by the memory available in the sensor nodes.

III. THE THREE-TIER SECURITY SCHEME

In the proposed scheme, we use two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. Polynomials from the mobile polynomial pool are used to establish the authentication between mobile sinks and stationary access nodes, which will enable these mobile sinks to access the sensor network for data gathering. Thus, an attacker would need to compromise at least a single polynomial from the mobile pool to gain access to the network for the sensor's data gathering. Polynomials from the static polynomial pool are used to ascertain the authentication and keys setup between the sensor nodes and stationary access nodes.
Prior to deployment, each mobile sink randomly picks a subset of polynomials from the mobile polynomial pool. In our scheme, to improve the network resilience to mobile sink replication attack as compared to the single polynomial poolbased approach, we intend to minimize the probability of a mobile polynomial being compromised if Rc sensor nodes are captured. As an adversary can use the captured mobile polynomial to launch a mobile sink replication attack, we achieve this by having a small fraction of randomly selected sensor nodes carry a polynomial from the mobile polynomial pool.
These preselected sensor nodes are called the stationary access nodes. They act as authentication access points for the network and trigger sensor nodes to transmit their aggregated data to the mobile sinks.

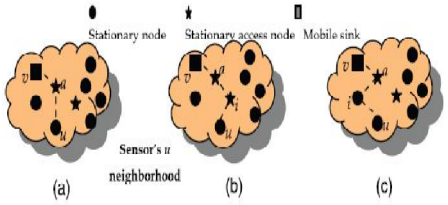


Figure.2. (a) Direct key discovery. (b) Indirect key discovery through intermediate stationary node i. (c) Indirect key discovery through intermediate stationary access node.

A mobile sink sends data request messages to the sensor nodes via a stationary access node. The mobile sink's data request messages will initiate the stationary access node to trigger sensor nodes to transmit their aggregated data to the requested sink. Each stationary access node may share a mobile polynomial with a mobile sink. All sensor nodes, including the stationary access nodes, randomly select a subset of polynomials from the static polynomial pool. The advantage of using separate pools is that mobile sink authentication is independent of the key distribution scheme used to connect the sensor network. We divide our scheme into two stages: static and mobile polynomial predistribution and key discovery between a mobile sink and a sensor node.

Stage 1 (Static and mobile polynomial predistribution)
Stage 1 is performed before the nodes are deployed. A mobile polynomial pool M of size ‖M‖ and a static polynomial pool S of size ‖S‖ are generated along with the polynomial identifiers. All mobile sinks and stationary access nodes are randomly given Km and one polynomial (Km > 1) from M. The number of mobile polynomials in every mobile sink is more than the number of mobile polynomials in every stationary access node. This assures that a mobile node shares a

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

common mobile polynomial with a stationary access node with high probability and reduces the number of compromised mobile polynomials when the stationary access nodes are captured. All sensor nodes and the preselected stationary access nodes randomly pick a subset of Ks and Ks-1 polynomials from S. (figure 2) show The key discovery between the mobile node and stationary node.

Stage 2 (Key discovery between mobile node and stationary node)

To establish a direct pairwise key between sensor node u and mobile sink v, a sensor node u needs to find a stationary access node a in its neighborhood, such that, node a can establish pairwise keys with bothmobile sink v and sensor node u. In other words, a stationary access node needs to establish pairwise keys with both the mobile sink and the sensor node. It has to find a common mobile polynomial with the mobile sink and a common static polynomial with the sensor node. To discover a common mobile/static polynomial, a sensor node i may broadcast a list of polynomial IDs, or alternatively, an encryption list α,Ekv,(α),v=1….,‖Ksi‖ where Kv is a potential pairwise key and the other node may have as suggested. When a direct secure path is established between nodes u and v, mobile sink v sends the pairwise key Kc to node a in a message encrypted and authenticated with the shared pairwise key Kv,a between v and a. If node a receives the above message and it shares a pairwise key with u, it sends the pairwise key Kc to node u in a message encrypted and authenticated with pairwise key Ka,u between a and u.

If the direct key establishment fails, the mobile sink and the sensor node will have to establish a pairwise key with the help of other sensor nodes. To establish a pairwise key with mobile sink v, a sensor node u has to find a stationary access node a in its neighborhood such that node a can establish a pairwise key with both nodes u and v. If node establishes a pairwise key with only node v and not with u. As the probability is high that the access node a can discover a common mobile polynomial with node v, sensor node u needs to find an intermediate sensor node i along the path u - i -a -v, such that intermediate node i can establish a direct pairwise key with node.

3.1 Security Analysis

We have analyzed the performance of the proposed scheme using two metrics: security and connectivity. For security, we present the probability of a mobile polynomial being compromised; hence, an attacker can make use of the captured mobile polynomial to launch a mobile sink replication attack against the sensor network. In connectivity, we estimate the probability of a mobile sink establishing secure links with the sensor nodes from any authentication access point in the network.

3.2 Threat Analysis

In this project, we analyze the security performance of the proposed scheme against a mobile sink replication attack. As stated in the previous section, for an attacker to launch a mobile sink replication attack on the network, the adversary has to compromise at least one polynomial from the mobile polynomial pool. To achieve this, the adversary must capture at least a specific number of stationary access nodes that hold the same mobile polynomial.

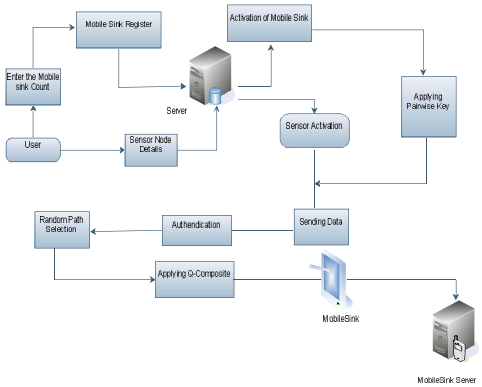


Figure 3.1 System Architecture

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

IV. ALGORITHM USED IN THREE-TIER SECURITY SCHEME

Step 1: First the base station os server gets started. Then, the all sensor node and mobiles sinks sub server are get registered and activated.
Step2: A predistribution pairwise key is generated and securely distributed between sensor node and mobile sink to check whether sensor node and mobiles sinks are in activation mode or not. The same pairwise key is used for encryption and decryption.
Step 3: Once the pairwise key distributed then sensor are ready to browse the information from the environmental accepts.
Step 4: The data of information has to send base station. Before sending the it gets encrypted and authenticated by mobile sinks; if sensor is non-compromised and authorized client then data is retrieved by mobile sinks from sensor.
Step 5:AES algorithm is used for encryption and decryption and for authentication CRC32 bit algorithm is used
Step 6: Finally, the server retrieves the data and stored in database.

V. RESULTS

The main motive of project is to provide security and protect data from attackers. For that we are implementing with three – tier security scheme which includes ;-

1. Pairwise key distribution
2. Authentication
3. Encryption and Decryption technique

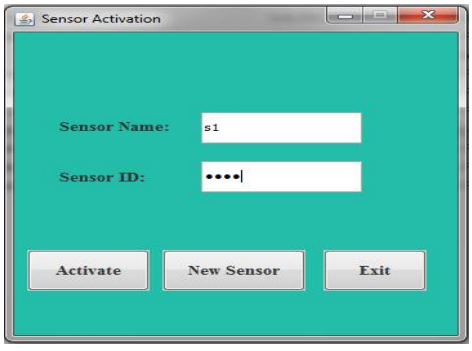


Fig 6.1 Activation of the mobiles sinks after new registration of the MSs.

Fig 6.2 Activation of the new sensor node after getting registration .

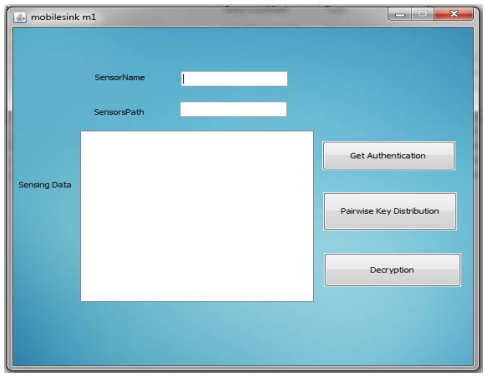
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017



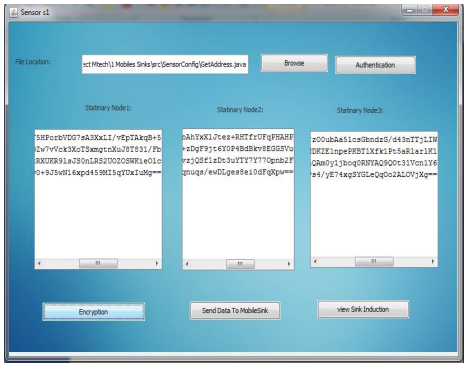
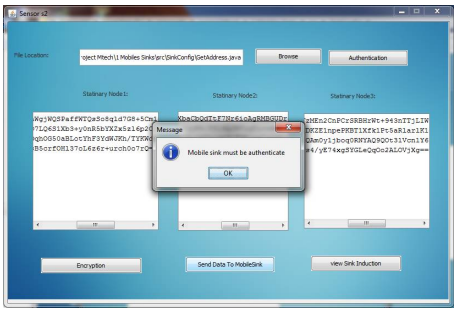


Fig 6.3 the above fig A predistribution pairwise key is generated and securely distributed between sensor node and mobile sink to check whether sensor node and mobiles sinks are in activation mode or not. The same pairwise key is used for encryption and decryption

Fig 6.4 the above fig show encryption and decryption of files where it uses the AES algorithm



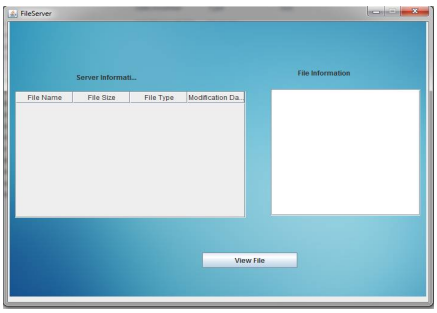


Fig 6.5 the above fig show authentication which uses CRC32 bit algorithm is used. It checks sensor node which is a valid authorized client or not.

Fig 6.6 the information is stored in the server which is send by the sensor

VI. CONSULSION

In this paper, a proposed general three-tier security framework for authentication and pairwise key establishment between mobile sinks and sensor nodes. The proposed scheme, based on the polynomial pool-based key predistribution scheme substantially improves the network resilience to mobile sink replication attacks compared to the single polynomial pool-based key predistribution approach. Using two separate key pools and having few stationary access nodes carrying polynomials from the mobile pool in the network may hinder an attacker from gathering sensor data, by deploying a replicated mobile sink. In this paper, further improves the security against stationary access node replication attack by strengthening the authentication mechanism between stationary access nodes and sensor nodes.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

REFERENCES

[1].I.F. Akyildiz, W. Su, A power aware enhanced routing (PAER) protocol for sensor networks, Georgia Tech Technical Report, January 2002, submitted for publication.
[2]. A. Bakre, B.R. Badrinath, I-TCP: indirect TCP for mobile hosts, Proceedings of the 15th International Conference on Distributed Computing Systems, Vancouver, BC, May 1995, pp. 136–143.
[3] S. Cho, A. Chandrakasan, Energy-efficient protocols for low duty cycle wireless microsensor, Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI Vol. 2 (2000), p. 10.
[4] R. Colwell, Testimony of Dr. Rita Colwell, Director, National Science Foundation, Before the Basic Research Subcommitte, House Science Committe, Hearing on Remote Sensing as a Research and Management Tool, September 1998.
[5] G. Coyle et al., Home telecare for the elderly, Journal of Telemedicine and Telecare 1 (1995) 183–184.
[6] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. ACM Conf. Computer Comm. Security (CCS '02), pp. 41-47, 2002.
[7].Y. Tirta, Z. Li, Y. Lu, and S. Bagchi, "Efficient Collection Sensor Data in Remote Fields Using Mobile Collectors," Proc. 13th Int'l Conf. Computer Comm. and Networks (ICCCN '04), Oct. 2004.