Wireless Sensor Network Monitoring Using Three Tier Security Scheme

J. Anne Steffi[1], S. Dilip Kumar[2]

1 M.Tech Student, Computer Science and Engineering,,PRIST University, Trichy, Tamilnadu, India

2 Assistant Professor, Department of Computer Science and Engineering PRIST University, Trichy, Tamilnadu, India

ABSTRACT:

Wireless sensor network (WSN) uses mobile sinks for web application which provides efficient data accumulation, localized sensor reprogramming, and for distinguishing and revoking compromised sensors. An attacker can easily obtain the key by means of capturing the small fraction of nodes. The sensor network uses existing key for pre-distribution scheme which provides pair-wise key establishment and also for authentication. The employment of mobile sinks for data collection elevates a new security challenge: in the basic probabilistic and q-composite key pre-distribution schemes. Hence this article describes a three-tier architecture for the use of any pair wise pre-distribution, which needs two separate key pools one for mobile sink to access network and another for pair-wise key establishment between the sensors. To further reduce the damages caused by stationary access node replication attacks, we have strengthened the authentication mechanism between the sensor and the stationary access node in the proposed framework. Through the detailed analysis this paper explains the higher security to avoid mobile sink replication.

1. INTRODUCTION:

Recent advances in electronic technology have paved the way for the development of a new generation of wireless sensor networks (WSNs) 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, and habitat monitoring [1]. The sensed data often need to be sent back to the base station for analysis. However, 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 (e.g., some intermediate may modify the data passing by, capturing sensor nodes, launching a wormhole attack [3], sybil attack [4], selective forwarding [5],[6] sinkhole [7]), and increase in the energy consumption at nodes near the base station, reducing the lifetime of the network. Therefore, mobile sinks (MSs) (or mobile soldiers, mobile sensor nodes) are essential components in the operation of many sensor network applications, including data collection in hazardous environments localized reprogramming, and military navigation.

However, the problem of authentication and pair-wise key establishment in sensor networks with MSs is still not solved in the face of mobile sink replication attacks. For the basic probabilistic and q-composite key pre-distribution 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.

To address the above-mentioned problem, we have Developed a general framework that permits the use of any pair-wise key pre-distribution scheme as its basic component, to provide authentication and pair-wise 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 pair-wise key establishment, based on the polynomial pool-based key pre-distribution scheme. The proposed technique will substantially improve network resilience to mobile sink replication attacks compared to the single polynomial pool-based key pre-distribution approach, as an attacker would have to compromise many more sensor nodes to launch a successful mobile sink replication attack. An attacker would have to compromise many more sensor nodes to launch a successful mobile sink replication attack. In the new security framework, a small fraction of the preselected sensor nodes called the stationary access nodes act as authentication access points to the network, to trigger the sensor nodes to transmit their aggregated data to mobile sinks.

A mobile sink sends data request messages to the sensor nodes via a stationary access node. These data request messages from the mobile sink will initiate the stationary access node to trigger sensor nodes, which transmit their data to the requested mobile sink. The scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool.

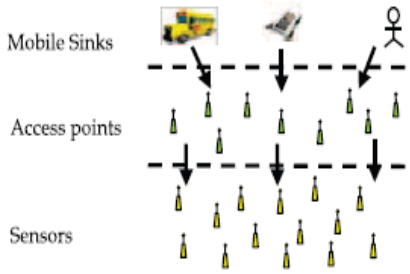

Fig. 1. The three-tier security scheme in WSN with mobile sinks.

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 node the above security approach makes the network more resilient to mobile sink replication attacks compared to the single polynomial pool-based key pre-distribution scheme, 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.

2. 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 or 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.

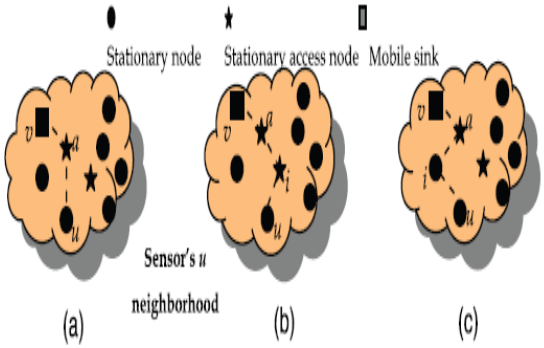

Fig. 2. (a) Direct key discovery. (b) Indirect key discovery through intermediate stationary node *i*. (c) Indirect key discovery through intermediate stationary access node *i*.

Stage 1(Static and mobile polynomial pre-distribution):

Mobile polynomial pool M of size jMj and a static polynomial pool S of size jSj are generated along with the polynomial identifiers. All mobile sinks and stationary access nodes are randomly given Km and one polynomial ($K_m > 1$) 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 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 K_s and K_s _ 1 polynomials from S. Fig.2 shows the key discovery between the mobile node and stationary node.

Stage 2 (Key discovery between mobile node and Stationary node):

To establish a direct pair-wise 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 pair-wise keys with both mobile sink v and sensor node u. In other words, a stationary access node needs to establish pair-wise 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 $\alpha, E_{Kv}(\alpha)$, v=1. . . $|K_{si}|$, where $_{Kv}$ is a potential pair-wise 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 pair-wise key K_c to node a in a message encrypted and authenticated with the shared pair-wise key $K_{v,a}$ between v and a. If node a receives the above message and it shares a pair-wise key with u, it sends the pair-wise key K_c to

node u in a message encrypted and authenticated with pairwise key $K_{a,u}$ between a and u.

If the direct key establishment fails, the mobile sink and the sensor node will have to establish a pair-wise key with the help of other sensor nodes. To establish a pair-wise 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 pair-wise key with both nodes u and v. If node a establishes a pair-wise 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 pair-wise key with node a.

2.1 Security Analysis

The performance of the proposed scheme is analyzed using two metrics: security and connectivity. In connectivity, we estimate the probability P_{conn} of a mobile sink establishing secure links with the sensor nodes from any authentication access point in the network as

$$P_{conn} = 1-(1-c/n)^{m}$$

Where n represents the total number of sensor nodes in the network, c is the average number of neighbor nodes for every sensor node before deployment of the stationary access nodes, and m is the number of stationary access nodes in the network. The probability that a mobile sink and a stationary access node share a mobile polynomial—in other words, the probability P_m; the mobile sink, and stationary access node can establish a key directly—is expressed by

$$P_m=K_m/|m|$$

The probability P_s, where two sensor nodes share a common static polynomial—the probability that the two sensors can establish a secure link directly is estimated by

$$P_s = 1- (|S|2K_s) . (2K_s K_s) / (|S|K_s)^2$$

The probability Psa, where a sensor node and a stationary access node share a common static polynomial—the probability that the two nodes can establish a pair-wise key directly—is estimated by

$$P_{sa} = 1- (|S|2K_s - 1) . (2K_s\text{-}1\ K_s\ \text{-}1) / (|S|K_s) . (|S|K_s\text{-}1)$$

The probability P_a, where two stationary access nodes share a common static/mobile polynomial, is estimated by

$$P_a = 1- (|M|-1).(2.|S|(K_s – 1)) . (2(K_s\text{-}1)\ K_s\ \text{-}1) / (|M|) . (|S|K_s\text{-}1)^2$$

The probability Pd of a mobile sink and a sensor node establishing a pair-wise key (directly or indirectly) can be estimated by

$$P_d = 1–(1-P_{sa}\ P_m)^{g.} (1 - P_m P_{sa}\ P_s)^{g,d} . (1 – P_m P_a P_{sa})^{g(g-1)}$$

Where d denotes the average number of neighbors that a sensor can contact, and g denotes the average number of stationary access nodes that the node has in its neighborhood.

2.2 Threat Analysis

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. It follows from the security analysis of the Blundo scheme, that for any polynomial w in the mobile polynomial pool of degree tm, an attacker cannot recover the polynomial w, if no more than tm stationary access nodes that had chosen w are captured by the attacker. If more than tm stationary access nodes with w as their mobile polynomial are captured by the attacker, then the attacker can recover the mobile polynomial w, and thus be able to launch a mobile sink replication attack against the sensor network. We assume that an attacker randomly captures Rc sensor nodes, Rc > tm. To simplify our estimation for the probability Pr of a mobile polynomial being compromised, we consider the captures of sensor nodes are independent. Now let w be a polynomial in the mobile pool. The probability of w being chosen for a stationary access node is 1/|M|, the probability that any captured node is a stationary access node is m n, and the probability that a captured node is a stationary access node and it hold w is 1/ |M| X m/n. Therefore, the probability that this polynomial being chosen exactly by x stationary access nodes among Rc captured nodes is

$$P(x) = (RcXx).(1/|M| X m/n)^{x}.(1 – 1/|M| X m/n)^{Rc-x}$$

3. THE ENHANCED THREE-TIER SECUIRTY SCHEME

This scheme delivers the same security performance as the single polynomial pool approach when the network is under a stationary access node replication attack. In both schemes, for any sensor node u that needs to authenticate and establish a pair-wise key with a stationary access node A, the two nodes must share at least a common polynomial in their polynomial rings. To perform a stationary access node replication attack on a network, the adversary needs to compromise at least a single polynomial from the static pool. This can be obtained easily by capturing arbitrary sensor nodes in the network. Then, the adversary can make use of this compromised polynomial by a replicated stationary access node to enable insecure access to the network. When successful access to the network has been obtained through the compromised static polynomial, the replicated stationary access node transmits recorded mobile sink data request messages. Next, the sensor nodes that have the compromised polynomial in their rings will insecurely authenticate and establish a

pair-wise key with the replicated node and thus deliver their data to the replicated node.

In this section, we remedy the security performance of the proposed scheme in the case of a stationary access node replication attack. We use a one-way hash chain algorithm in conjunction with the polynomial pool scheme. In addition to the static polynomial, a pool of randomly generated passwords is used to enhance the authentication between sensor nodes and stationary access nodes.

To establish an authentication between a sensor node and a stationary access node in the enhanced scheme, the two must share a common static polynomial. In the access node verification, to verify the authenticity of a stationary access node, the sensor node performs a single hash operation on the hash value that is sent from the stationary access node.

3.1 Security analysis

This paper evaluates the connectivity of the enhanced three-tier security scheme. We estimated the P_{conn} and the preloaded hash values of P_{wi} in each of stationary access nodes and the sensor nodes respectively.

$$P_{conn}= 1 – (1-p \text{ x } c/n)^{m}$$

Where p is the probability that a stationary access node and a sensor node share at least a common chosen password for access node verification

$$P= 1- (|W|XGs+Ga).(Gs+ GaXGs)/(|W|Gs).(|W|Ga)$$

We also estimated the probability Pg of the mobile sink being connected directly or indirectly to a sensor node via a *stationary access* node that shared with the sensor node, at least one common static polynomial and a common chosen password P_{wi}, for which the node was able to verify the access node by. To drive the probability Pg, we used a similar analysis as that used for the estimation of probability Pd, except that no sensor neighbor could act as an intermediate node; thus,

Pg could be estimated by

$$Pg = 1 – (1 - pP_{sa}P_{m})^{g} . (1 – pP_{m}P_{a}P_{sa})^{g(g-1)}$$

3.2 Threat Analysis

In the stationary access node replication attack, the adversary needs to capture at least one polynomial from the static pool and at least one hash value $H^{r-1}()$ of a chosen password. To analyze the security performance of the enhanced three-tier scheme, we estimated probability P_{hp} of a non compromised sensor node being under a stationary access node replication attack, when x number of nodes were being captured. To calculate the probability P_{hp} for a non compromised sensor node that had a hash value $H^{r}(Pw_{i})$ in its hash value ring and static polynomial y in its static polynomial ring, we were required to obtain the probabilities of both $H^{r-1}(Pw_{i})$ and polynomial y, as they were being compromised when the x nodes are captured.

The probability P_h that a given hash value is not chosen by a non compromised stationary access node is 1-Ga/|M| X m/n. If there are x compromised nodes, the probability that a given hash value $H^{r-1}(P_{wi})$ is not captured is $(1\text{-}Ga/|W| \text{ X } m/n)^{x}$. As in, the probability of the hash value being captured is, thus,

$$P_h = 1 – (1 – Ga/|W| \text{ X } m/n)^{x} .$$

Ph increases dramatically as we increased the ratio of the stationary access nodes from 1 to 8 percent. In the case of the captured static polynomial y of degree t, the attacker cannot determine the non compromised static polynomial based key, if no more than t nodes have been captured. Thus, the probability of polynomial y being compromised is

$$P_p=1 - \sum_{j=0}^{j=t} p(j)$$

The enhanced three-tier security scheme has a better security performance in terms of network resilience to stationary access node replication attack than the previously proposed scheme. For access node ratios greater than 2 percent, both versions of the three-tier security scheme have a similar network resiliency against access node replication attacks.

4. CONCLUSION

In this paper, we proposed a general three-tier security framework for authentication and pair-wise key establishment between mobile sinks and sensor nodes. The proposed scheme, based on the polynomial pool-based key pre-distribution scheme substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key pre-distribution 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. Analysis indicates that with 10 percent of the sensor nodes in the network carrying a polynomial from the mobile pool, for any mobile polynomial to be recovered, the attacker would have to capture 20.8 times more nodes as compared to the single polynomial pool approach. We have further improved the security performance of the proposed scheme against stationary access node replication attack by strengthening the authentication mechanism between stationary access nodes and sensor nodes. We used the one-way hash chains algorithm in conjunction with the static polynomial pool-based scheme.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless Sensor Networks: A Survey,” *Computer Networks*, vol. 38, no. 4, pp. 393-422, 2002.

[2] T. Gao, D. Greenspan, M. Welesh, R.R. Juang, and A. Alm, “Vital Signs Monitoring and Patient Tracking over a Wireless Network,” Proc. *IEEE 27th Ann. Int’l Conf. Eng. Medicine and Biology Soc. (EMBS)*, Sept. 2005.

[3] L. Hu and D. Evans, “Using Directional Antenna to Prevent Wormhole Attacks,” *Proc.*

Network and Distributed System Security Symp., 2004.
[4] J.R. Douceur, "The Sybil Attack," *Proc. First Int'l Workshop Peer-to- Peer Systems (IPTPS '02)*, Mar. 2002.
[5] B.J. Culpepper and H.C. Tseng,"Sinkhole Intrusion Indicators in DSR MANETs," *Proc. First Int'l Conf. Broadband Networks (Broad- Nets '04)*, pp. 681-688, Oct. 2004.
[6] H. Deng, W. Li, and D.P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," *Proc. IEEE Comm. Magazine*, pp. 70-75, 2002.
[7] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," *Proc. MobiCom*, pp. 56-67, 2000.