The Three Tier security scheme in wireless sensor network With mobile sinks

DEEPIKA R , NAVYA K M, NAYANA KUMARI M, SOWMYA T H
rv.deepika009@gmail.com, Navya.km91@gmail.com,
Nayanakumari91@gmail.com ,Sowmyath01@gmail.com

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 article 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, we have strengthened the authentication mechanism between the sensor and the stationary access node in the proposed framework. Through detailed analysis, we show that our security framework has a higher network resilience to a mobile sink replication attack as compared to the polynomial pool-based scheme.

Index Terms—Distributed, security, wireless sensor networks.

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 hazar-dous 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 multihop may weaken the security strength (e.g., some intermediate may modify the data passing by, capturing sensor nodes, launching a wormhole attack [3], a sybil attack [4], selective forwarding [5], [6], sinkhole [7]), and increasing 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 [8], [9], [10], localized reprogramming, oceano-graphic data collection, and military navigation [11]

In many of these applications, sensor nodes transmit critical information over the network; therefore, security services, such as , authentication and pair wise 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 non-trivial task. Traditional schemes in ad hoc networks using asymmetric keys are expensive due of their storage and computation cost. These limitations make key predistribution schemes [12], [13], [14], [15], [16], [17], [18] the tools of choice to provide low cost, secure communication between sensor nodes and mobile sinks.

However, the problem of authentication and pairwise key establishment in sensor networks with MSs is still not solved in the face of mobile sink replication attacks. For the basic probabilistic [12] and q-composite [13] 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.

To address the above-mentioned problem, we have developed a general framework [19] 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 MSs. 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 [14]. The proposed technique will substantially improve network resilience to mobile sink replication attacks compared to the single polynomial pool-based key predistribution approach [14], as an attacker would have to compromise many more sensor nodes to launch a successful mobile sink replication attack. In the new security framework [19], a small fraction of the preselected sensor nodes (see Fig. 1), 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.

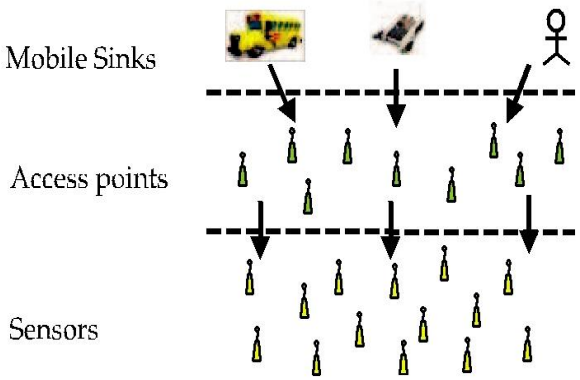

Fig. 1. The three-tier security scheme in WSN with mobile sinks.

The scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool.

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 net-work more resilient to mobile sink replication attacks compared to the single polynomial pool-based key predistribution scheme [14], 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.

To make the three-tier security scheme more robust against a stationary access node replication attack, we have strengthened the authentication mechanism between the stationary access nodes and sensor nodes using one-way hash chains algorithm [20] in conjunction with the static polynomial pool-based scheme [14]. Our analytical results indicate that the new security technique makes the network more resilient to both mobile sink replication attacks and stationary access nodes replication attacks compared to the single polynomial pool-based approach.

This paper is organized as follows. Section 2 discusses some existing schemes relevant to those proposed in this paper. Section 3 presents the security and threat analysis for a mobile sink replication attack, using the proposed scheme [19].

2 RELATED WORK

The key management problem is an active research area in wireless sensor networks. Eschenauer and Gilgor [12] 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. [13] 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 [12] and the q-composite [13] 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 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. [14]. They developed a general framework for pairwise key establishment using the polynomial-based key predistribution protocol [21] and the probabilistic key distribution in [12] and [13]. 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.

3 THE THREE-TIER SECURITY SCHEME

In this study, we have chosen the Blundo scheme [21] to construct our approach. As we shall see, the Blundo scheme provides a clear security guarantee. Use of the Blundo scheme, therefore, greatly eases the presentation of our study and enables us to provide a clearer security analysis.

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 pool-based approach, we intend to minimize the probability of a mobile polynomial being compromised if R_c 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.

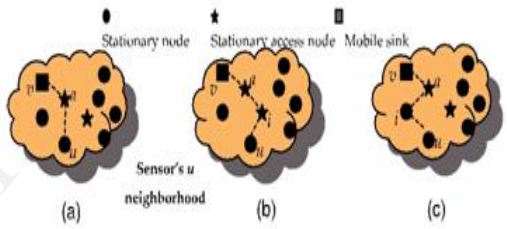

Fig. 2. (a) Direct key discovery. (b) Indirect key discovery through intermediate stationary node i. (c) Indirect key discovery through intermediate stationary access node i.

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. 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 K_m 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 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 both mobile 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 $\alpha, E_{kv}(\alpha)$, v=1, . . . ,$|K_{si}|$, where K_v is a potential pairwise key and the other node may have as suggested in [12] and [13]. When a direct secure path is established between nodes u and v, mobile sink v sends the pairwise key K_c to node a in a message encrypted and authenticated with the shared pairwise key $K_{v,a}$ between v and a. If node a receives the above message and it shares a pairwise key with u, it sends the pairwise key K_c to node u in a message encrypted and authenticated with pairwise key $K_{a,u}$ between a and u.

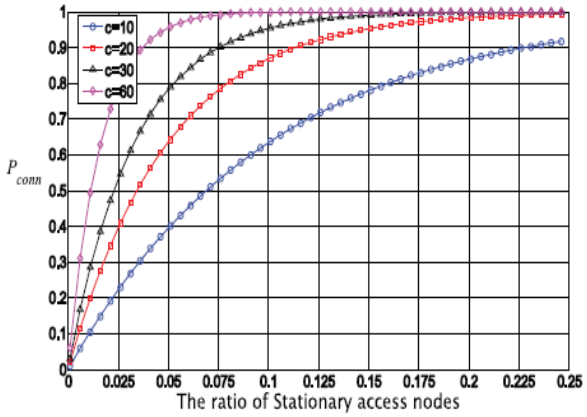

Fig. 3. The probability P_{conn} that a sensor has at least one stationary access node in its neighborhood versus the ratio of access nodes.

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 a 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 a.

3.1 Security Analysis

We have analyzed the performance of the proposed scheme using two metrics: security and connectivity [19]. 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 P_{conn} (see Appendix A for detailed derivation, which can be found on the Computer Society Digital Library at http://doi.ieeecomputersociety.org/10.1109/TPDS. 2010.185) of a mobile sink establishing secure links with the sensor nodes from any authentication access point in the network as 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,

$$P_{conn} = 1 - \left(1 - \frac{c}{n}\right)^m,$$

Fig. 3 shows P_{conn} versus the ratio of stationary access nodes.

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

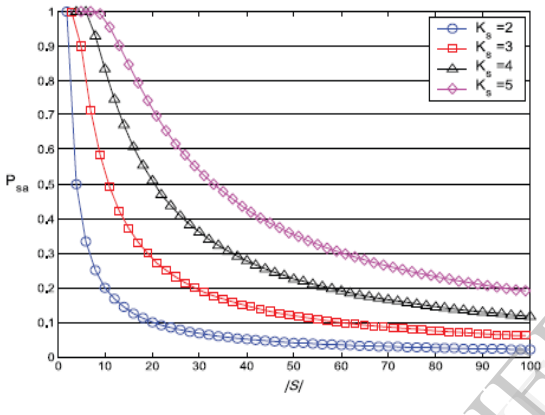

Fig. 4. The probability P_{sa} that a sensor and stationary access node share a static polynomial versus the size |S|

$$P_m = \frac{K_m}{|M|}.$$

The probability Ps, where two sensor nodes share a Common static polynomial the probability that the two
Sensors can establish a secure link directly is estimated by

$$P_s = 1 - \frac{\binom{|S|}{2K_s} \cdot \binom{2K_s}{K_s}}{\binom{|S|}{K_s}^2}.$$

The probability P_{sa}, where a sensor node and a stationary access node share a common static polynomial the probability that the two nodes can establish a pairwise key directly is estimated by

$$P_{sa} = 1 - \frac{\binom{|S|}{2K_s - 1} \cdot \binom{2K_s - 1}{K_s - 1}}{\binom{|S|}{K_s} \cdot \binom{|S|}{K_s - 1}}.$$

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

$$P_a = 1 - \frac{(|M| - 1) \cdot \binom{|S|}{2 \cdot (K_s - 1)} \cdot \binom{2 \cdot (K_s - 1)}{K_s - 1}}{|M| \cdot \binom{|S|}{K_s - 1}^2}.$$

Fig. 4 shows the relationship between the probability P_{sa} and the combination of |S| and K_s, respectively.

All figures clearly show that the closer |S| and K_s are the more likely two sensor nodes can establish a pairwise key directly.

The probability P_d (see Appendix B, in the online supplemental material, for detailed derivation) of a mobile sink and a sensor node establishing a

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

pairwise key (directly or indirectly) can be estimated by
stationary access nodes that the node has in its neighborhood.

3.2 Threat Analysis

In this section, 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. It follows from the security analysis of the Blundo scheme, that for any polynomial w in the mobile polynomial pool of degree t_m, an attacker cannot recover the polynomial w, if no more than t_m stationary access nodes that had chosen w are captured by the attacker. If more than t_m stationary access nodes

with w as their mobile polynomial are captured by the attacker, then the attacker can recover the mobile poly-nomial w, and thus be able to launch a mobile sink replication attack against the sensor network. We assume that an attacker randomly captures R_c sensor nodes, $R_c > t_m$. To simplify our estimation for the probability P_r 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 $1/|M| \times m/n$. Therefore, the probability that this polynomial being chosen exactly by x stationary access nodes among R_c captured nodes is

$$P(x) = \binom{R_c}{x} \cdot \left(\frac{1}{|M|} \times \frac{m}{n}\right)^x \cdot \left(1 - \frac{1}{|M|} \times \frac{m}{n}\right)^{R_c - x}.$$

Thus, the probability that any polynomial from the mobile pool being recovered by an attacker is

$$P_r = 1 - \sum_{x=0}^{t_m} P(x).$$

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 SecuritySymp., 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.

[8] A. Kansal, A. Somasundara, D. Jea, M. Srivastava, and D. Estrin,"Intelligent Fluid Infrastructure for Embedded Networks," Proc. Second ACM Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '04), June 2004.

[9] Y. Tirta, Z. Li, Y. Lu, and S. Bagchi, "Efficient Collection of Sensor Data in Remote Fields Using Mobile Collectors," Proc.13th Int'l Conf. Computer Comm. and Networks (ICCCN '04), Oct.2004.

[10] A. Rasheed and R. Mahapatra, "An Energy-Efficient Hybrid Data Collection Scheme in Wireless Sensor Networks," Proc. Third Int'l Conf. Intelligent Sensors, Sensor Networks and Information Processing,2007.

[11] W. Zhang, G. Cao, and T. La Porta, "Data Dissemination with Ring-Based Index for Wireless Sensor Networks," Proc. IEEE Int'l Conf. Network Protocols (ICNP), pp. 305-314, Nov. 2003.

[12] 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.

[13] H. Chan, A. Perrig, and D. Song, "Random Key Pre-Distribution Schemes for Sensor Networks," Proc. IEEE Symp. Research in Security and Privacy, 2003.

[14] D. Liu, P. Ning, and R.Li. Establishing, "Pairwise Keys in Distributed Sensor Networks," Proc. 10th ACM Conf. Computers and Comm. Security (CCS '03), pp. 52-61, Oct. 2003.

[15] H. Chan, A. Perrig, and D. Song, "Key Distribution Techniques for Sensor Networks," Wireless Sensor Networks, pp. 277-303, Kluwer Academic, 2004.

[16] D. Liu and P. Ning, "Location-Based Pairwise Key Establishments for Static Sensor Networks," Proc. First ACM Workshop Security AdHoc and Sensor Networks, 2003.

[17] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," Proc.10th ACM Conf. Computers and Comm. Security (CCS '03), pp. 62-72,Oct. 2003.

[18] A. Rasheed and R. Mahapatra, "An Efficient Key Distribution Scheme for Establishing Pairwise Keys with a Mobile Sink in Distributed Sensor Networks," Proc. IEEE 27th Int'l Performance Computing and Comm. Conf. (IPCCC '08), pp. 264-270, Dec. 2008.