Survey on Enhanced Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks

Mr. Shailesh M. Umap[1]
[1]ME. (WCC),
Priyadarshini College of Engineering ,
Nagpur , MS (India),

Mr. C. R. Pote[2]
[2]Asst. Professor, CT Dept.
Priyadarshini College of Engineering ,
Nagpur- (MH), India,

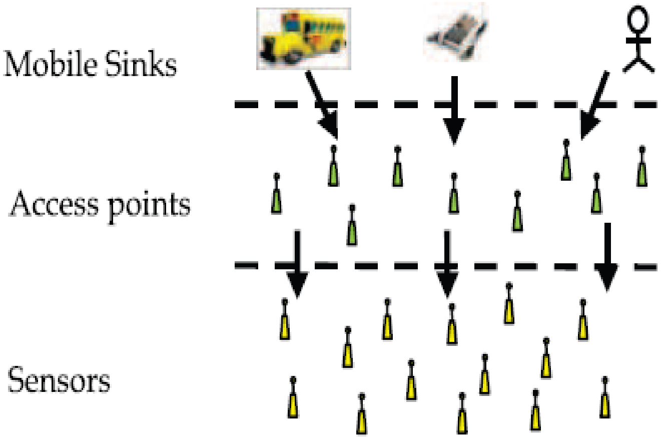
***Abstract*--Recent developments on Wireless Sensor Networks have made their application in a wide range such as military sensing and tracking, health monitoring, traffic monitoring, video surveillance and so on. Mobile sinks (MSs) are vital in many wireless sensor network (WSN) applications for efficient 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, The problem of authentication and pair wise key establishment in sensor networks with mobile sink is still not solved in the mobile sink replication attacks. In q-composite key pre distribution scheme, a large number of keys are compromised by capturing a small fraction of sensor nodes by the attacker. The attacker can easily take a control of the entire network by deploying a replicated mobile sinks. Those mobile sinks which are preloaded with compromised keys are used authenticate and initiate data communication with sensor node.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**

Keywords:Wireless Sensor Network, Pair Wise Key Establishment, Random Key Pre Distribution, Mobile Sink, Encryption Technique.

I. INTRODUCTION:

Recent development in electronic and computer technologies made the way for emergent of Wireless Sensor Networks (WSN). The WSN consists of wide distributed sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to pass their data through the network to a destination. The advancement of wireless communication technologies and rooted computing, are being widely adapted into many applications through sensor networks and many active researches on related subject are being carried out. Several sensor nodes are connected to build the wireless sensor networks. 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 , a sybil attack [, selective forwarding , sinkhole), 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 [1],[2] localized reprogramming, oceanographic data collection, and military navigation [3].In many of these applications, sensor nodes transmit. In many of these applications, sensor nodes transmit critical information over the network; therefore, securitys ervices, such as, authentication and pairwise key establishment between sensor nodes and mobile sinks, are important. 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 [5] and q-composite [6] 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.

IJERT



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 [10], as an attacker would have to compromise many more sensor nodes to launch a successful mobile sink replication attack. In the new security framework [4], 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.

II. RELATED WORK

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 [9] in conjunction with the static polynomial pool-based scheme. 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. [6] further extended
this idea and developed two key predistribution schemes:

IJERT

q-composite key predistibution scheme :- That also used a key pool,but required two sensor node to compute a pairwise key from at least q -predistibuted keys that they shared.

Random Pairwise key scheme:- That randomly picked pairs of sensor nodes and assigned each pair of unique random keys.

The pairwise key establishment problem, however, is still not solved. For the basic probabilistic [5] and the q-composite [6] 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.

III. THE THREE-TIER SECURITY SCHEME

In this proposed system that used Blundo scheme [7] to construct o ur approach. As the Blundo scheme provides a clear security guarantee. In the proposed scheme, that use two separate polynomial pools:

The Mobile 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. Each mobile sink randomly picks a subset of polynomials from the mobile polynomial pool.

Static Polynomial Pool :- That are used to ascertain the authentication and keys setup between the sensor nodes and stationary access nodes.

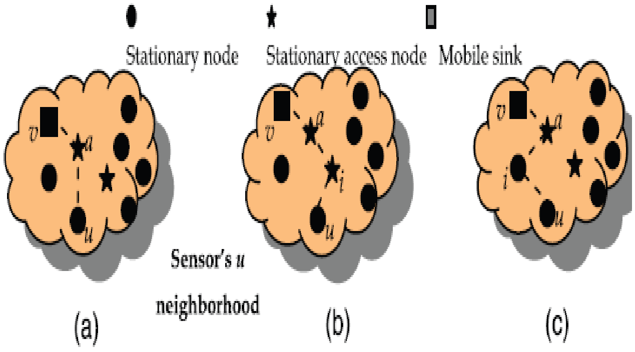


Fig:- (a) Direct key Discovery
(b) Indirect key discovery through intermediate stationary node i
(c) Indirect key discovery through intermediate stationary access node i

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. 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.
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). This stage 1 is performed before the nodes are deployed. A 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 (Km > 1) fromM. 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 Ks and Ks _ 1 polynomials from S. Figure 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. 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.

IV. THE ENHANCED THREE-TIER SECURITY SCHEME

The three-tier security scheme provides better network resilience against mobile sink replication attack compared to the single polynomial pool approach. 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 pairwise key with a stationary access node A, the two nodes must share at least a common polynomial in their polynomial rings. 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 [9] algorithm in conjunction with the polynomial pool scheme, addition to the static polynomial, a pool of randomly generated passwords is used to enhance the authentication between sensor nodes and stationary access nodes.In the enhanced security scheme, each sensor node, such as u, is preloaded with a subset of Ks polynomials randomly chosen from the static pool . In addition to the Ks preloaded static polynomials, node u randomly picks a subset of Gs passwords from the password pool.. 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.

V. CONCLUSION

In this paper, a 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 improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key predistribution approach .[8]. 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.I 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.To given best security to the enire tier using best algorithm for each tier. Application of different encryption algorithms (one algorithm per tier)

REFERENCES

[1] 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

[2] 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

[3] 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.

[4] A. Rasheed and R. Mahapatra, "A Key Pre-Distribution Scheme for Heterogeneous Sensor Networks," Proc. Int'l Conf. Wireless Comm. and Mobile Computing Conf. (IWCMC '09), pp. 263-268, June 2009.

[5] 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.

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

[7] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences," Proc. 12th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '92), pp. 471-486, 1993.

[8] 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.

[9] L. Lamport, "Password Authentication with Insecure Communication," Comm. ACM, vol, 24, no. 11, pp. 770-772, Nov. 1981.

[10] 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.

[11] 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.

[12] 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.

[13] L. Hu and D. Evans, "Using Directional Antenna to Prevent Wormhole Attacks," Proc. Network and Distributed System Security Symp., 2004.

[14] J.R. Douceur, "The Sybil Attack," Proc. First Int'l Workshop Peer-to-Peer Systems (IPTPS '02), Mar. 2002

IJERT