TKP : Three Level Key Pre-distribution with Mobile Sinks for Wireless Sensor Networks

Tanuja R*, Souparnika P Arudi*, S H Manjula*, K R Venugopal*, L M Patnaik**
*Department of Computer Science and Engineering
University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India
**Honarary Professor, Indian Institute of Science, Bangalore, India
r_tanuja@yahoo.com

***Abstract*— Wireless Sensor Networks are by its nature prone to various forms of security attacks. Authentication and secure communication have become the need of the day. Due to single point failure of a sink node or base station, mobile sinks are better in many wireless sensor networks applications for efficient data collection or aggregation, localized sensor reprogramming and for revoking compromised sensors. The existing sytems that make use of key predistribution schemes for pairwise key establishment between sensor nodes and mobile sinks, deploying mobile sinks for data collection has drawbacks. Here, an attacker can easily obtain many keys by capturing a few nodes and can gain control of the network by deploying a node preloaded with some compromised keys that will be the replica of compromised mobile sink. We propose an efficient three level key predistribution framework that uses any pairwise key predistribution in different levels. The new framework has two set of key pools one set of keys for the mobile sink nodes to access the sensor network and other set of keys for secure communication among the sensor nodes. It reduces the damage caused by mobile sink replication attack and stationary access node replication attack. To further reduce the communication time it uses a shortest distance to make pair between the nodes for comunication. Through results, 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 with less communication time .**

***Index Terms*— Key predistribution, Security, Wireless Sensor Networks.**

I. Introduction

Wireless Sensor Network (WSN) is a wireless network consisting of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location or a base station. The more modern networks are bi-directional, also enabling control of sensor activity. WSNs are found to be extremely useful for a large area of applications. Sensor networks can be deployed for habitat monitoring, environmental monitoring including forest fire detection, air pollution and green house monitoring, industrial and consumer applications. They are extremely useful in military applications that demand high security for nuclear and chemical attack detection, battlefield surveillance and so on[1].

Secure transmission of data is a crucial issue to be addressed in WSNs. Due to broadcast nature of transmission WSNs are vulnerable to various security attacks and since the nodes are exposed they can be destroyed. Most important security requirements are : Data Confidentiality, Data Integrity, Availability, Data freshness, Self-Organization, Secure Localization, Time Synchronization, Access control and Authentication.

Security is critical for such networks deployed in hostile environments. Most sensor networks actively monitor their surroundings, and it is often easy to tamper the network to get the data and deduce information other than the data monitored. Information leakage often results in privacy breaches of the network in environment. Moreover, the wireless communication employed by sensor networks facilitates eavesdropping and packet injection by an adversary. The combination of these factors demands for sensor networks at design time to ensure operation safety, secrecy of sensitive data, and privacy for people in sensor environments.

However, when the sensing field is too far from the base station, transmitting the data over long distances using multihop may further weaken the security. The intermediate may modify the data passing by capturing of sensor nodes, launching a wormhole attack [2], sybil attack [3], selective forwarding and sinkhole [4] attack. Forwarding data to base station would increase 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 better option in the operation of many sensor network applications, including data collection in hazardous environments [5], localized reprogramming, oceanographic data collection, and military applications.

Therefore, the security in sensor network is extremely important. Many security algorithms have been designed for wired and wireless networks but they cannot be used in wireless sensor networks because of the limited energy, memory and computation capability. Key management protocols are the basis of the secure communications and are the fundamental security mechanism in wireless sensor network [6].

Motivation: Public key encryption techniques are expensive for a WSN due to the higher coputation and

978-1-4799-1823-2/15/$31.00 ©2015 IEEE

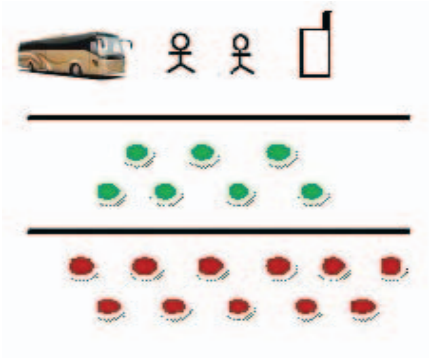

Fig. 1. Three tier security scheme

storage cost. Various authentication and key predistribution based on symmetric schemes exists for sensor networks. Data gathering or reprogramming sensor networks using mobile sinks has the problem of authentication and key establishment among these sensor nodes. In the solutions based on the basic probabilistic and q-composite key pre distribution schemes, when a small set of sensor nodes is compromised the attacker can easily obtain a large number of keys. Thus an attacker can 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 to make pair between sensor nodes and Mobile Sinks based on the polynomial pool-based key predistribution 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. In addition during the process of making pair between the nodes for data transmission shortest path is selected.

Contributions: The three-tier security scheme is robust against mobile sink replication attack and stationary access node replication attack, as this scheme makes use of a one-way hash chains algorithm along with the static polynomial pool based scheme. There is no method to decide which pair of nodes is better to communicate through stationary access nodes. The main problem with this is the communication overhead, and as a result of this it takes a considerable amount of time. However, establishing pair wise keys in wireless sensor networks is not a trivial task, particularly due to the resource constraints on sensors. So in order to overcome these drawbacks, we have developed a efficient three tier scheme with shortest distance for communication which takes less time to establish a communication and transmit data.

Organization: The remaining part of the paper is organized as follows: Related works are presented in section II. Background is discussed in section III. Preliminaries discussing the network model and adversary model is presented in section IV. Section V describes problem definition and algorithm. Implementation and performance evaluation is shown in section VI. Finally, section VII gives the conclusions of the paper.

II. Related Works

Recently, many researchers have been engaged in developing schemes that address the unique challenges in security of WSNs. Zia and Zomaya [7] have made an effort to document the security issues in WSNs. Attacks, countermeasures and threat models have been proposed in different layers.

Key distribution for the sensor network is extensively studied. Generally two approaches are given. One is key distribution at the initial network deployment stage through a Base station and and the other is key predeployment. Zhu *et al*., [8] have proposed a key management protocol, Localized Encryption and Authentication Protocol (LEAP), that offers many security benefits to WSNs. It employs one base station and assumes it to be trustworthy. It does not include defence against hacked or compromised base station. Delan Alsoufi *et al*., [9] have proposed a solution in order to overcome the security issue with one base station by employing multiple base stations.

One of the main concerns when designing a key management scheme is the network scalability. Yu *et al*., [10] have proposed a new scalable key management scheme for WSNs, which provides a good secure connectivity coverage. For this purpose, they make use of the unital design theory. They show that the basic mapping from unitals to key pre-distribution allows one to achieve high network scalability. Nonetheless, this naive mapping does not guarantee a high key sharing probability. Walid Bechkit *et al*., [11] propose an enhanced unital-based key pre-distribution scheme providing high network scalability and good key sharing probability.

Blundo *et al*., [12] proposed a key distribution scheme for dynamic conferences, a method by which initially an (off-line) trusted server distributes private individual pieces of information to a set of users. In this setting, any group of t users can compute a common key by each user computing using only his private piece of information and the identities of the other t - 1 group users. Keys are secure against coalitions of up to k users, that is, even if E users pool together their pieces they cannot compute anything about a key of any t-size conference comprised of other users. The polynomial-based scheme proposed applies to settings where a limited coalition of up to a certain security parameter k of adversaries are expected. A basic application is a secure conference key generation.

Donggang Liu and Peng Ning ., [13] have developed two pair wise key pre distribution schemes, a closest pair wise

keys pre distribution scheme and a location-based pair wise keys scheme using bivariate polynomials, by taking advantage of sensors expected locations. Establishment of pair wise keys is a fundamental security service, which forms the basis of other security services such as authentication and encryption. This paper presents several techniques for establishing pair wise keys in static sensor networks. These techniques take advantage of the observation that in static sensor networks, although it is difficult to precisely pinpoint sensors positions, it is often possible to approximately determine their locations.These schemes can achieve better performance if such location information is available and that the smaller the deployment error (i.e., the difference between a sensors actual location and its expected location) is, the better performance they can achieve.

III. Background

WSN mainly face the problem of mobile sink replication attack. To overcome this problem, Amar Rasheed and Rabi N. Mahapatra [14] proposed an efficient three tier security framework for authentication and pair wise key establishment, based on polynomial pool based key pre-distribution scheme. This technique is able to give network resilience to mobile sink replication attacks. They preselect few sensor nodes as stationary access nodes, which acts as authentication access points that are capable of making the sensor nodes to send their data to mobile sinks. They use two separate polynomial pools: a mobile polynomial pool and a static polynomial pool. Authentication between mobile sinks and stationary access nodes are established by polynomials from the mobile polynomial pool. Polynomials from the static polynomial pool are used to ensure the authentication and keys setup between the sensor nodes and stationary access nodes.Our work present an efficient pairwise key establishment among the set of polynomials that match between the two levels with the shortest path.

IV. Preliminaries

This section presents our network model, assumptions made about the network and the anticipated adversary.

A. Network Model

The proposed scheme uses Blundo scheme [12] based on polynomial pools. Polynomial pool-based key predistribution uses a polynomial pool instead of a single polynomial key pool. Polynomials from the mobile polynomial key pool are used to establish authentication among mobile sinks and stationary access nodes to gain access to the network for the sensor data gathering. Polynomials from the static polynomial pool are used for authentication and keys setup between the sensor nodes and stationary access nodes. Before deployment a random subset of polynomials from the mobile polynomial pool is given to mobile sinks, and a small set of sensor nodes called as stationary access nodes are given a polynomial from mobile polynomial pool. To launch a mobile replication attack an attacker has to get atleast a single polynomial from mobile polynomial pool to gain access to the network. Similarly all sensor nodes and stationary access nodes are given a random subset of polynomials from static polynomial pool. The stationary access nodes, allow mobile sinks to access the sensor network for data gathering. Thus, an attacker would need to compromise at least a single polynomial from the static pool to make a stationary access node replication attack.

- A mobile sink sends data request messages to the sensor nodes through a stationary access node.
- The mobile sinks data request messages will initiate the stationary access node to trigger sensor nodes to transmit their aggregated data to the requested sink.

We assume a network that is composed of large number of homogeneous sensors. The two senors can communicate with each other directly or via other sensor after key match. Keys can be matched in different ways that is we can have (i) direct key discovery. (ii) Indirect key discovery through intermediate stationary node or (iii) Indirect key discovery through intermediate stationary access node .

V. Problem Definition and Algorithm

Since sensor nodes are deployed in harsh, unattended remote areas wireless sensor networks are susceptible to various security attacks due to lack of tamper resistance, sensor node failures, limited processing capabilities and non-availability of human assistance. Since communication is wireless, secure ways for communicating data are not available. Hence a user can enter the network and obtain data for the event of his interest by compromising sensor nodes. Given a sensor network with mobile sinks instead of a base station, data can be gathered from the stationary nodes through access nodes using mobile polynomials in a secure way through a shortest path .

A. Algorithm

The algorithm consists of three phases:
(i) Static and mobile polynomial key predistribution
(ii) Key discovery between mobile node and stationary node
(iii)Selecting shortest path among the feasible paths

1) Polynomial Key Predistribution: Given a sensor network, let N =$\{ N_1, N_2, N_3, \ldots, N_n \}$ be a set of *n* stationary sensor nodes. S =$\{ S_1, S_2, S_3, \ldots, S_m\}$ be a set of *m* stationary access nodes and MS =$\{ MS_1, MS_2, MS_3, \ldots, MS_r \}$ be a set of *r* mobile sinks. A mobile polynomial pool *M* and a static polynomial pool *S* are generated.The mobile sinks and stationary access nodes are randomly given K_m and one polynomial ($K_m > 1$) from M. The 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.

2) Key discovery between mobile node and stationary node: The pairwise key between sensor node *u* and mobile sink *v* is established by a stationary access node *a*. A sensor node *u* needs to find a stationary access node *a* in its neighborhood, such that, stationary node *a* can establish pairwise keys with both mobile sink *v* and sensor node*u*. That is, a stationary access node needs to establish pairwise keys with both the mobile sink and the stationary node. To achieve this node *a* has to find a common mobile polynomial with the mobile sink and a common static polynomial with the sensor node. For this sensor node will broadcast a list of polynomial IDs. When a secure path is established between nodes *u* and *v*, the mobile sink *v* sends the pairwise key k_c to node *a* in a message encrypted and authenticated with the shared pairwise key k_{va} 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_{au} between *a*and *u*.

When there is no direct key establishment between the mobile sink and the sensor node then the key establishment is done through intermediate nodes. To establish a secure direct path their should be a stationary access node which shares a common mobile polynomial with mobile sink and a common static polynomial with sensor node. If no such direct path is established it is done through an intermediate stationary access node.

3) Selecting the shortest path: The key establishmen through direct or intermediate nodes may have more than one path between the sensor node and the mobile sink. We use the shortest path calculated with Dijkstra algorithm to use shortest distance. In other words, if the mobile polynomial key match between mobile sink and stationary access node and static polynomial key match between stationary nodes and stationary access nodes exist with different intermediate nodes then a shortest path is selected.

B. Security Analysis

VI. Implementation and Performance Evaluation

A. Simulation Setup

We evaluate the performance of our scheme by simulation and compare it with earlier schemes. The simulation was run using $MATLAB$. Nodes are randomly deployed into $100\times100m^2$. The region is divided into 10×10 cell units. Nodes are randomly distributed and ensured that the number of sensor nodes is greater than stationary access nodes eand number of stationary access nodes are greater than mobile sinks. Static and mobile polynomials are distributed before deployment. Events are randomly simulated in later stages for mobile replication and stationary access node replication attack. The results show the comparison with previous schemes

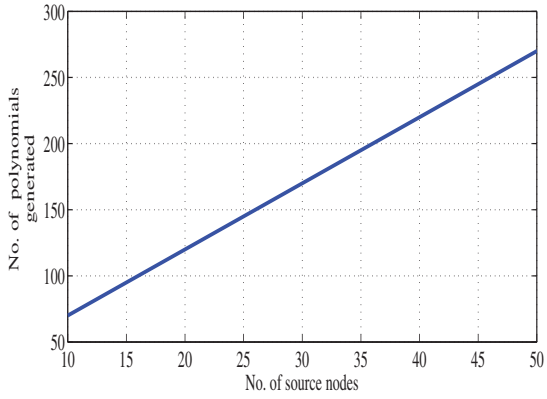

Fig. 2. Number of source node v/s no. of polynomials generated

B. Results and Analysis

Figure 2 depicts that as the number of sensor nodes in the network increases the polynomials generated in the polynomial pool also increases. If x is the number of sensor nodes present in the network then (5*x)+20 number of polynomials are generated in the polynomial pool. Hence the number of polynomials generated increases linearly with the increase of the number of nodes. Since the number of polynomials increases the Attacking becomes difficult with few compromised nodes..

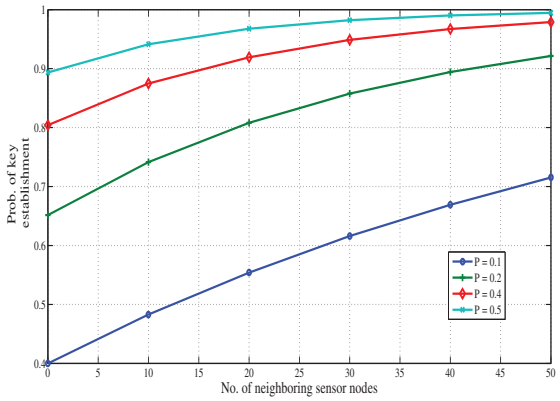

Fig. 3. Number of Neighboring sensor nodes v/s probability of key establishment

Figure 3 depicts the Probability of a mobile sink establishing a pairwise key with a sensor node versus the number of sensor neighbours.The probability *P* of a mobile sink and a sensor node establishing a pairwise key (directly or indirectly) is estimated and for different values of Probability the results are obtained.

Figure 4 gives the comparison of the our proposed TLKP scheme with [14]. The time taken for data transmission and connection establishment when a Shortest path Algorithm is used with that when not used is seen in the figure 4. When a

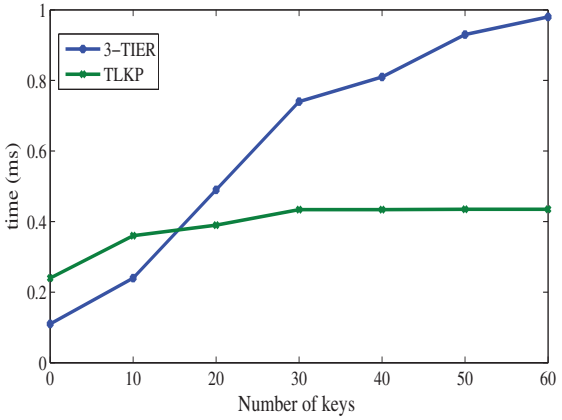

Fig. 4. Number of Keys v/s Time

Shortest Path Algorithm is not used the time increases with the increase in the distance between the source and the destination which is indicated in the graph. This is due to the selection of mobile sink and sensor node with a first polynomial key match. Whereas, when any Shortest Path Algorithm like Dijkstras Algorithm is used the time taken for data transmission and key establishment is reduced with the higher probability for key mathes. When their exists many paths direct or indirect shortest path is selected. So by using Shortest Path Algorithms we can reduce the time taken for data transmission and connection establishment for longer distances.

VII. Conclusions

In wireless sensor networks security and privacy support with minimum cost is a major concern. Authentication and key establishment of mobile sink nodes by the sensor network has been addressed due to the problem of mobile sing replication attacks. In this paper we have proposed a technique that supports security using three level polynomial key predistribution to overcome mobile replication attack and stationary access node replication attack. Also as the communication time is prime concern we achieve by reducing the number of hops and considering the minimum distance among the three levels. This can be seen in the simulated results.

References

[1] Akyildiz I, Su W, Sankarasubramaniam Y and Cayirci, "Wireless Sensor Networks ': A Survey," *Computer Networks,* vol. 38, no. 4, Mar 2002.

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

[3] Douceur J R, "The Sybil Attack, *Proc. First Intl Workshop Peer-to-Peer Systems ,",* vol. 38, no. 4, Mar 2002.

[4] Deng H,Li W, and Agrawal D.P, "Routing Security in Wireless Ad Hoc Networks," *Proc. IEEE Comm. Magazine,* pp. 70-75, 2002.

[5] Tanuja R, Sukeerthi B J, Apoorva Raju, Manjula S H, Venugopal K R, Patnaik L M, "SDCS : Secure Data Centric Sensor Networks with Multi-query Optimization," *Proc. IEEE Conf. (INDICON 2013),* Dec 2013.

[6] Choi K J and Song J, "Investigation of Feasible Cryptographic Algorithms for Wireless Sensor Network," *Proceedings of δ^{th} International Conf. on Advanced Communication Technology (ICACT 2006)* , pp.1379-1381, Feb 2006.

[7] Tanveer Zia and Albert Zomaya, "Security Issues in Wireless Sensor Networks," *Proc. Intl Conf. Systems and Networks Communication (ICSNC 06),* Oct.2006.

[8] Zhu S, Setia S and Jadojia S, "LEAP+ : Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *ACM transactions on Sensor Networks,* vol. 2, pp.500-528, Nov. 2006.

[9] Delan Alsoufi, Khaled Elleithy, Tariq Abuzaghleh and Ahmad Nassar, "Security in Wireless Sensor networks : Improving the LEAP protocol ," *International Journal of Computer Science and Engineering Survey (IJCSES)* vol.3, no.3, June 2012.

[10] Yu Z and Guan Y, "A Key Management Scheme Using Deployment Knowledge for Wireless Sensor Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol.19, no.10, pp.1411-1425, Oct.2008.

[11] Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah and Vahid Tarokh, "A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks," *IEEE Transactions on Wireless Communications* vol.12, no.2, Feb 2013.

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

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

[14] Amar Rasheed and Rabi N. Mahapatra, "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks," *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS* vol.23, no.5, MAY 2012.