ENHANCED THREE TIER SECURITY ARCHITECTURE FOR WSN AGAINST MOBILE SINK REPLICATION ATTACKS USING MUTUAL AUTHENTICATION SCHEME

Linciya.T[1] and Anandkumar. K.M[2]

[1]P.G Scholar, Department of Computer Science and Engineering, Easwari Engineering College, Chennai, India
linciya.thomas@gmail.com

[2]Assistant Professor (Sl.Gr.), Department of Computer Science and Engineering, Easwari Engineering College, Chennai, India
kmanandmss@gmail.com

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. Wireless sensor nodes are restricted to computational resources, and are always deployed in a harsh, unattended or unfriendly environment. Therefore, network security becomes a tough task and it involves the authorization of admittance to data in a network. 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. To determine the above problem the system adduces the three-tier security framework for authentication and pair wise key establishment between mobile sinks and sensor nodes. The previous system used the polynomial key pre distribution scheme for the sensor networks which handles sink mobility and continuous data delivery to the neighbouring nodes and sinks, but this scheme makes high computational cost and reduces the life time of sensors. In order to overcome this problem a random pair wise key pre distribution scheme is suggested and further it helps to improve the network resilience. In addition to this an Identity Based Encryption is used to encrypt the data and Mutual authentication scheme is proposed for the identification and isolation of replicated mobile sink from the network.

KEYWORDS:

Wireless Sensor Network, Pair wise Key Establishment, Random Key Pre distribution, Mobile Sink, ID Encryption, Mutual Authentication Scheme.

1. 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 large number of small autonomous devices are embedded in the sensors which are interconnected to

DOI : 10.5121/ijwmn.2013.5207

form a sensor network. The WSN make use of a number of sensor nodes within or neighbouring the area of event to not only collect and integrate but also process and relay the information. Sensor nodes are equipped with integrated sensors that has the capability to process the collected data and for short range radio communication. The randomly deployed sensor nodes in the area of scrutiny collect the sensor data in typical application scenarios.

In application such as military sensing and tracking, environment monitoring, patient monitoring and tracking, smart environment, etc are sensed by the deployed sensor. Those sensors are interconnected to form the sensor network and are deployed in hostile environment where they are prone to different malicious attack. There are various attacks in the WSN. For example, messages can me spoofed during the transit and then the copy of the message can be sent to the recipient in the altered form. One can also intrude with a node and alter its behaviour. The types of counter measures can be addressed by different types of attacks.

The most formidable attack in wireless sensor network is the replication attack. The attacker compromises a node and uses its secret cryptographic key materials to effectively colonize the network with the clones of it. Foe collects all the credentials like keys, identity etc once the node has been captured. Those captured credentials are reprogrammed by the attacker and the nodes are replicated using those credentials in order to eavesdrop the transmitted messages or compromise the functionality of the network. The replication attack is carried in two ways: mobile sink replication attack and stationary access node replication attack. There are some solutions available for stationary access point replication attack compare with mobile sink replication attack. Many important functions of the sensor network such as routing, resource allocation, misbehaviour detection, network resilience, throughput etc are remarkably injurious by replication attack. The above problem of replication attack can be solved through polynomial pool pr distribution scheme.

There are number of key pre distribution schemes for solving the problem of authentication and pair wise key distribution which do not exhibit desirable network resilience. The breach of security in one node makes the entire sensor network unsafe. The new security challenge for data collection is by avocation of pair wise key establishment and authentication in the mobile sinks. In the basic probabilistic and q-composite key pre distribution schemes, the attacker gain the control of entire network by deploying a replicated mobile sink preloaded with some compromised keys. Those compromised keys can be achieved by an attacker by obtaining large number of keys by capturing a small fraction of nodes.

To handle the afore-said problem, we use pair wise key pre distribution scheme that provide authentication and pair wise key establishment amid sensor nodes and Mobile Sink. To expedite the study of a new security technique, a general three-tier security agenda is established for authentication and pair wise key establishment, based on the polynomial pool-based key pre distribution scheme.

In polynomial pool-based key pre distribution scheme both mobile sink and stationary access point generates the separate subset of keys which results in the high computational cost. In order to overcome this problem Random pair wise pre distribution scheme is used to reduce the computational cost and provides security against the replication attacks in the proposed system. In Random pair wise pre distribution scheme only mobile sink generates a key with key identifiers and broadcasted to stationary access point and sensor node. Fig 1 represents the system architecture of the prospective system.

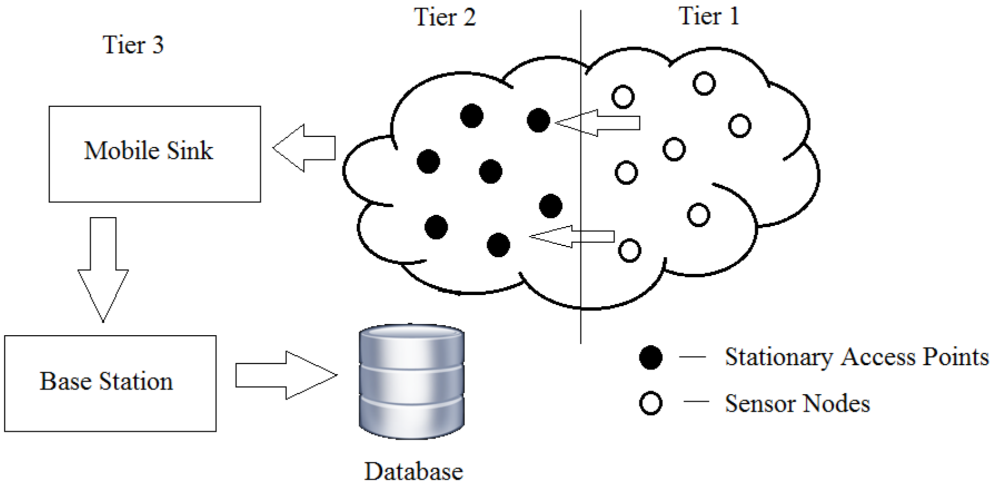


Fig 1. System Architecture

The rest of the paper is organized as follows. Section 2 discusses the previous work on related topics and Section 3 gives the models and assumptions. Section 4 describes proposed Random Pair wise Pre distribution in detail. Section 5 discusses the encryption algorithm. Section 6 discusses the analysis results and Finally, Section 7 concludes the paper.

2. RELATED WORKS

A comprehensive literature review was carried out on node replication attacks and other security issue in static and mobile wireless sensor networks. This literature survey revealed versions mathematical and operational methods for solving the problems. The key management problem is a progressive research area in wireless sensor networks. Eschenauer and Gilgor [4] proposed a probabilistic key pre distribution scheme which helps to bootstrap the initial trust between the sensor nodes. The discriminative distribution and countermanding of keys to sensor nodes and node re-keying without substantial computation and communication capabilities are briefly explained in this scheme. For the random subset of keys from a large key pool before deployment, the probabilistic key pre distribution scheme is used. As an outcome, two nodes have assured a prospect to share at least one key after deployment.

The characteristic of network connectivity and security can be poised by key management scheme. The core idea is the sensor node randomly picks a set of keys from a key pool before deployment, so that any two sensor nodes had a certain prospect to share at least one common key. The problem existing in this key pre distribution is the probability of establishing a common key between communicating nodes, and the ability to tolerate compromised nodes is highly dependent on the memory available on the sensor nodes. In other words, these schemes still require each node to be assigned a large number of keys for a high-performance WSN, and some solutions for this problem focus on pre deployment knowledge, post deployment knowledge, the state of the sensors, and overlapping key strings. However, these solutions are not quite viable since their key sharing mechanism is not enough to be efficient. One of the most important information is the signal range of the sensor node that might significantly improve the performance of the key sharing mechanism however, this is not exploited in these schemes.

Liu et al.[3] The sensor nodes are communicated securely with each other using cryptographic techniques by enabling bi variate key polynomial. This is one of the most primary security services. The resource constraints of the sensor nodes makes it not feasible for sensors to use key polynomial scheme. The scheme assures a direct key established between any two neighbour sensors in any deployment group. Better trade-off is achieved between communication overhead, network connectivity and security against node capture compared to the existing key pre-distribution schemes. Ultimately, it also supports dynamic node addition after the initial deployment of the nodes in the network.

Chan et al. [2] further unmitigated this proposal and developed two key predistribution schemes: the q-composite key predistribution scheme and the random pairwise keys scheme. In q-composite key predistribution scheme two sensor nodes are required to compute compute a pairwise key from the shared q predistributed keys. In random pairwise keys scheme pair of sensor nodes are randomly picked and assign each pair a unique random key. Comparing to the basic probabilistic key predistribution scheme the above schemes improved the security. They developed a general scaffold for pairwise key establishment using the polynomial-based key pre distribution protocol [5] and the probabilistic key distribution in [6] and [7]. Tolerating not more than t compromised node, where the value of t was limited by the memory available in the sensor nodes can be carried in this scheme.

Amar Rasheed et.al [1] developed for group key pre distribution. The pair wise key establishment in the context of sensor networks is the ultimate aspiration. This system is unreservedly secure and t-collusion resistant. The network resilience is significantly improved to the mobile sink replication attack. The small fraction of preselected sensor nodes are called as sensor nodes. In this new security agenda, stationary access nodes act as an authentication access point to a network to elicit the sensor node to transmit the collected to the mobile sink. The data request message from the mobile sink to sensor node is transmitted through stationary access node. These data request will elicit the sensor node to transmit the data from sensor node to mobile sink through stationary access point.

3. MODELS AND ASSUMPTIONS

3.1 Network Model

We consider a sensor networks, where a large number of sensor nodes are randomly distributed in the two dimensional area and remain stationary after deployment, and all of them have similar capabilities and equal significance. One sink which has the mobility named as mobile sink which collects the data from all other sensor nodes. Each sensor node sends its data packets to sink nodes through access point. For the secure data transmission we go three tier security scheme.

3.2 Three Tier Security Scheme

The two separate polynomial pools are used in three tier security scheme: the mobile polynomial pool and the static polynomial pool. For data gathering from the sensor through the mobile sink the polynomials from mobile polynomial pool are used. To gain access to the network for the sensor's data gathering, an attacker needs to compromise at least a single polynomial. For key setup between the sensor nodes and stationary access nodes the polynomials from static polynomial pool are used.

Afore mention to deployment, The subset of polynomials from the mobile polynomial pool is picked by each mobile sink. The randomly selected sensor nodes called stationary access nodes carry a polynomial from the mobile polynomial pool. These nodes acts as the authentication point for the network which triggers the sensor node to transmit the data. The data request is transmitted to sensor node from the mobile sink through stationary access node. This data request will initiate the sensor node to transmit the collected data. Every stationary access node may share a mobile polynomial with a mobile sink. The subset of polynomials from both static and mobile polynomial pool is randomly picked by stationary access point and sensor node. The main benefit to use separate pools is the mobile sink authentication is autonomous of the key distribution scheme used to unite the sensor network

3.2.1 Key Discovery between a Mobile Sink and a Sensor 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 neighbourhood, such that, node a can establish pair wise keys with both mobile sink v and sensor node u. Fig 2 shows a direct secure path establishment between nodes u and v, mobile sink v sends the pair wise key to node a in message encrypted and authenticated with the shared pair wise key ;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 to node u in a message encrypted and authenticated with pair wise key; u between a and u.

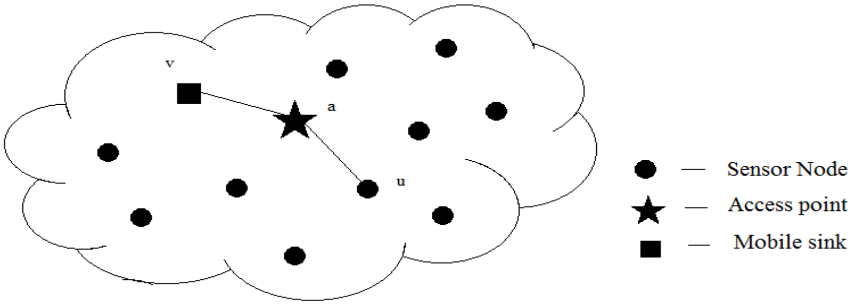


Fig 2. Direct Key Establishment

Fig 3 illustrates that the mobile sink and the sensor node will have to establish a pair wise key with the help of other sensor nodes using indirect key discovery. To establish a pair wise key with mobile sink u, a sensor node v has to find a stationary access node a in its neighbourhood 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).

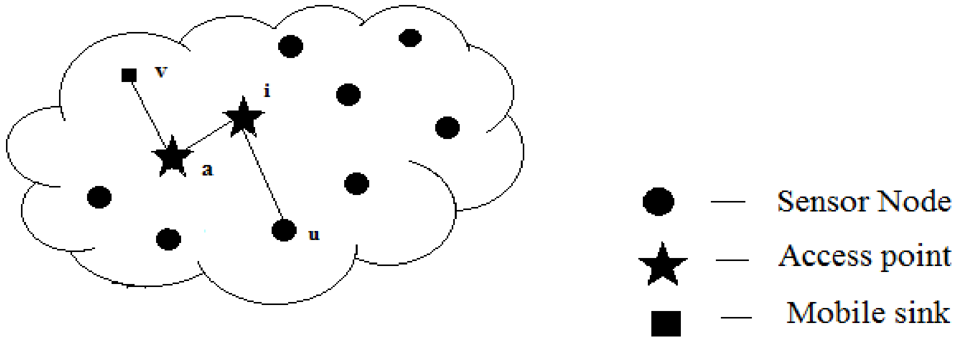


Fig 3. Indirect Key Discovery through Intermediate Stationary Access Node

Fig 4 shows that the mobile sink and the sensor node will have to establish a pair wise key with the help of other sensor nodes using indirect key discovery. To establish a pair wise key with mobile sink u, a sensor node v has to find a stationary access node a in its neighbourhood 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 sensor 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).

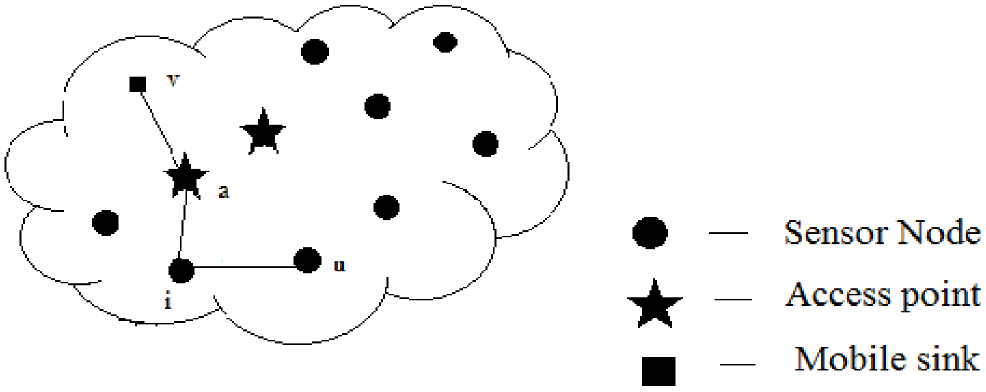


Fig 4. Indirect Key Discovery through Intermediate Stationary Node

4. RANDOM PAIR WISE KEY PRE DISTRIBUTION

In this section, we first list phases for pair wise key setup in Random Key Pre distribution (RKP) schemes

A. Phases in Random Key Pre distribution Schemes

Four main phases for key setup in RKP schemes are presented as follows.

1. Key pre distribution phase:

   A mobile sink has a polynomial pool.

   - generate a large key pool of size ;
   - different keys for each sensor from the key pool to form a key ring are selected randomly;
   - In the memory of the sensor the key ring is loaded.
   - Each sensor is loaded with unique node identifier or key identifier.

2. Sensor deployment phase:

   Sensors are erratically picked and uniformly dispersed in a large area. Typically, the average number of neighbors of a sensor is much smaller than the total number of deployed sensors.

3. Key discovery phase:

   Two steps are involved in the key discovery phase. In the first step, each sensor attempts to discover shared key(s) with each of its neighbors. To accomplish this, the sensor can broadcast its key ring identifier to its neighbours. After the first step of the key discovery phase, the sensor knows all its neighbors. The set of all neighbors of sensor is represented by W_i and $| W_i|=n'$. The set of neighbours of sensor i who share at least one key with the sensor i is represented by R_i. Thus, we have $W_i = Q_i \cup R_i$ and $|Q_i|+| R_i|= n'$. In the second step, every sensor i broadcasts its set Q_i. Using the sets received from neighbors, a sensor can build a key graph based on the key-share relations among neighbors.

4. Pair wise key establishment phase:

   If sensor shares at least one key with a given neighbor, the shared key(s) can be used as their pair wise key(s).

In the proposed system the random pair wise key is used for the security and for reducing the computational cost. Figure 5 shows the functional architecture for the three tier security scheme. Sensor nodes collect the data from the remote area and send to the mobile sink. The data that are collected from sensor node is forwarded to access point which in turn sent to mobile sink. For secure transmission of data we generate keys from the polynomial pool. The key is generated in sensor node then it encrypt the collected data using the generated key and transfer it to the mobile sink.

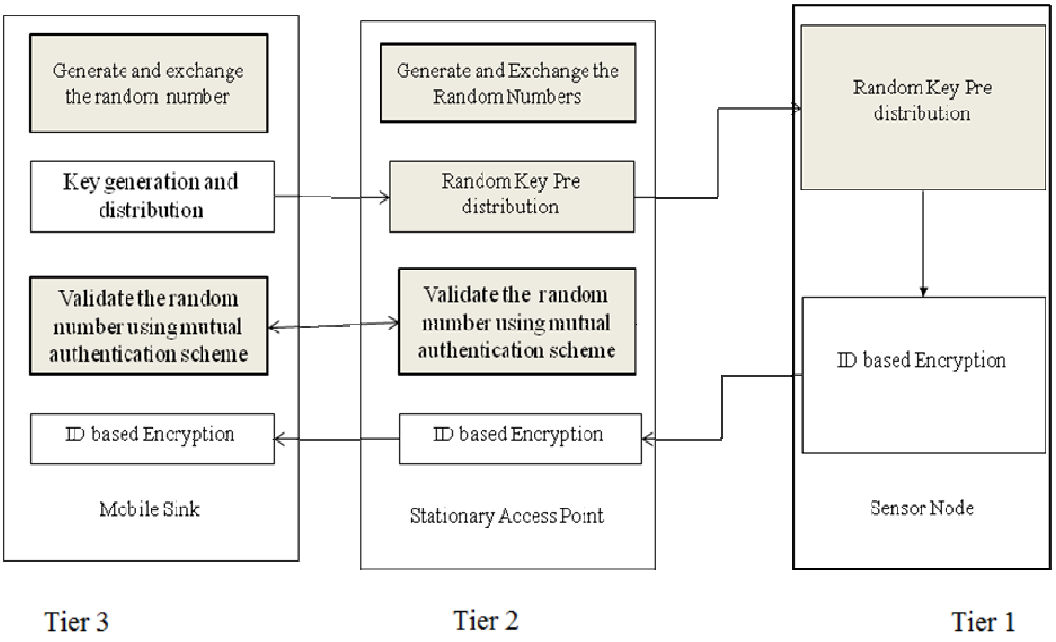

Generate and exchange the random number
Key generation and distribution
Validate the random number using mutual authentication scheme
ID based Encryption
Mobile Sink
Generate and Exchange the Random Numbers
Random Key Pre distribution
Validate the random number using mutual authentication scheme
ID based Encryption
Stationary Access Point
Random Key Pre distribution
ID based Encryption
Sensor Node
Tier 3
Tier 2
Tier 1

Fig 5. Functional Architecture of the Proposed System

For the encryption of the data using the key ID based encryption algorithm is used. For the ID based encryption algorithm its essential for the private key generator which is to be located in the base station from which the master key to be stored in the mobile sink.

5. ID BASED ENCRYPTION ALGORITHM

ID-based public key infrastructure involves a trusted Key Generation Center (KGC), and users. The basic operations consist of **Set Up** and **Private Key Extraction**. KGC runs BDH parameter generator to generate two groups G_1,G_2 and a bilinear pairing e: $G_1 \times G_1 \rightarrow G_2$. Itchooses an arbitrary generator P ε G_1 and defines two cryptographic hash functions:

$$H_1 : \{0,1\}^* \rightarrow G_1,$$
$$H_2 : \{0,1\}^* \rightarrow G_2.$$

- **Set Up:** KGC chooses a random number s ε Z_q^* and set P_{pub}=sP . Then the KGC publishes system parameters params={G_1,G_2,q,P,P_{pub},H_1,H_2}, and keep s as master-key.

- **Private Key Extraction:** An identity information ID to KGC is submitted by the user. The user's public key is computed by KCG as $Q_{ID}=H_1(ID)$ and reversion private key as $S_{ID}= sQ_{ID}$.

The holder of private key S_{ID} to decrypt a message sent to her under the public key $Q_{ID.}$
Let m denote the message to be encrypted.

- **Encryption:**
Compute U=rP where r $\varepsilon_R Z_q^*$. Then compute

$$V = m \oplus H_2(e(P_{pub}, rQ_{ID})) \qquad (1)$$

Output the cipher text (U,V)

- **Decryption:**

  Decryption is performed by computing

$$V\oplus H_2(e(U,S_{ID})) = V \oplus H_2(e(rP,sQ_{ID})) \quad (2)$$
$$= V \oplus H_2(e(sP,rQ_{ID})) \quad (3)$$
$$= V\oplus H_2(e(P_{pub},rQ_{ID})) \quad (4)$$
$$= m$$

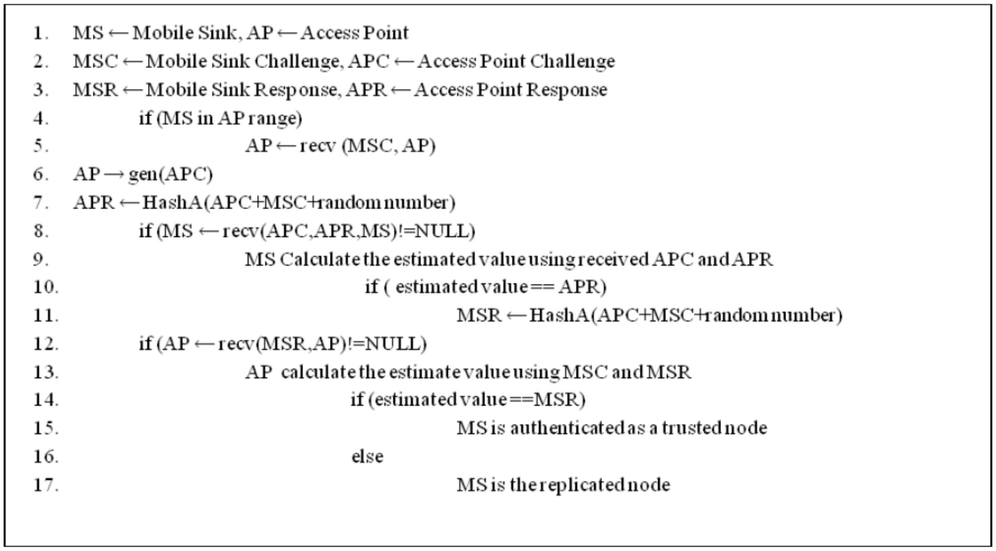
The node ID is used for the creation of the private key and public key for the secure transmission of data from the sensor node to the mobile sink. Hence ID based encryption algorithm is adhibited for the encryption and decryption of the data.

6. Mutual Authentication Scheme

Challenge–response authentication is an authentication process by verifying an identity using the required authentication information. This authentication information is usually a value and that are to be computed in response for inevitable challenge. Challenge–response authentication helps to crack the problem of exchanging session keys for encryption. This is chiefly effective for man-in-the-middle attack, because without knowing the secret the attacker will not be able to derive the session key. Through this protocol we are able to state things other than the secret value. Every challenge–response sequence is unique to ensure a challenge by employing a cryptographic nonce in the authentication protocol.

Mutual authentication is percolated using a challenge–response handshake in both directions. Mutual authentication is the process to authenticate the both ends of transmission that is authentication between sender and receiver. This is the basic function for both private and public communication. It is also known as two-way authentication where two parties authenticating each other suitably. It refers to a one node authenticating themselves to another node and that node authenticating itself to the first node in such a way that both parties are assured of the others' identity.

Mutual authentication scheme is anticipated in this paper for identifying the replicated mobile sink. Figure 6 describes the pseudo code for mutual authentication scheme. Mobile Sink (MS) sends mobile sink challenge (MSC) to the Access point (AP). AP generates the challenge and Access point response (APR) calculates the hash function using APC, MSC and the random number. If MS receives is not equal to null then MS calculates the estimated value using APC and APR. If the estimated value equal to APR then mobile sink response (MSR) evaluates the hash function using APC, MSC and random number. If AP receives MSR and AP is not equal to null then AP calculates the estimated value using MSC and MSR. If the estimated value equals to MSR then MS is authenticated as a trusted node or else MS is the replicated node.



```
MS ← Mobile Sink, AP ← Access Point
MSC ← Mobile Sink Challenge, APC ← Access Point Challenge
MSR ← Mobile Sink Response, APR ← Access Point Response
        if (MS in AP range)
                AP ← recv (MSC, AP)
AP → gen(APC)
APR ← HashA(APC+MSC+random number)
        if (MS ← recv(APC,APR,MS)!=NULL)
                MS Calculate the estimated value using received APC and APR
                        if ( estimated value== APR)
                                MSR ← HashA(APC+MSC+random number)
        if (AP ← recv(MSR,AP)!=NULL)
                AP  calculate the estimate value using MSC and MSR
                        if (estimated value==MSR)
                                MS is authenticated as a trusted node
                        else
                                MS is the replicated node
```

Fig 6. Pseudo code for Mutual Authentication Scheme

7. RESULT ANALYSIS

The proposed scheme has been implemented and analysed in the network simulator NS2. The possible outcomes when there is a change in the key size is to be determined. The various sets of key size is given and the change of key size broadcasted from mobile sink to stationary access node and stationary access node to sensor node is to be determined. Table 1 shows the calculation of broadcasting the key from the mobile sink to stationary access node and stationary access node to sensor node.

Table 1. Calculation of Broadcasting the Key of Various Size

Size of Key Generated in Mobile Sink	Size of Key Broadcasted to Stationary Access Node	Size of Key Generated in Stationary Access Node	Size of Key Broadcasted to Sensor Node
5	4	5	4
10	9	10	9
20	19	20	19
30	29	30	29
40	39	40	39

If the key size is larger it should be stored in a disk file which can be discovered by someone else. Thus large key size is not only convenient to use but also it is a security risk. It considerably takes longer time to encrypt and decrypt messages and broadcast the generated key. So it is convenient to use the smaller key size. The key size used in this project is 4 (32 bit). Thus the following analysis shows that as the size of the polynomial pool increases the probability of sharing the key size also increases

The key is generated in the static polynomial pool and it is broadcasted to the sensor node. Fig. 7 and Fig. 8 represent the sharing of the key from static polynomial pool to the stationary access node and sensor node.

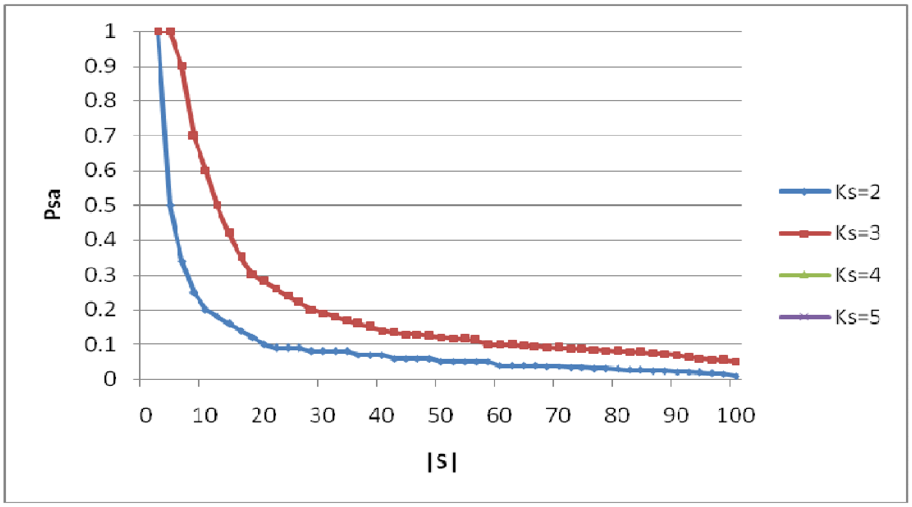


Fig 7. The probability $\boldsymbol{P_{sa}}$ that a sensor and stationary access node share a static polynomial versus the size $|\boldsymbol{S}|$

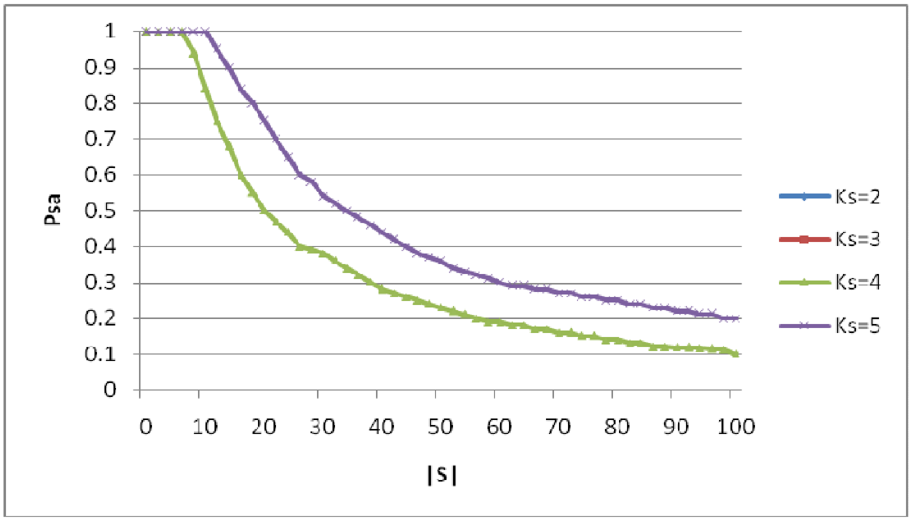


Fig 8. The probability $\boldsymbol{P_{sa}}$ that a sensor and stationary access node share a static polynomial versus the size $|\boldsymbol{S}|$.

7. CONCLUSIONS

The security performance of the three tier scheme can be carried out 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.

The network resilience is significantly improved to the mobile sink replication attack using random pair wise key pre distribution compared to single polynomial pool-based key pre distribution approach. The use of key pools and stationary access nodes that carry polynomials from the mobile pool of the network will inhibit an attacker from collecting sensor data, by deploying a replicated mobile sink. The proposed key distribution scheme reduces the computational cost in the nodes.

REFERENCES

[1] Amr Rasheed, Rabi Mahapatra. N. (2012) ‘The Three-Tier Security Scheme in Wireless Sensor Network with Mobile Sinks’ IEEE Transactions on Parallel and Distributed system, IEEE Computer Society, VOL. 23, NO. 5, pp 958-965.

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

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

[4] L. Eschenauer and V.D. Gligor(2002) “A Key-Management Scheme for Distributed Sensor Networks,” Proc. ACM Conf. Computer Comm. Security, pp. 41-47.

[5] H. Chan, A. Perrig, and D. Song(2004), “Key Distribution Techniques for Sensor Networks,” Wireless Sensor Networks, Kluwer Academic, pp. 277-303.

[6] D. Liu and P. Ning,(2003) “Location-Based Pairwise Key Establishments for Static Sensor Networks,” Proc. First ACM Workshop Security Ad Hoc and Sensor Networks.

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

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

[9] H. Deng, W. Li, and D.P. Agrawal,(2002) “Routing Security in Wireless Ad Hoc Networks,” Proc. IEEE Comm. Magazine, pp. 70-75.

[10] Parno B, Perrig A, Gligor V.(2005) “Distributed Detection of Node Replication Attacks in Sensor Networks” In: Proceedings of the IEEE Symposium on Security and Privacy; pp.49-63.

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

[12] M.Conti, R. Di Pietro,L.V. Mancini and A. Mei (2007)“A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks” In ACM MobiHoc, pages 80-89.

[13] Jun-Won Ho, Donggang Liu, Matthhew wright (2009) “ Distributed Detection of replica node attacks with group deployment knowledge in wireless sensor networks”, Ad Hoc Networks, pp:1476-1488.

[14] Chia-Mu, Chun-Shien, Lu., and Sy-Yen Kuo (2008) “Mobile Sensor Network Resilient Against Node Replication Attacks”, SECON ’08. 5th Annual IEEE communications Society conference, pp.597-599.

[15] Chia-Mu, Chun-Shien, Lu., and Sy-Yen Kuo (2009) “Efficient Distributed and Detection of Nodes Replication Attacks in Mobile Sensor Networks”, IEEE 2009.

[16] A. Rasheed and R. Mahapatra,(2007) “An Energy-Efficient Hybrid Data Collection Scheme in Wireless Sensor Networks,” Proc. Third Int’l Conf. Intelligent Sensors, Sensor Networks and Information Processing.

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

[18] L. Hu and D. Evans(2004), “Using Directional Antenna to Prevent Wormhole Attacks,” Proc. Network and Distributed System Security Symp.

Authors

T.Linciya received B.Tech- Computer Science and Enginering (2011) from Kalasalingam University, Srivillputhur and persuing M.E- Computer Science and Engineering in Easwari Engineering College, Chennai. The current project is regarding Three tier security scheme.

Anandkumar K.M. received the B.E. degree in the year 2000 from Bharathiyar University and M.Tech in the year 2006 from Dr.M.G.R.University and currently doing the research in Anna University, Chennai. He is an assistant professor in the Department of Computer Science and Engineering, Easwari Engineering College, Anna University, Chennai. His main research interests focus on Pervasive Computing, Wireless Sensor Networks and Healthcare applications. He published many papers in National and International Conferences. He is an active lifetime member of ISTE and CSI in India.