ORIGINAL RESEARCH PAPER
Volume-6 | Issue-10 | October-2017 | ISSN No 2277 - 8179 | IF : 4.176 | IC Value : 78.46
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

WIRELESS SENSOR NETWORKS IN THREE-TIER SECURITY SCHEME USING POLYNOMIAL BOOL BASED ALGORITHMS

Computer Science

D. Jayachitra M.Sc, M.Phil. MCA., Assistant Professors Department of Computer Science Nehru Memorial College (autonomous) Puthanampatti, Tamilnadu, India.

N. Nithya M.Phil. Scholar, Department of computer Science, Nehru memorial college (autonomous) Puthanampatti, Tamilnadu, India.

ABSTRACT

Wireless Sensor Networks (WSNs) are simple to deploy and allow stretchy installation which has to enable them to be used for numerous applications. Due to these properties, they face distinct information security threats. Security for WSNs is very much needed, because of its sensitive information transmission. The sensor network is exposed to many types of attacks because they are deployed in public background. So it is necessary to secure sensor networks, this can be achieved by introducing authentication and pairwise key establishment mechanisms to sensor nodes. In the proposed system, some nodes are select as a stationary access node to provide authentication access between mobile sinks and sensor nodes. The key distribution mechanism uses two types of key pools: the mobile key pool and the static key pool, the keys in the mobile key pool are shared between mobile sinks and SANs the keys in the static key pool are shared between SANs and Static sensor nodes. This paper proposes a general three-tier security framework for authentication and pairwise key establishment between mobile sinks and sensor nodes. This paper algorithm the polynomial pool-based key pre-distribution scheme considerably improve network resilience to mobile sink replication attack compares to the single polynomial pool-based key predistribution approach.

KEYWORDS

WSN, Mobile Sink, Polynomial Pool Based Approach, Distributed, security, wireless sensor networks.

I. INTRODUCTION

A WSN-Wireless sensor network consists of spatially distributed independent sensors. These sensors are used to monitor physical or environmental conditions, such as temperature, sound, pressure, etc... The idea of using the single polynomial pool is certainly outdated as it opens windows to many node replication attacks. Since single polynomial authentication is compromised move on to create 2 polynomial pool namely static polynomial pool and mobile polynomial pool. The static polynomial pool will supply keys to sensor nodes and access points whereas mobile polynomial pool will supply keys to access points and mobile sinks.

A typical sensor node contains a transceiver, microcontroller, memory, power source, sensor and an analog-to-digital converter. Sensor nodes are inexpensive, thus introducing many constraints in the performance parameters like storage capacity, power requirements and processing speed. The unpredictable communication and unattended operation in WSN make the security battle. These sensors have the ability to communicate either with each other or directly to an external base-station (BS). The BS is a stationary node or a mobile node which is used to connect the sensor network to an existing communication infrastructure. However, when the sensing field is too far from the base station, transmitting the data over long distances using multi-hop may weaken the security strength; therefore, mobile sinks (MSs) are important components in the operation of many sensor network applications. Wireless communication helps adversaries to perform a variety of reactive, active and stealth type of attacks. In passive mode, adversaries silently listen to radio channels to capture data, security credentials, or to collect enough information to derive the credentials. In active attacks, adversaries may actively intercept key management systems, capture and read the contents of sensor nodes. They can use wireless devices with various capabilities to play man-in-the-middle or to hijack a session. They can insert, modify, replay or delete the traffic, jam a part or whole network. The security requirements of WSN are:

- Data Confidentiality,
- Integrity,
- Authentication,
- Freshness
- Availability
- Self-organization in WSN
- Secure Localization

Some common attacks an adversary can make to WSN are a denial of service (dos), collisions, exhaustion, unfairness neglect and greed attack, homing, routing information alteration, black holes, flooding.

II. RELATED WORK

Amar Rasheed et.al [1] developed for group key per distribution. The pairwise key establishment in the context of the sensor network is the ultimate aspiration. This system is unreservedly secure and t-collision resistant. The network resilience is significantly improved to the mobile sink replication attack. The small fraction of preselected sensor nodes is 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.

Chan et al. [2] further unmitigated this proposal and developed two key redistribution schemes: the q-composite key pre-distribution scheme and the random pairwise keys scheme. In q-composite key predistribution, two sensor nodes are essential to computing a pairwise key. 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

Liu et al. [3] the sensor nodes are communicated strongly with each other using the cryptographic technique by enabling by variety key polynomial. This is one of the most primary security services. The resource constraints of the sensor nodes make it not feasible for sensors to use key polynomial scheme. The scheme assures a direct key established between any two neighbor sensors in any deployment group.

I.F. Akyildiz, W. Su, Y. Sankarasubramaniam [4] further decreased the communication cost by using group deployment knowledge. Ho *et al.* also presented an SPRT method for replica detection in mobile sensor networks, in which all sensors are mobile. Pietro, Oliveri *et al.* considered another type of mobile sensor network in which mobile sinks visit stationary sensors and collect the data once in each round.
T. Gao, D. Greenspan, M. Welesh [5] suggested an efficient method of membership verification for re-authentication of the mobile node and shows the performance analysis of our membership verification. Using this method, they proposed an efficient and scalable re-authentication protocol over wireless sensor network. Also, they provided performance and security analysis of the protocol.

K.Han, T. Shon and K. Kim [6] extend our novel and efficient node authentication and key exchange protocol that support Irregular distribution. Compared with previous protocols, this protocol has only a third of communication and computational overhead. The previous improvement enables the resourceful node re-authentication and key exchange even when the sensors are irregularly distributed to the smart home and WPAN for supporting various convergence services. In order to verify the proposed approach, they performed three kinds of validation according to communication pass, message size, and

security analysis.

Z. Liu, J. Ma Q. Huang, and Sang Jae Moon [7] presented an Asymmetric Key Pre-distribution Scheme. Instead of assuming that the network is comprised entirely of identical users in conventional key pre-distribution schemes, the network now consists of a mix of users with different missions, i.e., ordinary users and keying material servers. The group of the client using secret key preloaded in their recollection and public keying material retrieved from one keying material server can compute a session key.

P. F. Oliveira and J. Barros [8] considered the problem of secret key distribution in a sensor network with multiple scattered sensor nodes and a mobile device that can be used to bootstrap the network. Their main contribution is a set of security protocols that rely on simple network coding operations to provide a robust and low-complexity solution for sharing secret keys among sensor nodes, including pairwise keys, cluster keys, key revocation, and mobile node authentication.

III. TIER FRAMEWORK ARCHITECTURE

3.1 1-Tier Architecture

All the processing is done on only one machine and a number of clients attached to this machine (Mainframe), One-tier architecture involves putting all of the required components for a software application or technology on a single server or platform. One-tier architecture is also known as single-tier architecture basically, a one-tier architecture keeps all of the elements of an application, including the interface, middleware, and back-end data, in one place. It is an application that could be installed and run on a single computer. The need for a distributed model for Web application and cloud hosting explanation has created many situations where one-tier architecture is not sufficient.

3.2 2-tier architecture

The two-tier architecture is software architecture in which a presentation layer or interface run on a client, and a data layer or data structure get stored on a server. The client and Server are placed in different locations. Other kinds of multi-tier architectures add additional layers in distributed software design.

3.3 3-tier architecture

3-tier architecture is a client-server architecture in which the functional process logic, data access, computer data storage and user interface are developed and maintained as an independent module on the separate platform. A three-tier architecture is a software design pattern and well-established software architecture. The 3 tier in three-tier architecture is Presentation Tier: Occupier the top level and display information related to service available on a website. This tier communicates with other tiers by sending results to the browser and other tiers in the network.

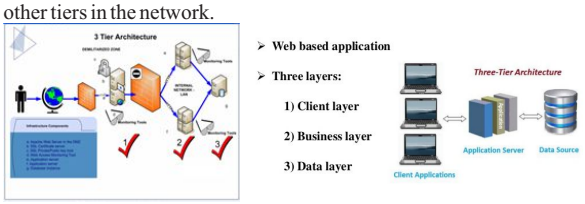


Figure 3.33-Tier architecture3.4 Algorithms

3.4. 1 Random pairwise key predistribution

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

A. Phases in Random Key Predistribution 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 ;
- The different key 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 neighbors. After the first step of the key discovery phase, the sensor knows all its neighbors. The set of all neighbors of the sensor is represented by W_i and $|W_i|=n'$. The set of neighbors of sensor i who share at least one key with the sensor i is represented by R_i. Thus, we have $W_i = Q_i R_i$ and $|Q_i|+|R_i|= n'$. In the second step, every sensor i broadcast 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. Pairwise key establishment phase:
If sensor shares at least one key with a given neighbor, the shared key(s) can be used as their pairwise key(s)

3.4.2 POLYNOMIAL POOL BASED APPROACH

The polynomial pool based approach is divided into two stage. They are (i) Static and mobile polynomial pre-distribution and (ii) Key discovery between mobile node and stationary node. Tame-based key pre-distribution approach, where we exploit tame auto morphisms to get symmetric and two-one bivariate maps for the pairwise key establishment. This tame-based approach can provide deterministic authentication between two parties. The tame transformation ti = (ti,1,…,ti,m) is defined as either a linear transformation or of the following form in any order of variables a1,a2,…,an with polynomials di,j,

$ti,1\ (a1,\ldots,an) = a1+di,1(a2,\ldots,an) = b1$
$ti,2\ (a1,\ldots,an) = a2+di,2(a3,\ldots,an) = b2$
$ti,j\ (a1,\ldots,an) = aj+di,j(aj+1,\ldots,an) = bj$
$ti,n\ (a1,\ldots,an) = an = bn$

If the tame transformation is invertible then it is called as tame auto morphism

Let **G** be a finite field of 2^l elements. Let $\mu^1, \mu^2, \mu^3, \mu^4$ be tame mappings of the $n+r$ dimensional affine space $\mathbf{G}^{n+r.}$ Let the composition $\mu^1, \mu^2, \mu^3, \mu^4$ be π. The mapping π and the $\mu i's$ will be hidden. Let the component expression of π be

$(\pi 1(a1,\ldots,an+r) = \pi n+r(a1,\ldots,an+r))$

The field **G** and the polynomial map $(h1,\ldots,hn+r)$ will be announced as the public key. Given a plaintext

$(a'1,\ldots,a'n) \epsilon \mathbf{G}n$
Assume that,

$b'i=hi(a'1,\ldots,a'n)$
then the ciphertext will be

$(b'1,\ldots,b'n+r) \epsilon \mathbf{G}n+r$
Given μi and $(b'1,\ldots,b'n+r)$, it is easy to find $\mu\text{-}1i(b'1,\ldots,b'n+r)$

The private key will be the set of maps $\{\mu 1, \mu 2, \mu 3, \mu 4\}$. The security of the system rests in part on the difficulty of finding the map π and the factorization of the map π into a product of tame transformations $\mu i's$.

Polynomial bool based Scheme is the main scheme used for finding the polynomial share of each node. Every node is assigned within id. And the steps of this scheme are given below.

1. Each node has an id rU which is unique and is a member of finite field Zp.
2. Three elements a, b are chosen from Zp.
3. Polynomial f(x, y) = (a + b(x + y) + cxy) mod p is generated, where p is a prime.
4. For each node, polynomial share gu(x) = (an+ bnx) mod where an= (a +brU) mod p and bn= (b + crU) mod p informed and re-distributed.
5. In order for node U to be able to communicate with node the following computations have to be performed:

6. Ku,v= Kv,u= f(ru,rv) = (a + b(ru+rv) + crurv)mod p.
7. U computesKu,v= gu(rv).
8. V computes Kv,u= gv(ru)
9. If Ku,v=Kv,u, then the nodes share the same polynomial and then they can establish communication.

ALGORITHM USED IN ADVANCED THREE-TIER SECURITY SCHEME

Step 1:
First, the base station OS server gets started. Then, the all sensor node and mobiles sinks sub-servers are getting registered and activated.

Step2:
A pair-wise key is generated and distributed between the sensor node and mobile sink to check whether both are in activation mode or not. The same pairwise key is used for encryption and decryption.

Step 3:
Once the pairwise key distributed then the sensor is ready to browse the information from the environmental accepts.

Step 4:
The data of information has to send base station. Before sending it gets encrypted and authenticated by mobile sinks; if the sensor is non-compromised and authorized client then data is retrieved by mobile sinks from the sensor.

Step 5:
Polynomial pool based, random pairwise key algorithms are used for encryption and decryption and for authentication 64-bit algorithm is used

Step 6:
Finally, the server retrieves the data and stored in database

IV.EXPERIMENTAND RESULTS

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

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

Table 1. Calculation of Broadcasting the Key of Various Size

The key size is larger it should be stored in a disk file which can be discovered by someone else. This large key size is not only convenient to use but also it is a security risk. It significantly takes a longer time to encrypt and decrypt the message 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). The following analysis shows that as the size of the polynomial pool increases the probability of sharing the key size also increase. The key is generated in the static polynomial pool and it is broadcasted to the sensor node. Fig 4.1 and Fig. 4.2 represent the sharing of the key from the static polynomial pool to the Stationary access node and the sensor node.

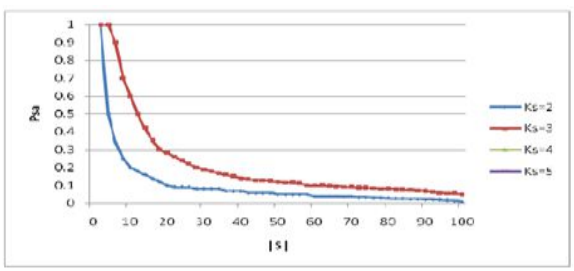


Fig 4.1The probability Psx that a sensor and stationary access node share a static polynomial versus the size|S|

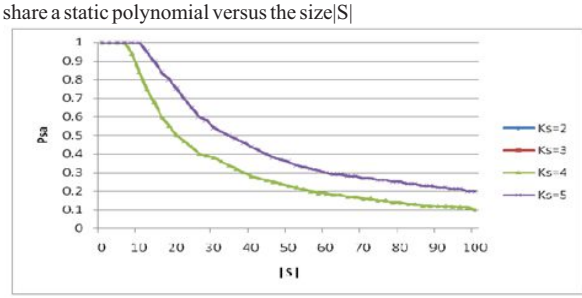
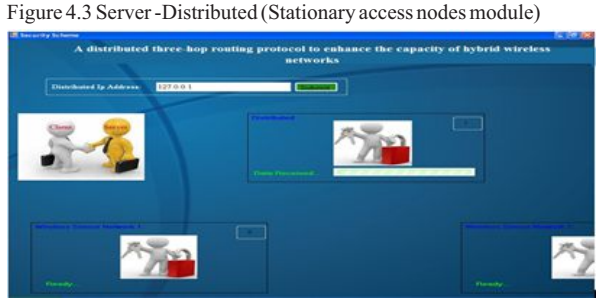


Fig 4.2 The probability P_{sx} that a sensor and stationary access node share a static polynomial|S|

Figure 4.3 Server -Distributed (Stationary access nodes module)



4.4 Enhanced three-tier security scheme method

4.5 Client Receiver File

IV. CONCLUSION

In this concept paper 2-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 pre-distribution scheme substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool based key pre-distribution approach.Using two separate key pools and having few stationary access nodes carrying polynomials from the mobile pool in the network. This paper enhanced the protection performance of the future scheme against stationary access node reproduction attack by intensification the authentication mechanism between stationary access nodes and sensor nodes. To give the best security to the 3-tier using an almost excellent algorithm for each tier. Application of different encryption algorithms.

REFERENCES

[1] 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.
[2] H. Chan, A. Perrig, and D. Song, "Random Key Pre-Distribution Schemes for Sensor Networks," Proc. IEEE Symposium. Research in Security and Privacy, 2003.
[3] 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.
[4] 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.
[5] 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.
[6] J. Kim, J. Baek, T. Shon, IEEE, and Kwangjo Kim, Member, IEEE," Efficient Mobile Sensor Authentication in Smart Home and WPAN", IEEE-2010
[7] H. Wang and Y. Zhang IEEE, Honggang Wang, Member, IEEE, Hamid Sharif, Senior Member, IEEE, and Hsiao-Hwa Chen, Fellow, IEEE, "A Multimedia Quality-Driven Network Resource Management Architecture for Wireless Sensor Networks With Stream Authentication", IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 12, NO. 5, AUGUST 2010
[8] K.Han, T. Shon and K. Kim IEEE, and Rabi N. Mahapatra, Senior Member, IEEE, "The Two-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks', IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 5, MAY 2012
[9] Z. Liu, J. Ma Q. Huang, and Sang Jae Moon "Key Predistribution Approach in Wireless Sensor Networks Using LU Matrix", IEEE SENSORS JOURNAL, VOL. 10, NO. 8, AUGUST 2010
[10] P. F. Oliveira and J. Barros" Secure and Efficient Broadcast Authentication in Wireless Sensor Networks", IEEE TRANSACTIONS ON COMPUTERS, VOL. 59, NO. 8, AUGUST 2010