ANALYSIS OF POLYNOMIAL AND TAME POOL BASED THREE-TIER SECURITY SCHEME FOR WIRELESS SENSOR NETWORKS

[1]S.Grace Diana, [2]P.Ramamoorthy
[1]PG scholar, Department of ECE, SNS College of Technology, Coimbatore
[2]Dean, Department of ECE, SNS College of Technology, Coimbatore
[1]gracediana.s72@gmail.com, [2]covairam33@gmail.com

Abstract: When the base station is long way from the sensor nodes the security strength is reduced. To overcome this problem the concept of Mobile Sinks (MS) is introduced. Still there is a chance of major attack called as Mobile Sink replication attack. One method to eliminate this attack is using pool keys. Normally there are two common types of pool keys are available they are : i)Polynomial pool keys and ii)Tame pool keys. In this paper we study the three layer security using tame pool of keys and polynomial pool of keys. According to the study we prefer tame pool. The reason for preferring tame pool over polynomial pool is that they provide deterministic authentication whereas polynomial pool of keys provide only probabilistic authentication also the polynomial pool key computation reduces the lifetime of the network. The polynomial pool key generation uses Blundo scheme and for secret sharing it uses Merkle Puzzle scheme.

Keywords: Tame pool keys, Polynomial pool of keys, Mobile sinks, Mobile sink replication attacks, Symmetric mappings, Merkle puzzle, Blundo scheme.

1. INTRODUCTION

Advances in wireless networking, engineering technology and integration have enabled a new generation of massive-scale sensor networks suitable for a range of commercial and military applications [1]. With such new technologies come new challenges for information processing in sensor networks. The data that are gathered by the sensor nodes has to be transmitted to the base station. In many cases the distance between the base station and the sensor networks are more. In such cases the security strength is reduced. Therefore, Mobile Sinks are required in many sensor network applications. A sensor network is designed to perform a set of high-level information processing tasks such as detection, tracking, or classification. Applications of sensor networks are wide ranging and can vary significantly in application requirements, modes of deployment, sensing modality, or means of power supply.

In many applications they have to send very sensitive information over a secure environment. Sensor networks are deployed in a hostile environment, security becomes extremely important as these networks are prone to different types of malicious attacks. We can provide authentication and security using pair wise key distribution schemes. But when using Mobile sinks they introduce a new type of security challenge called as Mobile Sink Replication attack [2]. To address this problem the general three tier framework is formed and security is managed in each layer.

2. RELATED WORK

There have been a number of key management schemes developed for sensor networks. Eschenauer and Gilgor proposed a basic probabilistic key pre-distribution technique to establish pairwise keys in sensor networks. Farshid Delgosha and Faramarz Fekri proposed a hypercube multivariate scheme (HMS) that is a threshold-based scheme. In the HMS, a hypercube in the multidimensional space is designed and a number of multivariate polynomials are assigned to every point on the hypercube[5]. Haowen Chan, Adrian Perrig and Dawn Song present three new mechanisms for key establishment using the framework of pre-distributing a random set of keys to each node. They are (i)Random pairwise scheme, (ii)q-composite scheme, and (iii) Multipath key reinforcement scheme[3].

Qi Mi, John A. Stankovic, Radu Stoleru introduce Secure Walking GPS, a practical and cost effective secure localization and key distribution solution for real, manual deployments of WSNs. Using the location information provided by the GPS and inertial guidance modules on a special master node, Secure Walking GPS achieves accurate node localization and location based key distribution at the same time. Xueying Zhang,

Howard M. Heys and Cheng Li focus on the energy efficiency[4] of secure communication in wireless sensor networks (WSNs). Their research considers link layer security of WSNs, investigating both the ciphers and the cryptographic implementation schemes, including aspects such as the cipher mode of operation and the establishment of initialization vectors.

3. THE THREE-TIER GENERAL FRAMEWORK:

In this section, a new framework to provide security for sensor networks is introduced. In this framework, a small fraction of nodes are chosen to be stationary access nodes. They are selected prior to deployment. They act as authentication access points to the network, to trigger the sensor nodes to transmit their aggregated data to mobile sinks. A mobile sink can get data form the sensor nodes only through these stationary access points. Thus we require two separate key pools. They are the mobile pool and the static polynomial pool[4].

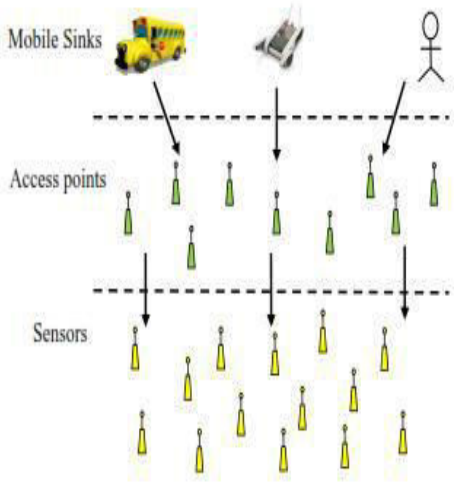

Figure 1: Three-tier scheme

Mobile pool provides necessary authentication between the Mobile sink and the Stationary access points. The static pool provides the necessary authentication between the Stationary access points and the sensor nodes that are carrying the data. The sensor nodes can store up to 210 keys and the mobile sink can store up to 1200 keys. This is because the mobile silk has high energy since it has to move around to gather the data from other sensor nodes.

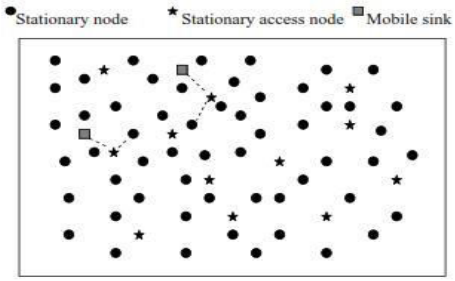

Figure 2: Schematic diagram

The use of two pools makes it difficult for the attacker to launch mobile sink replication attacks. But still the network is vulnerable to Stationary access node replication attack. To provide additional security between Stationary access points and the Sensor nodes the hash functions are preferred. Any method like MD-5 or SHA-512 can be used. Thus the security is strengthened by using one way hash algorithm in conjunction with the pool based scheme[4].

4. POLYNOMIAL POOL BASED APPROACH:

The polynomial pool based approach is divided into two stages. They are (i) Static and mobile polynomial pre-distribution and (ii) Key discovery between mobile node and stationary node[5].

4.1 Blundo Scheme:

Blundo scheme is used to generate the key from polynomial pool. A key setup server takes a random symmetric polynomial f(a,b) of degree „t" with coefficient over the finite field GF(q) where q is large enough to accommodate the symmetric key that has been generated. To load the keys into node say „x' it is necessary to find the value of f(x,b) by evaluating f(a,b) at a=x.

If two nodes say x and y needs to establish key between them then they have to evaluate others ID in its own polynomial. That is node x have to evaluate f(x,b) at b=y.Similarly node y have to evaluate f(y,b) at b=x.

4.2 KEY ESTABLISHMENT:

First the mobile sink broadcasts hello message that contains the MS id (MSID). The stationary access node that is within the range of MS that has heard the hello message can evaluate the keys using this MSID and polynomial shares f(x,b). Consider that there are S keys

computed. The node x sends one message per key containing the node ID and S client puzzle. This is called as Merkle puzzle. If the MS responds correctly to at least one puzzle then they share a common key. Then the key is hashed and used as the session key. Similar step is carried out between the stationary access node and the stationary sensor node.

This has high computational cost. The sensor node has only limited amount of energy. The above mentioned process drains the energy resource of the sensor node. Thus the life time of the whole network is reduced. They also have high overhead.

5. TAME POOL BASED APPROACH

We develop a novel 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,…,an) = a1+di,1(a2,…,an) = b1

ti,2 (a1,…,an) = a2+di,2(a3,…,an) = b2

ti,j (a1,…,an) = aj+di,j(aj+1,…,an) = bj

ti,n (a1,…,an) = an = bn

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

We then present a general framework for the key pre-distribution, on the basis of the tame-based approach. It turns out that this tame map can substitute the conventional polynomial in any existing polynomial-based scheme to offer deterministic authentication service. The analysis demonstrates that, in addition to being able to provide deterministic authentication service, the scheme not only has significantly better performance, but can also achieve greater resilience on security than existing schemes.

It is referred as tame pool-based key pre-distribution because there exists a pool of symmetric-tame maps used in the framework. The process of the framework consists of three phases: symmetric-tame map pre-distribution, direct key establishment and indirect key establishment. The setup server distributes symmetric-tame map shares to each sensor node in the symmetric-tame map pre-distribution phase [7]. After deployment, two sensor nodes will try to establish a direct pairwise key through direct key establishment phase first. If it successes, the process stops; otherwise, the two nodes perform indirect key establishment to establish an indirect pairwise key with assistance of other nodes.

The tame-based approach is t-is limited by memory constraint on sensor node. Also they provide deterministic authentication. The number of Stationary access points can be reduced in this approach.

5.1 Methodology

Let G be a finite field of 2l elements. Let ì1, ì2, ì3, ì4 be tame mappings of the n+r dimensional affine space Gn+r. Let the composition ì1 ì2 ì3 ì4 be ð. The mapping ð and the ìi's will be hidden. Let the component expression of ð be (ð1(a1,…,an+r)= ðn+r(a1,…,an+r))

The field G and the polynomial map (h1,…,hn+r) will be announced as the public key. Given a plaintext (a'1,…,a'n) ϵ Gn

Assume that,

b'i=hi(a'1,…,a'n)

then the ciphertext will be
(b'1,…,b'n+r) ϵ Gn+r

Given ìi and (b'1,…,b'n+r), it is easy to find

ì-1i(b'1,…,b'n+r)

The private key will be the set of maps { ì1, ì2, ì3, ì4}. The security of the system rests in part on the difficulty of finding the map ð and the factorization of the map ðinto a product of tame transformations ìi's.

6. RESULT AND DISCUSSION

The security given by both the system is very strong. But in Wireless Sensor Network only the security is not the issue, it is necessary to check the energy consumption and also delay of the network. These two

parameters play a vital role in improving or reducing the lifetime of the network.

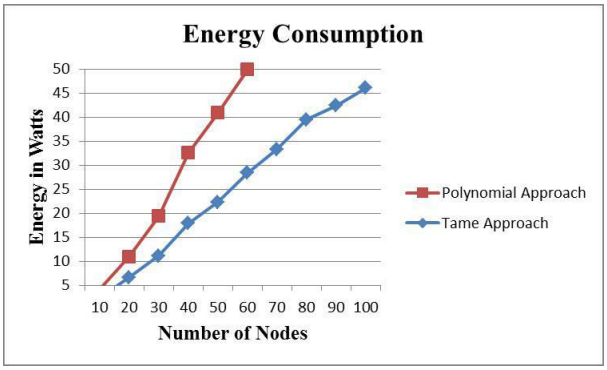

Figure 3: Energy Consumption graph

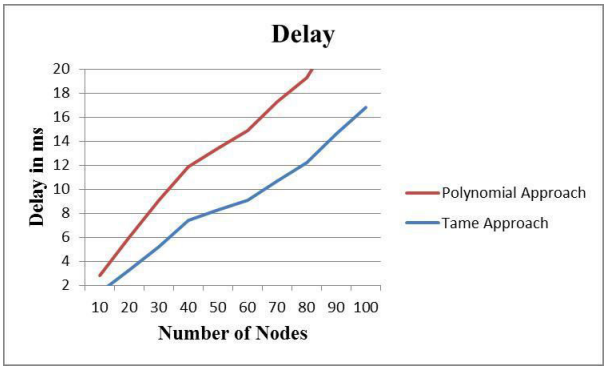

Figure 4: Delay graph

7. CONCLUSION AND FUTURE WORK: Countermeasure attack schemes and security services such as sink authentication and pairwise key establishment are important in many sensor networks applications. In this paper, we examined two security challenges for wireless sensor network with MS. They are mobile sink replication attack and stationary access node replication attack. The solution is pairwise key establishment between sensor nodes and MS using Tame pool or Polynomial pool of keys to tolerate nodes capture and mobile sink replication attack. They provide deterministic and probabilistic authentication respectively. Sink mobility imposes extra communication overhead on these constrained resource sensor nodes to establish secure links with the MS. This extra communication overhead is obtained because of the frequent exchange of cryptography keying information between the sensors and MS. The issue of overhead is the only constraint in this tame pool and polynomial pool based approach. The future work has to mainly consider the overhead issue. Thus by reducing the overhead the life time of the network can still be increased in addition to security.

REFERENCES

[1] WSNs by John A.Stankovic, Department of Computer Science, University of Virginia, Charlottesvile, June 19, 2006.

[2] G.J. Pottie, and W.J. Kaiser, "Wireless integrated network sensors," Communication of the ACM, vol. 43, no. 5, pp. 51-58, May 2000.

[3] Liang Song, Dimitrios Hatzinakos, "Architecture of Wireless sensor networks with Mobile Sinks: Sparesely Deployed sensors", IEEE Transactions, July 2006.

[4] Z. Vincze, D. Vass, R. Vida, A. Vidacs, and A. Telcs, "Adaptive sink mobility in event-driven muti-hop wireless sensor networks," Proc. of the 1st International Conference on Integrated Internet Ad Hoc and Sensor Networks (InterSense"06), vol. 138, no. 13, pp. 1-10, 2006.

[5] I. Chatzigiannakis, A. Kinalis, and S. Nikoletseas, "Sink mobility protocol for data collection in wireless sensor networks," Proc. of the 4th ACM International Workshop on Mobility Management and Wireless Access (MOBIWAC"06), pp. 52-59, 2006.

[6] Amar Adnan Rasheed, " Security in Wireless Sensor Networks with Mobile Sinks"" IEEE Transactions, May 2010.

[7] Yen- Hua Liao, Chin-Luang Lei, Ai-Nung Wang and Wen-Chi Tsai, "Tame Pool based Pairwise Key Pre-distribution for Large Scale Sensor Networks", National Taiwan University, February 2011.

[8] © [2007] IEEE. Reprinted, with permission, from [The 3rd IEEE Int"l. Conf. Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP '07), An energy efficient hybrid data collection scheme in wireless sensor networks, A. Rasheed and R. N. Mahapatra].

[9] M. Demirbas and Y. Song, "An rssi-based scheme for Sybil attack detection in wireless sensor networks," The1st Workshop on Advanced Experimental Activities on Wireless Networks and Systems (EXPONWIRELESS 2006), pp. 564–570, 2006.

[10] S. Capkun and J.-P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," Proc. of the IEEE InfoCom, pp. 1917–1928, 2005.