ENHANCED SECURITY FRAMEWORK AND ARCHITECTURE FOR WSN AGAINST MOBILE SINK REPLICATION ATTACKS

Srinath.Yasam*

B.M.Rao*

S.Phani Kumar*

D.Janaradhan*

Abstract :

Mobile sinks (MSs) are vital in many wireless sensor network (WSN) applications for efficient data accumulation, localized sensor reprogramming, and for distinguishing and revoking compromised sensors. However, in sensor networks that make use of the existing key predistribution schemes for pairwise key establishment and authentication between sensor nodes and mobile sinks, the employment of mobile sinks for data collection elevates a new security challenge, However, in sensor networks that make use of the existing three tier security framework, elevates a new security challenge i.e an attacker can easily create a replicated node and can gain control of the data in the network. To reduce the damage caused by access node replication attack, strengthening the authentication mechanism between the sensors and access nodes is vital For this purpose, the single polynomial pool is converted to a double polynomial pool for providing security over the existing system. Also, security is increased by separating the access points into two layers namely, access nodes-D and access nodes-I along with a more secure authentication mechanism called WHIRLPOOL that produces a 512 bit encrypted text using iyaguchi-Preneel scheme of cipher text generation. Our proposed algorithm ensures the necessary security mechanism for Wireless Sensor Networks and also does not degrade the performance of quality of service.

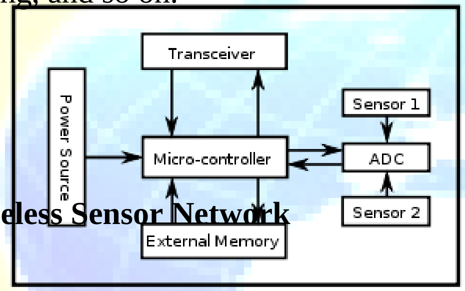
Keywords : Security, Replication Attack, Wireless Sensor Networks, Whirlpool, Key Management

* Assistant .Professor in Department of CSE ,PACE Institute of Technology & Sciences, Ongole

Introduction

1.1 Sensor Node

A sensor node is a node in a wireless sensor network that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network [2]. The main function of sensor is 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. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.



1.2 Wireless Sensor Network

Wireless sensor network (WSN) is an emerging class of systems made possible by cheap hardware, advanced programming tools, complex algorithms, long lasting power sources and energy efficient radio interfaces. Wireless sensor network is a new paradigm in designing fault tolerant mission critical systems, to enable varied applications like threat detection, environmental monitoring, traditional sensing and actuation and much more. It is an emerging area of inter-disciplinary research between people in the electrical engineering, computer science, and among their various disciplines [2].

A WSN consists of spatially distributed autonomous sensors to monitor physical or environmental conditions such as temperature, sound, pressure etc. There are more modern networks such as bidirectional for enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battle field surveillance and these types of networks are used in many industrial and consumer applications such as industrial process monitoring and control, machine health monitoring and so on. Sensor network nodes has typically several parts namely a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source which are usually a battery or an embedded form of energy harvesting.

Three –Tier Architecture of Mobile Sink

The three-tier security scheme was robust against a

stationary access node replication attack, as this scheme makes use of a one-way hash chains algorithm[2] along with the static polynomial pool based scheme[4]. But the scheme suffers from many drawbacks.

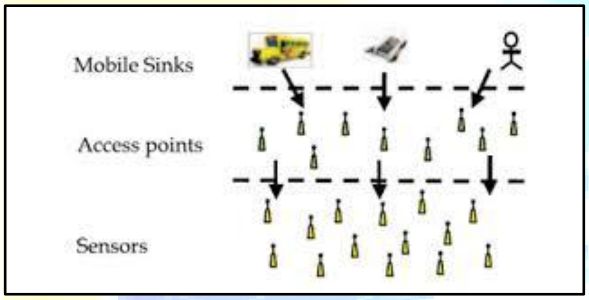


Fig 1.1 Three Tier Architecture

They don't make use of a structured scheme. It is very difficult to know the correct number of polynomials required for having a connection. The main problem with this is the communication overhead, and as a result of this it takes a considerable amount of time. So in order to overcome these drawbacks, we have developed a grid based communication which takes very little time to establish a communication. This grid based communication is between the access nodes and the mobile sinks.

II. RELATED WORK

2.1 SECURITY IN WIRELESS SENSOR NETWORKS

Many works in past has been carried out by various researchers. Some of the important citations has been presented here. Among them, Hasan Tahir presented his work on Wireless Sensor Networks. In his work, the current applications of wireless sensor networks are in the fields of medical care, battlefield monitoring, environment monitoring, surveillance and disaster prevention. Many of these applications require that the sensor network be deployed in an area that is hostile, inaccessible and mission critical. Keeping this in mind a network administrator has to see the security risks involved and how to tackle it if a security threat arises.

Security Methods for Wireless Sensor Networks is proposed by Xiuli Ren in which wireless sensor networks can be used for a wide range of potential applications such as military target tracking, environment monitoring, patient monitoring and scientific exploration in dangerous environments. When sensor networks are deployed in a hostile terrain, security becomes extremely important, as they are prone to different types of malicious attacks. Due to the resource limitations of sensor nodes, existing network security methods, including those developed for Mobile Ad-Hoc Networks, are not well suitable for wireless sensor networks.

2.2 KEY MANAGEMENT IN WIRELESS SENSOR NETWORKS

Similarly, many works have been proposed in the past and some of them are cited here. Eric Ke Wang, et al proposed an Efficient and Secure Key Establishment Scheme for Wireless Sensor Network. The data authentication becomes very important when transferring data. Key management and generation becomes a must to do task. But public key management is not secure enough. Their paper proposes an effective way to generate keys and enhance security using diffie-helmann key exchange algorithm. A Key Management Method of Wireless Sensor Network was proposed by Xuemei You. In his work, the actual situation of current wireless sensor network pair-wise key management research, analysis and comparison between the existing two type of pair-wise key management solution is made according to the evaluation metrics proposed in this article. This cited paper brings out the fact that proper pair wise key management can be chosen according to the environment chosen. Also, this paper also brings out the basic limitations when we are using WSN.

2.3 CRYPTOGRAPHIC ALGORITHMS

There are many works pertaining to cryptographic algorithms. Some of the important works have been cited in the project work. Archana Tiwari, et al presented Performance Evaluation of Cryptographic Algorithms. They presented two most widely used symmetric encryption techniques Data Encryption Standard (DES) and Advanced Encryption Standard (AES). From their paper it is very much clear that DES and AES are very much fragile because of the avalanche effect. Modied-DES Encryption Algorithm was proposed by Walid Zibideh, et al. In their work, due to the fact that wireless channels are an open medium to intruders and their attacks, encryption is a vital process to assure security over these channels. However, using well-known encryption algorithms to encrypt data in wireless communication will result in a catastrophic error due to the avalanche effect, which is implemented in these algorithms to assure security. In their paper, we propose a medication to the Data Encryption Standard (DES) to make it secure and prone to the bit errors caused by the wireless channel.

III. WIRELESS SENSOR NETWORKS

A Wireless Sensor Networks is built of ”nodes” from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a micro controller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoe box down to the size of a grain of dust, although functioning ”motes” of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth.

IV ENHANCED THREE TIER SYSTEM ARCHITECTURE

Basically a sensor node in a wireless sensor networks performs some operations, gathers information and communicates with the other nodes. The main components of the sensor nodes are micro-controller, transceiver, external

memory and power source. The enhanced three tier architecture scheme discussed here consists of four layers namely sensor nodes, access nodes with direct contact, and access nodes in indirect contact and mobile sinks. At the initial stage keys from the single polynomial pool has been shared between the sensor nodes and the mobile sinks for communication. Since the single polynomial has been used, the attacker can easily replicate the node, capture the key and misbehave in the network.

Therefore in order to enhance the security, two polynomial pools namely static polynomial pool and mobile polynomial pool are created which is called the three tier security mechanism. Even though there is a security mechanism by sharing key from two polynomial key pool for layered communication between layers, the replication attacks still persists. The attacks that are possible in the three tier security scheme are mobile sink replication attack and access point replication attack, out of which mobile sink replication attack is reduced to small percentage by the implementation of this scheme. In order to avoid the access point replication attack, it is divided into access points which are in direct contact with the sensor nodes mobile sinks and access points which are not in direct contact with the sensor nodes-mobile sinks. In this enhanced scheme, keys from static polynomial pool is shared by the following layers namely sensor nodes, D access nodes, I access nodes. And keys from the mobile polynomial pool are shared by the following layers namely I access nodes and

mobile sinks. The access nodes which are in indirect contact share the keys from the mobile polynomial pool and some percentile of keys from the static polynomial pool. Therefore an attacker who captures an access node will get either a static key alone or both static and mobile key(hybrid key).

By capturing a node with the direct contact, which has only static key, an attacker cannot be able to send the data to intended destination because the data will be re routed. Once again an attacker capturing the access node which is indirect will get both the keys, but then also it is least possible for an attacker to reach the destination as intended. The following architecture describes the enhancement of the three tier security scheme, which is more resilient towards replication attacks [2].

V POLYNOMIAL POOL BASED MECHANISM

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].

5.1 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.

5.2 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 atleast 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.

6. TAME POOL BASED APPROACH:

We develop a novel tame-based key pre-distribution approach, where we exploit tame auto orphisms to get symmetric and two-one bivariate maps for the pair wise key establishment. This tame-based approach can provide deterministic authentication between two parties. The tame transformation

$ti = (ti,1,\ldots,ti,m)$ is defined as either a linear transformation or of the following form in any order of variables $a1,a2,\ldots,an$ 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.

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 [6]. 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.

7. 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.

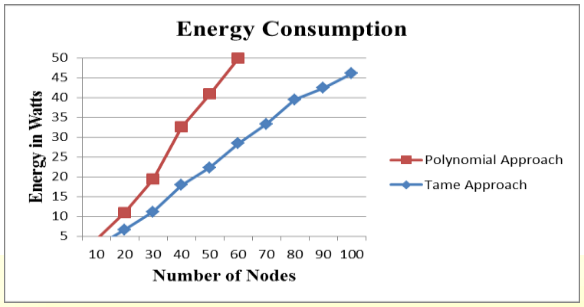


Fig.6.1 Energy Consumption graph

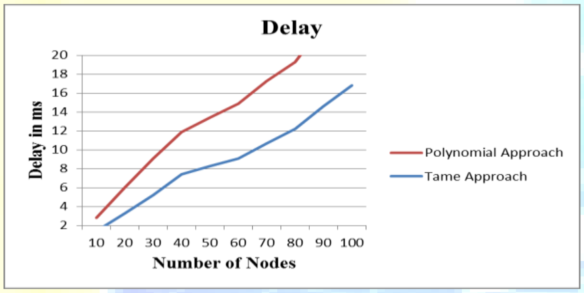


Fig.6.2 Delay graph

8. CONCLUSION

The enhanced three-tier security framework has increased the security between sensor nodes and mobile sinks. By splitting the access point layer, we have achieved more resilience and protection against access point and mobile sink replication attacks. Analysis indicates that after separation of layers and key distribution, the probability of access point replication attack is reduced. The proposed scheme on polynomial pool based key pre distribution substantially improved the network resilience to mobile sink replication attacks compared to single polynomial pool based scheme. We have further improved the security performance of the proposed scheme against access point replication attack by strengthening the authentication between access nodes and mobile sinks.

8.1 FUTURE WORK

Although the enhanced three tier security scheme is more resilient towards access point replication attack, it is weak against wormhole attack. As time progresses, more type of threats will haunt WSNs. So, more complex security frameworks and stronger authentication schemes should be developed.

REFERENCES

[1]R.Mahapatra A.Rashid, “A key predistribution scheme for heterogenous sensor networks”, IEEE Conference, 2009.

[2] Rasheed, A. A. and Mahapatra, R. N. 2012 ‘The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks. IEEE Transactions on parallel and distributed systems, Vol. 23, pp. 958̃965.

[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] M.Praveen Kumar Naregalkar Akshay, “An efficient approach for sensor deployments in wireless sensor network”, IEEE conference, 2011.

[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]. Yen- Hua Liao, Chin-Luang Lei, Ai-Nung Wang and Wen-Chi Tsai, “Tame Pool based Pairwise Key Pre-distribution for Large.

[7] E.Cayirci Y.Shankarasubramaniam, “Wireless sensor networks: A survey”, Proceedings of the IEEE, vol. 38, num. 4, 2002.

[8] Wen Tao Zhu, “Node replication attacks inwireless sensor networks: Bypassing the neighbor-based detection scheme”, IEEE conference, 2011

[9]. Amar Adnan Rasheed, “ Security in Wireless Sensor Networks with Mobile Sinks”‟ IEEE Transactions, May 2010