ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 5, May 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Security Framework of Wireless Sensor Network for Mobile Sink Attack

Kaustubh K. Markande[1]
Department of Computer Network
G.H. Raisoni College of Engineering & Management
Chas, Ahmednagar
University of Pune, Maharashtra – India

Prof. Amruta Amune[2]
Department of Computer Network
G.H. Raisoni College of Engineering & Management
Chas, Ahmednagar
University of Pune, Maharashtra – India

Abstract:** Wireless Sensor Network for efficient data accumulation, localized sensor reprogramming and for collecting data from various sensor nodes across area. Existing three tier security framework, introduced a new security challenge, an attacker create a replicated node and gain control of the data in sensor network. Security framework is more resilient to mobile sink replication attacks. Replication attack reduced by the authentication between the sensors and access nodes. So, the single polynomial pool is converted to a double polynomial pool for providing security over the system. In proposed algorithm ensures security mechanism for Wireless Sensor Networks and also does not reduced the performance.

***Keywords:** Wireless Sensor Network (WSN), Stationary Access Point (SAP), Sensor Node (SN), Mobile Sinks (MS).*

I. Introduction

A Wireless sensor network (WSN) consists of distributed autonomous sensors. Single polynomial pool is outdated as it many node replication attacks. Since single polynomial authentication is not ensuring, we move on to create two polynomial key pools namely static polynomial key pool and mobile polynomial key pool. Static polynomial key pool will supply keys to sensor nodes and access points. Mobile polynomial pool will provide keys to access points and mobile sinks. Using two separate polynomial key pools and having few sensor nodes that carry keys from mobile key pool will make it not easy for the attacker to generate a mobile sink replication attack on the sensor network by accessing few node of sensor networks. Security framework makes the network more resistant to mobile sink replication attack as compared to single pool based key pre-distribution scheme; stationary node replication attack problem still not solved. One-way hash algorithm is used for solving above problem with static polynomial pool based scheme to improve the security. To enhanced security used scheme for stationary nodes (access points) are divided into two layers access nodes-D and access nodes-I with direct contact and nodes with indirect contact. These sensors are used to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. Data transmit cooperatively through the network; networks are bi-directional enables control of sensor activity. Industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

1.1 KEY PRE-DISTRIBUTION

Key Pre-distribution term defined as loading keys into sensor nodes prior to deployment. Two nodes of network find a common key between them then deployment. There is various challenges in key pre-distribution like memory/energy efficiency, security and scalability.

II. Related Work

1. Linciya.t1 and anand kumar. k.m2,"enhanced three tier security architecture for wsn against mobile sink replication attacks using mutual authentication scheme", international journal of wireless & mobile networks (ijwmn) vol. 5, no. 2, april 2013

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 neighboring 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.

2. Amol Magar, B.S. Sonawane, "An Efficient Security Scheme In Wireless Sensor Network With Mobile Sink", International Journal of Advance Research and Innovation Vol 7 Issue 3,2013

Sensor networks may be deployment in hostile environments, especially in military applications. Small low cost sensor devices each equipped with limited resources are networked and are used for various critical applications. Making such sensor network secure is a challenging issue. Under such situations, the sensors may be captured, and the data may be intercepted and/or modified by the attacker. Therefore security services such as authentication and pair wise key establishment is a critical issue to maintain network operations. In the traditional schemes an attacker can easily obtain large number of keys by capturing small fraction of nodes and initiate data communication with any sensor node. Here the main focus is on the sensor network that uses mobile sink to gather the sensed data from the network. A new security technique- Three tier security scheme is proposed to provide authentication and pair wise key establishment between sensor nodes and mobile sinks. The proposed scheme makes use of two polynomials pools: static polynomial pool and mobile polynomial pool which will improve network resilience to the mobile sink replication attack.

3. T. Subramani1, S.Ravi Varma , R.Kabileshwaran," A Security Framework for Replication Attacks in Wireless Sensor Networks", International Journal of Modern Engineering Research (IJMER) Vol. 3, Issue.

5, Sep - Oct. 2013 pp-2908-2915

Mobile sinks play a great role in many Wireless Sensor Network applications for efficient data accumulation, localized sensor reprogramming and for collecting data from various sensor nodes across the globe. 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. Although the three-tier security framework is more resilient to mobile sink replication attacks, it is weak against access point replication attacks. 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 Miyaguchi-Preneel scheme of cipher text.

4. P. Santhi1 , Md. Shakeel Ahmed2 , Sk. Mehertaj3 , T. Bharath Manohar4 ,"An Efficient Security Way of Authentication and Pair wise Key Distribution with Mobile Sinks in Wireless Sensor Networks" International Journal of Modern Engineering Research (IJMER), Vol. 3, Issue. 4, Jul - Aug. 2013 pp-2553-2562

Wireless sensor networks (WSN) are the emerging application in many industrial and missile sector. Mobile sinks (MSs) are vital in many wireless sensor network 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 pre-distribution 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: in the basic probabilistic and q-composite key predistribution schemes, an attacker can easily obtain a large number of keys by capturing a small fraction of nodes, and hence, can gain control of the network by deploying a replicated mobile sink preloaded with some compromised keys. The proposed work, three-tier framework permits the use of any pairwise key predistribution scheme as its basic component. The new framework requires two separate key pools, one for the mobile sink to access the network, and one for pairwise key establishment between the sensors.

III. PROPOSED WORK FOR SECURITY FRAMEWORK

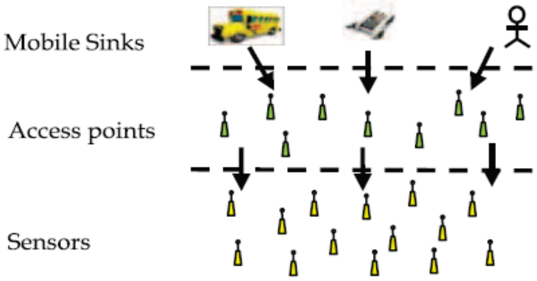

Fig3.1 Security Framework Architecture

The stationary access point shown at above act as authentication access points to the network for triggering the sensor nodes to transmit their data to the mobile sinks device. Mobile sink device sends data request message to the sensor nodes through stationary access point. Data request messages from the mobile sink device to stationary access node to triggering sensor nodes of network, which transmit requested data to mobile sink. Security framework generally uses two separate polynomial key pools as the mobile polynomial pool and the static polynomial pool. Polynomials from mobile polynomial pool are used to establish authentication between mobile sinks and stationary access point which enable mobile sinks to access the network for data gathering. Polynomial from static pool is used to establish authentication and key setup between sensor nodes and stationary access point.

3.1 SENSOR NODE DEPLOYMENT

In this module create sensor nodes. User enter the some information like as, IP address, port number and status of the node to register in the database.

3.2 CREATING MOBILE SINKS

In this module just create mobile sink. User enter the some information like as, number of mobile sinks he wants to create, mobile sink name, IP Address, port number, status of the mobile sink to register in the Database.

3.3 AUTHENTICATION & PAIR WISE KEY DISTRIBUTION

In the framework authenticate all the sensor node and mobile sink and these authenticated mobile sinks are managed by polynomial key pool both static and dynamic In the framework used two separate polynomial key pools and having few sensor nodes that stored polynomial keys from the mobile key pool will make it more complex for the attacker to generate a mobile sink replication attack on the sensor network by accessing only a few arbitrary sensor nodes.

IV. WHIRLPOOL ONE WAY HASH ALGORITHM FUNCTION

STEP I: Let K1, K2 denotes the keys in the key pool.

STEP II: Let Ks, Km denotes the number of keys in the static and mobile key pool.

STEP III: DK1,K2 denotes the data transfer using the keys K1 and K2.

STEP IV: Access point involved in data transmission picks a key K1 from the Ks number of keys in the static pool and a key K2 from the Km number of keys in the mobile pool.

STEP V: Selecting a key from the static key pool:

A. Ks C1 Probability of choosing a key from the static key pool, PK1 = 1/Ks C1

B. Selecting a key from the mobile key pool: Km C1

STEP VI: Probability of choosing a key from the static key pool, PK2 = 1/Km C1

Let PCC denotes the probability of arriving at the correct combination of keys.

Let S denotes the strength of the algorithm which depends on the length of the key, length of the encrypted text and the encrypted mechanism.

STEP VII: Let Pbef denote the probability of access point replication attack before separation of layers.

Pbef = (1/Ks C1) + (1/Km C1) + PCC + S …(1)

Let Paft denote the probability of access point replication attack after node separation.

STEP VIII: Direct contact nodes will share the key only from the static key pool. Let x be the small percentage of the keys gets added to the mobile key pool(Hybrid key pool)

STEP IX: Selecting key from the static and mobile key pool,

Y = (Km C1) * (x C1)

Paft = (1/Ks C1) + (1/Y) + PCC + S …(2)

Comparing (1) and (2), its clear that

Paft <<Pbef

V. PERFORMANCE ANALYSIS

This section presents the results of a practical performance evaluation of security framework system. Although these techniques do not produce an optimal solution but the solution produced are sufficiently close to the optimal one and key generated by it are simple.

Table: Performance evaluation based on Resiliency, scalability and Mobility

Sr No	Scheme	Resiliency	Scalability	Mobility
1	**Pairwise Key Establishment**	65%	70%	75%
2	**Basic**	60%	78.30%	81%
3	**Qcomposite**	58.7%	74.00%	83%
4	**Random**	63.8%	78%	90%
5	**Polynomial Pool Based**	70%	85%	92.5%

Table: comparison between Polynomial pool Base and Existing Scheme

PARAMETER/ SCHEME	Pairwise Key Establishment	Basic	Q composite	Polynomial Pool Based
Resiliency	Reduced	Less	Less	**Increase**
Overhead	Less	reduced	More	**More**
Scalability	Scalable	Infinite	Scalable	**Infinite**
Mobility	Node	Node	Node	**Ensure node**
Mutual Authentication	No	No	No	**Not ensure**

VI. Result

We have tested this security framework for some existing scheme with polynomial pool based scheme; following section includes experimental review of these.

Here we show some results from the some existing system and security framework system. The goal of This security framework analysis is to test &validate our approach. The problem statement for this system is as follows:

The problem of authentication and pair wise key establishment in sensor networks with MSs is still not solved in the face of mobile sink replication attacks. For the basic probabilistic and q-composite key pre distribution schemes, an attacker can easily obtain a large number of keys by capturing a small fraction of the network sensor nodes, making it possible for the attacker to 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.

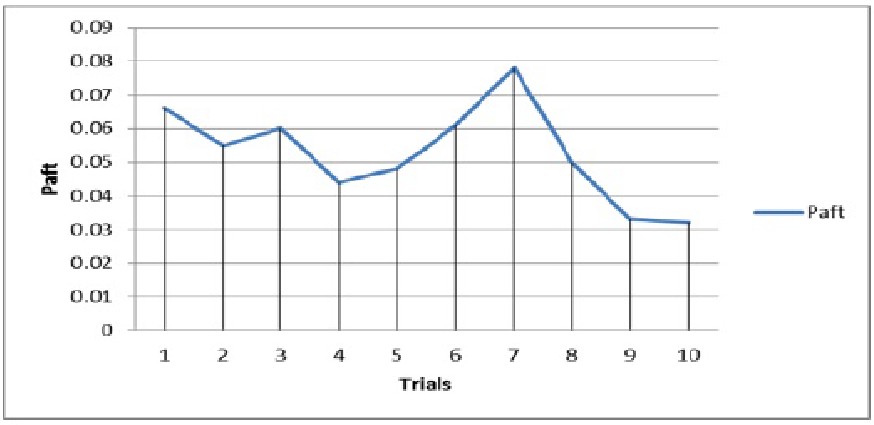

Fig 1: Graph generated By the probability Based Scheme

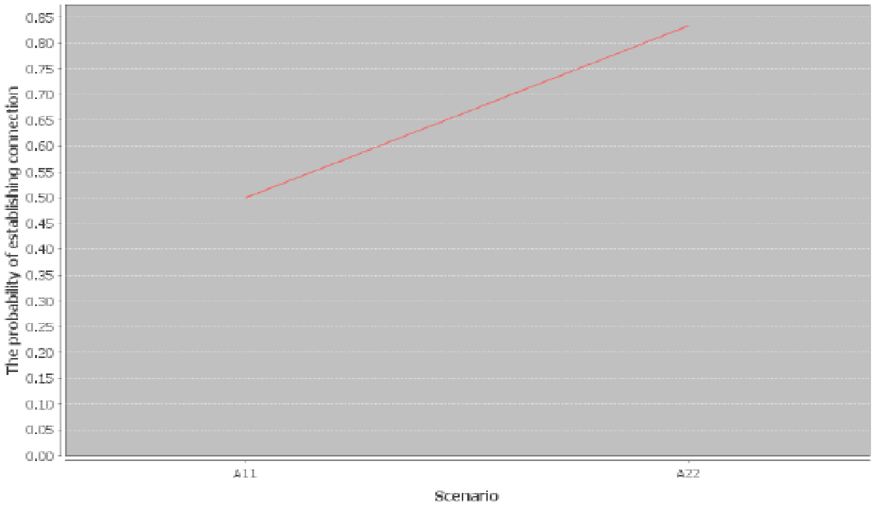

Fig3.1: Grid Based Scheme

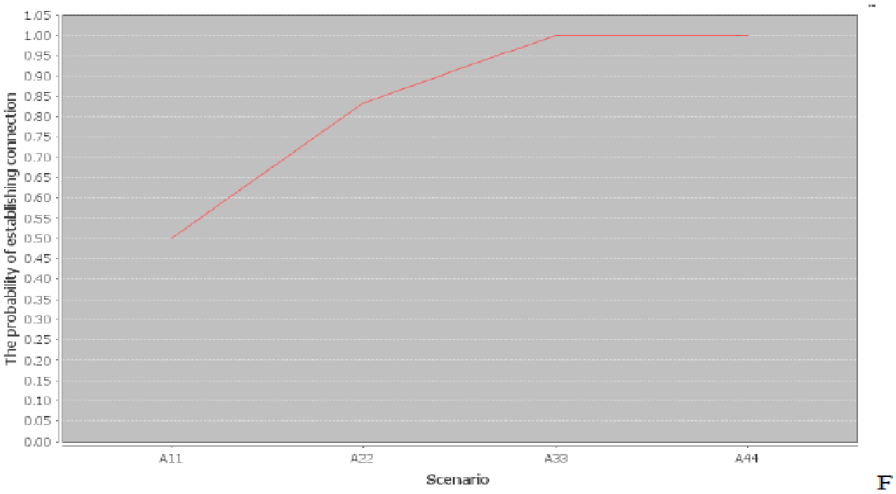

Fig3.2: Grid Based Scheme

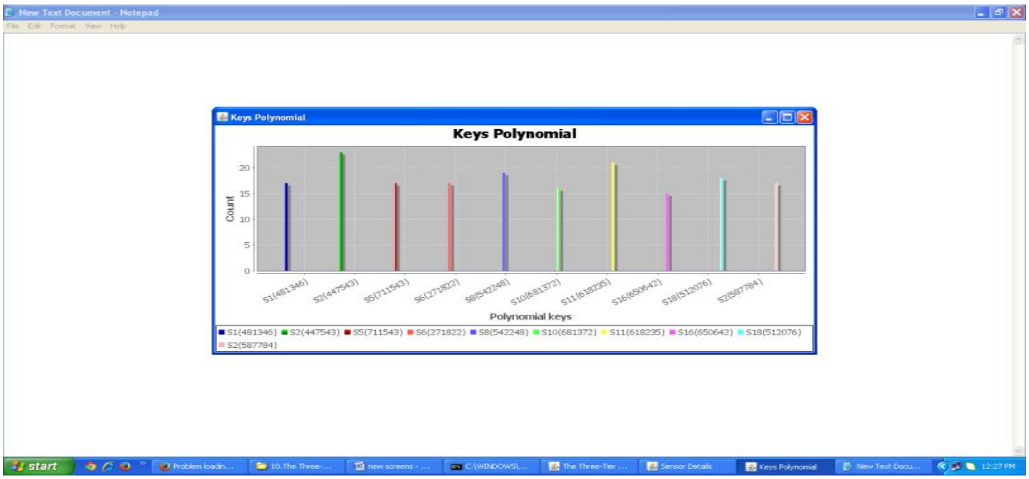

Fig 2: Graph generated by Polynomial pool based Scheme

VII. Conclusion

Security framework in wireless sensor network for authentication and pair wise key establishment between mobile sinks device and sensor nodes of network. Security framework based on the polynomial pool-based key pre distribution scheme improved network resilience to mobile sink replication attacks as compared to the single polynomial pool-based key pre distribution approach. Security framework divide key pool in two separate key pools and having few stationary access nodes carrying polynomials keys from the mobile pool in the network and attacker from gathering sensor data, by deploying a replicated mobile sink.

Acknowledgement

I like to thanks people for helping me for giving importance guidance about project work. I am very thankful to those who help me during my paper publishing as well as project dissertation stage. I am thankful to journal for giving me best opportunity to publish my paper. I am sincerely thankful to my head of department, my project guide and other staff members from department for supporting me.

References

1. Amar Rasheed, Student Member, IEEE, and Rabi N. Mahapatra, Senior Member, IEEE "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
2. T. Subramani1, S.Ravi Varma2, R.Kabileshwaran 3 "A Security Framework for Replication Attacks in Wireless Sensor Networks",International Journal of Modern Engineering Research (IJMER)Vol. 3, Issue. 5, Sep - Oct. 2013 pp-2908-2915
3. Uma P1, Manjula Devi T H2 ,"an efficient security scheme providing authentication and pairwise key distribution with mobile sinks in wsn's"International Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 5, May 2013

4. Amol abhiman magar, pursuing m.tech,2b.s.sonawane,Asst. Professor, “ an efficient security schemes in wireless sensor networks with mobile sinks”, International Journal Of Advanced Research and Innovation -Vol.7, Issue .III, 2012

5. Leenu Rebecca Mathew1, Jyothish K John2, Tibin Thomas3, Karthik M4 “Three Tier Security Schemes In Wireless Sensor Networks With Mobile Sinks Using Grid”International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013

6. L. Eschenauer and V.D. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” Proc. ACM Conf. Computer Comm. Security (CCS ’02), pp. 41-47, 2002.

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

8. D. Liu, P. Ning, and R.Li. Establishing, “Pairwise Keys in Distributed Sensor Networks,” Proc. 10th ACM Conf. Computers and Comm. Security (CCS ’03), pp. 52-61, Oct. 2003.

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