ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 10, October 2013*

# Three Tier Security Schemes In Wireless Sensor Networks With Mobile Sinks Using Grid

Leenu Rebecca Mathew[1], Jyothish K John[2], Tibin Thomas[3], Karthik M[4]

M. Tech in Computer Science and Information Systems, Department of Computer Science and Engineering , Federal Institute of Science and Technology, Angamaly, India[1]

Assistant Professor, Department of Computer Science and Engineering, Federal Institute of Science and Technology, Angamly, India[2]

M. Tech in Computer Science and Information Systems, Department of Computer Science and Engineering , Federal Institute of Science and Technology, Angamaly, India[3]

M. Tech in Computer Science and Information Systems, Department of Computer Science and Engineering , Federal Institute of Science and Technology, Angamaly, India[4]

**Abstract**: Wireless Sensor Network (WSN) is an area of research that has various applications both for mass public and military. A wireless sensor network is composed of many sensors which can be used to monitor physical or environmental conditions, such as temperature, sound, pressure. After collecting these data they should pass this data through the network to a main location. A Sensor Node in Wireless Sensor Network lacks resources such as processing capability, memory capacity, battery power, and communication capability. Because of the limited resources on sensor nodes, the use of conventional key management techniques in wireless sensor networks is limited. Key establishment is the most important cryptographic primitive in all kinds of applications where security is a concern. Authentication and pair wise key establishment are critical in sensor networks. In this paper, we provide a survey of key management schemes in wireless sensor networks.

.

**Keywords**: Key Pre distribution, key management, Pair wise key, polynomial pool base, q-composite

## I. INTRODUCTION

Wireless sensor networks (WSNs) comprise a large autonomous devices[13] monitoring environmental conditions. Sensor nodes then pass the collected readings to a central server through a network of sensor nodes. Sensor, wireless communication device, small micro- controller and energy source comprises this small device, called sensor node. The central server collects all the readings and then processes them according to the application. Sensors are not so costly, low-power devices which have limited resources. They are small in size, and have wireless communication capability within short distances.

WSN have many applications in various fields including military[12], environmental, health , industry ,data collection in hazardous environments [12] and all these applications require secure communications. Wireless networks are more vulnerable to attacks than wired ones because of the broadcast nature of transmission medium, resource limitation on sensor nodes and uncontrolled environments where they are left unattended .Sybil attacks[1], black hole attacks, DoS attacks, wormhole attacks etc are the major malicious attacks present in WSNs[2]. Therefore, the security in sensor network is extremely important. Many securities had been designed for wired and wireless networks but they can't be used in wireless sensor networks because of the limited energy, memory and computation capability. Key management protocols are the basis of the secure communications and are the fundamental security mechanism in wireless sensor network.

WSN mainly face the problem of mobile sink replication attack. To overcome this problem A. Rasheed [20] proposed a three tier security framework for authentication and pair wise key establishment, based on polynomial pool based key pre-distribution scheme [6].This technique was able to give network resilience to mobile sink replication attacks. They had preselected sensor nodes as stationary access nodes, which acts as authentication access points that are capable of making the sensor nodes to send their data to mobile sinks. They use two separate polynomial pools: a mobile polynomial pool and a static polynomial pool. Authentication between mobile sinks and stationary

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 10, October 2013*

access nodes are established by polynomials from the mobile polynomial pool. Thus, an attacker would need to compromise at least a single polynomial from the mobile pool to gain access to the network for the sensor's data gathering. Polynomials from the static polynomial pool are used to ensure the authentication and keys setup between the sensor nodes and stationary access nodes.

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 [19] along with the static polynomial pool based scheme [13]. But the scheme suffers from many drawbacks.

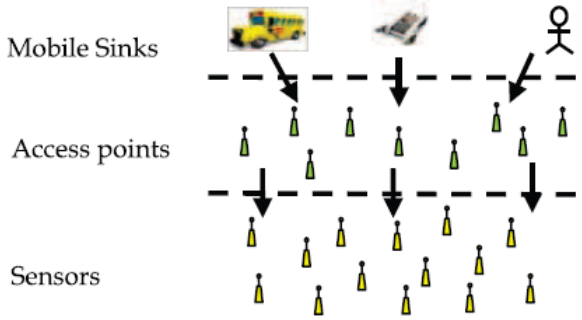


Fig 1: Three Tier Scheme

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.

The remainder of this article is organized as follows: Section II describes the related work. Section III describes the proposed scheme. Section IV gives the results of using the new scheme. Section V gives the conclusion of using this new method and the advantages of the new scheme.

## II. RELATED WORK

In order to exchange data securely in WSN, the keys must be shared among the nodes [3]. Eschenauer and Gilgor[4] proposed a probabilistic key pre distribution which is the Basic Scheme. The main idea was to randomly pick a set of keys from a key pool by a sensor node and any two nodes able to find at least one common key can use that key as their shared secret to initiate communication. Chan et al [3] extended the basic scheme and developed two key pre distribution schemes: the q-composite key pre distribution scheme and the random pair wise keys scheme. Q composite key pre distribution scheme requires at least q common keys so as to have a communication link between any two nodes. In Random pair wise scheme instead of storing (N-1) keys, there is only Np =Nxp keys by each node, where p is the probability that two nodes in the network are connected. Liu and Ning [10] proposed the Polynomial key pre-distribution scheme which makes use of a setup server which randomly produces a bivariate symmetric polynomial $f(x, y) = f(y, x)$ of $k$ degree over finite field GF(q), $q > n$. A key setup server computes a polynomial share of $f(x, y)$, $f(i, y)$ for each sensor $i$. If two nodes are present ie i and j,then i can compute the common key $f(i, j)$ by evaluating $f(i, y)$ at point $j$, while $j$ can compute the same key $f(j,i) = f(i, j)$ by evaluating $f(j, y)$ at point $i$. To have a pair wise key, both sensor nodes need to evaluate the polynomial at the ID of the other sensor node.

Zhu et.al., [21] described that LEAP (Localised Encryption And Authentication Protocol), a key management protocol for sensor network that is designed to support in network processing. This method can be used for supporting various communication models. The main purpose of this scheme is that they can provide authentication, confidentiality and robustness. Amar Rasheed et.al., [19] proposed a scheme which uses polynomial pool based key pre distribution in conjunction with the probabilistic key pre distribution scheme to establish a pair wise key between mobile sink and any sensor node. This scheme ensures that the sensor node can establish a pair wise key with a mobile sink with high probability and without sacrificing security. A. Rasheed et.al., [17] also described a key distribution scheme which is based on random key pre distribution for hete rogeneous sensor network that can achieve better performance and security as compared to homogenous network. The proposed scheme reduces the storage requirements by using generation keys.

## III. PROPOSED SCHEME

Proposed scheme makes use of Blundo's scheme to have two polynomial pools. One is the mobile pool which is between the access nodes and mobile sink and the other is the static pool between the access nodes and sensor nodes. In this proposed system, we are making use of Grid architecture along with the mo- bile polynomial pool. Similar to the Three Tier Security Scheme, this also makes use of the one way hash chain algorithm along with static based polynomial pool. This scheme overcomes the drawbacks of Three Tier Security framework by introducing a grid communication between the mobile sinks and access nodes .This Grid will give the correct polynomial by which the communication can takes place, then there is no need of searching for the polynomial shares. This technique can reduce the communication overhead.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 10, October 2013*

Table 1: Comparison Of Different Schemes

| SCHEME | RESILIENCY | OVERHEAD | SCALABILITY | MOBILITY | MEMORY | MUTUAL AUTHENTICATION |
|---|---|---|---|---|---|---|
| Single Network Wide Key | Reduced Resiliency | Single key is used ,so less overhead | Reduced Scalability | Can Handle node mobility | Can deal with memory constraints | Can't ensure mutual authentication |
| Pair wise Key Establishment | Resiliency is improved | Less overhead | Gives scalability | Can Handle node mobility | Memory Constraints can be handled | No mutual authentication |
| Trusted Key Pre Distribution | Reduced resiliency | Since a trusted party is used, more overhead | Reduced Scalability | Can't Handle node mobility | Can handle memory constraints | Ensure mutual authentication |
| Basic Scheme | Resiliency is reduced | Overhead is reduced | Infinite Scalability | Ensures Node mobility | Can't deal with memory constraints | Can't ensure mutual authentication |
| Q-Composite Key Pre distribution | Improved Resiliency | More Overhead | Offers Scalability | Offers Node Mobility | Can't deal with memory constraints | Can't ensure mutual authentication |
| Random Pair wise Scheme | Resiliency is improved | Less Overhead | Offers Scalability | Offers Node Mobility | Can't deal with memory constraints | Ensures Mutual Authentication |
| Knowledge Based | Less Resiliency | Less Overhead | Scalability is reduced | Can't ensure node mobility | Can deal with memory constraints | Can't ensure mutual authentication |
| Polynomial Pool Based Scheme | Increased resiliency | More Overhead | Offers Infinite scalability | Ensure Node Mobility | Can't deal with memory constraints | Can' ensure mutual authentication |
| LEAP: | Increased Resiliency | More Overhead | Offers Scalability | Can't ensure node mobility | Can deal with memory constraints | Ensures Mutual Authentication |
| BABEL Scheme | Higher Resilience | More Overhead | Provides Scalability | Can Handle Mobility | Requires more memory | Provides mutual authentication |

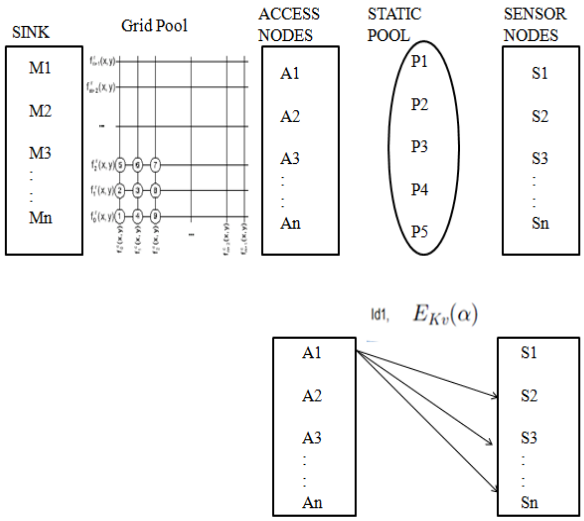


Fig 2:Grid Based Architecture

Blundo's Scheme is the main scheme used for finding the polynomial share of each node. Every node is assigned with an 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,care chosen from Zp.
3. Polynomial f(x,y) = (a + b(x + y) + cxy) mod p is generated, where p is aprime.
4. For each node, polynomial share gu(x) = (an+ bnx) mod p where an= (a +brU) mod p and bn= (b + crU) mod p is formed and pre-distributed .
5. In order for node U to be able to communicate with node V the following computations have to be performed:
6. Ku,v= Kv,u= f(ru,rv) = (a + b(ru+rv) + crurv )mod p.
7. U computes Ku,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.

*A .Finding key Discovery Between Access Nodes and Sinks Using grid*

If a network consists of N sensor nodes, an (m x m) grid with a set of 2m polynomials is constructed, where m=√N. Each row i in the grid is associated with a polynomial fi r(x, y) and each column of the grid is associated with a polynomial share fi c(x, y). In the first stage, the setup server gives an gives the polynomial shares of a particular column and row to the node so as to use this information for key discovery and path key establishment. <i, j> is used to represent an intersection of the node. In the second stage, in order to establish a connection with another node say i and j, it checks for common rows or columns with j i.e., ci = cj or ri = rj. If ci=cj then both nodes may have fci c (x, y) and they can use the polynomial-based key pre distribution

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 10, October 2013*

scheme to establish a pair wise key directly. If ri=rj then both nodes may have fri r(x,y) and they both have polynomial shares of fri r (x, y), and can establish a pair wise key accordingly. If neither of these conditions is true, nodes i and j go through path discovery to establish a pair wise key. To do so, node i can find an intermediate node through which it can establish a pair wise key with node j. The main advantage of this scheme is that they can reduce the communication overhead and can give the exact number of polynomials.

## IV. RESULTS

This section analyzes the performance of the proposed system. Here, the performance is evaluated based on the grid communication capabilities. This analysis makes use of the grid structure and shows how the probability of establishing connections with base station increases as we increase the number of access points.

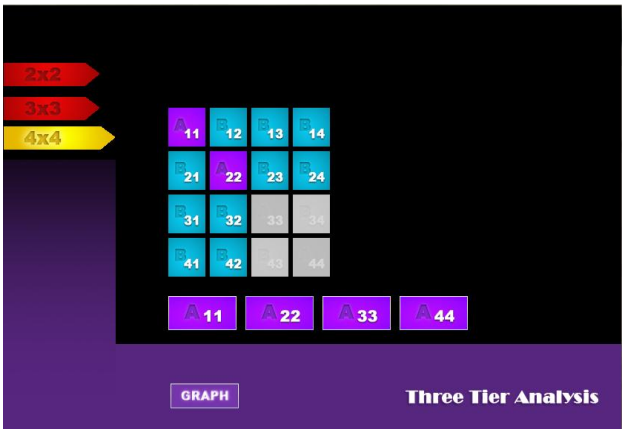


Fig 3: 4*4 grid having two access points

Figure 3 shows that if there are two access point in a 4*4 grid, A11 A22. Then there can be ten base stations with which they can communicate.

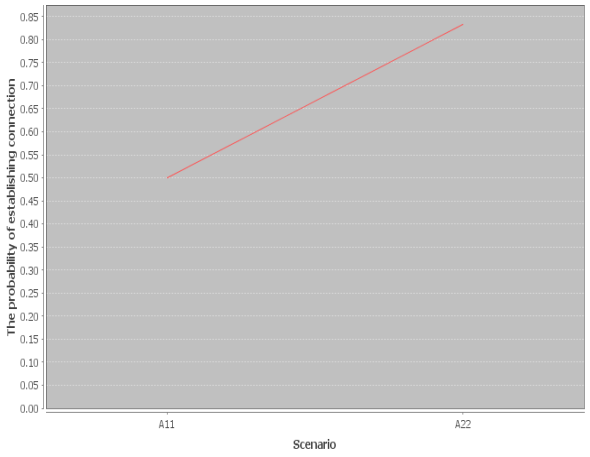


Fig 4: Probability Of Establishing Communication

Figure 4 shows that A11 can communicate with six base stations and A22 can communicate with four more base stations. This shows that the probability of establishing communication increases when A22 comes. The probability of establishing communication increases from 0.5 to 0.83.

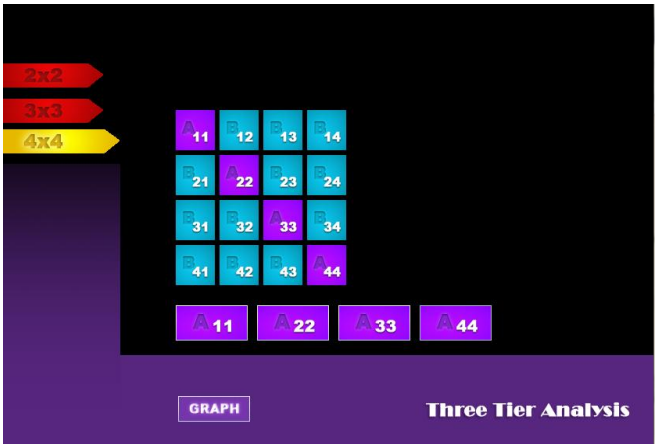


Fig 5: 4*4 grid having four access points

In the above figure, it is clear that when four access point is selected, there is no addition of base stations. So that the number of base stations to which the communication takes place remains same.

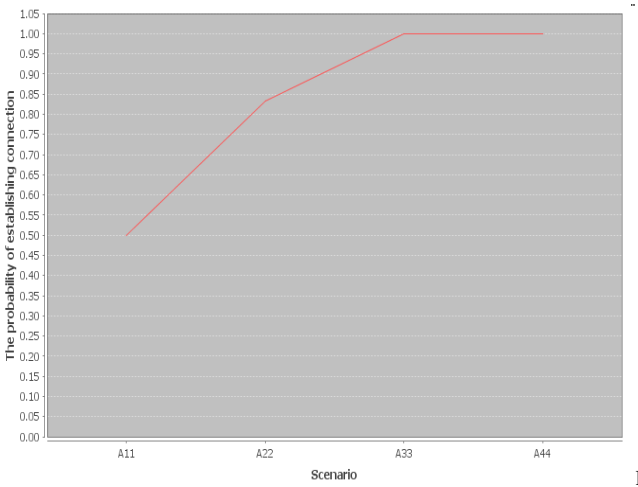


Fig 6: Probability Of Establishing Communication

The figure shows that when four access points are present, the probability of establishing communications remains the same even if we are increasing the access point, because there is no increase in the number of base stations with which they can communicate. So there is no change in the graph.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 10, October 2013*

## V. CONCLUSION

In this project, I have proposed a three-tier security using grid framework for authentication and pair wise key establishment between mobile sinks and sensor nodes. The proposed scheme, based on the polynomial pool-based key pre distribution scheme improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key pre distribution approach [13]. Here two separate key pools are used. Also few stationary access nodes carrying polynomials from the mobile pool in the network may prevent an attacker from gathering sensor data, by deploying a replicated mobile sink. The security of the proposed scheme against stationary access node replication attack is strengthened by the authentication mechanism between stationary access nodes and sensor nodes.

For this the one-way hash chains algorithm [18] in conjunction with the static polynomial pool-based scheme [13] is used. Since the grid based communication is established between the mobile sink and the access nodes, there is no communication overhead. The id of mobile sink can be taken from grid itself. The main advantage of the proposed method is the structured architecture. There will be a greater chance for nodes to establish a pair wise key with others without communication overhead as the sensors are deployed in a grid-like structure. Also this has nice resilience to node capture until a certain percentage of nodes are compromised. The polynomial by which it establishes communication with access nodes is known. So there is no need of sending messages to each other. Hence the grid based scheme will be faster.

## ACKNOWLEDGMENT

I would like to thank from the bottom of my heart, the Head of the department of Computer Science & Engineering, **Dr. J.C.Prasad** for encouraging me.

I express my profound gratitude to my project guide **Mr.Jyothish K. John** for the valuable help and guidance in the preparation of my project.

## REFERENCES

[1] B.J. Culpepper and H.C. Tseng, "Sinkhole Intrusion Indicators in DSR MANETs," Proc. First Int'l Conf. Broadband Networks (Broad- Nets '04), pp. 681-688, Oct. 2004.
[2] Lai B, Kim S, Verbauwhede I. Scalable session key construction protocol for wireless sensor networks. In: Proceedings of the IEEE workshop on Large Scale Real-time and Embedded Systems LARTES, December 2002.
[3] Chan H, Perrig A. PIKE: peer intermediaries for key establishment in sensor networks. In: Proceedings of the 24th annual joint conference of the IEEE computer and communications societies (INFOCOM ″05), Miami, FL, USA, March 2005. p. 524–35.
[4] 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.
[5] H. Chan, A. Perrig, and D. Song, "Random Key Pre-Distribution Schemes for Sensor Networks," Proc. IEEE Symp. Research in Security and Privacy, 2003.
[6] 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.
[7] K. Ren, K. Zeng, and W. Lou. A new approach for random key pre-distribution in large-scale wireless sensor networks. Wireless communication and mobile computing, 6(3):307–318, 2006.
[8] F. Zhao and L. Guibas. Wireless sensor networks. Elsevier Inc, pages 23–24, 2004.
[9] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, ―Wireless sensor network security: A survey,‖ in Security in Distributed, Grid, and Pervasive Computing, Y. Xiao, Ed. Boca Raton, FL: CRC, 2007
[10]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.
[11] A. Rasheed and R. Mahapatra, "An Efficient Key Distribution Scheme for Establishing Pairwise Keys with a Mobile Sink in Distributed Sensor Networks," Proc. IEEE 27th Int'l Performance Computing and Comm. Conf. (IPCCC '08), pp. 264-270, Dec. 2008.
[12] A. Rasheed and R. Mahapatra, "A Key Pre-Distribution Scheme for Heterogeneous Sensor Networks," Proc. Int'l Conf. Wireless Comm. and Mobile Computing Conf. (IWCMC '09), pp. 263-268, June 2009.
[13] A. Rasheed and R. Mahapatra," 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.
[14]J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey,‖ in *Security in Distributed, Grid, and Pervasive Computing*," Y. Xiao, Ed. Boca Raton, FL: CRC, 2007.
[15]Sencun Zhu, Sanjeev Setia , Sushil Jajodia **,** "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks" Proc. 10th ACM Conf. Computers and Comm. Security (CCS '03), pp. 62-72, Oct. 2003.
[16] Deng, Y. S. Han, S. Chen, and P. K. Varshney. A Key Management Scheme for Wireless Networks Using Deployment Knowledge. In *The 23rd Conference of the IEEE Communications Society (Infocom)*, Hong Kong, March 2004.
[17] H. Chan, A. Perrig, and D. Song, "Key Distribution Techniques for Sensor Networks," Wireless Sensor Networks, pp. 277-303, Kluwer Academic, 2004.
[18] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," Proc. 10th ACM Conf. Computers and Comm. Security (CCS '03), pp. 62-72,Oct. 2003.
[19] 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.
[20] Sanjay Kumar, Deepti Dohare and Mahesh Kumar "An Efficient Key Distribution Scheme for Wireless Sensor Networks using polynomial based schemes" 2012 International Conference on Information and Network Technology (ICINT 2012).
[21] Zhiguo Wan, Kui Ren, Bo Zhu, Bart Preneel, and Ming Gu, "Anonymous User Communication for Privacy Protection in Wireless Metropolitan Mesh Networks,"ieee transactions on vehicular technology, vol. 59, no. 2, February 2010.