ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 2, February 2013

Security and Privacy in Emerging Wireless Networks with Mobile Sinks

S.Rajeshwari, R.Santhosh

Abstract **Mobile sinks (MSs) are more significant in many wireless sensor network (WSN) applications for well-organized data gathering and for unique and revoking compromised sensors. Mobile sinks are act as intermediate node. However, in sensor networks that make use of pairwise key establishment and authentication between sensor nodes and mobile sinks. In existing describes a three-tier general structure that permits the use of any pairwise key pre-distribution scheme. It requires two separate key pools, one for the mobile sink to entrance the network, and one for pairwise key establishment between the sensors. In addition it reduces the compensation caused by stationary access node replication attacks and improved the security performance of the proposed scheme of stationary access node replication attack.**

***Index Terms*— Distributed, Security, Thread, Wireless Sensor Network.**

I. INTRODUCTION

New advances in electronic technology have covered the way for the development of a new generation of wireless sensor networks (WSNs) [1] that make use of such sensors that follows (a) sense particular parameters connecting to their location, (b) procedure them either nearby or in a scattered method, and (c) correspond the processed information to Base station which in turns one or more central processing centers (CPCs). Such sensor networks can be used in a wide range of applications, such as Patient Tracking over a Wireless Network [2] and habitat monitoring [1]. The sensed data after need to be send back to the base station. However, when the sensing field is too distant from the base station, transmitting the data over lengthy distances using multi hop may fail the safety power (e.g., some middle can adjust the data transient by, capturing sensor nodes, debut a wormhole attack [3], a Sybil attack [4], discriminating forwarding [5], [6], sinkhole attack [7]), and increase the power utilization at nodes near the base station, dropping the lifetime of the network. Therefore, mobile nodes are important components in many sensor network applications, including data set in dangerous environments [8], [9], [10], restricted reprogramming and armed forces steering [11].

Manuscript received Feb 10, 2013.

S.Rajeshwarii, *Department of Computer Science and Engineering, Karpagam University, Coimbatore, Tamilnadu.*

R.Santhosh, *Department of Computer Science and Engineering, Karpagam University, Coimbatore, Tamilnadu.*

In a lot of these applications, sensor nodes send out serious in rank over the network; therefore, security services, authentication and pairwise key establishment are important. Conventional schemes in ad hoc networks using asymmetric keys are costly due of their storage and addition cost. These limitations make key pre-distribution schemes [12]-[18] the tools of choice to provide low cost, safe communication.

Though, the basic probabilistic [12] and q-composite [13] key pre-distribution schemes used for stationary access node replication attacks can simply find a huge number of keys by capturing a little portion of the network sensor nodes, building it likely for the assailant to take control of the whole network by deploying a virtual mobile sink, preloaded with some compromised keys to validate and then start data message with any sensor node.

In three-tier safety framework that uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool and also using two separate key pools and having few sensor nodes that carry keys from the mobile key pool will make it other complex for the assailant to start a mobile sink replication attack on the sensor network by capturing only a few illogical sensor nodes. Somewhat, the attacker would also have to incarcerate sensor nodes that take keys from the mobile key pool. Keys from the mobile key pool are used mainly for mobile sink authentication, and thus, to gain admission to the network for in sequence congregation.

To build the three-tier security scheme more strong means the authentication mechanism between the stationary access nodes and sensor nodes should be stronger by using one-way hash chains algorithm [20] in conjunction with the static polynomial pool-based scheme [14] and MD5 algorithm [21] in the use of key generation. In analytical results indicate that the sensing field is too distant from the base station, transmitting the data over lengthy distances increase the power utilization and dropping the lifetime of the network. So reduce the above problem, introduce the proposed scheme using Diffie Hellman Key agreement algorithm for new security method makes the network suppler to both mobile sink replication attacks and stationary access nodes replication attacks compared to the single polynomial pool-based approach.

To help the study of a general three tier safety framework for certification and pairwise key organization, based on the polynomial pool-based key pre distribution scheme [14]. The future method will significantly advance network suppleness to mobile sink imitation attacks compared to the three tier security framework, as an attacker would have to concession many more sensor nodes to launch a successful mobile sink replication attack.

This paper is organized as follows. Section 2 presents the security and threat analysis for a three tier security framework [19]. Section 3 shows the algorithms. Section 4 shows the security and threat analysis for proposed scheme. Section 5 shows the Simulation result and Section 6 draws conclusions.

II. The Three Tier Security Frame Structure

In this plan used two split polynomial pools: the mobile polynomial pool and the fixed polynomial group. Polynomials from the portable polynomial group are second-hand to found the verification between mobile sinks and inactive contact nodes, which will allow these mobile sinks to access the sensor network for statistics congregation. Thus, an attacker would need to give and take at least a single polynomial from the mobile pool to increase admittance to the network for the sensor's records crowd. Polynomials from the static polynomial pool are used to determine the confirmation and keys complex between the sensor nodes and stationary access nodes.

Prior to operation, each mobile sink arbitrarily picks a subset of polynomials from the mobile polynomial pool. In this idea to get better the network flexibility to mobile sink duplication attack as compared to the single polynomial pool based move toward, and also propose to minimize the probability of a mobile polynomial being compromised. As a challenger can use the captured mobile polynomial to open a mobile sink duplication attack, and achieve this by having a little part of erratically

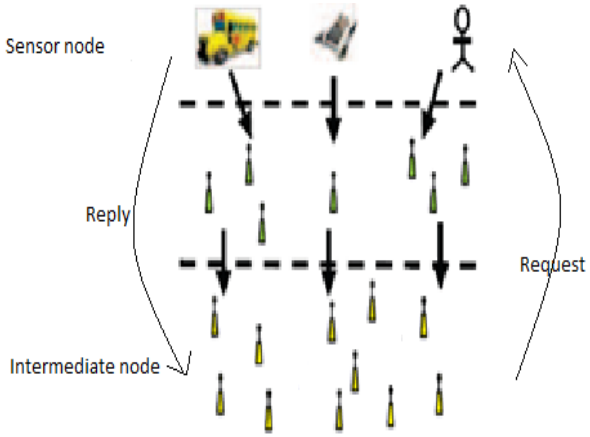

Fig.1.The three-tier security structure work flow process

chosen sensor nodes take a polynomial from the mobile polynomial pool. The three tier security structure working flow process is shown in the above Fig 1.

The working flow processes of the sensing data are stored in the sensor node. The collecting data are transmitted to the intermediate node. One way hash chain algorithm [20] is used to sequent transmits the data from sensor node to intermediate node. Then the password provide to the sensor node and intermediate node by using the MD5 algorithm [21]. In the intermediate node after collecting the data from sensor node the request message send to the sensor node. After getting the reply message from the sensor node, that's the authentication secure was positive (password was same or same sequence) then only the intermediate node was transmitted to the destination. All sensor nodes, as well as the inactive access nodes, arbitrarily choose a division of polynomials from the standing polynomial pool. The improvement of using part pools is that mobile sink verification is self-governing of the key allocation scheme used to attach the sensor network.

2.1 Security Analysis

To analyzed the performance of this process using two metrics: security and connectivity [19]. For safety, the prospect of a mobile polynomial creature compromised; hence, an attacker can formulate apply of the captured mobile polynomial to commence a mobile sink imitation attack next to the sensor network. In connectivity, the chance of a mobile sink establishing safe and sound relatives with the sensor nodes from any substantiation access point in the network.

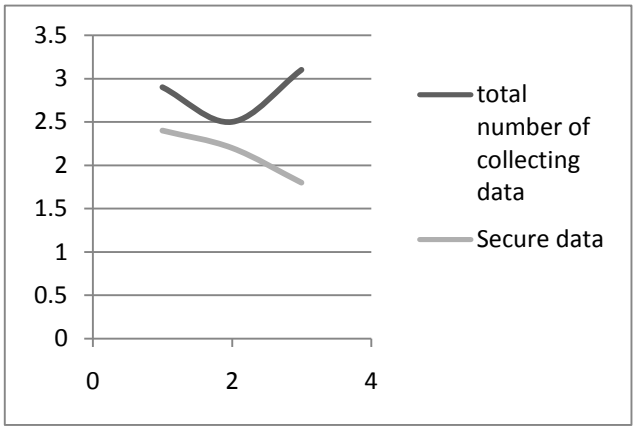

Fig.2. Variation of the number of collecting data and Secure data

To analyze the safety routine of the mobile sink replication attack. As confirmed in the earlier section, for an attacker to open a mobile sink copying bother on the network, the enemy has to conciliation at slightest one polynomial from the mobile polynomial pool. To reach this, the challengers have to incarcerate at least an explicit number of stationary access nodes that grip the matching mobile polynomial. The results are shown in the Fig 2. It follows from the sanctuary study of the Blundo plan, that for one polynomial in the mobile polynomial pool of level, an invader cannot recuperate the polynomial, if no more than at a standstill contact nodes that had selected are captured by the assailant.

2.2 Threat Analysis

In the inactive access node replication attack, the challenger wants to capture at least one polynomial from the static pool and at least one hash value of a selected code word. To analyze the safety routine of the three-tier scheme, estimated probability of a noncom promised sensor node creature under in mobile access node duplication attack. The challenger must detain at least a precise number of motionless admission nodes that embrace the identical portable polynomial. It follows beginning the safety examination of the Blundo format that for any polynomial in the portable polynomial group of degree. An assailant cannot pick up the polynomial, if no more than motionless access nodes that had selected to capture by the invader. If extra than motionless admission nodes with their movable polynomial are captured by the aggressor, then the aggressor can get better the transportable polynomial and thus be clever to start a

transportable go under duplication assault beside the antenna network.

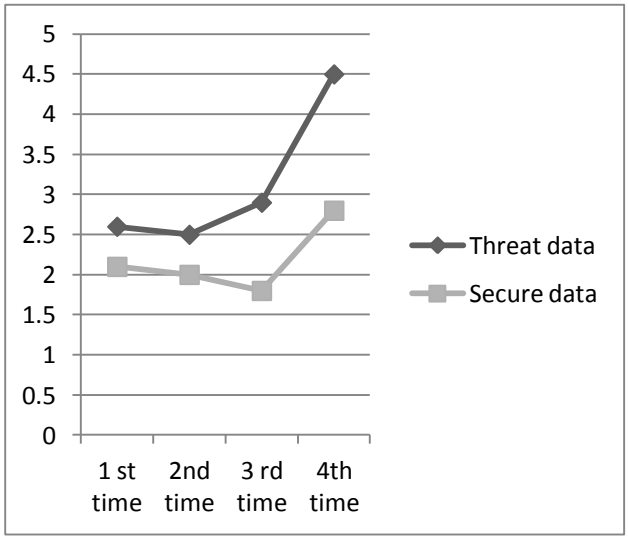

Fig.3. Difference between Secure data and unsecure data

Fig. 3 shows the variation of the secure and unsecure data. In three tier security structure have some disadvantages like the increase power utilization and dropping the lifetime of the network due to the more unsecure data in the transmitting time.

III. Authentication Algorithms

Three various algorithms are used to implement this concept for randomly key distribution, password authentication and improve the transmission of the secure data.

a. One Way Hash Chain Algorithm

The One way hash chain algorithm is used to randomly send the data from one end to another. Hash function h: u->v have some properties.

- The function h takes a message of random duration as the go into and produces a message digest of fixed length as the output.
- The function h is one way in the sense that given u, it is easy to compute h(u)=v.
- Given u, it is computationally infeasible to find u`.
- It is computationally infeasible to find any pair u, u`.

b. MD5 Message-Digest Algorithm

The MD5 algorithm [21] takes as enter a message of uninformed length and produces as productivity a 128-bit "fingerprint" or "message digest" of the contribution. It is conjectured that it is computationally infeasible to manufacture two communications having the equal message process, or to manufacture any message having a given pre specified objective message digest. It is used for digital cross applications, where a great file must be "condensed" in a safe way before being encrypted with a secret key.

c. Diffie Hellman Algorithms

Diffie Hellman prospect a key agreement idea for production harmony on an assembly key over concerned networks. The method allows two parties converse both other in a safe announcement with a decided assembly key. Its safety measures are based on solving separate logarithm trouble.

IV. Proposed Scheme

The proposed system based on the Diffie Hellman key agreement algorithm. In this process overcome the disadvantages of the three tier frame structure about the transmitting the data over lengthy distances, increase the power utilization, dropping the lifetime of the network and more unsecure data to been send. In this algorithm was allows two parties converse both other in a safe announcement with a decided assembly key.

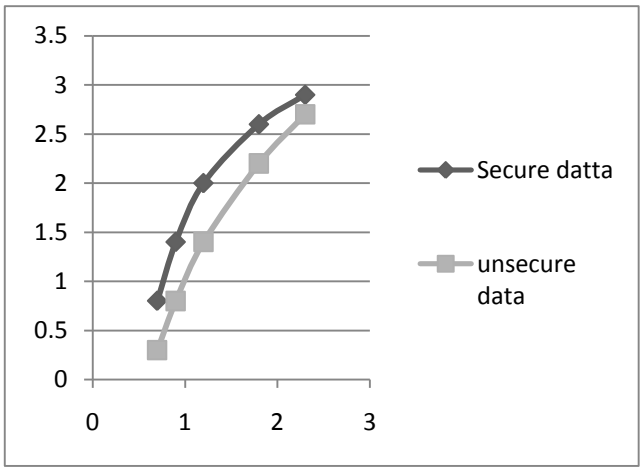

Fig.4. Proposed Scheme Result

Fig 4 shows the result of the proposed scheme compared between secure and unsecure data. The result is fewer amounts of unsecure data were arrived and also that data was found using the Diffie Hellman algorithm. The advantages of the proposed scheme were increased the lifetime of the network, fast transmitted secure data with timely manner.

V. Simulation

This project was developed using NS2 simulation. The NS2 was selected as the simulator in part because of the choice of skin it provides or partially because it has a release foundation code this can be adapted or complete.

Network simulator (NS) is not an object–oriented, separate occurrence simulator for networking investigates. NS provides large hold for replication of TCP, routing over hyper or wireless networks. The simulator is not a result of an ongoing effort of research or developed. Even though there is not a considerable confidence in NS, it is not a polished product yet or bugs is being discovered or corrected continuously.

NS is not printed in C++, with an OTcl1 analyst as a control or pattern boundary. The C++ part, which is not speedy to run but stifle to modify, is not used for thorough procedure execution. The Otcl fraction, on the additional hand, which

runs much hole but can be misrepresented extremely quickly promptly, is not used for reproduction pattern. One of the payments of the not split-language plan move toward is not this it allows for quick production of huge scenarios. To minimally use the simulator, it is not enough to know OTcl. On the other hand over, one drawback is not this modifying or extending the simulator requires encoding or debugging in equally languages.

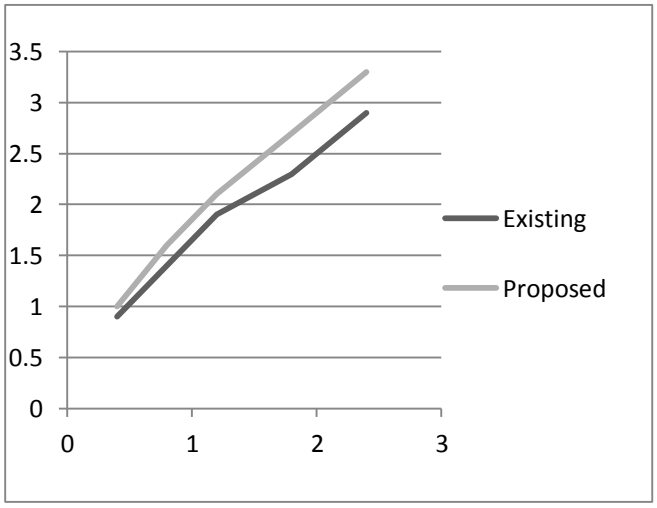

Fig.5 Simulation Result

The result of the simulation increased the security, lifetime and performance of transmitting data in the proposed scheme compared to the existing system. Fig 5 shows the result of simulation.

VI. CONCLUSION

This paper, the proposed scheme of reduces the compensation caused by stationary access node replication attacks and improved the security, performance and lifetime of the transmitting data used by increase the verification device between inactive access nodes and antenna nodes. Diffie Hellman algorithm is used to increase the above process. A common three-tier frame structure for certification and pairwise key organization between portable sinks and antenna nodes. Using two breaks up key pools and having little inactive contact nodes transport polynomials from the portable pool in the system can delay an assailant from assembly sensor data. In future analyzed indicates that 20% of security, performance and lifetime of the transmitting data were increased compared to the three tier frame structure.

REFERENCES

[1] 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.

[2] 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.

[3] L. Hu and D. Evans, "Using Directional Antenna to Prevent Wormhole Attacks," Proc. Network and Distributed System Security Symp., 2004.

[4] J.R. Douceur, "The Sybil Attack," Proc. First Int'l Workshop Peer-to-Peer Systems (IPTPS '02), Mar. 2002.

[5] 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.

[6] H. Deng, W. Li, and D.P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," Proc. IEEE Comm. Magazine, pp. 70-75, 2002.

[7] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," Proc. MobiCom, pp. 56-67, 2000.

[8] A. Kansal, A. Somasundara, D. Jea, M. Srivastava, and D. Estrin, "Intelligent Fluid Infrastructure for Embedded Networks," Proc. Second ACM Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '04), June 2004.

[9] Y. Tirta, Z. Li, Y. Lu, and S. Bagchi, "Efficient Collection of Sensor Data in Remote Fields Using Mobile Collectors," Proc. 13th Int'l Conf. Computer Comm. and Networks (ICCCN '04), Oct. 2004.

[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] W. Zhang, G. Cao, and T. La Porta, "Data Dissemination with Ring-Based Index for Wireless Sensor Networks," Proc. IEEE Int'l Conf. Network Protocols (ICNP), pp. 305-314, Nov. 2003.

[12] 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.

[13] H. Chan, A. Perrig, and D. Song, "Random Key Pre-Distribution Schemes for Sensor Networks," Proc. IEEE Symp. Research in Security and Privacy, 2003.

[14] 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.

[15] H. Chan, A. Perrig, and D. Song, "Key Distribution Techniques for Sensor Networks," Wireless Sensor Networks, pp. 277-303, Kluwer Academic, 2004.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] L.Lamport, "Password Authentication with Insecure Communication," Comm. ACM, vol, 24, no. 11, pp. 770-772, Nov. 1981.

[21] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences," Proc. 12th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '92), pp. 471-486, 1993.

[22] R. Rivest, "The MD5 Message-Digest Algorithm," RFC 1321, Apr. 1992.

S.Rajeshwari received her B.E degree in Computer Science and Engineering from Sri Subramanya College of Engineering and Technology palani in 2011 and currently doing her M.E-Computer Science and Engineering degree in Karpagam University.

R.Santhosh received his B.Tech degree in Information Technology from K.S.R College of Technology in 2006, M.E degree in Software Engineering from Sri Ramakrishna Engineering College in 2009, M.B.A in Education Management from Alagappa University in 2011 and pursuing Ph.D in Computer Science and Engineering at Karpagam University. He is currently working as an Assistant Professor in the department of Computer Science and Engineering at Karpagam University.