ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013

AN EFFICIENT SECURITY SCHEME PROVIDING AUTHENTICATION AND PAIRWISE KEY DISTRIBUTION WITH MOBILE SINKS IN WSN'S

Uma P[1], Manjula Devi T H[2]

Student, Department of Telecommunication Engineering, Dayananda Sagar College Of Engineering, Bangalore, Karnataka, India[1]

Associate Professor, Department of Telecommunication Engineering, Dayananda Sagar College Of Engineering, Bangalore, Karnataka, India[2]

Abstract: 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.

Keywords: Pair wise key pre distribution, Mobile polynomial pool, Static polynomial pool

I. INTRODUCTION

Wireless sensor networks have become ubiquitous and pervasive in applications such as military, health monitoring, data acquisition in hazardous environment, and habitat monitoring. A typical sensor network may include hundreds to several thousands of sensor nodes that are low cost, and have limited computation power and energy consumption. There are three types of communication in a sensor network: sensor to sensor, sensor to sink, and sink to sensor. Here we focus on a sensor network that uses mobile sink to gather sensor data. Security is a critical issue when sensor networks are deployed in hostile environment where they are exposed to a variety of malicious attacks. For eg., an adversary can easily monitor the traffic, capture sensor nodes, impersonate a mobiles sink to gather sensor data and provide misleading information. In many of these applications, sensor nodes transmit critical information over the network. Therefore security services such as authentication and pair-wise key establishment between sensor nodes and mobile sinks are important. However the resources constraints of the sensors and their nature of communication over a wireless medium make data confidentiality and integrity a non-trivial task. To overcome the sink and nodes replication attacks, a three tier security scheme is developed that make use of any pair-wise key pre-distribution scheme as its basic component, to provide authentication and pair-wise key establishment between sensor nodes and mobile sinks. This technique will improve the network security to mobile sink replication attacks compared to the previous schemes where an attacker has to compromise many sensor nodes in the network to achieve a successful mobile sink replication attack. Although the above security approach makes the network more resilient to mobile sink replication attack, it is still vulnerable to stationary access node replication attack. To make three tier security scheme more effective against a stationary access node replication attack, we have strengthened authentication mechanism between stationary access nodes and sensor nodes using one way hash algorithm in conjunction with static polynomial pool based scheme.

II. RELATED WORK

Amar Rasheed et.al., [1] developed a general framework that permits the use of any pairwise key pre distribution scheme as its basic component to provide authentication and pairwise key establishment between sensor nodes and mobile sinks.John R. Douceur., [2] discussed that large scale peer to peer systems face security threats from faulty or hostile remote computing elements. Yuldi Tirta et.al., [3] explained the use of mobile collectors also reduce the necessity of multi-hop routing so that energy of intermediate nodes can be conserved and only few collectors are needed and they can be re-fuelled easily than recharging thousands of sensor nodes.Wensheng Zhang et.al., [4] introduced an index based data dissemination which avoids both unnecessarily transferring sensing data and flooding control

messages to whole network. Laurent Eschenauer et.al., [5] discussed that distributed sensor networks (DSN) are ad hoc mobile network that include sensor nodes with limited computation and communication capabilities. This scheme relies on probabilistic key sharing among the nodes of a random graph and uses a simple shared key discovery protocol for key distribution revocation and node re-keying. Haowen chan et.al., [6] discussed q-composite random key pre-distribution scheme and multipath key reinforcement scheme to address boot strapping problem. Donggang Liu et.al., [7] discussed closest pair-wise key pre-distribution scheme and a location based pair-wise key scheme using bivariate polynomial for providing security to sensor nodes. Sencun Zhu et.al., [8] described that LEAP (Localised Encryption And Authentication Protocol), a key management protocol for sensor network that is designed to support in network processing, while providing security properties similar to those provided by pair-wise key sharing schemes. Amar Rasheed et.al., [9] 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 guarantees that any sensor node can establish a pair wise key with a mobile sink with high probability and without sacrificing security. A. Rasheed et.al., [10] described a key distribution scheme based on random key pre distribution for heterogeneous sensor network to achieve better performance and security as compared to homogenous network. The proposed scheme reduces the storage requirements by using generation keys. Leslie Lamport et.al., [11] discussed that in remotely accessed computer systems, a user identifies him to the system by sending a secret password. The method uses one way encryption function. Gaining access to stored information can be eliminated by using one way function to encode the password.

III. PROBLEM DESCRIPTION

In this paper, two separate polynomial pools: mobile polynomial and static polynomial pools are used to provide clear security guarantee. The polynomials from the mobile polynomial pool are used to establish the authentication between mobile sinks and stationary access nodes, which will enable these mobile sinks to access sensor network for data gathering. Polynomials from static polynomial pool are used to ascertain the authentication and key setup between sensor nodes and stationary access nodes. The main aim is to provide authentication and pair-wise key establishment between sensor nodes and mobile sinks which substantially improve network resilience to mobile sink replication attacks.

IV. EXISTING SYSTEM

In the basic probabilistic and q-composite key pre-distribution schemes, an attacker can easily obtain large number of keys by capturing a small fraction of network sensor nodes, making it possible for the attacker to take control of the entire network by deploying replicated mobiles sink, preloaded with some compromised keys to authenticate and then initiate data communication with any sensor node. Traditional schemes in ad-hoc networks using asymmetric keys are expensive due to their storage and computation cost. These limitations make key pre-distribution schemes the tools of choice to provide low cost, secure communication between sensor nodes and mobile sinks. In basic probabilistic key distribution each sensor node randomly picks a set of keys from the key pool before deployment, so that any two sensor nodes had a certain probability of sharing at least one common key. The q-composite key pre distribution scheme is based on the basic probabilistic scheme but it requires two sensors to share at least q-pre distributed keys to establish a pair wise key.

V. PROPOSED SYSTEM

A general framework is developed in order to provide authentication and pair-wise key establishment, based on polynomial pool based key pre-distribution scheme. The proposed technique will improve network resilience to mobile sink replication attacks as an attacker would have to compromise many more sensor nodes to launch a successful mobile sink replication attack. The scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool and hence more security is provided than previous approaches. A mobile sink sends data request messages to the sensor nodes via a stationary access node. These data request messages from the mobile sink will initiate the stationary access node to trigger sensor nodes, which transmit their data to the requested mobile sink.

A. PROPOSED SYSTEM ARCHITECTURE

Fig. 1 represents the overall flow of the project. The stationary access nodes shown above act as authentication access points to the network to trigger the sensor nodes to transmit their aggregated data to the mobile sinks. A mobile sink sends data request message to the sensor nodes via stationary access nodes. These data request messages from the mobile sink will initiate the stationary access node to trigger sensor nodes, which transmit their data to requested mobile sink. The proposed scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. Polynomials from mobile polynomial pool are used to establish authentication between mobile sinks and

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013

stationary access nodes 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 nodes.

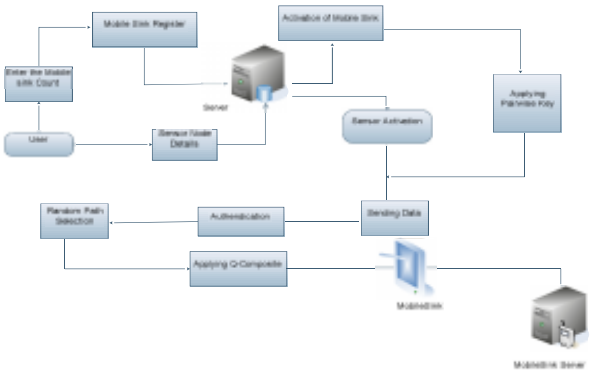


Fig 1: General Three Tier Scheme

B. SENSOR NODE DEPLOYMENT

In this module, we create many sensor nodes. Users enter the sensor name, IP address, port number and status of the node to register in the database. While entering the next node user has to check in the database where that node already exists in the database. Later for activation of sensor nodes the user should enter the details of the particular sensor node which he wants to activate and click on the activate icon that appears in the dialogue box and the nodes get successfully activated.

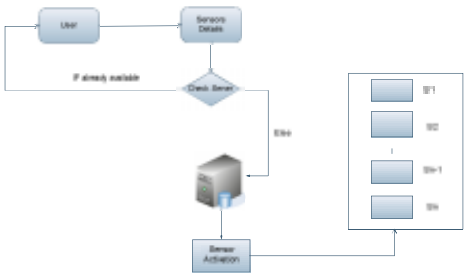


Fig 2: Sensor node deployment

C. *CREATING MOBILE SINKS*

In this module, we create mobile sink. User should enter the number of mobile sinks he wants to create, mobile sink name, I P Address, port number, status of the mobile sink to register in the Database. While entering the next mobile sink user has to check in the database where that particular mobile sink already exists in the database. Later for successful activation of mobile sink, user shuld enter the details of the mobile and click on the activate icon.

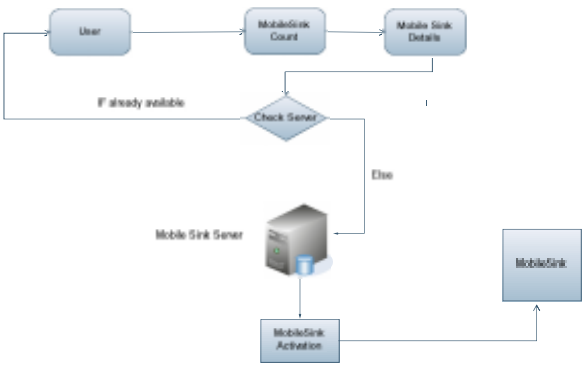


Fig 3: Creating mobile sinks

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013

D. AUTHENTICATION AND PAIR WISE KEY DISTRIBUTION

In this module, we are going to authenticate all the sensor node and mobile sink and these authenticated mobile sinks are managed by polynomial pool both static as well as dynamic. Using two separate key pools and having few sensor nodes that carry keys from the mobile key pool will make it more difficult for the attacker to launch a mobile sink replication attack on the sensor network by capturing only a few arbitrary sensor nodes. Rather, the attacker would also have to capture sensor nodes that carry keys from the mobile key pool. Keys from the mobile key pool are used mainly for mobile sink authentication, and thus, to gain access to the network for data gathering.

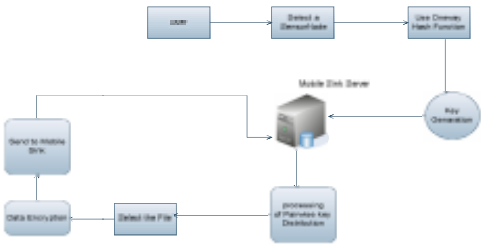
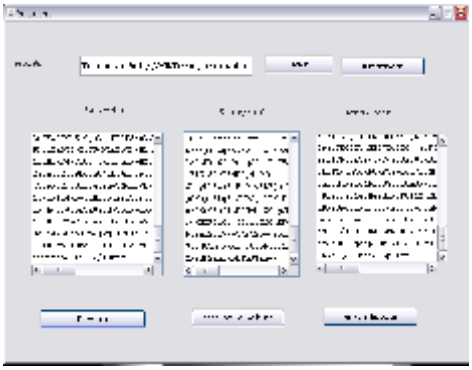


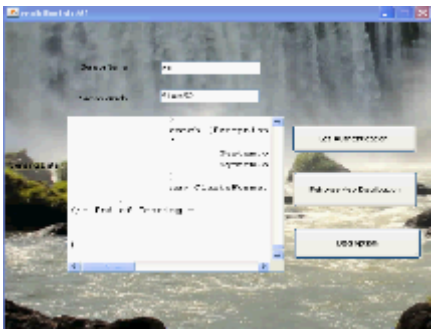
Fig 4: Pair wise key distribution scheme

VI. RESULTS

ISSN: 2319-8753

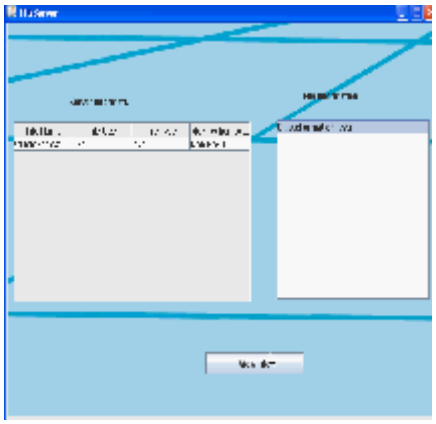
International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013





ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013



VII. CONCLUSION

The proposed scheme based on polynomial pool based pre distribution scheme substantially improves network resilience to mobile sink replication attack compared to single polynomial pool based pre distribution approach. Analysis indicates that with 10 percent of sensor nodes in the network carrying a polynomial from the mobile pool, for any mobile polynomial to be recovered, the attacker would have to capture 20.8 times more nodes as compared to the single polynomial pool approach.

REFERENCES

[1] Amar Rasheed, Rabi N Mahapatra, "The Three Tier scheme in wireless sensor networks with mobile sinks", IEEE Trans. Parallel and Distributed Systems, vol 23, Issue 5, pp. 958-965, May.2012
[2] J.R. Douceur, "The Sybil Attack," Proc. First Int'l Workshop Peer-to-Peer Systems (IPTPS '02), Mar. 2002.
[3] 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 (ICCN '04), Oct. 2004.
[4] 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.
[5] 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.
[6] H. Chan, A. Perrig, and D. Song, "Random Key Pre-Distribution schemes for sensor Networks," Proc. IEEE Symp. Research in Security and Privacy, 2003.
[7] D. Liu, P. Ning, "Location-Based Pairwise Key Establishments for static Sensor Networks," wireless Sensor Networks, pp. 277-303, Kluwer academic, 2004.
[8] S. zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Secuity Mechanisms for Large-scale Distributed sensor Networks," Proc. 10th ACM Conf. Computers and Comm. Security (CCS '03), pp. 62-72, Oct. 2003.
[9] 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.
[10] A. Rasheed and R. Mahapatra, "A Key Pre-Distribution Scheme for heterogenouse Sensor Networks," Proc. Int'l Conf. Wireless Comm. And Mobile Computing Conf. (IWCMC '09), pp. 263-268, June 2009.
[11] L. Lamport, "Password Authentication with Insecure Communication," Comm. ACM, vol, 24, no. 11, pp. 770-772, Nov. 1981.