Enhanced Three Tier Security Scheme for Data Transfer in Mobile Sensor Networks by Using Mobile Sinks

Kadiri Sireesha [#1], Mr. Jagadish Gurrala[*2]

M.Tech Scholar [#1], Assistant professor[*2]

Department of Computer Science & Engineering,
Anil Neerukonda Institute of Technology & Sciences
Bheemunipatnam (Municipality), Sangivalasa - 531162
Vishakapatnam (District), AP (INDIA).

Abstract

A **wireless sensor network (WSN)** of spatially distributed autonomous sensors 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. Mobile sinks (MSs) plays a very important role in many wireless sensor network (WSN) applications for efficient data accumulation, localized sensor reprogramming, and for distinguishing and revoking compromised sensors. Mobile sinks provides a great security in WSN as there was a lot of chance for attacker to easily obtain the keys by capturing a small fraction of nodes which in turn leads to gain the control of the network. In this paper we mainly describe a three-tier general framework that permits the use of any pairwise key predistribution scheme as its basic component. The proposed new framework requires two separate key pools, one key is used for authentication between mobile sink (client) to Access Point or Router in order to access the network, and another for pairwise key establishment between the server and router . As an enhancement we have also implemented a security of data by encrypting the data and giving security with the help of AES encryption algorithm,inorder to give more security for the data while transferring from server to client. Our simulation results clearly tells that our new three tier security framework has higher network resilience to a mobile sink replication attack as compared to the polynomial pool-based scheme.

Keywords

Wireless Sensor Networks, Mobile Sinks, Distributed Environment, Autonomous, Replication Attack

1. Introduction

A **wireless sensor network (WSN)** of spatially distributed autonomous sensors 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.

Recent advances in electronic technology have laid the way for the development of a new generation of wireless sensor networks (WSNs) consisting of a large number of low-power, low-cost sensor nodes that communicate wirelessly [1]. Such sensor networks can be used in a wide range of applications, such as, military sensing and tracking, health monitoring [2], data acquisition in hazardous environments, and habitat monitoring [1]. The sensed data often need to be sent back to the base station for analysis. However, when the sensing field is too far from the base station, transmitting the data over long distances using multihop may weaken the security strength (e.g., some intermediate may modify the data passing by, capturing sensor nodes, launching a wormhole attack [3], a sybil attack [4], selective forwarding [5], [6], sinkhole [7]), and increasing the energy consumption at nodes near the base station, reducing the lifetime of the network. Therefore, mobile sinks (MSs) (or mobile soldiers, mobile sensor nodes) are essential components in the operation of many sensor network applications, including data collection in hazardous environments [8], [9], [10], localized reprogramming, oceanographic data collection, and military navigation [11].

In many of these applications, sensor nodes transmit critical information over the network; therefore, security services, such as, authentication and pairwise key establishment between sensor nodes and mobile sinks, are important. However, the resource constraints of the sensors and their nature of communication over a wireless medium make data confidentiality and integrity a nontrivial task. Traditional schemes in ad hoc networks using asymmetric keys are expensive due of their storage and computation cost. These limitations make key predistribution schemes [12], [13], [14], [15], [16], [17], [18] the tools of choice to provide low cost, secure communication between sensor nodes and mobile sinks.

However, the problem of authentication and pairwise key establishment in sensor networks with MSs is still not solved in the face of mobile sink replication attacks. For the basic probabilistic [12] and q-composite [13] key predistribution 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 node.

To address the above-mentioned problem, we have developed a general framework that permits the use of any pairwise key predistribution scheme as its basic component, to provide authentication and pairwise key establishment between sensor nodes and MSs. To facilitate the study of a new security technique, we first cultivated a general three-tier security framework for authentication and pairwise key establishment, based on the polynomial pool-based key predistribution scheme [14]. The proposed technique will substantially improve network resilience to mobile sink replication attacks compared to the single polynomial pool-based key predistribution approach [14], as an attacker would have to compromise many more sensor nodes to launch a successful mobile sink replication attack.

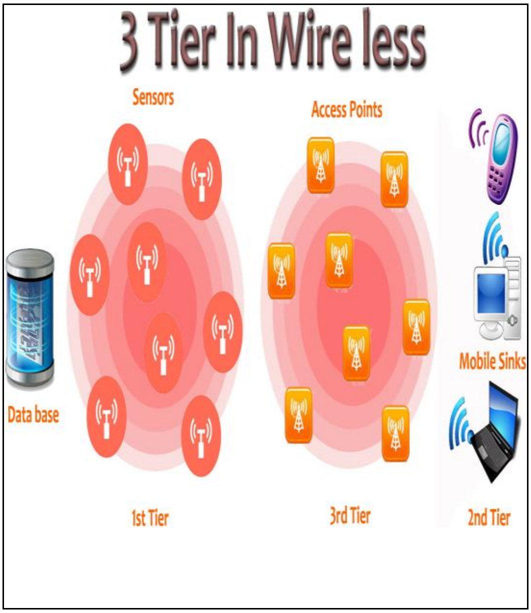

Figure. 1. Represents the three-tier security scheme in WSN with mobile sinks

2. Background Theory

In this section we will describe the background work and assumptions that are used in the proposed paper.

The key management problem is an active research area in wireless sensor networks. Eschenauer and Gilgor [12] proposed a probabilistic key predistribution scheme to bootstrap the initial trust between the sensor nodes. The main idea was to let each sensor node randomly pick a set of keys from a key pool before deployment, so that any two sensor nodes had a certain probability of sharing at least one common key. Chan et al. [13] further extended this idea and developed two key predistribution schemes: the q-composite key predistribution scheme and the random pairwise keys scheme. The q-composite key predistribution scheme also used a key pool, but required two sensor nodes to compute a pairwise key from at least q predistributed keys that they shared. The random pairwise keys scheme randomly picked pairs of sensor nodes and assigned each pair a unique random key. Both schemes improved the security over the basic probabilistic key predistribution scheme.

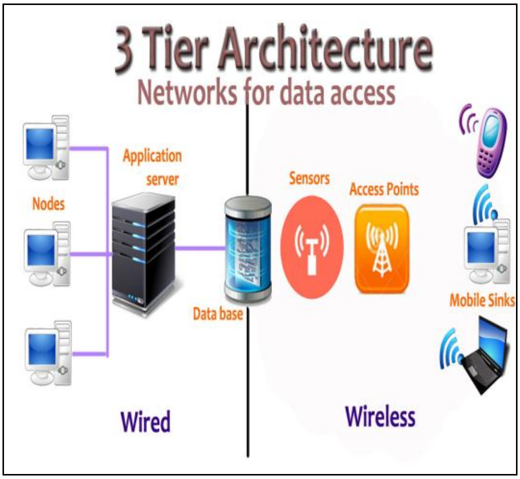

Figure. 2. Combined three-tier security scheme in WSN both Wired and Wireless Networks

3. The Enhanced Three-Tier Security Scheme

In this paper we are going to implement the enhanced three tier security scheme for providing a better security with the help of mobile sinks and also with the help of cryptography algorithm like AES for encrypting and decrypting the data while transferring through the network.

The three-tier security scheme provides better network resilience against mobile sink replication attack compared to the single polynomial pool approach. This scheme delivers the same security performance as the single polynomial pool approach when the network is under a stationary access node replication attack. In both schemes, for any sensor node u that needs to authenticate and establish a pairwise key with a stationary access node A, the two nodes must share at least a common polynomial in their polynomial rings. To perform a stationary access node replication attack on a network, the adversary needs to compromise at least a single polynomial from the static pool. This can be obtained easily by capturing arbitrary sensor nodes in the network. Then, the adversary can make use of this compromised polynomial by a replicated stationary access node to enable insecure access to the network. When successful access to the network has been obtained through the compromised static polynomial, the replicated stationary access node transmits recorded mobile sink data request messages. Next, the sensor nodes that have the compromised polynomial in their rings will insecurely authenticate and establish a pairwise key with the replicated node and thus deliver their data to the replicated node.

In this section, we remedy the security performance of the proposed scheme in the case of a stationary access node replication attack. We use an AES encryption algorithm as an enhancement of this paper in order to give security of the transferring data between client and server. This encryption technique gives a more security for the three tiers in wireless sensor networks.

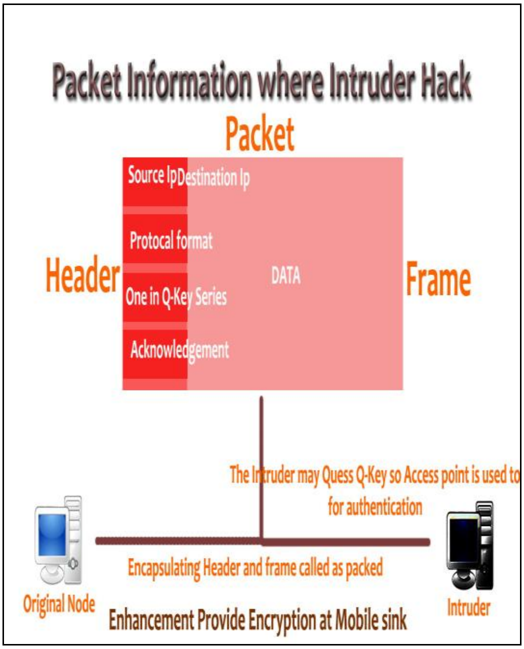
Packet Information where Intruder Hack
Packet
Source Ip
Destination Ip
Protocal format
One in Q-Key Series
Acknowledgement
Header
DATA
Frame
The Intruder may Quess Q-Key so Access point is used to
for authentication
Encapsulating Header and frame called as packed
Original Node
Intruder
Enhancement Provide Encryption at Mobile sink

Figure. 3. Represents the Enhanced three-tier security scheme in WSN by doing Encryption at Mobile Sink

4. Implementation Roles

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods. The proposed consists of totally four modules:

4.1 Server Creation Module

In this Module, we need to deploy a node separately as a server through which the server is able to operate the clients and routers which are connected in a distributed mobile environment. The server should be always in start state if the client or any router wants to process its task. If the server is in off state the client or Access point can't able to login into the system. In the server node we are going to configure the client and router system IP address.

4.2 Router Module

In this Module, we need to deploy a node separately as a router through which the server sends a key for activating the router in order to pass the data to the respective client which is assigned accordingly by the server. The router may be available either in same system or number of different systems if it is located in LAN.

4.3 Client Module

In this Module, clients can be any number of nodes which can deploy in different systems in LAN.The client has the facility to receive the data from the server in a secure manner through the configured path between server and router and in turn from router to client. During this transmission the client has a facility to substitute the key at the key substitution level in order to identify whether the data have been received from correct source or not. If the key is valid the client can receive the data which is send from the server, if not the client can't able to access the data.

4.4 Encryption Module

This is the last module in which we have used as an extension for our application where the data can be encrypted during the transfer between server to router and router to client. So this encryption module gives more security for the proposed application.

5. Conclusion

In this paper, we proposed a general three-tier security framework for authentication and pairwise key establishment between mobile sinks and sensor nodes. The proposed scheme, based on the polynomial pool-based key predistribution scheme substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key predistribution approach. Using two separate key pools and having few stationary access nodes carrying polynomials from the mobile pool in the network may hinder an attacker from gathering sensor data, by deploying a replicated mobile sink. Also in this paper we have implemented cryptography algorithm for encrypting the data during transfer between server and mobile sinks.

6. 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

ACMConf. 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.

7. About the Authors

Kadiri Sireesha is currently pursuing her 2 Years M.Tech (CSE) in Department of Computer Science and Engineering at Anil Neerukonda Institute of Technology & Sciences, Bheemunipatnam (Municipality), Sangivalasa, Visakhapatnam. Her area of interests includes Mobile Computing, Networks.

Mr. Jagadish Gurrala, received his Masters' in Computer Science and Technology with specialization in Computer Networks from Andhra University, Visakhapatnam. He is currently working as Assistant Professor in Anil Neerukonda Institute of Technology & Sciences, Visakhapatnam. His research interests include network security in wireless mobile networks, mobile ad hoc networks, cloud computing, performance analysis, Quality of Service on Routing protocols in MANET, Wireless sensor network. He published and presented many papers internationally.