ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

High Security Framework Using Pair-Wise Key Distribution in WSN with Mobile Sink

M.Pavithran, G.Kowsalya

PG student, Department of Computer Science and Engineering, Muthayammal Engineering College, Namakkal, India

Assistant Professor, Department of Information Technology, Muthayammal Engineering College, Namakkal, India

ABSTRACT: Wireless Sensor Networks are contains distributed sensor nodes to monitor physical or environmental conditions. The sensor nodes can exchange information or share data by using presented key predistribution schemes. So the attacker can easily take number of keys and using that keys attacker control the whole network or particular sensor node. So we proposed a high security framework using pair-wise key distribution. These frameworks use two separate key pools to provide security for all sensor nodes in Wireless Sensor Networks.

KEYWORDS: Wireless Sensor Networks; Security; Mobile polynomial pool; Static polynomial pool; Key Distribution

I. INTRODUCTION

A Wireless Sensor network is contains a huge number of sensor nodes that are deploy in a broad area with very low power-driven sensor nodes [1]. The sensor networks are capable of be consumed in a various information and telecommunications system applications. The nodes in WSN are very small devices among wireless communication capability that can collect information like temperature, motion, light, sound, etc and progression different sensed information and transfer it to the nearest other nodes to base station. The below Fig: 1 shows the scenarios of Wireless Sensor Network.

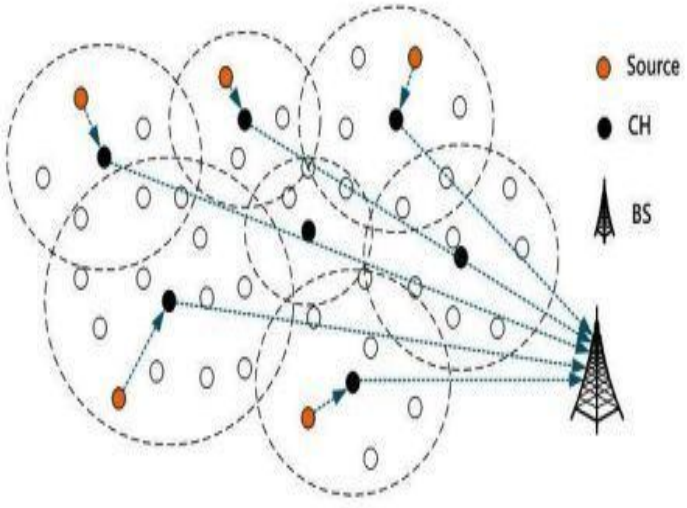

Fig.1. Wireless Sensor Networks

One of the major design goals of Wireless Sensor Networks is to carry out the data communication and prevents connectivity degradation [2]. Data sensing and reporting in WSNs is depending on the application. The Wireless Sensor networks are having different requirements rather than other wireless networks [3].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

The design of the routing protocols for Wireless Sensor Networks are challenging because of the several network constraints. This suffers from the limitations of several network resources, for e.g., central processing unit, energy, storage and bandwidth.

A. *Basic Characteristics of Wireless Sensor Networks:*

Wireless Sensor Networks contains the following Characteristics:

- Self Healing,
- Self Protection Capabilities,
- Self Configuration and
- Self Optimization

B. *Applications of Wireless Sensor Networks:*

In below we given some classic applications for Wireless Sensor Networks,

✓**Environmental applications:** Monitoring a large geographic area with human being there.
✓**Military applications:** To monitor and track the enemy troop movement or movements of terrorists.
✓**Industrial applications:** The low cost sensor nodes [4] are attached to the equipment to monitor performance.
✓**Medical applications**: Tracking of the functioning of the heart
✓**Urban applications:** Used in the security monitors in shopping malls, etc.

II. PROBLEM STATEMENT

The multiple sensor nodes are necessary to overcome environmental obstacles like obstructions, line of sight (LOS) constraints etc [5]. The Base station first sends the request to particular sensor node through all intermediate sensor nodes in WSN. The sensor node when get the request it check the key and verify it. If it's correct then only it shares the data to base station. The sensed data often need to be sent back to the base station for analysis. All sensor nodes use the keys to communicate data. But the attacker can create large number of keys and using that key too control entire networks or any sensor node and then start to data communication to any other sensor nodes.

The Base Station (BS) can send the request to any one sensor node means the attacker can send the data of any other node and can control the whole network. So the sink node and BS cannot get proper information or data. The structure of Wireless Sensor Networks with target node and sink node are shown in Fig: 2.

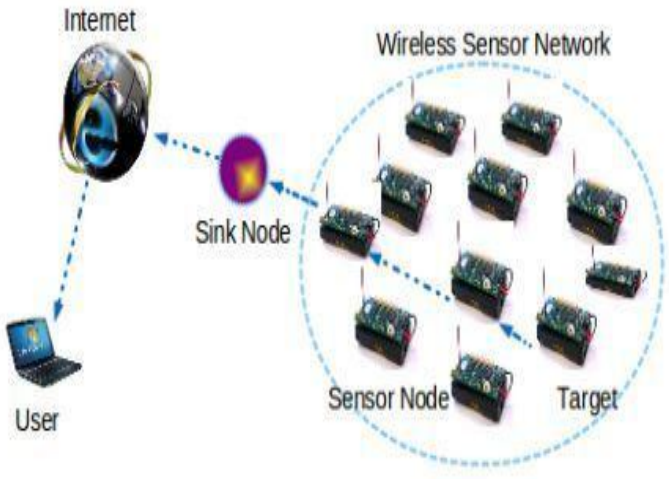

Fig.2. Wireless Sensor Networks with sink node

III. PROPOSED SYSTEM

The proposed system uses a high security framework called Three-tier Security Scheme using pair-wise key distribution in Wireless Sensor Networks (WSNs). These frameworks use two different key pools to provide security

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

for all sensor nodes in Wireless Sensor Networks. The general three-tier security framework for authentication and pair-wise key establishment is works based on the polynomial pool-based key predistribution scheme [6].
This scheme can be uses two separate polynomial pools:

A. Mobile Polynomial pool- It's authenticates between sink nodes and stationary access nodes.

B. Static Polynomial pool- It's authenticated and setup the keys between the sensor nodes and stationary access nodes.

Using these two different key pools and having some sensor nodes that carry unique keys from the mobile key pool will make it more difficult the attacker to launch the mobile sink replication attacks in the wireless sensor networks by capturing only a few arbitrary sensor nodes.
This Three-tier security scheme uses different keys for all sensor nodes i.e., any nodes cannot uses the same keys. These keys are generated in one key pool [7]. If any two nodes can communicates through a common shared key. The Three-tier security scheme can use the middle tier to compare two nodes and allow correct node to send correct data to sink node and Base Station (BS).

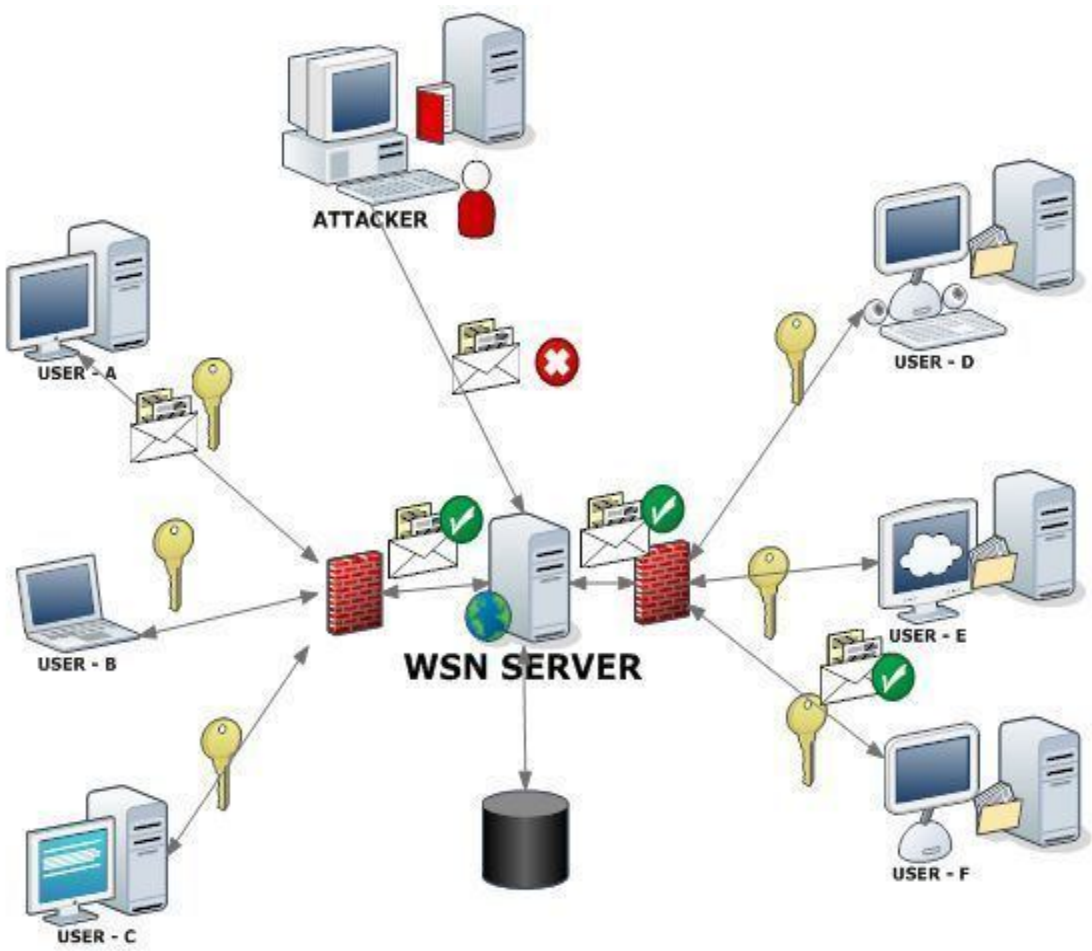

Fig.3. Working principles of predistribution key scheme in WSNs

IV. CONCLUSION AND FUTURE WORK

The three-tier security framework is uses the pair-wise key establishment between mobile sink node and sensor nodes. So it can get the data or information from correct sensor node. Because it uses the node comparison and authentication using predistributed key scheme. In future work, we investigate the new approach for provide high resiliency and eliminating the threats impose by captured keys by revoking.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

REFERENCES

1. D. Liu, and P. Ning, "Location-Based Pair wise Key Establishments for Static Sensor Networks," Proceedings of First ACM Workshop Security Ad Hoc and Sensor Networks, 2003.
2. H. Deng, W. Li, and D.P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," Proceedings of IEEE Communication Magazine, pp. 70-75, 2002.
3. C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," Proc. Mobicom, pp. 56-67, 2000.
4. 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.
5. Archana Bharathidasan, and Vijay Anand Sai Ponduru, "Sensor Networks: An Overview," Department of Computer Science University of California, Davis, CA 95616.
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. 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.