RESEARCH ARTICLE OPEN ACCESS

ADVANCED SECURITY TECHNIQUE THROUGH SENSOR NETWORK

S Amaresan M.C.A., M.Phil, M.E.,*, M Chandragandhi**
*(H.O.D., Assistant Professor, Department of Computer Science, PONNAIYAH RAMAJAYAM INSTITUTE OF SCIENCE AND TECHNOLOGY PRIST University, and THANJAVUR
Email: amaresan.cse.1974@gmail.com)
** (M.C.A., Scholar Department of Computer Science, PONNAIYAH RAMAJAYAM INSTITUTE OF SCIENCE AND TECHNOLOGY PRIST University, and THANJAVUR
Email: jaikuttychandra@gmail.com)

----------**********----------

Abstract:

Humans are frequently innovating new technologies to fulfill their needs. Wireless sensor networks (WSNs) are a still developing technology consisting of multifunction sensor nodes that are small in size and communicate wirelessly over short distances. Sensor nodes incorporate properties for sensing the environment, data processing and communication with other sensors. The unique properties of WSNs increase flexibility and reduce user involvement in operational tasks such as in battlefields. Wireless sensor networks can perform an important role in many applications, such as patient health monitoring, environmental observation and building intrusion surveillance. In the future WSNs will become an integral part of our lives. However along with unique and different facilities, WSNs present unique and different challenges compared to traditional networks. In particular, wireless sensor nodes are battery operated, often having limited energy and bandwidth available for communications. Mobile sinks (MSs) are vital in many wireless sensor network (WSN) applications for efficient data accumulation, localized sensor reprogramming, and for distinguishing and revoking compromised sensors. However, in sensor networks that make use of the existing key pre distribution schemes for pair wise key establishment and authentication between sensor nodes and mobile sinks, the employment of mobile sinks for data collection elevates a new security challenge: in the basic probabilistic and q-composite key pre distribution schemes, an attacker can easily obtain a large number of keys by capturing a small fraction of nodes, and hence, can gain control of the network by deploying a replicated mobile sink preloaded with some compromised keys. This article describes a three-tier general framework that permits the use of any pair wise key pre distribution scheme as its basic component. The new framework requires two separate key pools, one for the mobile sink to access the network, and one for pair wise key establishment between the sensors. Mobility is exploited in the field of wireless sensor network to circumvent multi-hop relaying and to reduce energy consumption at nodes near the base station, and hence elongate the lifetime of the network. Mobile elements already exist in the deployment environment; a network node can be attached to these mobile elements for data collection.

Keywords **— Mobile sinks (MSs), wireless sensor network (WSN), Applications, Mobility.**

----------**********----------

I. INTRODUCTION

Wireless sensor networks are potentially one of the most important technologies of this century. Recent advancement in wireless communications and electronics has enabled the development of low-cost, low-power, multifunctional miniature devices for use in remote sensing applications. The combination of these factors has improved the viability of utilizing a sensor network consisting of a large number of intelligent sensors, enabling the collection, processing analysis and dissemination of valuable information gathered in a variety of environments. A sensor network is composed of a large number of sensor nodes which consist of

sensing, data processing and communication capabilities. Instead of sending the raw data to the nodes responsible for the fusion, they use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data. Some of the popular applications of sensor network are area monitoring, environment monitoring (such as pollution monitoring), and industrial and machine health monitoring, waste water monitoring and military surveillance. In Mobile Sink Wireless Sensor Networks (MSWSN), all sensors are static other than the sink node. Mobile nodes are the destination of messages originated by sensors, i.e., they represent the endpoints of data collection in the network. They can either autonomously consume collected data for their own purposes or make them available to remote users by using a long range wireless Internet connection. In sensor nodes are static and densely deployed in the sensing area. One or multiple Mobile sinks (MS) move throughout the network to collect data from all sensors. Communication between the source sensors and the MS is either single hop or multi-hop. During the data collection technique in mobile sink sensor networks, security is an important factor. Node need to be authenticate before start the data collection process. At the same time sensors also need to authenticate the sink. After authentication takes place the start the data communication process with specified rule. During the data collection sensor send their data with encrypting the data packets and send it to the sink node. When sink receive the data it decrypt the packet and check for the adversary modification during data transmission. This node authentication, data encryption and decryption use different cryptography technology. Using cryptography function it secures the communication process.

II. OBTAINABLE METHOD

The key management problem is an active research area in wireless sensor networks. Proposed a probabilistic key redistributions 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. Further extended this idea and developed two key pre distribution schemes: the q-composite key pre distribution scheme and the random pair wise keys scheme.

III. PROJECTED METHOD

Proposed a general three-tier security 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 substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key pre distribution 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.

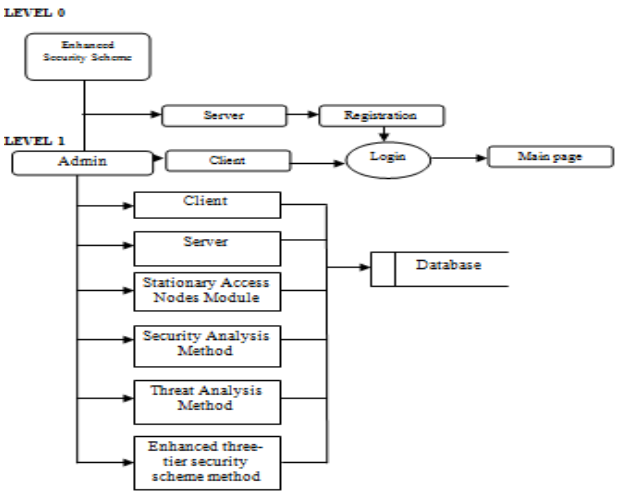

Fig 1 system diagram.

IV. COMPONENT NARRATIVE

A. Stationary access nodes section

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 the sensor network for data gathering. 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 ascertain the authentication and keys setup between the sensor nodes and stationary access nodes.

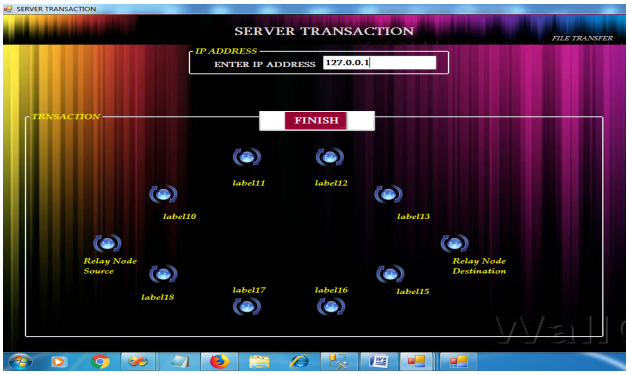

Fig2 Server transaction ***Stationary access nodes section***

B. Safety measures scrutiny section

An analysed the performance of the proposed scheme using two metrics: security and connectivity. For security, we present the probability of a mobile polynomial being compromised; hence, an attacker can make use of the captured mobile polynomial to launch a mobile sink replication attack against the sensor network.

C. Threat Analysis section

The security performance of the proposed scheme against a mobile sink replication attack. As stated in the previous section, for an attacker to launch a mobile sink replication attack on the network, the adversary has to compromise at least one polynomial from the mobile polynomial pool. To achieve this, the adversary must capture at least a specific number of stationary access nodes that hold the same mobile polynomial.

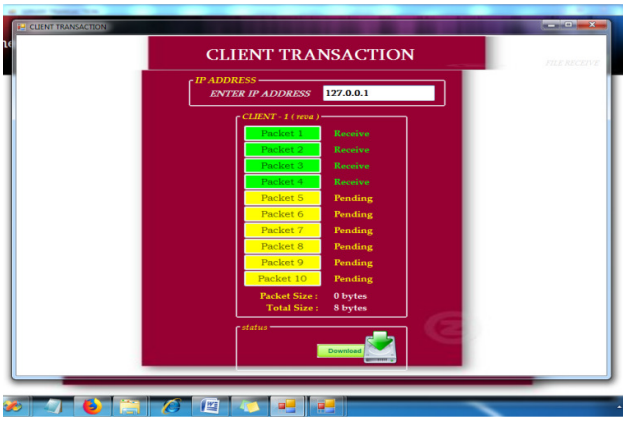

Fig 3 transaction analysis of session

D. Enhanced three-tier security scheme method

As described in the previous section, 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.

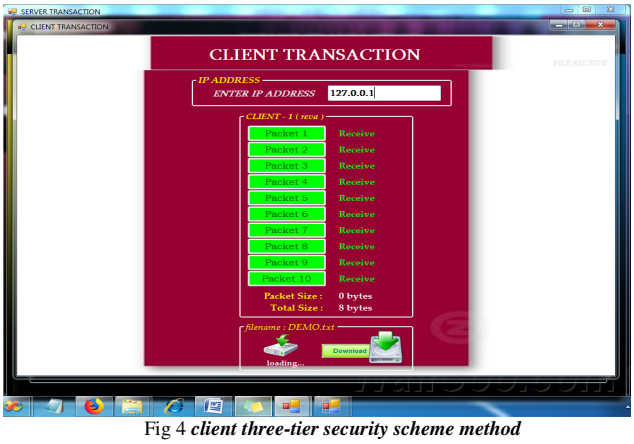

Fig 4 ***client three-tier security scheme method***

V. KEY IN PROPOSE

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

VI. KEY OUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

VII. CONCLUSIONS

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. Analysis indicates that with 10 percent of the 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. We have further improved the security performance of the proposed scheme against stationary access node replication attack by strengthening the authentication mechanism between stationary access nodes and sensor nodes. We used the one-way hash chains algorithm in conjunction with the static polynomial pool-based scheme.

Causal Productions permits the distribution and revision of these templates on the condition that Causal Productions is credited in the revised template as follows: "original version of this template was provided by courtesy of Causal Productions (www.causalproductions.com)".

FUTURE ENHANCEMENT

It will be produced a very powerful and cost-effective devices that they may be used in many other applications(such as underwater r acoustic sensor systems , sensing based cyber-physical systems , time critical application , connective sensing and spectrum , privacy and security management . In future, sensor network will be everywhere in order to make future technologies/environment/infrastructure as smart as possible as explained by Dr. Khan. These includes:

- Healthcare
- Smart homes thorough sensors
- Environment monitoring, security, IoT, etc.

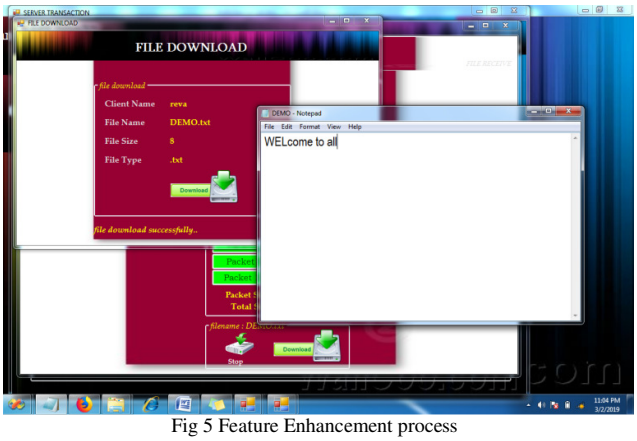

Fig 5 Feature Enhancement process

REFERENCES

[1] L. Eschenauer and V. Gligor, "A Key Management Scheme for Distributed Sensor Networks" , CCS 2002

[2] J.Leeand and D.R.Stinson. Deterministic key predistribution schemes for distributed sensornetworks. Lecture Notes in Computer Science 3357 (2005), 294-307

[3] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, "Security in mobile ad hoc networks: Challenges and solutions" (2004). IEEE Wireless Communications. 11 (1), pp. 38-47.

[4] Y. Zhang, W. Lee, "Intrusion detection in wireless ad-hoc networks", ACM MobiCom, 2000

[5] Karlof, C. and Wagner, D. "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications (Anchorage, AK, May 11, 2003).

[6] Adrian Perrig, David Wagner and Jack Stankovic, "Security in Wireless Sensor Networks", In Communications of the ACM, 47(6), June 2004.

[7] Shi E, Perrig A (2004), "Designing Secure Sensor Networks", Carnegie Mellon University, Appears in Wireless Communication Magazine, 11(6), December 2004.

[8] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," ACM Trans. Programming Languages and Systems, vol. 4, no. 3, July 1982, pp. 382–401.

[9] Gerla, M.; Kaixin Xu; Xiaoyan Hong, "Exploiting mobility in large scale ad hoc wireless networks", CCW 2003, pp. 34 – 39

[10] Kashif Kifayat, Madjid Merabti, Qi Shi, David Llewellyn-Jones, "Application Independent Dynamic Group-Based Key Establishment for Large-scale Wireless Sensor Networks", China Communication Journal, Special issue on Communication and Information Security in Feb, 2007