International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 6, Nov - Dec. 2013 pp-3328-3335 ISSN: 2249-6645

An Efficient Polynomial Pool-Based Scheme for Distributed Heterogeneous Wireless Sensor Networks

M. Senthil Kumar[1], M. Gopinath[2]
[1]Assistant Professor, Department of ECE, Ranganathan Engineering College,Coimbatore, Tamil Nadu, India,
[2]PG Scholar, Department of ECE, Ranganathan Engineering College,Coimbatore, Tamil Nadu, India,

ABSTRACT: *The Sinks are vivacious in many wireless sensor network (WSN) solicitations for competent data accumulation, confined sensor reprogramming, and for extricating and revoking conceded sensors. However, in sensor networks that make use of the temporal key dissemination schemes for pairwise key naissance and endorsement between sensor nodes and mobile sinks, the engross of mobile sinks for data assortment exalts a new reassurance challenge: in the basic probabilistic and q-composite key redistribution schemes, a mugger can easily procure a hefty number of keys by apprehending a small fraction of nodes, and hence, can gain control of the network by arraying a simulated mobile sink preloaded with some conceded keys. This critique designates a multifarious level general framework that authorities the use of any pair wise key redistribution scheme as its basic component. The new framework necessitates two separate key pools, one for the mobile sink to retrieve the network, and one for pair wise key disposition between the sensors. To auxiliary condense the reimbursements initiated by predetermined access node replication attacks; we have underwired the authentication mechanism between the sensor and the stationary access node in the propositioned framework. Through detailed analysis, we show that our security framework has sophisticated network resilience to a mobile sink replication attack as compared to the polynomial pool-based scheme.*

Keywords: *Distributed Security, Wireless Sensor Networks, Mobile Sinks*

I. INTRODUCTION

The Recent advances in electronic technology have paved 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. Such sensor networks can be used in a wide range of applications, such as, military sensing and tracking, health monitoring, data acquisition in hazardous environments, and habitat monitoring. 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 multichip may weaken the security strength (e.g., some intermediate may modify the data passing by, capturing sensor nodes, launching a wormhole attack, a sybil attack, selective forwarding sinkhole), 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 localized reprogramming, oceanographic data collection, and military navigation.

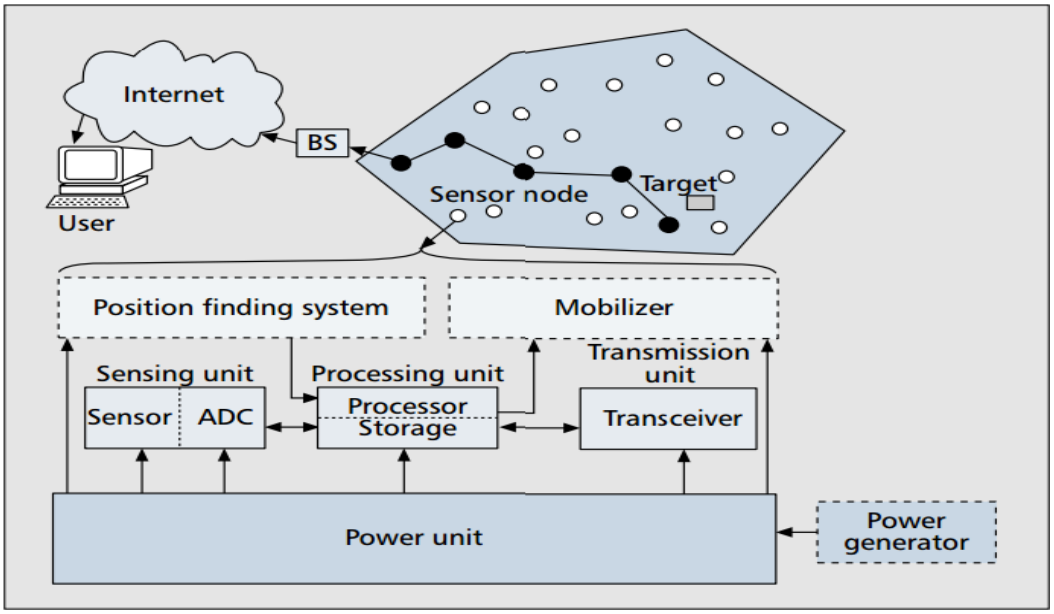

Fig. 1.1 Various Components in Sensor Nodes

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.

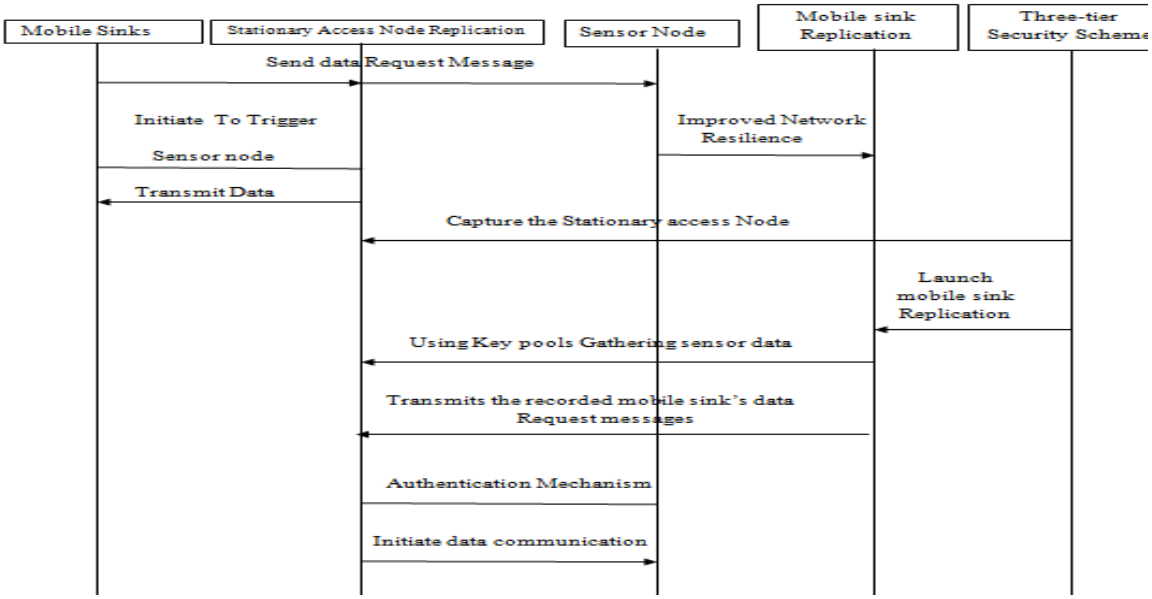

Fig. 1.2 Sequential Process of Mobile Sink Replication in Sensor Nodes

These limitations make key redistribution scheme 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 and q-composite key redistribution 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 pair wise key redistribution 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 redistribution scheme.

The proposed technique will substantially improve network resilience to mobile sink replication attacks compared to the single polynomial pool-based key redistribution approach, as an attacker would have to compromise many more sensor nodes to launch a successful mobile sink replication attack. In the new security framework, a small fraction of the preselected sensor nodes, called the stationary access nodes, act as authentication access points to the network, to trigger the sensor nodes to transmit their aggregated data to mobile sinks. 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. The scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. 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.

II. LITERATURE SURVEY

Classic routing strategies [12], [13] are usually based on a hierarchical organization of the nodes in the network. In fact, the simplest way to aggregate data flowing from the sources to the sink is to elect some special nodes which work as aggregation points and define a preferred direction to be followed when forwarding data. In addition, a node may be marked as special depending on many factors such as its position within the data gathering tree [4], its resources [35], the type of data stored in its queue [16], [7], or the processing cost due to aggregation procedures [8]. According to the tree-based approach [1], [3], [6] a spanning tree rooted at the sink is constructed first. Subsequently, such a structure is exploited in answering queries generated by the sink. This is done by performing in network aggregation along the aggregation tree by proceeding level by level from its leaves to its root. Thus, as two or more messages get to a given node, their aggregate can be computed exactly. However, this way of operating has some drawbacks as actual wireless sensor networks are not free from failures. More precisely, when a packet is lost at a given level of the tree, e.g., due to channel impairments, the data coming from the related sub tree are lost as well. In fact, a single message at a given level of the tree may aggregate the data coming from the whole related sub tree. In spite of the potentially high cost of maintaining a hierarchical structure in dynamic networks and the scarce robustness of the system in case of link/device failures, these approaches are particularly suitable to design optimal aggregation functions and perform efficient energy management.

In fact, there are some studies where the sink organizes routing paths to evenly and optimally distribute the energy consumption while favouring the aggregation of data at the intermediate nodes [6], [9], [10]. In [9] the authors compute aggregation topologies by taking into account the residual energy of each node through linear programming. Further

algorithms can be found in [4], [5], [11], [12]. In [11] the authors investigate which nodes in the network can be exploited as aggregation points for optimal performance. In [14], [12] the focus is on the nodes that should be entrusted with the transmission of the sensed values, whereas in [15] the emphasis is put on the proper scheduling of sleeping/active periods. Often, optimal paths are calculated in a centralized manner at the sink by exploiting different assumptions on the data correlation and selecting the best aggregation points by means of cost functions [13]. Recently, also tree-based schemes for real time or time-constrained applications have been proposed [14]–[16]. The pairwise key establishment problem, however, is still not solved. For the basic probabilistic [12] and the q composite [13] key pre-distribution schemes, as the number of compromised nodes increases, the fraction of affected pairwise keys also increases quickly. As a result, a small number of compromised nodes may affect a large fraction of pairwise keys. Although, the random pairwise key does not suffer from the above-mentioned problem, given a memory constraint, the network size is strictly limited by the desired probability that two sensor nodes share a pairwise key, as also by the number of neighbour nodes with which a sensor can communicate. An enhanced scheme using the t-degree bivariate key polynomial was proposed by Liu et al. [14]. They developed a general framework for pairwise key establishment using the polynomial-based key pre-distribution protocol [21] and the probabilistic key distribution in [12] and [13]. Their scheme could tolerate no more than compromised nodes, where the value of t was limited by the memory available in the sensor nodes.

III. METHODOLOGY

3.1 Existing Method

Three different routing metrics, that aims at an appropriate tradeoff between the detection performance and the energy expenditure. In particular, each metric relates the detection performance explicitly in terms of probabilities of detection and false alarm, with the energy consumed in sensing and routing. Prior to deployment, each mobile sink randomly picks a subset of polynomials from the mobile polynomial pool. In our scheme, to improve the network resilience to mobile sink replication attack as compared to the single polynomial pool based approach, we intend to minimize the probability of a mobile polynomial being compromised if Rc sensor nodes are captured. As an adversary can use the captured mobile polynomial to launch a mobile sink replication attack, the routing problems are formulated as combinatorial optimization programs, and we provide solutions drawing on operations research.

3.2 Disadvantages

The Neyman–Pearson criterion widely adopted for target detection and surveillance related applications. This formulation, as far as we are aware, is the first one which accounts for both the energy consumption in sensing and routing, and detection performance (in terms of detection probability and false alarm probability) at the same time. The detection performance and the energy expenditure are considered jointly in a different but interesting way by which an appropriate tradeoff between them is attained. Provide algorithms for solving those formulated integer programming problems, based on state-of-the-art operations research results.

3.3 Proposed Method

The study presented 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 redistribution scheme substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key redistribution approach.

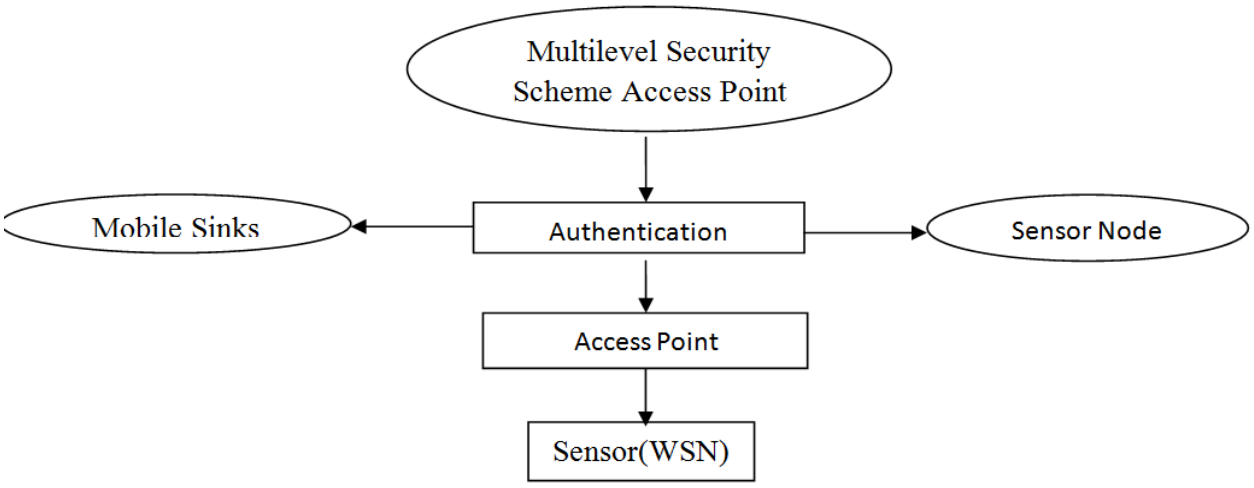

Fig 3.1 Data Flow Diagram

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. They act as authentication access points for the network and

trigger sensor nodes to transmit their aggregated data to the mobile sinks. A mobile sink sends data request messages to the sensor nodes via a stationary access node. The mobile sink's data request messages will initiate the stationary access node to trigger sensor nodes to transmit their aggregated data to the requested sink. Each stationary access node may share a mobile polynomial with a mobile sink. All sensor nodes, including the stationary access nodes, randomly select a subset of polynomials from the static polynomial pool. The advantage of using separate pools is that mobile sink authentication is independent of the key distribution scheme used to connect the sensor network. We divide our scheme into two stages: static and mobile polynomial pre-distribution and key discovery between a mobile sink and a sensor node.

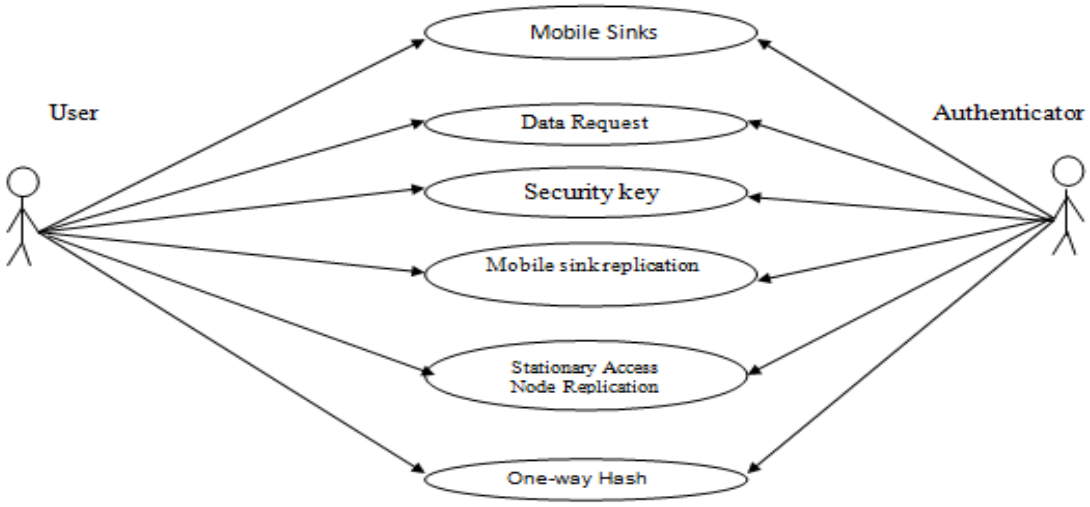

Fig 3.2 Use Case Diagram

3.4 Advantages

The three-tier security scheme is more robust against a stationary access node replication attack. The authentication mechanism between the stationary access nodes and sensor nodes using one-way hash chains algorithm in conjunction with the static polynomial pool-based scheme. 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. 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 redistribution scheme. 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.

IV. POLYNOMIAL POOL-BASED SCHEME

List of Modules

1. **Mobile Sink**
2. **Q-Composite Key Scheme**
3. **Sensor Nodes**
4. **Mobile Sink Replication**
5. **Access Node Replication**

Module Description

1. **Mobile Sink**

In this module, 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.

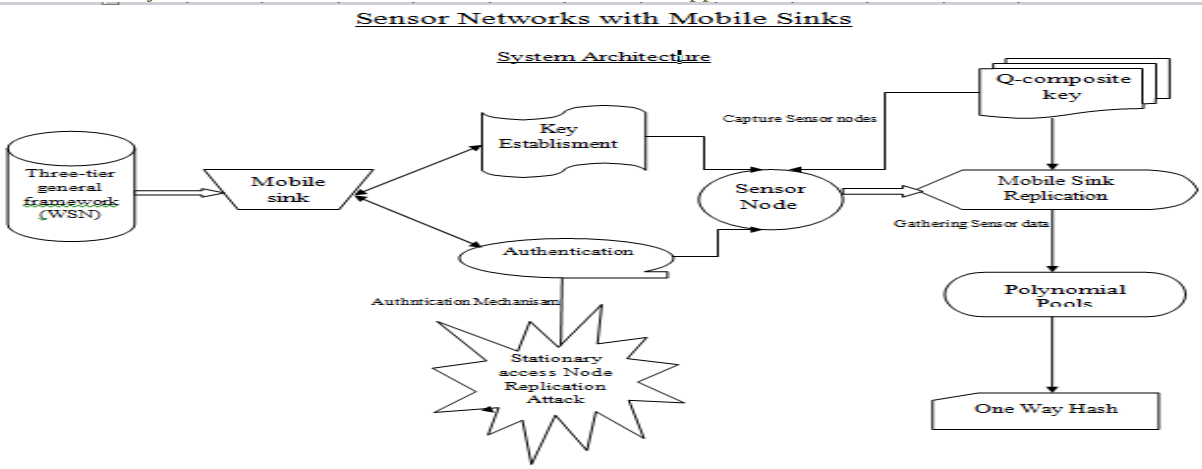

Fig. 4.1 Proposed Method Architecture

2. Q-Composite Key Scheme

Since this module is a three-tier 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. 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. The adversary must capture at least a specific number of stationary access nodes that hold the same mobile polynomial.

3. Sensor Nodes

This module is based on the polynomial pool-based key redistribution scheme substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key redistribution 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.

4. Mobile Sink Replication

In this module, the attacker is able to launch a replication attack similar to the mobile sink replication attack. After a fraction of sensor nodes have been compromised by an adversary, captured static polynomials can be loaded into a replicated stationary access node that transmits the recorded mobile sink's data request messages to trigger sensor nodes to send their aggregated data.

5. Access Node Replication

In this module, we have strengthened the authentication mechanism between the stationary access nodes and sensor nodes using one-way hash chains algorithm in conjunction with the static polynomial pool-based scheme. They developed a general framework for pairwise key establishment using the polynomial-based key redistribution protocol and the probabilistic key distribution in the basic probabilistic and q-composite key redistribution 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.

V. EXPERIMENTAL RESULT

".NET" is also the collective name given to various software components built upon the .NET platform. These will be both products (Visual Studio.NET and Windows.NET Server, for instance) and services (like Passport, .NET My Services, and so on). The code that target .NET, and which contains certain extra Information - "metadata" - to describe itself. Whilst both managed and unmanaged code can run in the runtime, only managed code contains the information that allows the CLR to guarantee, for instance, safe execution and interoperability. The multi-language capability of the .NET Framework and Visual Studio .NET enables developers to use their existing programming skills to build all types of applications and XML Web services. The .NET framework supports new versions of Microsoft's old favorites Visual Basic and C++ (as VB.NET and Managed C++), but there are also a number of new additions to the family. Visual Basic .NET has been updated to include many new and improved language features that make it a powerful object-oriented programming language. These features include inheritance, interfaces, and overloading, among others. Visual Basic also now supports structured exception handling, custom attributes and also supports multi-threading.. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential

SCREENSHOTS

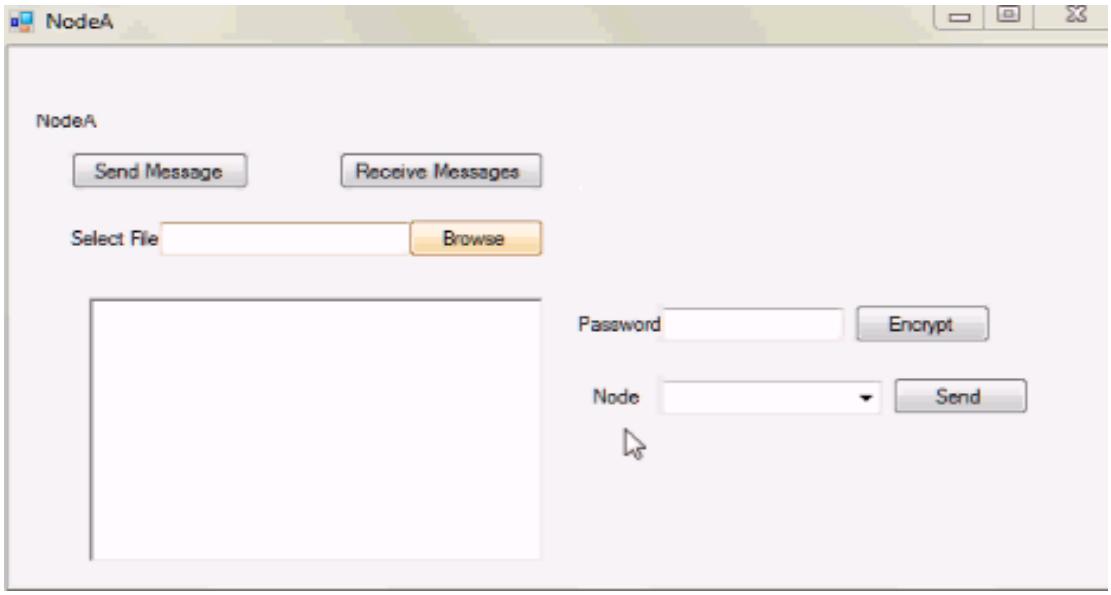

Fig. 5.1 Three Level Security in WSNs

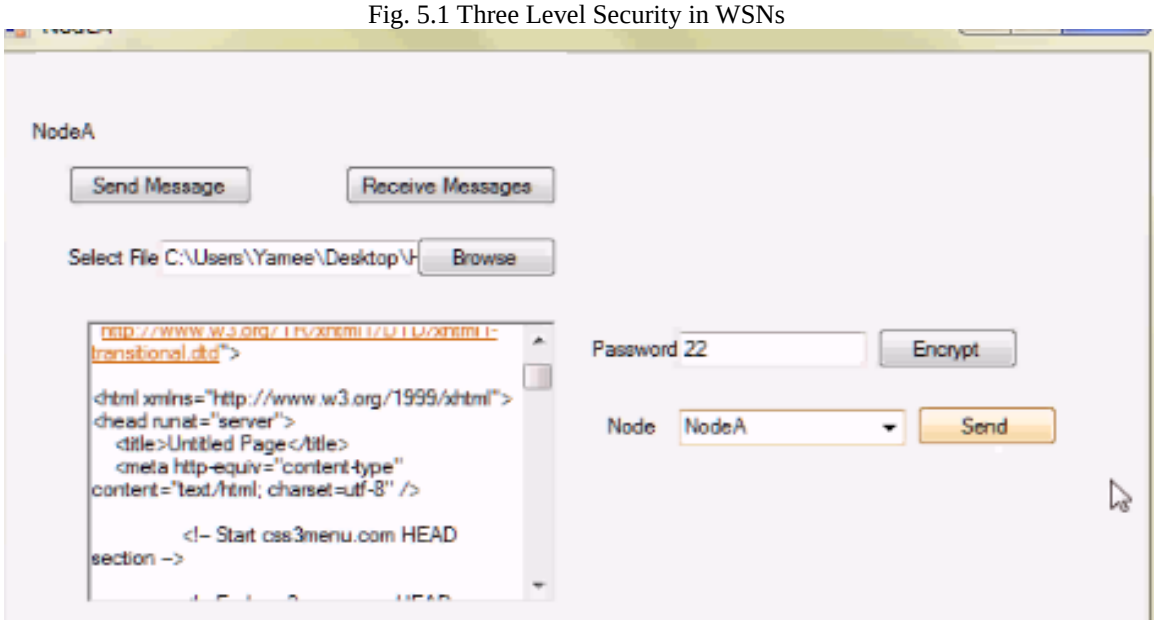

Fig. 5.2 Sending Data in WSNs

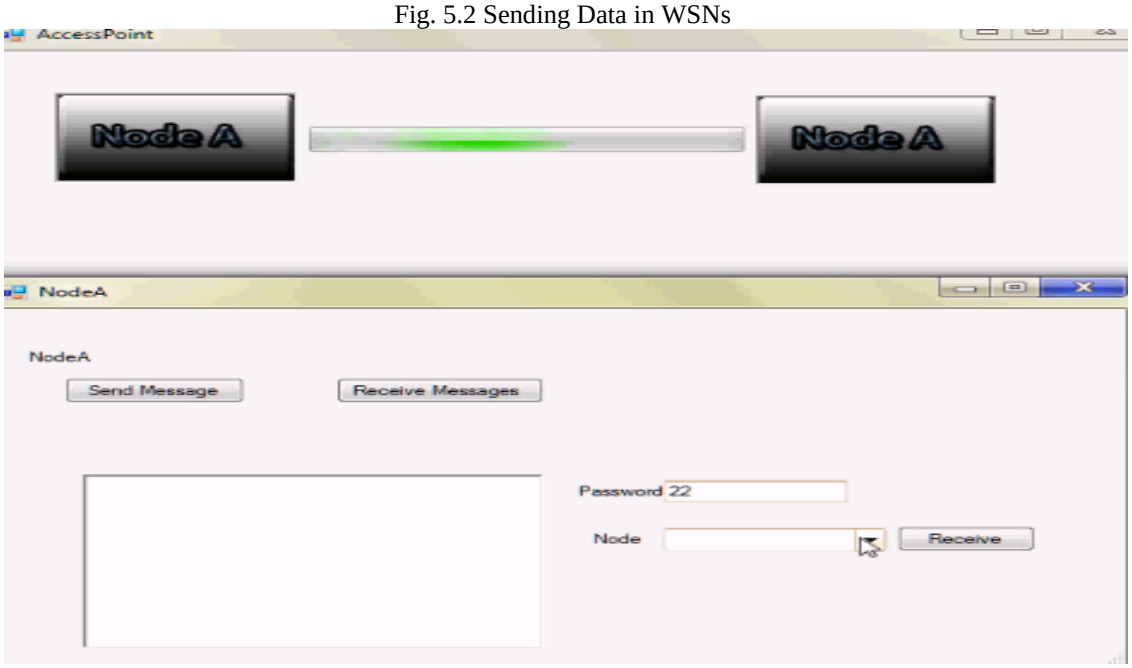

Fig. 5.3 Data Sending from Node 1 to Node 2 in WSNs

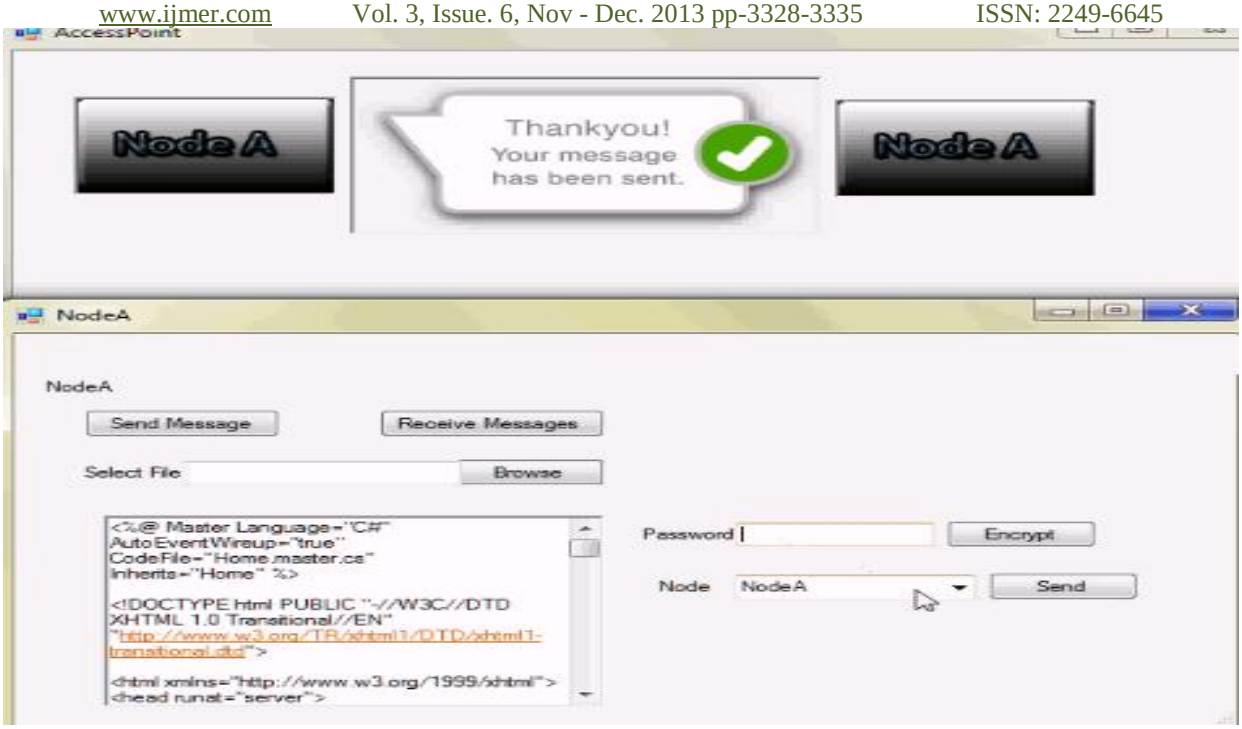

Fig. 5.4 Message Received with Authentication in WSNs

Fig. 5.5 Preventing the Message from Unauthorized User in WSNs

VI. CONCLUSION

In this paper, we have projected 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 redistribution scheme substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key redistribution approach. Using two isolated 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 multiple times more nodes as compared to the single polynomial pool approach.

6.1 Future Work

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.

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. Welsh, R.R. Juang, and A. Alm, *"Vital Signs Monitoring and patient Tracking over a Wireless Network", Proc. IEEE 27th Ann. Intl. 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 Intl. 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 Intl. 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 Intl. Conf. Network Protocols (ICNP), pp. 305-314, Nov. 2003.*

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

[13] 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.*

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

[15] 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.*

AUTHOR DETAILS

M. Senthil Kumar was born in Ramanathapuram District, Tamil Nadu, India in 1982. He obtained his B.Sc., M.Sc. and M.Tech. degrees in Electronics in the years 2002, 2004 and 2006 respectively. He has more than 7 years of teaching experience. He has presented more than 30 research papers in various national and international conferences. He has also published more than 5 research papers in reputed international journals. He has guided several UG and PG students for their project work. His area of interest is Energy Conservation and Optimization Techniques in Wireless Sensor Networks. Currently, he is with Ranganathan Engineering College, Coimbatore, India, as Assistant Professor in the Department of Electronics and Communication Engineering.