International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 4, Jul - Aug. 2013 pp-2553-2562 ISSN: 2249-6645

An Efficient Security Way of Authentication and Pair wise Key Distribution with Mobile Sinks in Wireless Sensor Networks

P. Santhi[1], Md. Shakeel Ahmed[2], Sk. Mehertaj[3], T. Bharath Manohar[4]
[1,3]*M.Tech 2ndyr, Dept of CSE,PBRVITS(Affiliated to JNTU Anantapur), Kavali,Nellore.Andhra Pradesh.India.*
[2] *Assoc. Prof., Dept of CSE, PBRVITS(Affiliated to JNTU Anantapur), Kavali,Nellore.Andhra Pradesh.India.*
[4] *Asst. Professor, Dept of CSE, CMR College of Engineering &Technology, (Affiliated to JNTU Hyderabad)Hyderabad.Andhra Pradesh.India.*

Abstract: *Wireless sensor networks (WSN) are the emerging application in many industrial and missile sector. Mobile sinks (MSs) are vital in many wireless sensor network 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 pairwise 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 predistribution 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. The proposed work, three-tier framework permits the use of any pairwise 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 pairwise key establishment between the sensors. To further reduce the damages caused by stationary access node replication attacks, the authentication mechanism between the sensor and the stationary access node is strengthened in the proposed work. This framework has higher network resilience to a mobile sink replication attack as compared to the polynomial pool-based scheme.*

Keywords: *Wireless sensor networks (WSN), Mobile sinks (MSs) & replication attacks,Polynomial pool based scheme.*

I. INTRODUCTION

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.

In wireless sensor networks, the sensed data from sensor nodes are 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, 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.

II. MOTIVATION

In wireless sensor 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 the tools of choice to provide low cost, secure communication between sensor nodes and mobile sinks.

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

To facilitate the study of a new security technique, a general three-tier security framework is first cultivated for authentication and pair-wise key establishment, based on the polynomial pool-based key pre-distribution scheme.

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.

Advantages

- The proposed technique will substantially improve network resilience to mobile sink replication attacks compared to the single polynomial pool-based key pre-distribution approach, as an attacker would have to compromise many more sensor nodes to launch a successful mobile sink replication attack.
- For the attacker to launch a mobile sink replication attack on the sensor network by capturing only a few arbitrary sensor nodes.

III. III.LITERATURE SURVEY

The key management problem is an active research area in wireless sensor networks.

Eschenauer and Gilgor proposed a probabilistic key pre-distribution 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. extended probabilistic key predistribution 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.

An enhanced scheme using the t-degree bivariate key polynomial was proposed by Liu et al.. They developed a general framework for pairwise key establishment using the polynomial-based key predistribution protocol and the probabilistic key distribution. Their scheme could tolerate no more than t compromised nodes, where the value of t was limited by the memory available in the sensor nodes.

LITERATURE REVIEW

Routing Security in Wireless Ad Hoc Networks
Hongmei Deng, Wei Li, and Dharma P. Agrawal, University of Cincinnati

A mobile ad hoc network consists of a collection of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration. MANET is an emerging research area with practical applications. However, wireless MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability. Routing plays an important role in the security of the entire network. In general, routing security in wireless MANETs appears to be a problem that is not trivial to solve. In this article we study the routing security issues of MANETs, and analyze in detail one type of attack — the “black hole” problem — that can easily be employed against the MANETs. We also propose a solution for the black hole problem for ad hoc on-demand distance vector routing protocol.

Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks
Chalermek Intanagonwiwat; Ramesh Govindan; Deborah Estrin

Advances in processor, memory and radio technology will enable small and cheap nodes capable of sensing, communication and computation. Networks of such nodes can coordinate to perform distributed sensing of environmental phenomena. In this paper, we explore the directed diffusion paradigm for such coordination. Directed diffusion is data-centric in that all communication is for named data. All nodes in a directed diffusion-based network are application-aware. This enables diffusion to achieve energy savings by selecting empirically good paths and by caching and processing data in-network. We explore and evaluate the use of directed diffusion for a simple remote-surveillance sensor network.

Vital Signs Monitoring and Patient Tracking Over a Wireless Network
Tia Gao, Dan Greenspan, Matt Welsh, Radford R. Juang, and Alex Alm

Patients at a disaster scene can greatly benefit from technologies that continuously monitor their vital status and track their locations until they are admitted to the hospital. We have designed and developed a real-time patient monitoring system that integrates vital signs sensors, location sensors, ad-hoc networking, electronic patient records, and web portal technology to allow remote monitoring of patient status. This system shall facilitate communication between providers at the disaster scene, medical professionals at local hospitals, and specialists available for consultation from distant facilities.

Using Directional Antennas to Prevent Wormhole Attacks
Lingxuan Hu David Evans, Department of Computer Science, University of Virginia, Charlottesville, VA

Wormhole attacks enable an attacker with limited resources and no cryptographic material to wreak havoc on wireless networks. To date, no general defenses against wormhole attacks have been proposed. This paper presents an analysis of wormhole attacks and proposes a countermeasure using directional antennas. We present a cooperative protocol

whereby nodes share directional information to prevent wormhole endpoints from masquerading as false neighbors. Our defense greatly diminishes the threat of wormhole attacks and requires no location information or clock synchronization.

Data Dissemination with Ring-Based Index for Wireless Sensor Networks∗
Wensheng Zhang, Guohong Cao and Tom La Porta; Department of Computer Science and Engineering, The Pennsylvania State University

In current sensor networks, sensor nodes are capable of not only measuring real world phenomena, but also storing, processing and transferring these measurements. Many data dissemination techniques have been proposed for sensor networks. However, these techniques may not work well in a large scale sensor network where a huge amount of sensing data are generated, but only a small portion of them are queried. In this paper, we propose an index-based data dissemination scheme to address the problem. This scheme is based on the idea that sensing data are collected, processed and stored at the nodes close to the detecting nodes, and the location information of these storing nodes is pushed to some index nodes, which act as the rendezvous points for sinks and sources. We further extend the scheme with an adaptive ring-based index (ARI) technique, in which the index nodes for one event type form a ring surrounding the location which is determined by the event type, and the ring can be dynamically reconfigured for fault tolerance and load balance. Analysis and simulations are conducted to evaluate the performance of the proposed index-based scheme. The results show that the index-based scheme outperforms the external storage-based scheme, the DCS scheme, and the local storage-based schemes with flood-response style. The results also show that using ARI can tolerate clustering failures and achieve load balance.

IV. SYSTEM ANALYSIS

Network simulation is a technique where a program models the behavior of a network either by calculating the interaction between the different network entities (hosts/routers, data links, packets, etc) using mathematical formulas, or actually capturing and playing back observations from a production network. The behavior of the network and the various applications and services it supports can then be observed in a test lab; various attributes of the environment can also be modified in a controlled manner to assess how the network would behave under different conditions. When a simulation program is used in conjunction with live applications and services in order to observe end-to-end performance to the user desktop, this technique is also referred to as network emulation.

Motivation for Simulations

- Cheap -- does not require costly equipment
- Complex scenarios can be easily tested
- Results can be quickly obtained – more ideas can
- be tested in a smaller timeframe
- The real thing isn't yet available
- Controlled experimental conditions
- Repeatability helps aid debugging
- Disadvantages: Real systems too complex to model

Most of the commercial simulators are GUI driven, while some network simulators require input scripts or commands (network parameters). The network parameters describe the state of the network (node placement, existing links) and the events (data transmissions, link failures, etc). Important outputs of simulations are the trace files. Trace files can document every event that occurred in the simulation and are used for analysis. Certain simulators have added functionality of capturing this type of data directly from a functioning production environment, at various times of the day, week, or month, in order to reflect average, worst-case, and best-case conditions

Most network simulators use discrete event simulation, in which a list of pending "events" is stored, and those events are processed in order, with some events triggering future events -- such as the event of the arrival of a packet at one node triggering the event of the arrival of that packet at a downstream node.

Some network simulation problems, notably those relying on queuing theory, are well suited to Markov chain simulations, in which no list of future events is maintained and the simulation consists of transiting between different system "states" in a memory less fashion. Markov chain simulation is typically faster but less accurate and flexible than detailed discrete event simulation. Some simulations are cyclic based simulations and these are faster as compared to event based simulations.

Advantages of simulation

* Normal analytical techniques make use of extensive mathematical models which require assumptions and restrictions to be placed on the model. This can result in an avoidable inaccuracy in the output data. Simulations avoid placing restrictions on the system and also take random processes into account; in fact in some cases simulation is the only practical modeling technique applicable
* Analysts can study the relationships between components in detail and can simulate the projected consequences of multiple design options before having to implement the outcome in the real-world.
* It is possible to easily compare alternative designs so as to select the optimal system.

* The actual process of developing the simulation can itself provide valuable insights into the inner workings of the network which can in turn be used at a later stage.

Disadvantages of simulation

* Accurate simulation model development requires extensive resources.
* The simulation results are only as good as the model and as such are still only estimates / projected outcomes.
* Optimization can only be performed involving a few alternatives as the model is usually developed using a limited number of variables.
* Simulations cost a lot of money to build and are very expensive to make

Input data

Simulation models are generated from a set of data taken from a stochastic system. It is necessary to check that the data is statistically valid by fitting a statistical distribution and then testing the significance of such a fit. Further, as with any modelling process, the input data's accuracy must be checked and any outliers must be removed.

Output data

When a simulation has been completed, the data needs to be analysed. The simulation's output data will only produce a likely estimate of real-world events. Methods to increase the accuracy of output data include: repeatedly performing simulations and comparing results, dividing events into batches and processing them individually, and checking that the results of simulations conducted in adjacent time periods "connect" to produce a coherent holistic view of the system The main idea is to partly implement HTTP, FTP and TCP protocols.

Routing is the process of selecting paths in a network along which to send network traffic. Routing is performed for many kinds of networks, including the telephone network (Circuit switching) , electronic data networks (such as the Internet), and transportation networks. This article is concerned primarily with routing in electronic data networks using packet switching technology.

In packet switching networks, routing directs packet forwarding, the transit of logically addressed packets from their source toward their ultimate destination through intermediate nodes, typically hardware devices called routers, bridges, gateways, firewalls, or switches. General-purpose computers can also forward packets and perform routing, though they are not specialized hardware and may suffer from limited performance. The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing. Most routing algorithms use only one network path at a time, but multipath routing techniques enable the use of multiple alternative paths.

Routing, in a more narrow sense of the term, is often contrasted with bridging in its assumption that network addresses are structured and that similar addresses imply proximity within the network. Because structured addresses allow a single routing table entry to represent the route to a group of devices, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging) in large networks, and has become the dominant form of addressing on the Internet, though bridging is still widely used within localized environments.

Routing schemes differ in their delivery semantics:

- unicast delivers a message to a single specified node;
- broadcast delivers a message to all nodes in the network;
- multicast delivers a message to a group of nodes that have expressed interest in receiving the message;
- anycast delivers a message to any one out of a group of nodes, typically the one nearest to the source.

Path selection

Path selection involves applying a routing metric to multiple routes, in order to select (or predict) the best route.
In the case of computer networking, the metric is computed by a routing algorithm, and can cover such information as bandwidth, network delay, hop count, path cost, load, MTU, reliability, and communication cost (see e.g. this survey for a list of proposed routing metrics). The routing table stores only the best possible routes, while link-state or topological databases may store all other information as well.

Because a routing metric is specific to a given routing protocol, multi-protocol routers must use some external heuristic in order to select between routes learned from different routing protocols. Cisco's routers. A local network administrator, in special cases, can set up host-specific routes to a particular machine which provides more control over network usage, permits testing and better overall security. This can come in handy when required to debug network connections or routing tables.

As the Internet and IP networks become mission critical business tools, there has been increased interest in techniques and methods to monitor the routing posture of networks. Incorrect routing or routing issues cause undesirable performance degradation, flapping and/or downtime. Monitoring routing in a network is achieved using Route analytics tools and techniques.

Protocols: TCP, UDP, HTTP, Routing algorithms etc

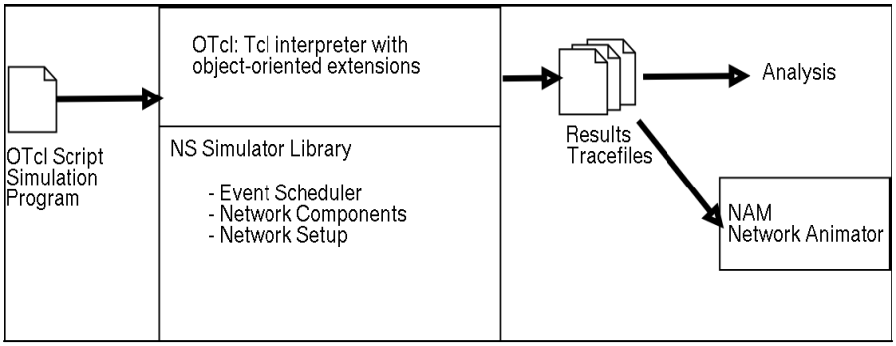
- Traffic Models: CBR, VBR, Web etc
- Error Models: Uniform, bursty etc
- Radio propagation, Mobility models
- Energy Models

- Topology Generation tools
- Visualization tools
- Extensibility

Simulators help in easy verification of protocols in less time, money

- NS offers support for simulating a variety of
- protocol suites and scenarios
- Front end is oTCL, back end is C++
- NS is an on-going effort of research and development

V. SYSTEM DESIGN & ARCHITECTURE DIAGRAMS



STRUCTURE OF NS2

MODULES

- ❖ Deployment of Nodes
- ❖ Data collection to Access points
- ❖ Data collection to sink
- ❖ Three tier security scheme

DEPLOYMENT OF NODES

We consider a wireless sensor network with N nodes. Let N denote the set of all nodes in the network. The communication among all n nodes is based on a tree topology with the sink as the root. The tree is formed in the initial phase as follows. The sink first broadcast a message with a hop counter. The nodes receiving the message will set the message sender as the parent node, increase the hop counter by one, and broadcast it to their neighbors. If a node receives multiple messages, it will select the one with the minimum hop counter to broadcast and set the sender of the message as its parent. Data are transferred along the edges in this communication tree. To transmit one data unit, the energy cost of the sender and receiver are etr and ere respectively, and etr is also relevant to the distance between the sender and receiver. To simplify the problem, we set the length of each tree edge to one unit, which means that sensor nodes have a fixed transmission range and the energy cost of transferring data is only proportional to the data size.

DATA COLLECTION TO ACCESS POINTS

In the wireless sensor network, we proposed a 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. The following figure, we represented a wireless sensor network, where node 1 and 2 are chosen as stationary access nodes. The sensor nodes sends data packet to stationary access nodes.

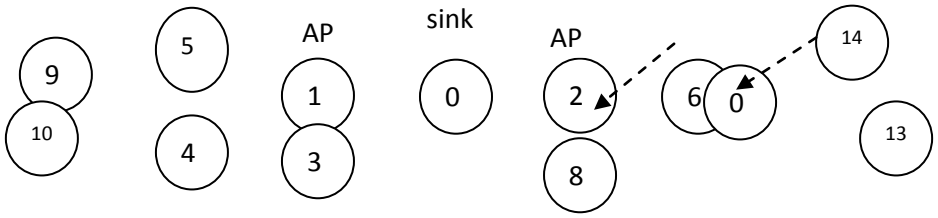


Fig: Data Collection to Access Nodes

DATA COLLECTION TO SINK

The stationary access nodes, collects data from mobile sensor nodes. These collected data packets sent to mobile sink from stationary access nodes. The scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. The following figure, we represented a wireless sensor network, where node 0 is the sink, node 1 and

2 are chosen as stationary access nodes. The sensor nodes sends data packet to stationary access nodes. Then the stationary access nodes send the collected data to sink

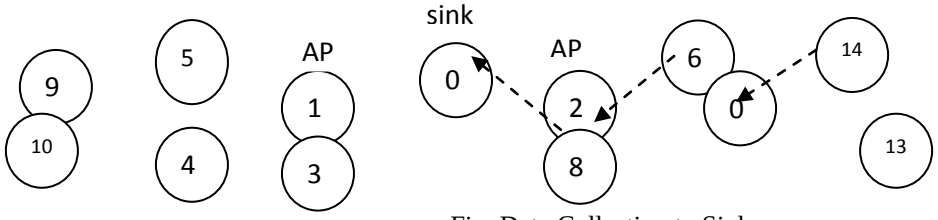


Fig: Data Collection to Sink

THREE TIER SECURITY SCHEME

Two separate polynomial pools are used. The mobile polynomial pool and the static polynomial pool are used. We use, MD5 algorithm for generating key pool for mobile sensor nodes and Sink separately. 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. Polynomials from the static polynomial pool are used to ascertain the authentication and keys setup between the sensor nodes and stationary access nodes. Thus, it is hard for an attacker to compromise at least a single polynomial from the mobile pool to gain access to the network for the sensor's data gathering.

UML DIAGRAMS:

USE CASE DIAGRAM:

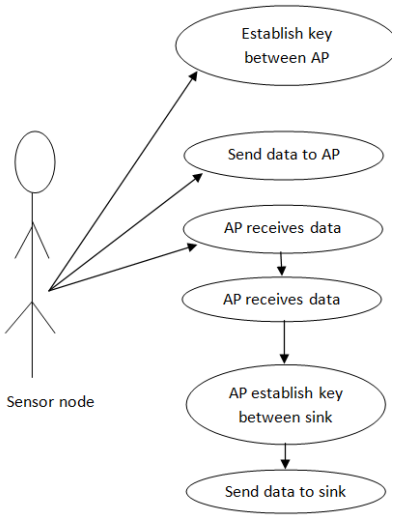
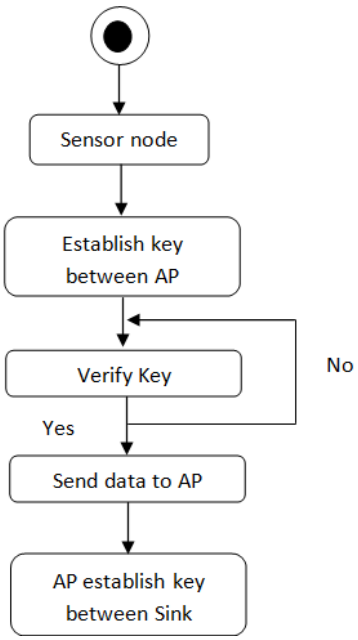


Fig: Use case diagram

ACTIVITY DIAGRAM:



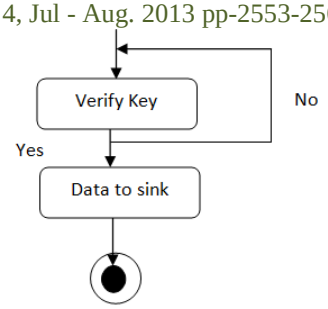


Fig: Activity Diagram

SEQUENCE DIAGRAM:

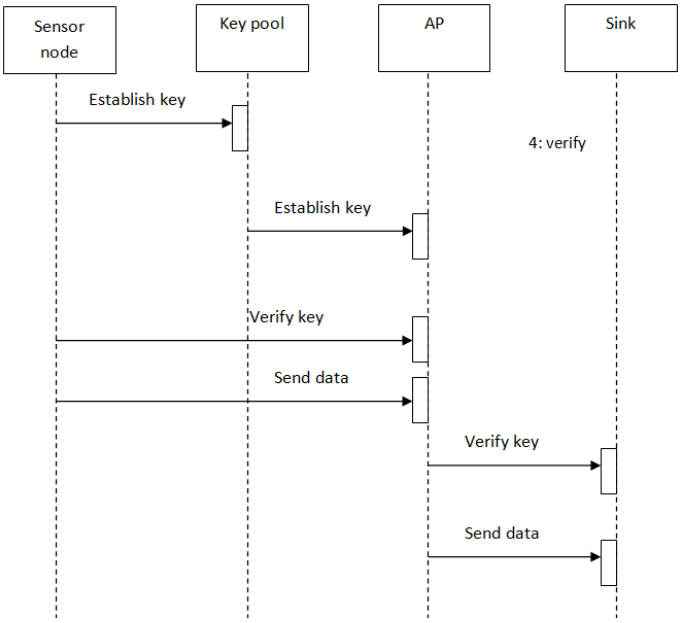


Fig: Sequence Diagram

COLLABORATION DIAGRAM:

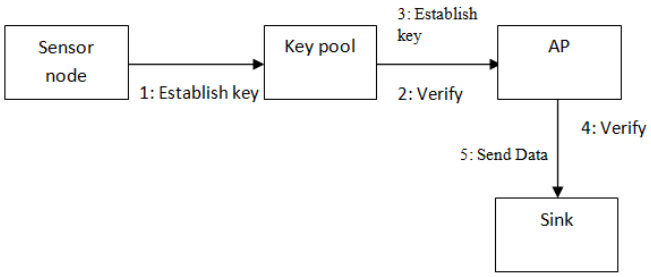
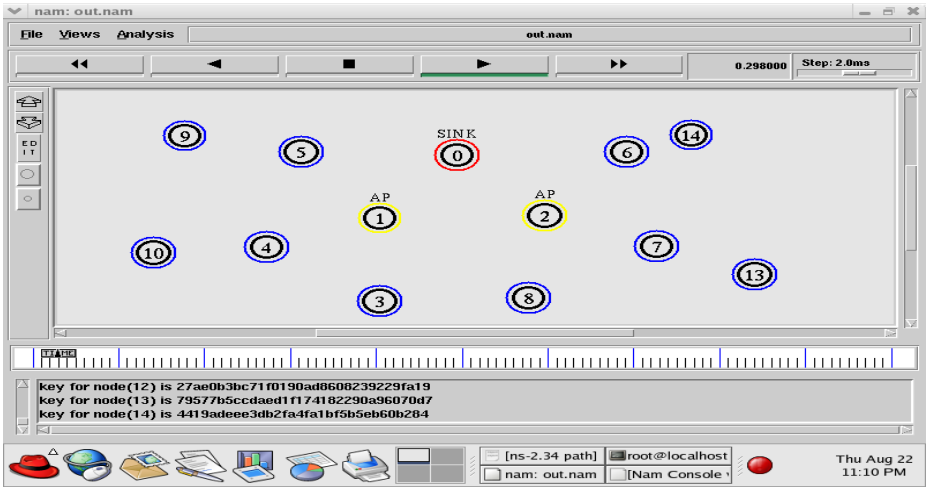
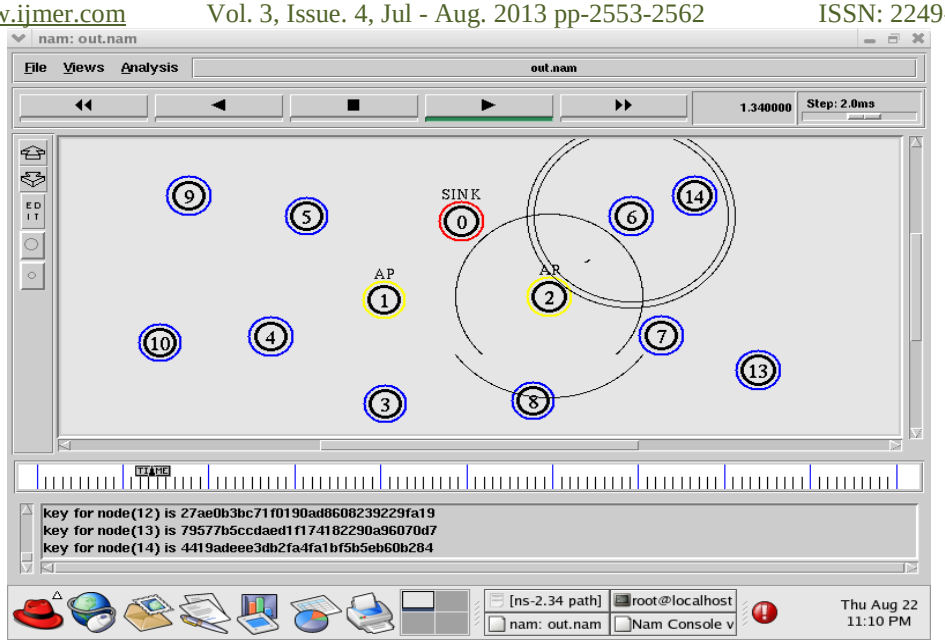
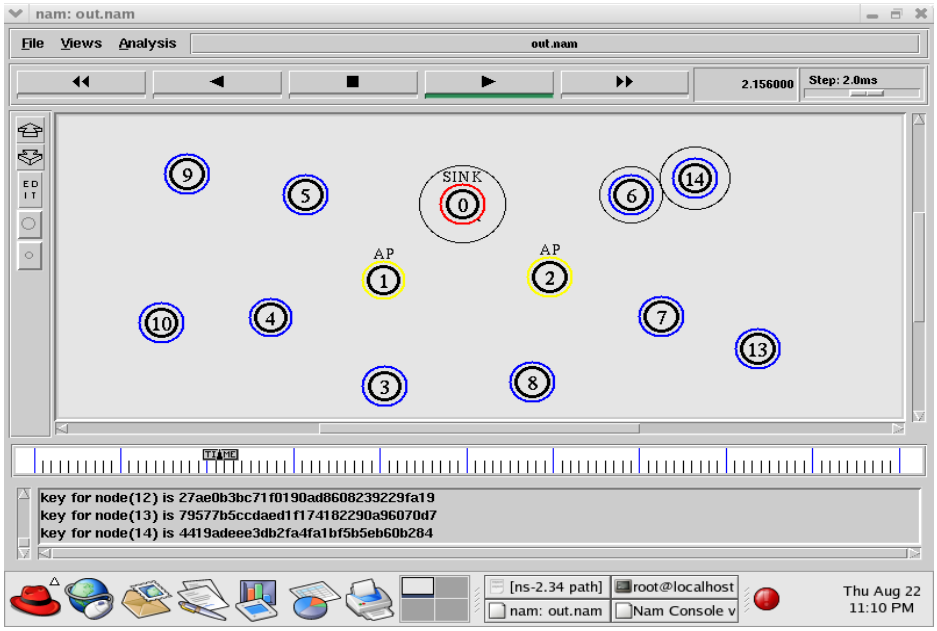


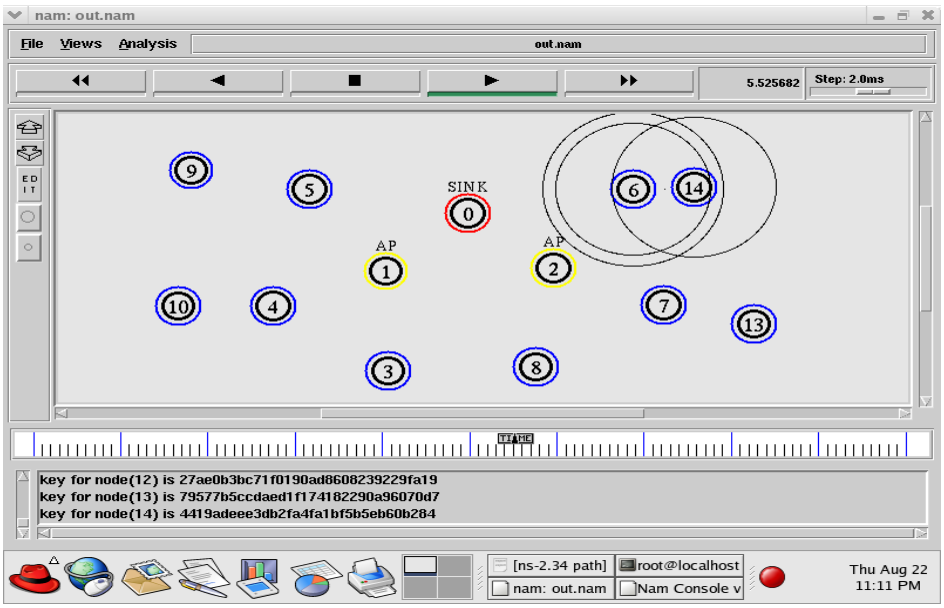
Fig: Collaboration Diagram

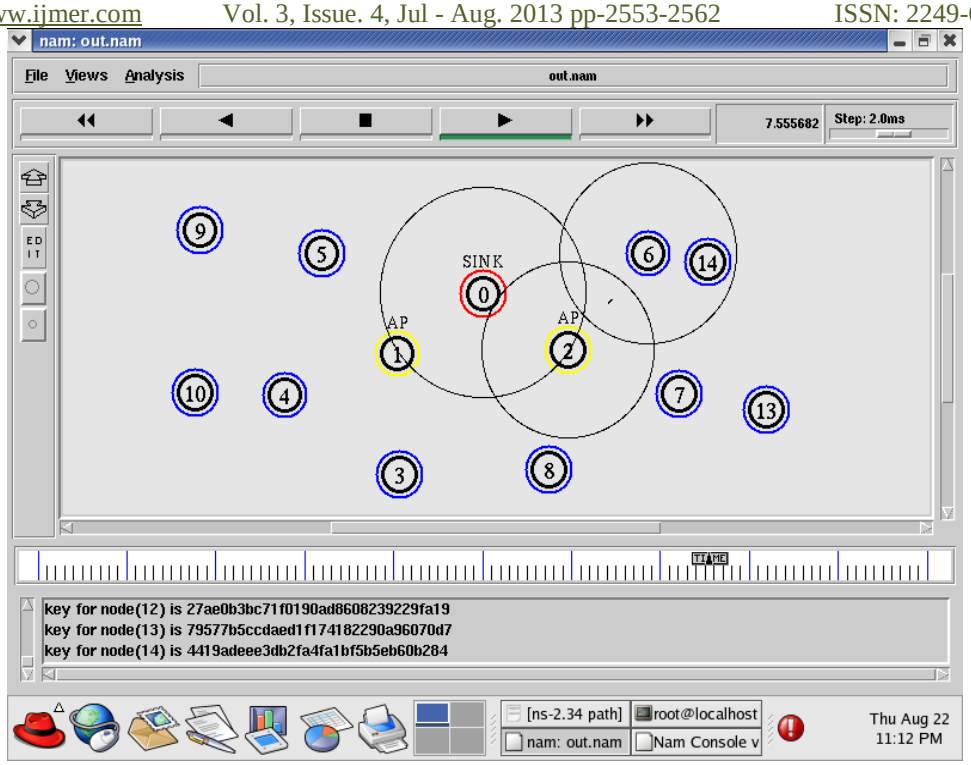
VI. EXPERIMENT & RESULT

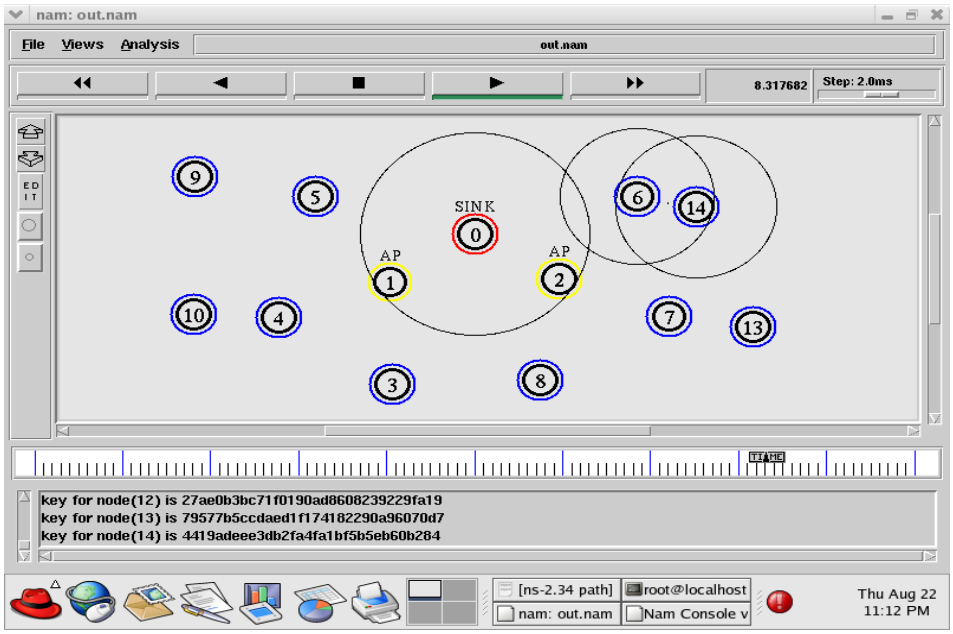



nam: out.nam
File Views Analysis
out.nam
1.340000
Step: 2.0ms
SINK
AP
AP
key for node(12) is 27ae0b3bc71f0190ad8608239229fa19
key for node(13) is 79577b5ccdaed1f174182290a96070d7
key for node(14) is 4419adeee3db2fa4fa1bf5b5eb60b284
[ns-2.34 path]
root@localhost
nam: out.nam
Nam Console v
Thu Aug 22
11:10 PM


nam: out.nam
File Views Analysis
out.nam
2.156000
Step: 2.0ms
SINK
AP
AP
key for node(12) is 27ae0b3bc71f0190ad8608239229fa19
key for node(13) is 79577b5ccdaed1f174182290a96070d7
key for node(14) is 4419adeee3db2fa4fa1bf5b5eb60b284
[ns-2.34 path]
root@localhost
nam: out.nam
Nam Console v
Thu Aug 22
11:10 PM


nam: out.nam
File Views Analysis
out.nam
5.525682
Step: 2.0ms
SINK
AP
AP
key for node(12) is 27ae0b3bc71f0190ad8608239229fa19
key for node(13) is 79577b5ccdaed1f174182290a96070d7
key for node(14) is 4419adeee3db2fa4fa1bf5b5eb60b284
[ns-2.34 path]
root@localhost
nam: out.nam
Nam Console v
Thu Aug 22
11:11 PM





Screens Description:
Blue colour circles are Normal Sensor Nodes.
AP node is the Stationary Access Point, and Sink is the Mobile Sink,
Sensed Data Transmitted to the Base Station via Mobile Sink, in this Scheme we use Access Point (Stationary Access Points) in between Sensor Node and Mobile Sink.
Access Points acts as the Access Points to enter into the Sensor Network.
Ie., Sensor Node Sending Data to Mobile Sink through Access Point .
14-6-2-0
14-----is the Sensor Node
6----------Neighbour Node to 14(Indirect Path)
2- ---is the Access Node
0----- is the Mobile Sink

VII. CONCLUSION

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. The security performance of the proposed scheme is increased against stationary access node replication attack by strengthening the authentication mechanism between stationary access nodes and sensor nodes.

ACKNOWLEDGMENT

I would like to express my sincere thanks to my Guide and my Co-Authors for their consistence support and valuable suggestions.

REFERENCES

[1] 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.
[2] L. Hu and D. Evans, "Using Directional Antenna to Prevent Wormhole Attacks," Proc. Network and Distributed System Security Symp., 2004.
[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] Amar Rasheed, Rabi N Mahapatra, "The Three Tier scheme in wireless sensor networks with mobile sinks", IEEE Trans. Parallel andDistributed Systems, vol 23, Issue 5, pp. 958-965, May.2012
[8] 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.
[9] W. Zhang, G. Cao, and T. La Porta, "Data Dissemination With Ring-Based Index for Wireless Sensor Networks," Proc. IEEE Int'l Conf. NetworkProtocols (ICNP), pp. 305-314, Nov. 2003.
[10] 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.
[11] 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.
[12] A. Rasheed and R. Mahapatra, "A Key Pre-Distribution Scheme for heterogenouse Sensor Networks," Proc. Int'l Conf. Wireless Comm. AndMobile Computing Conf. (IWCMC '09), pp. 263-268, June 2009.