ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

Multitier Authentication for Addressing Replication Attacks in WSNs

G.Swathi[1], J.Raghunath[2], D.Venkatesh[3]

M.Tech, Student, CSE, Gate Institute of Technology, Gooty, India[1]

Asst. Professor, IT, Gate Institute of Technology, Gooty, India[2]

Dean, CSE & IT, Institute of Technology, Gooty, India[3]

Abstract : The existing security mechanisms of Wireless Sensor Networks (WSNs) authenticate communication between sensor nodes and mobile sinks. However key predistribution is a problem. Moreover the usage of mobile sinks for data collection also throws new security challenges. When one or more nodes are compromised, an attacker can collect large number of security keys. With the keys stolen an attacker can replicate a mobile sink and collect sensitive data illegally. Many schemes came into existence for secure communications in WSN. However, three – tier security scheme proposed by Rasheed and Mahapatra uses two key pools. One pool is for mobile sink and the other pool for pair wise key establishment between sensors. It also has mechanisms between access node and sensor node to avoid node replication attacks. In this paper we implemented this three tier security scheme. NS2 simulations revealed that the security framework is robust to node and sink replication attacks.

Keywords – WSN, mobile sink, security

I. INTRODUCTION

Innovations in electronic technology have made it possible to have network among low cost and low powered sensor nodes. Such network is known as Wireless Sensor Network. This network is used in many real time applications. The applications are both in civilian and military circles. These networks are basically to sense the data around it and send the details to sink or base station. These are useful to sense events in no-man areas, observation of animal habitat, health monitoring and even observation of house hold happenings [1]. In case of natural calamities, hazardous environments also WSN is very useful to obtain data. The data senses by sensors in all these applications are collected by base station or sink for analysis and decision making. When sensing area is far from the sink data has to be transmitted long distance. This may cause security problems. As data is transferred though intermediary nodes, they are vulnerable to attacks such as sinkhole [2], selective forwarding [3], [4], Sybil attack [5] and wormhole attack [6]. The attacks also make the sensors near by the base station to consume more energy thus reducing the lifetime of WSN. For this reason mobile sinks are used so as to reduce security problems. The mobile sinks are carried by mobile soldiers, mobile sensor nodes [7], [8]. The mobile sinks are also used in applications such military navigation, oceanographic data collection, and localized programming [9].

In many applications critical information is sent by sensor nodes. Such data needs to be protected from malicious attacks. This is achieved by pair wise key establishment and authentication between nodes in the network. However, implementation of such security in WSN is not easy as the network is resource constrained. The traditional security mechanism does not work with WSN directly. To overcome this problem many key predistribution schemes [10], [11], [12], [13], [14], [15] came into existence. They are capable of providing secure communication between mobile sinks and sensor nodes. However, these solutions could not handle mobile sink replication attacks. The key distribution schemes provided in [10] and [11] could not prevent an attacker to steal security keys once a node is compromised. This will help attacker to launch mobile sink replication attack and take full control over the network.

To overcome this problem a general framework is proposed in [16]. Rasheed and Mahapatra [17] improved it further with three tier security framework based on polynomial pool. This security framework can improve the robustness of the WSN as it can prevent sink replication and node replication attacks. The three tier security framework is as shown in fig. 1.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

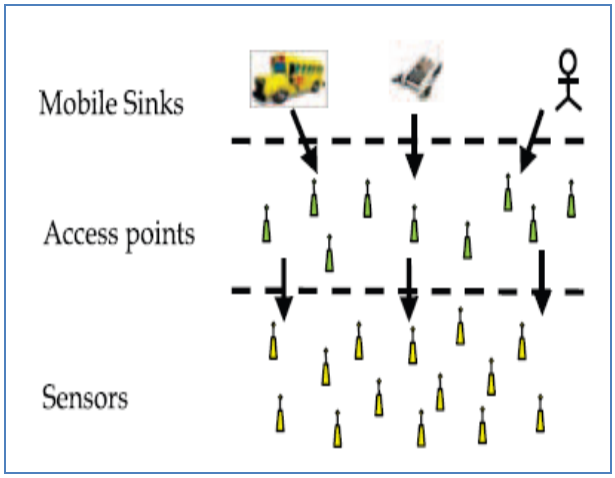

Fig.1 – Illustrates the three tier security scheme

As can be seen in fig. 1, the nodes in the network formed as three layers. The mobile sinks collect data from sensor nodes through access points. The access points are sensor nodes that are meant for another level of security. The data request from mobile sinks goes to access points. The access points trigger the sensor nodes to send data to mobile sinks. The sensor nodes actually collect data from field. The sensed data reaches mobile sinks for analysis and decision making. Two polynomial pools are used in this framework. They are known as mobile polynomial pool and static polynomial pool. With two key pools and less number of nodes to carry the keys make the attackers difficult to launch sink replication attack. Sensor nodes carry keys of mobile polynomial pool. For this reason for attackers it is very difficult to compromise nodes in the network. The tree tier security scheme also prevents stationary access node replication attack as there is secure communication between stationary access points and sensor nodes.
The remainder of this paper is structured as follows. Section II reviews relevant literature. Section III provides details about the three tier security scheme. Section IV provides information about experiments and results while section V concludes the paper.

II. PRIOR WORK

In WSN security concerns are due to its limitations in resources. To secure WSNs a probabilistic key predistribution scheme was proposed in [10]. This will make the initial trust between nodes possible. The idea behind this is to allow the sensor nodes to pick keys randomly from the pol. Another such scheme is known as q-composite key. It also uses a pool but needs a pair wise key computation. This scheme picks pairs of sensor nodes randomly and they are assigned a pair of keys uniquely. These two schemes ensured more secure communication inWSN. However, they could not solve the problem of pair wise key establishment. When compromised nodes are increased in the WSN that uses these schemes, the affected pair wise keys also increased. Moreover the network size is limited in the above schemes which cause more security problems.

Lie et al. [12] proposed a new scheme that uses t-degree vicariate key based polynomial which took care of key predistribuion. A protocol [18] is used for this purpose. The protocol could allow more than t number of compromised nodes. Finally in [17] a three tier security scheme is proposed for WSN. The network can have three tiers. They are sink tier, stationary access tiger and sensor tier. This scheme uses two polynomial pool of keys. One pool is known as mobile polynomial pool and the other pool is known as static polynomial pool. These pools are used between the tiers. There is secure communication between mobile sinks and stationary access nodes and between stationary access nodes and sensor nodes. Thus this scheme makes the communication in WSN robust. The three tier security scheme is presented in the next section.

III. SECURITY SCHEME

The security scheme used in this paper is taken from [17]. The three tier security framework is as shown in fig. 1. The scheme has three tiers namely mobile sink tier, stationary access nodes tier and sensor nodes tier. Communication takes place among the three tiers with due authentication. The keys required by the scheme are kept in two polynomial pools. The pools are known as static polynomial pool and mobile polynomial pool. Keys from mobile Polynomial pool are used by mobile sinks to establish secure communication with stationary access points. This will help the mobile sinks to gather data from sensor nodes. In order to gain control over data, an attacker has to compromise one polynomial at least. This will prevent mobile sink replication attack.

The keys from static polynomials are used between sensor nodes and stationary access points to have secure communication. From mobile polynomial pool, the mobile sinks pick a set of polynomials. These polynomials are taken from mobile polynomial pool. The pool based approach prevents the polynomial to get compromised. This will allow the WSN to prevent stationary access node replication attack. The three tier framework picks a small set of sensor nodes randomly and designated as stationary access points. These access points acts as mediators between the sensor nodes and mobile sinks. The mobile sinks make data request to access points. In turn the access points trigger the sensor nodes to send data to sinks.

Security Analysis

We analyze the security provided by the three tier architecture, using metrics such as connectivity and security.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

Security is analyzed with respect to the possibility of attacks. When one of the polynomials from mobile polynomial pool is compromised by attacker, it is possible to launch mobile sink replication attack. With respect to connectivity the probability of Pconn is estimated as follows.

$$P_{conn} = 1 - \left(1 - \frac{c}{n}\right)^m,$$

A stationary access point and a mobile sink can share a polynomial (Pm) which can be computed as follows.

$$P_m = \frac{K_m}{|M|}.$$

There is a probability that two sensor nodes can share a static polynomial. This probability is computed as follows.

$$P_s = 1 - \frac{\binom{|S|}{2K_s} \cdot \binom{2K_s}{K_s}}{\binom{|S|}{K_s}^2}.$$

In the same fashion, a mobile sink node and a stationary access point can share a common polynomial. This probability is computed as follows.

$$P_{sa} = 1 - \frac{\binom{|S|}{2K_s - 1} \cdot \binom{2K_s - 1}{K_s - 1}}{\binom{|S|}{K_s} \cdot \binom{|S|}{K_s - 1}}.$$

There is also probability of sharing a polynomial from static polynomial pool between two stationary access nodes. This is computed as follows.

$$P_a = 1 - \frac{(|M| - 1) \cdot \binom{|S|}{2 \cdot (K_s - 1)} \cdot \binom{2 \cdot (K_s - 1)}{K_s - 1}}{|M| \cdot \binom{|S|}{K_s - 1}^2}$$

IV. EXPERIMENTS AND RESUTLS

Experiments are made using NS2 simulations. A PC with 4 GB RAM and Core 2 Dual processor is used. The operating system is Ubuntu. Various experiments are conducted with different set of nodes in each tier. Some of the simulation results are presented here.

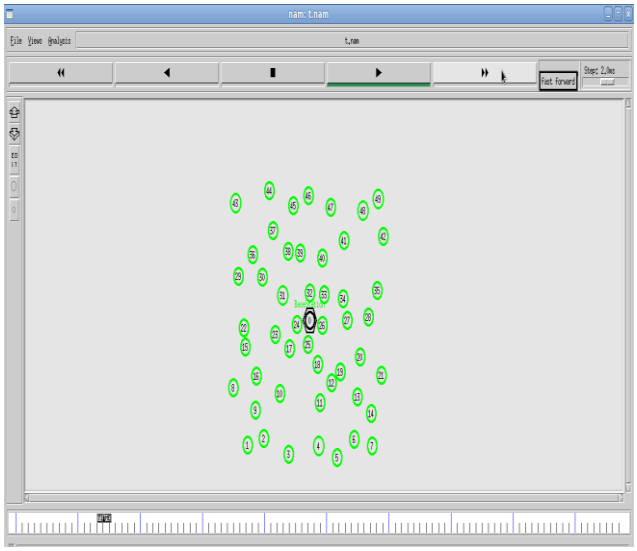

Fig. 2 – WSN Tiers Partially Formed

As can be seen in fig. 1, it is evident that node 0 is considered base station. It collects information from sensor nodes through cluster heads. However, this figure shows formative stage of the three tiers. The sensor nodes moved far from the base station and the in the next stage, they will gradually positioned into three tiers namely base station, cluster heads, and sensor nodes.

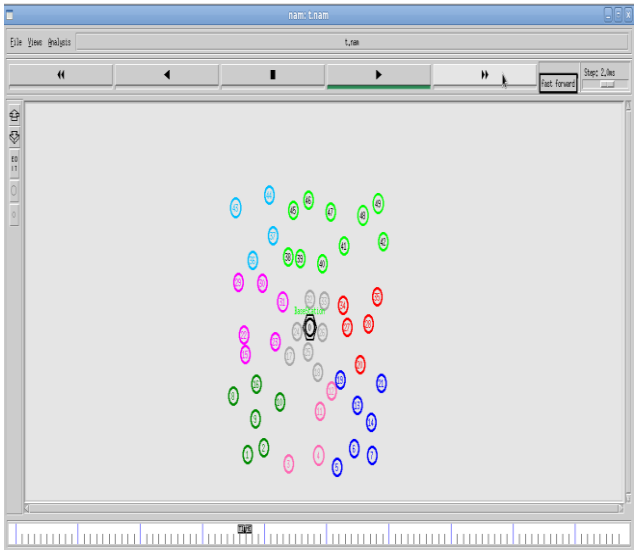

Fig. 3 – WSN with 7 Clusters

As seen in fig. 3, it is evident that there are seven clustered formed. Each cluster is shown in different color. However, the cluster formation is not yet completed. After this one of the nodes will act as cluster head. This will be done gradually. The next screen shows it.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

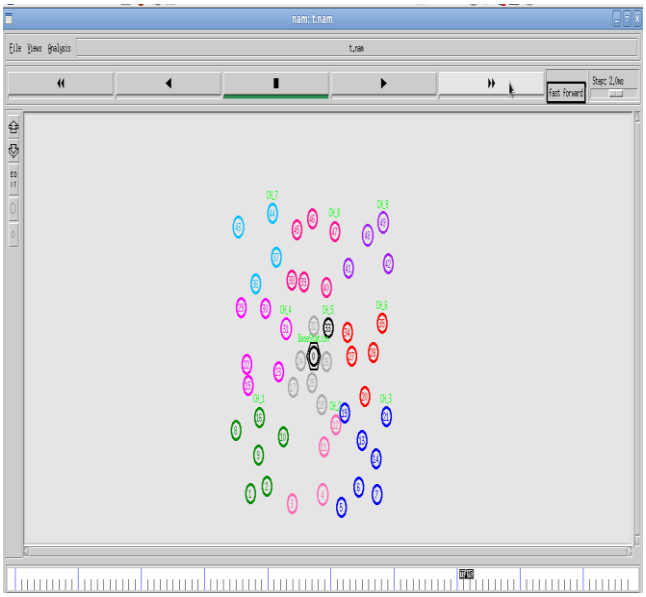

Fig. 4 – WSN with 3 Tiers

As can be seen in fig. 4, it is evident that 7 clusters are having cluster head. Each cluster has its own cluster head. It is responsible to collect data from sensors and send it to the base station. When data request is made from base station, authentication takes place. Then it triggers cluster head to collect data from sensors. Even before that another level of security is provided between the cluster head and sensor.

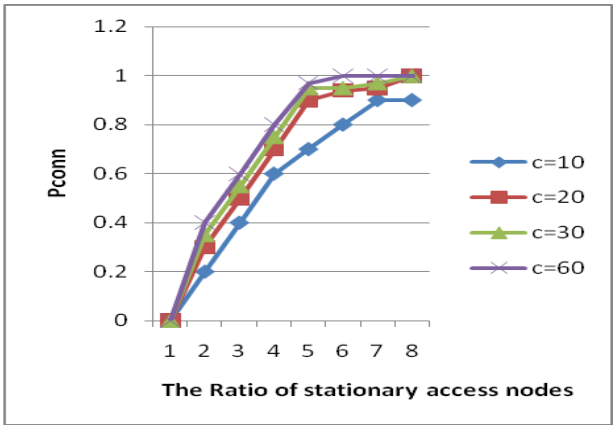

Fig. 5 – Ratio of access nodes vs. Pconn

As can be seen in fig. 5, the horizontal axis represents ration of stationary access nodes while the vertical axis represents Pconn value. The results reveal the probability of Pconn versus the ratio of access nodes.

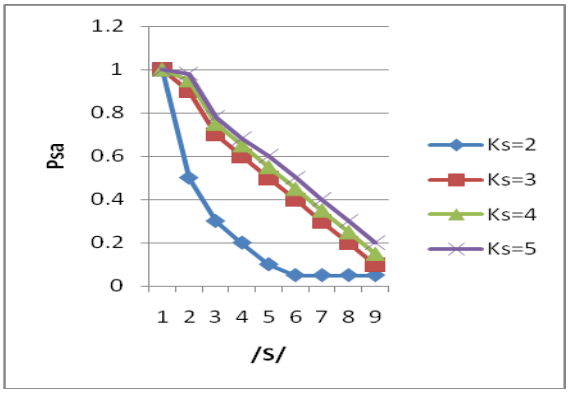

Fig. 6 – Probability of Psa vs. size

As can be seen in fig. 6, the horizontal axis represents size while the vertical axis represents Psa value. The results reveal the probability of a sensor node and a stationery access node sharing a static polynomial.

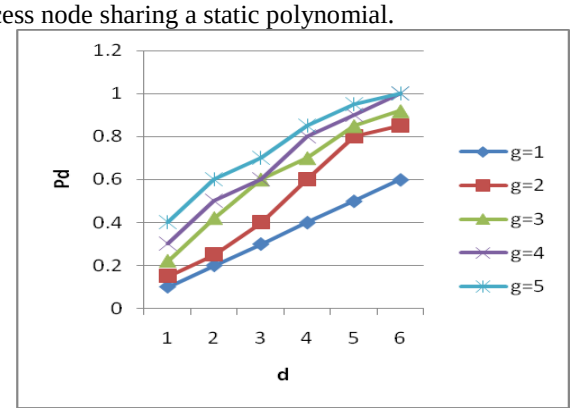

Fig. 7 – Probability (Pd) vs. the number of sensor neighbors (d)

As can be seen in fig. 7, the horizontal axis represents the number of sensor neighbors while the vertical axis represents Pd value. The results reveal the probability a mobile sink to have pair wise key with sensor node versus the number of sensor neighbors.

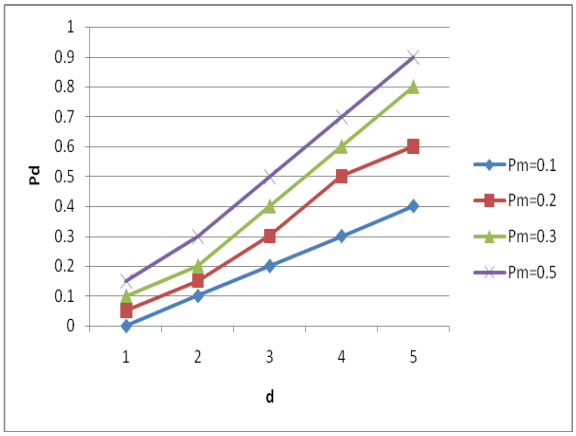

Fig. 8 – Probability (Pd) vs. the number of sensor neighbors (d)

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

As can be seen in fig. 8, the horizontal axis represents the number of sensor neighbors while the vertical axis represents Pd value. The results reveal the probability a mobile sink to have pair wise key with sensor node versus the number of sensor neighbors.

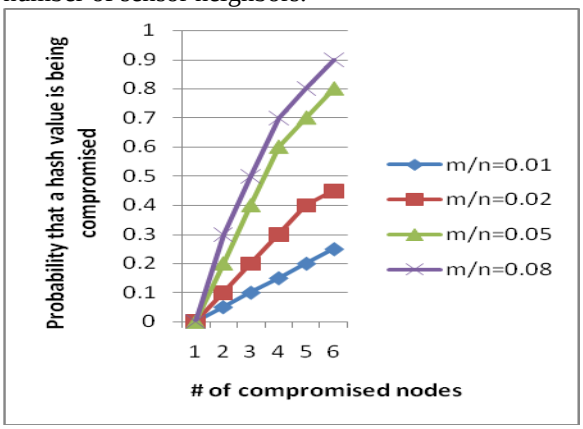

Fig. 9 – Compromised hash value probability vs. number of compromised nodes

As can be seen in fig. 9 the horizontal axis represents number of compromised nodes while the vertical axis represents probability that a hash value is being compromised.

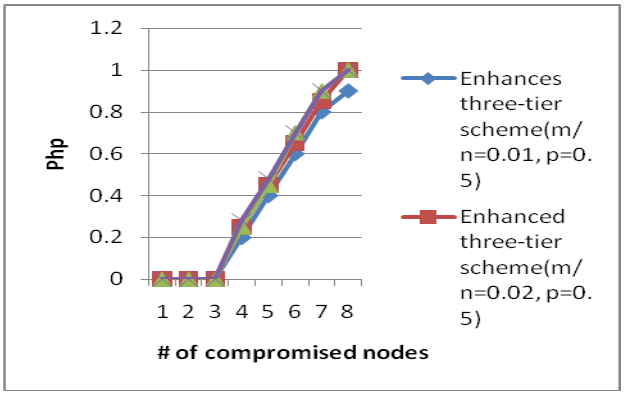

Fig. 10 – Probability of non compromised node under stationary access node replication attack

As can be seen in fig. 10 the horizontal axis represents number of compromised nodes while the vertical axis represents probability of non compromised node under stationary access node replication attack.

V. CONCLUSION

In this paper we implemented and analyzed the three tier security framework proposed by Rasheed and Mahapatra [17] using NS2. The three tier framework is based on key predistribution scheme which is based on polynomials. Two polynomial pools are used in this framework in order to avoid mobile sink replication attack and also stationary access point replication attack. As few access nodes carry polynomials, the scheme can effectively prevent the attacker from launching the two types of replication attacks. The scheme enhances security to the extent possible to prevent stationary access node replication attack as well. The NS2 simulations implemented by us reveal that the three tier security scheme is robust to the said replication attacks.

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] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," Proc. MobiCom, pp. 56-67, 2000.
[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] H. Deng, W. Li, and D.P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," Proc. IEEE Comm. Magazine, pp. 70-75, 2002.
[5] J.R. Douceur, "The Sybil Attack," Proc. First Int'l Workshop Peer-to-Peer Systems (IPTPS '02), Mar. 2002.
[6] L. Hu and D. Evans, "Using Directional Antenna to Prevent Wormhole Attacks," Proc. Network and Distributed System Security Symp., 2004.
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] H. Chan, A. Perrig, and D. Song, "Random Key Pre-Distribution Schemes for Sensor Networks," Proc. IEEE Symp. Research in Security and Privacy, 2003.
[12] 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.
[13] H. Chan, A. Perrig, and D. Song, "Key Distribution Techniques for Sensor Networks," Wireless Sensor Networks, pp. 277-303, Kluwer Academic, 2004.
[14] 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.
[15] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," Proc. 10th ACM Conf. Computers and Comm. Security (CCS '03), pp. 62-72, Oct. 2003.
[16] A. Rasheed and R. Mahapatra, "A Key Pre-Distribution Scheme for Heterogeneous Sensor Networks," Proc. Int'l Conf. Wireless Comm. and Mobile Computing Conf. (IWCMC '09), pp. 263-268, June 2009.
[17] Amar Rasheed, Student Member, IEEE, and Rabi N. Mahapatra, Senior Member, IEEE, "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks". IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 5, MAY 2012.
[18] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences," Proc. 12th Ann. Int'l Cryptology Conf. Advances in.