# Securing Wireless Sensor Network using Intelligent Techniques

K. Priyadharshini
(Affiliated to Anna University)
GKM College of Engineering and Technology
Chennai – 600 063
India

G. Hemalatha
(Affiliated to Anna University)
GKM College of Engineering and Technology
Chennai – 600 063
India

K. Selvamani
College of Engineering
Guindy Campus
Anna University
Chennai – 600 025
India

## ABSTRACT

In wireless sensor networks (WSNs), the sensor nodes transmit critical information over the network. Therefore security services such as authentication and pair wise key establishment between sensor nodes and mobile sinks are important. However, the problem of authentication and pair wise key establishment in sensor networks with mobile sinks is still a critical problem in the face of mobile sink replication attacks. 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 the network sensor nodes. This makes it possible for an attacker to take control over the entire network. Thereby deploying a replicated mobile sink, preloaded with some compromised keys to authenticate and initiate data communication with any sensor node. To address this issue a general framework needs to be developed that permits the use of any pair wise key pre distribution scheme which requires two separate key pools one for the mobile sink to access the network and other for the pair wise key establishment between the sensors. Moreover, to detect such mobile sinks and replication attacks an intelligent agent is deployed at every level in the network. The agents play a major role and perform with the idea of knowledge base and rule manager.

## Keywords

Wireless Sensor Network; Intelligent Agent; Mobile Sink; Rule Manager; Replication Attack

## 1. INTRODUCTION

### 1.1 Sensor Node

A sensor node is a node in a wireless sensor network that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network [2]. The main function of sensor is to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

### 1.2 Wireless Sensor Network

Wireless sensor network (WSN) is an emerging class of systems made possible by cheap hardware, advanced programming tools, complex algorithms, long lasting power sources and energy efficient radio interfaces. Wireless sensor network is a new paradigm in designing fault tolerant mission critical systems, to enable varied applications like threat detection, environmental monitoring, traditional sensing and actuation and much more. It is an emerging area of inter-disciplinary research between people in the electrical engineering, computer science, and among their various disciplines [2].

A WSN consists of spatially distributed autonomous sensors to monitor physical or environmental conditions such as temperature, sound, pressure etc. There are more modern networks such as bidirectional for enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battle field surveillance and these types of networks are used in many industrial and consumer applications such as industrial process monitoring and control, machine health monitoring and so on. Sensor network nodes has typically several parts namely a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source which are usually a battery or an embedded form of energy harvesting.

### 1.3 Enhanced Three-tier Security Scheme

The three-tier security scheme [2] 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. When successful access to the network has been obtained through the compromised static

polynomial, the replicated stationary access node transmits recorded mobile sink data request messages. Next, the sensor nodes that have the compromised polynomial in their rings will insecurely authenticate and establish a pairwise key with the replicated node and thus deliver their data to the replicated node. In this section, we remedy the security performance of the proposed scheme in the case of a stationary access node replication attack. This work proposes a one-way hash chain algorithm in conjunction with the polynomial pool scheme. In order to detect such attack in each layer in the network an intelligent agent is used.

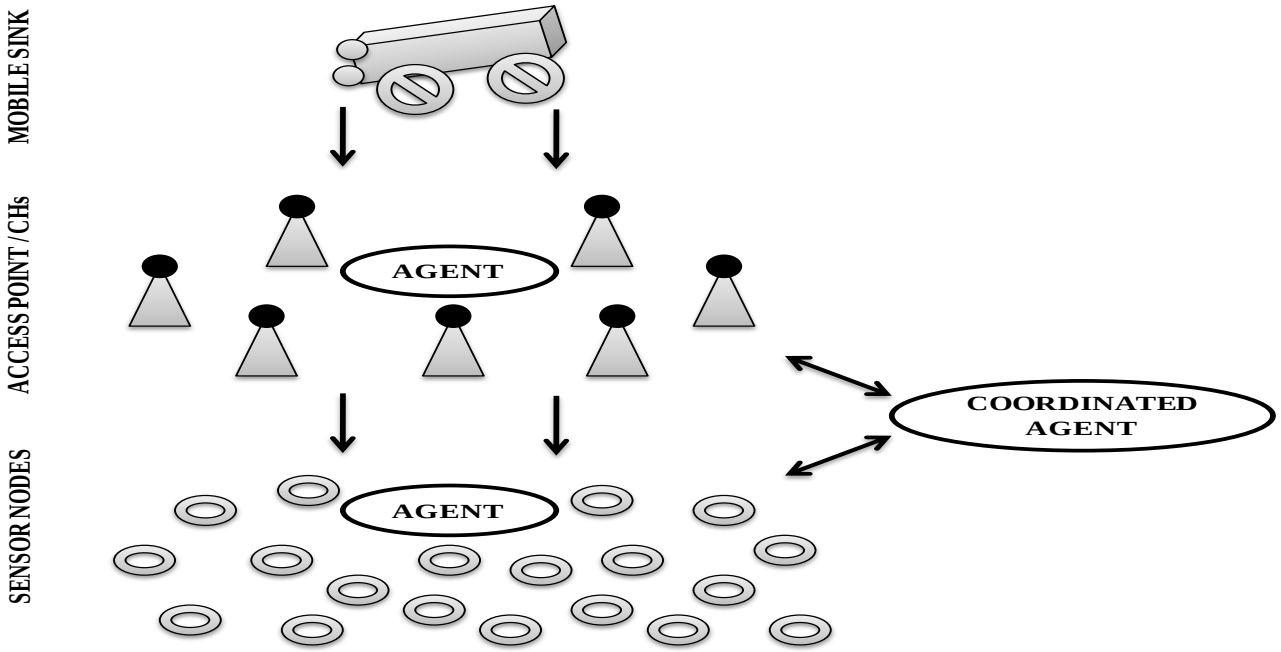


**Fig 1: Enhanced three-tier security model**

These agents have to communicate with the coordinated agent (CA). The CA has to be connected with rule manager and knowledge base. The past history of the nodes has to be recorded in knowledge base. Based upon the rule, the CA will check for the action taken by agent.

## 1.4 Intelligent Agent

An agent based method is a class of computational models for simulating the actions and interactions of autonomous agents with a view for assessing their effects on the system as a whole. These models simulate the simultaneous operations and interactions of multiple agents in an attempt to re-create and predict the appearance of complex phenomena. The process of an agent lies from the lower (micro) level to higher (macro) level for the system. The key notation is a simple behavior rule that generate complex behavior. Also agent model consists of dynamically interaction with rules that operates in real world complexity [5].

These agents reside in networks and in lattice-like neighborhoods. The location of the agents and their responsive and purposeful behavior are encoded in algorithmic form in computer programs.

Agent based models complement traditional analytic methods. Where analytic methods enable humans to characterize the equilibrium of a system, agent based models allow the possibility of generating that equilibrium. Agent based models also can be used to identify lever points, defined as moments in time in which interventions have extreme consequences, and to distinguish among types of path dependency. Rather than focusing on stable states, the models consider a system's robustness—the ways that complex systems adapt to internal and external pressures so as to maintain their functionalities. The task of harnessing that complexity requires consideration of the agents themselves—their diversity, connectedness, and level of interactions [4].

# 2. RELATED WORK

General three-tier security framework for authentication and pair wise key establishment, based on the single Pool-based key pre distribution scheme [9] is the previous technique. The proposed technique substantially improves the 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 [2]. 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 [2]. 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.

Although the 3-tier security approach [2] makes the network more resilient to mobile sink replication attacks compared to the single polynomial pool-based key pre distribution scheme, it is still vulnerable to stationary access node replication attacks. In these types of attacks, 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.

# 3. PROPOSED ARCHITECTURAL DESIGN

The proposed Architectural design for preventing the various types of attacks is shown in Figure 2.

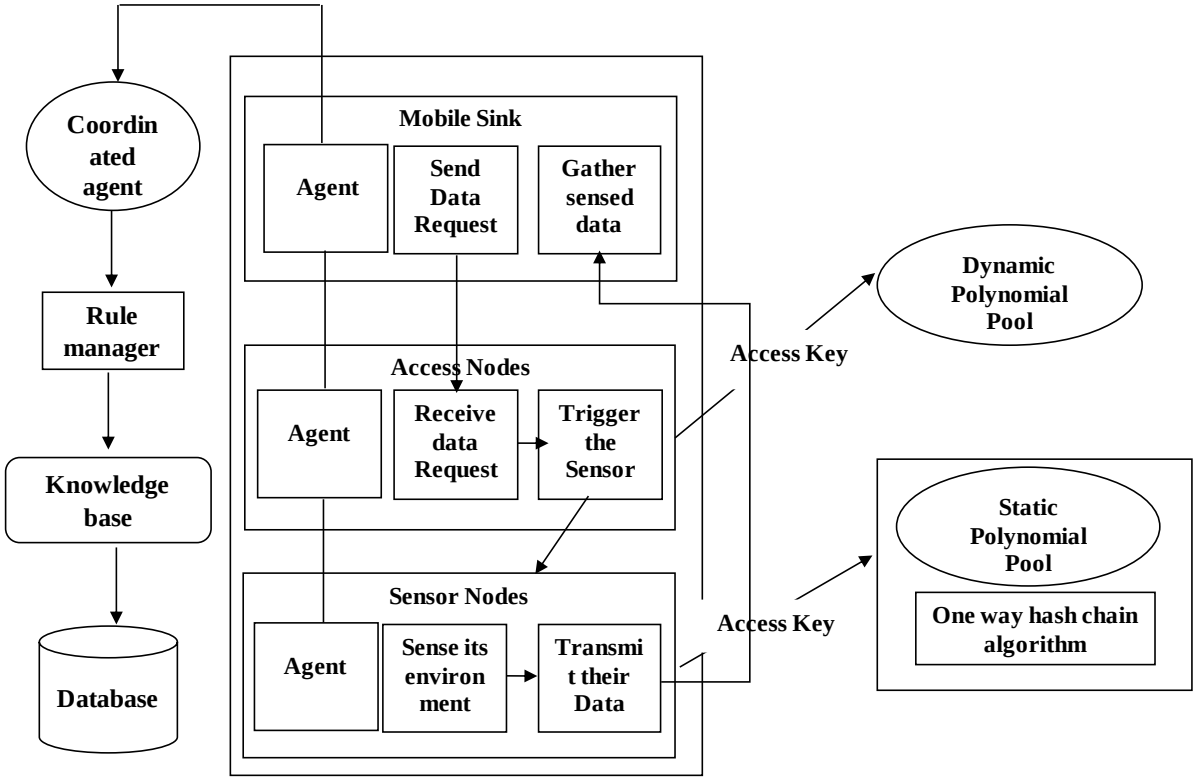


**Fig 2: System Architectural design**

## 3.1 Coordinated Agent and Knowledge Base

The agent at each layer has to communicate with the coordinated agent (CA). The CA is connected with rule manager and knowledge base. The past history of the nodes has to be recorded in knowledge base. Based upon the rule, the CA will check for the action to be taken. Coordinating agent will control all the action performed by individual agents.

### *3.1.1 Polynomial key distribution*

Two separate polynomial pools have been used for establishing the authentication between the networks. Each mobile sink randomly picks a subset of polynomials from the mobile polynomial pool. A small fraction of randomly selected sensor nodes carry a polynomial from the mobile 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.

The proposed three-tier security scheme will substantially improve the 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.

To make the three-tier security scheme more robust against a stationary access node replication attack, 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.

A natural progression from the last topic of Ignition Primary Circuits is to analyze the different types of trigger signals used to switch the primary circuit at the appropriate time. This particular type of pick-up generates its own signal and therefore does not require a voltage supply to power it. Recognizable by its two electrical connections, the pick-up is used as a signal to trigger the ignition amplifier or Electronic Control Module (ECM). As the metal rotor spins, a magnetic field is altered which induces an Alternating Current (AC) voltage from the pick-up. This type of pick-up could be described as a small alternator because the output voltage

rises as the metal rotor approaches the winding, sharply dropping through zero volts as the two components are aligned and producing a voltage in the opposite phase as the rotor passes. The waveform is known as a sine wave.

## 3.2 Rule Manager

Rule manager acts based on the past history of the user. The process of managing and controlling the behavior of the network is the role of Rule manager. It also optimizes the operational and functional properties of WSNs. The main function is to ensure that the sensor node is the Network operates properly, maintain the performance of the network and control the large no of nodes without human intervention. Moreover, Rule manager provides a set of management functions namely

- Integrate configuration
- Operation
- Administration
- Security
- Maintenance and service

Commitment rules (or desires) are pre-defined conditions to evaluate beliefs. If beliefs match commitment rules, the corresponding commitment management function (intention) will be executed. This agent-based approach [8] is designed for applications where only a partial view of the state of the network as a whole can be known at any one location or time IABP agents make power management decisions locally based on requirements of an application. By using agents, information exchange between nodes in a neighborhood in order to make a local decision can be eliminated since agents collect node data and process it to meet a specified goal. For example, the base station could inject a mobile agent into a sensor network to evaluate battery level of sensors in the network. This agent could also command nodes to reduce the sampling rate of sensors if their battery level is low. This scheme allows the base station to assess network states locally rather than gathering sensor node states to the base station. Power management [7] is also strongly related to other network attributes such as coverage, accuracy, battery longevity, and latency. The proposed agent-based approach can perform complex decision making for various energy saving strategies. Users can specify desired sampling frequency, transmission range, and node mobility. Agents can be used to redirect traffic or change a link between nodes in the network to ensure a balance between energy conservation and network coverage. When a node's battery level is critical, the agent finds another nearby node that can forward data. End users can also control sampling frequency by commanding sensor nodes to transmit only when there is something worth reporting. The energy preserved by reducing transmissions allows a greater sampling rate of sensor nodes, which usually increases the accuracy of sensor data. However, when data polling rates are reduced, there is a risk of missing a crucial event. End users can command that nodes reduce their transmission power in order to conserve power. However, since reducing transmission power reduces communication range, this scheme may compromise network connectivity. The degree of agent mobility freedom allowed in the network can influence the latency of data collected from sensor nodes to the user.

In Wireless Sensor Network, the sensor nodes transmit critical information over the network therefore, security services such as authentication and pair wise key establishment between sensor nodes and mobile sinks are important. However, the problem of authentication is solved by polynomial pool based pre-distribution scheme.

# 4. IMPLEMENTATION

## 4.1 Polynomial Pool Based Pre-distribution Scheme

Polynomial based key pre-distribution scheme [10], distributes a polynomial share (a partially evaluated polynomial) to each sensor node by using which every pair of nodes can generate a link key. Symmetric polynomial P(x, y) (P(x, y) = P(y, x)) of degree is used. The coefficients of the polynomial come from GF (q) for sufficiently large prime q. Each sensor node stores a polynomial with $\lambda + 1$ co-efficient which come from GF (q). Sensor node Si receives its polynomial share of fi(y) = P (i, y). Si (resp. Sj) can obtain link key Ki, j = P (i, j) by evaluating its polynomial share fi(y) (resp. fj (y)) at point j (resp. i). Every pair of sensor nodes can establish a key. The solution is $\lambda$-secure; meaning that coalition of less than $\lambda+1$ sensor nodes knows nothing about pair-wise keys of others. Polynomial pool-based key pre-distribution scheme considers the fact that not all pairs of sensor nodes have to establish a key. It combines Polynomial based key pre-distribution scheme with the key- pool idea in to improve resilience and scalability.

## 4.2 Performance Evaluation

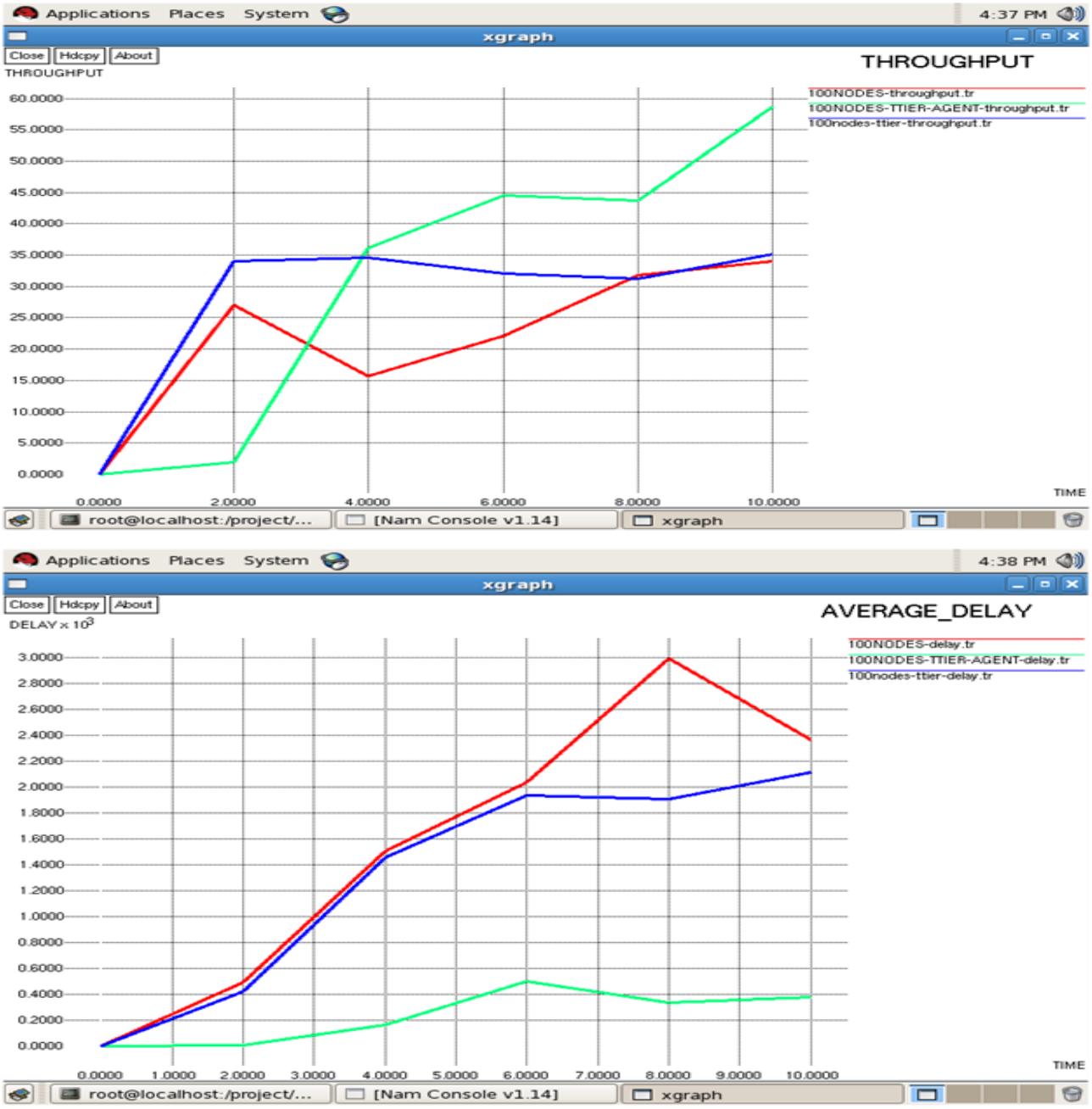


**Fig 2: Comparison of three-tier security between Throughput and Average end to end delay metrics**

As compared with three tier security scheme, the proposed scheme shows better results when Intelligent agents were used. Also it provides better power management. The number of attacks found by using intelligent agent is compared with throughput and average end to end delay metrics, the results are shown in Figure 3.

## 5. CONCLUSIONS

The proposed an Intelligent agent based three tier security scheme for authentication and pairwise key establishment between mobile sink and sensor nodes. The proposed scheme, based on the intelligent agent and polynomial pool based key pre distribution scheme has to detect and avoid such attack and also provide authentication between stationary access nodes and sensor nodes. Agents are inherently suited where the decision making context is - highly dynamic, resource bounded and the information is partial and inaccurate. The solution can be further extended to cover other vulnerabilities and attacks.

## 6. ACKNOWLEDGMENTS

We wish to express our heartfelt thanks to all the staff member of the Department of Computer Science and Engineering, GKM College of Engineering and technology and College of Engineering, Guindy Campus, Anna University, Chennai – 600 025 for their help and co-operation.

## 7. REFERENCES

[1] Akyildiz, F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. 2002 'Wireless sensor networks: a survey. Computer Networks, Vol. 38, pp. 393–422.

[2] Rasheed, A. A. and Mahapatra, R. N. 2012 'The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks. IEEE Transactions on parallel and distributed systems, Vol. 23, pp. 958–965.

[3] Blundolz, C., De Santis, A., Herzberg, A., Kutten, S., Vaccaro, U. and Yung, M. 1993 'Perfectly-Secure Key Distribution for Dynamic Conferences", Bnckell E. F. (Ed.): Advances in Cryptology - CRYPT0 '92, LNCS 740, pp. 471–486.

[4] Chen, M., Kwon, T., Yuan, Y. and Leung, V. C. M. 2006 'Mobile Agent Based Wireless Sensor Networks. Journal of Computers, Vol. 1, pp. 14–21.

[5] Ota, K., Dong, M. and Li, X. 2009 'TinyBee: Mobile-Agent-Based Data Gathering System in Wireless Sensor Networks', IEEE Int'l Conf. on Networking, Architecture, and Storage.

[6] Rasheed, A. A. and Mahapatra, R. N. 2007 'An Energy-Efficient Hybrid Data Collection Scheme in Wireless Sensor Networks', Proc. Third IEEE Int'l Conf. Intelligent Sensors, Sensor Networks and Information Processing, pp. 703–708.

[7] Rasheed, A. A. and Mahapatra, R. N. 2008 'An Efficient Key Distribution Scheme for Establishing Pairwise Keys with a Mobile Sink in Distributed Sensor Networks', Proc. 27th IEEE Int'l Performance Computing and Comm. Conf. (IPCCC '08), pp. 264–270 .

[8] Tynan, R., Marsh, D., O'Kane, D. and O'Hare, G. M. P. 2005 'Intelligent Agents for Wireless Sensor Networks', Fourth Int'l Joint Conf. on Autonomous Agents and Multiagent Systems 2005 (AAMAS '05), pp. 1179–1180.

[9] Rasheed, A. and Mahapatra, R. 2008 '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.

[10] Rasheed, A. and Mahapatra, R. 2009 'A Key Pre-Distribution Scheme for Heterogeneous Sensor Networks', Proc. Int'l Conf. Wireless Comm. and Mobile Computing Conf. (IWCMC '09), pp. 263–268.