IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. I (Jul.-Aug. 2016), PP 77-82
www.iosrjournals.org

Mobile Agents for Wireless Network Security

A. H. Mohamed[1] and K.H. Marzouk[1]
[1] *Solid State and Electronic Accelerators Dept., National Centre for Radiation Research and Technology (NCRRT), Atomic Energy Authority.*

Abstract: *Wireless sensor networks (WSNs) have widely applied in many applications. But, a security is considered one of their main problems. There are many different types of the security attacks faced WSNs. The suggested research focuses on using the mobile agents approach to improve the security systems for the WSN that can deal with the sinkhole and clone attacks. The suggested system has been applied for a WSN used in communicating between an electronic accelerator system and its control unit as a case of study. Comparing the obtained results by the proposed system and some traditional systems, the suggested system has proved its good acceptance for applicability in the real-time situations.*
Keywords: *Wireless Sensor Network Security; Mobile Agents; Network Security.*

I. Introduction

Wireless sensor networks (WSNs) have great focusing and attention by researchers due to their lower cost and attractive flexibility that enjoyed by both the users and the service provider. Some of the reasons for their widely spreading are: network implementation and coverage without cost of deploying and wiring. Besides, it is accessed by the users anytime and anywhere especially where connectivity to their places are difficult to reach by cabling, to complement the existing wired networks [1]. On the other hand, one of the main drawbacks of these WSNs is its inefficient security system.

But, the security of the wireless sensor networks is more important and complex rather than security of wired networks. As, wireless is broadcasting in nature, it becomes available for anyone within the range of the wireless' devices because it has an easy transport medium. However, it can be accessed easily by the attackers [2]. This increases the number of the threats that the security architecture must address. So, the security schemes in wired network cannot be used directly for the wireless sensor networks [3].

The wireless sensor networks face some additional problems that make it more challenges to secure. Open wireless medium, limited bandwidth, and system complexity are the main features of the wireless networks. They make the security of the wireless sensor networks more critical and complex rather than the wired ones [4].

On the other hand, mobile agents (MAs) approach provides a successful paradigm for distributed systems and dynamic network environment. For a WSN, mobile agent can be defined as a software component that is a code to be executed to have a function or a thread.

Mobile agents can move to the data at their destination nodes and so reduces the network traffic and latency. However, mobile agent can introduce an efficient solution in unreliable and low bandwidth connection cases [5].

Therefore, the proposed system suggests the uses of mobile agents for providing an efficient security system for the wireless sensor networks.

The rest of the paper is organized as follows: Section 2 Wireless Networks Security Types. Section 3 deals with the mobile agents and wireless network. In Section 4, mobile proposed security system is explained. In Section 5, applicability of the proposed system and its results are discussed. Finally, conclusion of the work in this research is presented in Section 6.

II. Wireless Sensor Networks Security Types

Security systems for the wireless sensor networks have additional unique challenges compared to a wired network due to the open nature of the access medium. In general, wireless networks suffer from higher number of security threats rather than the wired networks. The attackers can access the wireless sensor network easily due to its transport medium. Besides, the data are being broadcast via radio waves rather than transmitted over the wired networks [6]. However, there are various types of attack in WSN. Some of them are explained as follows:

- ***Sinkhole Attack***

In sinkhole attacks adversary changes the path of the entire traffic of the packets to a compromised node. So, the adversary's can attract traffic from a certain area through a compromised node and create a metaphorical sinkhole at the center. Sinkhole attacks can enable various other kinds of attacks such as selective forwarding [6].

- ***Wormhole Attack***

In the wormhole attack, an adversary tunnels' messages are received from certain node in the network and replays them for another node. Therefore, in a wormhole attack, the adversaries cooperate to provide a low-latency side-channel for communication. This ability may cause neighboring nodes to favor the attacker for routing.

- ***Sybil Attack***

Normally, a node can connect to a single set of coordinates from each neighbor nodes. In a sybil attack, an attacker enables multiple illegitimate identities in sensor networks. However, an attacker can appear to be in multiple places at the same time. This gives chances for the attacker to be selected as the next-hop in geographic forwarding.

- ***Clone Attacks***

In this type of attack (also known as node replication attack) an attacker adds a node to the nodes of the sensor network by replicating the node ID of an existing sensor node. This causes a disconnection of the WSN's communication such as packets can be corrupted or misrouted. However, failure in the sensor readings can be appeared. Moreover, these cloned nodes can be deployed in different locations of the sensor network. This can cause a failure for the whole wireless sensor network [8].

III. Mobile Agents and Wireless Networks

The traditional protocols of the WSNs have used the computer-to-computer communication as Remote Procedure Calling (RPC). It enables a computer to call procedures in another computer across the network [9]. Each message transmitted by the network either request or acknowledge is represented as a procedure's task. A request includes data that are the procedure's argument. While, the response includes data that represents its results. On the other side, mobile agents have used as an alternative method that belongs to computer- to-computer communication methodology. It is a remote procedure that has used Remote Programming (RP) to enable a computer to call procedures in another computer and supply the procedure to be performed [10]. The messages transport in the network contains a procedure only, while the data is static.

However, mobile agents are programs that can move from one computer to another in a network or at times to any host of their choice making them autonomous. Using the mobile agents for WSNs can improve their performance and saving the data. But, on the other side, moving the mobile agents around the network can face with some threats. Thus, there are four known threat MA, namely: The Agent- to-Host, Agent-to-Agent, Host-to-Agent, Other-to-Agent Host attacks are the kinds of security attacks that are possible in a Mobile Agent System [11].

Many security systems have been developed for wireless sensor networks using the mobile agents approach but they still suffer from some complexity and depend on their application [12-16]. So, the proposed system introduces a novel system that can improve the performance of the security system for WSNs.

IV. Proposed Security System

The proposed system has suggested the uses of mobile agents for the WSNs security. The suggested system uses mobile agents for collecting and analyzing the data in the wireless environment. It uses different types of agents to detect the attacks. They are: collector agent, misuse detection agent, attack detection agent, and alert agent.

1- Collector Agent

The collector agent collects the data from the wireless environment. Then, it stores the data in the file.

2- Misuse Detection Agent

The misuse detection agent is used to analyze the data acquired for having attacks in network, and reports it to alert agent.

3-Attacks Detection Agent

The attacks detection agent is used to detect the attacks face the WSN.

4- Alert Agent

The alert agent is used to alert the system if any attack occurs in the network.

However, the operation of the proposed system can be described as: The collector agent is used to acquire the data from the wireless environment and stores it as a file. This file is used by the misuse detection agent. It analyses the data by matching it to its reference. If there is any attack appeared, it reports it to alert agent and updates the database about the attack.

On the other side, the proposed security algorithm is concerned with two main types of attacks. They are: Clone and sink hole attacks. Each of these attacks is handled by a separate module.

a) Proposed Mobile Agents Based Clone Attack Detection (MACAD) Algorithm

The proposed Mobile Agents Based Clone Attack Detection (MACAD) Algorithm can be explained in the following steps:

1- Identify the location of each node (for ex: node A) in the network and also identify its location and signature for a group of its neighbor nodes (N).
2- Mobile agent gets the signed location claim of each node and stores it in its defined cell in the node's information matrix. This matrix is constructed through the mobile agent routing algorithm.
3- At run-time, each node must be verified by its signature and plausibility of location by each node in its neighboring group (N).
4- If more than one entry for signed location claim is appeared in a single cell of an information matrix of one node. This is achieved only when mobile agent has a different latest location claim for the same node i. In this case, mobile agent broadcasts the two conflicting claims as evidence to the network's nodes in order to prevent this repetition.
5- The proposed system broadcasts the event to every node in the entire network. Therefore, a real node will not replay for the inaccurate information from malicious.
6- The proposed system has used the mobile agents to execute steps 4 and 5.

b) Mobile Agent Based SinkHole Attack Detection (MASAD) Algorithm

This module of the proposed system has used the Mobile Agent Based Sink Hole Attack Detection (MASAD) Algorithm for routing the data by avoiding the sink hole attack. It can be explained as follows:

1- The node's information matrix is acquired through mobile agent routing algorithm.
2- If the network needs to send the data packets from node A to node B, it can be transmitted by the MASAD algorithm based on node A's information matrix referring to the cell in Ath row and Bth column).

3- The algorithm firstly examines matrix AB of A's matrix to determine the availability of communication. If matrix AB finds a connection between A and B. The data packets are sent to B directly and the algorithm ends the routing.
4- Otherwise, check the cache of node B in column B and find out all the items that are not equal to zero in B. These items are the second level nodes of node B. If all the items in B has no valid route between node A and node B, the routing ends.
5- Set the maximum number of hops to reach the destination as n.
6- Initialize m =1. Where m = current number of hops. Increment m by one for each second level node of node1 to node n. This process continues till it reaches to node A. So, there is a connection path between nodes A and B. The maximum repeated hop with less weight is selected as the optimal one every time. Achieving the maximum agent counter value that has less matrix's value of AB for every neighboring nodes A and B can decrease the chance of paths containing sink hole.

JADE (Java Agent Development framework) software framework is used to implement the proposed mobile agents' security system for wireless sensor network.

V. Applicability of the Proposed System and its Results

The proposed system has been applied for a wireless sensor network that can communicate between an electronic accelerator system and its control centre.

Simulation is carried out for randomly deployed area of 10m × 10m between the accelerator and the control centre. The proposed system and three common traditional systems: SHELL, LFAP, and PANJA are evaluated by applying for this test area [2]. The four systems are used to detect the clone and sinkhole attacks at different deployed nodes. The performance of the proposed system with and without incorporating the mobile agents is evaluated. Their obtained results from these systems are compared. The following figures present these comparisons between the test security systems.

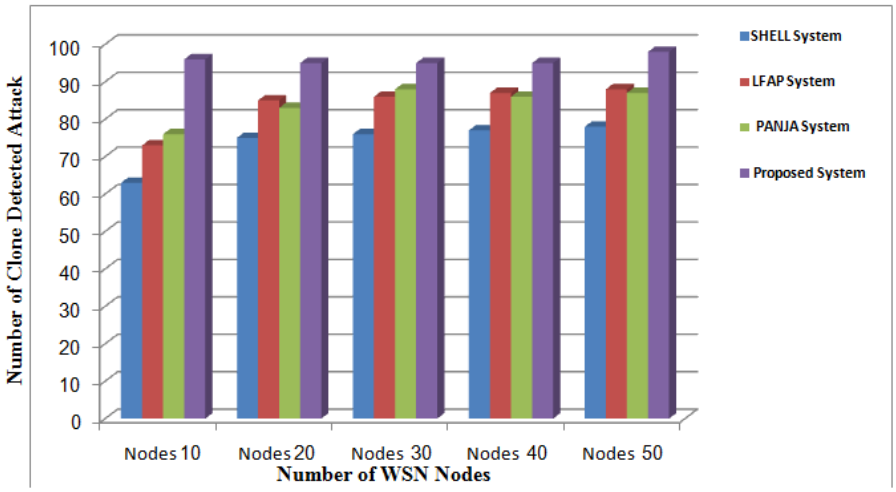

Fig. (1): Comparison between the number of Clone Detected Attack by the proposed system with mobile agents and the three traditional security systems at deployed nodes.

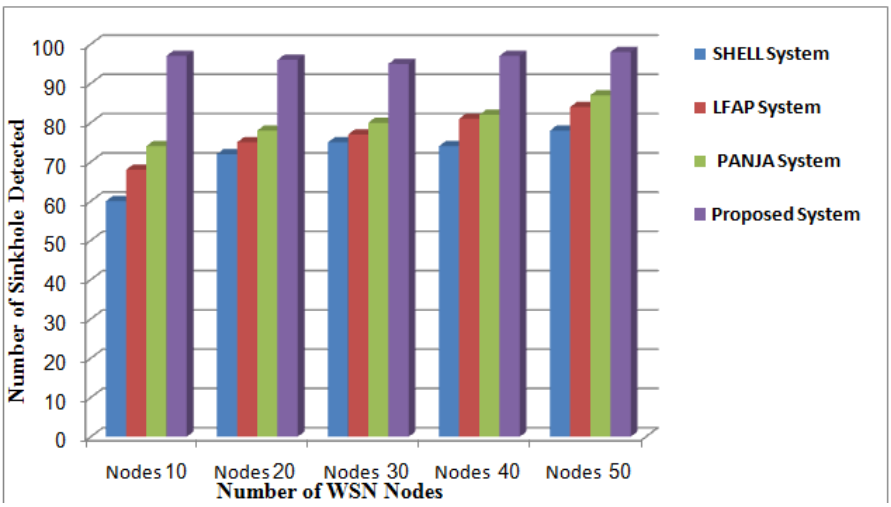

Fig. (2): Comparison between the number of Sinkhole Detected Attack by the proposed system with mobile agents and the three traditional security systems at different deployed nodes

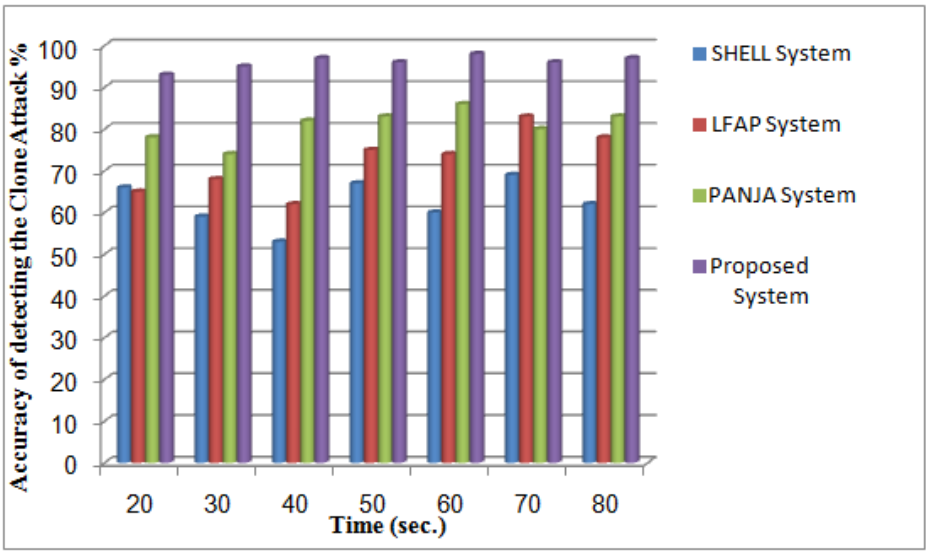

Fig. (3): Comparison between the accuracy of detecting clone Attack by the proposed system with mobile agents and the three traditional security systems

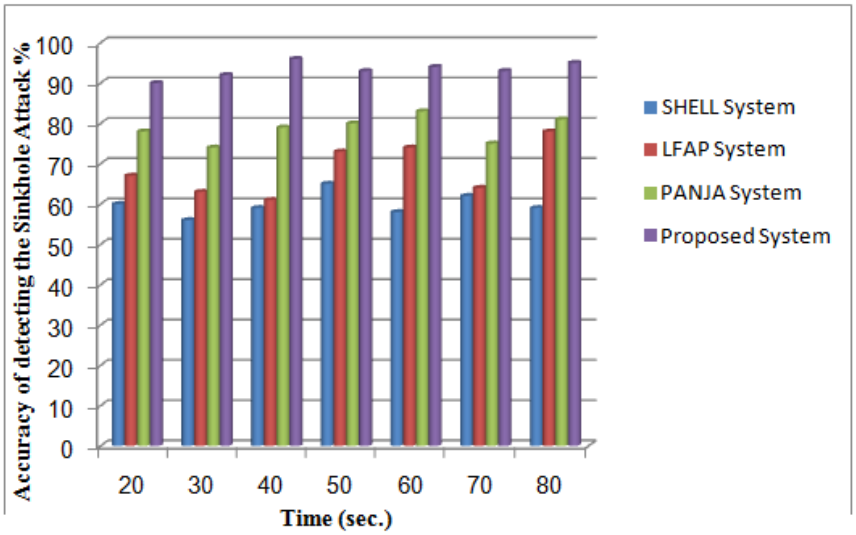

Fig. (4): Comparison between the accuracy of detecting Sinkhole Attack by the proposed system with mobile agents and the three traditional security systems

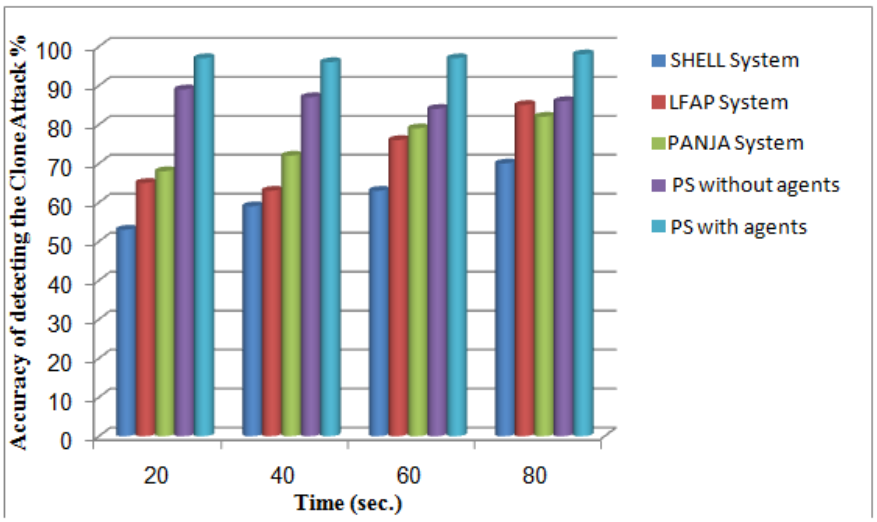

Fig. (5): Comparison between the accuracy of detecting Clone Attack by the proposed system with and without mobile agents and the three traditional security systems

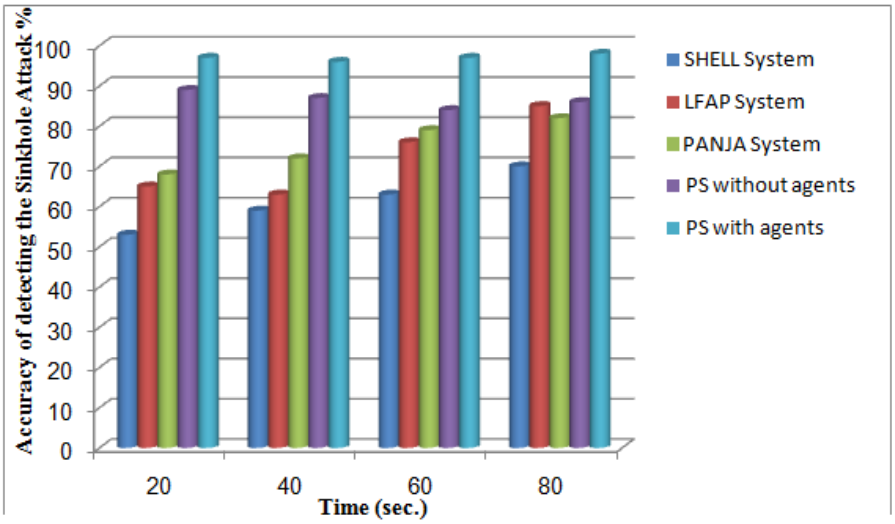

Fig. (6): Comparison between the accuracy of detecting Sinkhole Attack by the proposed system with and without mobile agents and the three traditional security systems

It is found that, the proposed system has detected more number of malicious nodes in all the tested cases when compared to those detected by the other three traditional security systems at different deploying nodes. Also, the accuracy of the proposed system is proved to be higher than those gotten from the tested traditional security systems.

On the other side, the achieved results show that the accuracy of the proposed system with incorporating the mobile agents have more accuracy rather than using it without the agents.

However, the obtained results proved the goodness of the proposed system with mobile agents and its improving for the WSN's security rather than the present systems.

VI. Conclusion

Secure communication is one of the major challenges in WSNs due to the various types of attacks that decrease the overall performance of the networks. So, the security based research and applications of WSN have attracted researchers' attention. The proposed system introduces incorporating the mobile agents methodology for the security system of the wireless sensor networks. It concerns detecting two main types of the WSNs' attacks, they are: clone and sinkhole attacks. To detect the clone attack, the suggested system learns the node locations for group of its neighbor nodes with very less communication overhead. By checking these neighbors, the security system can determine the real node from the claim ones. Also, this proposed system can provide necessary knowledge to every sensor node in a Wireless Sensor Network to determine the real communication path to avoid the packets to pass through the sinkhole attack. The proposed system has been applied for a WSN used to communicate between an accelerator system and its control centre. Its results are compared with those achieved from three common security systems.

From the obtained results, it is found that, the proposed system has improved the accuracy of detecting the clone and the sinkhole attacks in all the cases, because of:

1- The accuracy of the proposed security algorithm is increased due to the power of its conceptual security that concern tasks against the natural of each type of attacks without using the mobile agents.
2- The accuracy of the proposed system is increased more by using the mobile agents' methodology at different numbers of nodes. The mobile agents avoid movement of the data through the network. Accessing the data represents the goal of the attackers. So, although the media of the WSN is easy to access by attackers, the uses of the mobile agents prevent them from accessing the data. Therefore, the accuracy of the security system of WSN is significantly improved.

On the other hand, the proposed system has decreased the time of detecting the attacks by using the mobile agents at different numbers of nodes, because of:

1- The time of moving the data for the node having the tasks to be applied is higher than moving the mobile agents having the tasks. So, using the mobile agents has decreased the time.
2- Using the mobile agent can decrease the time for sending the messages and acknowledgments through the network. Thus, decreasing the analysis and number of operations needs to be done till achieved the required tasks.

Therefore, the suggested mobile agent security system has improved the performance of the present security system for the wireless sensor networks in the real situations. So, it has a significant success to be applied in the practical sites.

References

[1]. O. Abiona, et. al, (2013), " Wireless Network Security: The Mobile Agent Approach" , International Journal of Communications, Network and System Sciences, Vol. 6, pp.443-450.
[2]. A. K. Srivastava and A. Goel , (2011), " Security Solution for WSN Using Mobile Agent Technology " International Journal of Research and Reviews in Wireless Sensor Networks (IJRRWSN) Vol. 1, No. 3, September 2011, vol. 2, Issue1, pp.1-5.

[3]. H. Yang, F. Ricciato, L. Songwu and L. Zhang, (2006), "Securing a Wireless World," The Proceedings of IEEE, Vol. 94, No. 2, pp. 442-454.

[4]. S.Poornima and B.B.Amberker, (2010), "Agent Based Secure Data Collection in Heterogeneous Sensor networks", In proc. of Second International Conference on Machine Learning and Computing IEEE Computer Society of 2010 , pp.116-120.

[5]. B. Rachid, H. Hafid, (2014), " Distributed Monitoring for Wireless Sensor Networks: a Multi-Agent Approach, International Journal Computer Network and Information Security, Vol.10, pp.13-23.

[6]. X. Chen, K. Makki, K. Yen, and N. Pissinou, (2009), "Sensor Network Security: A Survey " IEEE Communications Surveys &Tutorials, Vol. 11, No. 2, Second Qarter 2009.

[7]. D Sheela and G Mahadevan,(October 2012), "Mollifying the Effect of Cloning, Sink Hole and Black Hole Attacks in Wireless Sensor Networks using Mobile Agents with Several Base Stations", International Journal of Computer Applications Vol. 55, No. 9, pp. 34-41.

[8]. D.Sheela, V.R. Srividhya, A.Vrushali, and J.Jayashubha, (2012), "A Mobile Agent Based Security System of Wireless Sensor Networks against Cloning and Sink Hole Attacks", International Conference on Computational Techniques and Artificial Intelligence (ICCTAI'2012) Penang, Malaysia, pp. 300-304.

[9]. B. M. Thippeswamy, (2015), "STEAR: Secure Trust-Aware Energy-Efficient Adaptive Routing in Wireless Sensor Network", Journal of Advances in Computer Networks, Vol. 3, No. 2, pp.146-149.

[10]. G. Zhan, W. Shi, and J. Deng, (2012), "Design and implementation of TARF: A Trust Aware Routing Framework For WSNs," IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 2, pp. 184-197, March/April 2012

[11]. D. D. Geetha, N. Nalini, (March 2014), " Trust based Neighbor Identification in Wireless Sensor Networks using Agents ", International Journal of Emerging Technology and Advanced Engineering , Volume 4, Issue 3 , pp.178-187.

[12]. Dr. H. Goyal, R. Sharma, (2013), " Intelligent Agent Operating in Wireless Sensor Networks: Review Paper ", International Association of Scientific Innovation and Research (IASIR), (An Association Unifying the Sciences, Engineering, and Applied Research), International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), pp.504-506

[13]. M. Chen, (2006), "Mobile Agent Based Wireless Sensor Networks", Journal of Computers, Vol. 1, No. 1, pp.14-21.

[14]. N. Hegde, Dr.S.kumar S.Manvi, (2014), "Simulation of Wireless Sensor Network Security Model Using NS2", International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 4, Issue1, pp. 113-119.

[15]. K. Nataraj, (2015), "Security Threats and Solution in Wireless Sensor Networks ", International Journal of Science and Research (IJSR), Volume 4, Issue 1, pp.873-876.

[16]. R.K. Verma S. jangra, (December 2013), "Significance of Mobile Agent in Wireless Sensor Network", International Journal of Advance Research in Computer Science and Management Studies Research Paper, Volume 1, Issue 7, pp.328-335.