ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(35), DOI: 10.17485/ijst/2016/v9i35/101813, September 2016* ISSN (Online) : 0974-5645

Enhanced Security for Wireless Sensor Networks Using Smart Mobile Agents

A. Vijayalakshmi* and T. G. Palanivelu

Department of Electronics and Communication Engineering, Sri Manakula Vinayagar Engineering College, Pondicherry University, Puducherry, India; vijilakshan@gmail.com, tgpvel@gmail.com

Abstract

Objectives: To enhance wireless sensor network security by selecting secure nodes for transmission and eliminating threat nodes from the routing path using Mobile Agent (MA) deployment. **Methods:** Smart Mobile Agents (SMAs) executes three different functionalities such as data gathering, transmission, and behavior monitoring, each of which is incorporated to Mobile Collector, Dispatcher, and Scrutinizing Agents respectively. **Findings:** Simulation results prove that SMA based network improves throughput by 55.56%, minimizes misdetection and disconnection probability by 21.6% and 20% respectively. SMA based network also decreases packet loss by 20%. **Improvements:** SMA deployed network shows better performance than non-SMA based networks as they are complex while integrating the multiple functionalities as a single task.

Keywords: Dispatcher Agent, Genus Function, Scrutinizing Agent, Smart Mobile Agents - Mobile Collector Agent, Wireless Sensor Networks

1. Introduction

The most important issue of Wireless sensor networks is the security issue. In order to overcome such an issue the client server model came into existence. Generally the client server model is defined in such a way that client request certain information to the server and the server on responding to the request forwards the required information, but in case of servers responding to the request of the multiple clients will lead to unnecessary energy consumption. To avoid such an issue mobile agents are used. The mobile agents migrate between the clients of the network. The function of the mobile agent is to behave accordingly to the network and in providing data dissemination to all the clients. In wireless sensor networks the traditional client/server method represents such that the client will be the destination and the server will be the source node. The source node on receiving requests from the client has to fetch the data and transmit to the sink node which leads to increase in bandwidth and energy consumption. In mobile agent approach, the sink nodes make the mobile agents to migrate to the objective region so that it aggregates the data collected and sends it to the sink node. The mobile agents has vast advantages such as reduced communication cost, asynchronous execution, direct manipulation, dynamic deployment of software, ease of distributed applications. The mobile agents must be programmed in such a way that it is amicable to all the systems in order to collect data and transfer the data[1]. The middleware architecture for mobile agents is proposed in wireless sensor networks applications and to overcome traditional client/server architecture models. Generally middleware is accomplished to operate on top of any operating systems in Wireless Sensor Network (WSN) and providing security for middleware is more demanding[2]. The middleware framework is designed in such a way that it will integrate with wireless network components and technologies and will adapt suitably with the distinctive changes in wireless sensor networks[3]. Since Mobile agents are confined with energy issues and task duration the

* *Author for correspondence*

emergence of multiple mobile agents has been proposed[4]. The Multi agent system which are autonomous and has the advantage of entering and leaving the network at any point of time can solve computational problems effortlessly[5]. The rest of the paper is organized as follows: section 2 describes problem identification. Section 3 explains the proposed method. Performance analysis and the results are described in section 4. The paper is concluded in section 5 and the figures are illustrated in section 6.

2. Problem Identification

In mobile agent based wireless sensor networks network optimization has been proposed; but for security some of the methods have been proposed, which doesn't provide security to all the attacks. Another drawback for employing mobile agents is computational overhead; if more number of mobile agents is adopted then computational complexity will be increased. So we propose a method which provides more security and utilize mobile agents with less computational complexity overhead.

3. Proposed Method

In this proposed system WSN consists of three types of agents: 1. Mobile Collector Agent, 2. Dispatcher Agent, and 3. Scrutinizing Agent. Mobile agents will have attributes such as control over network and follows a route in moving between the nodes in a network and in between different networks. They have the ability to make a decision independently; the mobile agent endorses time serving information according to the network and provides the stability to the network by reducing computational overhead, energy minimization and eases bandwidth constraints.

3.1 Mobile Collector Agent

The Mobile Collector Agent (MCA) covers the entire area of the network and it interacts with other agents. The MCA's executes broadcasting, routing and path clearances, forwarding and receiving, synchronizing communication and abstraction. It acts as both the listener and the commander. The MCA on listening to the scrutinizing agent it commands to the dispatcher agent. The source must broadcast to any one of the mobile collector agent for the process of determining the path. The MCA changes accordingly with respect to their utility, user mapping resources and energy. The collector agent is selected in such a way that it has the ability to map and interface itself with the user applications. In terms of energy transmissions the MCA's with high residual energy is chosen and in case of emergency the MCA that delivers packets with minimum delay must be preferred.

3.2 Dispatcher Agent

The dispatcher agent considers the features of a MCA. The dispatcher agent provides the privileges to all the mobile agents, these dispatcher agents are zone dependent or group dependent i.e a cluster of nodes within the broadcast range of dispatcher agent interact with the collectors through dispatcher agent. The dispatcher agents analyze the network for their congestion factor; when the congestion is high then each of the dispatcher load is distributed among the available dispatcher nodes within their range.

3.3 Scrutinizing Agent

The Scrutinizing Agent (SA) supervises transmissions, sequences and susceptibility of all the active and inactive nodes. The scrutinizing agent provides two different records: Forwarding record and Halting record. The nodes which have been scrutinized are identified as forwarding record and are privileged to transmit data. The nodes which act as an intermediate for transmissions but don't function as a source are known as halted nodes. These halting nodes are not allowed for user application transmission. The scrutinizing agent examines their behavior for consequent transmissions between the intermediates alone.

3.4 Genus Function

The dispatcher agent makes use of a secure private key for communication. The key is generated through ECC Genus function. The process of keying is briefly described as follows: Each of the genus function has two edges for fitness: raising and falling edge. In a raising edge, the node is assumed to be in forwarding state and in a falling edge, a node is said to be in halt state. Depending upon the state, the fitness function changes with respect to

the node state information: Forwarding State (Sequence Number, Next Node, DF, Drop) and in Halt State (Last Sequence Number, Drop, RERR, ACK)

3.5 Process of Hashing

For a genus function G, a temporal routing hash function H is initiated for all 'n' transmissions to active nodes "N" in the network in the region (X*Y). For all transmission from sender SA initiates H, based on the availability of MCA and validity of G. Validity of G is transmission dependent; G is void if there is an interference or congestion. Genus function factor is computed between 0 and 1 but not 0 for a sequential transmission node. Each node is independent to build its own Genus but it has to share with the SA. Any node that bypasses or denies sharing its Genus Function, then that particular node is declared as malicious.

3.6 Concealed Data Aggregation

Concealed Data Aggregation (CDA) provides secure data aggregation without delay. In CDA, the intermediate aggregator nodes don't store any information and so it provides end to end privacy between sensor nodes and sink. The decryption of data in the aggregator nodes increases the node compromise attack in aggregator nodes and it causes the revealing of large amount of information as well as the secret key to the adversary easily by losing the end to end confidentiality of data. So hop by hop encrypted data aggregation protocols does not provide critical solution for energy constrained WSNs. The CDA techniques allows aggregation on cipher text due to the Privacy Homomor Phism (PH) property on encrypted data rather than plain sensor data and provides energy efficient secure data aggregation solution to WSNs. Among them, asymmetric PH based CDA techniques are important due to their support of elliptic curve cryptography having reduced key size. Thus it provides better system security with reduced key size. So it is applicable for real time application requiring better security.

4. Performance Analysis

The proposed model is simulated using NS2 simulator. The network is created with 100 sensor nodes and 6 smart mobile agents. The performance of the network with and without smart mobile agents is analyzed. The simulated results proved that the performance of the network is enhanced using SMAs.

4.1 Simulation Results

Figure 1 illustrates the throughput comparison between Smart Mobile Agents (SMA) deployed network and SMA less network, where at 10s time, and the observed data rate for SMA less network is 1Mb, the same for SMA deployed network is 1.8Mb. As the false probe increases, misdetection of a node increases as shown in Figure 2. In both SMA and non-SMA scenario, misdetection rate increases. When compared to non-SMA, SMA has lesser misdetection ratio. The probability of eliminating a link due to its adversary effects among the available active links is called disconnection ratio. As the number of nodes increases, number of links increases eventually increasing the disconnection ratio. Figure 3 depicts that the disconnection observed for 30 nodes in an SMA deployed network and non-SMA deployed network are 44% and 64% respectively, the proposed SMA decreases the disconnection ratio by 20%. Packet loss refers to the drop that occurs in a transmission between source and destination. As the number of keys increases, vulnerability decreases, minimizing the packet drop. As SMA's are decision making systems, the packet loss is less due to frequent monitoring and change in dispatchers. From Figure 4 the packet loss percent for non-SMA for 100 keys is 27% whereas for the same number of keys, only 7% of packet loss observed in SMA. Therefore, SMA is said to minimize packet loss by 20%. The exposure to vulnerability and packet loss determines the security level of a network. As the number of keys increases, the security of a network increases. As SMA's are smart decision making agent nodes, they improve the security by instantaneous detection and elimination of threat, which hikes the security level of a network. Figure 5 depicts the security level observed for SMA deployed network and non-SMA network. The security level is enhanced for SMA deployed network.

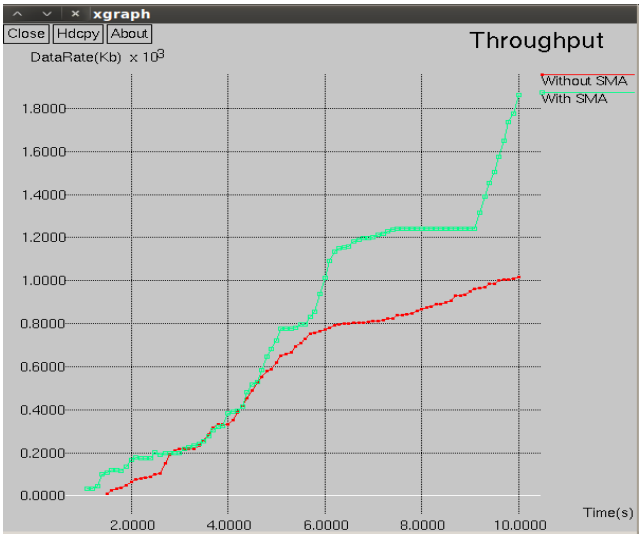

Figure 1. Throughput comparison.

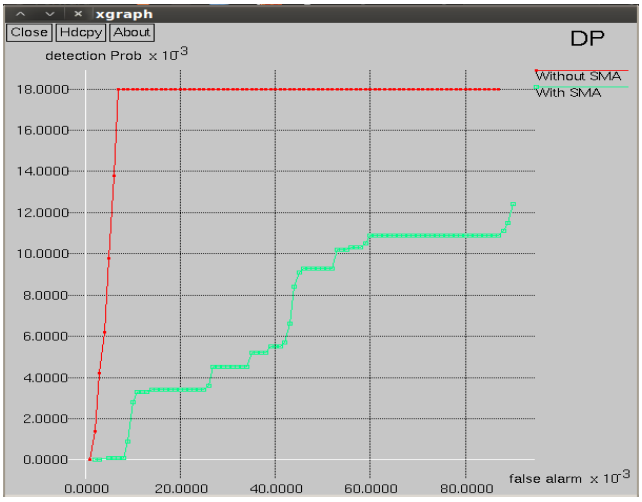

Figure 2. Misdetection probability comparison.

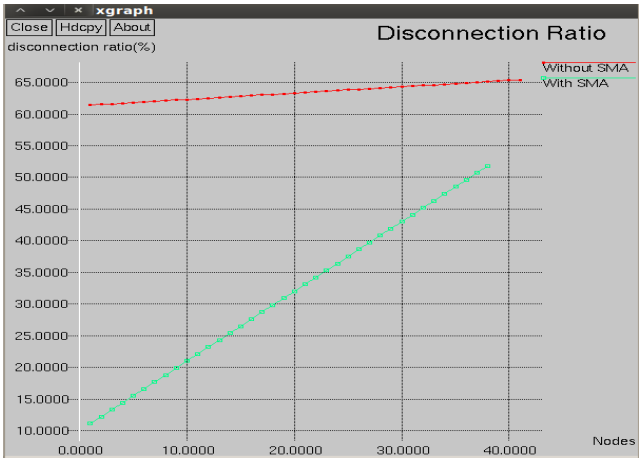

Figure 3. Disconnection ratio comparison.

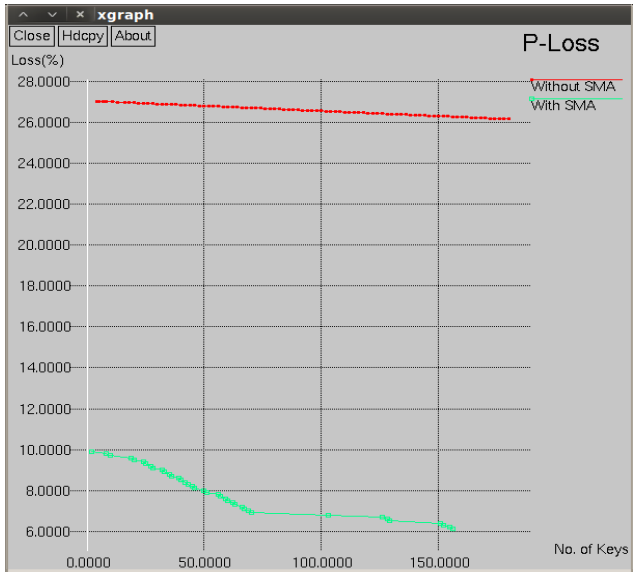

Figure 4. Packet loss comparison.

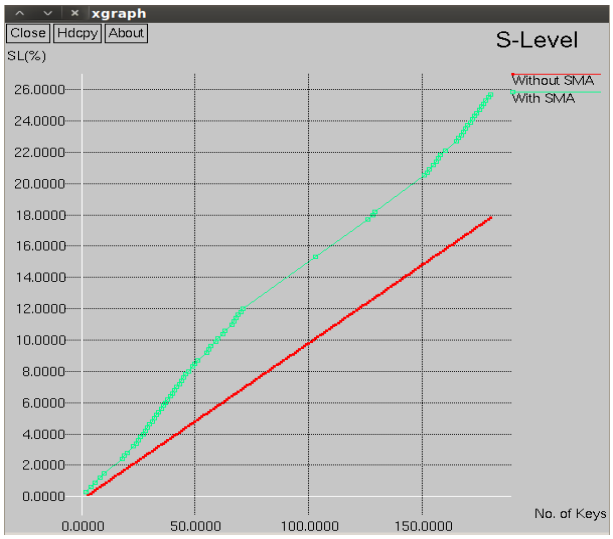

Figure 5. Security level comparison.

5. Conclusion

The proposed wireless sensor network with smart mobile agents such as Mobile Collector Agent, Dispatcher and scrutinizing agent improves the network performance providing high security level, lesser packet drop and improved throughput. The SMA based working is developed with scalability extending the agent support for large scale networks. The work can further be improved by retaining the networks performance considering various attacks.

6. References

1. Jian Xu, Xin Zhou, Jian Han, Fuxiang Li, Fucai Zhou. Data Authentication Model Based on Reed-solomon Error-correcting Codes in Wireless Sensor Networks. Institution of Electronics and Telecommunication Engineers Technical Review. 2013 May; 30(3):191-99.
2. Muhammad Usman, Vallipuram Muthukkumarasamy, Xin-Wen Wu, Surraya Khanum. Securing Mobile Agent based Wireless Sensor Network Applications on Middleware. http://ieeexplore.ieee.org/document/6380993/. Date Accessed: 13/12/2012.
3. Extending Middleware frameworks for Wireless Sensor Networks. http://ieeexplore.ieee.org/document/5345420/. Date Accessed: 4/12/2009.
4. Orhan Dagdeviren, Ilker Korkmaz, Fatih Tekbacak, Kayhan Erciyes. A Survey of Agent Technologies for Wireless Sensor Networks. Institution of Electronics and Telecommunication Engineers, Technical Review. 2010; 27:1-7.
5. Abdelhakim Hamzi, Mouloud Koudil, Jean-Paul Jamont, Michel Occello. Multi-Agent Architecture for the Design of WSN Applications. Wireless Sensor Network Journal. 2013 Feb; 5(2):14-25.