Detection of Malicious Nodes in Densely Populated Wireless Sensor Network Using Mobile Agents

Dr.T.G.Palanivelu[1] , A.Vijayalakshmi [2]

1.Professor, Department of Electronics & Communication Engineering, SriManakula Vinayagar Engineering College, Puducherry, India

2. Associate professor,Department of Electronics & Communication Engineering, SriManakula Vinayagar Engineering College, Puducherry, India

Abstract

Wireless sensor networks play important role in many applications for an effective observing and measuring properties of the physical world. The significant act of its intelligent behavior make it useful in important applications like military and disaster management. It is a highly distributed large scale system in which malicious nodes planted by strangers impose a threat for confidentiality and integrity along with denial of service in certain applications. To combat such situation security algorithms are incorporated in the context aware middleware arranged in the sensor nodes. Such a provision has got the drawback of more energy and overhead needs along with higher cost. In the method proposed here, a cost effective agent node based middleware is organized to identify malicious nodes and inform the friendly sensor nodes about the details of them. The agent based secured WSN (ABSWSN) system is simulated to establish its performance for overcoming the effect of the presence of malicious node. The agent based system performs better as far as processor time utilized and packet loss, giving higher throughput.

Keywords- mobile agent, malicious node, middleware ,WSN security

1. Introduction

Wireless sensor network employing billion of sensors all over the world are used for effective data collection towards monitoring different appliances remotely [1].The breakthrough in MEMS technology development of low power radio techniques and advances in low power embedded architecture, gave birth to WSN [2]. The availability of CMOS hardware is the main reason for the low cost deployment of the sensors in this network. Directed diffusion data centric routing associated with query processing made these networks quite reliable. Distributed data aggregation and multi object tracking resulted in effective data collection at a remote point with required speed and optimum latency. In recent application systems composed of state machines with command and event handlers, transition modules from one state to another is used for quick, low overhead, non blocking state transition[3]. In these networks many independent modules are allowed to efficiently share a single execution context. In order to achieve the necessary levels of concurrency, the system design using state machine based programming model as opposed to a thread based programming model has been adopted. The design of making each component of service as a state machine, it is possible to make very efficient use of CPU and memory resources[4].Sensor nodes can be used in many applications such as military, environmental and health[1]. In applications like military, there is a threat to the WSN on integrity and denial of service. The sensor node works with low power, limited resources dynamic network topology and various scales of network deployment. With all these constraints WSN has to manage the security requirement also[5].

The large deployment of WSN’s in harsh environments increase their exposure to malicious intrusion and attacks such as denial of service. The medium facilitates eavesdropping and adversarial packet injection to compromise the network functioning. Standard security mechanism cannot be arranged in WSN environment as it cannot provide heavy hardware weight and resource consumption. These factors impose the need to develop comprehensive and secure solution that achieve wider protection. Middleware arranged must take into consideration these facts while providing comprehensive solution to confidentiality, authentication, integrity, freshness and availability[6,7].To reduce the weight along with energy consumption of the sensor nodes, the middleware is arranged in the agent node.

There are two kinds of attacks by malicious nodes, namely passive and active attacks. Passive attacks obtain data exchange in the network for personal benefit without interrupting communication. The active attack implies the disruption of normal functionality of the network resulting in information interruption, modification or fabrication. Eavesdropping, traffic analysis and traffic monitoring comes under passive attacks. Active attacks include jamming impersonation, modification, denial of service and message replay towards false identification in messaging. Attacks may happen both internal and external, but in a well organized wireless sensor networks, the internal attack due to a compromised node can be avoided. The cyber attack of nodes whether it is internal or external may be identified as malicious one and their attacks are avoided suitably.

Earlier methods (Fig.1) involved sensor nodes of the system for analysis and identification of wireless environment to locate malicious nodes. The proposed method involves a mobile agent for identification of malicious node resulting in energy aware wireless sensor network. The mobile agent has security middleware apart from having middleware for dynamic source routing. In wireless sensor networks, agents are organized on a random path to visit all the sensor nodes for assisting their events(Fig.2).

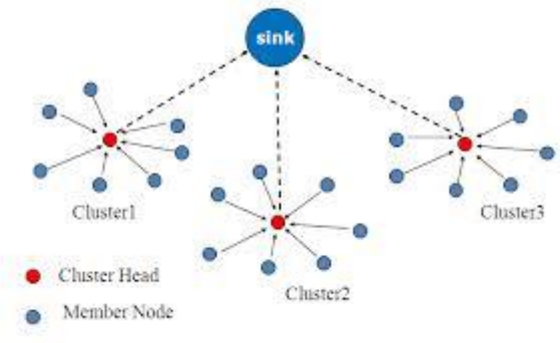


Fig.1.Wireless sensor network

The software infrastructure that glues together the network hardware, operating systems, network stacks and application is called the middleware. The middleware provide standardized system service to diverse applications in runtime environment to support and coordinate multiple aspects of the application. The middleware adopted invariably aim at providing mechanism to achieve adaptive and efficient utilization of system resources.

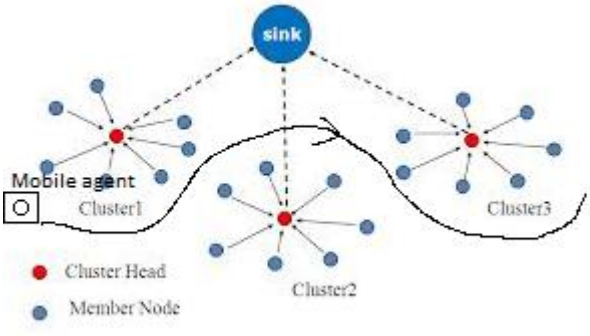


Fig.2.Mobile agent in wireless sensor network

The middleware arranged at various WSN will aid in managing i) limited power and resources ii) scalability, mobility and dynamic network topology iii) heterogenity iv) realworld integration using real time protocols v) application knowledge and data aggregation with reduced redundancy vi) security.The middleware arranged with the mobile agent shoulders these responsibilities and improve the lifetime of the sensor nodes.

Location computation of sensor nodes are also carried out by the middleware arranged. As these mobile agents have appropriate facility for sufficient energy storage and computation capacity its operation is quite reliable. The agent nodes use highly capable query language to interact with wireless sensor nodes and provide information with minimum latency by the process of flooding.

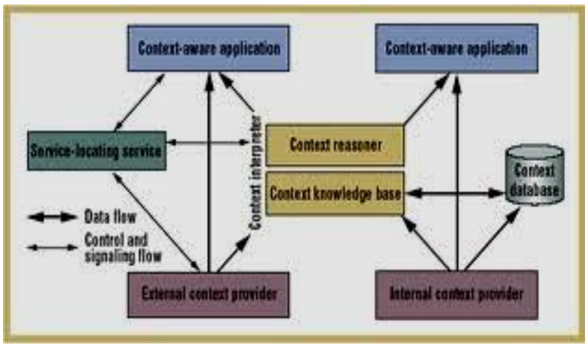

Context-aware application
Context-aware application
Service-locating service
Context interpreter
Context reasoner
Context knowledge base
Context database
Data flow
Control and signaling flow
External context provider
Internal context provider

Fig.3.Security oriented context aware middleware

2. Middleware For WSN Security

In the working environment of wireless sensor network, stranger nodes(malicious nodes) with criminal motive will enter. It is quite essential to isolate malicious nodes while routing and data distribution is taking place. Otherwise due to the activities of malicious nodes, there will be events of dropping of packets or routing them to a wrong destination. Sometimes the malicious nodes modify the packets which may result in wrong interpolation and decision. To avoid the malicious nodes, currently numerous algorithm and protocols have been developed and used but they increase the hardware and software complexities of the sensor nodes. This may result in the weight and the cost of the sensors. Hence a middleware based agent node topology is proposed amidst the distributed sensor node environment. These nodes make use of modern query languages to interact with other sensor nodes and collect the correct information for the cooperation[8].Embedded technology based hardware is employed for the agent . This kind of novel approach resolves many wireless sensor network issues enhancing application development. The middleware available with the agent bridge the gap between application and low level constraint of the sensors used (9).The agent node with security incorporated middleware is shown in fig.2. The external knowledge is collected through queries disseminated to various nodes in the wireless sensor network(fig4).A typical packet structure to inform the sensor node is shown in fig.5

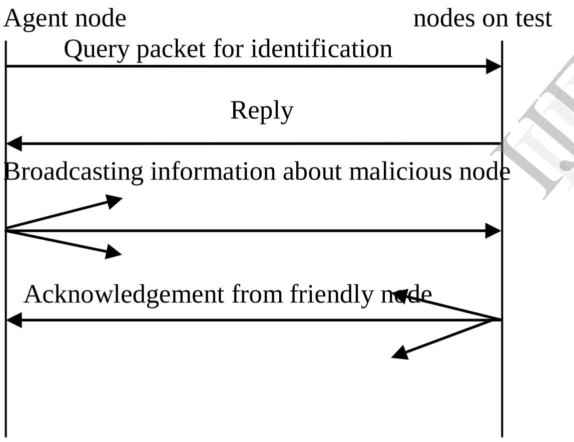
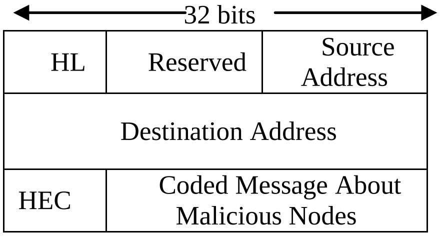

Agent node
nodes on test
Query packet for identification
Reply
Broadcasting information about malicious node
Acknowledgement from friendly node

Fig.4 Procedures during the query event of agent node

The mobile agent can provide identity code for collaborating candidate nodes with high order confidentiality. This is done with the help of different parameter keys like location and function. The agent will interact to the candidate sensor node by appropriate authentication of identity. By suitable query,it can collect data packets for providing them to candidate nodes. By suitable analysis and computation the agent detects the malicious node. The details of malicious node detection will be immediately flooded to all candidate sensor nodes and cluster heads. This facilitates the avoidance of malicious nodes in the system. The routing of data is done by selecting the correct candidate nodes for hopping. The agent node also provide information about the location of different nodes to the candidate nodes which is used in the construction of routing tables. Appropriate filtering of malicious node is carried out using the information received from mobile agent . Cluster topology is adopted to minimize energy latency and overhead. This kind of cluster based sections provide virtual machine data base system [11]. A message based middleware architecture called MIRES is employed with the mobile agent for the identification of malicious nodes. context aware middleware is adopted in the agent node which is quite effective in understanding the presence of malicious node.



HL	Reserved	Source Address
Destination Address		
HEC	Coded Message About Malicious Nodes	

Fig.5 Packet for providing information about malicious nodes

3. Simulation Results

The results of simulation carried are presented in fig.6 to fig.9. The simulation result presented in fig.6 indicates that more the malicious node present in the environment higher the processing time with the agent. This means that the mobile agent middleware was engaged for higher duration with higher number of criminal nodes. But if the middleware is with the sensor nodes, relatively higher processor time is required which will reduce its lifetime due to higher energy loss. In fig.7 it is noticed that with mobile agent middleware arranged the packet loss is negligible of the order of 0.03% But with sensor node security middleware the packet loss is observed to be more. From these results malicious node identification resulted in tolerable error rates due to negligible percentage of packet loss. From fig.8 it can be noticed that higher the percentage detection of malicious node were observed with mobile agent security arrangement whereas lower percentage detection observed with higher number of malicious nodes present. The mobility with the agent and cluster topology adopted could perform well in the detection of higher percentage of malicious nodes.The better capability of the agent node is due to its hardware & software architecture.

Such an arrangement cannot be provided in the candidate sensor middleware as there is a heavy size constraint .Fig.9 establish that higher the mean number of observation higher the percentage of detection

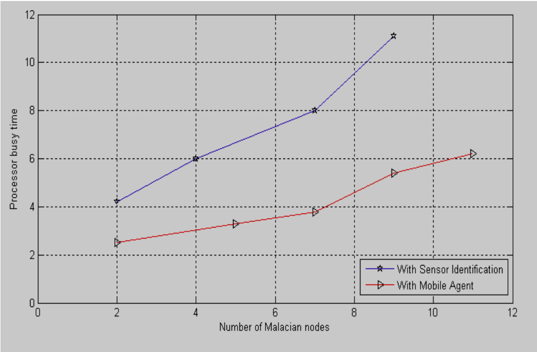


Fig.6 Effect of population of malicious node on processor time

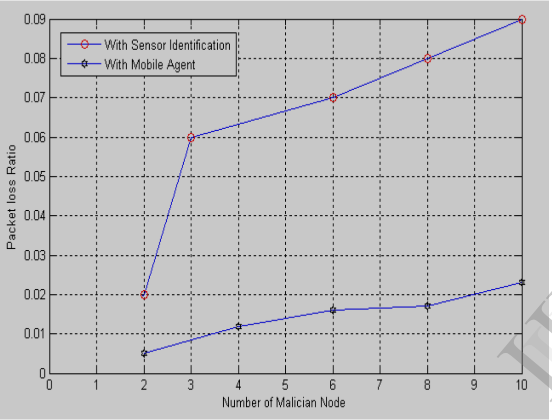


Fig.7 Effect of number of malicious node on packet loss

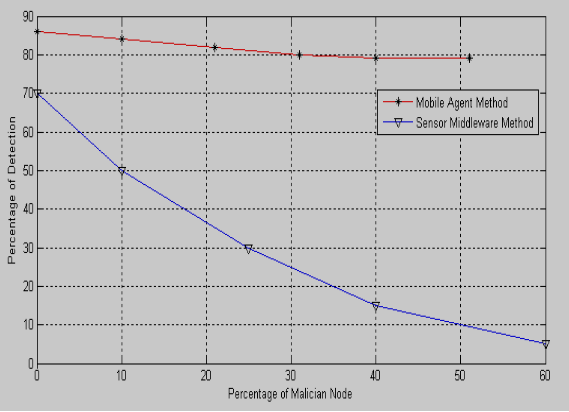


Fig.8 Effect of number of malicious node on percentage of detection

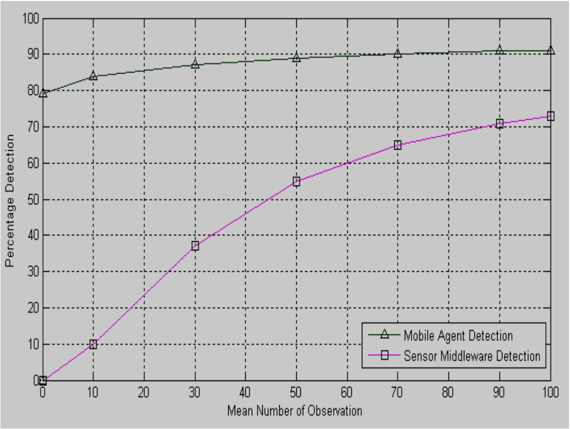


Fig.9 Number of observation on percentage detection

4. Conclusion and Future Work

Wireless sensor network security is provided using mobile agent in a cluster topology played important role in saving energy, minimizing latency and maximizing throughput while identifying the malicious nodes .The mobile agent provided an appropriate collaboration to sensor nodes in avoiding data transmission to sink. The work has been carried out for unicasting environment. In a multicasting environment the header structure and the complexity in routing algorithm need to be accounted in providing security. The multicasting environment can be explored for the suggested topology and its performance may be measured in future work.

REFERENCES

1. I.F. Akkyidiz and Weillian," A survey on sensor networks",IEEE communication magazine, Aug. 2007
2. Holger karl and Andreas willing, "Protocols and Architectures for wireless sensor networks" John Wiley and sons Ltd., 2008
3. M.H.Wary, J.N.Cao, J.Li and S.K.Das, "Middleware for wireless sensor networks -A survey " Journal of Computer Science and Technology, 23 (3), 305 – 325, May 2008
4. Biegel.G and Cahill.V,"A framework for developing mobile, context aware applications", Proceedings of the 2nd IEEE conference on pervasive computing and communication, pp.361-365, 2004.
5. Sandra kay miller, "Facing the challenge of wireless security" IEEE computers, July 2001, pp 16-18. E. Sonto etal, "A message oriented middleware for sensor networks" Procedings 2nd International workshop on middleware for pervasive and adhoc computing (MPAC2004) ACM press, 2004, pp.122-124.

6. C. Fox, G.Raman and C.Lu, " Mobile Agent middleware for sensor networks for application case study",Proceedings 4th International conference on information processing in sensor networks (IPSN 08) , IEEE press, 2005, pp. 382-387.
7. J. Zhao, R. Govindan and D. Estrin, "Computing aggregates for monitoring sensor networks" Technical report (02-773), USC, Sep. 2003.
8. Roman.M, Hers.C, Cerqueira, R.Tanganath A.Cambell RH, Nahrstedt.K, "A middleware infrastructure for active space", IEEE Trans. on pervasive computing, vol 1, issue 4. Oct-Dec. 2002, pp. 74-83.
9. Galpinl.I, Brenninkmeijer. C.Y.A Jabeen.F, Fernandas.A, Patrol N.N, " An Architecture for query optimization in sensor network, ICDE, 2008, pp. 1439-1441.
10. Brenninkmeijer. C.Y.A, " Querying networks requirements, Semantics, algorithms and cost models, Ph.D thesis, School of computer, University of Manchester ,2010.
11. G. Mac. N, Cubo. J, Franls, L, Pimentel. E, Configuring context aware middleware for wireless sensor networks, sensors 2012/2 pp. 8444-8570.

Dr.T.G.Palanivelu is presently working as Professor in Sri Manakula Vinayagar Engineering College, Puducherry. He was a former principal of Pondicherry Engineering college, Puducherry. He has more than 40 years of teaching experience. He published more than 100 papers in national & international journals. His research interest includes smart antennas, wireless communication, and Wireless Sensor Networks Security.

A.Vijayalakshmi is presently working as Associate Professor in Sri Manakula Vinayagar Engineering College, Puducherry. She has 14 years of experience in teaching field. She obtained her B.E. degree in Electronics & Communication Engineering from Madras University in 1998. She got Masters Degree in ECE from Pondicherry University. She is doing research in the area of Wireless Sensor Networks Security. Her area of interest includes Wireless Communication, Mobile Computing and Digital Signal Processing.