Volume 3, Issue 1, January 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Mobile Agent Security issue in Wireless Sensor Networks

Rupinder Singh Brar
Student of masters of technology
Depatment of Computer Science and Engineering
Shri Guru Granth Sahib World University
Fatehgarh Sahib, Punjab, India.

Harneet Arora
Assistant Professor ,
Department of Computer Science and Engineering
Shri Guru Granth Sahib World University
Fatehgarh Sahib, Punjab, India.

*Abstract--**The agent paradigm is currently attracting much research. A mobile agent is a particular type of agent with the ability to migrate from one host to another where it can resume its execution. In this paper security issues that need to be addressed before multi-agent systems have been discussed. It has been done by taking into consideration the implications of the characteristics given to agents and general properties of open multi-agent systems. The detailed review of the technology and methods applicable to mobile agent security systems has been illustrated in this paper.***

Keywords-WSN, Mobile agent, WSN security.

I. INTRODUCTION

Recent advances in micro-electro-mechanical systems (MEMS) technology, wireless communication digital electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate in short distance [2].

These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks based on collaborative effort of a large number of nodes. Sensor networks represent a significant improvement over traditional sensors, which are deployed in the following ways -

- Sensors can be positioned far from the actual phenomenon, i.e., something known by sense perception. In this approach, large sensors that use some complex techniques to distinguish the targets from environmental noise are required.
- Several sensors that perform only sensing can be deployed. The positions of the sensors and communications topology are carefully engineered. They transmit time series of the sensed phenomenon to the central nodes where computations are performed and data are fused.

A sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it. The position of sensor nodes need not be engineered or pre-determined. This allows random deployment in inaccessible terrains or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities.

Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an on-board processor. Instead of sending the raw data to the nodes responsible for the fusion, sensor nodes use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.

II. SECURITY ISSUES

There can number of malicious attack that are faced by sensor networks which can be define As follows:

A. Cloning Attack
B. Sinkhole Attack
C. Wormhole Attack
D. Sybil Attack
E. Node Replication Attack

A. Sinkhole Attack[4]

In sinkhole attacks adversary draws the entire traffic to a compromised node i.e. adversary's goal is to attract traffic from a specific area through a compromised node, creating a metaphorical sinkhole with the adversary at the center so that all packets pass through an adversary. Sinkhole attacks can enable various other kinds of attacks such as selective forwarding. Low-cost routes may be erroneously flooded to lure the traffic, or a wormhole attack could be mounted to actually provide a low-cost route. In either case, the objective is for the attacker to be positioned such that other selective forwarding attacks, or merely eavesdropping, are easier to do.

B. Cloning Attack[4]

This cloning attack is the entry point to a large span of insidious attacks. In such attack, an adversary uses the credentials of a compromised node to surreptitiously introduce replicas of that node into the network. These replicas are then used to launch variety of attacks that subvert the goal of the sensor application, and the operation of the underlying protocols. The detection of node replication attacks in a wireless sensor network is therefore a fundamental problem. Many protocols have been proposed in recent years for detecting node replication attack in sensor networks. Most of them however expose the following limitations: high performance overheads, unreasonable assumptions, necessity of central control, lack of smart attack detection etc.

C. Wormhole Attack[3]

In the wormhole attack, an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. Therefore in a wormhole attack, the adversaries cooperate to provide a low-latency side-channel for communication. This ability to understate ones distance from another node may cause neighboring nodes to favor the attacker for routing.

D. Sybil Attack[3]

In a Sybil attack an attacker makes multiple illegitimate identities in sensor networks either by fabricating or stealing the identities of legitimate nodes. Coupled with insecure location claims and an attacker can appear to be in multiple places at the same time. By making fake identities of nodes located at the edge of communication range all around a victim, chances are high that the attacker will be elected as the next-hop in geographic forwarding. It is only sensible to expect a node to accept a single set of coordinates from each of its corresponding neighbors, but by using the Sybil attack, an adversary can be found in more than one place at once.

E. Node Replication Attack[9]

In this type of attack (also known as clone attack) an attacker seeks to add a node to an existing sensor network by copying (replicating) the node ID of an existing sensor node. A node replicated in this fashion can badly cut off a sensor network's performance: packets can be corrupted or even misrouted. This can direct to a disconnected network, inappropriate sensor readings, etc. If an attacker can gain physical access to the entire network he can copy cryptographic keys to the replicated sensor an attacker loads its own nodes with the keys of and then deploys these cloned nodes in different locations of the sensor network.

i. Proposed Approach for Sink Hole and Clone Attack[4]

Mobile Agent Based clone Attack Detection Algorithm(MACAD)- This system is designed to make every node aware of location and identity of many nodes (Say n) so that Each neighbor of node A verifies the signature and checks the plausibility of Location of A.

When a node finds a collision different location claims with the same ID ,It broadcasts the two conflicting claims as evidence to revoke the replicas.

This system also makes every node aware of the entire network so that a valid node will not listen the cheating information from malicious or compromised node which leads to sink hole attack. The above said two jobs are achieved with the help of mobile agents. Data routing algorithm tells how a node uses the global network information to route data packets.

ii. Agent Routing Algorithm

The primary goal of agent is to deliver information of one node to others in the network. In order to achieve this goal with the least overload, we put forward a least visited neighbor first algorithm to control the navigation of mobile agent. An agent applies the algorithm to the information of node on which it currently resides, and decides its next destination. Each node has an information cache that agent scan update with more recent values.

Firstly, Update the information cache of node I with any newer information available in its own briefcase. In this step, information means how many times agent finds this particular node as a one hop neighbor to the previous node. Then, Agent gets the signed location claim= {IDi, Li, EP PRi {H (Idi || Li)} of node i. It is compared with the location claim of node i in the agent's briefcase. If it is similar, there is no updating for that field in agent's briefcase. Otherwise that field is updated with the latest location claim of node i. In next step determine which neighboring node has the least counter. It is the least visited neighbor. If this neighbor of i hasn't been visited in recent 3 times, the agent selects this neighbor as its next destination. Then next step after choosing the next destination, the agent updates its next destination's ID with the chosen destination node ID, and changes the history variables in the host node's information cache with the next destination node.

iii. MACAD (Mobile Agent Based Clone Attack Detection)Algorithm

The important steps of MACAD are:-

- Every node A prepares a signed location claim.

Fig.1:Signed location claim = IDA, LA, EP PRA{H(IdA || LA)}

- Mobile agent gets the signed location claim of node which is visited by it. The node's information matrix can be acquired through mobile agent routing algorithm.
- Each node A gets the information matrix (Table 1) verifies the signature and checks the plausibility of DAB(e.g. the distance between the neighbors cannot be bigger than the transmission range.)
- Signature verification is explained in the Fig 2.

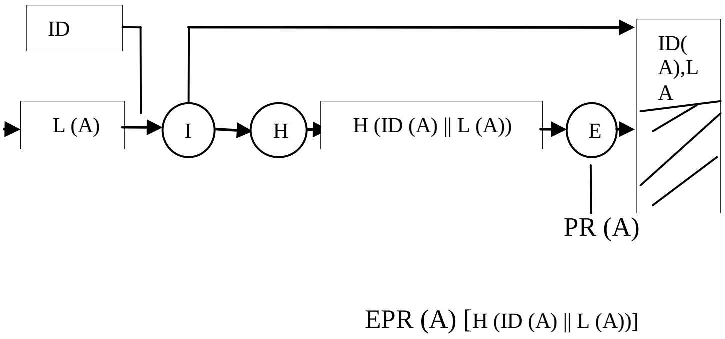

Fig.1 Preparation of location claim[4]

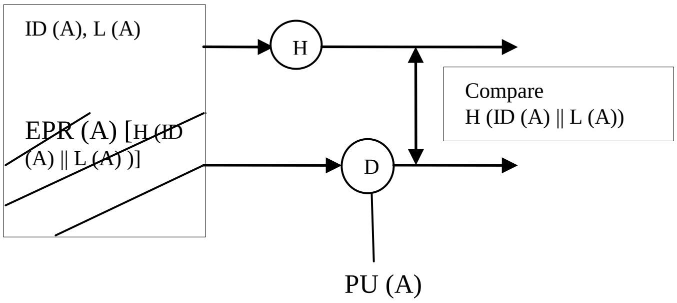

Fig.2 Signature Verification[4]

• Here, more than one entry for signed location claim may be made in a single cell of an information matrix of one node. It happens only when mobile agent carries a different latest location claim for the same node i. When a node finds a collision (2 different claims with same ID), It broadcasts the two conflicting claims as evidence to revoke the replicas.

iv. MASAD (Mobile Agent Based Sink Hole Attack Detection) Algorithm

This algorithm is used for routing the data by avoiding the sink hole attack. The node's information matrix can be acquired through mobile agent routing algorithm. When the data packets wanted to be sent to node B, it can be transmitted by the MASAD algorithm according to node A's information matrix.

Suppose node A is the source node, node B is the destination node. Communicating with node B, node A performs as follows: (here TabVal AB refers the cell in Ath row and Bth column)

Step1: Examine TabVal AB of A's matrix. If TabVal AB is not equal to 0 (has a non zero value), there is a connection between A and B. The data packets are sent to B directly . End routing. Otherwise, go to step2.

Step2: check the column, B , in the cache of node B, and find out all the items which are not equal to zero in B , these items are the child nodes of node B;

If TabValB != 0 for node1 to node n where n can be 1 to max number of nodes present in the network.

So, node1 to node n are child nodes of B. If all the items in B are equal to zero, then, there is no valid route between node A and nod B, and the routing ends.

Step3: Set the maximum number of hops to reach the destination as n.

Step4: Initialize k =1. Where k = current number of hops.(After finding child nodes of node1 to node n , will be incremented by one. k can reach upto n.) This process continues till it reaches to A.

Here maximum repeated hop with less weight is selected every time. i.e., Maximum agent counter value with less TabVal AB For every neighboring nodes A & B. It limits the chance of paths containing sink hole.

III. CONCLUSION AND FUTURE WORK

In this paper we propose a mobile agent based approach make node locations be learnt by other nodes with very less communication overhead. Also this approach is used to provide necessary knowledge to every sensor node in a Wireless Sensor Network not to believe the false path so that sink hole attack can be avoided at certain extent. The performance of the proposed approach has been examined through simulations.

As well as we can examine the node replication attacks and Sybil attacks and find the measure against them as these are also defined malicious attack to sensor networks in future work.

REFERENCES

[1] I.F. Akyildiz , et al., "A Survey on Sensor Networks," *IEEE Communications Magazine,* vol. 40, no. 8 ,pp. 102-114, 2002.

[2] Akyildiz I.F., W. Su*, Sankarasubramaniam Y., E. Cayirci, " Wireless sensor networks: a survey", *Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology* Atlanta, GA 30332, USA ,Received 12 December 2001; accepted 20 December 2001.

[3] Ashish Kumar Srivastava1 and Aditya Goel2 , " 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, ISSN: 2047-0037.

[4] D.Sheela, Srividhya.V.R, Vrushali, Amrithavarshini and Jayashubha J.," 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. Published:March 2012.

[5] Eric Sabbah, Adnan Majeed, Kyoung-Don Kang, Ke Liu, and Nael Abu-Ghazaleh , "An Application-Driven Perspective on Wireless Sensor Network Security*" Q2SWinet'06,* October 2, 2006, Torremolinos, Malaga, Spain. Copyright 2006 ACM 1-59593-486.

[6] Abdulrahman Hijazi, "Using Mobile Agents for Intrusion Detection in Wireless Ad Hoc Networks‖, WOCN", *Second IFIP International Conference,* pp. 362-366, June 2005.

[7] Zhang Yuyong, Jingde.," Mobile Agent Technology" , Beijing, Tsinghua University Press, 2003

[8] Saleh Kassem,Anwar ul jwari,"total system assurance system",IJCA special issue on *wireless information networks and business information system"WINBIS,*2011.

[9] Adrian Perrig, John Stankovic, And David Wagner , "SecurityIn Wireless Sensor Networks" COMMUNICATIONS OF THE ACM June 2004/Vol. 47, No. 6 pp53-57.

[10] D.B lange and M.Oshima , "Seven good reasons for mobile agent", *Communication of the ACM* vol.42.no3 pp88-89 2001.

[11] S.Poornima and B.B.Amberker, "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.

[12] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou , "Sensor Network Security: A Survey ", *IEEE Communications Surveys & Tutorials*, Vol. 11, No. 2, Second Quarter 2009.

[13] C.L. Fok, G.C. Roman, and C. Lu, "Mobile Agent Middleware forSensor Networks: An Application Case Study*",. Proceedings of the 4th International Conference on Information Processing in Sensor Networks (IPSN'05), IEEE Press*, 2005, pp. 382-387.

[14] S. Ganeriwal, S. Capkun, C.-C. Han, and M. Srivastava,, "Secure time synchronization service for sensor networks*", In Proceedings of the 4th ACM workshop on Wireless security (WiSe '05),* 2005, pp. 97–106.

[15] E. Shi and A. Perrig, "Designing secure sensor networks", *IEEE Wireless Communications, vol.* 11, no. 6, pp. 38–43, December 2004.

[16] C.L. Fok, G.C. Roman, and C. Lu, "Mobile Agent Middleware forSensor Networks: An Application Case Study", *Proceedings of the 4th International Conference on Information Processing in Sensor Networks (IPSN'05), IEEE Press*, 2005, pp. 382-387.

[17] T. Li, "Security map of sensor network,", *Infocomm Security Department, Institute for Infocomm Research, Tech.* Rep., 2005.