ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Mobile Agent Key Distribution in Wireless Sensor Network-A Review

Femi P.M[1], R.Rajendran[2]

M.Tech Student, Department of School of Computer Science, Mahatma Gandhi University, Kottayam, Kerala, India[1]

Reader, Department of Computer Science, School of Technological and Applied Science, Kottayam, Kerala, India[2]

ABSTRACT: Key distribution is the most important cryptographic primitive in wireless sensor network where security is a concern. In terms of security in WSN, Authentication and pair wise key establishment are playing Crucial roles. The aim of this study is to review the mobile agent based key distribution in wireless sensor network in relation with communication overhead, memory overhead, scalability and establishing security.

KEYWORDS: Wireless sensor network, Mobile Agents,Key distribution.

I. INTRODUCTION

A wireless sensor network consists of large number of low cost, low power multi-functional sensor nodes which are distributed in a certain area. Nodes which are very small in size made up of sensing, data processing and communicating components. It is obvious that Security is the significant factor in modern computing world. It must be true with Wireless Sensor Network (WSN) which is resource hungry. Moreover such networks run in hostile environment. As low-cost sensor networks became ubiquitous and used in different real world applications, it became indispensable to have secure key distribution mechanism[10][11] [12]in place. WSN have many applications in various fields including military [1], environmental, health, industry, data collection in hazardous environments and all of these applications require secure communications. Wireless networks are easier to attacks than wired networks because of the broadcast nature of transmission medium, resource limitation on sensor nodes and uncontrolled environments where they are left unattended .Sybil attacks [2], black hole attacks, DOS attacks, wormhole attacks are examples of such intrusions. The significance of using mobile agent in communication networks is to ensure dissemination of data or collection of data efficiently. The concept of Mobile Agent is [3] a software agent that can be transported to a remote node for execution, it will be called a mobile agent. Mobile agents can reduce the bandwidth consumption and path discovery by preceding the data at the source and sending only the proper results. The main difference between a mobile Agent and non-mobile Agent is the capacity of mobile agent to transfer its function to execute in remote elements. The main characteristics of mobile agent are

Autonomy: The agent must be able to operate without external intervention and control its action and its state.

Proactivity: The agent must be able to anticipate future situation, reaction appropriately in relation to established rules and policies.

Mobility: a mobile agent must be able to transfer itself to remote entities and continue its execution from its stopping point.

Dynamic adaptation:mobile agents can monitor the environment and react to change autonomously.Because of this they can adapt their future behaviour to information to retrieved.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Fault tolerance:mobile agent operation must continue,even when a communication break occurs,making remote communication impossible.The agent can wait until the connection is back migrating if necessary.

II. RELATED WORK

1.K. Shaila and S.H. Manjula et al.[4] In this paper using single encryption validation and doble encryption validation for the communication between nodes and the authentication of mobile nodes and has several advantage for increasing the security in communication.Here Consider all the sensors have equal capacity interms of memory, battery and processing power Compared with the normal nodes, mobile node has the different features such as large memory,extra energy,processing power. The availability of a mobile node is increased dynamically by changing its speed and the number of communications increased by introducing the session time. Two shared keys used for encrypting the data makes the data more secure. They prove a novel algorithm that provides robust and secure communication channel in WSNs. Double Encryption with Validation Time (DEV) using Key Management Protocol algorithm works on the basis of timed sessions within which a secure secret key remains valid. A mobile node is used to bootstrap and exchange secure keys among communicating pairs of nodes.Their simulation results show the performance of this scheme has better performance in both availability of a mobile node as well as in increasing the number of communications between the nodes and also increase the scalability of nodes in wireless sensor network.For implementation they are used a ns2.31 simulator in fedora 10.

2.Neeraj Nehra et al.[5] have implemented different agents for communication in wireless sensor network.Agent Manager- This is used to control the agent taken in Mobile agent secure location key establishment(MASLKE). The different agents selected in MASLKE,which are Location Calculation Agent (LCA), Set up Phase Agent (SPA) and Key establishment Agent (KEA). Each agent executes the predefined policy defined in MASLKE. LCA executes the location calculation algorithm in initial phase. This algorithm is used to find the location of nodes for which key establishment has to be made, i.e., base station, ClusterHeads and mobile nodes. SPA executes the two phased algorithm for set up before the procedure for key establishment begins. Finally KEA executes the algorithm for pairwise key establishment on nodes. Policy Manager- This is used to control the policies associated with the agents. It controls the policy structure and frequency of policy to be executed by the respective agent. The different policies selected in MASLKE are- key-location calculation, join and leave and key establishment.Agent Execution environment- To control the movement of agents in WSN, Platform for Mobile Agent Distribution and Execution (PMADE) is included in the architecture.

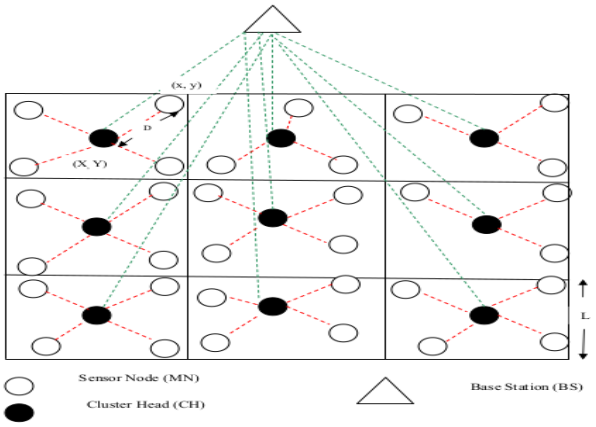

Fig1. Arrangment of bases station and nodes in MALSKE

PMADE provides various types of itinerary for MAs and their associated security and fault tolerance issues . Agent-agent communication Layers- There are various layers included in the architecture for MAs operations using mobile group approach . The design of MASLKE is agent based mechanism on large- scale sensor networks with resource

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

constraints. In this scheme, MA executes the algorithm for location calculation. Only cluster head sensors are in charge of key generation and distribution, which help to conserve resources in normal sensors. A distinctive feature of MASLKE is that location information is determined by MAs. Simulation study indicates that MASLKE has a good performance in terms of key-sharing between neighboring sensors, Success ratio, communication overhead and resilience against node capture.

3 .Ozgur Koray Sahingoz proposes a unmaned arial vehicle[6] used for public key distribution agent in the number of wireless sensor nodes. For example number of nodes distributed in the certain area
.• consider 2 nodes in the WSN system.They are node A and node B
• MCA(UAV) is the mobile certification authority .it is used as a key distribution center.
• K_{AB} is the communication pairwise keys between nodes A and B
• {M} Pub_A indicates encryption of message M with Public Key of node A

Setting up a symmetric key cryptography with usage of public keys of the neighbor nodes by asymmetric key cryptography is achieved with the following key agreement protocol:

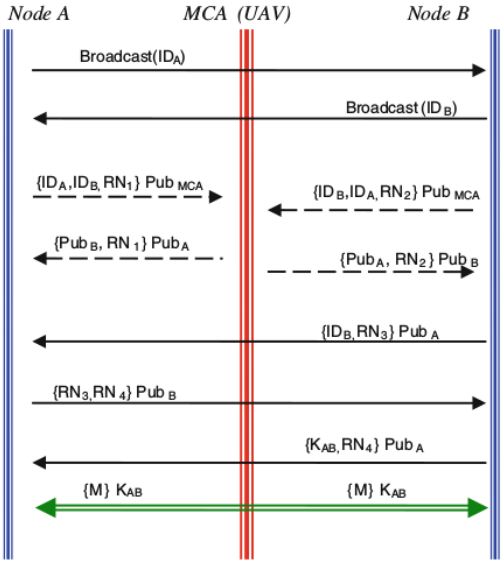

Fig 2. Key distribution and encryption model of the system

Step 1:A sensor node A broadcast its id (ID_A) to all of the neighbours including node B

Step 2:All the neighbours of node A should obtain a public key of node A from the key distribution center.

step 3:Node B uses public key of node A to encrypt messages which contain its identifier (ID_B) and a random number (RN_1), which is used to identify this transaction.

Step 4:Node A sends a message to Node B encrypted with Pub_B and containing B's random number (RN_1) as well as a new random number generated by Node A (RN_1)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

step 5:Node B selects a secret key K_{AB} and returns this and RN_2, which are encrypted using Pub_A , to assure A that its correspondent is B.

step 6:Both communicating parties establish a secret key for their communication.

Their simulation result show the system is scalable, and its performance is considerably better than single asymmetric key management systems.For transferring id and random numbers ,it uses a asymmetric key cryptography and after selecting secret key it uses a symmetric key cryptography.so this system has given a more security than other systems.Mobile agent is used for distributing public keys.So there is no possibility of trusted server attack.

4.Ramu Kuchipudi et.al [7]The proposed dynamic and hybrid key management scheme. Each sensor node stored their private key and public key of mobile agent (MA). After distribution of sensor nodes secure communication is take place. To achieve a secure communication , a node needs to know the ID of other node. A sender node gets IDs of other nodes and executes the key distribution algorithm. Figure 3 illustrates the operations involved in secure key distribution.

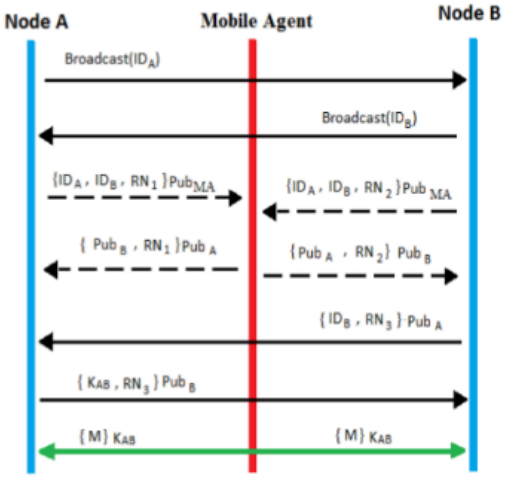

Fig 3. Secure key distribution model

consider 2 nodes in the wireless sensor network are ready to communicate,Node A and Node B

• Mobile agent is a mobile node within an ad hoc network, and it is selected to provide

distributed key management center's functionality

• K_{AB} is the communication pairwise keys between nodes A and B

• {M} Pub_A denotes the encryption of message M with Public Key of node A

Step 1 : A sensor node (Node A) broadcast its id to all of the neighboring nodes.

step 2: Each neighbor (Node B and others) should obtain the Public Key of Node A from Mobile Agent

step 3: Node B uses Node A's public key to encrypt messages which contain its identifier (ID B) and a random number (RN 1), which is used to identify this transaction

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

step 4:Node A sends a secret key and also a random number of neighbor B which is encrypted by public key of B denoted as Pub_B.

This work is close to the work of Sahingoz [6] who proposed multi-level dynamic key management scheme for Wireless sensor network where UA V is the mobile certification authority used to distribute public keys. This paper proposed a key distribution scheme that makes use of mobile agents instead of Unmaned Arial Vehicle for public key distribution. Here a mobile agent manager is used for control the mobile agents.This key distribution can implemented in the large wireless sensor network.Cluster head sensors are in charge of key generation and key distribution.Mobile agents are distibutors of public key. It reduces communication overhead, memory overhead and computational overhead. Besides, it is resilient against node capture attacks.

5.Lijn Gao et al. Here mobile sink node is represented as a data collector [8]in wireless sensor network.It is used for collecting data from any time ,anywhere in the wireless sensor network. In this paper they classify the existing data collection methods according to mobile sensor network structure.Wireless sensor networks provide a new platform for distributed information processing and computing models, which combined the natural world and human organically. They summarize the existing data collection protocol of mobile sink type network. protocols and algorithms can be avoid the the botteleneck problem in the wireless sensor network while the time of mobile data collection. However, data aggregation rate is largely restricted by the moving speed and course of mobile node.

6.Pardeep Kumar et al.[9] for giving a security in wireless sensor network ,they take an another apporoach using mobile agents.Here also mobile agent should visit all the sensor nodes within its broadcasting range. Symmetric key cryptography approach is used for key distribution.

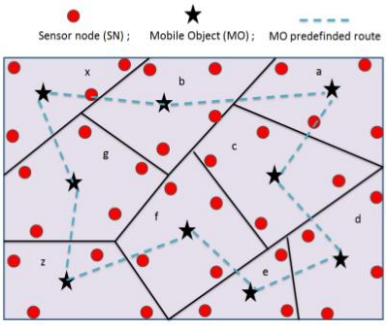

Fig 4.Wireless sensor network is divided into N cells(eg:a,b,c..)

Here wireless sensor network region is divided into voronoi cells. Mobile agent is visits to the wireless sensor networks and collects the sensor data. The aim of mobile agents is to distribute the new secret keys (for every i th visit) to the sensor nodes and collect the sensed data from each nodes. In mobile agent moving to route through the center of the Voronoi cells. Also it detect the misbehavior of malicious nodes or compromised key and also it revoke them. For the security purposes, They consider that nodes in one cell cannot directly communicate with the other cells nodes.So They can attain high efficiency in computation and communication cost and also provides strong security.

III. CONCLUSION

All reviewed papers recommend some different ideas of strengthening WSNs security using strengths of the Mobile Agent technology. Lot of key distribution protocols are used for giving security in wireless sensor network.Here I focused on strength of mobile agent while giving security in WSN.Some of the papers using only symmetric key cryptography for giving security, also they consider computation and communication cost. Some paper targeting

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

energy consumption using the characteristics of the mobile agent while collecting data from the wireless sensor network. Others try to take the advantages of both asymmetric and symmetric key cryptography for the security purpose.So they can reduce the diffferent existing problems in wireless sensor network.

REFERENCES

[1] A. Rasheed and R. Mahapatra, "A Key Pre-Distribution Scheme for Heterogeneous sensor networks",Proc. Int'l Conf. Wireless Comm. And Mobile computing Conf. (IWCMC '09), pp. 263-268, June 2009.
[2] Lai B, Kim S, Verbauwhede I, "Scalable session key construction protocol for wireless sensor networks" In: Proceedings of the IEEE workshop on Large Scale Real-time and Embedded Systems LARTES, December 2002.
[3] Houda labled, "wireless adhoc and sensor networks " chapter 11 ,wireless adhoc and sensor networks .
[4] K. Shaila and S.H. Manjula, K.R. Venugopal,L.M. Patnaik,"Mobile node authentication using key distribution scheme in wireless sensor networks"Int. J. Ad Hoc and Ubiquitous Computing, Vol. 12, No. 1, 2013
[5] Neeraj Nehra, R.B.Patel, "MASLKE: Mobile Agent Based Secure Location Aware Key Establishment in Sensor Networks",IEEE Transactions On Image Processing, vol. 9, No. 11, 2000.
[6] Ozgur Koray Sahingoz "Multi-Level Dynamic Key Managementfor Scalable Wireless Sensor Networks with UAV", Springer Science+Business Media Dordrecht 2013.
[7] Ramu Kuchipudi,Dr. Ahmed Abdul Moiz Qyser,Dr. V .V. S. S. S Balaram,"A Dynamic Key Distribution in Wireless Sensor Networks with reduced communication overhead",International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) - 2016
[8] Lijn Gao , Hang Yin , Yuhua Wei , Le Wang ,"Data Collection Methods Based on Mobile Sink Node",International Conference on Advances in Mechanical Engineering and Industrial Informatics (AMEII 2015)
[9] Pardeep Kumar , Pawani Porambage, Mika Ylianttila , Andrei Gurtov, "A Mobile Object-based Secret Key Distribution Scheme for Wireless Sensor Networks",2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing .
[10] Koduri Kavya , M .V. Dilip Kumar,"A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks",International Journal of Emerging Engineering Research and Technology Volume 2, Issue 8, November 2014, PP 18-23.
[11] Snehal M. Gaikwad, Vidhya Dhamdhere,"A Pairwise and Triple Key Distribution with Homomorphic Cryptography in Wireless Sensor Network",International Journal of Innovative Multidisciplinary Research Academy Volume-1, Issue-1 January 2015.
[12] D. Dhayalan & Nandhini. S. "Certificate less Effective Key Management in Dynamic Wireless Sensor Network",Imperial Journal of Interdisciplinary Research (IJIR) Vol-2, Issue-4, 2016 ISSN: 2454-1362.