SECURITY SOLUTION for WSN USING MOBILE AGENT TECHNOLOGY

Ashish Kumar Srivastava [#1], Aditya Goel [*2]

[#]*Research Scholar Department of Information technology, MANIT Bhopal, India*

[*]*Associate Professor Department of Electronics engineering, MANIT Bhopal, India*

***Abstract*— Wireless sensor network (WSN) have diverse field of application, but it is very much prone to the security threats. The different types of security attack which limits its application in various unsecure environments are sink Hole Attack, Sybil attack, wormhole attack, node replication attack etc. Any security measures need to provide four basic requirements that are Confidentiality, Integrity, Authentication and Availability (CIAA). This paper focuses on the study of security threats to the WSN and based on that threats paper proposes a novel security solution using a mobile agent technology. The mobile agent-based technique allows WSN applications to exhibit self-healing, self-configuration and self-optimization and programmability properties. "One deployment multiple applications" is an emerging trend in the development of WSNs.**

***Keywords*— WSN, mobile Agent, WSN Security.**

I. INTRODUCTION

Sensor network predict a future in which thousands of sensor nodes will be embed in almost every aspect of life [1]. The objective is to create an intelligent environment which is sufficient to collect considerable amounts of important information, acknowledging critical events automatically, and reacting correctly, though military applications are the most apparent, sensor networks having potential in a broad range of areas. Typical applications include disaster relief applications, environment control and biodiversity mapping, emergency response information system, machine surveillance and preventive maintenance, medical monitoring energy management, inventory control, and battlefield management [2]. If sensor networks have to achieve their potential, the secure communication techniques must be applied in order to guard the system. Security requirement in military applications is apparent, but even more application uses, such as home health monitoring, require confidentiality and authentication. WSNs are ideal for observing chemical, biological, or environmental threats over large arenas, but maliciously generated fake alarms could completely challenge the result of the system. So we can say that depending on the application, security can be vital [3]. The widespread deployment and success of sensor networks is directly associated with the security strength of WSN. In communication systems, security persist one of the most important challenges, principally as private or susceptible information becomes more widely available. Conventional security methods cannot be directly applied to WSN as the inherent constraints of sensors devices prohibit computationally intensive algorithms. New approaches, therefore, need to be implemented. Furthermore; WSNs experience vastly different challenges than large-scale wired networks. Eavesdropping is as easy as turning on a radio receiver, while message packets are often implemented as extremely small and simple structures. The lives of soldiers on a battlefield depend on a wireless security that can combine real time accessibility with sufficient privacy. Tradeoffs between power consumption and complexity yield a great range of possible protocols, at times leaving appropriate choices obscured. Without a doubt security schemes optimized for wireless sensor networks have not been fully developed. In this paper we present a novel security solution based on mobile agent technology that fits the demands and restrictions of WSNs. The flexibility and efficiency of mobile agents offer several advantages when used in distributed intrusion detection systems (IDSs). Mobile agents are software entities which can function autonomously in a particular environment. They are able to carry out some activities in a flexible and intelligent manner. They can migrate from one node to another, learn, and collaborate with other agents. These agents are sent to some key network nodes to collect, process, and analyse suspicious data and anomalous behaviours. Agents in different nodes can exchange their data and collaborate mutually to detect distributed attacks [4]. Because agents can be deployed to other nodes to collect and process data, the network load is reduced and balanced effectively. To reduce bandwidth consumption by moving the data processing elements to the location of the sensed data, these transmissions would incur most of the energy expenditures of the nodes [5]. In practice, several other WSN issues, such as secure routing and secure data fusion can be effectively tackled by mobile agent systems. Mobile agent middleware gives the solution for this problem. MA provides dynamic reprogramming of WSNs by injecting new agents where old agents die. Mobile agent middleware support adaptability and mobility [6]. In total this research paper, provides a brief review of existing security techniques for WSN and suggest some novel security technique for WSN using agent based technology.

2. LITERATURE SURVEY

The different directions of progressing research in wireless sensor network are based on security challenges that cover various classes of security attacks and how sensor networks can defend against those attacks. Another, way to address security in wireless sensor network can be on a per-layer basis, in lieu a per-attack basis. Under this consideration, cryptographic protocols can be designed to provide security in a particular layer and cooperate with cryptographic protocols in other layers to accomplish defense for the nodes and the network. This layer based categorization of security protocols can assist towards a clearer realizing of WSN security and better protocol design. However, in practical sensor networks protocol design, such when implementing in TinyOS platform, there does not exist a clear schematic way for separating the various layers. Nevertheless, one could break the wireless sensor network stack in TinyOS into four major different layers: the physical layer, the link/MAC layer, the routing layer, and the application layer. On this foundation we could range security protocols in a corresponding layered taxonomy, as shown in Figure1.1 [7]. Protocols in upper layers use security services provided by lower layers or are contingent on their reliable functionality. There are also other security emergences like intrusion detection that cannot be separated in this layered based approach as they are more general problems that spam different layers.

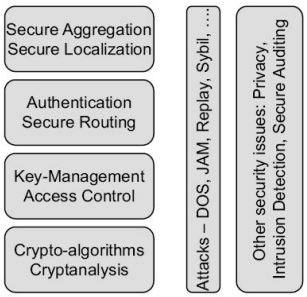

Figure2.1 Sensor networks security map based on a layered approach.

2.1. Category of security solution

Currently, research on security solutions for WSNs has focused mainly in the following three categories:

- ***Key management****:*

A lot of work has been done [8] in establishing cryptographic keys between nodes to enable encryption and authentication. These protocols can be categorized as link layer protocols.

- ***Authentication and Secure Routing:***

Several protocols [9] have been proposed to protect information from being revealed to an unauthorized party and guarantee its integral delivery to the base station. These protocols works at routing layer.

- ***Secure services****:*

Certain progress has been made in providing specialized secure services, like secure localization [10], secure aggregation [11] and secure time synchronization [12]. These services work at application layer.

2.2. *Types of Attack on WSN*

There are various types of attack in WSN. Some of them are explained as follows [13]:

- ***Sinkhole Attack***

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.

- ***Wormhole Attack***

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.

- ***Sybil Attack***

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.

- ***Node Replication Attacks***

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.

3. PROPOSED SECURITY SOLUTION

Our proposed model is purely based on the four basic requirements for the WSN security that are Confidentiality, Integrity, Authentication and Availability (CIAA). Till now we could able to develop model for security solutions of two basic requirements that are confidentiality, Integrity. Hence our security model is divided as follows:

3.1 *Agent based Confidentiality maintenance model for WSN.*

Confidentiality is the property of protecting the content or information all users other than those intended by the legal owner of the information. In WSN the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security. Confidentiality in sensor networks can be defined as:

- A sensor node should not reveal its data to the neighbors. For example, in a sensitive military application where an adversary has injected some malicious nodes into the network, confidentiality will prevent them from gaining access to information regarding other nodes.

- Establishing and maintaining confidentiality is extremely important when node identities and keys are being distributed to establish a secure communication channel among sensor nodes.

As per the literature the current security concern is key management technique in WSN, some of the researcher have developed a key management and authentication technique for ad hoc network [18] to maintain confidentiality in communication. We tried to propose a software mobile agent based key management technique as shown in fig2.1.

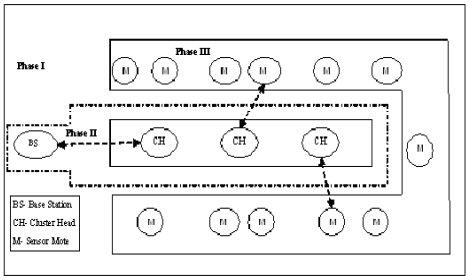

Fig 3.1 : Agent based Confidentiality protection model for WSN

Our proposed model is having three phases they are Initial Key distribution phase, Control phase and Execution phase. With the help of mobile agent (MA) our proposed scheme modify existed keys randomly in any time for different kind of sensor data and control information.

- ***Phase I: Initial Key Distribution***

This phase is completed before the deployment of the motes in the WSN. The Base Station (BS) generates a key range for each motes (***Mi***) elliptic curve (***E***). For each Mi, E is defined over a function ***fIDm (x)*** where x is the base field characteristic ***IDm*** is mote's identification [14, 15]. The initial key distribution of the key range is performed before the deployment of the motes in the WSN, so the computation and communication cost will be minimum.

- ***Phase II : Control phase***

This phase starts after deployment of motes in the WSN, where each mote decides their Cluster head (CH). Each CH is assigned a point P generated by BS from the elliptic curve polynomial [15]. After receiving the point, the CH broadcast it to its cluster member motes. Now all the motes in that cluster use this point and compute cluster key ***Kch*** by applying it to key range To update the cluster key, the BS selects a new point ***P'*** from the elliptic curve which is associated with the polynomial of that. As the BS directly communicates with the CHs, it sends the new point. After that CHs broadcast their new point to their cluster regions. The motes compute the new cluster key ***K'ch*** using ***P'***.

$$K'ch = P' + fIDm\ (x). \qquad (1)$$

- ***Phase III : Execution Phase***

In this phase, the different sort of data are identified, decrypted and communicated with BS according to need. Almost all existing key distribution schemes are depend upon the number of sensor motes and degree of their connectivity in a WSN. Our proposed model is free from these constraints which make it more reliable, secure, and flexible from other existing key distribution schemes.

3.2 Agent based Integrity maintenance model for WSN.

Integrity is a property of protecting information from alteration by unauthorized users. Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed while on the network. Even if the network has confidentiality measures in place, there is still a possibility that the data's integrity has been compromised by alterations. Some of the researchers have proposed and innovative agent Based Secure data collection in

heterogeneous sensor networks but the integrity of the network is always being in question if:

- A malicious node present in the network injects bogus data.
- Disruptive conditions due to wireless channel cause damage or loss of data.

The proposed model for data integrity check in WSN using agent based technology is elaborated in fig3.2.1.

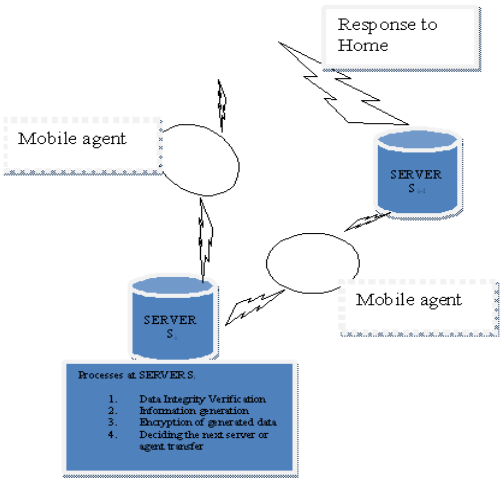

Fig3.2. Agent based Integrity maintenance model for WSN

- ***Agent at the Creator (S0):***

The creator or owner creates and starts the agent with the dummy offer o_0 (to check from the return agent whether this item is modified or not) and random number r_0. Also it has to sign the dummy offer $Sig_{pr0}(o_0)$ with private key Pr^0 for non-repudiation purposes and to encrypt those data for confidentiality Enc_{Pb0} $(Sig_{pr0}(o_0), r_0)$ with the help of the public key Pb_0 and forward it to the succeeding host S_1 . It also generates the temporary public and private key (tPb_0, tPr_0) to sign the identity of the next host Sig_{tpr0} *(S1).*

$$S_0 \rightarrow S_1: O_0 \qquad (2)$$

The hash function is applied to the encrypted identity, temporary public key and random number to identify the man in the middle attack. Every host in the network should have the public key of the other hosts. Finally, the agent originator S_0 signs the final encapsulated offer with its private key $Pr_0$and sends its encapsulated offer (O_0) to the next selected host S_1 with the agent.

- ***Agent at host or server (S1):***

The agent from S_0 migrates to S_1 with the encapsulated offer O_0. After receiving the encapsulated offer, S_1 has to verify it for integrity and authenticity. The encapsulated offer is unveiled using the public key Pb_0.The identity of S_1 is recovered by tPb_0 and the S_0 is recovered by Pb_0; then, the identity sequence is verified from the initial offer O_0. In general, the first remote host has nothing to verify in the identity sequence but it has to check whether the identity of the current server is encapsulated in the protected offer or not.

$$S_1 \rightarrow S_2: O_0, O_1, tPb_1 \qquad (3)$$

The S_1 will generate its offer o_1 and random number r_1 and then compute C_1 with the public key of originator Pb_0. Next, it has to encrypt the next server identity and the temporary public key of the previous server using the temporary public key $(Sig_{tpr1}(S_2, tPb_0), tPb_1, r_0)$ and append with the preceding server's last two identities $Sig_{pr0}(S_0)$, $Sig_{tpr0}(S_1)$ as $Sig_{pr0}(S_0)$, $Sig_{tpr0}(S_1)$,$Sig_{tpr1}(S_2, tPb_0)$, tPb_1, r_0 . Then it has to decide on the next server to dispatch the mobile agent. Finally, S_1computes $O_1 = Sig_{tPr1}(C_1, vh_1)$ and appends it with the preceding server's encapsulated offer and dispatches to the succeeding server S_2. This process of verification and computation will continue until the agent is back to its home with the required information or offer by the owner.

- **Agent returns to home S0**

Finally, the agent returns to its home and gives the collected offers to its owner. The owner will recover all the encapsulated offers $O_0, O_1, , O_2, , O_3, \ldots O_{i-1}, O_i , O_{i+1}, \ldots O_n$ with the help of the temporary public key of every host. Where O_n is recovered by the tPb_n and then O_{n-1} is recovered with the help of the tPb_{n-1}, which is available in the hash function of the encapsulated offer O_n. After the verification of the integrity, the agent owner will recover the offers ***offers*** $o_0, o_1, , o_2, , o_3, \ldots o_{i-1}, o_i , o_{i+1}, \ldots o_n$ on using the public key of the equivalent host and make use of it to check the integrity.

TABLE 3.1: COMPARISON BETWEEN MOBILE AGENT BASED SECURITY MODEL FOR WSN AND TRADITIONAL APPROACHES.

Comparison Parameters	Proposed Model	Traditional Approaches [24]				
		Eschenauer and Gligor	Du, Deng, Han and Varshney	SHELL	LEAP	PANJA
network load	Reduce	Reduce	High	Average	Average	Average
network latency	Reduce	Reduce	High	Average	Average	Average
authentication	No	No	Yes	Yes	Yes	Yes
Complexity	less	Less	High	High	Medium	Not
Scalability	Yes	Yes	Not	Average	Medium	High
adapt dynamically	Yes	NO	No	Average	No	Yes
collaborative operations	Yes	Yes	No	Yes	No	Yes
robust and fault-tolerant	Yes	Yes	Yes	Yes	No	NO

4. CONCLUSION AND FUTURE WORK

Today security based research and applications of WSN have attracted people's attention. But inbuilt characteristics of sensor nodes, such as inadequate communication and computing capacity, constrained power energy and storage space, the security solutions for WSN become difficult. In this paper, we studied the various security requirement of WSN and based on it we tried to propose a novel security solution by using mobile agent technology. We have proposed Agent based Confidentiality maintenance model for WSN and Agent based Integrity maintenance model for WSN Finally, we compared some basic parameters of both the proposed model and traditional approaches and we find that the proposed model can provide better security solution and enhance WSN utility for various applications. Our conclusion is that the new proposed mechanism is especially suitable for Wireless Sensor Network. In future we are trying to practically implement the proposed security models and develop some other security model based on agent based technology Such as security model of SPAM detection, security model for Authentication using agent based technology.

REFERENCES

1. I.F. Akyildiz , et al., *"A Survey on Sensor Networks,"* IEEE Communications Magazine, vol. 40, no. 8 ,pp. 102-114, 2002.
2. Eric Sabbah, Adnan Majeed, Kyoung-Don Kang, Ke Liu, and Nael Abu-Ghazaleh *"An Application-Driven Perspective on Wireless SensorNetwork Security" Q2SWinet'06*, October 2, 2006, Torremolinos, Malaga, Spain. Copyright 2006 ACM 1-59593-486.
3. Adrian Perrig, John Stankovic, And David Wagner *"SecurityIn Wireless Sensor Networks"* COMMUNICATIONS OF THE ACM June 2004/Vol. 47, No. 6 pp53-57.
4. Abdulrahman Hijazi, "*Using Mobile Agents for Intrusion Detection in Wireless Ad Hoc Networks*", WOCN, Second IFIP International Conference, pp. 362-366, June 2005.
5. D.B lange and M.Oshima *"Seven good reasons for mobile agent"* Communication of the ACM vol.42.no3 pp88-89 2001.
6. 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.
7. T. Li, *"Security map of sensor network,"* Infocomm Security Department, Institute for Infocomm Research, Tech. Rep., 2005.
8. S. Camtepe and B. Yener, *"Key distribution mechanisms for wireless sensor networks: a survey,"* Rensselaer Polytechnic Institute, Troy, New York, Technical Report 05-07, March 2005.
9. E. Shi and A. Perrig, *"Designing secure sensor networks,"* IEEE Wireless Communications, vol. 11, no. 6, pp. 38–43, December 2004.
10. L. Lazos and R. Poovendran, *"SeRLoc: Robust localization for wireless sensor networks,"* ACM Transactions on Sensor Networks, vol. 1, no. 1, pp. 73–100, 2005.
11. T. Dimitriou and I. Krontiris, *Security in Sensor Networks*. CRC Press, 2006, ch. Secure In-network Processing in Sensor Networks, pp. 275–290.
12. 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.
13. 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
14. Hankerson, D.,Hernandez, L. J., and Menezes *A. Software implementation of elliptic curve cryptography over binary fields*, CHESS 2000,LNCS 1965, 1-24,2000.
15. D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer, 2004.
16. I.F. Akyildiz , et al., "*A Survey on Sensor Networks*," IEEE Communications Magazine, vol. 40, no. 8 ,pp. 102-114, 2002.
17. Blumenthal J, et al., "*Wireless sensor networks—New challenges in software engineering*", IEEE, pp. 551–556, 2003.
18. ZHANG Yi and ZHU Lina and FENG Li "*Key Management and Authentication in Ad Hoc Network based on Mobile Agent*" Journal of Networks, Vol. 4, No. 6, August 2009.
19. 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.
20. Johnson C. Lee And Victor C. M. Leung, University Of British Columbiakirk H. Wong, Jiannong Cao, And Henry C. B. Chan,Hong Kong Polytechnic University *Key Management Issues In Wireless Sensor Networks:Current Proposals And Future Developments* IEEE Wireless Communications October 2007.pp76-84