TMW - Time-Endorsement by Mobile Agent in Wireless Sensor Network

Ambika.N
Dayananda Sagar College of Engg, Bangalore
Student of Bharatiar University, Coimbatore.
ambika.nagaraj76@gmail.com

Dr.G.T.Raju
RNSIT, Bangalore.
drgtraju_rnsit@yahoo.com

ABSTRACT
Wireless sensor network is an area where there has been a lot of significant developments. These sensors are hugely utilized in many applications like military applications, home automation, and environment surveillance. An application where confidential data is being transmitted requires to be protected from different types of attacks. Though the nodes are authenticated, they are liable to get compromised. The nodes may get compromised by the adversaries and may leak out confidential information. These sensors are subjected to different types of attacks like wormhole attack, Sybil attack, Denial-of-service attack and sinkhole attack. Depending on the type of application utilized level of security can be implemented. This paper utilizes the mobile agent to distribute secret key utilizing one-time pad algorithm. The encryption key hence varies from one cluster to another. To add additional security, comparison is done between the time of dispatch sent by cluster head and monitor nodes.

General Terms
Algorithm, Performance

Keywords
Wireless security, Wireless sensor network, Intrusion prevention technique

1. INTRODUCTION
Wireless sensor network [1,2] has made a lot of progress in short time. These sensors are utilized to monitor, sense and track the object of interest. The readings are noted at regular interval of time or when an event occurs depending on the application, where it is deployed. These sensor networks are utilized in innumerable applications [3-6] like habitat and environmental monitoring, health care, military and industry machinery surveillance, home automation etc. As these devices are application specific, same sort of security may not be cost-effective and at the same time may not serve the purpose. Though the transmitted data is confidential, the level of confidentiality is application specific.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Copyright ©2011 IIJ: The Research Bulletin of Jordan ACM - ISWSA; ISSN: 2078-7952 (print); 2078-7960 (online)

Every node in the network has a set of programs related to its activities to perform. Hence the network needs to be protected from adversaries. The network can be made secure in two ways. One of them being, by utilizing one of the preventive techniques. Intrusion prevention system is a device that monitors different types of threats, tries to block or stop such an activity and reports activity. Deploying a firewall, encryption, authentication are some of the intrusion prevention techniques. Secondly, one of the detection techniques designed to monitor the violation of security policy, generate the report and disperse the report to the base station can be utilized.

This paper utilizes the encryption technique to prevent adversaries gaining control over the network. The mobile agent distributes the keys to the cluster heads utilizing one-time pad algorithm. This ensures certain degree of security to the network. To provide additional integrity to the network, monitor nodes are been deployed which provides assurance to the communicated data. The rest of the paper is organized as follows. Section 2 discusses about the related work. Section 3 discusses the system model. Section 4 shows the simulated results. Section 5 gives the conclusion.

2. RELATED WORK
LEACH [7,8] Low-Energy Adaptive Clustering Hierarchy which takes the hierarchical approach and organizes the nodes into clusters. LEACH uses TDMA to achieve communication between nodes and their cluster heads. The cluster head in turn forwards the messages received from its cluster nodes to the base station. LEACH uses a transmitter-based code assignment scheme. Communication between a node and its cluster head are achieved by using direct spread spectrum. The cluster is assigned unique spreading code which is used by all the nodes in the cluster to transmit the data to their cluster head. Spreading codes are assigned to cluster heads on a first-in, first-served basis, starting with the first cluster head to announce its position followed by subsequent cluster heads. The communication between cluster head and a base station is achieved using fixed spreading code and CSMA.

HEED [20] is a cluster based algorithm used in ad-hoc networks. The protocol incurs low overhead in terms of processing cycles and messages are exchanged. It also achieves fairly uniform cluster head distribution across the network. The cluster head is chosen depending on many factors like residual energy in the nodes, their proximity to their neighbors, node degree.

SLEACH [21] utilizes leach concept with an additional feature to withstand the adversaries or the compromised nodes. SLEACH is divided into four phases and fit inexpensive cryptographic operations to each part of the protocol functionality to create an efficient, practical protocol. The algorithm utilizes one-way hash chains and symmetric cryptographic operations to accomplish the purpose.

CLUSMA[22] is a middleware framework for communication between sensor nodes in Wireless sensor network. It is based on...
clustering technique (CLUS) and it uses Mobile Agent. It gives a sketch of the middleware and the actual implementation of the framework is in progress. The main objective of this middleware is to utilize the networks functions and resources in an effective way. The proposed framework is based on mobile agent and hence will work in homogenous as well as heterogeneous environment. The proposed framework will provide security in heterogeneous environment by using mobile agents in a cluster which will communicate with agents in other clusters.

In MASLKE [23] Mobile Agent Based Secure Location aware Key Establishment, mobile agents find the location of sensor nodes and this information is used for key generation and distribution. MASLKE provides secure key exchange in intra and inter domain of the network and achieves high connectivity in WSN.

The paper [24] presents a One-Time Password (OTP) mechanism to provide authentication, with particular application to thin clients in wireless networks. Many of the current OTP mechanisms have high client side computation costs, high communication costs, or limited login times. To cope with these problems, this paper proposes a new one-time password scheme using a smart card. In the scheme, a novel modification to the Depth-First Search (DFS) based on a unique tree structure to generate a private key is presented.

3. SYSTEM MODEL
3.1 Embedding symmetric keys and deploying the nodes

Sensor nodes are deployed in unattended areas. Fig 1 illustrates the deployment of different types of nodes in the network. The keys are embedded along with unique ID before deployment. After deploying the nodes they need to identify each other in order to form a cluster[7,8] to transmit data. These clusters consist of cluster head, cluster members and monitor node. The monitor node is previously chosen and embedded with a different type of encryption key. These monitor nodes are programmed in way that they do not communicate with neither of the nodes but remain in the cluster to monitor other nodes. Every cluster has a monitor node to scrutinize the activity of the cluster.

The cluster members are given its own slot to transmit data. Sending unencrypted data can allow the adversary to collect the details and use it to become a part of the cluster. Hence the data has to be encrypted before it is being transmitted. There are two ways of encrypting data. The symmetric encryption is where the nodes utilize the same key to encrypt and decrypt the data. Public key [12-14] encryption are those that utilizes two keys one to encrypt and other to decrypt the data.

This paper utilizes symmetric encryption [9-11] to encrypt the data. The sensor nodes utilize certain amount of energy to receive and dispatch data. Using symmetric cryptographic keys saves the energy to certain extent. The nodes authenticate themselves by utilizing symmetric keys and join the group. The nodes in the cluster can be static or dynamic by nature. In this paper the nodes in the cluster are static by nature.

3.2 Using mobile agent to authenticate and distribute encryption key

Even after authentication while forming the cluster, the nodes in the cluster are prone to internal attacks. These kinds of attack will not only inject false data but also consume lot of energy. Hence tracking these compromised nodes is very essential. As the confidentiality of transmitted data increases, the attacks are quite often.

Military applications are those where the communication secrecy is a must. Hence encryption key utilized to encrypt the data has to change quite often. The mobile agent is assumed to be tamper resistant and has a timer which is synchronized with the base station. One-time pad algorithm [25] [26] is a type of encryption technique utilized to distribute the keys by the mobile agent. This technique encodes each bit of plain text into encrypted message by performing XOR on the plain text and the secret random key to obtain cipher text.

In this approach, the secret key is chosen depending on the time of authentication. The mobile agent [15-19] authenticates the cluster head. The time of authentication is stored in the cluster head. Utilizing the time of authentication as a parameter, a secret key is chosen from the set of keys stored inside the mobile agent.

This secret key is furnished to the cluster head, which in turn distributes to other cluster members. The node in the cluster encrypts the sensed data by performing XOR on the plain text and secret key resulting in cipher text. This cipher text is transmitted to the cluster head by all the cluster members. The cluster head in turn aggregates all the sensed data sent by other members of the cluster, node ID in the encrypted form. The cluster head attaches the dispatching time and sends the data.

Utilizing mobile agent to store the codes to encrypt the data minimizes the burden on the cluster members in terms of memory and energy consumed to generate the encrypted key. Additionally the secret key distributed to the cluster is random; hence keys are hard to comprehend by the adversaries.

Every cluster has a monitor node, which is primarily deployed to sense the timing of the departing packets from cluster head. The
monitor nodes encrypt the departure time with its ID and forward it to the next hop, not to its own cluster head. All the cluster heads, which forwards the packet, attaches its encrypted ID and departure time. Fig 2 illustrates the working of the algorithm.

### 3.3 Report Generation

After receiving the packets from the network, the base station analyzes the data being received. The base station compares of the departure time obtained from the monitor nodes and cluster head. If the result of comparison made is different, it concludes that the cluster head is compromised. It broadcast these details to the entire network, so that all the nodes put the cluster head into the black list.

Every cluster has a monitor node which maintains a table consisting of the entry of the time of incoming packet and the outgoing packet. This monitor node keeps on discerning the cluster head and the members in the cluster. If it only accepts the incoming packet without dispatching it, it acquaints the base station about the activity. As every node in the cluster is given its own slot to send the data, if the data does not arrive during that session, base station is notified. There is also another possibility, where the node can send or broadcast packets exceeding its limit. In such a situation, the monitor node notifies the base station about this, which in turn notifies other nodes in the network. One more possibility is where the cluster head only accepts data but does not forward it to next hop or the base station. In this case after some observation, the monitor node notifies the base station.

### 4. SIMULATED RESULTS

The work is being simulated taking multiples of 100 nodes into consideration. Simulation result shows that the paper takes care of denial-of-service attack, Sybil attack and worm hole attack and sink hole attack.

Utilizing pre-deployment or post-deployment keys cannot secure the network to greater extent. Pre-deployment or post-deployment keys are generated utilizing a function accepting some parameters. The adversary, after knowing some keys can get a hold on the other nodes easily. Hence this proves to be an insecure method.

Sybil attack is where the identities of the nodes are duplicated. The node will be able to have multiple identities. By utilizing different encryption keys it creates a defense mechanism against this attack. The node which creates a replica of the other node can be identified by this technique.

Wormhole attack is where the attacker records the packet at one location in the network, tunnels them to another location and retransmits in to the network. As the mobile agent issues different encryption key to the cluster heads, this method provides better security for the data and helps to control the replay of data to a larger extent.
forwarding the data to the next hop or base station. In this paper, monitor nodes will be actively observing the activities of the cluster and will send a report to the base station when it comes across any such circumstance. Simulated result shows 35% of nodes data are secure against Denial of Service attack.

![Energy Consumption Chart]

**Fig 5. Energy Consumption**

Energy is an important resource for the nodes. As these nodes are deployed in unattended areas, they cannot be recharged. But at the same time security also becomes a major concern. Simulated results show that there is an increase of 26.6% of energy consumption compared to the approach using single encryption key.

5. **CONCLUSION**

Security is one of the major concerns in any type of network. The nodes in the network are liable to get compromised, which leads to leakage of confidential information and wastage of resources. Military applications, where security highly confidential data becomes very essential. This paper utilizes the mobile agent to distribute secret key utilizing one-time pad algorithm. It utilizes time as a constraint to authenticate the source of data. To assure that the data dispatched is consistent, the time of dispatch of packets is taken into consideration. To add additional security, cluster heads along its path includes its ID in encrypted form. Denial of Service attack, worm hole attack, sink hole attack and Sybil attack is minimized to a larger extent.

6. **REFERENCES**


Ambika N has completed her MCA in the year 2001 and M.Phil in the year 2008. She is presently doing her PhD from Bharathiar University, Coimbatore. She is working as lecturer for MCA Department, Dayananda Sagar College, Bangalore. Paper titled “Figment Authentication Scheme in Wireless Sensor Network” was selected to be published at International Conferences, SecTech and DRBC 2010, held as Part of the Future Generation Information Technology Conference, FGIT 2010, Jeju Island, Korea, December 13-15, 2010 and is been listed in The Smithsonian/NASA Astrophysics Data system. The enhanced paper titled “Enhanced Figment Authentication Technique for Wireless Sensor Network” is been published in computer science Journal, Volume 1, Issue 1, April 2011.

Dr. G.T. Raju has completed his B.E in the year 1992, M.E in the year 1995 and was awarded PhD in the year 2008. He has published 4 Papers in International Journals, 15 Papers have been published at renowned International Conferences and 5 Papers at renowned National Conferences. He has 25 years of experience. He is presently working as professor and head for the department of Computer Science and Engineering, RNSIT, Bangalore.