Research Paper

Volume : 3 | Issue : 4 | April 2014 • ISSN No 2277 - 8179

Improved Key Selection Techniques for Wireless Sensor Networks

Engineering

KEYWORDS : Cluster, Cluster head, Pairwise key, Public key, WSN

R.Dhanalakshmi M.Tech Network Engg Scholar, Dept. of Computer Science and Engg; Kalasalingam University, Krishnankoil, Srivilliputtur, Tamilnadu, India.

K.Pradeepa Assistant Professor, Dept. of Computer Science and Engg; Kalasalingam University, Krishnankoil, Srivilliputtur, India.

ABSTRACT

Wireless Sensor Networks (WSNs) are more vulnerable to security attacks than wired networks because of their wireless and dynamic nature. It is important to define whether an incoming message originates from a reliable node or not. The primary answer for this is the use of cryptographically marked messages. There are two fundamental arrangements for marking messages: namely symmetric and asymmetric algorithm based cryptography. In the asymmetric key cryptography, public/private key sets are utilized to encrypt and decrypt messages. However, it can cause severe computational, memory, and energy overhead. On the other side, symmetric key cryptography is superior to asymmetric key cryptography in terms of speed and low energy cost, but at the same time, it needs to design an efficient and flexible key distribution schemes for improving key selection performance. In this paper, it is proposed a dynamic key management system for WSNs with the cluster head as a key distribution and coordination center for asymmetric keys. Public keys of the sensor nodes are dispatched by cluster head and symmetric keys set with these key combinations.

1. Introduction

Recent advantages in Wireless network are being deployed for a wide variety of application including military sensing and tracking, environment monitoring and tracking, smart environments, etc. and so it is clear that security requirement to be taken into account during the design time itself. Furthermore, the greater part of the WSN may dependably without any interference. Hence incorporating security in wireless sensor networks is very challenging [4]. Wireless sensor network are more vulnerable to various type of attacks such as jamming attack, eavesdropping, packet reply attack, Sybil attack and injection of false message through compromised nodes. The key distribution and management are considered to be the core of secure communication. In our proposed mechanism, a dynamic key for WSNs with cluster head as a key distribution and coordination center for asymmetric keys and symmetric key for secure as pairwise key.

2. Related Work

Some of the points to be noticed is that the key pre-distribution within the group and cluster will be broken by Dos attack [1]. Cluster nodes are randomly assigned to cluster head which provides low energy and light weight Lin SHEN and Xiangquan SHI. [3] Bechkit. W proposed a unital based key pre-distribution to achieve high network scalability during providing high secure connectivity coverage and overall improved performance. [5] Gupta. A proposed an common keys as shared Symmetric key and secure between links which means path key establishment the source node transfers the secret key to the destination node but this also has drawback, the solution as Multiple node disjoint paths between source and destination.

Random pair-wise key has an secure communication, Authentication, Energy saving, Cluster head can communicate directly with base station in network but all the nodes are not sharing key proposed by Kun Zhang and Cong Wang[2]. [4] [8] Gaurav Sharma et. al proposed cryptography as a standard method to provide security in a network, cryptography security can be provided through by symmetric key, asymmetric key and hash function.

But cryptographic algorithm is robust in nature so it does not use more memory, more power and more energy so the network lifetime can be increased. [6]Chan et al. proposed a multipath key reinforcement plan for WSN where security is more important than data transmission. The issue in essential plan is that the common key which secures a security interface between two node A and B, may reside in the memory of different node in the system and by capturing those nodes an attacker can attack that secure connection between A and B. [7] Kesavan proposed a security approach using skip jack algorithm is that secret key is embedded with the source code of every node to protect the keys in its non volatile memory, if the node is captured physically but the sensitive information cannot be retrieved by the attackers because the key selection protocol uses the node ID and some basis mathematical function to select the key for current data transmission but the key selection protocol highly depends on the counter value that is incremented periodically calculated by the nodes. The counter value further depends on the time synchronization between the nodes. This time synchronization is considered to be an overhead.

3. Proposed Approach

In this section, we present the overall details of our approach that ensures the following security properties:

Forward Secrecy: Even if an attacker recovered the adjacent Key in the cluster but the additional cluster keys are impossible to recover.

Privacy: Even the node is captured by an attacker; the secret key in the node's memory cannot be retrieved.

Data Confidentiality: Data Confidentiality guarantees that any intruder or other neighboring system could not get confidential information intercepting the transmissions.

Our approach has three types of keys:

Cluster Key: Each sensor node have neighbors' public keys to authenticate each neighbor in cluster.

Pairwise Key: For ensuring secure communication to agree on a pairwise session key. KAB provides confidential communication between a cluster member and its cluster head.

Individual Key: Each sensor node has a unique key shared with the center. This key is used for secure communication between a sensor node and the center.

3.1 Network Assumptions

Our approach assumes wireless sensor network in which the nodes are dynamic with similar computational and communication capabilities. The network uses Clustering technique for key distribution and secure communication. In a cluster, all the nodes maintain different keys, but every node uses same key for different communications with the base station (BS).

3.2 Design Goals

Our proposed approach is designed to overcome the Time syn-

chronization problem with secure communication.

3.3 Clustering Technique

Clustering is the process of organizing objects in to groups whose members are similar in some way, where one node in each cluster as cluster head, responsible for some tasks. Clustering provides a mutual organization of sensor nodes that simplifies coordination of transmission among neighboring nodes. This function reduces interference in multiple access broadcast environment. Each cluster contains a cluster head (CH), one or more sensor nodes. The cluster head schedules the transmission of public key for each node in the cluster, this provides communicate frequently between cluster members, which provides direct communication with a more distant node. In addition, a node moving in the same cluster without overlapping zone doesn't make any problem since it doesn't affect the cluster structure.

The clustering technique consists of three types of nodes: Mobile Certification Authority (an administrator) which will be present only at the initialization step then it can leave the network; a set of cluster head (CH) provides master services. Each node has a private and a public key. In the architecture, we consider that each cluster head is a mobile certification authority for its cluster members. To develop a secure WSN system, this minimizes resource consumption and maximizes security performance. Consist of many nodes, which are distributed into a large area and one (or more) Mobile Certification Authority (MCA) and coordination center of the system.

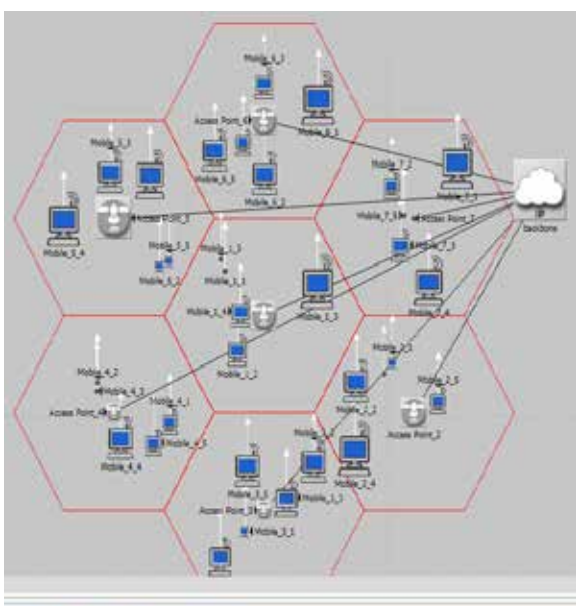

Figure1. Network Model of Cluster

3.4 Key Preloaded in sensor node

The best key distribution method is preloading the secret keys into sensor node before they are deployed. Similarly, some secret information needs to be pre-loaded into sensor nodes before they are deployed. In our proposed approach, sensor nodes are preloaded each with one unique secret key, shared with the other sensor node. Sensor nodes must authenticate themselves with the other sensor node using their corresponding unique keys. During this process, the other sensor node generates ID and loads each node with this key. The ID can be seen as the network key and will be used during the cluster formation process. Note that all members should prove their validity to the sink. So for each node, a unique key is used to authenticate the own node, shared with the destination sensor node (KAB) and is deleted after the first round.

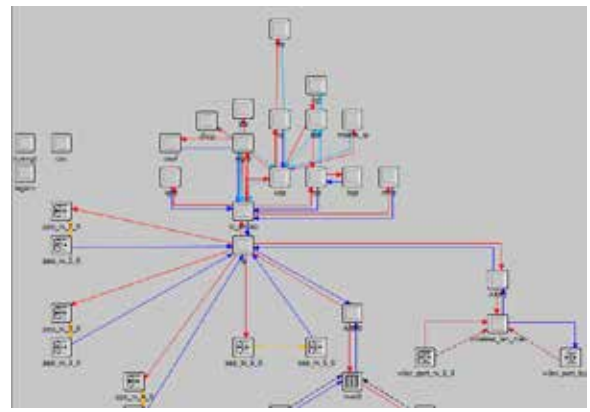

Figure2. Node Model of Cluster and Cluster head

3.5 Neighbors' public key distributed over cluster head

After the cluster setup, the cluster heads schedule and inform each cluster member. The sensor nodes are actively transmitting or listening for a period of the time and off the remainder. The sensor nodes transmit only at their scheduled time. This allows the sensor nodes to listen to the communication in their respective clusters. It is through this passive listening that the sensor nodes are able to develop trust relationships with their neighbors. Nodes that constantly drop packets or which behave in a selective or selfish manner can be easily detected by their neighbors. Each sensor node stores and maintains a trust key value of its neighbors.

3.6 Secure communication using pair-wise keying

Pairwise keying process provides basic security services in wireless sensor networks. That enables sensor nodes to communicate securely with each other using cryptographic techniques. These tolerate sensor node compromise by limiting the scope of every key. Thus, a sensor node compromise only affects past and future messages sent to or from that sensor node; other traffic is unaffected. Greater robustness against sensor node compromise does come at a cost, particularly in the overhead involved for key management.

If a sensor node communicates with a large number of sensor nodes, it must store many keys and select the appropriate ones when communicating. Since, sensor nodes are constrained in resources, this storage cost involved can be prohibitive. This technology provides Pairwise key establishment and management techniques which help in making the network secure.

Public key, Parameter Creation	
A Cluster head chooses and publishes a Prime Public key P and an key c having large prime order in C^*_P	
Private key Computations	
Node A	Node B
Choose a secret key a. Compute Node A ≡ c^a (mod P)	Choose a secret key b. Compute Node B ≡ c^b (mod P).
Public key Exchange of key values	
Node A sends A to Node B → A B ← Node B sends B to Node B	
Further Private key Computations	
Node A	Node B
Compute the key value B^a (mod P).	Compute the key value A^b (mod P).
The shared secret key value is $B^a = (c^b)^a = c^{ab} = (c^a)^b = A^b$ (mod P).	

Table1. Diffie-Hellman Key Exchange Algorithm

Volume : 3 | Issue : 4 | April 2014 • ISSN No 2277 - 8179

3.7 Key Distribution and Encryption Model of the system

In our proposed approach, clustering is initiated by sensor nodes. Consider if any two key are process as Node A and Node B are two communicating sensor nodes in the WSN System. MCA is a cluster head within an ad hoc network, and it is selected to provide distributed key management center's functionality. KAB is the communication pairwise keys between nodes A and B. {M} PubA denotes the encryption of message M with Public Key of node A.

Step 1 A sensor node (Node A) broadcast a message, which contains its ID (IDA) to its neighbours.

Step 2 Each neighbor (Node B and others) should obtain the Public Key of Node A from MCA.

Step 3 Sensor Node B uses Sensor Node A's public key to encrypt messages which contain its identifier (IDB) and a random number (RN1), which is used to identify this transaction

Step 4 Sensor Node A sends a message to Sensor Node B encrypted with PubB and containing B's random number (RN1) as well as a new random number generated by Node A (RN2).

Step 5 Sensor Node B selects a secret key KAB and returns this and RN2, which are encrypted using PubA, to assure A that its correspondent is B.

Step 6 The communicating parties (Sensor Nodes) are agreeing on a Pairwise key and they can use this for secure communication.

Public key, Parameter Creation	
A Trusted party selects and publishes a Prime Public key P and a key element c modulo p of large prime order.	
Node A	Node B
Key Creation	
Choose Private key $1 \le a \le p-1$. Computes $A = c^a \pmod p$. Publishes the public key A.	
Encryption	
	Choose Plaintext m. Choose random ephemeral key k. Uses Node A public key A to compute $c_1 = ck \pmod p$ and $c_2 = MA^k \pmod p$. Sends ciphertext (c_1, c_2) to Node A.
Decryption	
Compute the key value $(c_1^a)^{-1} . c_2 \pmod p$ This key value is equal to M = KAB.	

Table2. Diffie-Hellman KeyCreation, Encryption And decryption

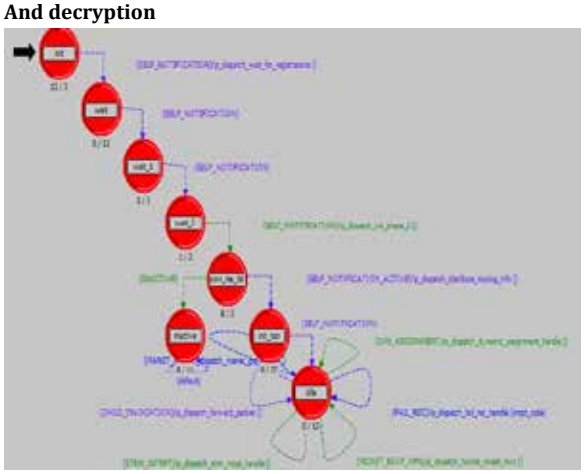

Figure3. Process Model of Clustering

Table3. Notations

Symbols	Explanation
BS	Base Station
CH	Cluster Head
ID	Identifier of Node
IDA	Identifier of Node A
IDB	Identifier of Node B
PubA	Encrypted value of Node A
PubB	Encrypted value of Node B
K KAB RN MCA	Pairwise key Pairwise key of A and B Random Number Mobile Certified Authority

4. Simulation and Analysis

This section compares the performance of proposed to algorithm with skip jack algorithm. The performance evaluation includes synchronization delay. The sensor nodes are simulated to deploy over a cluster with adjustable communication range and fixed sensing range. Simulation is performed using OPNET simulator. We have compared the performance of Clustered Time Synchronization with skip jack. The reason is clear that due to clustering the sensor nodes within the cluster have not to transmit for long distances and message exchange is also very less as compare to the other that save a significant amount of energy. Our proposed scheme reduces the number of data exchanges. In WSNs, most of the energy is consumed for transmitting and receiving of data, therefore reduction in data exchange also reduce the energy consumption.

Status	Hostname	Duration	Sim Time Elapsed	Time Elapsed
Aborted	localhost	13m 00s.	0s.	0s.
Aborted	localhost	13m 00s.	0s.	0s.
Aborted	localhost	13m 00s.	0s.	0s.

Figure5. DES Execution Result

In wireless sensor networks, the data transmission of sensor node is more susceptible to eavesdropping and tampering due to open communication environments. The substance of messages may be tampered, creating the BS to receive inaccurate data and waste a considerable measure of electric power in transmitting the pointless messages. In this section, the confidentiality and integrity of the proposed security approach is analyzed for the defense of several attacks.

Confidentiality: Confidentiality of sensor node is ensured by the use of symmetric encryption to encrypt ordinary traffic between the base station (BS) and sensor nodes. For more confidentiality we have enforced this approach using periodic key update to prevent long term attacks.

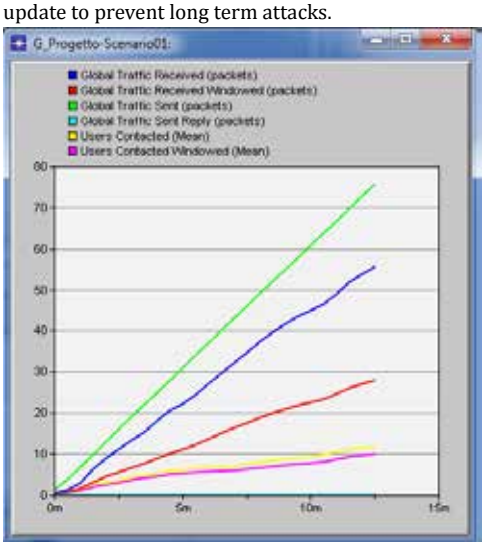

Figure6. In our proposed approach

Authentication: Authentication of sensor node is ensured by using public key (Pub) cryptography by the base station (BS); this public key (Pub) is preloaded to each sensor node before deployment which ensures the authentication of the base station (BS) using the corresponding private key as well as sensor nodes, since only legitimate node has the valid public key (Pub) preloaded before deployment.

Eavesdropping: This type of attack consists to passively listen to the exchanged data. In the proposed system, attack is avoided using symmetric encryption between each communicating entities of sensor node enforced using an automatic key update.

5. Conclusion and Enhancements

Cluster for Wireless Sensor Network was proposed to synchronize the entire nodes of the entire network. In the cluster technique, it adopted Pairwise key exchange mechanism to achieve the time synchronization between the Base Station and Cluster Heads. In the clustering phase, it adopted ID broadcast mechanism to finish the time synchronization between cluster heads and cluster members. The simulation results showed that the DH algorithm compared to skip jack algorithm, had faster convergence speed, low power consumption and better synchronization precision.

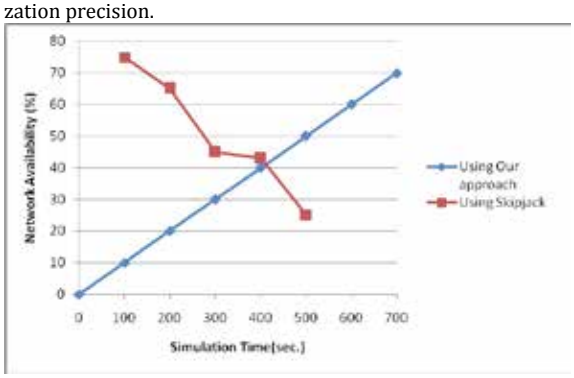

Figure7. Percentage of Network Availability over the Time

Our approach identifies the attacks like Reply attack, Dos attack, when network is affected due to pre-distribution of keys to cluster node. To address these security concerns, it would be imperative to study the recent technological advances in distributed systems.

Acknowledgments

We like to thank the management of Kalasalingam University for providing facility for doing research in networks laboratory,

REFERENCE

[1] Lin SHEN and Xiangquan SHI, "A dynamic cluster-based key management protocol in wireless sensor network," IJICS, vol.13,no. 2,pp.146-151, june.2008. | [2] Kun Zhang and Cong Wang and Cuirong Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," 4th International Conference on, vol.9,no. 2,pp.1-5,2008. | [3] Bechkit, W. and Challal, Y. and Bouabdallah, A. and Tarokh, V "A Highly Scalable Key Pre Distribution Scheme for Wireless Sensor Networks," in Proc. Wireless Communications, IEEE Transactions on,vol.12, Feb. 2013, pp. 948-959. | [4] Gaurav Sharma, Suman bala, Anil k. Verma, "Security frameworks for wireless sensor networks-review," 2nd international conference on communication, computing and security[ICCCS-2012]. | | [5] Gupta, A. and Nuggehai, P. and kuri, J., "An Efficient Scheme for establishing Pairwise keys for wireless sensor networks," in Proc. 2nd IEEE Conference. 2007, pp. 1-9. | [6] Chao song and Ming Liu and Jiannong cao and Yuan Zheng and Haigang and Guihai Chen, "Security of wireless sensor networks," Computer Communications, 2009, vol-32, pp. 1316-1325. | [7] V.Thirupathi kesavan and S.Radha Krishnan, "Multiple keys based security for wireless sensor Networks," IJCNIS, April, 2012, vol 4, pp. 68-76. | [8] Jinat Rehana, "Security of Wireless Sensor network," IJICS, vol.13, no. 2, pp.146-151, june.2009. | [9] OPNET Technologies, www.opnet.com | [10] H. Chan, A. Perrig, and D. Song, "Key Distribution Techniques for Sensor Networks, "Wireless Sensor Networks, ch.1, pp. 277-303,2004. | . | [11] H. Chan, V. D. Gligor, A. Perrig, and G. Muralidharan, "On the Distribution and Revocation of Cryptographic Keys in Sensor Networks," IEEE Trans. Dependable and Secure Computing, vol. 2, no. 3, pp. 233-247, Jul.-Sep. 2005. | | [12] X. Chen, K. Makki, K. Yen, N. Pissinou, "Sensor network security: a survey", IEEE Communications Surveys & Tutorials, Vol. 11(2), 52-73, 2009. |