

SECURED KEY DISTRIBUTION TECHNIQUES IN WIRELESS SENSOR NETWORKS

MADDU GOVINDAMMA¹, SRIRANGAM VAMSEE KRISHNA², Dr .T .PEER MEERA LABBAI³

^{1,2,3} COMPUTER SCIENCE&SRM UNIVERSITY,

Abstract— *The data security & communication needs the correct encryption key mechanisms. Here we described the Effective key management which is not authorised i.e; certificate less which is used in communication security that deals with moving of nodes. The CL-EKM gives updates of movement of clusters by ensuring the forward and backward mobility of nodes maintaining key privacy. This protocol also provides the key revocation for adjusted nodes & reduces the adjustment of nodes by using communication link. Our aim is to reduce the energy consumption and to improve the security levels through key protocols to maintain the privacy we use pair wise key protocol.*

Keywords— *Network security , Pre- distribution schemes , Cryptography , Clustering , Certificate-less key ,Performance evaluation*

I. INTRODUCTION

Network security

Network security maintains the rules & formalities for avoiding the misuse of systems and changes that are happening without authorization of the user security involves the specific access rights and to resources related to information security and to access control in particular. Here these access rights for the network are controlled by the administrators here all the users for the computers or any networking systems will be provided with the ID and a PASSWORD to ensure the secrecy and privacy for a particular user.

Network security covers a variety of network topology, usage of network i.e; public and private. Public key is used in an office where information gets shared between the colleagues while private is for personal computer for having their personal information . In many organizations, enterprises and other types of institutions network security maintenance will be very less as they need to transfer or sometimes the use of system or computer for a particular person was not given.

Network security mainly depends upon giving access to a particular person. This can be done in several ways one is giving user id and password, but this is not be that secret as the password if known to any other person this wont work ,so some more additional features are added such as we finger print or retinal scan . Network security is also maintained for the topology or the computer ,also maintained for the topology or the computer or system that it should not get the virus .This can be done by having firewall communication between two hosts can be maintained privately by crypting into some code . If any random person reads the message cannot be understood. Now-a-days new technique was employed known as honey pot . In this method honey pot will distract the mind of attackers by spending their time and energy on the decay server while data of a real server will be served pre-distribution schemes for sensor nodes.

Pre-distribution schemes

Now a days use of computer became very less as laptops and smart phones came into existence, the use of these was increased due to the extra features that are added to these systems gives mobility to the systems. They can be taken when ever and where ever needed . So now a days wireless systems can be deleted by the sensor nodes. Here we have some random key pre-distribution techniques for sending message between the wireless systems through sensor nodes. Here in this scheme we shall assume that the sensor nodes does not have any knowledge of the systems or nodes that are available. If we have some knowledge or information about any system or node then there will be priority which will not give good results while dealing with the wireless networks and this can be done for the unnecessary key assignments which lead to the wrong predictions

Here in this model the all sensor nodes will find a secret key that combines with their neighbours. In this model there are various phases like key pre-distribution scheme ,shared key discovery phase, path-key establishment phase , setting up key –space pools local connectivity , Resilience against node capture by extending these methods we can get the key distribution methods for sending secure measures in wireless method.

CRYPTOGRAPHY

This word actually means totally writing the hidden secret which can be used for exchange of data or message in maintaining the secrecy and security cryptography consists of two phases encryption & decryption, encryption is a process of changing the normal or ordinary information to the intellectual text, that is it is not a normal plain text as it will not be understood by a normal person when they read it.

The study of methods that are used for encryption of information without the usage of key which are generally required to do is known as cryptanalysis. This can contain various algorithms which are to be implemented. In olden days the cryptography is mainly used for sending only messages or data that are in the form of text these are mainly used by spies, military leaders, ambassadors, etc. This can be done by replacing one or group of letters with others. This method is known as substitution method, breaking or unrevealing of a message without using frequency analysis is essentially required. The knowledge of key will be maintained secure when decryption key will be contained with only person who you want to send the message. Due to the development of digital computers and electronics, enhanced this very much as we can use the binary format or bit sequences which are recently developed and used in the supermarkets and other places due to the complexity that occurred in the binary bit cryptography

CERTIFICATE LESS KEY

Here certificate less implies that its not authorised i.e; the keys can be passed through unauthorised nodes. Normally keys are generated by the certificate (authorised one) which have complete power and fully trusted ones. This may cause problem when compromising the nodes are done to rectify that certificate less keys will be generated i.e; it has total trust but not full power in case of any compromising nodes it cannot turn off the unauthorised one so it is safe to have the keys even during the failure of authorised nodes for certificate less key generation we need three different types of information that are other users public key, id, third party public information.

Here very high security should be maintained by checking the third party which is to be used, the node which we are selecting should not be compromised directly by any methods. Certificate less key consists of four types of keys

1. Public-private key 2. individual node key 3. Pair wise key 4. Cluster key

Public-private key

Normally in the cryptographic field, there are mainly two kinds of keys, public key and private key when a group of people who are having same authentication powers then public key will be generated as all the persons will contain same authority to use it while when a hierarchical system is maintained. Then the private key is generated such that only one person will have all the powers for using the key.

Public key cryptographic mechanisms are mostly based on the mathematical problems while the private key cryptographic mechanisms are based on symmetric problems in digital signature. When the message is encrypted it will be done in the sign of private key but it will be verified by everyone who gets the access of senders public key. Here this can prove that the node can have both private and public key at a time. Public key cryptography was used in the electronic communication in highly secured manner when the information is passing through the internet. In this the attackers who are not having this key cannot do anything this is also used in key exchange.

Individual node key

Every node that is under the network i.e; Base station. The base station provides an identity or label for all the nodes. The individual node key is useful when there is node that wants to encrypt a message if can use its own key or generating the message. These keys are also helpful during the compromising of the nodes. It has its own label even if that nodes was compromising by any algorithm or process. The base station creates the individual nodes is placed or positioned in the network the base station gives the separate key for the node known as individual node key.

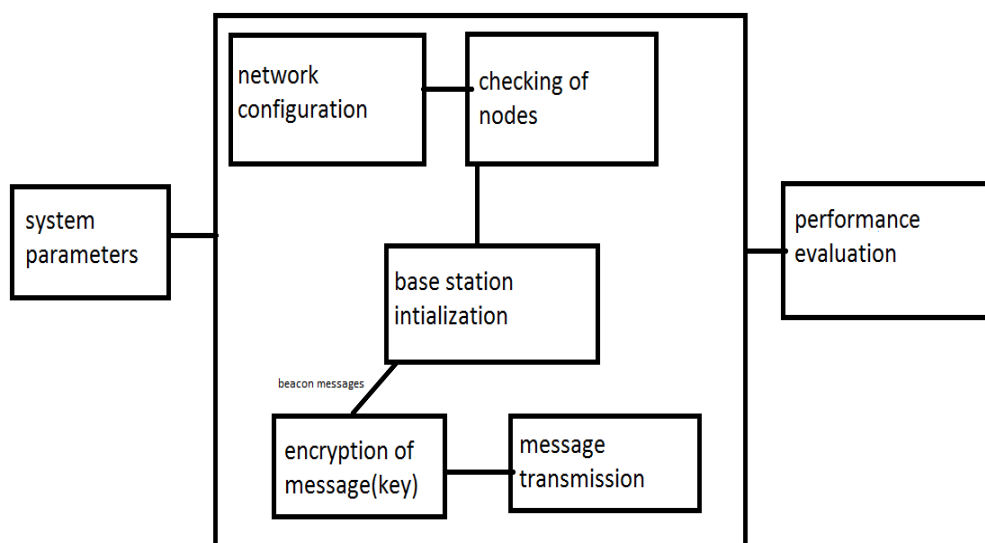
Pair wise key

If the node contains both the private and public key then it is known as pair wise key. Now the node can send personal messages as well as group message when ever there is a case of joining into the cluster, the cluster head's public key of cluster should be contained in the node and it becomes the personal key inside it.

Cluster key

A group of nodes is known as cluster. The group should contain same key known as cluster key. The cluster key is always used to send message in the cluster itself i.e; Like if any new nodes are added or any existing node leaves the cluster, all the cluster members need to know which node is adding or leaving the cluster. This is the information which can only be sent to all the other nodes by cluster key.

ARCHITECTURE



System parameters

These are the parameters that are used to setup the system . Here we are using parameters like channel, propagation , antenna , queue, AODV. These are set to do our program as it should work in the real world. These parameters defines the variables and it gives the data structures that we are using. The parameter gives features or measurable factors that can be used for defining any system .In the case of adopting a new code for customers the system parameters are applicable .The difference between the system constant and system parameter is that the parameter can be changed at the run time but should be constant. It should be changed only during writing the code, not at the run time. Parameters are generally specified by the predicates known as values.

Networks Configuration

As the new network is placed in the system, there should be some parameter and the registrations of the individual nodes needs to be done. These parameters are nothing but system parameters which can help to create the topography, gives the topology about how the nodes should be placed .Routing table gives the routing of packets through the nodes for generating the nodes with active participation. It should have the type, len , antenna type , channel topology instance, router trace, agent trace, movement trace.

Initialization of Base station

For initializing the base station it should know its agents, so we need to provide the agent values. Select a node for the base station, give a separate colour for the node, define the energy for the node and get the activation mode by setting the energy to the max for the base station and max-min to the cluster heads and min to the unauthorised nodes. The valve of the energy will be randomized while creating the node in the process of initialization

Encryption of message(key)

Here when the message is passed that means that the message has entered, first convert to the Hexval value and then to the decimal value and convert to the binary bits by using the HMAC algorithm. Key will be generated for each node. The ECC algorithm is used for encrypting the message and then its ends for the routing methods.

Message transmission

Here the encrypted message is passed to the base station. Then the base station will check for the routing path to send the message to the destination node by compromising the nodes. The Base station now gets the address of all other nodes by sending the Beacon messages. Then the packet and nodes key data will be transmitted.

Performance evolution

It is the integrative process for calculating the performance that is being done in the whole process. In this while by sending the message packets, performance can be evaluated. This can be done in four methods.

Packet delivery ratio

It is the number of packets delivered to the total number of packets generated.

Packet loss ratio

The number of packets if lost or missed or cannot be reached to the destination are not counted to the total number of packets generated, is known as packet loss ratio. This gives the total number of lost packets or unreached packets in the network.

Delay ratio

The time taken for the packet to transfer from source to the destination is known as delay time.

Energy consumption

The total energy consumption equals to the sum of energy consumed by all nodes in the network.

Working of the architecture

Here first we need to create the system parameters for communication in the network for data transmission. Then we need to create the nodes by specifying the position on the network and then provide flag to activate the node. Now initialize the base station and the cluster heads. The authentication of nodes is done by sending the beacon message by getting the addresses of each and every node and routing table is maintained by each & every node for knowing the address of other nodes. The cluster formation will be done on the basis of distance and the other one is based on active node then it will be added to the cluster head. Now the node will contain the cluster key and also contains all four types of keys within it. The information about node leaving the cluster will be known only through the cluster key. The next step in this process is getting the data from the user. After receiving the data the original data is converted to hexaval (hexa value), 16 bit code. This code is converted to decimal value which in two gives the binary packets. For these binary data we should apply XOR application with the node id and generate the new pair generation key. Using the ECC cryptography the message is secured as the decryption needs the node id to retrieve the data. The base station sees the shortest path and accurate path for sending the data packets from the source to destination node.

Results

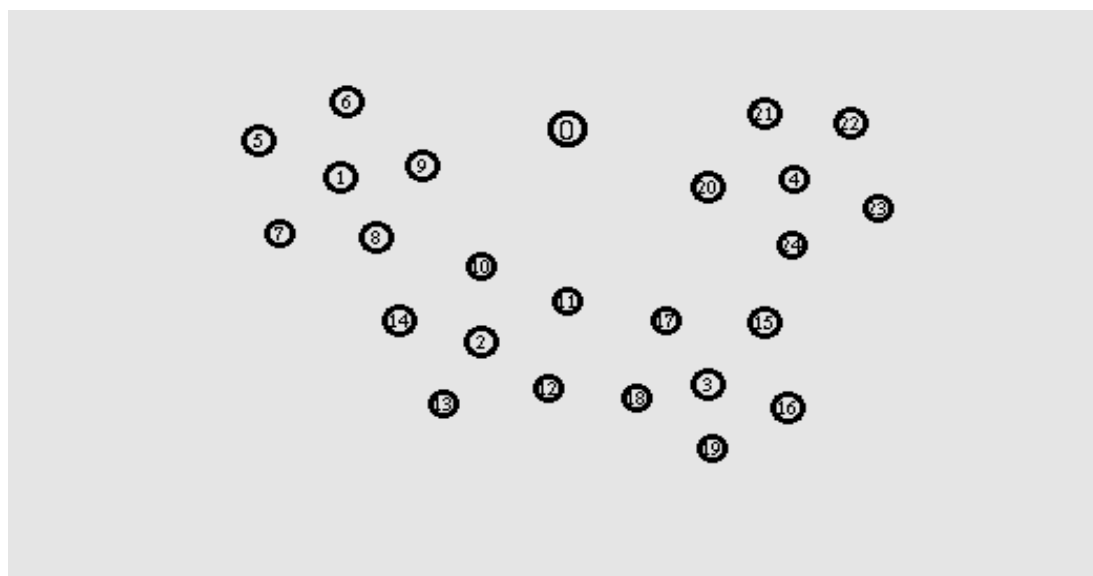


Fig 2. nodes formation

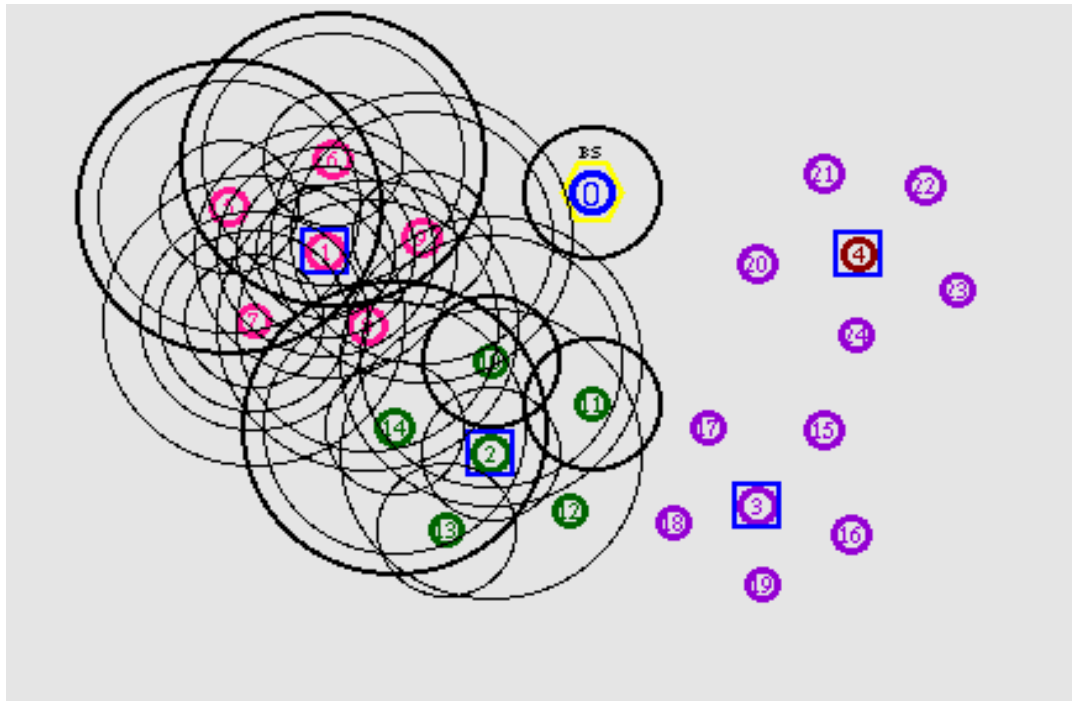


Fig 3. initilasiation of nodes

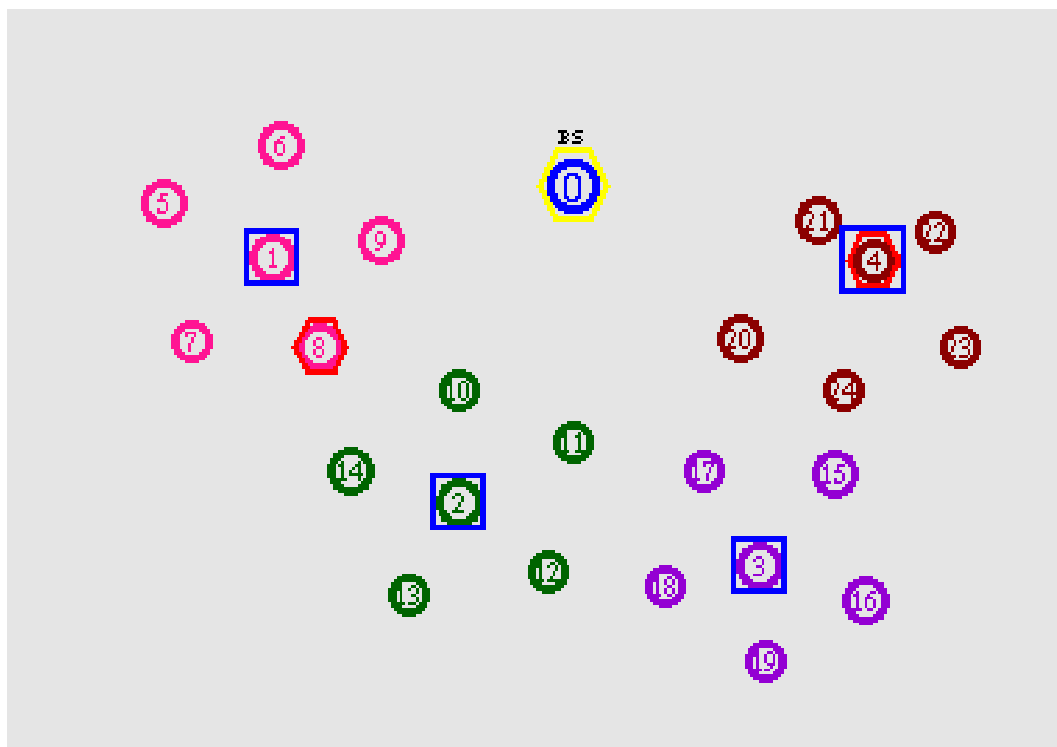


Fig 4. mobility of nodes

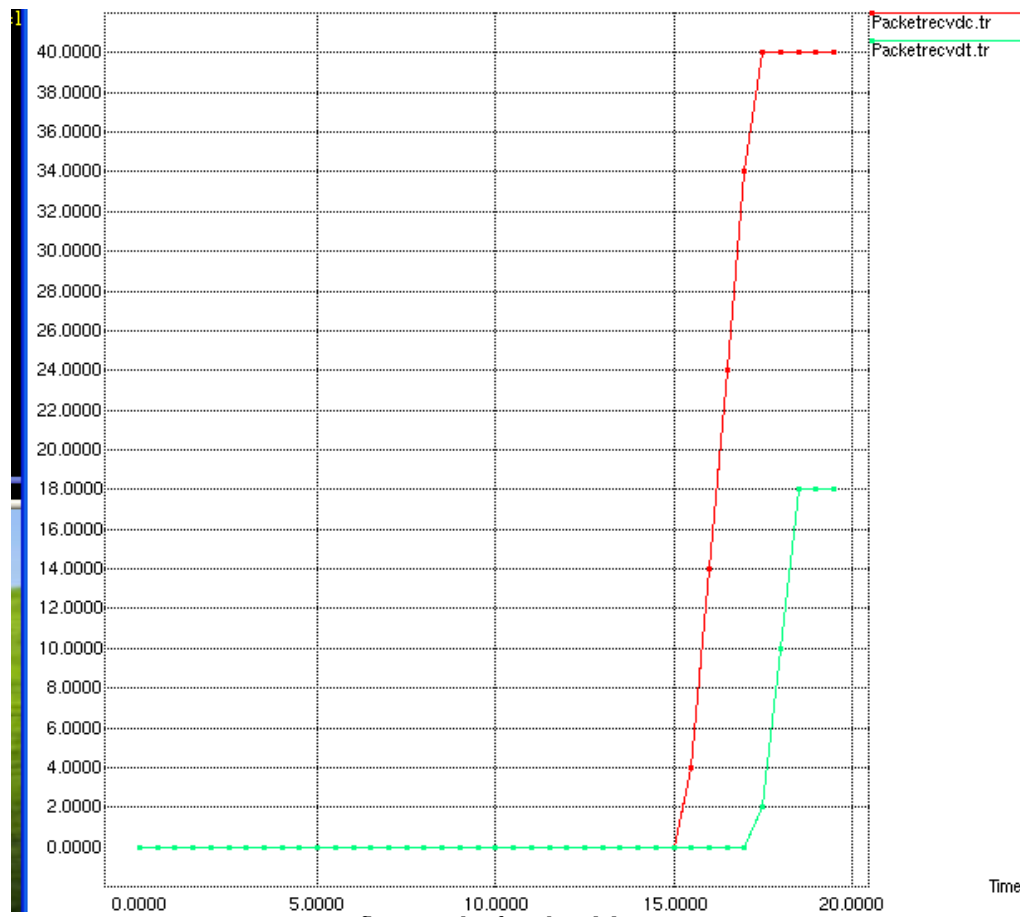


Fig 5. flow graph of packet delivery ratio

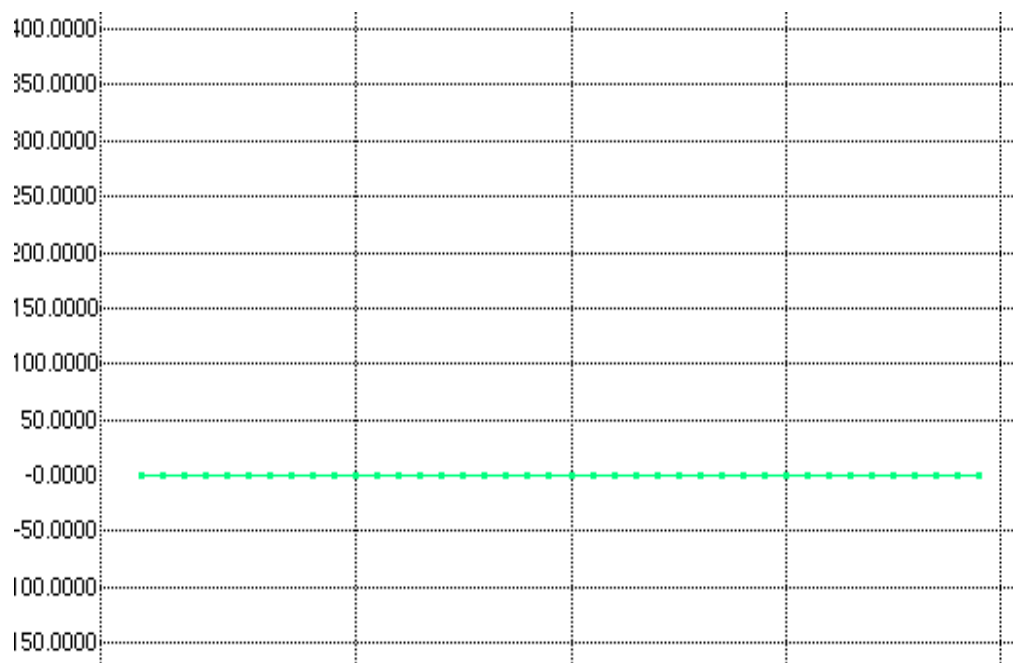


fig 6. flow graph of packet loss ratio

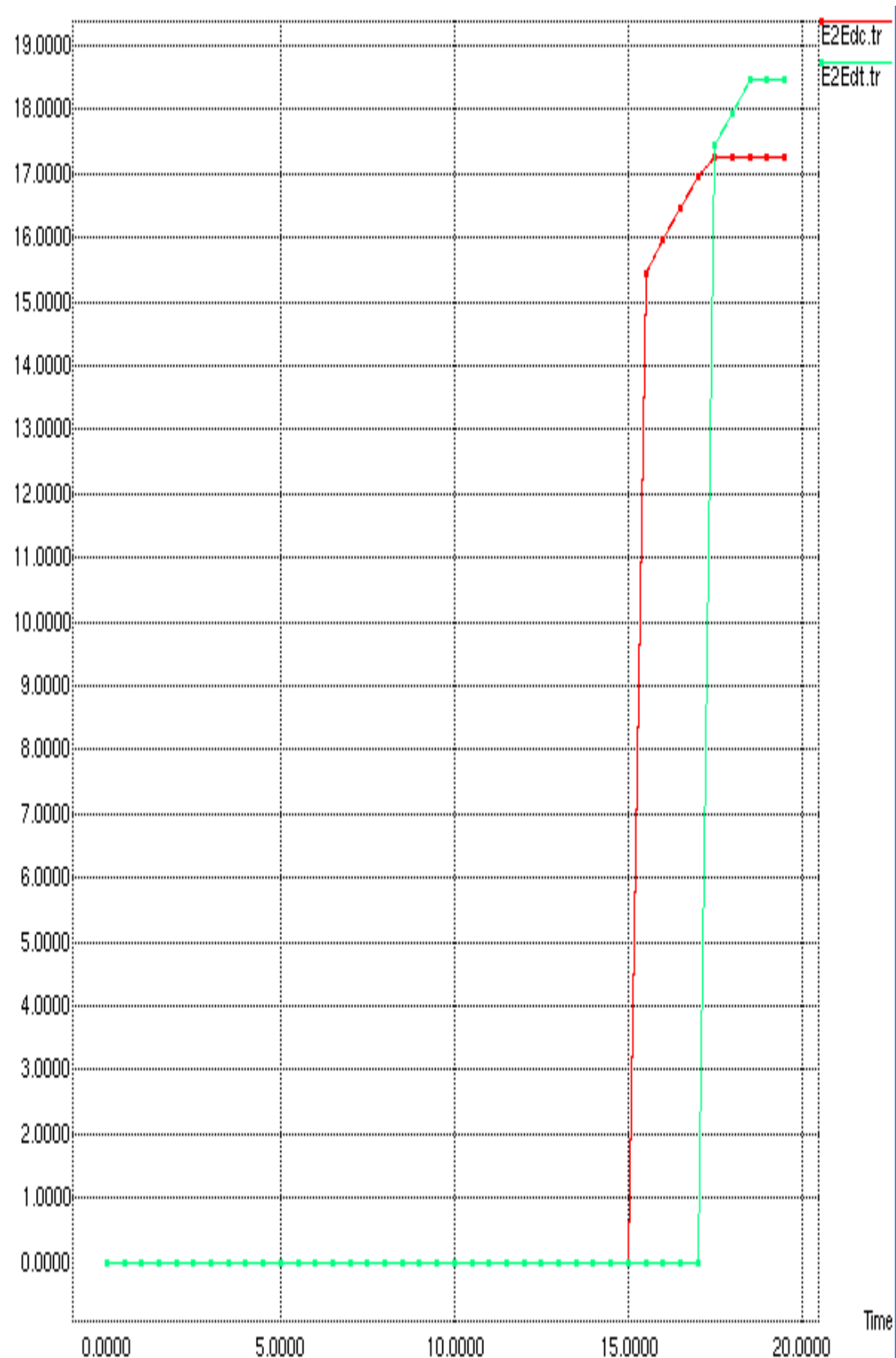


Fig 7. flow graph of end to end delay

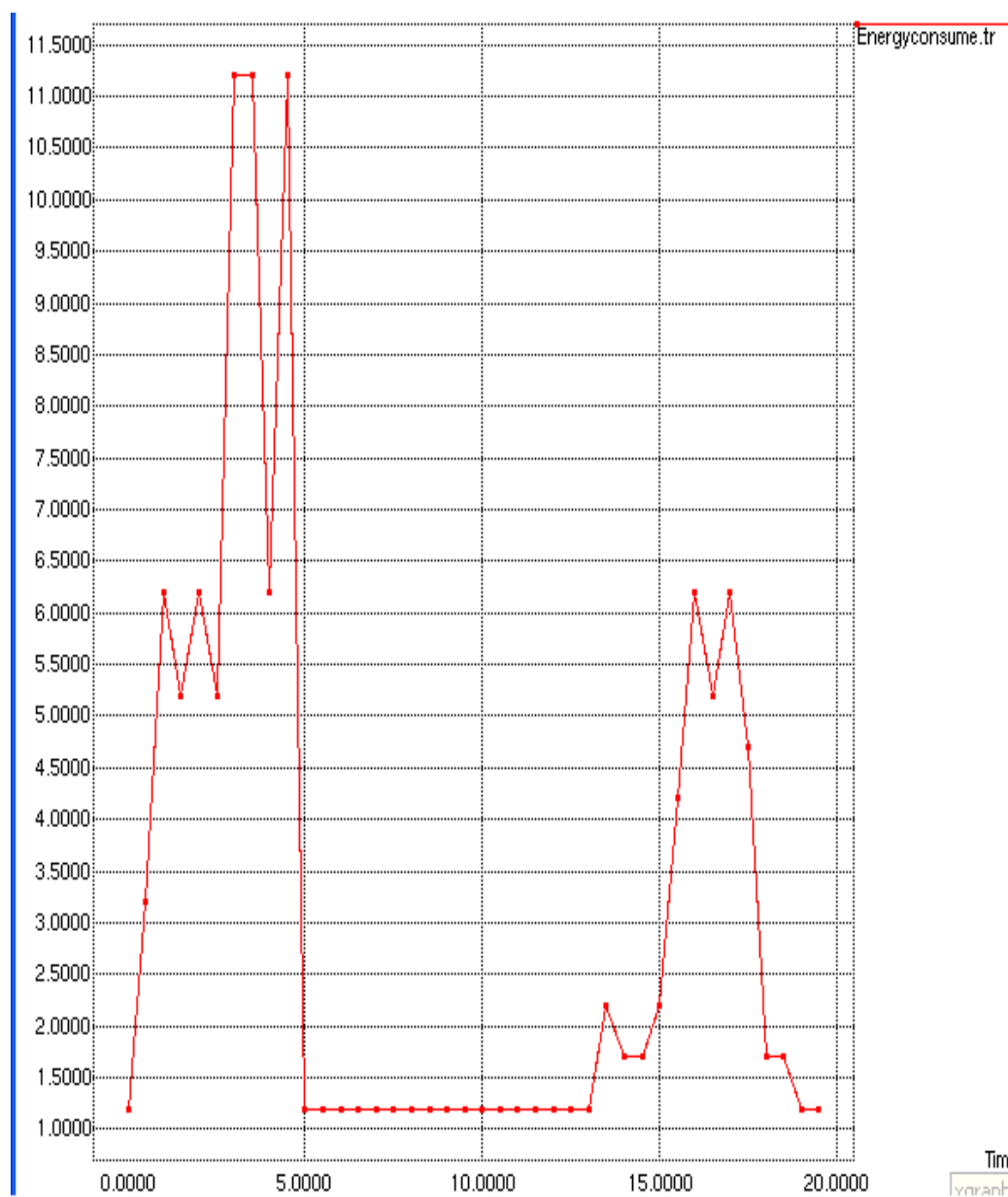


Fig 8. Flow graph of energy consumption

Conclusion

The security of message transferring is achieved by maintaining the effective key management, but in this case generation of keys is given to the authorized nodes only if there is any compromised of the authorized node is happened then security is not maintained. So in this paper we are using certificate less key generation that is using unauthorized nodes which can also generate the keys with high security. So in the case unauthorized node compromises the data will be at the main node soothe security is highly maintained as the unauthorised node is generating the key. It needs only less energy to generate it. So overall energy consumption will be reduced.

Acknowledgement

The success and final outcome of this project requires guidance and assistance from different sources and we are fortunate to have this all among the completion of the project. Whatever we have done is largely due to such guidance and assistance and we will not forget to thank them . We express our sincere thanks to the Head of the Department, Department of Computer Science Engineering Dr. B . AMUDHA for the help and infrastructure provided to us to complete the project successfully and her valuable guidance. We owe our performance gratitude to our project guide Dr. T. PEER MEERA LABBAI who took keen interest in our project work and guided us all along till the completion of our project work by providing all the necessary information for developing good systems

References

- H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symp. SP*, May 2003, pp. 197–213.
- W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A key predistribution scheme for sensor networks using deployment knowledge," *IEEE Trans. Dependable Secure Comput.*, vol. 3, no. 1, pp. 62–77, Jan./Mar. 2006.
- W. Du, J. Deng, Y. S. Han, P. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 2, pp. 228–258, 2005.
- M. Rahman and K. El-Khatib, "Private key agreement and secure communication for heterogeneous sensor networks," *J. Parallel Distrib. Comput.*, vol. 70, no. 8, pp. 858–870, 2010.
- M. R. Alagheband and M. R. Aref, "Dynamic and secure key management model for hierarchical heterogeneous sensor networks," *IET Inf. Secur.*, vol. 6, no. 4, pp. 271–280, Dec. 2012.

BIOGRAPHY

Vamsee krishna was currently pursuing B.tech from SRM university, in the stream of computer science and engineering, I was very much interested in knowing the facts about wireless network communication which lead to do a project on network communication.

Govindamma was currently pursuing B.tech from SRM university, in the stream of computer science and engineering