Communication ins Wireless Sensor Networks through Needham-Schroeder protocol

REENA MALIK **NISHA MALIK**
Department of Computer Science & Engineering Department of Computer Science & Engineering Faculty of Technology,UTUTula's institute
Dehradun, Uttarakhand 248197, India Dehradun, Uttarakhand 248197, India
Email:reenamalik2908@gmail.com Email:reenamalik2908@gmail.com

Abstract— now a day's wireless sensor network is in demand. Through wireless sensor network we can build a single device which have feature like communication, sensing and computation. As deployment of sensor networks increase, security issue becomes the main factor that need more concern. There are many issues in the data communication when dealing with sensor network. This paper uses needham-schroeder protocol for different clusters and plus one needham-schroeder protocol between different cluster head and sink node to save energy and time of communication of sensor node.

Index Terms—Authentication, data distribution, Wireless communication network, Wireless sensor network, Symmetric-key distribution, Key distribution centre, Needham-Schroeder protocol.

1 INTRODUCTION

The performance issue of wireless communication network and wireless sensor network become important due to their architecture. The architecture of wireless communication network is very complex. Failure of components of wireless communication network is very common and its resources are very limited which directly affect its performance. Example if battery of wireless communication network is limited then wireless communication network will not be able to work for long time. Nodes of wireless communication network are mobile in nature. They keep on moving in network and thus cause network link to be unavailable for maximum time. This affects the performance of wireless communication network. Nodes in wireless communication network are accomplished to receive and transmit to others node in the network. Nodes can sensor node computer etc. there exist wireless communication link between each nodes. If they are connected directly then it is ad hoc network and they can also be connected through base station. In ad hoc network if two nodes are not in range of each other they can communicated through intermediate node. Nodes can be wireless or wireless plus mobile. For fixed nodes different topology are used. Authentication is process to authenticate user. It is of two type peer entity authentication and data origin authentication. In peer entity authentication it authenticate receiver and sender after connection is established between them where as data origin authentication is used to authenticated source of authentication exchange take place between two parties in which message is passed to authenticate each other. Wireless sensor network is part of wireless communication network.Typically, a wireless sensor network comprises more but less resourceful nodes than those in the other types of wireless communication network.Each sensor node is capable of processing a limited amount of data[1]. To provide secure communications for the WSNs, all messages have to be authenticated [2]

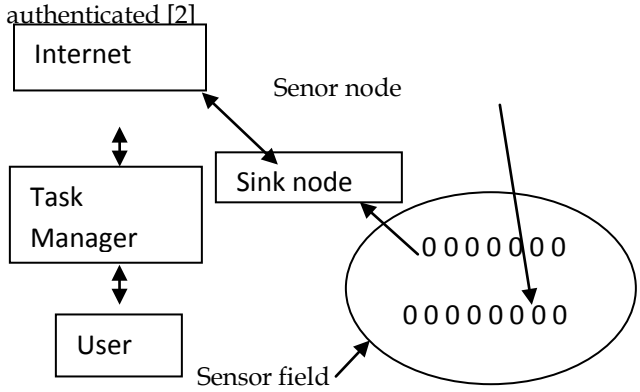

Fig 1 flow of communication in wireless sensor network

Fig 2.Kerberos servers

Figure 1 depicts the communication in wireless sensor network which consist of numbers of sensor nodes. Security requirements in WSNs are similar to those of wireless ad hoc networks due to their similarities [3].Each sensor node is capable of processing a limited amount of data[1].Data distribution is the process of distributing data among nodes in the network. Symmetric key distribution is the process in which key is distributed in symmetric method. It requires a shared key between two entities. It has a key distribution method which is also known as trusted third party and shared secret key is shared with them. An ad hoc network with mobile nodes is a mobile wireless ad hoc network (MANET) [4].

2 RELATED WORK

Kerberos authentication scheme [2] is used for the authentication of base station in sensor network. It has been name after three-headed dog that is part of mythology of Greek. Latest version that is being used is version 5.

Servers involved in Kerberos areauthentication server (AS) and ticket-granting server (TGS)

AS is a part of key distribution centre. User register themselves with AS and then AS provide them a identity and their password. AS maintain these details in its database. AS confirm user and provide them with a session key if verification is complete and also sends ticket to the other server that is ticket-granting server. TGS gives the concern ticket to the end user. It also provide session key between parties after its own verification.

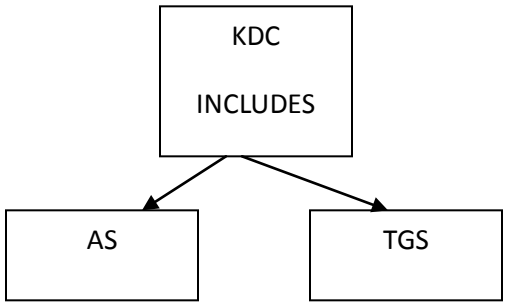

Figure 2 depicts that AS server and TGS server are part of key distribution centre.

Drawback of Kerberos servers

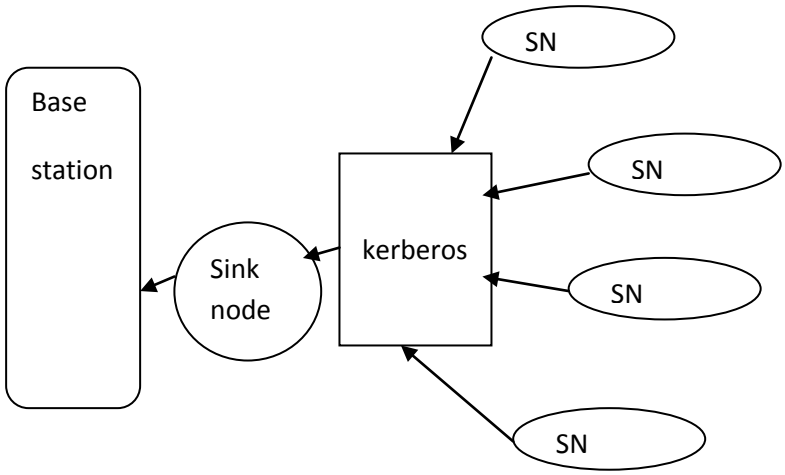

Fig 3 Sensor nodes connected with a single Kerberos

Figure 3 depict the architecture of related work. The main drawback was that there is only one Kerberos used for so many sensor networks. Suppose large number of sensor nodes request for authentication at the same time then they have to wait for long time as Kerberos is very busy. Thus this delays their connection with sink node. Lots of energy and time is wasted. This problem needs to be solved.

R3 3 PROPOSED METHOD

To overcome the above problem this method is proposed. in this we use Needham-Schroeder protocol. In this we use two R_A and R_B. Let p1 be one party for communication and p2 be other party of communication.

1. p1 will send a message to KDC which also include R_A, his and p2 identity.
2. KDC send encrypted message that is encrypted with p1,s key to p1 which consist of R_A, p2 identity, session key and encrypted message for p2.
3. p1 send p2's ticket to him
4. p2 send a challenge to p2 i.e. R_B, that is encrypted with session key.

5. p1 response to it with R_B-1.

In this method we form number of cluster of sensor nodes in which sensor node in one cluster is connected to one Needham-Schroeder protocol and

This protocol is connecting to cluster head. All cluster head is connected to one Needham-Schroeder protocol and this protocol is then connected to sink node. All cluster head node can also communicate with each other through the protocol that connects them.

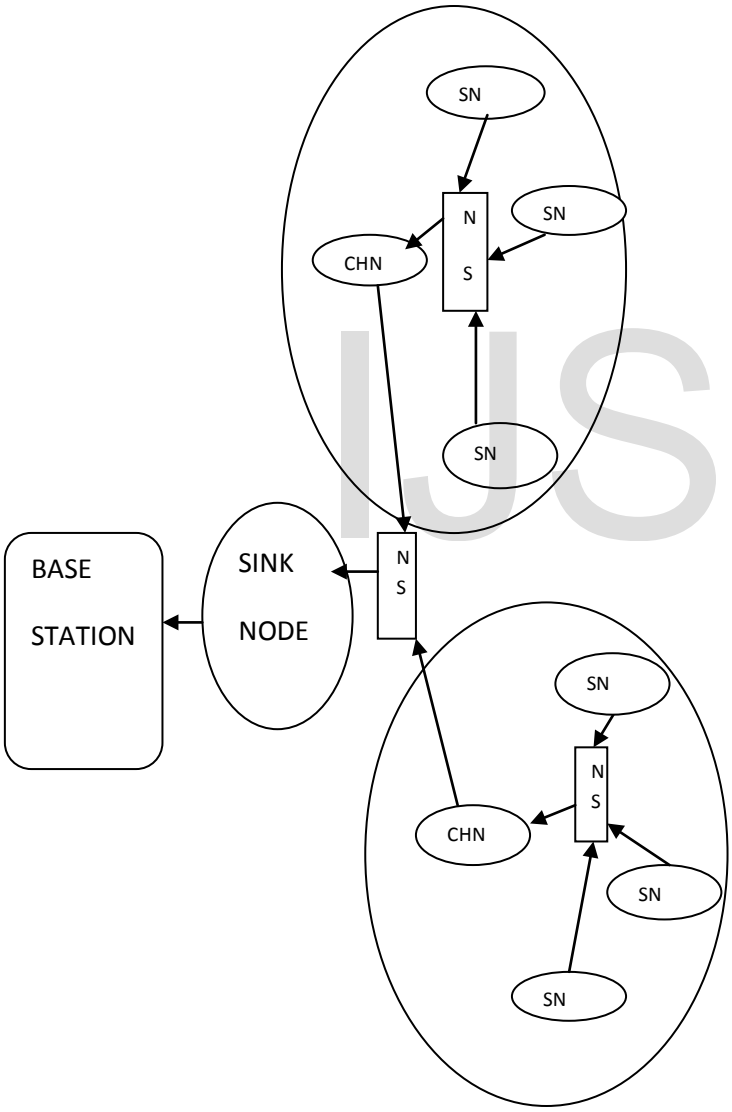

Fig 4 clustering using Needham-Schroeder protocol

Figure 4 depict the clustering and communication mechanism. SN stands for sensor nodes, CHN for cluster head node, NS for Needham-Schroeder protocol. It is clear that there is more than one cluster and each has its own Needham-Schroeder protocol. Sensor nodes in respected cluster can request Needham-Schroeder protocol for authentication. In cluster communication is between cluster head node and one sensor node. After that cluster head communicate with Needham-Schroeder protocol that is connected with sink node. This communication is more reliable than the previous proposed method. Needham-Schroeder protocol that is connect to sink node protect node from unauthorized users.

4 CONCLUSIONS

This method provides reliable communication among sensor nodes. The data that is communicated between them is also secure. It also saves energy. Unauthorized user cannot communicate with sink node. Cluster head node can communicate with any other cluster head node. Further work will be implementing to reduce the usage of energy.

REFERENCES

[1] C. Shen, C. Srisathapornphat, and C. Jaikaeo, Sensor Information Networking Architecture and Applications,IEEE Pers. Commun., Aug. 2001, pp. 52–59.

[2]Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, Security Issues in Wireless Sensor Networks, international journal of communicationsIssue 1, Volume 2, 2008

[3] K. Lu et al., A Framework for a Distributed Key Management Schemein Heterogeneous Wireless Sensor Networks, IEEE Transactions on Wireless Communications, vol. 7, no. 2, Feb. 2008, pp. 639-647

[4] S. Jiang, N. Vaidya, and Wei Zhao, Dynamic Mix Method in Wireless Ad Hoc Networks. In Proc. IEEE Milcom, Oct 2001

[5] J. Kohl, B. Neuman and T. Ts'o The Evolution of the Kerberos Authentication Service, in Brazier, F., and Johansen, D.Distributed Open System Los Alamitos, CA: IEEE Computer Society Press, 1994

[6] QasimSiddique, Kerberos Authentication in Wiireless Sensor Networks, Annals. Computer Science Series. 8th Tome 1st Fasc,2010.