Kerberos Based Secure Communication in Wireless Sensor Networks

Kriti Jain
Department of Computer Science & Engineering
TULA's Institute, The Engineering and Management College,
Dehradun, Uttarakhand 248197, India
Email:kriti.engineer@gmail.com

Upasans Bahuguna
Department of Computer Science & Engineering
TULA's Institute, The Engineering and Management College,
Dehradun, Uttarakhand 248197, India
Email:Upasanabahuguna4@gmail.com

Neeti Bisht
Department of Computer Science & Engineering
TULA's Institute, The Engineering and Management College,
Dehradun, Uttarakhand 248197, India
Email: neeti.bisht11@gmail.com

ABSTRACT

The wireless sensor network is an emerging field that combines sensing, computation, and communication into a single tiny device. As sensor networks frame closer towards well-known deployment, security issues become a vital concern. So far, much work has focused on making sensor networks realistic and useful, but still security in data communication is big issue for research. This paper proposed the idea of having different Kerberos authentication architecturefor the different clusters in sensor network to save energy of the sensor nodes and to save time for data communication between the sensor nodes.

Keywords: Wireless Communication Network, Wireless sensor network, data dissemination, Kerberos authentication

1. INTRODUCTION

The proliferations of wireless communication networks (WCN), such as mobile *ad hoc* networks (MANET), and wireless sensor networks (WSN), make their performance issues equally important, if not even more important, because a WCN is more complex in nature than the wired CN, its components are less resourceful, and the components are more susceptible to failures. Limited resources (*e.g.*, battery, memory, and bandwidth) reduce the intrinsic performance of WCN, and thus methods to improve the metrics in WCN are imperative. The node mobility in WCN makes network links have higher unavailability rates and makes the performance analysis of a WCN even more difficult.A WCN comprises a set of nodes each of which is capable of transmitting to or receiving from other nodes. The nodes in the network, among others, can be a computer, concentrator, end user terminal, mobile station, repeater acting as a transmitter/receiver, or a sensor node. Two nodes in a WCN, in contrast to a *wired* CN, are connected by wireless communication links either directly (without infrastructure – the *ad*

hoc mode) or through a base station (the infrastructure mode). In an *ad hoc* WCN, the wireless nodes communicate with each other without using a fixed infrastructure, and when two nodes are not within their transmission range, the intermediate nodes relay the messages between nodes. In some networking environments, such as wireless home or office with stationary workstations, the network nodes are wireless but non–mobile (*stationary*). In others, the network nodes are both wireless and *mobile* [1]. The stationary nodes form a fix topology or a random topology (*ad hoc*), if deployed randomly. An *ad hoc* network with mobile nodes is a *mobile wireless ad hoc network* (MANET)[2]. MANET is a new frontier for WCN and is different from a traditional WCN in many ways. One major difference is that a routing path in MANET uses a sequence of *mobile* nodes, a wireless link connecting each pair of the nodes.

The *wireless sensor network* (WSN) is another class of WCN. Nodes in WSN, forming a certain topology, can be mobile or stationary and deployed randomly (*ad hoc*). Typically, a WSN comprises more but less resourceful nodes than those in the other types of WCN.Each sensor node is capable of processing a limited amount of data[3].

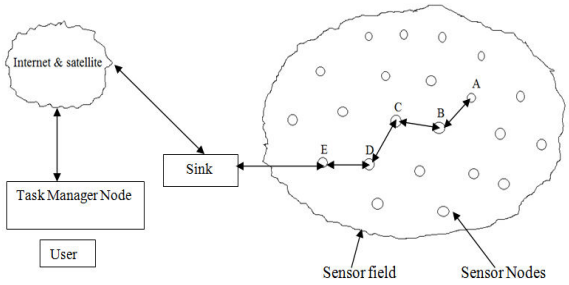

Figure 1 Communication architecture of wireless sensor networks

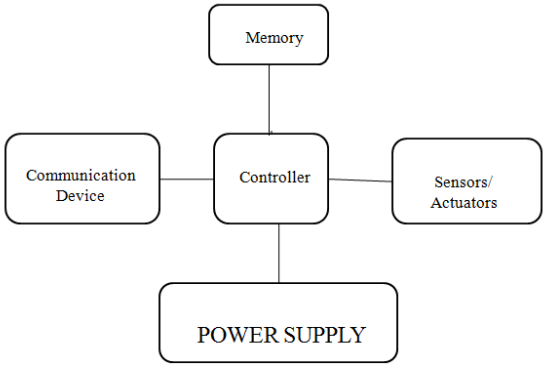

Figure 2 Sensor Node Architecture

Figure 1 and Figure 2 depicts the communication and sensor node architecture in wireless sensor network.
Earlier, the sensor networks consist of many small number of sensor nodes that were wired to a central processing station. Nowadays, the major focus is on wireless Sensing nodes.
Because of the character of wireless communications, resource constraint on sensor nodes, size and density of the networks, unidentified topology prior to deployment, and high danger of physical attacks to unattended sensors, it is a confront to provide security in WSNs. The main security requirement is to provide confidentiality, integrity, authenticity, and availability of all messages in the presence of resourceful adversaries. To provide secure communications for the WSNs, all messages have to be authenticated[4]. Modification of information is possible because of the nature of the wireless channels and uncontrolled node environments.An opponent can use natural impairments to modify information and also render the information unavailable. Security requirements in WSNs are similar to those of wireless ad hoc networks due to their similarities [5].

2. RELATED WORK

Kerberos authentication scheme[4] is used for the authentication of base station in sensor network. It provides a centralized authentication server whose work is to authenticate user by providing him the ticket to grant request to the base station. Earlier proposals have provided architecturefor the authentication of base station in the wireless sensor network based on the Kerberos server authentication scheme [5].

2.1 Kerberos Architecture:

With reference to the figure below there are two main components of Kerberos server
• Authentication Server
• Ticket Granting Server

Authentication Server

The Authentication server knows the password of all the users and stores them in a centralized database. The authentication server shares a unique secret key with every server. These keys have been distributed to the user using a security mechanism.

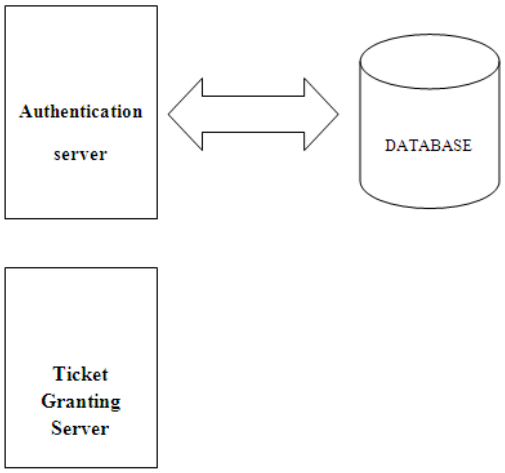

Figure 3 Kerberos Architecture

Ticket Granting Server

The Ticket granting server performs the work of issuing tickets to users who have been authenticated to authentication server. The first work that is to be performed is that the user first requests a ticket from the authentication server, then this ticket is saved by the user. Each time the user authenticate itself, the ticket granting server grants a ticket for the particular server/Base Station. The user save each of the service granting ticket and uses it to authenticate to a server whenever a particular service is requested.

2.2 Loopholes in earlier proposed research work

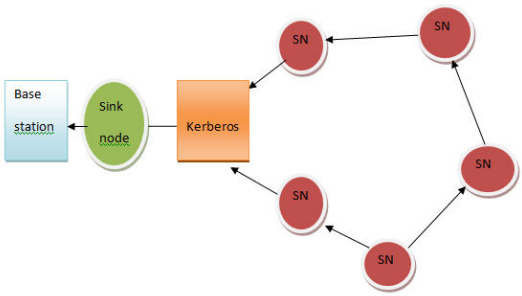

Figure 4 Sensor network with a single Kerberos

The major loopholes in earlier sensor networks were that each node in a wireless sensor networkhad only a single authentication centre i.e. the Kerberos. Due to this, all the sensor nodes had to wait for a long time for their authentication and to establish connection with the sink node and the base station. The major disadvantage of this technique of communication was that each node suffered from energy loss with the wastage of time. There was a need to overcome this problem and check the efficient solutions for it.

3. PROPOSED TECHNIQUE

This paper proposes a solution for the above mentioned problem. Instead of serving one node at a time with the same Kerberos, clusters of sensor nodes in a wireless sensor network can be formed, each having its own authentication centre i.e. the Kerberos. This proposed solution will serve each node in the wireless sensor network by authenticating it through the particular Kerberos of that cluster and then letting the nodes to communicate with the sink node and finally the base station.

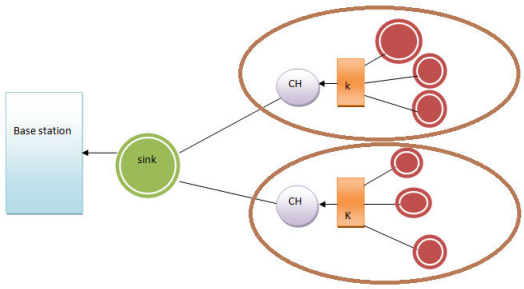

Figure 5 Clusters of sensor nodes each with a Kerberos

From the above figure, the proposed solution can be easily understood. Here there are more than one clusters of sensor nodes having their own authentication centre i.e. Kerberos. Each node of a cluster communicates with the authentication centre provided in the concerned cluster and then contacts to the sink node and further to the base station. This proposal will save the power of the sensor nodes and will make the communicating network efficient and reliable.

3.1 ADVANTAGE OF PROPSED TECHNIQUE

This technique can avoid more time and heavy traffic load with less energy consumption. In traditional network when more than one node send request to the Kerberos it takes more time to response which results in processing delay and leads to loss in energy of sensor nodes in sensor network. By implementing proposed technique where different Kerberos are

used for different clusters, they will process the nodes request at the same time and this will result in less processing delay as well as will save the energy of the processing nodes. Hence it will be energy efficient technique.

4. CONCLUSION

The main purpose of this paper is to provide secure data communication among sensor nodes. The proposed model uses Kerberos authentication services in clustered sensor network. This will help to detect unauthorized objects in cluster itself rather than detecting it in complete network. On implementing Kerberos technique in every cluster will save the time as well as will improve the lifetime of the sensor nodes in wireless sensor network. Future work will include the implementation of this proposed technique in every possible scenario.

5. REFRENCES

[1]Kurose JF and Ross KW, Computer networking, a top-down approach featuring the internet, *third edition.Addison Wesley*, Reading, MA,2005.

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

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

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

[5] 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

[6] 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

[7] Qasim Siddique, Kerberos Authentication in Wiireless Sensor Networks, *Annals. Computer Science Series. 8th Tome 1st Fasc*,2010.