Securing Spontaneous Wireless Ad-Hoc Networks – A Real Time Approach

Miss. Megha Ashok Patil
Dept. of Computer Networking
KSIET, Hingoli,
India

Dr. R. R. Sawant
Dept. of Computer Networking
KSIET, Hingoli,
India

Abstract — **The popularity of mobile devices and wireless networks has significantly increased over the recent years. With the advancement of wireless technologies like Wi-Fi, Bluetooth, a new concept of networking has emerged. Spontaneous wireless ad hoc network is an emerging model of wireless communication, for wireless devices i.e. nodes, which forms for certain period of time, with independent central server, having no interference from an expert user, at the same place. When these devices interconnect with each other, trust is based on the first visual contact between the users of these devices; we present a symmetric key protocol for creation and management of spontaneous wireless ad hoc network, without any fixed infrastructure. It contains all functionalities required to operate without any external support.**

Keywords— Spontaneous wireless AD Hoc Networks, nodes.

I. INTRODUCTION

When a set of mobile devices come within the defined range of wireless links and participate an setting up a wireless ad hoc networks for interaction, sharing resources is called as spontaneous wireless ad hoc network. Spontaneous wireless ad hoc networks are infrastructure less networks because they don't need any supporting infrastructure [1], [2]. Authentication is based on first visual contact, as it come in the network range of wireless networks, our proposal is based on underlying technology Wi-Fi, authentication in spontaneous networks provides secure communication by preventing unauthorized usage.

A spontaneous wireless ad hoc network enables, a group of users to communicate with each other, also they are very close to each other sharing services, during a certain period of time. Device used in this networks are usually having limited resources, low energy consumption [1]. Nodes are able to enter or leave the network and they are portable lack of infrastructural support and susceptible wireless lick attacks security in ad hoc come inherent weakness providing adequate security mechanism, for ad hoc network is a challenging task. As the spontaneous wireless ad hoc networks do not have any predefined infrastructure, all the network services are configured on the fly. Due to this reason security is a critical issue. Since nodes use the open radio medium in a potentially insure environment, they are particularly prone to malicious attacks, such as denial of service [10].

II. SECURE SPONTANEOUS PROTOCOL

A spontaneous wireless ad hoc network is formed by wireless nodes, when they meet in a physical place in a concrete time. Devices co –operate in order to provide services, such group or node to node communication application execution, resources sharing. In our protocol the service integration is performed automatically with minimum intervention of user because this network is purposefully intended to be used by non-expert users.

When a new device wants to join the network it must follow the following steps [4].

i) Integrate the device into the network.
ii) Discover the services and resources offered by the network.
iii) Access the services offered by the network.
iv) Perform collaborative tasks.

We have implemented session key revocation system in our protocol in order to grant or revoke services to network nodes based on trust relationship. Nodes can use services only until it is trusted; if it achieves trust again it can use services.

III. WORKING OF PROTOCOL

Security is established based on the service required by the users, by building a trust network to obtain a distributed certification authority. A user is able to join the network because he/she knows someone that belongs to it. There are no anonymous users, because confidentiality and validity are based on user identification. Our protocol helps to create secure spontaneous wireless ad hoc network which will be distributed in nature with the help of different mobile devices, cooperation among these nodes. Operating procedure is as follows.

1. Network Setup
2. Trusted User and node creation
3. New node Joining
4. New network creation
5. Data transfer

1. Network Setup

The user can register and login with the owner permission whether to join new node and or an existing node or to create a network. The owner provides session key based on the requirements of the trusted user.

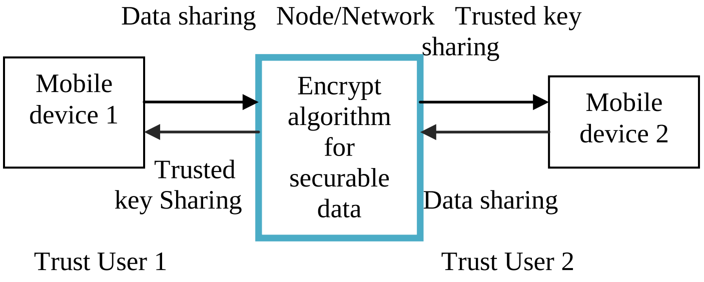

Fig1: Architecture diagram for Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation

2. Trusted User and node creation

In this module, the trusted user gets login by admin permission. The data is shared between two trusted users by session key generation for their respective data's and encrypting their files. The user can only access the services with the encrypted key if the user has the privilege to access the service. Validation of integrity and authentication is done automatically in each node. And this forms a Spontaneous Wireless Ad Hoc node creation between trusted authorities (users).

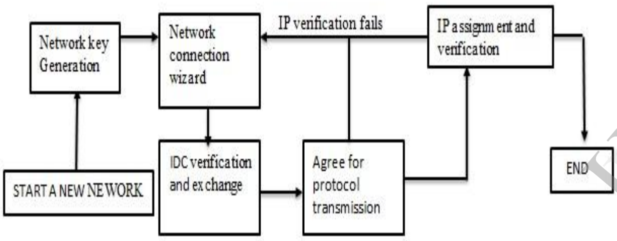
Network key Generation
Network connection wizard
IP verification fails
IP assignment and verification
START A NEW NEWORK
IDC verification and exchange
Agree for protocol transmission
END

Fig2: Architecture diagram for new node joining.

3. New node Joining

The joining module is done with 3 phases:

(1)Joining Procedure

After joining the node, they are provided with IDC(Identity card and Certificate). This system enables us to build a distributed certification authority between trusted nodes. For e.g. When node A wants to communicate with another node B and it does not have the certificate for B, it requests it from its trusted nodes. After obtaining this certificate the system will validate the data; if correct then it will sign this node as a valid node.

(2)Services Discovery

If a node asks for the available services. Services can be discovered using Web Services Description Language (WSDL).

(3)Establishing Trusted Chain and Changing Trust Level

There are only two trust levels in the system. Either a node A trusts another node B or it doesn't trust it. Trust relationship can be asymmetric.

4. New network creation

In this module, we create a new network for the trusted users. First node in the network will be responsible for setting the global settings of the spontaneous network. The second node first configures its user data and network security.

Our protocol relies on a sub layer protocol **Wi-Fi.** After encountering the device, the authentication request is sent to another user, if authentication is accepted, it asks for data exchange. If failed the device won't exchange data. The authenticated node can perform the following tasks:

- Display the nodes.
- Modify the trust of the nodes and Update the information.
- Send data to all nodes.
- Leave the network.
- Process an authentication request etc., based on a secure protocol for spontaneous wireless ad hoc network.

5. Data transfer module

A node receives a data packet that is encrypted with AES algorithm. When the server process received the packet, it is decrypted at the user side.

IV. PERFORMANCE ANALYSIS

Following graph shows the memory consumed, when a new node joins a spontaneous network, by both nodes, for all the processes required to set up and maintain the network.

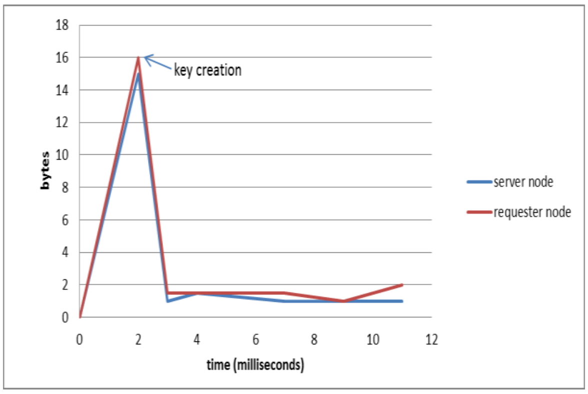

Fig3: Memory used by both nodes from the certification creation to the data transfer.

V. CONCLUSION

We designed a secure spontaneous protocol in a user friendly manner that permits the creation and management of spontaneous wireless Ad Hoc network which is reliable for communication among participants of network. It imitates human relationship. Each user try to maintain the network by maintain trust. The security proposals such as DOS attack removal enables secure communication in spontaneous infrastructure less network. Power consumption is major factor in this network hence we used smaller key size which results in both computational capacity and low power consumption.

VI. REFERENCES

[1] Raquel Lacuesta, Jaime Lloret, Senior Member, IEEE, Miguel Garcia, Student Member, IEEE, and Lourdes Pen˜ alver-“ A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation”- IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 4, APRIL 2013.

[2] L.M. Feeney, B. Ahlgren, and A. Westerlund, “Spontaneous Networking: An Application-Oriented Approach to Ad-hoc Networking,” IEEE Comm. Magazine, vol. 39, no. 6, pp. 176-181,June 2001.

[3] S. Preuß and C.H. Cap, “Overview of Spontaneous Networking -Evolving Concepts and Technologies,” Rostocker Informatik-Berichte, vol. 24, pp. 113-123, 2000.

[4] R.Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver, “A Spontaneous Ad-Hoc Network to Share WWW Access,” EURASIP J. Wireless Comm.And Networking, vol. 2010, article 18, 2010.

[5] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, “ASurvey of Key Management Schemes in Wireless Sensor Networks,”Computer Comm., vol. 30,nos. 11/12, pp. 2314- 2341, Sept. 2007.

[6] J.Latvakoski, D. Pakkala, and P. Paakkonen, “A CommunicationArchitecture for Spontaneous Systems,” IEEE Wireless Comm.,vol. 11, no. 3, pp. 36-42, June 2004.

[7] S. Zhu, S. Xu, S. Setia, and S. Jajodia, “LHAP: A Lightweight Hop by- Hop Authentication Protocol For Ad-Hoc Networks,” Ad Hoc Networks J., vol. 4, no. 5, pp. 567-585, Sept. 2006.

[8] R. Lacuesta and L. Pen˜ alver, “Automatic Configuration of Ad-Hoc Networks: Establishing Unique IP Link-Local Addresses,” Proc. Int’l Conf. Emerging Security Information, Systems and Technologies (SECURWARE ’07), 2007.

[9] L.M. Feeney, B. Ahlgren, A. Westerlund, and A. Dunkels,“Spontnet: Experiences in Configuring and Securing SmallAd Hoc Networks,” Proc. Fifth Int’l Workshop Network Appliances,Oct. 2002.

[10] Engr. Saad Masood Butt,”A Survey of Security Approaches For Wireless Adhoc Networks”, IJMST, Vol 1;Issue1 Paper 4, March 2013