ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

An Impulsive Wireless Adhoc Network for Secured Protocol

Chandra Mounika P[1], Subba Rao k[2]

PG Scholar, Software Engineering, LBRCE, Mylavaram, India[1]

Professor, Information Technology, LBRCE, Mylavaram, India[2]

Abstract: Mobile Adhoc network is a group of wireless nodes that form a network without any kind of infrastructure support. Security in wireless adhoc networks is hard to transmit the data. By using an impulsive wireless adhoc network we can easily provide security for the data transmission. An impulsive adhoc network uses hybrid even symmetric or asymmetric keys. It establishes trust between users in order to exchange the secret keys to encrypt the data. Depending on first visual contact the trust will be based among users. Our proposal is a complete protocol towards oneself safe convention that can make the users to share information in secured manner. This protocol contains all functions required to operate without any external support. It has been verified and implemented in order to check the performance and procedure of protocol in adhoc networks.

Keywords: Impulsive, data transmission, security, hybrid scheme, session keys.

I. INTRODUCTION

A wireless adhoc network is a decentralized type of network. It is adhoc because it does not rely on pre-existing infrastructure such a routers in wired networks or access points in wireless networks. These networks are referred to any set of networks [1] [3]. Each device in MANET is free to move independently in any direction and can change its link to other device often. The main challenge in building a MANET is equipping each device to maintain continuous information required to proper route traffic as shown in fig.1.[2] So that they may operate themselves or may connect to large networks.

First, the network must operate independent of an access point infrastructure, even the connectivity among nodes changes rapidly. Second, the network must operate independent of a pre-established or centralized network management infrastructure, while still providing administrative services needed to support application.

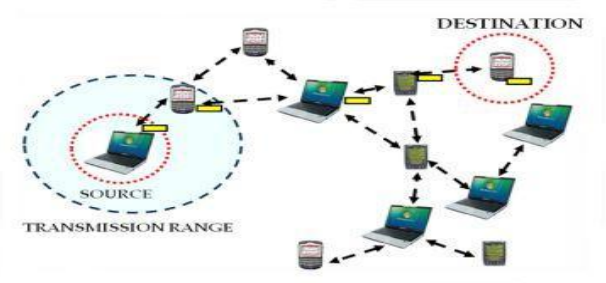

Fig. 1. Data transmission in wireless networks

II. IMPULSIVE NETWORK

Impulsive adhoc networks are formed by set of mobile terminals. These are used to communicate with each other, sharing resources, services or computing time during a limited period of time as shown in fig.2. These types of networks have no dependent centralized servers [5][6]. Impulsive networks can be wired or wireless networks. Tasks that are performed in these networks are User identification, authorization, service name, address to be assigned, security and operation [8]. It includes powerful host machines such as PDAs, laptops and mobile phones.

Impulsive network contains the following features:
1. Network boundaries are poorly defined.
2. The network is not planned.
3. Hosts are not preconfigured.
4. No central servers are required.
5. Users are not experts.

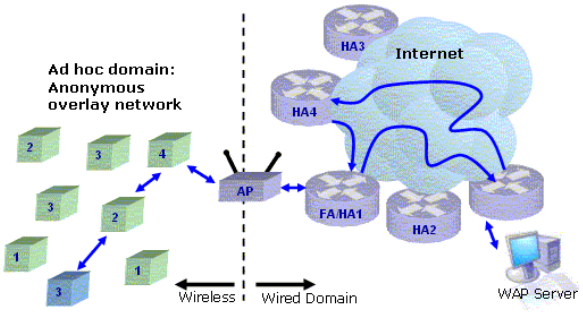

Fig. 2. Impulsive network creation

III. PROCEDURE

Impulsive adhoc networks are formed by a set of mobile terminals that are placed in a close location to communicate with each other, sharing resources, services or computing time during a limited period of time and in limited space forms. These types of networks have no dependent centralized servers.

A. Network Joining

This step allows the device to communicate with each other including the automatic configuration of logical and physical parameters. The system is based on the certificate and an identity card (IDC).[1][3] The IDC contains two types of components such as public and private components in which the public component contains a Logical Identity (LID).A LID is unique for every user and allows nodes to identify it. Then the data is signed with user's private key using Secure Hash Algorithm (SHA-1)

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

to obtain IDC signature of user [2]. No Central authority like certification authority is used to validate IDC.At each node the integrity and authentication is done automatically. The certification authority among trusted nodes is enabled by the system.

B. Trusted chain creation

This system consists of two trust levels. Node A either trusts or does not trust another node B. The node A trusts node B when it receives the validate ID from B. The relationship can be asymmetric. If node A did not want to establish the trust level with node B can go through trusted chains. Depending upon the nodes behaviour over time the trust level can be changed[4]. It can stop trusting if it identifies that trust chain does not exist

C. Protocol Management

By using the information given by the user, network creation will be done. Each node in the network will be identified by an IP address [10][11]. It is very difficult for users to remember the IP address, but using distributed DNS we can reduce the overhead of network.

By completing the authentication process each node gets information such as public key, LID from other nodes in the network.[10] If there are any changes in the network the information will be automatically updated using distributed CA's. So there is no need of central authority.

IV. IMPLEMENTAION OF NETWORK PROTOCOL

This protocol allows creating the independent and decentralized impulsive networks. The co-operation among the nodes allows for group services, communication and security. The first node plays a key role in establishing the impulsive network. Each node must configure their own data which includes IP port and user data. Node must configure with their logical and physical parameters when joining to network. Internet access in the impulsive network could be more than one and every node must share different services among themselves. When users want to join network can follow the following ways:

1. Identification of node
2. Authentication of node in network
3. Address assignment of nodes.

A. Security

Portable nodes that need to communicate with each other are reduced time slot for the formation of impulsive adhoc networks. The problem of adhoc networks are similar to these networks, but are increased because they are formed by temporal networks given by group of nodes in which users do not know about creation, when nodes do not know with each other and also the phase of connection establishes and initial key exchanges takes place[7] [10]. Security requirements in traditional and impulsive network are same such as privacy, integrity, verification, confidentiality and availability.

The configuration service depends on the size of the network. By comparing impulsive with traditional network two fundamental areas must be addressed. At first, there must be a trust formation, key management and membership control. And second there must be network availability and security routing.

B. Authentication Procedure

The authentication process for new device B is shown in fig.3. The node A validates the received data and sends broadcasting message to B in order to check whether the data is used in the network [8] [11]. IP address checking packet is sent for two times randomly to avoid simultaneous checks and reach all devices. When the IP checking packet was received by the authenticated device, it sends the authentication reply to the new devices. If any wrong step is taken place an error message is sent to the newly authenticated node, so that it is able to perform several network operation and configuration task. So that some of them are transparent.

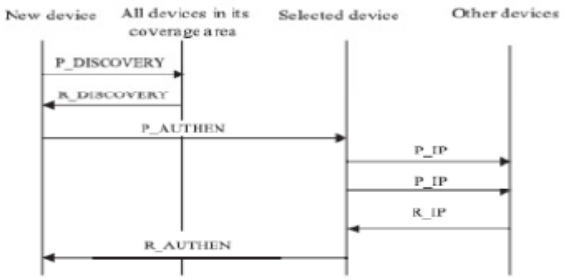

Fig.3 Authentication Procedure

C. Session key

An impulsive network is established for a limited period of time. The user certification has an expiration time. After the expiration time, user can authenticate with the node in network or else node will be blocked. Session key revokes periodically because it has an expiration time [6] [11]. A node must keep session key until it leaves the network. If node is disconnected from network and session key has been re-newed and will not be able to become part of network until again authentication with some other node in the network.

V. CONCLUSION

In this paper, the protocol design will helps to build a secure network. This network is a social network also related to human relationship. It provides unique identity for each node. Security has been provided with various cryptographic techniques. It is a user friendly application with minimum user interaction. Also we can add access control list over shared resources to provide more security from unauthorized user. And we have proposed some procedures for self-configuration like assigning unique IP address to each device, managing DNS and accessing the services automatically. It also provides more security to data sharing with intrusion detection.

REFERENCES

[1] 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.

[2] J. Lloret, L. Shu, R. Lacuesta,and M.Chen, "User-Oriented and Service-Oriented Spontaneous Ad Hoc and Sensor Wireless

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Networks," Ad Hoc and sensor Wireless Networks,vol.14,nos.1/2,pp.1-,2012
[3] S. PreuB 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. Gracia, and L. Penalver, " A Spontaneous Ad-Hoc Network to share WWW Access," Eurasia J. Wireless comm..And Networking, vol.2010, article 18, 2010.
[5] Nayana K, Sangeethaa Sukumaran, " Spontaneous Adhoc Network Creation Using Distributed Dns,"vol.3 2014
[6] Zhiqiang shi, Ionescu, D., Dongli Zhang, "A Token Based Method for congestion and Packet Loss Control " Latin America Transactions, IEEE (Revista IEEE America Latina) (Volume:11, Issue:2) March 2013.
[7] Raju K P, Sandesh Kumar B V," Data transmission using Secure Protocol for Spontaneous Wireless Ad Hoc Networks", IJETT, volume 12 number 3-jun 2014
[8] Y. Xiao, V. k. Ravi, B.sun, X. DU, F .Hu,and M. Galloway, "A survey of key management Schemes in Wireless Sensor Networks, "Computer comm., vol.30, nos.11//12,pp.2314-2341,sept.2007.
[9] Nikhil Varghane, Bhakti Kurade, Chandra as Pote, "Network Creation for spontaneous Wireless ADHOC Network", vol.3 Issue.2,Feb 2014.
[10] M. Mukesh and K.R. Rishi," Security Aspects in Mobile Ad Hoc Networks (MANETS): Technical Review," Int'1 J. Computer Applications, vol.12,no 2,pp.37-43,dec.2010.
[11] R.Lacuesta and L.Penaver, "IP Addresses Configuration in Spontaneous Networks," Proc. Ninth WSEAS Int'1 conf. Computers (ICCOMP'05), July 2005.

BIOGRAPHIES

Chandra Mounika P is a PG Scholar in Software Engineering, Lakireddy Bali Reddy College of Engineering, and Mylavaram.

Dr. K. Subba Rao, M. Tech. (S.E), PhD Working as Professor in Department of IT, Lakireddy Bali Reddy College of Engineering, Mylavaram.

DOI 10.17148/IJARCCE.2015.4663