Creation of Authenticated Protocol for Impulsive Wireless Ad hoc Networks

M. Geetha
M.Tech: Department of CSE
SIETK, Puttur, INDIA

G. Prasad babu M.E
Associate Professor
Department of CSE
SIETK, Puttur, INDIA

P. Nirupama M.E
Head of the department
Department of CSE
SIETK, Puttur, INDIA

Abstract- **An authenticated protocol is presented for routing purposes based on user trust and also describes the way how to use the authenticated protocol In order to create an impulsive wireless Ad Hoc networks which will be used in order to exchange the initial data and the secret keys. This protocol is also used for intruder detection i.e. detecting malicious nodes in the network. The secret keys will be used to encrypt the data. The authenticated protocol will run on the basis of the symmetric / asymmetric scheme and the trust between the users. Trust will build upon direct contact (Face-to-Face) between the users. Our proposed protocol is an automated one which can create the network and share the services through that network securely without any infrastructure. This authenticated network not only allows sharing the services but also allows starting new services among the existing users in it in secured way. There is no intermediate of external support, this protocol itself have all the functions needed. This abstract follows clear explanation of different stages in network, the communication, protocol messages and the network management.**

***Keywords-* Authenticated protocol; ad-hoc; Impulsive network; Security; Intrusion detection;**

I. RELATED WORK

An Adhoc Network is a connection of wireless systems, transferring data between themselves with no pre-existing infrastructure available. Adhoc networks are now important because of their independence of pre-existing fixed infrastructure and can be quickly deployed when needed and inexpensively too. Due to their independence of pre-existing infrastructure and pre-configuration there exists many problems. Some of them are solved as explained below

One of the main problems when configuring ad-hoc networks is that in these networks they don't have a central server with all the information of the network. If a new user wants to become as a part of a network he must configure his device firstly. So, Raquel Lacuesta Gilaberte and Lourdes Peñalver Herrero [2] proposed a distributed protocol to network data configuration based on the use of diffusion tools (multicast/broadcast) and where the user's intervention isn't necessary. The protocol focuses on IPv4 link-local addresses configuration to make the creation of MANETs (Mobile Ad hoc Networks).The proposed protocol is based on the use of a distributed service among the devices that form the network, which allows us to configure the nodes of an ad hoc network in an automatic form. In this the node's IP addresses configuration will have two main phases: first, a local connection address must be generated by the node which wants to form part of the network, second, the not duplicity of the proposed IP must be checked by one of the nodes that are already part of the network, to perform this checking the node must use broadcast/multicast techniques sending a packet which was configured with the proposed IP as target node. If a node is already using this IP, it responds to the source node, in this case the IP can't be used by the new node and it has to generate a new IP proposal. This protocol is efficient only where nodes can have limited resources and the network can have a dynamic topology.

L.M Feeney [3] discussed about the automatic/dynamic configuration, security and peer to peer operation. In automatic/dynamic configuration there are two existing technologies being developed within the Internet Engineering Task Force (IETF) that can be leveraged to implement this: IPv6 stateless address configuration and zero configuration networking. In security, Authentication in the spontaneous network can leverage the fact that the network is created by people, who inherently implement complex trust models while interacting with each other. In peer to peer operation Jet File is a distributed file system largely based on peer-to-peer communication. Nodes share data with each other without going through any central server. The function that is not delegated to the participating nodes is keeping track of the latest version of each file.

Marc Danzeisen [4] implemented a cellular framework for successful spontaneous network establishment. This offers a dashboard-like tool, which can, with the help of a cellular network, ease the formation of spontaneous networks among heterogeneous nodes. Furthermore the provided implementation is able to secure the acquired communication links in the spontaneous network and therefore protect the exchanged information against possible abuse.

Most ad hoc networks do not implement any network access control, leaving these networks vulnerable to resource consumption attacks where a malicious node injects packets into the network with the goal of depleting the resources of the nodes relaying the packets. To thwart or prevent such attacks, it is necessary to employ authentication mechanisms that ensure that only authorized nodes can inject traffic into the network. So S. Zhu, S. Xu [5] presented LHAP a scalable and light-weight authentication protocol for ad hoc networks. LHAP is based on two techniques: (i) hop-by-hop authentication for verifying the authenticity of all the packets transmitted in the network and (ii) one-way key chain and TESLA for packet authentication and for reducing the overhead for establishing trust among nodes. The security of LHAP is analyzed and shown LHAP is a lightweight security protocol through detailed performance analysis.

Fundamental aspect in wireless network creation & wireless communication is use of security so a secure protocol is proposed by Raquel Lacuesta [1] for spontaneous wireless ad hoc network which uses an hybrid public, private key scheme and the trust between users in order to exchange the initial data and to exchange the secret keys that will be used to encrypt the data. It presents a securityprotocol for routing purposes, based on trust. It presents two secure and energy-saving spontaneousad hoc protocols for wireless mesh client networks where two different security levels (weak and strong) are taken into account in the path when information is transmitted between users.

The proposed protocol is more efficient than previous secure protocol. In these adhoc networks intruders who enter into the network are detected in our paper.

II. INTRODUCTION

A wireless ad-hoc network is a collection of mobile/semi-mobile nodes with no pre-established infrastructure, forming a temporarynetwork. Each of these nodes has a wirelessInterface and communicates with each otherover either radio or infrared. Laptop computersand personal digital assistants(PDA'S) thatcommunicate directly with each other aresome examples of nodes in an ad-hoc network.In the ad-hoc network nodes are often mobile,but can also consist of stationary nodes, suchas access points to the Internet. Semi mobilenodes can be used to deploy relay points inareas where relay points might be neededtemporarily. Wireless networking is anemerging technology that allows users to access information and services electronically,regardless of their geographic position [6].

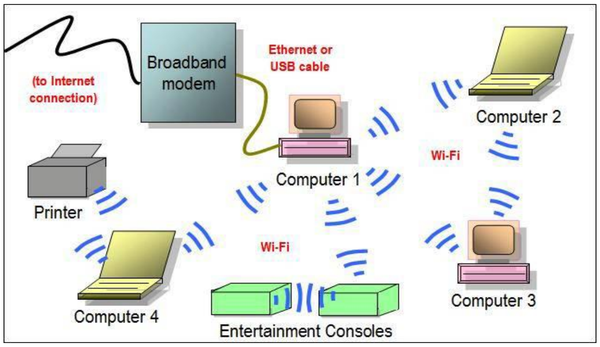

Figure 1: wireless ad hoc network

There are five key challenges in wireless ad hoc networks. They are:

1. Network boundaries must be poorly defined
2. The network is not planned before
3. Hosts are not pre-configured earlier
4. There are no central servers in the network
5. Users may not be experts

There are some characteristics for impulsive networks:

1. Wireless communication
2. Mobility
3. Do not need infrastructure
4. but can use it, if available
5. small, light equipment

Intrusion detection system (IDS) [7] plays an important role in detecting different types of attacks. In general, the main function of intrusion detectionsystem is to protect the network, analyze and find out intrusions among audit and normal audit data, and this can be considered as a classification problem. Intrusion detection system can be mainly classified into two methods i.e. misuse detection and anomaly detection n methodsbased on detection method. The misuse detection method runs on database of well-known attack signatures; the system stores patterns (or signatures) of known attacks and uses them to compare with the actual actions. Anomaly-based intrusion detection is another process to intrusion detection. Anomaly detection works on the principle that "attack behavior" is somewhat different from "normal user behavior". Thereare some Anomaly detection algorithms thathave the advantage over a signature-based detection that they can also detect novel attacks. In spite of this, Anomaly detections methods are able to detect new types of intrusions, most of these anomaly-based IDSs affected from a high rate of false alarms due to a shortage in their discrimination ability.

III. WORKING OF PROTOCOL

This authentication protocol is used to create and manage the distributed and decentralized impulsive networks with small interaction of user and integration of distinct devices (mobile phones, laptops, PDA'S etc.). Cooperation between distinct devices provides different services like security, data delivery, group transmission etc. In order to create an impulsive network, follow the steps mentioned below:

1. Joining a new node
2. Accessing the services
3. Constructing trust chain

A. Joining a new node

Network based Intrusion Detection System (NIDS) is used to create a new node and join it to an existing node by following respective procedures given by host. After joining the node, they are provided with an IDC (Identity card) and certificate. This IDC contains both public key and private key, whereas public key contain user information like user name,user id ,IP address etc. and private key contain user signature.The certicate authority can be given by any one of the node already present in the network, so it enables us to build a distributed certification authority among trusted nodes.

For example, if node B wants to join the network, then it has to generate a network key, after that we have to check whether there is a new network connection or not. If yes, exchange the IDC with node A then the node B is authenticated, and check for whether it agree transmission protocols and speed or not. If yes,IP assignment is done then check whether there is any IP duplication or not.If there is any duplicate IP address then the process will begin again as shown in algorithm below.

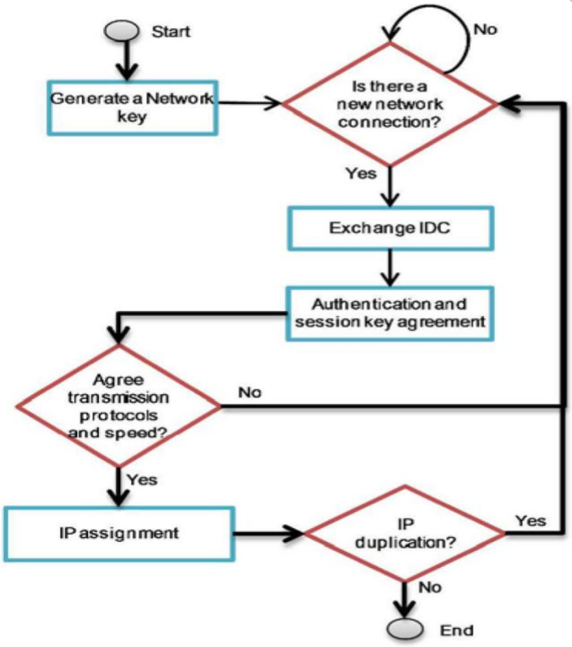
Start
Generate a Network key
Is there a new network connection?
No
Yes
Exchange IDC
Authentication and session key agreement
Agree transmission protocols and speed?
No
Yes
IP assignment
IP duplication?
Yes
No
End

Figure2: Algorithm for joining a new node in network

B. Accessing the services

All the nodes present in the network has the agreement with each other for accessing the services.A node can ask other devices to know available services. Those services can be discovered by Web Services Description Language. This impulsive networks does not use any central server, but other service discovery mechanisms are used[8].To transform the information between users the fault tolerance is based on the routing protocol. Services provided by A are accessible only if there is a path to A, if there is no path to A the service will automaticallyget disappear [3]. Each and every node present in the network can request the services from all the other nodes that it trusts.The trust is developed only when there is a direct contact between users. A request to several nodes is made through diffusion processes. When the data or information cannot be received throughthese nodes, it can then ask other nodes. The information in network can also be updated by sending requests from one node to other. The reply will contain the IDC's of all nodes in the network. Authentication is provided to the information sent by these nodes. If the information is received from a trusted node then its validity is also done, since trusted nodes have been responsible for authenticating their previous certificates. So, by this method any type of service can be implemented securely.

C. Constructing trust chain

We consider only two trust levels in the system, either trust or does not trust. Node A either trusts or does not trust another node B. The user interface of application installed in the device asks B to trust A when it receives the validated IDC(Identity card) from A. Trust relationship can be asymmetric. If node A did not generate trust level with node B directly, it can be established through trusted chains network, e.g., if A node trusts C node and C node trusts B node, then A node may trust B node. Trust level can change over time depending on the node's behavior. Thus, node A may decide not to trust node B although A still trusts C and C trusts B. It can also stop trusting if it discovers that previous trust chain does not exist anymore [1]

IV. CONCLUSION

We designed an authenticated protocol for impulsive wireless adhoc network, which allows creation and management of the network. The security is established based on the face to face contact between the users. It helps us to avoid the intruders accessing the services. To transfer the information between users we used the symmetric/asymmetric schemes. This allows the secure communication between the end users.

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] 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.

[3] 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.

[4] M. Danzeisen, T. Braun, S. Winiker, D. Rodellar, "Implementation of a Cellular Framework for Spontaneous Network Establishment,"Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005.

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

[6] Rahul malhotra,Gurpreet Singh "An overview of on demand wireless adhoc networks protocols: DSR and TORA"Int. J. Comp. Tech. Appl., Vol 2 (5), 1641-1651

[7] Nikhil Varghane, Prof. Bhakti Kurade, Prof. Chandradas Pote "Intrusion Detection, Secure Protocol &Network Creation for Spontaneous Wireless AD HOC Network"IJCSMC, Vol. 3, Issue. 2, February 2014, pg.389 – 394

[8] L. Liu, J. Xu, N. Antonopoulos, J. Li, and K. Wu, "Adaptive Service Discovery on Service-Oriented and Spontaneous Sensor Systems," Adhoc and Sensor Wireless Networks, vol. 14, nos. 1/2, pp. 107-132, 2012.