Data transmission using Secure Protocol for Spontaneous Wireless Ad Hoc Networks

Raju K P¹, Sandesh Kumar B V².

¹Electronics & Communications, S J B Institute of Technology, Bangalore, India.
²Asst. professor, Electronics & Communications, S J B Institute of Technology, Bangalore, India.

Abstract:- Ad-Hoc wireless network is an infrastructure less network, i.e. there is no centralized coordination for the network operations. As and when a new node comes in the vicinity of the network it will spontaneously form the network. This paper presents data transmission using a secure protocol for spontaneous wireless ad hoc networks which uses an hybrid symmetric/asymmetric 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. Our proposal is a complete self-configured secure protocol that is able to create the network and share secure services without any infrastructure. Network creation stages are detailed and the communication, protocol messages, and network management are explained. Our proposal has been verified and implemented in order to check the procedure and performance of the protocol in ad hoc networks.

Keywords:- Data transfer, spontaneous wireless network, Ad-hoc network, secure protocol.

I. INTRODUCTION

Spontaneous ad hoc networks are formed by a set of mobile terminals placed in a close location that communicate with each other, sharing resources, services or computing time during a limited period of time and in a limited space, following human interaction pattern. People are attached to a group of people for a while, and then leave. Network management should be transparent to the user. A spontaneous network is a special case of ad hoc networks. They usually have little or no dependence on a centralized administration.

We consider only wireless spontaneous networks in this paper. Their objective is the integration of services and devices in the same environment, enabling the user to have instant service without any external infrastructure. Because these networks are implemented in devices such as laptops, PDAs or mobile phones, with limited capacities, they must use a lightweight protocol, and new methods to control, manage, and integrate them. The existing papers propose a secure spontaneous network protocol based on user trust that provides node authenticity, integrity checking, and privacy.

The network and protocol proposed in this paper can establish a secure self-configured environment for data distribution and resources and services sharing among users. 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. Thus, the certification authority is distributed between the users that trust the new user. We apply asymmetric cryptography, where each device has a public-private key pair for device identification and symmetric cryptography to exchange session keys between nodes[1]. There are no anonymous users, because confidentiality and validity are based on user identification.

II. METHODOLOGY

Our protocol permits the creation and administration of distributed and decentralized spontaneous networks with little mediation from the client, and the incorporation of distinctive gadgets (PDAs, cells, ...
laptops, and so on.). The data transmission with security can be obtained[2].

II.a. SPONTANEOUS NETWORK SECURITY PROCEDURE FOR JOINING THE NETWORK.

This step enables devices to communicate, including the automatic configuration of logical and physical parameters. The system is based on the use of an IDentity Card (IDC) and a certificate. The IDC contains public and private components. The public component contains a Logical Identity (LID), which is unique for each user and allows nodes to identify it. Then, the data summary is signed with the user’s private key. The routing protocol used here is GPSR (greedy based and perimeter based).

II.b. CREATING TRUSTED CHAIN.

There are only two trust levels in the system. Node A either trusts or does not trust another node B. The software application installed in the device asks B to trust A when it receives the validated IDC from B. Trust relationship can be asymmetric. If node A did not establish trust level with node B directly, it can be established through trusted chains, e.g., if A trusts C and C trusts B, then A may trust B.

II.c ENCRYPTION AND DECRYPTION OF DATA.

In this paper we use the rsa algorithm for encryption and decryption of data. The private key and public keys are also created using the same algorithm.

II.D. MANAGEMENT OF PROTOCOL AND NETWORK.

The system is created utilizing the data gave by users, hence, every node is distinguished by an IP address. Administrations are imparted utilizing TCP associations. The network is constructed utilizing IEEE 802.11b/g technology which has high information rates to impart or share resources. We have saved the short-range technology (Bluetooth) to permit verification of nodes when they join the system. After the authentication process, each node learns the identity card of other known nodes, a public key and a LID. This information will be updated and completed throughout the network nodes. This structure provides an authenticated service that verifies the integrity of the data from each node.

II.E. PROTOCOL OPERATION.

In order to design the diagrams of the protocol, we have used the Unified Modeling Language (UML). The UML is a visual specification standardized language that is built to model object oriented systems. We use keys, activities, and use cases (diagrams offered by the standard) to define the processes, the structure of the classes in the system, and the behavior of objects or operations. Once the validation/registration process of the user in the device has been done, he/she must determine whether to create a new network or participate in an existing one. If he/she decides to create a new network, it begins the procedure shown in Fig2. The authentication process will be followed by each and every node. And later the IP assignment of nodes will be performed.

The authenticated node can perform the following tasks:

- Display the nodes.
- Modify the trust of the nodes.
- Update the information.
- Other nodes certificate request.
- Process an authentication request.
- Reply to an information request.
- Forward an information request.
- Send data to one node.

To request a certificate, the node sends a request certificate message to its trusted nodes. The application generates a packet to request the certificate to its trust nodes which are selected from the database. To process the received request, the node checks if it can reply to the request, if not, the node sends the search to other nodes (that it trusts or known nodes). Then, the node has to validate the
certificate and sends it to the requesting node. When the server process receives the packet, it processes the packet in order to take the certificate and checks its validity access to the certificate data. Fig.4 shows the steps of this procedure

### III. IMPLEMENTATION OF PROTOCOL

When a device wants to join a spontaneous network it has to start the process by sending a Discovery request packet (01), which contains the Logical IDentity of the user in order to let the destinations know the sender device receivers will reply with the Discovery reply packet (02) with their Logical Identity, their IP address, and network veil. This information is then used to take in the chose device to validate and to propose an IP inside that network IP range. The authentication demand packet (03) is utilized for the new device authentication.

The authentication reply packet (04) affirms that the proposed IP and the email are novel in the network, so the new device is authoritatively verified. In the event of duplication, a blunder packet is sent. The IP and email checking packet (05) is utilized by the authenticator device to check that nobody in the network has the same email or IP address as the one proposed by the new device. The IP and email checking reply packet (06) is sent to the authenticator device in place to check that the IP and email are special.

In the event that the IP is copied, the device must restart the authentication transform after the era of another IP. The redesign demand to one hub (07) is utilized to ask for information to a particular known...
hub and the overhaul reply from one hub (08) is used to reply with the information asked for by the overhaul demand packet to one hub. Obscure information might be asked for from all hubs in the network by sending the overhaul appeal to all network hubs packet by flooding (09). The reply with the information asked for is called overhaul reply to all network hubs packet (10). The Certificate solicitation to trusted hubs (11) and the Certificate solicitation to known hubs (12) are utilized to ask for the certificate from all trusted and all known hubs, individually. Both packets are answered to by the certificate reply packet (13). Data are sent utilizing the Packet for sending data (14). This packet is sent when the user chooses to correspond with one or more hubs. These data could be sent in plain or encoded content. The slip packet (15) can be sent to show that this operation is not conceivable, since the authentication has fizzled, or in light of the fact that the hub does not have the obliged data.

**Fig.6** - Procedure to decrypt an encrypted data packet.

**IV. EXPERIMENTAL RESULTS**

In the fig.7 new incoming node is made to join the network. New incoming node will get authenticated if it has been trusted and later the assignment of address and exchange of public keys will take place between the source node and destination node in order to establish a path for data communication.

In the fig.8 we see that new incoming node that is source node has been connected to the destination node. That a path has been established. In this case the path has been established through other trusted and authenticated nodes. And thus the data can be transmitted with security between the source node and destination node in spontaneously created Ad-hoc network.

The fig.9 shoes the plot of maximum number of nodes vs available memory. Fig.10 shows the plot of network size vs delay.

**Fig.7** - Joining of new node.

**Fig.8** - Path establishment and data transfer.
In this paper, we demonstrate the configuration of a convention that permits the creation and management of a spontaneous wireless ad hoc network to transmit data. It is focused around an informal community impersonating the conduct of human connections. Therefore, every client will work to keep up the network, enhance the services offered, and give data to other network clients. We have given a few methodologies to setup toward oneself, a remarkable IP address is assigned to every gadget, the DNS could be overseen proficiently and the services might be found consequently. We have additionally made an easy to use requisition that has negligible collaboration with the client. A user without advanced technical learning can set up and partake in a spontaneous network. The security plans included in the convention permit secure correspondence between end users (acknowledging the asset, handling, furthermore vitality constraints of ad hoc gadgets). We have performed a successful data transmission in secure Ad–hoc spontaneous network. The protocol can be used in regular resource-constrained devices (cell phones, PDAs, etc.). Enhancement of the protocol can be obtained by using more advanced protocols which can overcome the limitations in GPSR. and the data rates can be improved.

References