Volume : 3 | Issue : 5 | May 2014 • ISSN No 2277 - 8179

Spontaneous Ad HOC Network Creation Using Distributed Dns

Engineering

KEYWORDS :

Nayana K — PG Scholar, Department of Computer Science and Engineering, Vedavyasa Institute of Technology, University of Calicut, Kerala, India

Dr.Sangeethaa Sukumaran — Vice Principal, Vedavyasa Institute of Technology, University of Calicut, Kerala, India

ABSTRACT

This research presents a secure protocol for spontaneous wireless ad hoc networks. The spontaneous ad hoc network is formed by a set of mobile terminals placed in a closed location that communicate with each other. A complete self-configured secure protocol that is able to create the network and share secure services without any infrastructure is proposed .The nodes in the network will share the resources, services or computing time during a limited period of time and in a limited space. In this scheme a hybrid symmetric/ asymmetric mechanism and the trust between users in order to exchange the initial data and to exchange the secret key is adopted. Trust is based on the first visual contact between users. The protocol includes all functions needed to operate without any external support. The design and development is done in devices with limited resources. Various stages in network creation, communication between end users, and network management are explained. The security schemes included in the protocol allows secure communication between end users .Each user will work to maintain the network, improve the services offered, and provide information to other network users .In addition a distributed DNS mechanism is introduced in order to make a user-friendly network.

I. INTRODUCTION

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure.

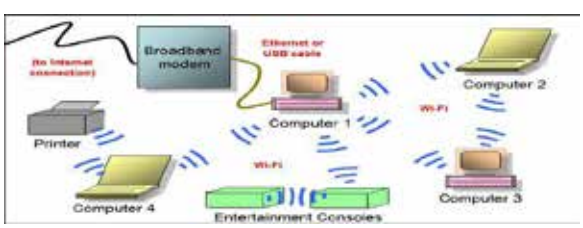

Fig. 1 ad hoc network

A wireless ad hoc network is a decentralized type of wireless network., The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding data.

An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of IEEE 802.11 wireless networks. It also refers to a network device's ability to maintain link status information for any number of devices in a 1-link range, and thus, this is most often a Layer 2 activity. Because this is only a Layer 2 activity, ad hoc networks alone may not support a routable IP network environment without additional Layer 2 or Layer 3 capabilities.

Wireless ad hoc networks can be further classified by their application:

1.1 MOBILE AD HOC NETWORKS (MANET)

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. *Ad hoc* is Latin and means "for this purpose".

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

1.2 ATTACKS

We can classify attacks as passive or active.

Passive Attacks: In a passive attack an unauthorized node monitors and aims to find out information about the network. The attackers do not otherwise need to communicate with the network. Hence they do not disrupt communications or cause any direct damage to the network. However, they can be used to get information for future harmful attacks. Examples of passive attacks are eavesdropping and traffic analysis. Eavesdropping Attacks, also known as disclosure attacks, are passive attacks by external or internal nodes. The attacker can analyze broadcast messages to reveal some useful information about the network. Solutions protecting the radio interface from attacks such as eavesdropping (and jamming) attacks have been proposed in the literature, e.g. spread spectrum communication and frequency hopping .Traffic Analysis is not necessarily an entirely passive activity. It is perfectly feasible to engage in protocols, or seek to provoke communication between nodes. Attackers may employ techniques such as RF direction finding, traffic rate analysis, and time-correlation monitoring. For example, by timing analysis it can be revealed that two packets in and out of an explicit forwarding node at time t and t+€ are likely to be from the same packet flow.

Traffic analysis in ad hoc networks may reveal:

- the existence and location of nodes.
- the communications network topology.
- the roles played by nodes.
- the current sources and destination of communications and
- the current location of specific individuals or functions (e.g. if the commander issues a daily briefing at 10am, traffic analysis may reveal a source geographic location).

Active Attacks: These attacks cause unauthorized state changes in the network such as denial of service, modification of pack-

ets, and the like. These attacks are generally launched by users or nodes with authorization to operate within the network. We classify active attacks into four groups: dropping, modification, fabrication, and timing attacks. It should be noted that an attack can be classified into more than one group.

Dropping Attacks: Malicious or selfish nodes deliberately drop all packets that are not destined for them. While malicious nodes aim to disrupt the network connection, selfish nodes aim to preserve their resources. Dropping attacks can prevent end-to-end communications between nodes ,if the dropping node is at a critical point. It might also reduce the network performance by causing data packets to be retransmitted, new routes to the destination to be discovered, and the like.

Unfortunately most routing protocols (DSR is an exception) have no mechanism to detect whether data packets have been forwarded or not. However, they can be detected by neighboring nodes through passive acknowledgement or hop-by-hop acknowledgement at the data link layer.

An attacker can choose to drop only some packets to avoid being detected; this is called a selective dropping attack. Besides data packets or route discovery packets, an attacker can also drop route error packets, causing the source node to be unaware of failed links (thus interfering with the discovery of alternative routes to the destination).

1.3 SECURITY

Microsoft does not allow advanced encryption and security protocols for wireless Ad hoc networks on Windows. In fact, the security hole provided by Ad hoc networking is not only the Ad hoc network itself, but the bridge it provides into other networks Ad hoc networks can pose a security threat. Ad hoc networks are defined as peer-to-peer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.

1.4 SPONTANEOUS AD HOC NETWORK

A spontaneous ad hoc network is type of ad hoc network that is formed in a certain time during a period of time, with no dependence on a central server and without the intervention of an expert user, in order to solve a problem or carry out a specific task . This network is built by several independent nodes coming together at the same time and in the same place to be able to communicate with each other. Nodes are free to enter and leave the network and they could be mobile or not. Spontaneous networking happens when neighbouring nodes discover each other within a short period of time; however, the velocity of discovery is paid in terms of energy consumption . Spontaneous networks are conceptually in a higher level of abstraction than ad hoc ones; they are basically those which seek to imitate human relationships in order to work together in groups, running on an existing technology. Their objective is the integration of services and devices in an environment which allows the provision to the user of an instant service with minimum manual intervention. The concept of spontaneous networks was introduced in depth by LauraMarie et al.

1.4.1 Features

The main features in spontaneous networks are the following.

(i) Network boundaries are poorly defined.
(ii) The network is not planned.
(iii) Hosts are not preconfigured.
(iv) There are not any central servers.
(v) Users are not experts.

One of the main issues that difference the spontaneous networks from other fixed or mobile networks is that they facilitate the integration of services and devices, setting up both the new services and the configuration parameters of the devices. It has to be done without the user intervention or interference in the operation of the network. The malfunction or failure of one of the devices or services does not compromise the viability of the community. Any resources being used by the community which malfunction are automatically released and the service is deregistered.

A spontaneous network enables a group of devices to work together collaboratively while they are located very close to each other with a minimum interaction. It can be used for sharing resources and internet services. Just one of the nodes has to be connected to Internet to share its connection and its resources to the whole network. Caching techniques are demanded in order to avoid the overload of the nodes. Moreover, configuration with a minimal interaction from the user and security on the communication should be established.

1.4.2 Application

There are many application areas for ad hoc spontaneous networks: industrial (communication between sensors, robots, and digital networks), business (meeting, stock control, etc.), military (hard and hostile environments), and teaching. The range of environments in which these networks can be applied is wide and may include conference services and other "ubiquitous computing" applications at home or office.

The rest of the paper will be organised as follows: In section 2, we see about the related works of the paper. In section 3, we discuss about the existing method. The proposed method is shown in the section 4. The conclusion of our paper is in section 5.

II. Related Works

In this section, we will see some of the related works to using different approaches:

Laura Marie Feeney, Bengt Ahlgren, Assar Westerlund described a Spontaneous networking, an application oriented approach to ad hoc networking [1]. According to them, An ad hoc network must operate independent of pre established or centralized network management infrastructure, while still providing administrative services needed to support applications. Address allocation, name resolution, service location, authentication, and access control politics represent just some of the functionality that must be supported - without pre configuration or centralized services. In order to solve these problems, it is necessary to leverage sonic aspect of the environment in which the network operates. They introduced the notion of *a* spontaneous network, created when *a* group of people come together for some collaborative activity. In this case, we *can* use the human interactions associated with the activity in order to establish *a* basic service and security infrastructure. They structured their discussion around a practical real-world scenario illustrating the use *of* such a network .identifying the key challenges involved and some of the techniques that can be used to address them.

Securing Passive Objects in Mobile Ad-Hoc Peer-to-Peer Networks [2] was presented in the year 2003 by Mayrhofer, F. Ortner, A. Ferscha, and M. Hechinger. According to that security and privacy in mobile ad-hoc peer-to-peer environments are hard to attain, especially when working with passive objects without own processing power. They introduced a method for integrating such objects into a peer-to-peer environment without infrastructure components while providing a high level of privacy and security for peers interacting with objects. The integration is done by equipping passive objects with public keys, which can be used by peers to validate proxies acting on behalf of the objects. To overcome the problem of limited storage capacity on small embedded objects, ECC (Elliptic Curve cryptosystem) keys are used.

III. PROPOSED WORK

3.1 INTRODUCTION

In this paper proposed a spontaneous ad hoc network and protocol .The network can establish a secure self-configured environment for data distribution and resources and services sharing among users. According to the users requirements a security mechanism is established by building a trust network to obtain a distributed certification authority. A user, who has knowledge belongs to the network can able to join the network. A certifi-

cate is distributed among the users in the network. The users in the network can trust the new users by authentication process. For managing the network, a distributive network management is used. There is no any central authority for network management. The distributive network management allows the network to have a distributed name service. Both asymmetric and symmetric cryptography are applied in this network. In the asymmetric application each device has a public-private key pair for device identification. Symmetric cryptography is used for sending message between different nodes in the network by exchanging the session keys between the nodes. Confidentiality and validity is based on user identification ,so there is no any anonymous users. A distributive Domain Name System is introduced in this network in order to make a user-friendly network.

3.2 SECURE SPONTANEOUS AD HOC NETWORK

3.2.1 Network Overview

It is a distributed and decentralized spontaneous ad hoc network with distributed DNS. There is a protocol for the creation and management of the network. The users have little intervention to the network. The network constitute of different devices such as cell phone, Laptop, PDAs etc. Provision and access to different services, such as group communication, collaboration in program delivery, security, etc. are different functions of the network, which can be done by the cooperation of the devices. Any devices can leave or join to the network without any cost, so the network members and services may change at any time. All devices contains the details about other devices currently existing in the network by the distributed structure. Creation procedure for spontaneous ad hoc network as follows.

STEP 1: Joining To the Existing Network

In this step, included the automatic configuration of logical and physical parameters. The network consists an IDC (Identity card) and a certificate for security purposes.IDC has two parts: public component and private component. Logical Id entity is the part of public component. it is used to identify each devices in the network because it is unique for each devices. It may contain information for identity. The user's public key, creation dates and expiration dates, IP address and user signature are also included in the Logical Identity. The SHA-1 algorithm is used for the creation of user signature.

Both IDC and certificate are optionally used for the security purposes.IDC is very important in this paper. All authentication process are done by using this IDC.Each existing device has an IDC.There is no central authority to validate the IDC because it is a distributed network. The authentication is done distributive manner. Each device is authenticated by any other trusted device in the network. Thus a distributed certification authority is exists in the network. If a new node A wants to join in to the existing network and wants to communicate with a node in that network. It request the certificate from a trusted node in that network. If the new node got certificate from the trusted node, then validation is done by the system. After the validation process, the node become another trusted node in that network. Then node can join another new node. All nodes in the network can act as both client and server. All nodes can request for service or authentication process from other nodes.

STEP 2: Services Discovery in The Network

All nodes in the network can add services, update its services, delete its services. Each node has different services. By using the service discovery process, each node can access the services of other trusted nodes in the network. But problem with this procedure is require more manual configuration. One node can access services of another node if it has direct path to that node.ie services discovery takes place only between the trusted nodes in the network.

STEP 3: Establishing Trusted Chain and Changing Trust Level Between The Nodes

There are two level of trust are exist in this network. In the first level, Node A either trust Node B or not. Another one is trust by chaining method. For Example the node A has not a direct trust between the node B.Then it make a trust through trust chain.ie If A trust C, C trust B, then A trust B.

3.3 NETWORK MANAGEMENT AND PROTOCOL USED IN THE NETWORK

At first information needed for the network creation is provided by the user. After getting that information ,network is created. In this network each node is identified by an IP address. But it is very difficult to remember by the user. So here using a distributed DNS which helps to reduce the overhead of the network.

After completing the authentication process, each node got information such as public key, LID from other nodes in the network. These information will be updated whenever there is any change in the existing in the network. Thus a distributed CA is maintaining in the network. So there is no need of any central authority.

There are different services on each node in the network. The nodes can access these services by service request process from trusted nodes. If a node doesn't provide any service to a particular node, then it can access service from another node in that network.

3.3.1 Creation of A New Network

For creating a new network, the first node will have to set up global settings of a spontaneous network. For to become a part of the network, the first node have to configure its own data such as IP, port number, unique id etc..

3.3.1.1 Procedure for joining a new member

The Fig. 3 shows the procedure for network creation. The second node have to perform the procedure as the first node done. Then an authentication is taking place in between these two node, and make a trust in between them. Each node, which wants to join in the network will have to done the procedure that done by the second node.

ACKNOWLEDGMENT

The authors gratefully acknowledge the support and facilities provided by Department of CSE, Vedavyasa Institute of Technology. Authors also extend their thanks to the Head of the Department of CSE Mrs.S.Kavitha Murugesan for his immense help during the course of the project.

REFERENCE

[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] R. Mayrhofer, F. Ortner, A. Ferscha, and M. Hechinger, "Securing Passive Objects in Mobile Ad-Hoc Peer-to-Peer Networks," Electronic Notes in Theoretical Computer Science, vol. 85, no. 3,pp. 105-121, Aug. 2003. | [3] 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. | [4] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: A Lightweight Hopby-Hop Authentication Protocol For Ad-Hoc Networks," Ad Hoc Networks J., vol. 4, no. 5, pp. 567-585, Sept. 2006. | [5] A. Noack and S. Spitz, "Dynamic Threshold Cryptosystem without Group Manager," Network Protocols and Algorithms,vol. 1, no. 1, Oct. 2009. | [6] R. Lacuesta and L. Pen˜ aver, "IP Addresses Configuration in Spontaneous Networks," Proc. Ninth WSEAS Int'l Conf. Computers (ICCOMP '05), July 2005. | [7] J. Latvakoski, D. Pakkala, and P. Paakkonen, "A Communication Architecture for Spontaneous Systems," IEEE Wireless Comm.,vol. 11, no. 3, pp. 36-42, June 2004. |