International Journal On Engineering Technology and Sciences – IJETS™
ISSN (P): 2349-3968, ISSN (O): 2349-3976
Volume 2 - Issue 5, May 2015

On Demand Wireless Network Creation And Management

Faisal E
Student
Kathir College of Engineering
Coimbatore
faisalecse@gmail.com

R.Subathra
Head /Department of CSE
Kathir College of Engineering
Coimbatore

T.K.P Rajagopal
Associate Professor
Kathir College of Engineering
Coimbatore

Abstract— Communication in wireless network is based on client server model where an infrastructure is required between two clients or mobile to communicate with each other even though they are closed to each other. In human communication model, two people those are physically closed to each other can talk directly without any server. Network created on demand is known as spontaneous networks. In spontaneous network there is no server or any infrastructure between nodes to communicate, anybody those who wants to communicate can join, communicate and leave the network without any central server. It is based on peer to peer networking, where nodes can join and leave network and share or distribute information to each other like human communication model. As spontaneous network is self configured a security is a major concern. This paper deals with the security in 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. Trust is based on the first visual contact between users. The network allows sharing resources and offering new services among users in a secure environment. The protocol includes all functions needed to operate without any external support. Network creation stages are detailed and the communication, protocol messages, and network management are explained
.Also intends to add Distributed Domain Name Service by using the Logical Identity(LID) and IP address of the nodes.

Index Terms— **Logical Identity, Ad hoc Network, On Demand Network**

I. INTRODUCTION

The exponential growth in the development and acceptance of mobile communications in recent years is especially observed in the fields of wireless local area networks, mobile systems, and ubiquitous computing. This growth is mainly due to the mobility offered to users, providing access to information anywhere, user friendliness, and easy deployment. Furthermore, the scalability and flexibility of mobile communications increase users' productivity and efficiency.Mobile Ad hoc network (MANET) is a group of wireless nodes that form a network without support of any kind of infrastructure. Following are features of MANET:

o Host movement frequent
o Topology change frequent
o No cellular infrastructure.
o Multi-hop wireless links.
o Data must be routed via intermediate nodes

Here the nodes in the network communicate in a peer-peer manner

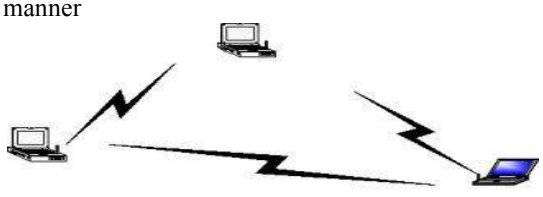

Figure 1.1: adhoc network

In human communication model, people come together form a group and start talking or communicating with each other by sharing their views, information and many more things. During this face to face communication anybody can talk, join or leave the group without taking any permission. There is not any central coordinator.

II. RELATED WORKS

The permanently growing networked IT-infrastructure, the need for more mobility as well as the expansion of computer-aided applications to new areas demand new methods to simplify the handling of IT systems. Spontaneous networking is a means for simple integration of devices and services into networks. It seems to be one way to achieve more flexibility, more mobility, a better usability and less administration effort.

L.M. Feeney, B. Ahlgren, and A. Westerlund have proposed the concept of spontaneous networking in . An ad hoc network work independent of any infrastructure but for some functionality such as address allocation, name resolution, service location, authentication, and access control policies, they required some administrative services. In order to solve these problems, it is necessary to leverage some aspect of the environment in which the network operates. Therefore they introduced the concept of spontaneous networking. It is created when group of people come together for some activity just like human communication model. They have explained five challenges of spontaneous network :

International Journal On Engineering Technology and Sciences – IJETS™
ISSN (P): 2349-3968, ISSN (O): 2349-3976
Volume 2 - Issue 5, May 2015

1. Network boundaries are poorly defined.
2. The network is not planned.
3. Hosts are not preconfigured.
4. There are not any central servers.
5. Users are not experts.

It propose the most popular peer-to-peer key management protocols for mobile ad hoc networks (MANETs). The protocols are subdivided into groups based on their design strategy or main characteristic. This survey aims to provide an overall perspective on the area of peer-to-peer key management for MANETs; the scope of the discussion includes key management schemes for fully self-organized MANETs and authority-based MANETs.

R. Lacuesta and L. Pen˜ aver have proposed work related to IP address configuration while joining a network . In networking a host or node need to be configured with an IP address for communication, IP address is nothing but an identity of node in a network like name of a human being is an identity of that particular person. Generally it is given by central server but in spontaneous networking there is no central server so IP address configuration and network management is done by nodes themselves

R. Lacuesta, J. Lloret, M. Garcia, and L. Pen alver have developed spontaneous ad hoc network providing detail of design and simulation for the first time . They have developed protocol for spontaneous network. Also, provide security to the network. They have provided steps to be followed while joining the network. They provide methods to establish a safe and authentic communication channel, assuming that the participants know the node which they are are speaking with. They also given protocol procedures and messages to be followed to transfer data. They provide mechanism to share www access service as shown in Figure 2

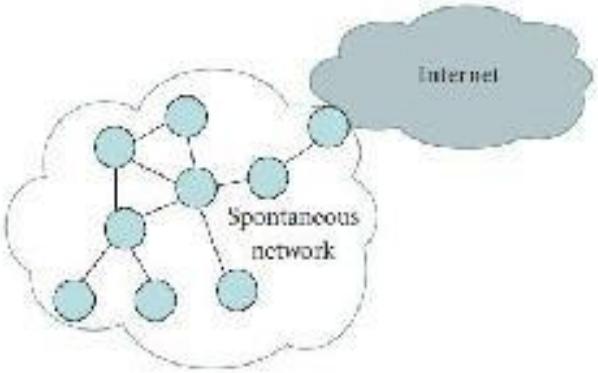

Fig:2.1 sharing of www access in spontaneous networks

Liu, J. Xu, N. Antonopoulos, J. Li, and K. Wu have proposed an Adaptive and Efficient Peer-to-peer Search (AEPS) approach for distribute d service discovery for dependable service integration based on a number of social behaviour patterns, which demonstrates the following functionalities:-operate with each other in a peer-to-peer (P2P) manner to quickly discover and self-configure any services available on the disaster area to deliver a real-time capability;2to deliver a sustainable capability according to environmental changes;-organize themselves in real time to generate higher flexibility and adaptability for disaster management systems and form groups spontaneously; access throughout the network. AEPS has no single point of failure, ensuring greater dependability and availability. AEPS is able to efficiently discover desirable services for decision making of disaster monitoring and relief by interacting with connected nodes with incomplete information and to support dependable dynamic service integration through coping with rapid and significant changes in the disaster area. AEPS builds a "social" network for each sensor node which contributes to effective service discovery.

III. ON DEMAND NETWORK DESCRIPTION

3.1 NETWORK OVERVIEW

Our protocol allows the creation and management of distributed and decentralized spontaneous networks with little intervention from the user, and the integration of different devices .Cooperation between devices allows provision and access to different services, such as group communication, collaboration in program delivery, security, etc. The network members and services may vary because devices are free to join or leave the network.

3.2 NETWORK CREATION AND MANAGEMENT

Spontaneous network should complete the following steps in order to be created.

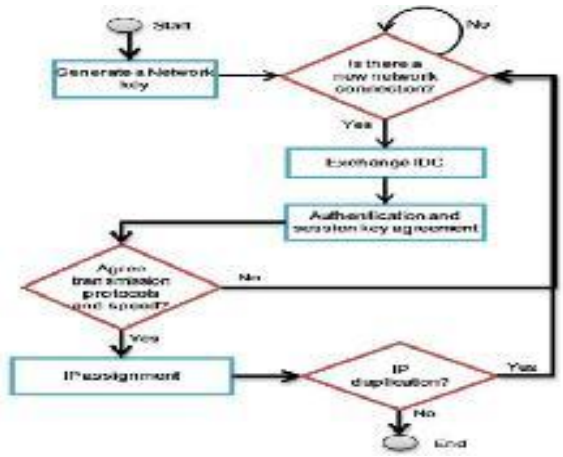

Fig: 3.2.1 Algorithm for joining a node

International Journal On Engineering Technology and Sciences – IJETS™
ISSN (P): 2349-3968, ISSN (O): 2349-3976
Volume 2 - Issue 5, May 2015

The following are the steps for Formation of authenticate spontaneous network.

Step1: Establishment
Step 2: Services Discovery
Step 3: Trusted Chain and Changing Establishment

Algorithm for network creation

3.2.1 ESTABLISHMENT

This step allows the 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 mechanisms. The public component contains a Logical Identity (LID), which is unique for each user and allows nodes to identify it. It may include information such as name, photograph or other type of user identification. It

also contains the user's public key, the formation and termination dates, an IP proposed by the user, and the user signature. The user signature is created by using the Secure hash Algorithm (SHA-1) on the previous data to obtain the data summary. Then, the data summary is signed with the user's private key. Then, the data summary is signed with the user's private key. The private module contains the private key.

The user introduces its personal data (LID) the first time he/she uses the system because the security information is generated then Security data are stored determinedly in the device for future use. Certificate of the user consists of a validated IDC; signed by a user j. The summary function obtained by SHA-1 is signed with private key, to obtain IDC signature of user. No central certification authority is used to validate IDC. In each node validation of integrity and authentication is done automatically. The certification authority for a node could be any of the trusted nodes. The formation of distributed certification authority between trusted nodes is enabled by the system. When node A wants to communicate with another node B and it does not have the certificate for node B. it requests it from its trusted nodes. After attaining this certificate the system will validate the data; if correct then it will sign this node as a valid node. All nodes both clients and servers, can request or serve requests for information or authentication from other nodes.

The first node creates the spontaneous network and creates a casual session key, which will be exchanged with new nodes after the verification phase. Phases of a node joining the network are: node verification and authorization, agreement on session key, transmission protocol and speed, and IP address and routing. When node B wants to join an existing network, it must choose a node within communication range to authenticate with previous node. The public key is sent by the previous node A. Then, node B will send its IDC signed by node A' public key. The validation node received data and verification of hash of message in order to check that the data has not been modified id done by Node A. In this step, Node A establishes the trust level of B node by looking physically at it (they are physically close), depending on whether nodes A knows B or not. Finally, A node will send its identity card data to B node. This data will be signed by B's public key and will establish the trust and validity by integrity confirmation and verification.Others can access data, services,

and B nodes certificates by a route linking other nodes in network, after the verification.

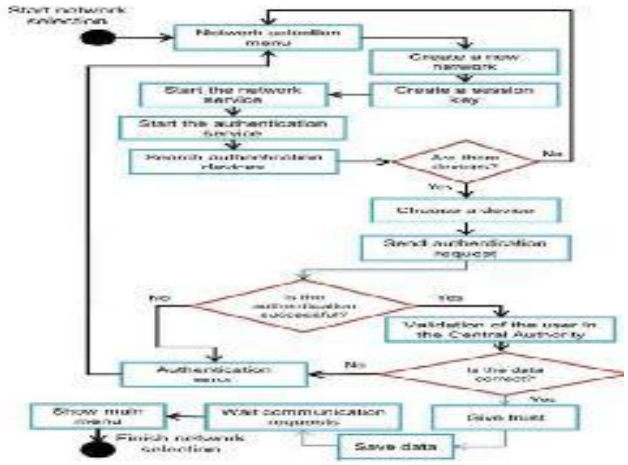

Fig 3.2.2: New network creation procedure

Symmetric key is used as a session key to cipher the confidential messages between trust nodes. It has less energy needs than the asymmetric key. In the above flowchart, the Advanced Encryption Standard (AES) algorithm used for the symmetric encryption scheme. It offers high safety because its design structure removes sub key symmetry. Further, execution times and energy consumption in cryptography procedures are suitable for low-power devices. The asymmetric key encryption scheme is used for distribution of the session key and for the user verification procedure.RSA is used for the asymmetric encryption. After the mutual authentication, first node i.e. A will encrypt the session key with B's public key and will send it to B. The transmission of protocols and the wireless connection speed is decided by them.

Lastly, node B will configure IP address and routing information. An IP address which has a fixed part in the first two bytes and the rest is formed by a random number which depends on the user's data is produced by B and secure routing protocol is borrowed from A. Formerly, B will send the data to procedure the routing information to A. Node A will check whether the IP is reproduced in the network. When B directs data to other network nodes A, e.g. node C, these

data will be authenticated by C (using hashing and verification methods).By looking physically, later, node C will establish the trust level with B .If no trust level is recognized, it will be done afterwards by using trusted chains.

3.2.2 SERVICES DISCOVERY

The accessibility of services is discovering by second node. Services can be discovered by Web Services Description Language (WSDL).Though our model is based on central server but in our spontaneous network we don't use it.

For knowing the available services, a user can ask for other devices. It has a contract to allow access to its services and to access the services offered by other nodes. In such services a large number of parameters which are not transparent to the user and require manual configuration. One issue is to manage the automatic incorporation tasks and use, for example, service agents. The fault tolerance of the network is based on the routing protocol used between users to send information. When node B leaves the network and disappears and also if there is a path to B only then the availability of services is provided to node B.

3.2.3 TRUSTED CHAIN AND ESTABLISHMENT

Node A either trusts or does not trust node B.These are only two trust levels in the system. When it receives the authenticated Identity card from B, the software application installed in the device ask node B to trust A. Trust relationship can be asymmetric. Trust level can be established through trusted chain if A did not establish trust level with node B directly. For example, If node A trusts C and C trusts B, then A may trust B. The changes in trust level can be over time depending on the node's behaviourist can also stop trusting if it discovers that previous trust chain does not exist anymore. The following steps must be followed when the device joins the network.

I. Integrate the Device into the Network.
(a)Agree the transmission protocol and speed.
(b)Configure node addresses, routing information and other resources.

II. Discovery of the Services and Resources Offered by the Devices.
(a)Discover the services and resources shared in the network. (b)Have a list of services and resources available in the network updated.

III. Access to the services offered by the Devices.
(a)Manage the automatic integration tasks and the use of, for example, agent service.
(b)Manage access security to the services.
(c)Manage the join and the leave of nodes of the network. IV. Collaborative task.
(a)Within the intranet, among the various members.

IV. CONCLUSION

In this paper, we show the design of a protocol that allows the creation and management of a spontaneous wireless ad hoc network. It is based on a social network imitating the behavior of human relationships. Thus, each user will work to maintain the network, improve the services offered, and provide information to other network users. We have provided some procedures for self-configuration: a unique IP address is assigned to each device, the DNS can be managed efficiently and the services can be discovered automatically. A user without advanced technical knowledge can set up and participate in a spontaneous network. The security schemes included in the protocol allow secure communication between end users. Distributed DNS is also proposed in this paper.DDNS provides the mapping between login id and ip address .

V. 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. Sh, R. Lacuesta, and M. Chen, "User-Oriented and Service-Oriented Spontaneous Ad Hoc and SensorWireless Networks," Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/ 2, pp. 1-8, 2012.

[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, "A Survey of Key Management Schemes in Wireless Sensor Networks," Computer Comm., vol. 30, nos. 11/12, pp. 2314-2341, Sept. 2007

[6] V. Kumar and M.L. Das, "Securing Wireless Sensor Networks with Public Key Techniques," Ad Hoc and Sensor Wireless Networks, vol. 5, nos. 3/4, pp. 189-201, 2008.

[7] 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.

[8] A. Noack and S. Spitz, "Dynamic Threshold Cryptosystem without Group Manager," Network Protocols and Algorithms, vol. 1, no. 1, Oct. 2009.

[9] J. Yan, J. Ma, F. Li, and S.J. Moon, "Key Pre-distribution Scheme with Node Revocation for Wireless Sensor Networks," Ad Hoc and Sensor Wireless Networks, vol. 10, nos. 2/3, pp. 235-251, 2010.

[10] M. Mukesh and K.R. Rishi, "Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review," Int'l J. Computer Applications,vol. 12, no. 2, pp. 37-43, Dec. 2010.