Security Based on User Trust in Spontaneous Wireless Ad Hoc Network Creation

[1]Nandireddy Sreenivasula Reddy, [2]J.Godwin Ponsam

Information Security and Computer Forensics,
SRM University, Kattankulathur, India
[1]sreenureddy@hotmail.com, [2]godwinsrm@gmail.com

***Abstract*— Security in wireless ad hoc networks is hard to achieve due to the absence of centralized management point. *Security in wireless ad hoc networks usually relies on the use of predistribution key mechanisms.* Spontaneous network is a special case of ad-hoc network, they are independent of central server having no interference of an extern user. In this paper, spontaneous wireless ad hoc network uses a hybrid symmetric/asymmetric scheme. Trust is based on first visual contact. A user is able to join the network , if user knows someone that belongs to network .A user can able to leave or join the network at any time .It is complete self-configured protocol, which is able to create a secure network and share services without any infrastructure. A user can create its own resources or they can request from its neighbor user, because it allows resource sharing and offer new services in a secure environment. Design of a protocol permits the management and creation of a spontaneous wireless ad hoc network.**

***Keywords*— Spontaneous network, ad hoc network, Distributed Certificate Authority**

I. INTRODUCTION

Spontaneous ad hoc networks are formed by a set of mobile terminals that are placed in a close location communicating with each other, sharing resources, services or computing time during a limited period of time and in a limited space forms. These types of networks have no dependent centralized servers. They can be wireless or wired by making Spontaneous network a Special case of ad hoc network. These networks need well defined, effective and user-friendly security mechanisms. Tasks to be performed in this type of network include: Identity of User, their authorization, address to be assigned, service name, safety and operation. The Significant dependency of Configuration services in spontaneous networks is on the size of the network, the nature of Participation of Nodes and running applications. Intentional interactions among users who have prefer to collaborate for some purpose are reflected by spontaneous network. That can be leveraged into order to create an ordered method for modifying the network configuration. This network has limited scope in both time and space. It includes powerful host machines, such as laptops or developing high-end personal digital assistants (PDAs) and mobile phones.

The Important features in spontaneous networks are mentioned below:-

1. Network boundaries are designed poorly.
2. The network is not pre planned.
3. Hosts are not preconfigured.
4. They don’t have any central servers.
5. Users are not experts.

In this network the services requirements mainly depends on the size of the network, the nature of Participation of Nodes and running applications. Normally wireless networks with setup use Certificate Authority (CA) servers to manage node trust and authentication. These systems usually have been used in sensor networks, Every time the networks cannot be practical as a CA node has to be external. Further, CA node must have higher computing capacity. In such networks, the key exchange mechanisms for node authorization and user authentication are needed to achieve a reliable communication and node authorization. Secured self-configured environment for data distribution and resources and services sharing among users can be established by this network and protocol. Security is based on the users service needs, and also to obtain a distributed certification authority it necessary to build trust networks. The network allows users to join because it belongs to someone who knows it. Hence, the new user is trusted by the certification authority. This allows the network to have a distributed name service and also distribution of network management. We have implemented asymmetric cryptography, where each device has a public-private key pair for device identification and symmetric cryptography between nodes to share session keys. There are unidentified users because validity and privacy are based on user identification

II. NEW NODE JOINING PROCEDURE

The security protocol for routing purposes, based on trust that allows the management and Creation of distributed and decentralized spontaneous networks with little intervention from the user, the integration of different devices is introduced by the flowchart that is shown in below fig about the creation overview of authenticate spontaneous network.

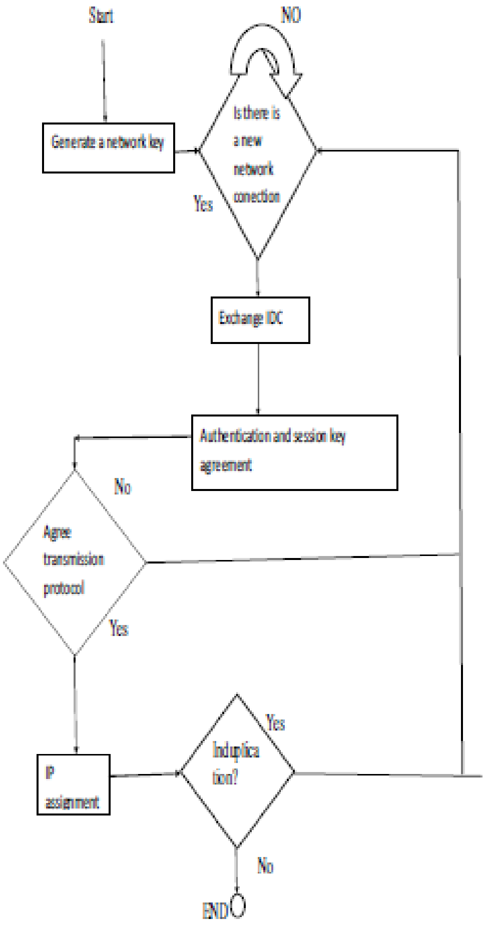
Start
NO
Generate a network key
Is there is a new network conection
Yes
Exchange IDC
Authentication and session key agreement
No
Agree transmission protocol
Yes
Yes
IP assignment
In duplica tion?
No
END

Fig. 1 Algorithm for joining a new node

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

A. Step1: Node Joining

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. 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 logical data (LID) the first time he/she uses the system because the security information is generated with secure data that are stored determinedly in the device for future use. Certificate of the user consists of a validated IDC; signed by a user k. 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 by 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, it requests from its trusted nodes. After attaining this certificate the system will validate the data. If data is 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. On the ground of Public Key Infrastructure and the symmetric key encryption scheme, Security management in the network is based.

Symmetric keys are used as a session key to cipher the confidential messages between trust nodes. It has less energy than the asymmetric key. In the above flowchart, (AES) algorithm for the symmetric encryption scheme. It offers high safety because of 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 the distribution of the session key and for user verification procedure.

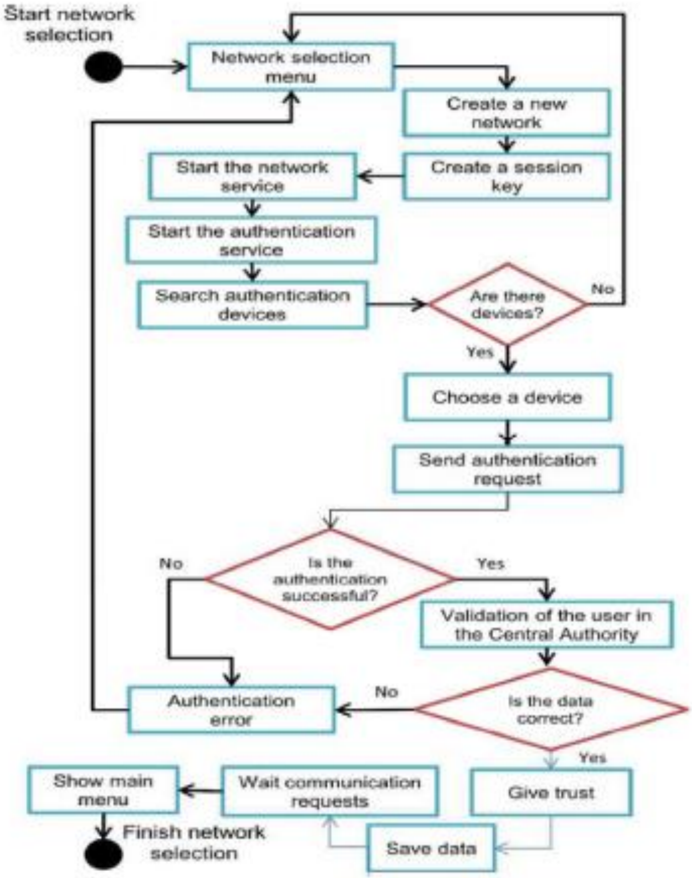

Fig.2 New network creation procedure

We used two types of asymmetric encryption schemes: Elliptic Curve Cryptosystem (ECC), because of its high performance and Rivest, Shammir &Adelman (RSA) algorithms. After the mutual authentication, first node i.e. A will encrypt the message with B’s public key and will send it to B. The transmission protocols and the wireless connection speed is decided. At lost, node B will configure IP address and routing information. In IP address the first two bytes has a fixed part and the rest is formed by a random number which depends on the user’s data, 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 replaced in the network. When B directs data to other network nodes, e.g. node C, validated these data by C (using hashing and verification methods like authentication).By looking physically, later, node C will establish the trust level with B .If no trust level is done at that time, it will be done afterwards by using trusted chains.

B. *Step 2: Services Requesting*

The services can be discovered 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 ad hoc network we don’t use any central server. To know the services in network, a user can ask its trusted nodes or neighbor nodes. 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.

C. Step 3: Trusted Chain and Changing Trust Level Establishment

Node A either trusts or does not trust node B .There are only two trust levels in this. When it receives the authenticated IDC from B, the application installed in the device ask node B to trust A. Trust relationship can be asymmetric. Trust level can be established through trusted chains if A don’t establish trust level with node B directly e.g. it can trusted chain, 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 behaviorist can also stop trusting if it discovers that previous trust chain no more exists.

The following steps must be followed when the device joins the network.

1. Integrate the Device into the Network.
    a. Agree the transmission protocol and speed.
    b. Configure node addresses, routing information and other resources.
2. Discovery of the Resources and Services 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.
3. 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.
4. Collaborative task.
    a. Within the intranet, among the various members.
    b. On the internet, with the other communities.

III. NETWORK CREATION

Devices must be aware of all the different tasks needed to communicate with each other and the configuration of both logical and physical parameters when they join network. Users carry their resources to the system. The connection can be shared and that device will be the one that provides the access to the WWW, if one of the users of the spontaneous network has Internet connection. Internet access in the spontaneous network could be more than one and each one of them could share different services. The intranet and its view to the outside world permits the community both internal and external cooperation. In this model a user contributes capabilities, technical resources to access external services, and other applications such as: reports, games, and other data which they may wish to share. Following Figure 3.shows the model example.

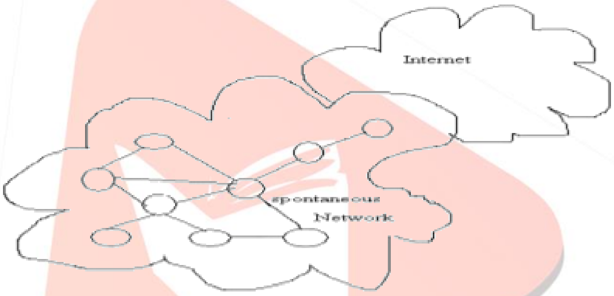

Fig.3 Network model.

The resources of the devices are used according to their available capacities. If one needs to carry out specific task but does not find this possible owing to the fact that the device does not have the enough resources another one user may be responsible for processing.

Tasks should be performed when a user joins the spontaneous network in the following ways:

a. Node identification

b. Identification between nodes

c. Address assignment

d. To join services

The above tasks should be carried out with security. When configuring an ad hoc network, one after the other main problems which arise is the generation of a unique IP address. The problem comes from not knowing the topology of the network, neither when being set up, nor later on modification. Most of the routing protocols assume that the mobile nodes are configured a priori with a unique IP address before becoming part of the network, except in this case. The problem comes from not significant the topology of the network, neither when being set up, nor later on alteration. A protocol must be capable of managing the generation of these IP addresses in order to run the network properly also A node may enter or leave the network at will at any time. the protocol must be able to identify the existence of duplicated IP addresses, which may occur, for example when two sub networks join together, or when a node which leaves one sub network with an IP (until then unique) joins another, or even when there is a substitution attack on the nodes or when two sub networks join together.

The problem of using DHT-based algorithms as self-organizing systems and others use hypercube to implement indirect routing is solved by Experts. We offer a distributed and decentralized solution, by facing these challenges and also after analyzing the working of ad hoc networks, within the framework we have set ourselves. Our proposal starts with the awareness that ad hoc spontaneous networks require a flexible protocol which adapts itself to any number of different nodes and to their various features. A range of different devices (cell phones, PDAs, laptops, etc.) may take part in the formation of these networks. For being a part of this network these nodes have to be configured. The operating of the wireless network must be alike to the one with IP configuration set-up: translation of DNSs, service identification, etc. despite the fact that our networks do not include central servers. On the contrary, it needs the minimum interference of the user because it will be used by no expert users, so the configuration must take place without any dependency. The formation of all the factors necessary to form such networks indicates to share information between the nodes. A chain of a random number of four bits, which lets restore the IP if it has been reproduced, and twelve bits obtained from the twelve last bits of the obtained hash when we pass a hash function to the user's data for the formation of rest of the IP.Second, we must check the IP repetition by one of the nodes that are already in the network. We need to check the node uses of broadcast technique through which they send a packet with the planned IP in order to perform. The new node gets response by it if a node is using this IP.It has to offer a new IP, as the IP cannot be used by the new node.

IV. SECURITY IN AD HOC NETWORKS

Portable nodes that need to communicate during a reduced time slot for the formation of Spontaneous ad hoc networks. The problems of ad hoc network are similar to these networks, but increased because they are temporal networks formed in a given moment by a group of nodes that often users do not know each other. However, they must work together for the proper process of the network. Safe communication must be guaranteed with the help of cryptographic techniques. However, many of the outlined protocols assume that the nodes know the session key, when we talk about the use of cryptography of private key as well as the use of cryptography of public key. Methods to establish a safe and authentic communication channel is provided by these networks, assuming that the participants know the node which they are speaking with. A fundamental topic in the environment of the security in spontaneous networks, when the nodes do not know each other and also the phase of connection establishment and initial exchange of keys. Security requirements in spontaneous networks and traditional networks are same: privacy, integrity, verification, no repudiation, and availability. Both data and routing information must be safe. The structures of ad hoc networks make these necessities much more difficult: dynamic topology, limited bandwidth, different capacity links and high error rates, energy and processing capacity limitations, absence of a central server, and often no prior information in the nodes to build the network. These limitations have to be covered by organization mechanisms and by the support among the nodes to maintain service quality, security, and almost inventions and access to the services. Like human relationships in the society, this behavior is also similar to them. Everyone must cooperate to preserve a secure world, to improve our quality of life, and have updated news. We know that the data are correct when they come from a person that we trust. In this society the trust is very important.

The Significance of the required configuration services depends on the size of the network, the applications to support it and the nature of the participants. Privacy, integrity, accessibility and control with verification must be offered without central administration and with energy limitations. Key generation, management, and distribution schemes that can be run on small CPUs are required by them. If we wish to create a spontaneous wireless network security comparable to the traditional networks two fundamental areas must be addressed. First, there must be a trust formation, key management, and membership control, and, second, there must be network availability and routing security.

Our goal is to develop techniques in order to enable the creation of small- and medium-scale ad hoc networks based on the spontaneity of both. On the grounds of physical proximity, wireless connectivity is based; it reflects the ways human beings interact. People who are near each other can link, share things with each other, and ask people to relay information to others. This is all done with an appropriate level of security.

To get an appropriate level of security we establish numerous protection mechanisms as follows.

(i) Identification of the Nodes (ii) Prevention of Proud Behaviour

(iii)Security in Routing Protocols against Manipulations.

V. PROTOCOL OPERATION

In order to design the diagrams we used, Unified Modeling Language (UML) is a visual description standardized language that is built to model object oriented systems which is use to build the protocol system. Keys, activities, and use cases are used to define the processes, the structure of the classes in the system, and the behavior of operations. User determines whether he/she have to create new network or participate in an existing one once registration/validation operation is performed in this process. First a session key will be generated with new network creation. Then, Services will be started by node. Lastly, it will wait for requests from other devices that want to join the network.. If the user wants to become part of an existing network, the node find a device that will give trust to it, save matching data and will be capable to begin communications. And with the existing one the node is responsible for authenticating the new node’s data, will perform a dispersal process to the nodes that are within its communication range. These nodes will forward the received packets to their neighbors until the data reach all nodes in the network. Validity and uniqueness of the new node’s data is verified by this process.

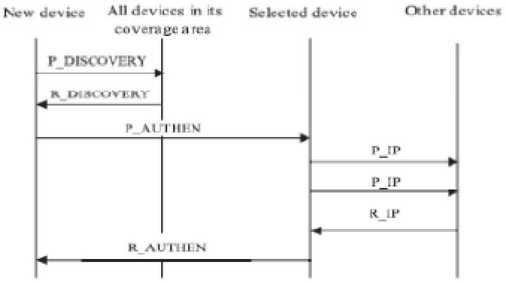

Fig.4 Authentication procedure

New device is with receiver node A validates the received data and sends a broadcast message to node B to check if these data are not used in the network (even the IP address) by the Authentication Process. In order to avoid simultaneous checks and reach all devices, this IP checking packet is sent randomly twice. It sends the verification reply to the new device, when the authentication device receives the IP checking reply. An error message is sent to the new device, if any step is incorrect. It is able to perform several tasks if the node is authenticated. Since others are used by the user to perform some operations in the network, some of them are performed transparently for the user. The structure of the programmed application in UML language is shown below.

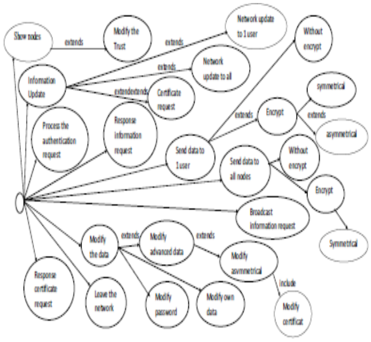

Fig.5 Node options after the authentication procedure

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
- Send data to all nodes
- Modify data
- Leave the network

The node sends a request certificate message to its trusted nodes, to request a certificate. A packet to request the certificate to its trust nodes which are selected from the database generates by the Application. All the steps followed by this procedure are shown in Fig. 6.

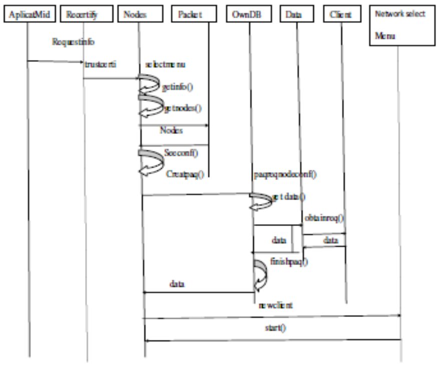

Fig.6. Procedure to request a certificate from trusted nodes

The node checks if it can reply to the request, if not, the node sends the search to the nodes (that it trusts or known nodes)to process the received request. The node sends the certificate to the requesting node for validating it. When the server procedure receives the packet, it processes the packet and checks its validity access to the certificate data in order to take the certificate.Fig.7 shows the steps of this procedure.

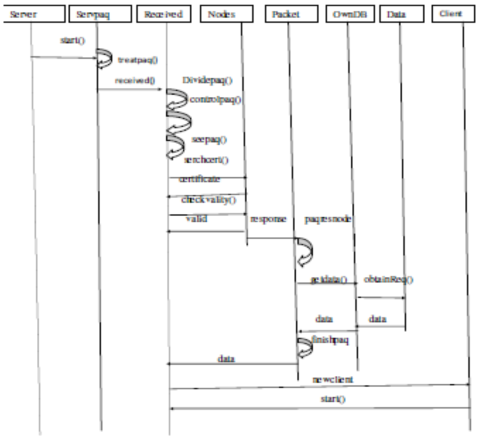

Fig.7 Procedure to process the request.

The user has to select the remote node and write the data, to send data encoded with the public key to a node. Then, the message is encrypted using the remote node’s public key.Fig.8. Shows the encryption and packet sending process. The application encrypts the data with the public Key generates the packet and sends it to the selected node.

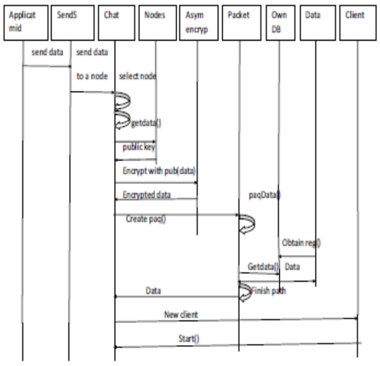

Fig.8 Procedure to send data encrypted with the public key

Every node will checks the packet whenever they received from other node. It is shows directly to the user, but if it is encrypted, if the received packet is encrypted with public key then decode with its private key or if it is encrypted by session key decrypt with session key. The below algorithm will explain Fig.9.

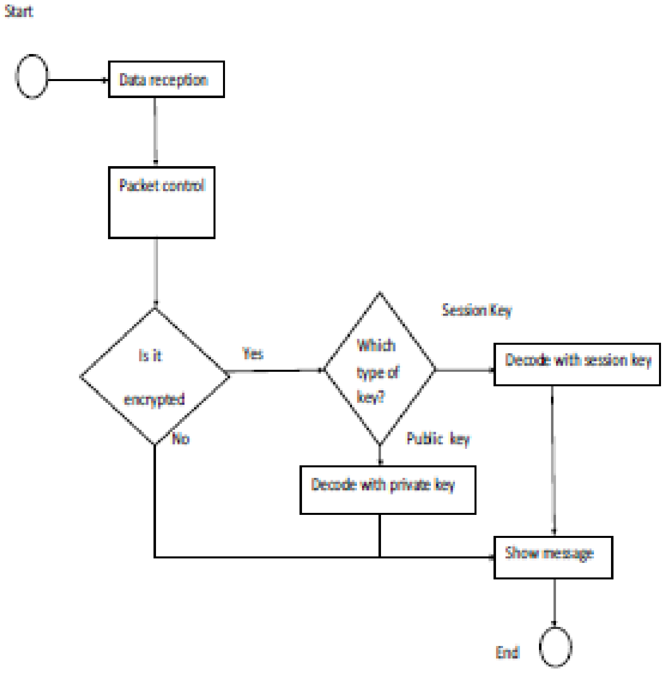

Fig .9 Algorithms when data packets are received.

VI. CONCLUSION

In this paper, the protocol design will helps to create and manage the spontaneous ad hoc network. This network will imitate the human relationships and it is based on social networking. Every user will work for maintenance of the network, by providing necessary services or resources .Node can be configured its own resources, because it is a self configured network. Each node is assigned by IP address, so that user can authenticate with its IP address. It is a user friendly application with minimal user interaction.

REFERENCES

[1] Raquel Lacuesta, Jaime Lloret, Senior Member, "*A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation*"IEEE,Miguel Garcia, Student Member, IEEE, and Lourdes Pen˜ alver

[2] L.M. Feeney, B. Ahlgren, and A. Westerlund, "*SpontaneousNetworking: An Application-Oriented Approach to Ad-hocNetworking,*" IEEE Comm. Magazine, vol. 39, no. 6, pp. 176-181, June 2001

[3] A. Noack and S. Spitz, "*Dynamic Threshold Cryptosystemwithout Group Manager*," Network Protocols and Algorithms,vol. 1, no. 1, Oct. 2009.

[4] K. Sahadevaiah and P.V.G.D. Prasad Reddy, "*Impact of SecurityAttacks on a New Security Protocol for Mobile Ad Hoc Networks*,"Network Protocols and Algorithms, vol 3, no. 4, pp. 122-140, 2011.

[5] *Laura Marie Feeney, Bengt Ahlgren, Assar Westerlund, Swedish Institute of Computer Science* Spontaneous Networking*:An Application-Oriented Approach toAd Hoc Networking*

[6] 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.

[7] L. Herrero and R. Lacuesta, "*A Security Architecture Proposal for Spontaneous Networks,*" Proc. Int'l Conf. Advances in the Internet Processing System and Interdisciplinary Research, Oct. 2003.

[8] K. Sahadevaiah and P.V.G.D. Prasad Reddy, "*Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks*," Network Protocols and Algorithms, vol 3, no. 4, pp. 122-140, 2011.

[9] 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.

[10] J. Rekimoto, "SyncTap: Synchronous User Operation for Spontaneous Network Connection," Personal and Ubiquitous Computing, vol. 8, no. 2, pp. 126-134, May 2004.