RESEARCH ARTICLE

A Secure Routing Protocol for Wireless Adhoc Network Creation

Rajashekharagouda Patil[#], Shreedharamurthy S K*

[#]Department of Electronics and Communication, U B D T College of Engineering Davangere, India
[*]Associate professor of Electronics and Communication, U B D T College of Engineering Davangere, India

[#]appurajpatil@gmail.com
[*]sks_murthy@yahoo.com

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 a secure protocol for spontaneous wireless Ad-hoc network which uses a 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 implemented in order to test the protocol procedure and performance.

Keywords— Ad-hoc network, node authentication, session key, network creation, memory consumption

I. INTRODUCTION

A spontaneous network is a special case of ad hoc networks. They usually have little or no dependence on a centralized administration. Spontaneous networks can be wired or wireless. Configuration services in spontaneous networks depend significantly on network size, the nature of the participating nodes and running applications. Spontaneous ad hoc networks require well defined, efficient and user-friendly security mechanisms. Tasks to be performed include: user identification, their authorization, address assignment, name service, operation, and safety. Generally, wireless networks with infrastructure use Certificate Authority (CA) servers to manage node authentication and trust. Although these systems have been used in wireless ad hoc and sensor networks they are not practical because a CA node has to be online all the time. Moreover, CA node must have higher computing capacity.

None of 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.

II. EXISTING SYSTEM

The existing system allows the creation and management of distributed and decentralized spontaneous networks with little intervention from the user, and the integration of different devices (PDAs, cell phones, laptops, etc.). 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. To complete the Spontaneous network creation three steps are involved Network Joining Procedure, Service Discovery and Establishing Trusted Chain and Changing Trust Level.

III. PROPOSED SYSTEM

The proposed security protocol is adaptable because new security cryptographic algorithms can be easily added. In order to perform an analysis and evaluation from the practical perspective, we provide most common attacks in spontaneous wireless ad hoc networks and how our proposal refuses them. We can observe that the secure mechanisms included in our spontaneous ad hoc network make it to accomplish high level of security. With this proposed scheme we analyze and evaluate the security scheme.

This model is analysed for Maximum stored nodes in available memory and Memory Consumption for server node and requester node during spontaneous network formation. This analysis is made on using secure encryption algorithm called AES on using the minimum number of protocol packets.
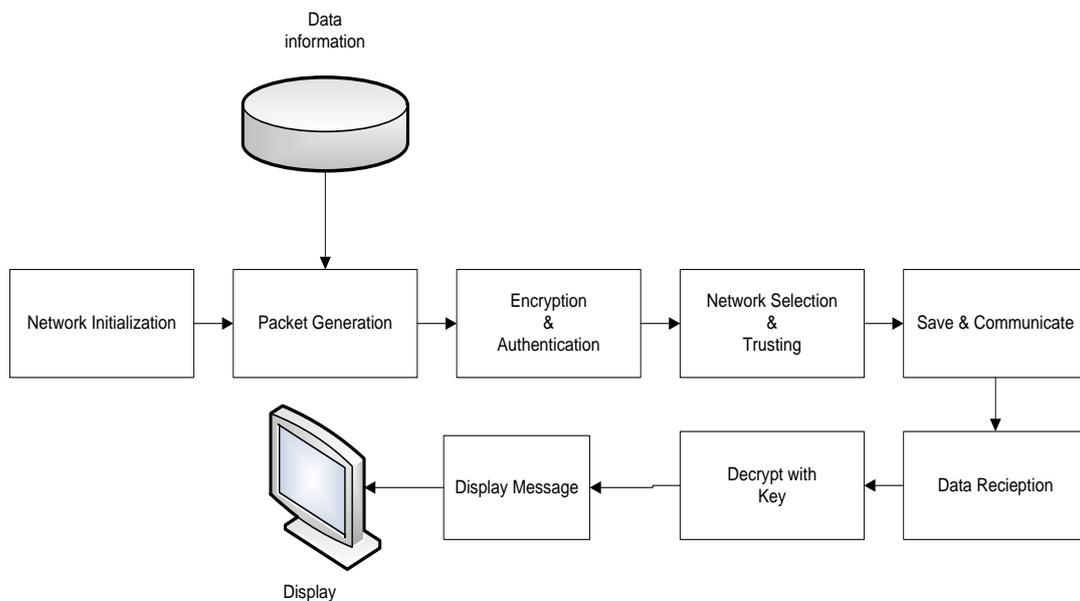

Fig.1Block diagram of proposed system

The main Objectives of Spontaneous network is to integrate 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 aim of this paper is to provide the Security informing the spontaneous ad-hoc wireless networks. Here authors used symmetric and asymmetric Encryption algorithms to provide the security.

Dynamic networks with flexible memberships, group signatures, and distributed signatures are difficult to manage. The challenge of this project is to develop a self-configured secure protocol that is able to create the network and share secure

services without any infrastructure. To achieve a reliable communication and node authorization in mobile ad hoc networks, key exchange mechanisms for node authorization and user authentication are needed storage scheme. The challenge is to 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.

IV. ALGORITHMS

Algorithm1- Algorithm for joining a new node.

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. It may include information such as name, photograph or other type of user identification. This idea has been used in other systems such as in vehicular ad hoc networks It also contains the user's public key (Ki), the creation and expiration dates, an IP proposed by the user, and the user signature. The user signature is generated during 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. The private component contains the private key (ki). 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 persistently in the device for future use.
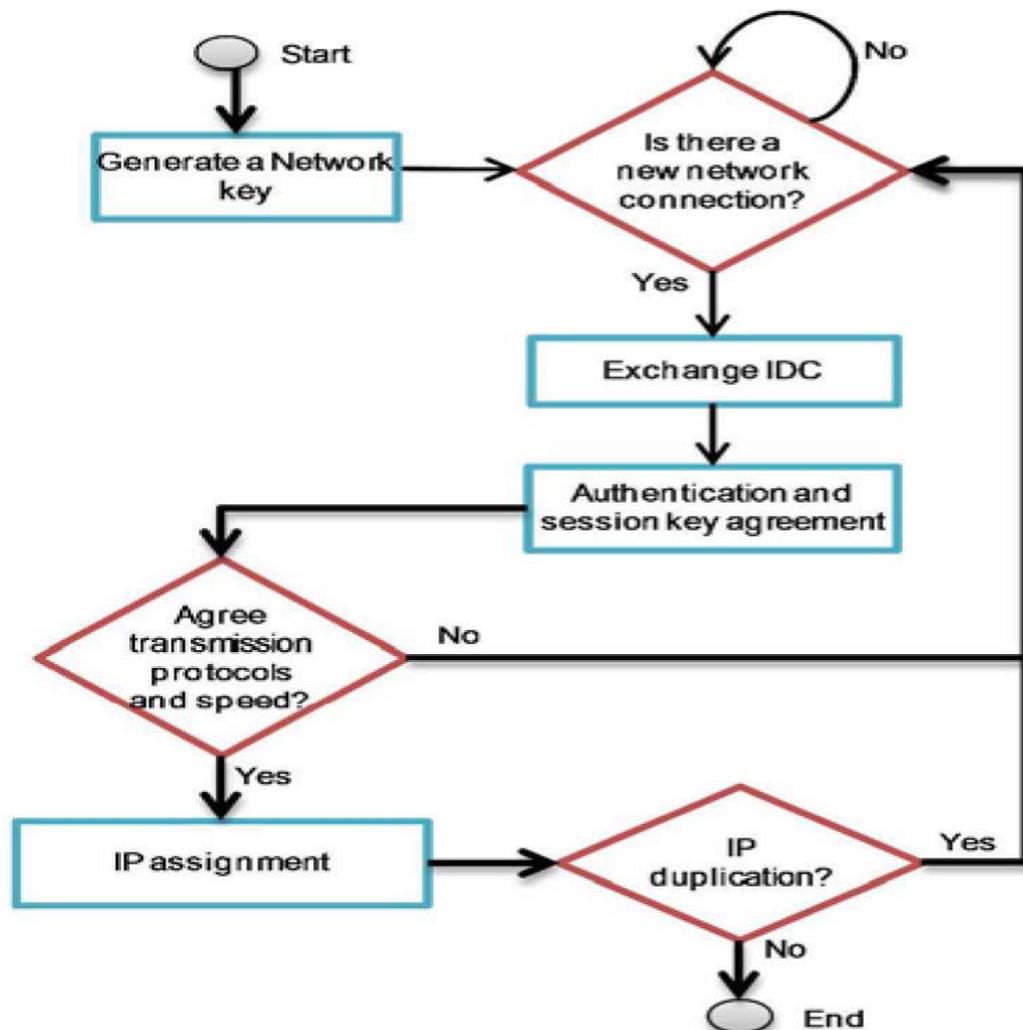

Fig.2 joining a new node

The first node creates the spontaneous network and generates a random session key, which will be exchanged with new nodes after the authentication phase. Fig. 1 shows phases of a node joining the network: node authentication 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 (e.g., node A). A will send its public key. Then, B will send its IDC signed by A's public key. Next, A validates the received data and verifies the hash of the message in order to check that the data has not been modified. In this step, A establishes the trust level of B by looking physically at B(they are physically close), depending on whether A knows B or not. Finally, A will send its IDC data to B (it may do so even if it decides not to trust B). This data will be signed by B's public key (which has been received on B's IDC). B will validate A's IDC and will establish the trust and validity in A only by integrity verification and authentication. If A does not reply to the joining request, B must select another network node (if one exists). After the authentication, B can access data, services, and other nodes certificates by a route involving other nodes in network.

Algorithm2- New network creation procedure

B asks for the available services. Services can be discovered using Web Services Description Language (WSDL). Our model is based on but in our spontaneous network we don't use a central server. Moreover, other service discovery services can be implemented in our system .A user can ask other devices in order to know the available services. It has an agreement to allow access to its services and to access the services offered by other nodes. Services have a large number of parameters which are not transparent to the user and require manual configuration. One issue is to manage the automatic integration tasks and use, for example, service agents. Other is to manage secure access to the services offered by the nodes in the network. The fault tolerance of the network is based on the routing protocol used to send information between users. Services provided by B are available only if there is a path to B, and disappear when B leaves the network.
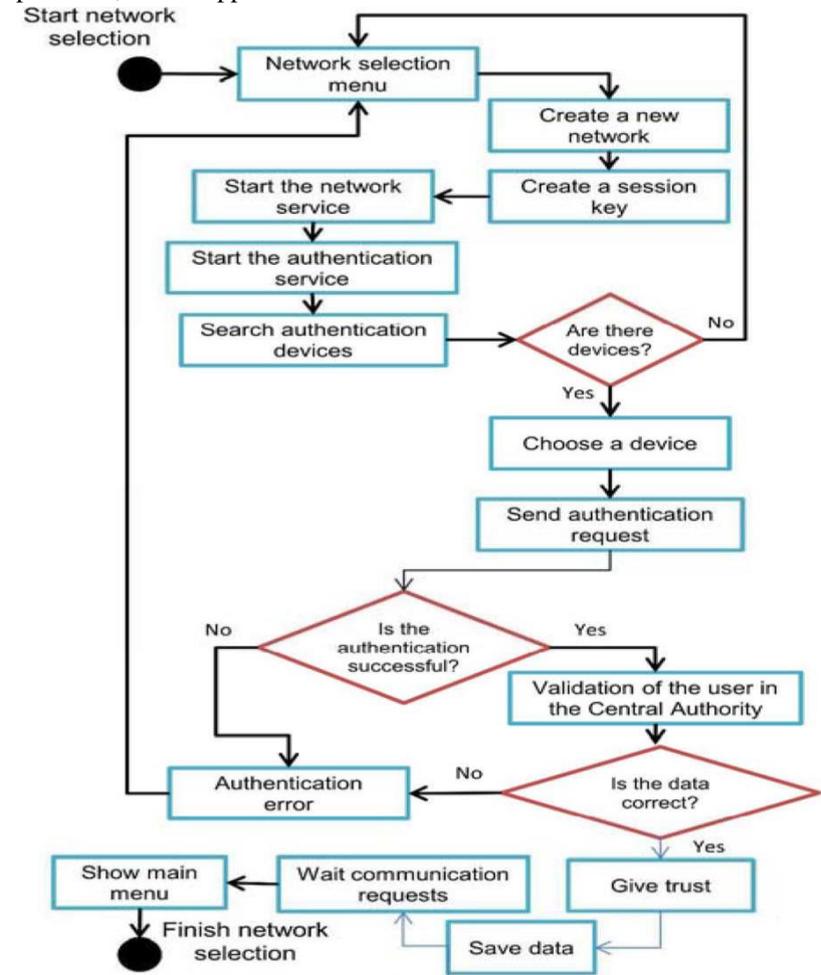

Fig.3 New network creation procedure

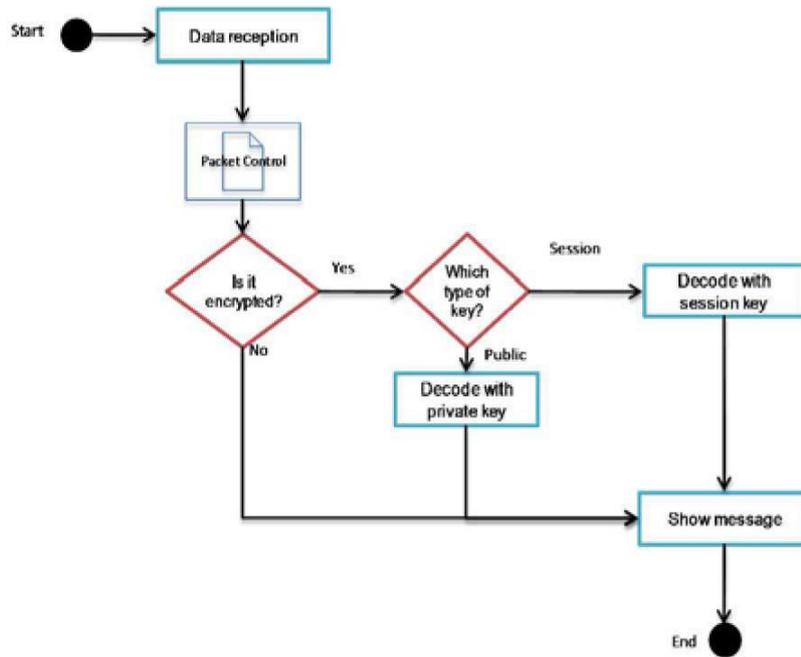Algorithm3: Algorithm when data packets are received.
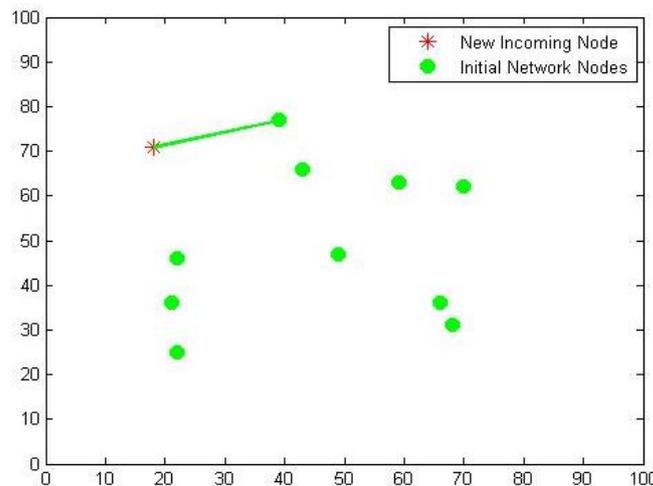

Fig.4 Algorithm when data packets received.

Fig.5 Snapshot of the network creation and authentication procedure.

V. PROTOCOL OPERATION

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 Fig. 3. First, a session key will be generated. Then, the node will start its services (including the network and authentication services). Finally, 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 follows algorithm, to find a device that will give trust to it, save corresponding data and will able to begin communications.

The node that belongs to the network, and is responsible for validating the new node's data, will perform a diffusion 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. This process allows verifying the validity and uniqueness of the new node's data.

When the node is authenticated, it is able to perform several tasks. Some of them are performed transparently for the user, but others are used by the user to perform some operations in the network. They are the user application options.
The authenticated node can perform the following tasks:

- Display the nodes.
- Modify the trust of the nodes.
- Update the information: It allows a node to learn about other nodes in the network and also to send its data to the network. This update could be for only one user or for all users in the network through a controlled diffusion process.
- Other nodes certificate request: A node could be requested from other node, from all trusted nodes or from all known nodes. In case of all known nodes, the node that replies to the request will always sign the data. The data will be considered validated if a trusted node has signed them.
- Process an authentication request: The node authenticates a requesting node by validating the received information, user authentication, and verifying the non-duplication of the LID data and the proposed IP.
- Reply to an information request: the requested information will be sent directly to the requesting node or routed if the node is not on the communication range.
- Forward an information request: The request will be forwarded if it is a broadcast message.
- Send data to one node: It can be sent symmetrically or asymmetrically encrypted, or unencrypted.
- Send data to all nodes: This process is doing by a flooding system. Each node retransmits the data only the first it receives the data. It can be sent symmetrically encrypted or unencrypted.
- Modify Data: User data can be modified and the password changed.
- Leave the network.

Each node has to check every received data packet. If the received packet is not encrypted, it is shown directly to the user, but if it is encrypted, the packet will be decipher during the encryption model used by the sender. The algorithm followed by the node is shown in Fig.4.

VI. CONCLUSION

The Proposed protocol allows the creation and management of a spontaneous wireless ad hoc network. It is based on a social network imitating the behaviour of human relationships. Thus, each user will work to maintain the network, improve the services offered, and provide information to other network users. This method provides some procedures for self-configuration: a unique IP address is assigned to each device.
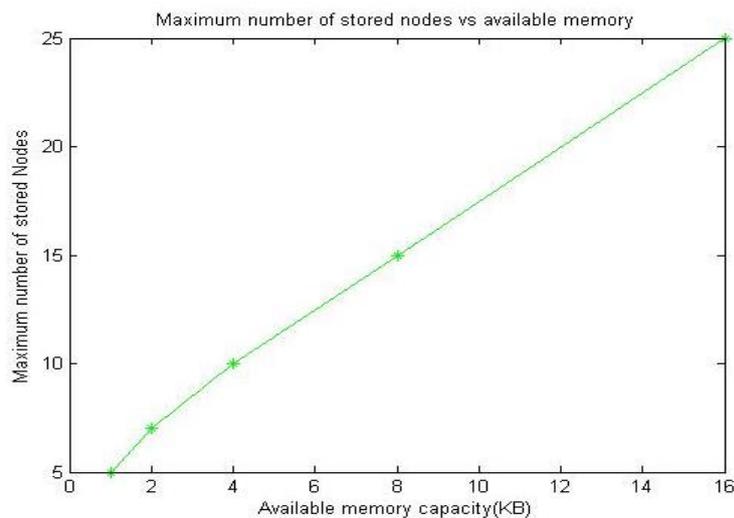

Fig.6 Snapshot of the Maximum number of stored nodes versus available memory.

We have also created a user-friendly application that has minimal interaction with the user. The security schemes included in the protocol allow secure communication between end users. Finally the analysis shows the improvement in the number of nodes handled by unit memory and memory consumption by both server and requester node.

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. Shu, R. Lacuesta, and M. Chen, "User-Oriented and Service-Oriented Spontaneous Ad Hoc and Sensor Wireless 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," RostockerInformatik-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.

Authors Bibliography

Rajashekhargouda Patil received the B.E. degree in Electronics and Communication Engineering from PES College of Engineering Mandya. At present pursuing the Master of Technology in Digital Communication and Networking Department at UBDT college of Engineering Davangere Karnataka, India.

Prof. Shreedharmurthy S.K. received the bachelor of engineering degree from JNNCE Shimoga and master of technology from NIE Mysore. He is currently an Associate Professor in Department of Science in Electronics and Communication Engineering at UBDT college of Engineering Davangere Karnataka, India.