INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A PROTECTED STEERING PROCEDURE FOR MANET SYSTEM DESIGN

Vatnala Chennagoud[1]

chennagoudvatnala@gmail.com

Abstract

Ad-hoc mobile System is an infrastructure less System, i.e. there is no centralized coordination for the System operations. As and when a new node comes in the vicinity of the System it will spontaneously form the System. This paper presents a Protected Procedure for spontaneous mobile Ad-hoc System 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 Protected Procedure that is able to create the System and share protected services without any infrastructure. System Design stages are detailed and the communication, Procedure messages and System management are explained. Our proposal has been implemented in order to test the procedure and performance.

Keywords: Ad-hoc System, node authentication, session key, System Design, memory consumption

1. Introduction

A spontaneous System is a special case of ad hoc Systems. They usually have little or no dependence on a centralized administration. Spontaneous Systems can be wired or mobile. Configuration services in spontaneous System s depend significantly on System size, the nature of the participating nodes and running applications. Spontaneous ad hoc System s requires 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, mobile System s with infrastructure use Certificate Authority (CA) servers to manage node authentication and trust. Although these systems have been used in mobile ad hoc and sensor Systems 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 Protected spontaneous System Procedure based on user trust that provides node authenticity, integrity checking, and privacy. The System and Procedure proposed in this paper can establish a protected 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 System to obtain a distributed certification authority. A user is able to Add the System because he/she knows someone that belongs to it. Thus, the certification authority is distributed between the users that trust the new user. The existing system allows the Design and management of distributed and decentralized spontaneous System s 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 System members and services may vary because devices are free to Add or leave the System. To complete the Spontaneous System Design three steps are involved System Adding Procedure, Service Discovery and Establishing Trusted Chain and Changing Trust Level.

The proposed securityProcedureis adaptable because new security cryptographic algorithms can be easily added.

Vol.2 Issue.6, Pg.: 41-46
June 2014

In order to perform an analysis and evaluation from the practical perspective, we provide most common attacks in spontaneous mobile ad hoc System s and how our proposal refuses them. We can observe that the protected mechanisms included in our spontaneous ad hoc System make it to accomplish high level of security. With this proposed scheme we analyze and evaluate the security scheme.

2. Design Model

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

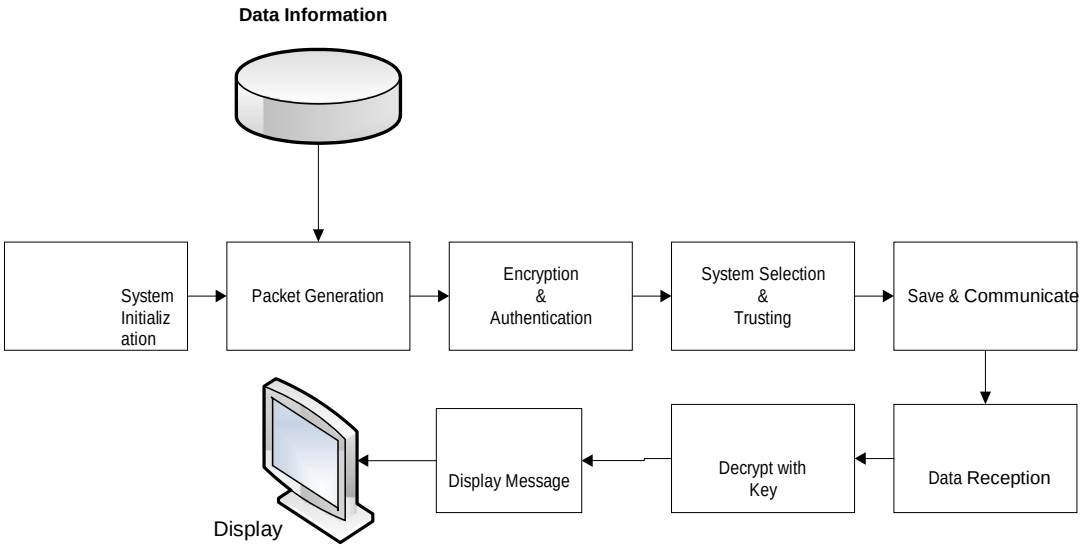

Fig.1Block diagram of Design

The main Objectives of Spontaneous System is to integrate services and devices in the same environment, enabling the user to have instant service without any external infrastructure. Because these System s are implemented in devices such as laptops, PDAs or mobile phones, with limited capacities, they must use a lightweight Procedure, and new methods to control, manage, and integrate them.

The aim is to provide the Security informing the spontaneous ad-hoc mobile System s. Here authors used symmetric and asymmetric Encryption algorithms to provide the security. Dynamic System s with flexible memberships, group signatures, and distributed signatures are difficult to manage. The challenge of this project is to develop a self-configured Protected Procedure that is able to create the System and share protected services without any infrastructure. To achieve a reliable communication and node authorization in mobile ad hoc Systems, key exchange mechanisms for node authorization and user authentication are needed storage scheme. The challenge is to establish a protected 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 System to obtain a distributed certification authority

3. Procedure

Procedure1- for Adding 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 System s It also contains the user's public key (Ki), the Design and expiration dates, an IP proposed by the user, and the user signature. The user signature is generated during the Protected 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.

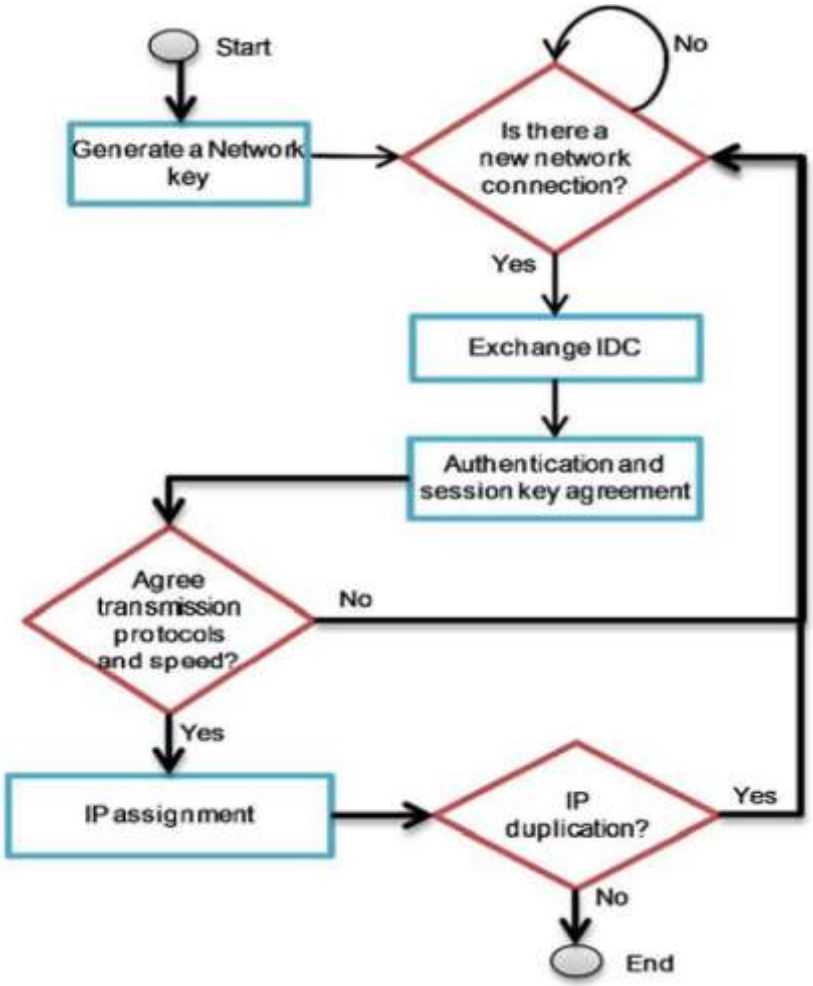

Fig.2 adding a new node

The first node adds the spontaneous System and generates a random session key, which will be exchanged with new nodes after the authentication phase. Fig. 1 shows phases of a node adding the System: node authentication and authorization, agreement on session key, transmission Procedure and speed, and IP address and routing. When node B wants to add an existing System, 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 Adding request, B must select another System node (if one exists). After the authentication, B can access data, services, and other nodes certificates by a route involving other nodes in System.

New System Design 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 System 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 protected access to the services offered by the nodes in the System. The fault tolerance of the System is based on the Steering 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 System

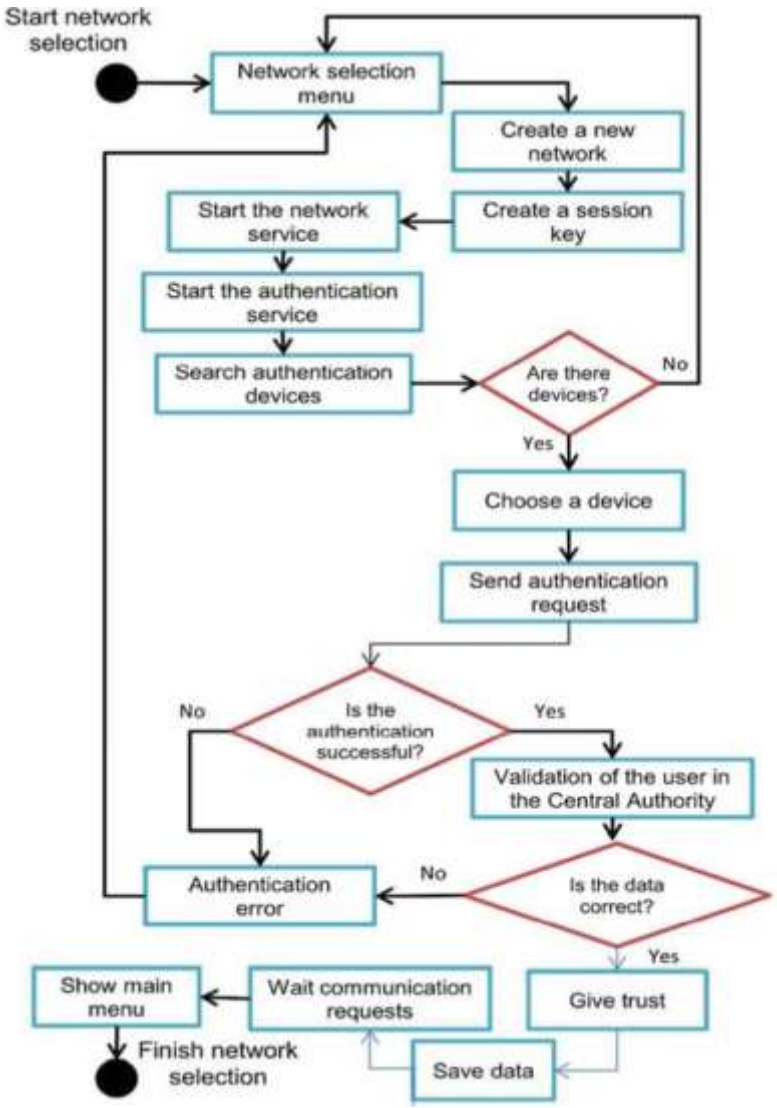

Fig.3 New System Design procedure

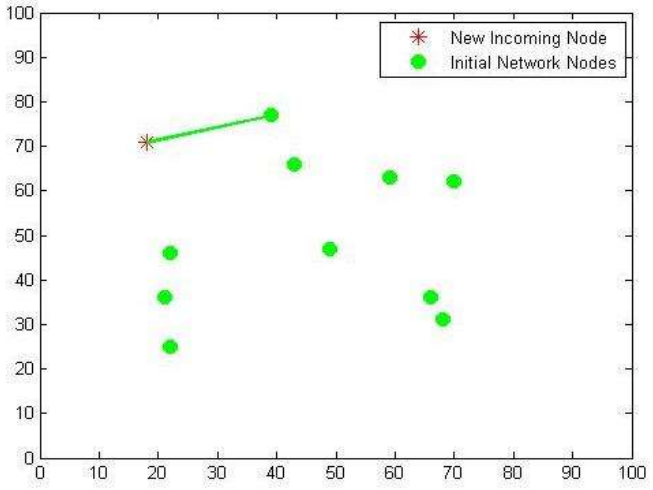

Fig.4 Analysis of Design and authentication procedure.

4. Procedure Action

Once the validation/registration process of the user in the device has been done, he/she must determine whether to add a new System or participate in an existing one. If he/she decides to add a new System, it begins the procedure shown in Fig. 3. First, a session key will be generated. Then, the node will start its services (including the System and authentication services). Finally, it will wait for requests from other devices that want to add the System. If the user wants to become part of an existing System, 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 System, 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 System . 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 System. 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 System and also to send its data to the System. This update could be for only one user or for all users in the System 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 System .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.

5. Conclusion

The Proposed Procedure allows the Design and management of a spontaneous mobile ad hoc System. It is based on a social System imitating the behavior of human relationships. Thus, each user will work to maintain the System, improve the services offered, and provide information to other System users. This method provides some procedures for self-configuration: a unique IP address is assigned to each device. We have also Add a user-friendly application that has minimal interaction with the user. The security schemes included in the Procedure allow protected 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 System ing: An Application-Oriented Approach to Ad-
hoc System ing," IEEE Comm. Magazine, vol. 39, no. 6, pp. 176-181, June 2013.
2. J. Lloret, L. Shu, R. Lacuesta, and M. Chen, "User-Oriented and Service-Oriented Spontaneous Ad Hoc and Sensor
Mobile System s," Ad Hoc and Sensor Mobile System s, vol. 14, nos. 1/2, pp. 1-8, 2012.
3. S. Preuß and C.H. Cap, "Overview of Spontaneous System ing -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 System to Share WWW Access,"
EURASIP J. Mobile Comm. and System ing, 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 Mobile
Sensor System s," Computer Comm., vol. 30, nos. 11/12, pp. 2314-2341, Sept.2007.
6. V. Kumar and M.L. Das, "Securing Mobile Sensor System s with Public Key Techniques," Ad Hoc and Sensor
Mobile System s, vol. 5, nos. 3/4, pp. 189-201, 2008.

Authors Bibliography

Vatnala Chenna goud completed his Master Computer Application in Osmania University. Hyderabad. A.P His Interested Areas are MANETS, Software Engineering.