An Efficient and Secure Scheme for the Spontaneous Networks using Hybrid Symmetric or Asymmetric Technology

Mr. Jithesh P
Department of CS&E
KVG College of Engg.
Sullia, DK, Karnataka
VTU, Belgaum

Mr. Kishor Kumar K
Assistant Professor
Department of CS&E
KVG College of Engg.
Sullia, DK, Karnataka
VTU, Belgaum

Dr. Antony P J
Director of PG Studies,
Department of CS&E
KVG College of Engg.
Sullia, DK, Karnataka
VTU, Belgaum

***Abstract*-The paper presents an efficient and secure protocol scheme for the spontaneous wireless adhoc networks without using the central authority or any other external authorities. The system uses a symmetric and asymmetric cryptography in this scheme. The users can share the resources and offer new services in a secure environment. The secure protocol scheme has the capability to create the network and share the services in a secure environment without any external support. The system presents a complete self configured secure protocol without using the central authority.**

Keywords-Spontaneous networks, distributed certification authority, symmetric cryptography.

I. INTRODUCTION

In the modern world, mobile communication is very necessary. The growth of mobile communication is mainly due to the mobility offered to users and providing the access to information anywhere. Spontaneous adhoc networks [1] are created by a group of mobile terminals placed in a close location that communicates with each other sharing the resources or services in a small period of time and in a limited space. The spontaneous networks are implemented in devices like laptops, PDA's or mobile phones.

Spontaneous networks are user friendly security mechanisms. It can perform the functions like user identification, authorization, address assignment and safety. The reliable communication and node authorization in mobile adhoc networks can be performed by key exchange mechanisms for the authorization of the nodes and user authentication. In this system security is implemented based on the service required by the users by creating a trust network to get a distributed certification authority.

In the system, the certification authority is distributed between the users that trust the new user. The network management system is also distributed that allows the network to have a distributed name service. In the network implementation, the system applies symmetric cryptography and asymmetric cryptography. Each device has a public-private key pair for device identification denotes the asymmetric cryptography. The symmetric cryptography is used to exchange session keys between nodes. The system allows the nodes to check the authenticity of their IP address [2].

II. RELATED WORK

Backstrom and Nadjm-Tehrani [3] developed the first real spontaneous network that offers services dynamically using the Jini technology. Feeney [4] developed Spontnet, a prototype implementation of a simple ad hoc network configuration utility based on the key ideas of spontaneous networks. Rekimoto [5] introduced the concept of synchronous user operation, a user interface technology for establishing spontaneous network connections between digital devices. Latvakoski [6] explains a communication architecture concept for spontaneous networks, combining application level spontaneous group communication and ad hoc networking.

Untz [7] proposes a lightweight and efficient interconnection protocol suitable for spontaneous edge networks. This method considers the problem of spontaneous edge networks. With this term 'Lilith', the system designate networks that interconnect hosts by means of different physical and link layer technologies and in which all or some of hosts are organized as a multihop ad

hoc network. Gallo [8] pursued two targets in spontaneous networks. One is to maximize responsiveness given some constraints on the energy cost and the other is to minimize the energy cost given certain requirements on the responsiveness. Danzeisen [9] apply WEP, the regular security mechanism used in Wireless LANs, available in the IEEE 802.11 wireless protocol. Wireless communication technologies enabled the possibility of building spontaneous networks between two or more users to exchange data.

Kotz [10] describe AnonySense that allows applications to submit sensing tasks that will be distributed across anonymous participating mobile devices. The system describes trust model, and the security properties that drove the design of the AnonySense system. This method does not tackle routing issues in spontaneous ad hoc wireless networks. Lacuesta [11] shows two secure spontaneous wireless ad hoc network protocols for wireless mesh clients that are based on the computational costs. They are weak protocol and the strong protocol. These protocols are related on the trust of the users and guarantee a secure protocol between the users and the mesh routers. Liu [12] propose an Adaptive and Efficient Peer-to-peer Search (AEPS) approach for dependable service integration on service-oriented architecture based on a number of social behavior patterns.

III. PROPOSED SYSTEM

The spontaneous network architecture is shown by the diagram. The network consists of one or several node. The user can do the network search to determine whether to create network or to participate in an existing one. After the authentication procedure, the nodes can perform several activities. It will also get services from the other trusted nodes.

A. *Node joining procedure*

The procedure allows the automatic configuration of logical, physical parameters and the communication. The system works on the use of an identity card and certificate. The identity card includes public and private components. The public component is used as the logical identity. The logical identity allows the nodes to identify it. The logical identity is unique for each user. The examples for the logical identity are name, photograph, port number, finger print etc.Apart from this, the public component contains user's public key, the creation and expiration dates, an IP address proposed by the user and the user signature. The system uses the secure hash algorithm (SHA-1) for the creation of the user signature. The SHA-1 algorithm will apply on the previous data to obtain the data summary. This data summary is signed with the user's private key. The private component contains the private key of the user. First of all, the user gives the personal information (logical identity) when he uses the system first time. This information will consider as the security information and stored permanently in the device for the future use.

The system is not using the centralized authority for the validation of the identity card. The nodes automatically do the validation of the integrity and authorization. The system can use any trusted node as the certification authority. Thus the system uses a distributed certification authority among the trusted nodes. The system will validate the data after collecting the certificate from a trusted node. In the network system, all the nodes can be act as both clients and servers. The first node is responsible for creating the spontaneous network. The node generates a random session key that will be exchanged with new nodes after the authentication phase.

The node joining procedure is as follows. First, the node will generate a network key. Then it will check for the existence of

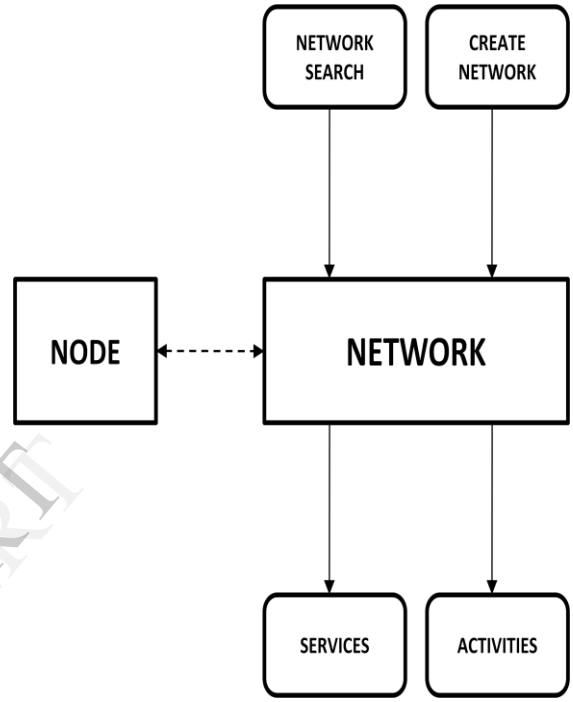

Fig. 1. Architecture of Spontaneous Networks

the new network connection. If a new network connection is there, it will exchange the identity card first. After this, node authentication and authorization takes place. Then the agreement on the session key, transmission protocol and speed takes place. The system checks for IP duplication is there or not. If IP duplication is there it will go for other IP assignment.

The security of the system is based on the symmetric cryptography and the asymmetric cryptography schemes. Here the symmetric key is used as a session key to encrypt the secret messages between trusted nodes. The system uses Advanced Encryption Standard (AES) for the symmetric encryption scheme. The asymmetric key encryption scheme is used for the distribution of the session key and for the user authentication process. The system uses RSA cryptographic algorithm for the asymmetric key encryption scheme.

B. *Discovery of the services*

A user can ask other devices in order to get the available services. The node has an agreement to allow access to its services and to access the services offered by other nodes. The system consists of two trust levels. One node can either

trust other node or not. The trust is based on the validated identity card. The trust can also be obtain using the asymmetric form or trusted chain method by using the transitive rule (p=q, q=r => p=r).The trust level can change overtime depending on the nodes behavior.

IV. PROTOCOL SCHEME AND NETWORK MANAGEMENT

The system is created using the information provided by users. In the network, each node is identified by an IP address. The network services are shared by TCP connections. By using the diffusion process, a request to multiple nodes is established. In the network, nodes can send request to update network information .Then they will get the identity cards of the all nodes in the network.

A. *Creation of the spontaneous networks*

The first node in the network will set the common settings of the network. The common settings include session identity and session key. Each node in the network is responsible for configure its own data. The data includes IP port and user data.

B. *Working procedure of the protocol scheme*

In the protocol operation, first the user makes the validation or registration process in the device. After that the user will decide whether to create a network or to participate in an existing one. The network creation algorithm is given below.

After the authentication process, the node can perform several operations .The operations include display the nodes, modify the trust of the nodes and update the information. The authenticated node can process an authentication request and it can also reply to an information request. It can send data to one node or all nodes and can modify the data. There is an option for the node to leave the network also.

1. Start
2. Start the network selection
3 .Display the network selection menu
4. Create a new network
5. Create a session key
6. Start the network service
7. Start the authentication service
8. Search for the authentication devices
9. If there are no devices in the communication range
Then goto step 3
10. Choose a device to communicate
11. Send authentication request to the device
12. If the authentication is not successful
Then print “Authentication error”goto step 3
13. Check the validation process of the user in the trusted nodes.
14. If the data is not correct
Then print “Authentication error” goto step 3
15. Give the trust to the nodes
16. Save the data
17. Wait for the communication request
18. Display the main menu
19. Finish the network selection
20. Stop

Fig. 2 Algorithm for the Spontaneous Network creation

The authenticated node will send the data encrypted with the public key to the other node. For this, the user has to select the remote node and write the data. Then the message is encrypted using the remote nodes public key. It generates a packet and sends to the remote node. The receiver node will check for the data packets.

If the packet is not encrypted, the message can be see directly to the user. If the message is encrypted, it will go for the checking of the type of the key. If the key is public, the decode operation will be done with the private key. Otherwise the key will be a session key. Then the packet will decode using the session key. After this decoding process, the message will be displayed to the user.

V. IMPLEMENTATION

The proposed system is a wireless network based application. Study on advantages and disadvantages of spontaneous networks are made. The various wireless devices for the spontaneous networks are also studied. A study on these software made, that is how to use in the project, how to execute and debug, how to install. The system is not using the database for the project. The system is using java language for the implementation phase. The first step in implementation phase is to collect the required software and how to install the software initial configuration into system. The first work is to generate keys for the node. The keys are public key, private key and session key. Port number, Unique ID and IP address is assigned to the node. The next step is for the network search. If a network exists, the node joins in the network otherwise it creates a new network. The modules of the proposed system are new network creation, request connection, authenticating new node, service management, service discovery, request certificate, issuing certificate and update request.

VI. PERFORMANCE DISCUSSION

The performance of the system is based on several measures. The first performance measure is based on the response time taken by the cryptographic operations. Here we are using RSA algorithm for the asymmetric cryptography. The system also using symmetric cryptography .In this system, symmetrical operations are used as the security operations for the protocol. The symmetric operations take the lower time cost. The other performance measures are the storage memory size needed for the configuration data and the memory needed to implement the protocol. The memory needed depends on the number of nodes participating in the spontaneous network. In the proposed system, the need of user intervention is low and self configuration is required for the nodes in the network. Here the security offered is more compared to others. The system is using java language for the implementation.

VII. CONCLUSION AND FUTURE WORK

The paper introduced an efficient and secure protocol scheme for the spontaneous networks without using the central authority. In the system, the user can participate in

the spontaneous network without any advanced technical knowledge. The security is issued for the services in the spontaneous network. As an extension, the system can add the intrusion detection mechanism in the spontaneous networks.

REFERENCES

[1] http://en.wikipedia.org/wiki/Computer_network#History.

[2] R. Lacuesta and L. Penalver, "Automatic Configuration of Ad-Hoc Networks: Establishing Unique IP Link-Local Addresses," Proc. Int'l Conf. Emerging Security Information, Systems and Technologies (SECURWARE '07), 2007

[3] J. Backstrom and S. Nadjm-Tehrani, "Design of a Contact Service in a Jini-Based Spontaneous Network," Proc. Int'l Conf. and Exhibits on the Convergence of IT and Comm., Aug. 2001.

[4] L.M. Feeney, B. Ahlgren, A. Westerlund, and A. Dunkels, "Spontnet: Experiences in Configuring and Securing Small Ad Hoc Networks," Proc. Fifth Int'l Workshop Network Appliances, Oct. 2002.

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

[6] 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.

[7] V. Untz, M. Heusse, F. Rousseau, and A. Duda, "Lilith: an Interconnection Architecture Based on Label Switching for Spontaneous Edge Networks," Proc. First Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (Mobiquitous '04), Aug. 2004.

[8] S. Gallo, L. Galluccio, G. Morabito, and S. Palazzo, "Rapid and Energy Efficient Neighbor Discovery for Spontaneous Networks," Proc. Seventh ACM Int'l Symp. Modeling, Analysis and Simulation of Wireless and Mobile Systems, Oct. 2004.

[9] M. Danzeisen, T. Braun, S. Winiker, D. Rodellar, "Implementation of a Cellular Framework for Spontaneous Network Establishment," Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005.

[10] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "Anonysense: Privacy-Aware People-Centric Sensing," Proc. Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '08), pp. 17-20, June 2008.

[11] R. Lacuesta, J. Lloret, M. Garcia, and L. Penalver, "Two Secure and Energy-Saving Spontaneous Ad-Hoc Protocol for Wireless Mesh Client Networks," J. Network and Computer Applications, vol. 34, no. 2, pp. 492-505, Mar. 2011.

[12] L. Liu, J. Xu, N. Antonopoulos, J. Li, and K. Wu, "Adaptive Service Discovery on Service-Oriented and Spontaneous Sensor Systems," Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/2, pp. 107-132, 2012.