Dynamic Key for Secure Communication among the Flexible Nodes

Vijay Kumar Mahto[1], D. PraveenKumar[2]

[1]M.Tech, Department of Computer Science and Engineering,
Hindustan University, Chennai-603103, India

[2]Assistant Professor, Department of Computer Science and Engineering,
Hindustan University, Chennai-603103, India

Abstract*: This project presents a dynamic key for secure communication among the flexible node 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. Trust is based on the first visual contact between users. Our proposal is a complete self-configured secure protocol that is able to create the network and share secure services without any infrastructure. 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. We have designed and developed it in devices with limited resources. 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. Finally, we provide a security analysis of the system.*

Keywords: Distributed protocol, secure protocol, Spontaneous network, Wireless ad hoc networks, Dynamic key.

1.Introduction

The modern era of communication there is 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. Spontaneous ad hoc networks are formed by a set of mobile terminals placed in a close location that communicate with each other, sharing resources, services or computing time during a limited period of time and in a limited space, following human interaction pattern. People are attached to a group for a while, and then they leave. Network management should be transparent to the user. A spontaneous network is a special case of ad hoc networks. They usually have little or no dependence on a central administration. Spontaneous networks can be wired or wireless. We consider only wireless spontaneous networks in this paper. Their objective is the integration of 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.

Configuration services in spontaneous networks depend significantly on network size, the nature of the participating nodes and running applications. Spontaneous networks imitate human relations while having adaptability to new conditions and fault tolerance (the failure of a device or service should not damage the functionality). Methods based on imitating the behavior of human relations facilitate secure integration of services in spontaneous networks. Furthermore, cooperation among the nodes and quality of service for all shared network services should be provided. 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. Security of data is a major concern in the present time. 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 (or is an external node) all the time. Moreover, CA node must have higher computing capacity. Security should be based on the required confidentiality, node cooperation, anonymity, and privacy. Exchanging photos between friends requires less security than exchanging confidential documents between enterprise managers.

Moreover, all nodes may not be able to execute routing and/or security protocols. Energy constraints, node variability, error rate, and bandwidth limitations mandate the design and use of adaptive routing and security mechanisms, for any type of devices and scenarios. Dynamic networks with flexible memberships, group signatures, and distributed signatures are difficult to manage. To achieve a reliable communication and node authorization in mobile ad hoc networks, key exchange mechanisms for node authorization and user authentication are needed. The related literature shows several security methods such as pre-distribution key algorithms, symmetric and asymmetric algorithms, intermediate node-based methods, and hybrid methods. But these methods are not enough for spontaneous networks because they need an initial configuration (i.e., network configuration) or external authorities.

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. The network management is also distributed, which allows the network to have a distributed name service. We apply asymmetric cryptography, where each device has a public-private key pair for device identification and symmetric cryptography to exchange session keys between nodes. There are no anonymous users, because confidentiality and validity are based on user identification.

2. Background and System Module

- Network construction
- Server
- User status
- Group key generation
- Data access

2.1 Network construction

This module is developed in order to create a dynamic network. In a network, nodes are interconnected with a particular group and the information can be shared among them. For the successful data transfer the network must be properly controlled and handled. Every node is interconnected & this forms a network.

2.2 Server

Here the server will have the entire details about all the group information. It distributes the data to client in a particular group. Server is responsible for maintaining all the group information. If any user will removed from a particular group means it will instruct to the group member to change the group id and send the SMS to all group members.

2.3 User status

Users can be moved from one group to another group and he will also participated in more than one group. Depending upon the user status they can share their information with the group member. All the user status information is to be maintained here. If a new user login or the existing user logged in or logged out all that information about a user must maintained for authenticate.

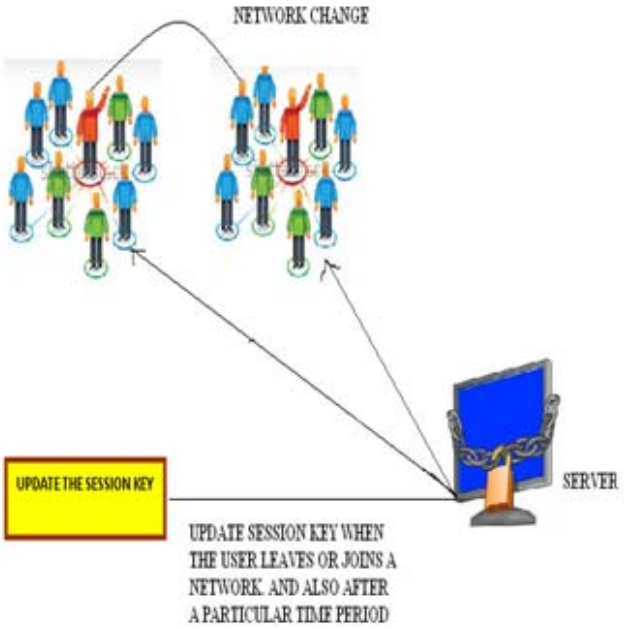
2.4 Group key generation

In this module we have to create group key as well as the individual key then share the key between the group members via SMS. Any changes occurs in the group then change the group key and then send that key to the other entire group member. This process is done whenever any changes made in that group.

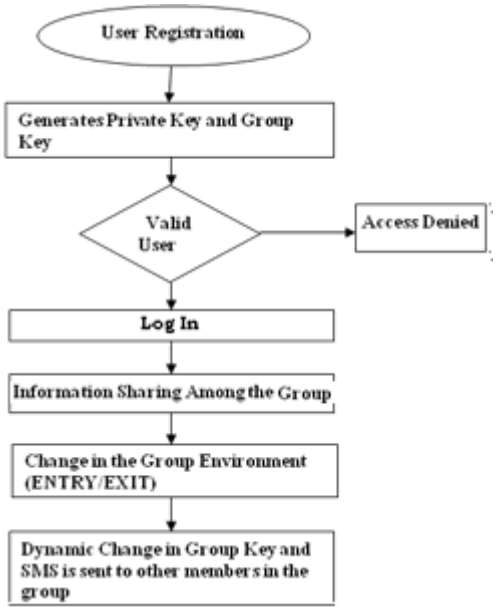
2.5 Data access

If a user wants to access any information about any user then he will give his individual key as well as the group key. If he want to access the information about the user, but the user is not belongs to their group is not possible. He can only access the user's information within their group only. Without knowledge of the other group key it is not possible to access the information.

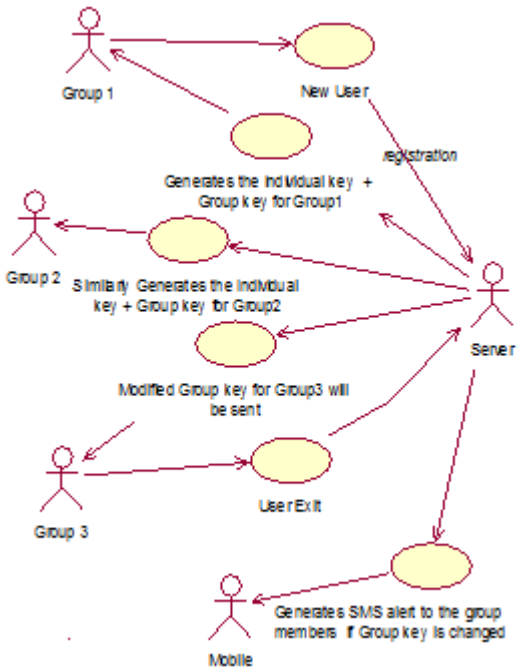
3. System Architecture



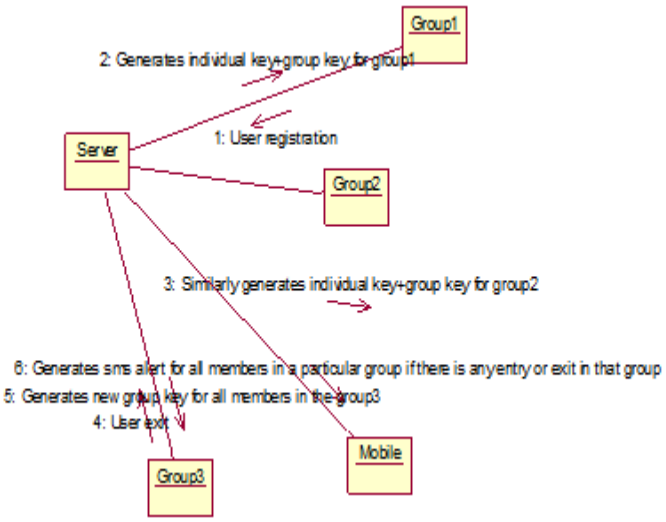
3.1 Dataflow diagram



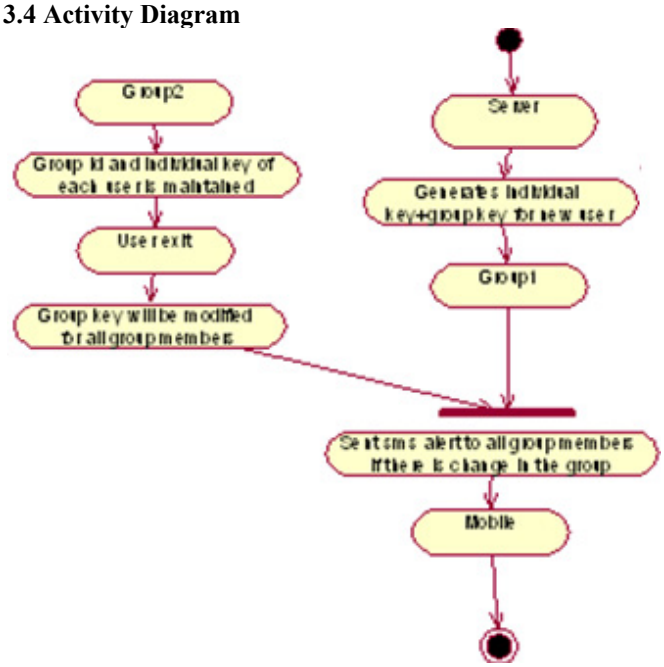
3.2 Use case diagram



3.3 Collaboration diagram



3.4 Activity Diagram



4. Conclusion

To summarize, In this project we have implemented a flexible group key management scheme to protect the network from attacker, so that, we can increase the security levels of the network. The performance level of our approaches will be better than other approaches.

References

[1] L.M. Feeney, B. Ahlgren, and A. Wester lund, "Spontaneous Networking: An Application-Oriented Approach to Ad-hoc Networking," IEEE Comm. Magazine, vol. 39, no. 6, pp. 176-181,
[2] June 2001.
[3] 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.
[4] S. Preuß and C.H. Cap, "Overview of Spontaneous Networking -Evolving Concepts and Technologies," Rostocker Informatik-Berichte, vol. 24, pp. 113-123, 2000.
[5] R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver, "A Spontaneous Ad-Hoc Network to Share WWW Access," EURASIP J. WirelessComm. and Networking, vol. 2010, article 18, 2010.
[6] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "ASurvey of Key Management Schemes in Wireless Sensor Networks,"Computer Comm., vol. 30, nos. 11/12, pp. 2314-2341, Sept.2007.
[7] V. Kumar and M.L. Das, "Securing Wireless Sensor Networkswith Public Key Techniques," Ad Hoc and Sensor Wireless Networks,vol. 5, nos. 3/4, pp. 189-201, 2008.
[8] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: A Lightweight Hopby-Hop Authentication Protocol For Ad-Hoc Networks," Ad HocNetworks J., vol. 4, no. 5, pp. 567-585, Sept. 2006.
[9] Noack and S. Spitz, "Dynamic Threshold Cryptosystemwithout Group Manager," Network

Protocols and Algorithms,vol. 1, no. 1, Oct. 2009.
[10] J. Yan, J. Ma, F. Li, and S.J. Moon, "Key Pre-distribution Schemewith Node Revocation for Wireless Sensor Networks," Ad Hoc andSensor Wireless Networks, vol. 10, nos. 2/3, pp. 235-251, 2010.
[11] M. Mukesh and K.R. Rishi, "Security Aspects in Mobile Ad HocNetwork (MANETs): Technical Review," Int'l J. Computer Applications, vol. 12, no. 2, pp. 37-43, Dec. 2010.

Author Profile

Vijay Kumar Mahto received the B. Tech degree in Information Technology from Hindustan Institute of Technology & Science in 2012 and currently pursuing M. Tech degree in Computer Science from Hindustan Institute of Technology & Science in 2014