



Procedure To Establish A Secure Self-Configured Environment For Data Distribution And Services Sharing Among Users

1Syam Kumar Nallamothu2Amanatulla Mohammad, 3Sayeed Yasin
Dept. of CSE, Nimra Institute of Science & Technology, Vijayawada, AP, India

Abstract:

A spontaneous network is a particular case of ad hoc networks. They usually have little or no dependence on a centralized administration. Spontaneous networks can be wired or wireless. We regard as 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. To resolve mentioned security issues we used an authentication phase and a trust phase. Moreover we presented a method to allow nodes to check the legitimacy of their IP addresses while not generating duplicated IP addresses. The mechanism helps nodes to authenticate by using their IP addresses. We have used this mechanism in the secure protocol presented in this paper.

Keywords: Distributed protocol, secure protocol, spontaneous network, wireless ad hoc networks.

Introduction:

Spontaneous ad hoc networks necessitate well defined, efficient and user-friendly security mechanisms. Tasks to be performed include user identification, their authorization, address assignment, name service, operation and safety. Usually wireless networks with infrastructure use Certificate Authority (CA) servers to supervise node authentication and trust. This paper presents a secure protocol for spontaneous wireless ad hoc networks which uses a hybrid symmetric/asymmetric scheme and the trust between users in order to switch over the initial data and to replace the secret keys that will be used to encrypt the data. Trust is based on the first visual contact between users. Our proposal is an absolute 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 executed in order to test the protocol procedure and performance. Ultimately we compare the protocol with other spontaneous ad hoc network protocols in order to emphasize its features and we provide a security analysis of the system.

Related Work: Gallo et al. pursued two targets in unprompted networks to make best use of responsiveness given some constraints on the energy cost and to minimize the energy cost given certain requirements on the responsiveness. Liu et al. show how networked nodes can originally support and cooperate with each other in a peer-to-peer (P2P) manner to quickly discover and self-configure any services available on the disaster area and bring real-time capability by self-organizing themselves in spontaneous groups to offer higher flexibility and adaptability for disaster monitoring and relief.

Existing Method:

The related literature shows quite a few security methods such as predistribution 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.

Disadvantages:

None of the existing methods propose a secure spontaneous network protocol based on user trust that provides node authenticity, integrity checking, and privacy.

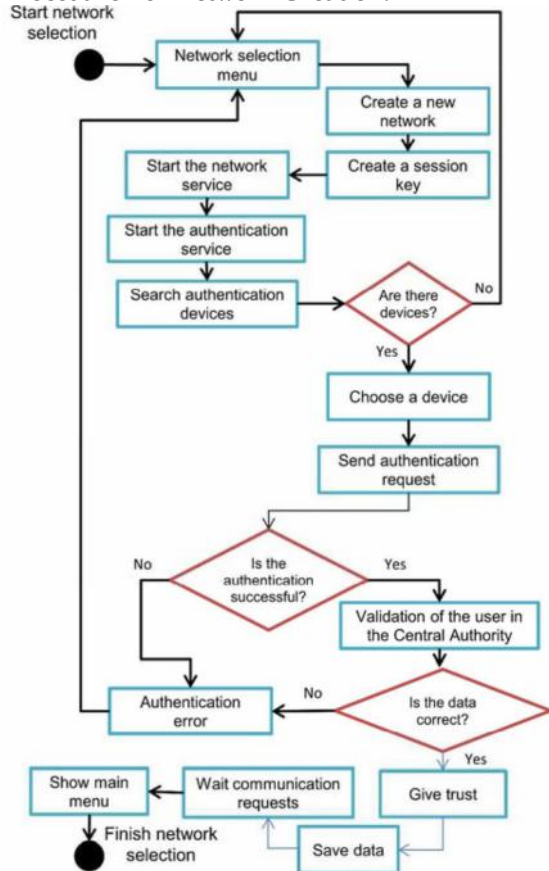
Proposed Method:

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.

Advantages:

The network and protocol proposed can establish a secure self-configured environment for data distribution and resources and services sharing among users.

Procedure For Network Creation:



Joining Procedure:

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.

Services Discovery:

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.

Trusted Chain And Changing Trust Level:

The network is created using the information provided by users, thus, each node is identified by an IP address. Services are shared using TCP connections. Nodes can also send requests to update network information. The reply will contain the identity cards of all nodes in the network. The

node replying to this request must sign this data ensuring the authenticity of the shipment. If it is a trusted node, its validity is also ensured, since trusted nodes have been responsible for validating their previous certificates.

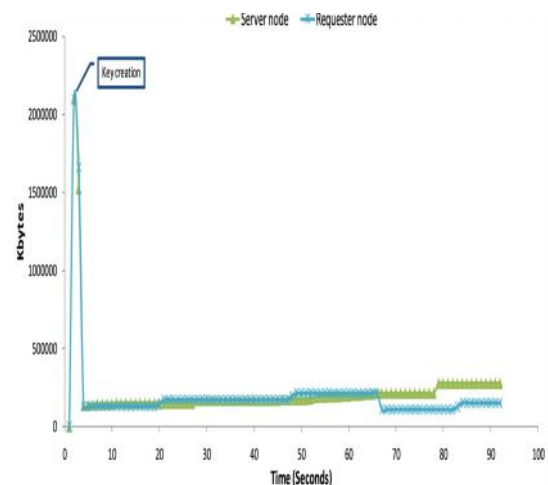
Protocol Operation:

The UML is a visual specification standardized language that is built to model object oriented systems. We use keys, activities, and use cases (diagrams offered by the standard) to define the processes, the structure of the classes in the system, and the behaviour of objects or operations. 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, To request a certificate, the node sends a request certificate message to its trusted nodes. The application generates a packet to request the certificate to its trust nodes which are selected from the database.

Protocol Implementation:

When a device wants to join a spontaneous network it has to start the process by sending a Discovery request packet which contains the Logical Identity of the user in order to let the destinations know the sender device. The receivers will reply with the Discovery reply packet with their Logical Identity, their IP address, and network mask. This information is then used to learn the selected device to authenticate and to propose an IP inside that network IP range. The authentication request packet is used for the new device authentication. The authentication reply packet confirms that the proposed IP and the email are unique in the network, so the new device is officially authenticated.

Experimental Results:



It shows when a new node joins the spontaneous network, by both nodes for all the processes from certificate creation to data transfer. The node that generates the network uses more memory

because it is incharge of sending two messages for the authentication process, one with the symmetric encryption and another with asymmetric encryption.

Conclusion:

The design of the protocol is based on a social network imitating the behaviour of human relationships that allow the creation and management of a spontaneous wireless ad hoc network. Each user will work to maintain the network, improve the services offered, and provide information to other network users. The DNS can be managed efficiently and the services can be discovered automatically. We have also created a user-friendly application that has minimal interaction with the user. A user without advanced technical knowledge can set up and participate in a spontaneous network. The security schemes included in the protocol allow secure communication between end users.

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," Rostocker Informatik-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.
- [7] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: A Lightweight Hopby-Hop Authentication Protocol For Ad-Hoc Networks," Ad Hoc Networks J., vol. 4, no. 5, pp. 567-585, Sept. 2006.
- [8] A. Noack and S. Spitz, "Dynamic Threshold Cryptosystem without Group Manager," Network Protocols and Algorithms, vol. 1, no. 1, Oct. 2009.
- [9] J. Yan, J. Ma, F. Li, and S.J. Moon, "Key Pre-distribution Scheme with Node Revocation for Wireless Sensor Networks," Ad Hoc and Sensor

Wireless Networks, vol. 10, nos. 2/3, pp. 235-251, 2010.

- [10] 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.
- [11] 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.
- [12] 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.



Creation.



AMANATULLAMOHAMAD received his M.Tech from CSE-NIMRA college of Engineering & Technology (JNTUK, Kakinada), Ibrahimpatnam, Vijayawada. He is currently working as an Assistant Professor in NIMRA Institute of Science & Technology in the Department of Computer Science & Technology in the Department of Computer Science & Engineering, Ibrahimpatnam, Vijayawada. He has more than four years Experience in teaching. Email: amanatulla@gmail.com



SAYEED YASIN received his MTECH in Computer Science & Engg from JNTU Hyderabad. He is pursuing Ph.D in Rayalaseema University, Kurnool. He is currently working as Assoc. Professor & HOD in Nimra Institute of Science & Technology the Department of Computers Science and Engineering, Vijayawada. He has more than Eight years of experience in teaching. His area of interests are wireless networks & programming. E-Mail: sdyasin761@gmail.com