International Journal of Science Engineering and Advance Technology, IJSEAT, Vol 2, Issue 11, November - 2014 | ISSN 2321-6905

International Journal of Science Engineering and Advance Technology

Enhanced Protocol for data exchange through Natural Wireless Ad Hoc Networks

[1] M.Vamsi Krishna,[2] R.Satya Ravindra Babu
1,2Dept. of CSE, Chaitanya Institute of Science & Technology, Kakinada, AP, India

Abstract:

Conviction is based on the primary illustration contact between users. Our proposal is a absolute self-configured protected procedure that is capable to generate the network and distribute secure services without any infrastructure. This paper presents a protected procedure for impulsive wireless ad hoc networks which uses a hybrid symmetric/ asymmetric method and the trust between users in order to substitute the initial data and to exchange the secret keys that will be used to encrypt the data.

1. Introduction

The objective of the procedure is the incorporation of services and devices in the same environment facilitating the user to have immediate service without any external infrastructure. Because these networks are executed in devices such as laptops, PDAs or mobile phones with limited abilities they must use a frivolous procedure and new methods to control manage and integrate them.

Impulsive ad hoc networks necessitate well defined, efficient and user-friendly security mechanisms. Tasks to be carried out include user identification, their authorization, address assignment, name service, operation and safety. Substituting photos between friends necessitates less security than exchanging private documents between enterprise managers. Moreover, all nodes may not be able to implement 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 supple memberships, group signatures and distributed signatures are hard to handle. To attain a dependable communication and node authorization in mobile ad hoc networks, key exchange methods for node authorization and user authentication are needed.

Consequently the certification authority is distributed between the users that trust the new user. The network management is also distributed which permits the network to have a distributed name service. We pertain asymmetric cryptography where each device has a public-private key pair for device recognition and symmetric cryptography to exchange session keys between nodes. There are no anonymous users because confidentiality and validity are based on user identification.

Spontaneous ad hoc networks are shaped by a set of mobile terminals placed in a secure location that converse 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 fond of to a group of people for a while and then leave. Network management should be translucent to the user. A spontaneous network is a special case of ad hoc networks. They typically have little or no confidence on a centralized administration. Spontaneous networks can be wired or wireless.

2. Related Work:

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

In, Untz et al. propose a lightweight and efficient interconnection protocol suitable for spontaneous edge networks. They design and implement Lilith, a prototype of an interconnection node for spontaneous edge networks. It uses MPLS and allows different communication paths on a per flow basis, provides seamless switching between operational and back-up paths, and makes available information on destination reachability.

Danzeisen et al. apply WEP, the regular security mechanism used in Wireless LANs, available by default in the IEEE 802.11 wireless protocol. Other proposals that did not discuss security aspects could also apply this default

solution. Although it was available to us, we did not use it because WEP is vulnerable to hacking attacks, and better solutions, e.g., WPA, WPA2 should be considered instead.
Spontaneous networks are also special case of humancentric networks. Cornelius et al. implemented and evaluated AnonySense, a general-purpose framework for anonymous opportunistic tasking and reporting, which allows applications to query and receive context through an expressive task language and by leveraging a broad range of sensor types on users' mobile devices, and at the same time respects the privacy of the users. This paper does not tackle routing issues in spontaneous ad hoc wireless networks. A paper that presents a security protocol for routing purposes, based on trust. It presents two secure and energy-saving spontaneous ad hoc protocols for wireless mesh client networks where two different security levels (weak and strong) are taken into account in the path when information is transmitted between users.

Literature Survey:

3. Problem Statement:

3.1: Existing System

The existing system 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.

Disadvantages :

- 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.

3.2: Proposed System

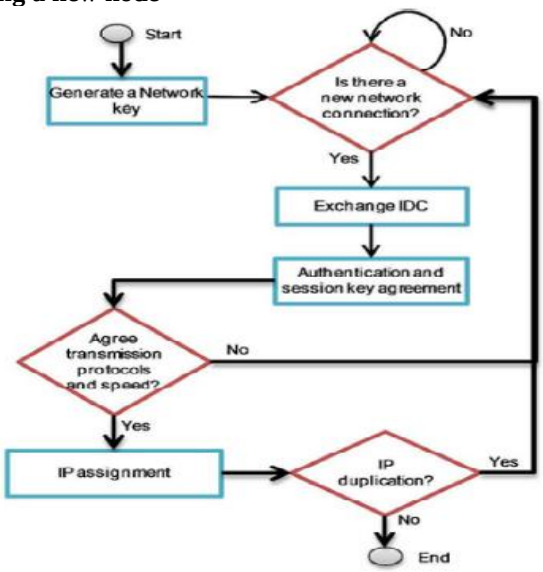
The network and protocol proposed in this paper can establish a secure self-configured environment for data distribution and resources and services sharing among users. Security is established based on the service required by the users, by building a trust network to obtain a distributed certification authority. A user is able to join the network because he/she knows someone that belongs to it.

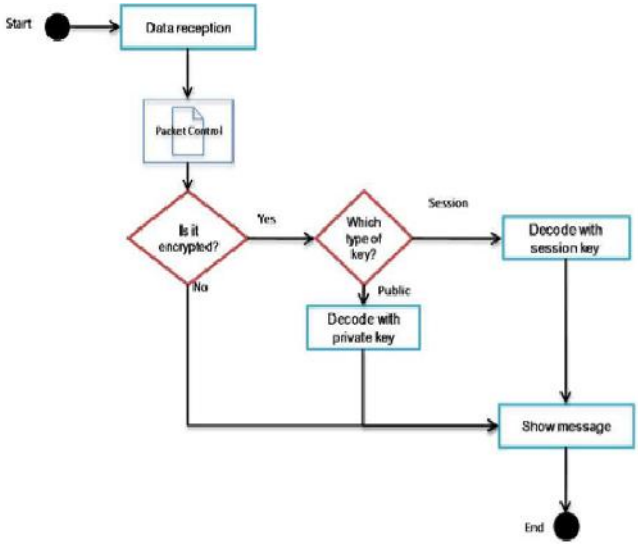
Advantages:

- We presented the basis to setup a secure spontaneous network.
- To solve mentioned security issues, we used an authentication phase and a trust phase.
- We presented a mechanism to allow nodes to check the authenticity of their IP addresses while not generating duplicated IP addresses.

4. SYSTEM ARCHITECTURE:

Joining a new node





Receiving Data Packets

5. Modules:

Modules Description:

Network Setup Model:

- The user can register and login with the owner permission whether to join new node and or an existing node or to create a network.
- The owner provides session key based on the requirements of the trusted user.

Trusted User and node creation Module:

- In this module, the trusted user gets login by admin permission.
- The data is shared between two trusted users by session key generation for their respective data's and encrypting their files.
- The user can only access the data file with the encrypted key if the user has the privilege to access the file.
- Validation of integrity and authentication is done automatically in each node.

New node Joining Module:

- By using Network based Intrusion Detection System (NIDS), the new node is created and they are joined to new nodes by respective procedures given by owner.
- The joining module is done with 3 phases:

New network creation module:

- In this module, we create a new network for the trusted users.
- The first node in the network will be responsible for setting the global settings of the spontaneous network.
- The second node first configures its user data and network security.
- Our protocol relies on a sub layer protocol **eg:** Bluetooth.
- After encountering the device, the authentication request is sent to another user.

Data transfer module:

- A node receives a data packet that is ciphered by a public key.
- When the server process received the packet, it is in charge of deciphering it with the private key of the user.

8. Conclusion:

In this paper, we show the design of a protocol that allows the creation and management of a spontaneous wireless ad hoc network. It is based on a social network imitating the behavior of human relationships. Thus, each user will work to maintain the network, improve the services offered, and provide information to other network users. We have provided some procedures for self-configuration: a unique

IP address is assigned to each device, 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 (bearing in mind the resource, processing, and energy limitations of ad hoc devices).

9. Enhancement:

The new paradigm is a hybrid of traditional broadcast encryption and group key agreement. In such a system, each member maintains a single public/secret key pair. Upon seeing the public keys of the members, a remote sender can securely broadcast to any intended subgroup chosen in an *ad hoc* way.

Even if all the nonintended members collude, they cannot extract any useful information from the transmitted messages. After the public group encryption key is extracted, both the computation overhead and the communication cost are independent of the group size

9. 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.

Sri. M. Vamsi krishna, well Known Author and excellent teacher Received M.Tech (AI &R), M.Tech (CS) from Andhra university is working as Professor and HOD, Department of CSE, Chaitanya Institute Science and Technology. He has 13 years of teaching & research experience. He has 20 publications of both national and international conferences /journals. His area of Interest includes AI, Computer Networks, information security, flavors of Unix Operating systems and other advances in computer Applications.

Mr.R.Satya Ravindra Babu is a student of Chaitanya Institute of Science and Technology, Madhavapatnam, JNTU, Kakinada. Presently he is pursuing his M.Tech [Computer Science and Engineering] from this college and he received his MCA in 2001 and M.Phil (Computer Science) in 2006 from Madurai Kamaraj University, Madurai, Tamil Nadu. His area of interest includes Cloud Computing, Computer Networks and Big Data, all current trends and techniques in Computer Science.