Research Paper

Volume : 3 | Issue : 5 | May 2014 • ISSN No 2277 - 8179

A Secure Authentication Protocol and Scalable Distributed Name System for Spontaneous Wireless Ad Hoc Networks

Engineering

KEYWORDS : Wireless ad hoc networks; spontaneous network; hybrid scheme; distributed name sysytem

Aswini S — S4 M.Tech, Dept of Computer Science & Engineering, N.S.S College of Engineering, Palakkad, Kerala, India

Mrs Maya Mohan — Assistant Professor, Department of Computer Science & Engineering, N.S.S College of Engineering, Palakkad, Kerala, India

ABSTRACT

In areas where there is little communication infrastructure or the existing infrastructure is inconvenient to use, wireless mobile users may still be able to communicate through the formation of spontaneous networks. A spontaneous network is a special case of wireless ad hoc networks. So the security needs in the spontaneous networks are much higher than those in the wired networks. This paper presents a well defined and efficient security mechanism for Spontaneous networks. Authentication protocol uses a hybrid symmetric/asymmetric scheme. Initial data exchange is based on the trust between users. Initial trust establishment is based on the visual contact between users. The protocol includes all functions needed to operate without any external support. To provide the secure group communication in spontaneous networks, a group key is used so that efficient symmetric encryption can be performed. A scalable Distributed Name System is also included in this paper. It can provide nodes in the network with secure name-to-address resolution and service discovery.

Introduction

A spontaneous network is a special case of ad hoc networks .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[1]. Its initial configuration is based on human interaction pattern [2]. In spontaneous ad hoc networks, mostly communication takes place among groups having some common objective, and the communication must be made reliable in regards of security and data transfer.

Performing communication in free space exposes ad hoc networks to different types of attacks [3]. So security is the major concern in spontaneous networks. To prevent such attacks, it is necessary to employ security mechanisms that ensure that only authorized nodes can participate in the network. To achieve reliable communication and node authorization, secure authentication protocols are needed. Encryption techniques are usually used to provide network security. It will leads to the need for secure key management mechanisms.

Existing security methods are mainly based on predistribution key algorithms [4]. A group based key pre-distribution scheme is proposed in [5]. Dynamic threshold cryptosystems are best suited to realize distributed signatures in dynamic networks [6]. But these methods are not suited for spontaneous networks because spontaneous network is a fully self organized network formed without initial configuration. It will be formed anytime, anywhere according to user needs. Also network size is usually small.

In this paper a new hybrid/ asymmetric scheme is proposed to improve the security in spontaneous networks. The proposed system will establish a secure self-configured environment for data distribution and resource sharing among users. Initial trust establishment is based on the visual contact between users and a distributed certification authority is also used for trust establishment [7]. Apply asymmetric cryptography for device authentication and symmetric cryptography to exchange information between nodes.

DNS (Domain Name Service) is used to provide the name-to-address resolution among nodes in the Internet [8]. Current DNS works on the basis of dedicated name servers. But it is inappropriate for name service in ad hoc networks due to the dynamic nature of ad hoc networks. If a node wants to find the IP corresponding to the name then it has to forward the request to the next server in the hierarchy of DNS servers. But for spontaneous networks such a hierarchy is difficult to maintain.

A new Distributed Name System is proposed in this paper to provide the name service. In spontaneous networks users can enter or leave the network at will. So a scalable, dynamic, and distributed key-value look up scheme is needed. Here each node will maintain a key-value look up map. This Name System will helps for the service discovery.

The sections are organized as follows. In section 2 related works are summarized. Proposed system is described in Section 3. Section 4 shows the simulation results . Finally section 5 gives the conclusion.

RELATED WORKS

L.M. Feeney, B. Ahlgren, A. Westerlund, and A. Dunkels have proposed Spontnet, a prototype implementation of a simple ad hoc network configuration utility based on basic concepts of spontaneous networking [9]. Spontnet allows users to distribute a group session key without previous shared context and to establish shared namespace. They also provide examples of collaborative applications that could be useful in a spontaneous networking environment.

Jaehoon Jeong, Jungsoo Park and Hyoungjun Kim proposed name service system based on secure multicast DNS for IPv6 Mobile Ad Hoc Networks in [10].They proposed an architecture of secure DNS system called as ANS (Ad Hoc Name Service System for IPv6 MANET) which can provide mobile nodes in IPv6 MANET with secure name-to-address resolution and service discovery on the basis of ANS and DNS service resource record (SRV).

Shahid Bashir, Baochun Li presents a key-value look up protocol (KELOP), for wireless ad hoc networks [11]. KELOP is a fully distributed best-effort protocol that relies only on the local information stored at each node to locate the closest estimates of the target. Instead of trying to locate the exact target node, KELOP's strategy is to work with the best estimate of the target node. This strategy results in low control-message overhead.

PROPOSED SYSTEM

Spontaneous Network Creation

A spontaneous network is created when a group of people come together for some collaborative activity. In this case, we can use the human interactions associated with the activity in order to establish the configuration infrastructure. The first node creates the spontaneous network and generates a random session key, which will be exchanged with new nodes after the authentication phase. However, each node must configure its own data (including the first node): IP, port, data security, and user data. This information will allow the node to become part of the network.

Joining Procedure

A node joining the spontaneous network only needs to perform some inexpensive authentication operations. To join the spontaneous network, each node should possess an Identity card (IDC). The identity card contains a Login ID, IP address proposed by the user, and the public key of the user. The public key and the corresponding private key of each user will be generated in the device itself. Fig. 1 shows the authentication procedure.

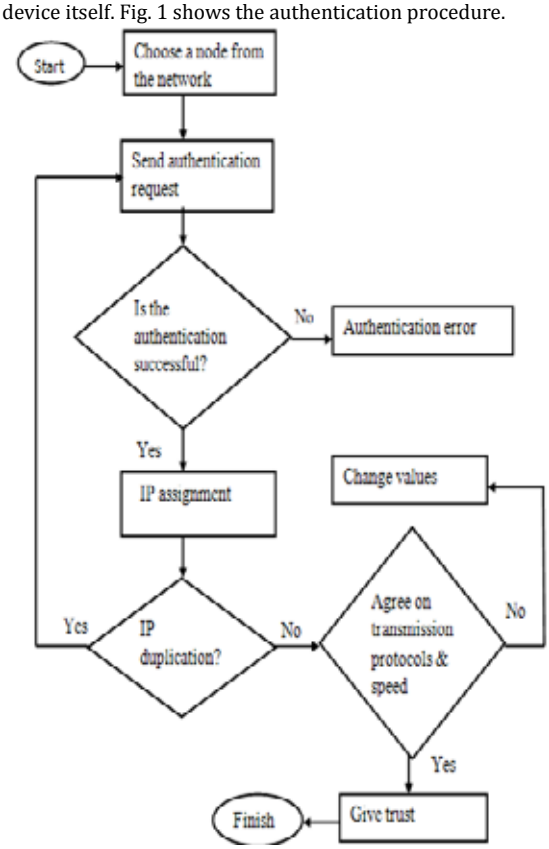

Fig.1: Authentication procedure

When a node B wants to join an existing network, it must choose a node within communication range and send an authentication request (e.g., node A). A will reply with its public key. Then, B will send its IDC encrypted with A's public key. Then, 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 and B should be physically close. Initial trust establishment is depending on whether A knows B or not. After validating B's IDC, A will send its IDC data to B. This will be signed by B's public key. B will validate A's IDC and will establish the trust and validity in A only by integrity verification and authentication. B can send authentication request to any of the existing node in the network.

Authentication is based on the asymmetric encryption algorithm. Rivest, Shamir & Adleman cryptographic algorithm (RSA) is used here. After successful authentication, a group key will be provided to the newly joined node for further communication. Advanced Encryption Standard (AES) algorithm is used for symmetric encryption. Group key will be used as the symmetric key. B generates an IP address which has a fixed part in the first two bytes and the rest is formed by a random number based on user data . Then the proposed IP address is send to all other nodes in the network to check whether the IP is duplicated in the network. It has to adjust it protocol and speed according to the network configurations. After that, B can access data, service provided by other devices in the network and also it can share its services to other nodes.

Secure Communication in Spontaneous Networks

When the node is authenticated, it is able to perform several tasks. For secure group communication group key is used. The communication between two nodes is secured by asymmetric encryption. Authenticated node can perform the following tasks.

- Request certificate from other nodes
- Send update request to other nodes
- Send information request
- Proper handling of authentication requests
- Discovery of services offered by the network
- Resource and service sharing

Secure Communication in Spontaneous Networks

Due to the dynamic topology, the current DNS (Domain Name System) is inappropriate for name service in mobile ad hoc network. In spontaneous networks, all are fully self organized nodes. So a distributed and scalable distributed name system is proposed here. To provide the name service each node has to maintain a key – value look up map. This will helps to map the login Id to the corresponding IP address of the device.

Authentication procedure is already described above. After the successful authentication of a new node, the node will become a trusted node in the network. All the trusted nodes of the network should have an entry in the key-value look-up map. This map should be maintained in all the network nodes. It needs updating at the time of node joining and node leaving. When the node leaves the network it will inform all other nodes that it is going to leave the network. Then the corresponding map entry is also deleted. This name service system is only suitable for networks with small size. It performs well for the spontaneous networks.

SIMULATION RESULTS

Netbeans IDE is used for the software simulation of spontaneous network. Security mechanisms and distributed name system is implemented using java programming. Javax.crypto package helps to implement the security mechanism. Java.util package is used to develop the distributed name system. Simulation results shows that distributed name system does not increase the communication cost. It will not increase the message overhead. Memory usage increases with the number of nodes in the network. But due to the small network size mobile devices can handle this.

CONCLUSION

This paper shows that, communication over spontaneous wireless ad hoc network is reliable in regards of security and data transfer. Here, the secure authentication protocol is based on the public key infrastructure and the data transmission scheme is based on the symmetric encryption. A distributed name system is used to perform name to IP address resolution and to discover shared services and resources. This is well suited for spontaneous networks due to its scalability. Simulation result shows that the proposed security scheme allows secure communication between nodes and distributed name system can provide nodes in the network with secure name-to-address resolution and service discovery. It does not cause any message overhead. Due to small size of networks, mobile devices can handle the memory requirements efficiently.

REFERENCE

[1] 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. | [2] L.M. Feeney, B. Ahlgren, and A. Westerlund, "Spontaneous Networking: An Application-Oriented Approach to Ad-hocNetworking," IEEE Comm. Magazine, vol. 39, no. 6, pp. 176-181, June 2001. | [3] 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. | [4] 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. | [5] Donggang Liu, Peng Ning, and Wenliang Du,"Group-based key predistribution for wireless sensor networks". TOSN, 4(2), 2008. | [6] A. Noack and S. Spitz, "Dynamic Threshold Cryptosystem without Group Manager," Network Protocols and Algorithms, vol. 1, no. 1, Oct. 2009. | [7] Raquel Lacuesta, Jaime Lloret, Miguel Garcia, Lourdes Pen˜alver,"Parallel Data Processing with MapReduce: A Survey", SIGMOD Record, Vol. 40, no. 4, Dec 2011 | [8] P. Mockapetris, "RFC-1034 Domain Names - Concepts and Facilities, " Network Working Group, 1987. | [9] 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. | [10] Jaehoon Jeong, Jungsoo Park and Hyoungjun Kim," DNS Name Service based on Secure Multicast DNS for IPv6 Mobile Ad Hoc Networks", Advanced Communication Technology, vol 1,2004. | [11] Shahid Bashir, Baochun Li, "KELOP: Distributed Key-Value Lookup in Wireless Ad Hoc Networks", ICCCN, page 471-476. IEEE, (2003) | |