IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Performance Evaluation of Spontaneous Wireless Ad Hoc Network

Swapnali D Patil[1], V.N.Nitnaware[2]

M.E Student, E&TC, Dr.D.Y. Patil School of Engineering Ambi, Talagaon, Pune, India[1]

Principal, E&TC, Dr.D.Y.Patil School of Engineering Ambi, Talagaon, Pune, India[2]

Abstract: Spontaneous wireless network is a scheme consists of ad hoc networking in which devices establish communication with nearby devices with anytime and anywhere without using any backbone network. The notion of ad hoc networks was often associated with communication on combat fields and at the site of a disaster area. It is a self-configured network for that we have to provide some basic services and application. To achieve this, authentication of devices is must. In this paper a secure protocol for spontaneous wireless ad hoc networks which uses an encryption 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. The protocol includes all functions needed to operate without any external support. Attacker node may send data which disturb the network. Main focus of paper is describes secure protocol with enhance security for spontaneous wireless ad hoc network.

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

I. INTRODUCTION

The 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 [1], [2]. People are attached to a group of people for a while, and then 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 centralized 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 behaviour of human relations facilitate secure integration of services in spontaneous networks [3]. Furthermore, cooperation among the nodes and quality of service for all shared network services should be provided [4].

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.

The rest of the paper is organized as follows: Section 2 presents the related work on spontaneous networks and shows the most well-known security mechanisms that can be applied to them. The proposed secure spontaneous network is detailed in Section 3. Section 4 analyses the simulation result by using different analytical parameter. Finally, Section 5 gives the conclusion and future work.

II. RELATED WORK

The related literature shows several security methods such as pre distribution key algorithms [5], symmetric and asymmetric algorithms, intermediate node-based methods [6], and hybrid methods [7]. But these methods are not enough for spontaneous networks because they need an initial configuration (i.e., network configuration) or external authorities (for example, central certification authorities). None of the existing papers propose a secure spontaneous network protocol based on user trust that

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

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 with node authenticity, integrity checking, and confidentiality. For node authentication and trust wireless network uses certificate authority.

III. SECURE SPONTANEOUS NETWORK

This protocol allows creating and managing distributed and decentralized spontaneous network. Cooperation of different devices can allows to access different services like group communication, security etc. members and services can be changed because the network allows devices to join and leave the network any time. 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. Spontaneous network should complete the following steps in order to be created [1].

A. Joining Procedure

Joining procedure is depending on IDC i.e. identity card which is holds by every user which is in network or not. ID Ccontains public as well as private key information public components contain logically identity which is unique for every user which uses for identification of node it also contains information such as name photographs or other user identification documents. It also contains public key, creation and expiration dates, an ip proposed by the user and user signature which is created by secure hash algorithm (SHA-1) [8]. Private components contains private key. Which is in communication range to validate itself (e.g. Node A) A will send its public key. Then, B will send its IDC signed by A's public key. Next, 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 establishes the trust level of B by looking physically at B (they are physically close),depending on whether A knows B or not. Finally, A will Send its IDC data to B (it may do so even if it decides not to trust B). This data will be signed by B's public key (which has been Received on B's IDC) [9]. B will validate A's IDC and will establish the trust and validity in A only by integrity verification and Authentication. If A does not reply to the joining request, B must select another network node (if one exists). After the Authentication, B can access services, data and other nodes certificates by a route involving other nodes in network. Once the A node is validated then session key which is randomly created by first node of network is then distributed to all nodes of network. For the node joining combination of symmetric and asymmetric key is used symmetric key is used for session key to encrypt the confidential message for that advanced encryption standard (AES) algorithm is used. Whereas a symmetric key cryptography is used for user identification and session key distribution which uses Rivest, Shamir and Adelman cryptography algorithm (RSA) is use for asymmetric key cryptography .finally the ip for new node is created and checked for ip duplication. The first node in the network will be responsible for setting the global settings of the spontaneous network (SSID, session key). However, each node must configure its own data (including the first node): IP, data, port, and user data. This information will help the node to become part of the network.

B. Service Discovery

B asks for the services. Services can be discovered by web services description language (WSDL). Our model is based on[10]. But in our spontaneous network we don't use a central server. Moreover, other service discovery Services can be implemented in our system [11].

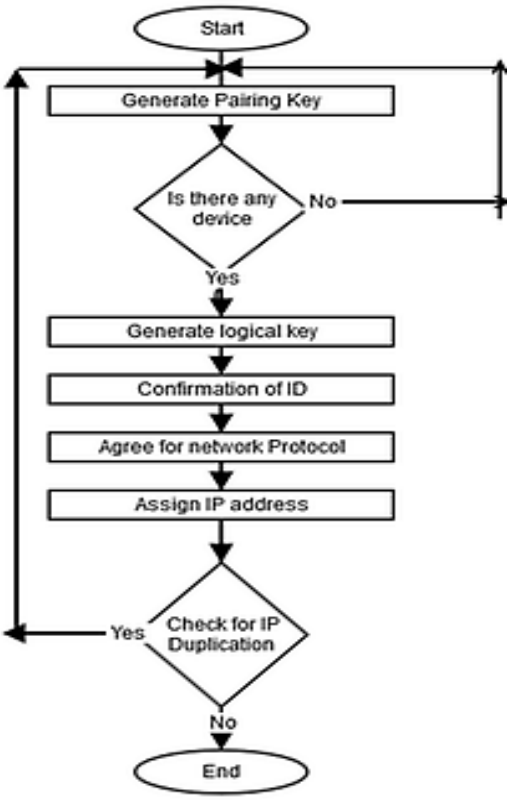

Fig. 1: Node Joining Flow

User can ask to other devices for available services it has an agreement to use available services and the services offered by other nodes. Services provided by B are available only if there is a path to B, and disappear when B leaves the networked.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

C. Establishing Trusted Chain and Changing Trust Level

There are only two trust levels in the system. Node A either trusts or does not trust another node B. The software application installed in the device asks B to trust A when it receives the validated IDC from B. Trust relationship can be asymmetric. If node A did not establish trust level with node B directly, it can be established through trusted chains, e.g., if A trusts C and C trusts B, then A may trust B. Trust level can change over time depending on the node's behaviour. Thus, node A may decide not to trust node B although A still trusts C and C trusts B. It can also stop trusting if it discovers that previous trust chain does not exist anymore.

IV. SIMULATION RESULT

In this section, the simulation results are presented. NS-2 (Network simulator) tool is used to create simulation environment. It is used for simulating wireless network with specific network protocol and their behaviour. We are going to present simulation scenario at activating the network security through analytical parameter like throughput, packet delivery ratio and end to end delay between numbers of nodes. AODV protocol is used for discovery and joining of nodes. On that basis we evaluate a spontaneous ad hoc network. In NS-2 we have to configure nodes for simulation as shown in Table 1. Below are the result for the throughput, packet delivery ration and end to end delay with respect to number of nodes.

TABLE I:SIMULATION PARAMETER

Parameter	Value
Area	600*600
No. of nodes	Variable
Routing Protocol	AODV
Antenna Model	Omni Directional
Type Of Mac	802.11
Simulation Time	100ms

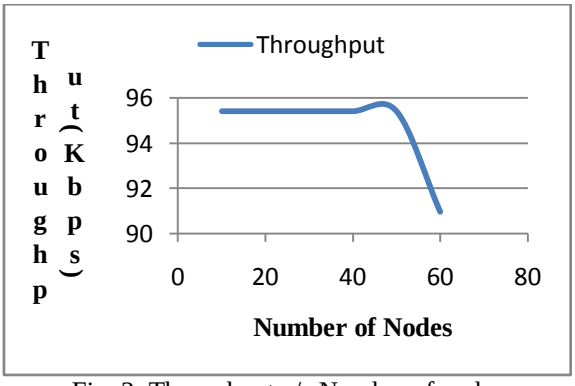

Fig. 2: Throughput v/s Number of nodes

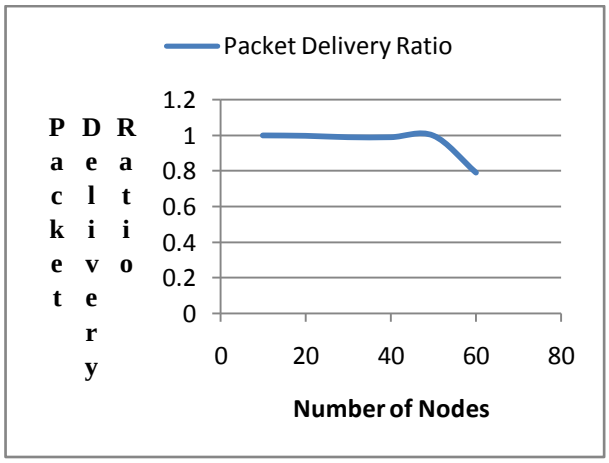

Fig. 3: PDR v/s Number of nodes

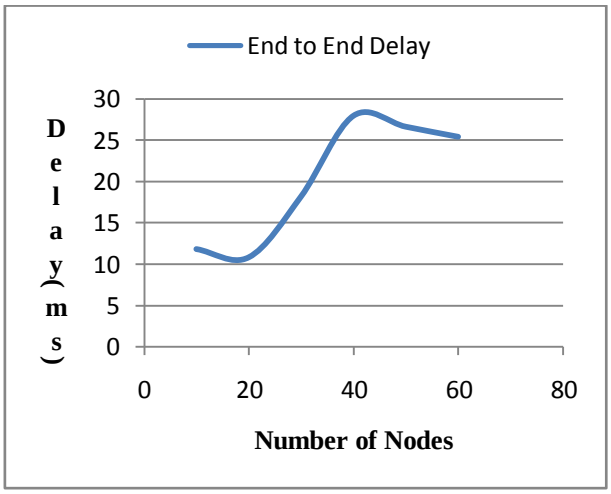

Fig. 4: End to End Delay v/s Number of nodes

V. CONCLUSION

In this paper, we show the design of a protocol that allows the creation and management of a spontaneous wireless ad hoc network. Thus, each user will work to maintain the network, improve the services offered, and provide information to other network usersThe 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). We have performed several tests to validate the protocol operation. We compare different parameter using AODV protocol for evaluation of spontaneous network. Security schemes are included using cryptographic techniques. The secure protocol allows confidential data sharing among trusted nodes. And the attacker detection approach protects the network and enhancing the level of security in ad hoc networks.

ACKNOWLEDGMENT

We are thankful to department of for all the support it has provided us. I am grateful to **Dr. V.N. Nitnaware** for sharing his knowledge with me and also grateful to the researcher and scientist working in this field from where I

gained valuable knowledge which helped me a lot to complete my work successfully.

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," RostockerInformatikBerichte, 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]. 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.
[6]. 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.
[7]. 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.
[8]. FIPS 180-1 - Secure Hash Standard, SHA-1,"National Institute of standardsandTechnolgy,"http://www.itl.nist.gov./fipspubs/fip180-1, Feb.27, 2012
[9]. S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: A Lightweight Hop by- Hop Authentication Protocol For Ad-Hoc Networks," Ad Hoc Networks J.,vol. 4, no. 5, pp. 567-585, Sept. 2006.
[10]. S.E. Czerwinski, B.Y. Zhao, T.D. Hodes, A.D. Joseph, and R.H. Katz, "An Architecture for a Secure Service Discovery Service," Proc. ACM/IEEE MobiCom '99, Aug. 1999.
[11]. L. Liu, J. Xu, N. Antonopoulos, J. Li, and K. Wu, "Adaptive ServiceDiscovery on Service-Oriented and Spontaneous Sensor Systems," Adhocand Sensor Wireless Networks, vol. 14, nos. 1/2, pp. 107-132, 2012.

BIOGRAPHY

This is **Swapnali D Patil** received bachelor of engineering in Electronics and Telecommunication in 2014. Cprrently Pursuing Master in Electronics and Tele communication. Research interests include wireless communication and signal & system.

DOI 10.17148/IJARCCE.2016.55102