INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A SURVEY ON NODE AUTHENTICATION IN SPONTANEOUS WIRELESS AD-HOC NETWORK

SARITA D. SAPKAL, PROF UMESH K. RAUT, PROF DEEPAK D. SAPKAL

Computer Department, MIT Pune, Computer Department, PVG's COET Pune.

Accepted Date: 15/02/2014 ; Published Date: 01/04/2014

Abstract: Authentication of nodes in the spontaneous wireless ad hoc networking is a vital task in wireless networking. These networks are formed by a set of nodes placed together in the close area which will communicate with each other, for limited time," anywhere anytime". To achieve this requirement of ad hoc networking we have to authenticate the individual node as they come in the network range of wireless network. We present a survey paper which will focus on the different ways of authentication policies and their privileges; we will also compare these policies.

Keywords: Ad-Hoc Network, Authentication, Deployment, Public key Cryptosystems, Wireless communication, Wireless Network.

PAPER-QR CODE

Corresponding Author: MISS. SARITA D. SAPKAL

Access Online On:

www.ijpret.com

How to Cite This Article:

Sarita Sapkal, IJPRET, 2014; Volume 2 (8): 719-726

INTRODUCTION

A Spontaneous Wireless Ad Hoc network is formed, when two or more nodes come together for interaction and for sharing resources. These networks are in the closed area and their existence is for limited period of time. The communication in wireless network is different from the traditional wired networks. The wireless network is always formed of mobile terminals or nodes; which have limited bandwidth, power and the capacity of computation is also limited. We must find out some new methods which fits the characteristics of the wireless communication. Here with we give literature survey which will focus on some methods of wireless communication.

I. LITURATURE SURVEY

The related literature survey of spontaneous wireless adhoc network shows several security methods for authentication such as challenge and response based authentication [1]. One of the most widely used security mechanism is Authentication in the wireless networking. It provides secure communication by preventing unauthorized usage. For the authentication of the mobile node or terminal, the credentials of the mobile unit are encrypted and then transmitted hop by hop for remote verification among the authentication server. In the challenge/ response based authentication, a user is identified with a shared security association (SA), which is a trust relationship with many parameters such algorithms for secure services and keys by an authentication server. During this process server sends the random number, Challenge value to the end user for encryption and verifies the returned value called response value with decryption. Visiting Mobile Unit in the foreign network sends an authentication request to an Access Point. The Access Point relays the request to a local authentication server (LAS), which only takes of the authentication for visiting Mobile Units from foreign networks. If the LAS has no information to verify the Mobile unit, it contacts the home authentication server (HAS) of the mobile unit through an authentication architecture. HAS sends the registration request to the Mobile unit's home agent which maintain the current location of the Mobile Unit (MU) Shown in the fig.1.

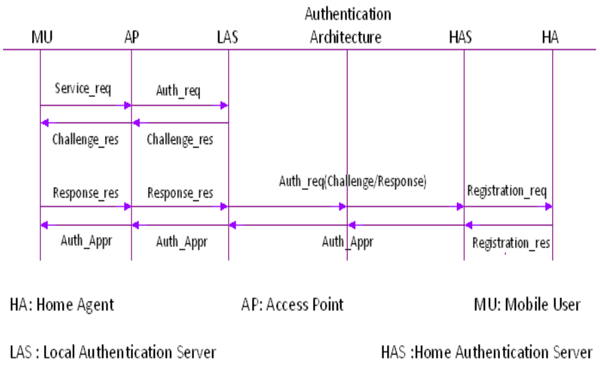

Fig1.Challenge/Response authentication in public wireless

The above solution for authentication in wireless network requires maintaining different database, related to the Mobile Nodes. An ad hoc network must operate independent of pre-established or centralized network management infrastructure, while still providing administrative services needed to support applications. Address allocation, name resolution, service location, authentication, and access control policies represent just some of the functionality that must be supported-without pre-configuration or centralized services [11].

Author Marc Danzeisen used a cellular network in formation of the spontaneous wireless adhoc networks. Authentication of mobile node is done with the Mobile subscriber Integrated Services Digital network Number (MSISDN) for every node, willing to communicate in ad hoc network[9]. The node should have the MSISDN number. Pre-configuration is required for mobile node. Hardware and software requirements are there in the system. This type of system is not beneficial in time and place specific spontaneous wireless adhoc networking.

Recent advances in ad hoc and sensor wireless networks have brought authers J. Lloret, L. Shu, R. Lacuesta to concentrate on new designs and deployment orientations. Even more, when the ad hoc (or sensor) wireless network integrate users and service. Quality of Service for each user must be guaranteed. On the other hand, the user behaviour and the services offered for the users could affect to the network performance. A spontaneous ad hoc (or sensor) network enables a group of users to communicate and work together collaboratively very close to each other, sharing services, during a period of time. They seek to imitate human relationships in order to work together in groups, running on an existing technology. Devices used for spontaneous ad hoc (or sensor) wireless networks have limited resources, few computing capacity and low energy consumption. User-oriented and service-oriented spontaneous ad hoc and sensor wireless networks can be used to solve a problem, to carry out a specific task, or just to share services and resources between users, with no dependence on a central server[2].

There is a wide range of environments in which these networks can be applied. This special issue tries to collect the most recent research of these types of networks. In paper [10] Rekimoto introduced the concept of synchronous user operation, for establishing spontaneous adhoc network connections in-between nodes. When two or more user wants to communicate with each other using their devices then they will presses and release the connection button on their devices. This method can also deal with multiple overlapping connection requests by detecting collision situations by devices. In this system author used Diffi Hellman algorithm for communication after connection is established between the nodes. The Sync Tap button can be specially installed for communication purpose, which increases the hardware requirements.

The permanently growing networked IT-infrastructure, the need for more mobility as well as the expansion of computer-aided applications to new areas demand new methods to simplify the handling of IT systems. Spontaneous networking is a means for simple integration of devices and services into networks. It seems to be one way to achieve more flexibility, more mobility, a better usability and less administration effort. This paper provides a definition of spontaneous networking and lists mandatory and optional features. It takes a closer look at the evolving technologies Jini (Java intelligent network infrastructure), JetSend, Inferno/Limbo, HAVi (Home Audio Video interoperability), and UPnP (Universal Plug and Play). Their basic concepts and functionalities are explained and their conformance to the principles of spontaneous networking is outlined [13].

The spontaneous ad-hoc network is defined as a type of an ad-hoc network, which is formed during certain period of time with independent central server having no interference of an expert user, for carrying out any specific task or solving a problem. This network is built by numerous independent nodes coming together in the same place and at the same time to be able to communicate with each other. Nodes are able to enter and leave the network and they could be portable. When adjacent nodes discover each other within a short period of time, Spontaneous networking occurs. When a set of mobile terminals which are placed in a close location that interconnect with each other and also when one of the secure protocol which uses an hybrid symmetric/ asymmetric scheme and the trust between users in order to share the initial data as well as to exchange the secret keys that will be used to encrypt the data, Spontaneous ad hoc networks are formed. Trust is based on the first visual contact between users. A Spontaneous ad-hoc network is a complete self-configured secure protocol which is able to create the network and share secure services without any setup. The network permits sharing resources and offering new services among users in a secure environment [6]. The protocol contains all functions required to operate without any external support. Design of a protocol permits the creation and management of a spontaneous wireless ad hoc network. Wireless sensor networks have many applications, vary in size, and are deployed in a wide variety of areas. They are often deployed in potentially adverse or even hostile environment so that there are concerns on security issues in these networks. Sensor nodes used to form these networks are resource-constrained, which make security applications a challenging problem. Efficient key distribution and management mechanisms are needed besides lightweight ciphers. Many key establishment techniques have been designed to address the trade off between limited memory and security, but which scheme is the most effective is still debatable [8]. In this paper, the author has provided a survey of key management schemes in wireless sensor networks. In the overall study we have seen no key distribution technique is ideal to all the scenarios where sensor networks are used; therefore the techniques employed must depend upon the requirements of target applications and resources of each individual sensor network. The paper[3][4][5] has shown symmetric, asymmetric and hybrid algorithms for network creation .These methods requires initial network configuration as well as the central authority for identification which is not feasible in spontaneous wireless adhoc networks. Wireless sensor networks (WSNs) have attracted a lot of researchers due to their usage in critical applications. WSN have limitations on computational capacity, battery etc which provides scope for challenging problems. Applications of WSN are drastically growing from indoor deployment to critical outdoor deployment. WSN are distributed and deployed in an unattended environment, due to this WSN are vulnerable to numerous security threats. The results are not completely trustable due to their deployment in outside and uncontrolled environments [12]. In this paper, the author focused on the security issue of WSNs and proposed a protocol based on public key cryptography for external agent authentication and session key establishment. The Authors Raquel Lacuesta, Jaime Lloret in the paper [1] has provided one secure solution for node authentication and deployment of the network. They have used trust model for exchanging the initial data. Rivest, Shamir and Adleman cryptographic algorithm (RSA) and Elliptic Curve Cryptosystem (ECC) algorithms are used for signing the certificates and for communication in the network respectively. RSA 1024 key size is basically used for the data in the year of 2010 which provides the accepted security level. To protect the data beyond 2010, RSA security recommends RSA 2048 key size as the minimum key size. As the key size increases we require more storage, more time consuming. The system does not provide a good solution for spontaneous wireless adhoc network. In the wireless networks nodes/terminals have limited power, limited capacity of computation. To achieve this requirement we should use the smaller key size, which will ultimately result in the consumption of computational capacity and power as well.

II. CONCLUSION

In this Paper, we have shown the different ways of the authentication of nodes in the Spontaneous Wireless Ad-Hoc Network. The AdHoc wireless network is created when two or more nodes come together for communication and to share resources, without any infrastructure. So power consumption is the major factor in the network. The comparison between different ways of authentication is given in Table1.

Table 1 : Comparison of Authentication Systems

Sr No	Paper Id	Description	Disadvantages
1	11	In This paper authors are using Mobile user, Home agent, Local authentication server Home authentication server. The authentication of nodes is done by central authority.	1) As central authority is used in the system the authority should be available 24 hours. 2) More storage is required. 3) Configuration of CA should be good.
2	**9**	**This paper uses cellular network for node authentication, which requires network configuration and external authority**	**1) Central authority is the middle man for authentication.** **2) Every node has to register their self in central authority.**
3	10	allows a user to establish device connections through synchronous button operations. When the user wants to connect two devices, one synchronously presses and releases the	1)Hardware requirement 2)Nodes who want to communicate has to press SyncTap button together at a time.(time miss match can be their)

4	3,4,5	These Papers shows the pre-distribution key algorithm for security.	1) Initial Network Configuration is required.
5	1	This paper uses the trust model and RSA algorithms for authentication to authenticate node in spontaneous wireless ad hoc network.	1) Use of RSA algorithm leads to Time consuming system.

III. ACKNOWLEDGMENT

This work is supported by my guide Prof. U.K.Raut. I am grateful to Prof D.D. Sapkal for his support. I am grateful to Prof. Mrs. S. S. Paygude (HOD of Computer Engineering Department) for providing infrastructure facilities.

I am also grateful to Prof. Jaime Lloret (Associate Professor in the Polytechnic University of Valencia), for his valuable time and technical support.

REFERENCES

1. Raquel Lacuesta, Jaime Lloret, Miguel Garcia,"A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation", IEEE Transactionm on Parallel and distributed systems, Vol. 24, No. 4, April 2013.

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. 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.

4. M. Mukesh and K.R. Rishi, Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review, Intl J. Computer Applications, vol. 12, no. 2,pp. 37-43, Dec. 2010.

5. J. Yan, J. Ma, F. Li, and S. J. Moon," Key Predistribution scheme with Nodes Revocation for Wireless Sensor Networks" Ad Hoc and Sensor Wireless Networks, vol.10,nos 2/3,pp.235-251,2010.

6. 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.

7. M. Danzeisen, T. Braun, S. Winiker, D. Rodellar, Implementation of a Cellular Framework for Spontaneous Network Establishment, Proc. IEEE Wireless Comm. and Networking Conf. (WCNC 05),Mar. 2005.

8. J. Rekimoto, SyncTap: Synchronous User Operation for Spontaneous Network Connection, Personal and Ubiquitous Computing, vol. 8, no. 2, pp. 126-134, May 2004.

9. Wei Liang, Wenye Wang "On performance analysis of challenges/response based authentication in wireless networks" Elsevier, Science Direct,4 Oct 2004.

10. 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.

11. S. Preuß and C.H. Cap, "Overview of Spontaneous Networking -Evolving Concepts and Technologies," Rostocker Informatik-Berichte, vol. 24, pp. 113-123, 2000.