Node Authentication in Spontaneous Wireless Ad-Hoc Networking: Survey

Sarita D. Sapkal, Umesh K.Raut, Archana A.Khandekar
MIT Kothrud, Pune University

Abstract

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

1. 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.

2. Literature Survey

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. [1].

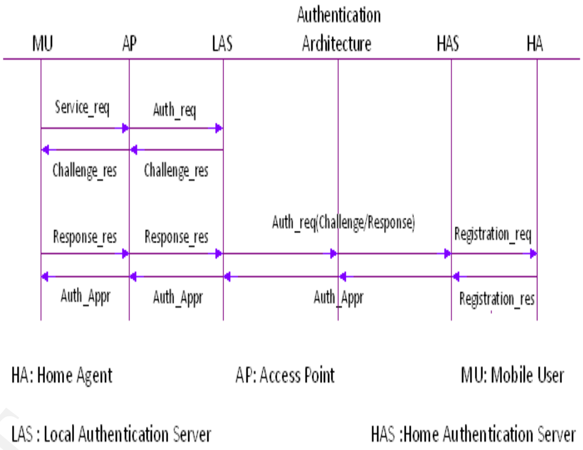

Figure1. Challenge/Response authentication in public wireless access networks

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 [2].

Recent advances in ad hoc and sensor wireless networks have brought us new designs and deployment orientations. Even more, when the ad hoc (or sensor) wireless network integrate users and services. On one hand, the 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. 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 [3].

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 [4].

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. 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 [5].

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. In this paper, we provide a survey of key management schemes in wireless sensor networks. We notice that 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 [6].

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 un attend 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. In this current paper, we fundamentally focused on the security issue of WSNs and proposed a protocol based on public key cryptography for external agent authentication and session key establishment. This proposed protocol is efficient and secure in compared to other public key based protocols in WSNs.

3. Conclusion

In this Paper, we have shown the different ways of the authentication of nodes in the Spontaneous Wireless Ad-Hoc Network. In Our future work we will provide authentication of node before creating network, which will increase the security in Wireless Ad Hoc Network. As

4. References

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

[2] 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.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.