International Journal of Information and Computation Technology (IJICT)
ISSN 0974-2239 Volume 3, Number 10 (2013)

Authentication and Authorization Issues For Multi-Hop Networks

Manvi Mishra[1], Shivangi Tyagi[2], Nikita Jaiswal[3] and Shivangi Johri[4]
[1]{**Assistant Professor** Department of Computer Science SRMSWCET, Bareilly, U.P., India}
[2, 3, 4]{**Research Scholar** Department of Computer Science SRMSWCET, Bareilly, U.P., India}

ABSTRACT

This paper treats the problem of authentication through the multi-hop communication, authorization to services access, and efficient collaboration between ad hoc nodes in order to assure efficient packet relaying during services access, thus alleviating major problems in ad hoc networks deployment. A novel solution is proposed allowing for authentication and authorization of services, while coupling the accounting process for each user (ad hoc node) with his level of collaboration in terms of participation in packets relaying for other nodes. The billing of services takes a novel notion, where it concerns not only `debit', which classically happens, but also `credit' as a reward for collaborative users. The authentication and authorization for services access mechanism has been implemented and integrated in an ad hoc mesh platform, where multimedia applications have been tested, and performance evaluation has been done.

Keywords: IEEE 802.1x, Multi–hop networking, DAC, MAC, RBAC.

1. INTRODUCTION

In all kinds of communication systems, authentication and authorization have always been an important issue. Especially for wireless communications with low infrastructure costs – such as wireless local area networks (WLANs), where the signals are transmitted over a wide area authentication and authorization is crucial. Authentication in WLANs based on IEEE802.11 can be done through an access control list. All MAC addresses that are allowed to access the network via an access point are stored in this list. The MAC addresses are hard coded on the RF cards. The problem of this approach is based on the fact that not the customer, but the MAC address on the RF card is authenticated. In this case, any other person may access the network if he is in possession of the card. This unauthorized access is available until the real owner knows about the stolen card and the MAC address is deleted from the access control list. Furthermore, this authentication mechanism entails a large administration complexity, which is not negligible for a closed user group such as an office, but will be dramatically in publicly accessible networks. Another possibility to get access for an unauthorized person is to spoof MAC addresses. In a case where a hacker knows the MAC address, it is possible for him to make any card look like an authorized card. For this action, a good knowledge of programming is necessary, but in this case the unauthorized access is very hard to detect in comparison to a stolen card. Some of the keywords are discussed below:

1.1 IEEE802.1x-. IEEE802.1x [3] is part of the IEEE802.1standard family that defines management functionality for IEEE802–based networks. Designed for securing wired and also wireless networks like the IEEE802.11, the WLAN standard 802.1x defines a generic framework that is able to use different authentication mechanisms without implementing these mechanisms outside the back-end authentication Infrastructure Extensible Authentication Protocol (EAP) [4] that defines a generic container to convey authentication method PDUs.EAP[5] messages are exchanged on the air interface between the mobile device (known as supplicant in 802.1x terminology) and base station (authenticator) by using an encapsulating protocol. On client–side, 802.1 xs is already available in the Windows XP operating system.

1.2Multi-hop Networking- Multi-hop, or ad-hoc[6], wireless networks use two or more wireless hops to convey information from a source to a destination. A mobile ad hoc network consists of a group of mobile nodes that communicate without requiring a fixed wireless infrastructure. It provides rapid deployment with

lower cost. Multi-hop ad-hoc networking is not a new concept having been around for 20 years. Single hop ad-hoc network just interconnect devices that are within the same transmission range. This limitation can be overcome by exploiting the multi-hop paradigm.

2. AUTHENTICATION AND AUTHORIZATION FOR MULTI–HOP NETWORKS

For our approach, we assume that we have an IEEE802.11 enabled access point with fixed connection to the Internet. This access point is under the control of the network provider and can be seen as the access to the home network. A subset of the wireless and mobile terminals can transmit directly to the access point. Other terminals may use the multi-hop capability of terminals or virtual access points (VAP) [2], [1] which are already connected to the home network. The main problem that arises in multi hop networks – in terms of security – is the authentication and authorization process. The authentication of nodes is not only important for the customer to avoid subscription fraud, but even for the network itself. The source of a packet has to be clearly identified to avoid the situation of hacked routing messages. The question arises, how a client achieves a valid shared secret key and how long is this key valid. Furthermore, how can the key be transported over a multi–hop network in a secure manner? The wireless terminals in the multi hop network can either be virtual access points or other customers that are connected to the multi hop network.

3. METHODOLOGY

The researches, practices, progresses, development and successes for the access management especially authentication and authorization are reviewed to see the global practices by the administrators or managers. Based on review and multi-hop users interview this paper gives idea about the current practices about authentication and authorization.

Access management typically is a combination of users' authentication and authorization, access permission operations, policies for license agreement and digital materials authentications or digital rights management. Authentication is the process of determining the validity of a user who claims to be, and authorization is the process of determining what resources a user is permitted to access. Access Management is necessary most for commercial digital contents because their access is restricted to its subscribers or licensed users.

3.1User Authentication: User Validity-The most common and familiar authentication process is Log-in ID and Password-based Access Log-in which identifies oneself to the system in order to obtain access. The primary use of a computer login procedure is to authenticate the identity of any computer user or computer software attempting to access the computer's services. Another popular authentication process is IP Filtering or IP authentication. This process is a packet filter that analyzes TCP/IP packets. Web Cookie is another process of user authentication, which can be used by a server to recognize previously-authenticated users. Web Proxy is another way to authenticate. The authentication system also performs the same cryptographic process on the challenge and compares its result to the response from the client. If they match, the authentication system has verified that the user has the correct password.

3.2User Authorization: Resource Access Permission-Authorization defines users' permissions in terms of access to digital resources and extent of its usage. Authorization is granted to the successfully authenticate users according to his/her rights information available in the Access Management System. Authorization also addresses the issue of responsibilities assigned to different personnel involved in development of a digital repository/library and their respective authorities in terms of addition, deletion, editing and uploading of records into a digital collection. Authorization is more challenging than authentication, especially for widely distributed digital content providers. There are standard access control models [Fig 1: describes the techniques] which are highly domain and implementation independent. We will discuss these models[7]:

3.2.1 Discretionary Access Control (DAC) - In a DAC Model, access is governed by the access rights granted to the user or user groups. An organization/administrator/creator can identify a set of operations and assign them to an object and to a set of users.

3.2.2 Mandatory Access Control (MAC)-In MAC, the data owner has limited freedom to decide on access control. Information is classified into different categories and each category is assigned a particular security level.

3.2.3 Role Based Access Control (RBAC) -RBAC is a widely used - and dominant - access control model, and most access control security products available in the market today are based on this model because its objectives are architectural.

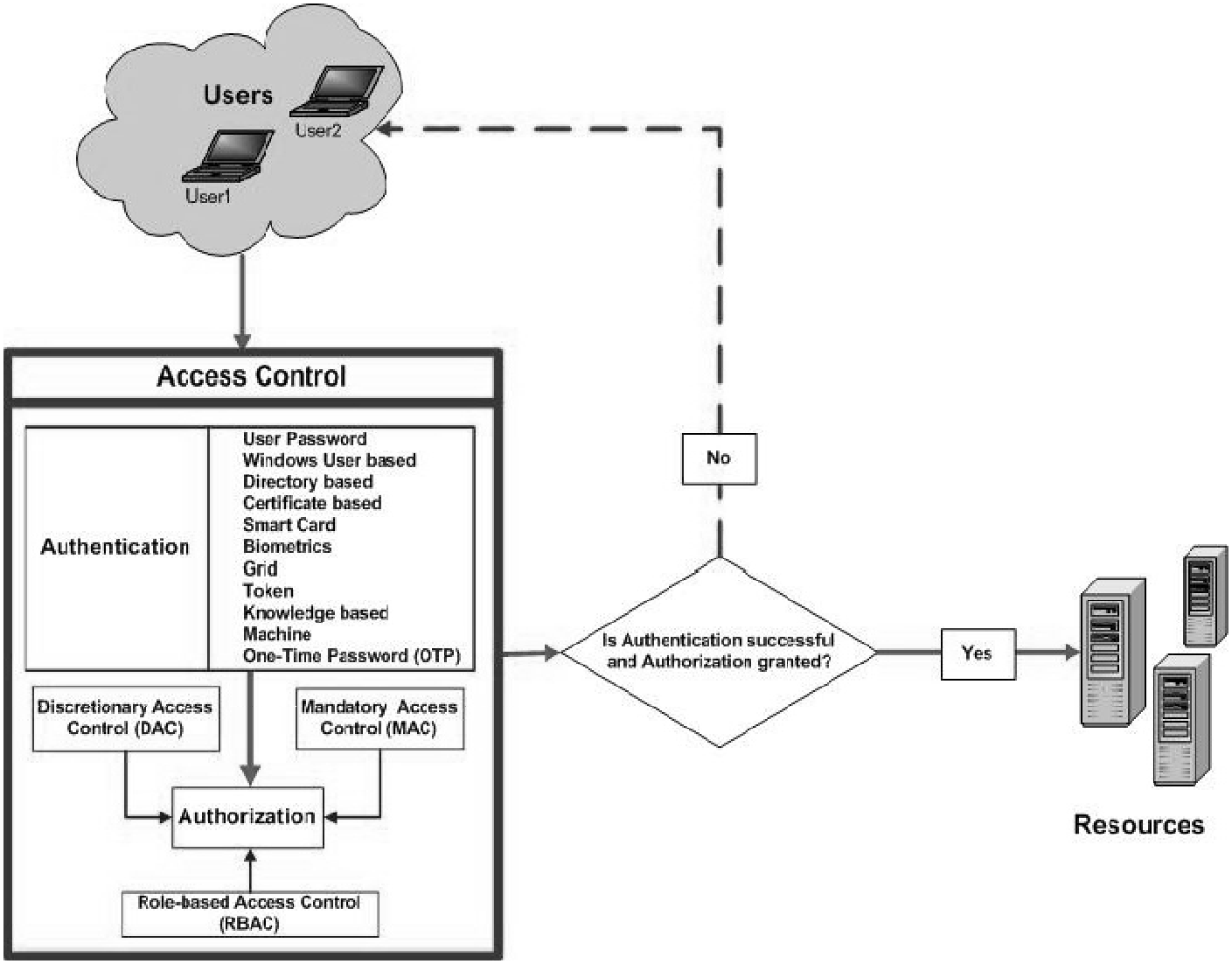

Fig 1: Authorization and Authentication Techniques

4. CONCLUSION

Through this paper we have discussed the various authentication and authorization issues and techniques to ensure security in ad-hoc and multi-hop networks. The whole thrust of access authorization and authentication issues are to restrict unauthorized users from accessing organization resources. The authentication techniques and access control techniques described in this research paper can be chosen based on an organization's need. The authentication and access control framework should be flexible enough to serve all the authentication techniques and future evolution in the area such as Biometrics. The access control framework should be able to handle an organization's authentication and authorization needs. We advocate the use of IEEE802.1 for authentication and security in multi hop networks.

REFERENCES

[1] F.H.P. Fitzek, P. Seeling, and M. Reisslein. Reference Models and Related Business Cases for Ad-Hoc Networks. In *In Proceedings of*
Wireless World Research Forum 6 (WWRF6) Section WG4 – Section WG4, June 2002. London.
[2] S. Krco, B. Hunt, and F.H.P. Fitzek. WhitePaper on Ad Hoc networks. In *In Proceedings of Wireless World Research Forum 6 – WG4*, June2002
[3] 3rd Generation Partnership Project. Security Architecture. 3GPP, June 2002. Release 5.
[4] L. Blunk and J. Vollbrecht. PPP Extensible Authentication Protocol (EAP). IETF RFC 2284, March 1998. http://www.rfc-editor.org/rfc/rfc2284.txt

[5] B. Aboba and D. Simon. PPP EAP TLS Authentication Protocol. IETF RFC 2716, October 1999. http://www.rfc-editor.org/rfc/rfc2716.txt.
[6] F.H.P. Fitzek, P. Seeling, and M. Reisslein. Reference Models and Related Business Cases for Ad-Hoc Networks. In *In Proceedings of Wireless World Research Forum 6 (WWRF6) Section WG4 – Section WG4*, June 2002. London.
[7]Designing Security Architecture Solutions – Jay Ramachandran.{63,64}