Available online at www.sciencedirect.com

SCIENCE DIRECT®

Computer Networks 48 (2005) 267–288

Computer Networks

www.elsevier.com/locate/comnet

On performance analysis of challenge/response based authentication in wireless networks ☆

Wei Liang, Wenye Wang *

Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27695-7911, United States

Received 17 September 2004; accepted 4 October 2004
Available online 30 December 2004

Responsible Editor: G. Morabito

Abstract

The emergence of public access wireless networks enables ubiquitous Internet services, whereas inducing more challenges of security due to open mediums. As one of the most widely used security mechanisms, authentication is to provide secure communications by preventing unauthorized usage and negotiating credentials for verification. Meanwhile, it generates heavy overhead and delay to communications, further deteriorating overall system performance. Therefore, it is very important to have an in-depth understanding of the relationship between the security and quality of service (QoS) through the authentication in wireless networks. In this paper, we analyze the impact of authentication on the security and QoS quantitatively. First, a system model based on challenge/response authentication mechanism is introduced, which is wide applied in various mobile environments. Then, the concept of security levels is proposed to describe the protection of communications with regard to the nature of security, i.e., information secrecy, data integrity, and resource availability. Third, traffic and mobility patterns are taken into account for quantitative analysis of QoS. Finally, we provide numerical results to demonstrate the impact of security levels, mobility and traffic patterns on overall system performance in terms of authentication cost, delay, and call dropping probability.

Keywords: Wireless networks; Challenge/response authentication; Security association; Performance analysis

1. Introduction

With the deployment of public access wireless networks, the demand for ubiquitous Internet services is dramatically increased, whereas inducing more challenges of security due to open mediums [1]. In order to provide secure services over wireless

☆ This work was supported in part by the National Science Foundation (NSF) under award ANI-0322893 and in part by the Center for Advanced Computing and Communication (CACC) 03-06 and 04-08.

* Corresponding author. Tel.: +1 919 513 2549; fax: +1 919 515 5523.
E-mail address: wwang@ncsu.edu (W. Wang).

1389-1286/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2004.10.016

networks, security mechanisms such as authentication and encryption are deployed at the expense of quality of service (QoS) because of the implementation overhead.

As one of the most widely used security mechanisms, *authentication* is a process to identify a mobile user (MU), authorize resources to the MU, and negotiate secret credentials for protecting communications [2]. In the authentication, an MU will submit credentials like certificates and challenge/response values [3–8], which will be verified with a security association (SA), a description on keys and encryption algorithms. With the authentication, network resources are protected by only allowing legitimate users to obtain services. The information secrecy and data integrity are also guaranteed because session keys may be generated during the authentication process for data encryption and message authentication. Thus, the network security in terms of protection for network resources, information secrecy, and data integrity is affected greatly by the authentication service.

In addition, an authentication service also has significant effects on the QoS. When certificates are used for authentication, it involves with the application of public/private-key based authentication mechanism, in which more time and power are consumed due to the computation complexity of encryption and decryption of data [9]. Thus, in order to achieve efficient authentication, challenge/response authentication mechanism based on secret keys is widely used in wireless networks [10–12]. However, the credentials of the MU are encrypted and transmitted hop-by-hop for remote verification among authentication servers in challenge/response authentication. This remote transmission and encryption/decryption of credentials increase the overhead of communications, thus influence many QoS parameters such as authentication cost, delay, and call dropping probability due to extended waiting time. Therefore, the tradeoff between security service and system performance should be concerned in different scenarios, because users have different preferences on security and performance from time to time.

Furthermore, the impact of authentication on QoS parameters is far more sophisticated for different mobility and traffic patterns, since the authentication requests are generated when an MU either requests resources, or crosses boundaries of subnets with on-going communications. Thus, the authentication based on different mobility and traffic patterns may greatly impact QoS parameters such as aggregated authentication cost in a network, because the cost needs to be calculated by adding up the costs in all of the authentication requests.

In order to improve the security and efficiency during the authentication, many authentication schemes are proposed, focusing on the design of lightweight and secure authentication protocols [2,5–7,10–20]. However, none of these work provide quantitative analysis on security and system performance, simultaneously, and nor do they model the relationship between security levels and system performance analytically, although some of them evaluate the system performance for certain security policies through simulations [15,20]. Moreover, mobility and traffic patterns are not considered, which are important features in wireless networks. Therefore, new authentication solutions may not be fully adapted to mobile environments with the concerns of security, mobility and traffic patterns.

In this paper, we analyze the effect of challenge/response authentication on security and system performance quantitatively. First, we propose a system model, which is highly consistent with many wireless networks such as Mobile IP and wireless local area network (WLAN). This consistency guarantees that our analysis is applicable in realistic mobile environments. Second, we classify the security levels with regard to the nature of security, i.e., information secrecy, data integrity, and resource availability, and study the effects of authentication on QoS at different security levels. The QoS parameters that we investigate in this paper include authentication cost, delay, and call dropping probability, all of which are considered in combination with *mobility and traffic patterns*.

Our earlier work [21,22] presented a framework of performance analysis, focusing on authentication delay and call dropping probabilities. In this paper, we not only provide the analysis details