Computers and Electrical Engineering 000 (2017) 1–15

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Secure and efficient hand-over authentication in WLAN using elliptic curve RSA☆

Murugan Krishna*, Varalakshmi Perumal

Department of Computer Technology, Anna University, India

ARTICLE INFO

Article history:
Received 6 January 2017
Revised 22 April 2017
Accepted 3 June 2017
Available online xxx

Keywords:
Authentication
Elliptic curve
RSA
Hand-over
HashHand
WLAN

ABSTRACT

Roaming of mobile nodes among multiple access points should be secure and efficient. Hand-over occurs when a mobile node migrates from one access point to another and establishes a new connection by terminating the previous one. However, designing an appropriate hand-over authentication protocol is a complex task because the processing efficiency and power of mobile node is restricted to a certain extent. The lesser security level and higher computation complexity are the main issues of the existing hand-off authentication protocols. To overcome these problems, Elliptic Curve RSA is proposed with modification in the initialization and authentication phases of the hand-off authentication protocol. The result of the proposed work shows the improvement in higher security level along with lesser computational cost. Further, the proposed algorithm is performing well against the various possible attacks.

1. Introduction

The Hand-over authentication protocol is an essential protocol for the wireless atmosphere. When an MN starts roaming from one Access Point (AP) to a new AP, it has to establish the connection with the second Access Point and has to terminate the connection with the existing one. The three most important parts involved in a hand-over authentication protocols are Authentication Server (AS), Access Points (APs) and the Mobile Nodes (MNs) as shown in Fig. 1. Before MN connects to the AP, each of the MN must be authenticated by the AS. Upon authentication, the AS provides a secret key to each MN. After that, the legitimate MN in the wireless system can join to the desired access point. If the MN needs to move from one AP (AP_1) to another AP (AP_2), it must be verified by the latter AP (AP_2) and then a new session key with the AP_2 must be established. This kind of migration verifications is termed as Hand-over Authentication.

Hand-over can be classified into hard hand-over and soft hand-over: In hard hand-over, initially, the connection with the source access point is broken. A new connection is then established with the destination access point. This type of hand-over is also known as break-before-make. A soft hand-over is one where the connection with the source access point is retained for a certain time in parallel with the channel in the target. Clearly, the connection to the target cell is established firmly before the connection with the source access point is demolished. When a soft hand-over makes the connection, the signal with the maximum strength compared to all the channels can be used for establishing the connection. In wireless communication, there may be many reasons a hand-over is needed. When the MN is under movement from one AP to some

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. S. Smys.

* Corresponding author.
E-mail addresses: krishna.muruga@gmail.com, krishnaa.muruga@gmail.com (M. Krishna), varanip@gmail.com (V. Perumal).

http://dx.doi.org/10.1016/j.compeleceng.2017.06.002
0045-7906/

Please cite this article as: M. Krishna, V. Perumal, Secure and efficient hand-over authentication in WLAN using elliptic curve RSA, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.06.002

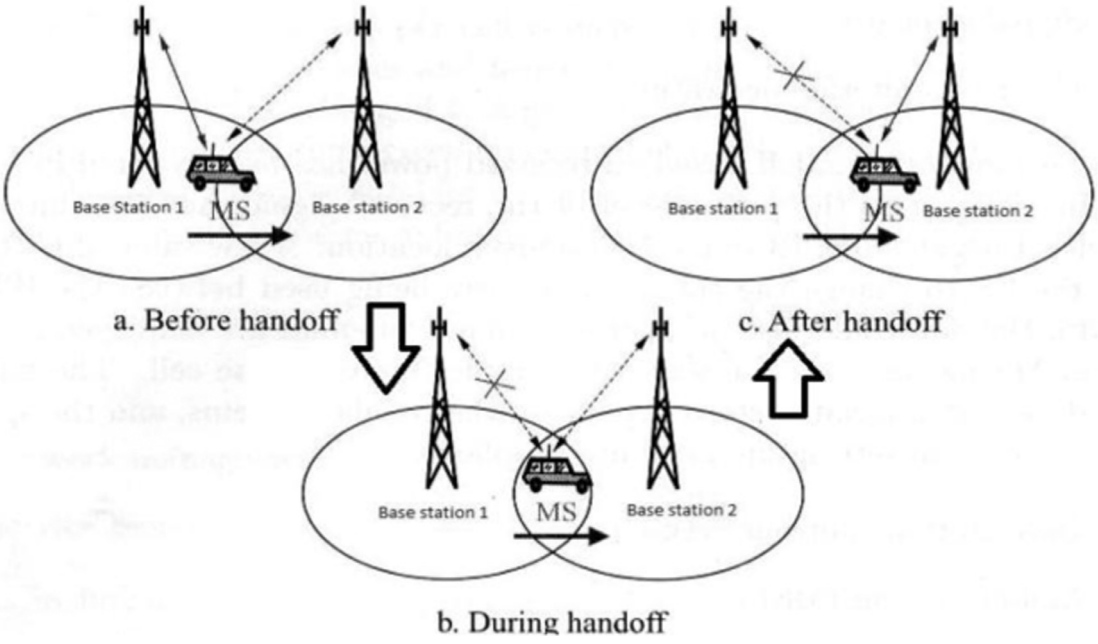

Fig. 1. Hand-over process overview.

other AP, the connection is initiated at the second AP in order to prevent the discontinuity of the connection when the MN moves entirely out of the range of the source AP.

The efficiency of the security level and computational complexity of the existing HashHand authentication protocol in hand-off process in mobile communication is not sufficient. To solve this problem, Elliptic Curve RSA (ECRSA) algorithm is proposed in this paper in which ECRSA is used in the initialization phase to further improve the security level. ECRSA is used in the authentication phase to improve the security level along with lesser computation cost.

The remainder of the paper has been organized as follows: Section 2 deals with the literature survey of the various research works related to Hand-over Authentication issues, while the various modules of the proposed work is described in Section 3. The security analysis which has been depicted in Section 4 gives an idea about the various attacks which can be prevented by the proposed system. The result comparison between the existing and the proposed system is done in Sections 5 and 6 concluded the overall work.

2. Literature survey

According to Zheng and Sarikaya [16], both 802.11r and HOKEY utilizes the key hierarchy to reduce the authentication delay. The limitations are the overhead of client-side certificates. To overcome this limitation, Yang proposed a Universal Authentication Protocols exclusively for Wireless Communication [15]. They employed an identity-based signature technique as well as a group based signature technique. This provides user anonymity against both eavesdropper and foreign visitor. But it is found that this approach cannot satisfy user traceability and key revocation is also not possible. At the same time, Chang and Tsai [14] proposed a Self-Verified Mobile Authentication framework with a valid key agreement specifically for wireless networks. By this approach, the home server need not store the keys shared with mobile users. Thus the mobile user privacy is guaranteed. Tang and Wu [13] proposed a mobile authentication idea based on Elliptic-curve-cryptosystem. This is based on elliptic curves over Finite Field. A notable striking difference between elliptic curve based Fields and non-elliptic fields like Galloi Field is that elliptic curve based areas achieve the same level of security but with smaller keys. This idea does not congregate the essential security requirements. The scalability is not achieved, and privacy protection is still not be improved.

Aboud [12] has also worked in the authentication concept based on Bilinear Pairing. Two groups G1 and G2 are considered. G1 is an additive cyclic group, and G2 is a cyclic multiplicative group. There is a condition that the groups G1 and G2 have the similar prime order q. P be the generator of G1. Based on these and hash functions H1, H2 and H3, keys are generated and verified. Choi and Jung [11] proposed Hand-over authentication based on chameleon hashing. It suffers from a man-in-the-middle attack. Under such situation, a malicious mobile user can fool both the legitimate mobile user and the visited access point. Moreover, the privacy of mobile users is not well-protected. Yang and Huang [10] proposed Universal Authentication Protocols for Anonymous Wireless Communications. It provides user anonymity in opposition to both eavesdropper and foreign visitor which satisfies the security requirement of hand-over authentication. It cannot satisfy

Please cite this article as: M. Krishna, V. Perumal, Secure and efficient hand-over authentication in WLAN using elliptic curve RSA, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.06.002