Cooperated Mutual Authentication between Mobile Base Stations in Tactical Networks

Yu-Jin Son[1], Keun-Woo Lim[1], TaeShik Shon[1], Young-Bae Ko[1]

[1] Graduate School of Information and Communication,
Ajou University, Republic of Korea
{yujin, kwlim27}@uns.ajou.ac.kr, {tsshon, youngko}@ ajou.ac.kr,

Abstract. This paper proposes a method of applying EAP-TLS (Extensible Authentication Protocol – Transport Layer Security) to mobile base stations (MBS) that construct a Wireless Mesh Network (WMN) in the Tactical Information Communication Networks (TICN). To secure the communication between soldiers and MBS, a reliable cooperated mutual authentication method is required to approve between MBS. We apply EAP-TLS for mutual authentication between mobile base stations that each hold authentication servers, then we propose a simplified substitute authentication scheme between MBS to reduce the overhead that occur from the authentication process.

Keywords: Mutual Authentication, Mesh Networks, Tactical Networks

1 Introduction

The next generation of tactical networks includes independent communication capabilities of soldiers that are managed by centralized communication command systems such as TICN [1]. In these systems, it is required for the base stations to have full mobility and move in coordination with the soldiers to provide efficient and reliable communication means. One of the main issues to cope with in these environments is managing network security. In commercial authentication schemes such as EAP-TLS [2] in 802.16, a master base station that has a link to the exterior networks will be responsible for managing the Authentication, Authorization, and Accounting (AAA) server to authenticate all mobile terminals in the network. In dynamic tactical environments, this may cause problems because the mobility of the base stations forces nodes to relay the authentication information between the MBS managing the AAA server and other MBSs. This may result in excessive authentication overhead, affecting data transmission in the tactical network.

To solve this problem, this paper proposes a method of migrating AAA servers to each MBS for more efficient EAP-TLS authentication between the stations and the directly connected mobile terminals. To account for rogue base stations [3], we propose a method of cooperated mutual authentication that can effectively utilize the existing EAP-TLS between the AAA servers by using WMN. We also propose a substitute node authentication using distributed methods that can reduce the number of transmitted control packets by simplifying the authentication operations.

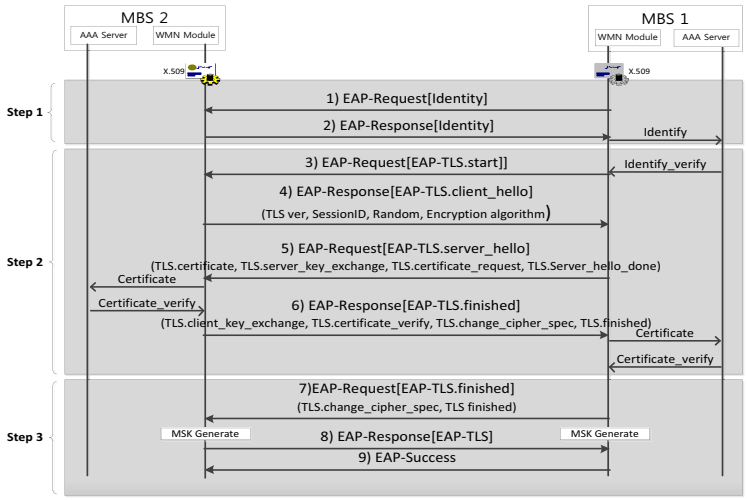

Fig. 1. The proposed scheme operating between two MBSs

2 Proposed Scheme

The proposed cooperated mutual authentication scheme assumes that each MBS in the network maintains an AAA server that is traditionally used for authentication of mobile soldier nodes. Fig. 1 shows the EAP-TLS authentication of two MBSs using the WMN module. The WMN module is responsible for transmitting and receiving the EAP messages, while managing the X.509 certificates. Therefore, the AAA server is only occasionally referenced to reduce computational complexity. The core process (mutual authentication between MBS) can be summarized into three steps:

Step 1. Initialization Phase: This phase involves the transmission of authenticator MBS1 to request identity of MBS2. MBS2 will transmit its ID back to the MBS1, which will forward the data to the AAA server for identification.

Step 2. Mutual Authentication Phase: Upon successful identification by the AAA server, MBS1 WMN will initiate the EAP-TLS and transmit message to the WMN module of MBS2. Without referring to its AAA server, MBS2 can transmit back a response message including the information shown in 4) of Fig. 1. Using the X.509 certificates, MBS1 and MBS2 can share the TLS server key, as shown in 5) and 6) of Fig. 1. Once the MBS1 WMN module receives the final EAP response from MBS2, it will transmit the certificate to the AAA server, which will try to approve it.

Step 3. Key Derivate and 4-way Handshaking Phase: Once the approving is complete, the MBS1 will create a TEK from the Premaster Secret key and use the TEK to transmit EAP-TLS.finished message back to MBS2. Then, MBS1 and MBS2 can generate the MSK, which will eventually be used to encrypt and decrypt data transmission between the two devices. After successful generation of the MSK, the final handshake is made to finalize the authentication process.

To reduce the overhead of the core mutual authentication process shown above, we utilize the cooperated substitute authentication scheme to simplify its process while maintaining its security level. The proposed process is as follows:

1) Initial State: For any MBS attempting authentication, if it does not contain MSK to any other MBS, it will undergo the core mutual authentication process.

2) Authentication of n > 1 MBS: Once a MBS successfully generates more than one MSK, it will encrypt and unicast its owned MSKs to all other authenticated

neighbor MBSs in single-hop range. The transmitted key_notify message will contain {MSK, Node_ID, Key_hop_count} for each key that will be transmitted. Key_hop_count will be accumulated every time it is transmitted.

3) Reception and maintenance of key_notify message: Any neighbor MBS that receives the key_notify message will decrypt it and store the information on the received_key table. If any MSK has a Key_hop_count over hop_threshold, it will be deleted from the table because a MSK from far distance will unlikely be used.

4) Simplified authentication using received_key table: If an authenticated MBS receives authentication request from a suspicious MBS that has not yet been authenticated by the MBS itself, it will check the Node_ID that is transmitted in step 1 of Fig. 2. If the Node_Id matches an entry in the received_key table, this means that the suspicious MBS has been previously authenticated by another trusted MBS. Therefore, the whole authentication process is reduced and the authenticated MBS will only initiate the MSK handshake process to match the key between each other. In a case where the MBS have more than one MSK to the same suspicious MBS, the authenticated MBS will randomly select one MSK and use it to establish secure data connection. If the Node_Id does not match any entry in the received_key table, then full authentication process is initiated.

The advantage of using our proposed cooperated mutual authentication method is that each mobile base station can manage its own AAA server, considerably reducing overhead that may occur in multi-hop authentication. Also, since the MSKs are shared between trusted and authenticated MBSs, the whole authentication process can be simplified to further reduce the overhead at the expense of small key sharing overhead.

3 Conclusion and Future Works

We have proposed a cooperated mutual authentication scheme in tactical networks that can maintain high level of security while reducing the overhead in the network. Our proposed scheme is mainly focused on the MBS such as the Wideband Network Waveform (WNW) in JTRS or the Mobile Subscriber Access Point (MSAP) in the TICN, but it can be also applied in other various applications. In the future, we will undergo extensive evaluation studies to verify the effectiveness of our scheme.

Acknowledgments. "This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency" (NIPA-2012-(H0301-12-2003))

References

1. D. Kim, et al.: Load Balancing with Mobile Base Stations in Tactical Information Communication Networks. In: IEEE WCNC (2011)
2. RFC 2716, *http://www.ietf.org/rfc/rfc2716.txt*
3. J. Huang, et al.: Secure Mutual Authentication Protocols for Mobile Multi-hop Relay WiMAX Networks against Rogue Base/Relay Stations. In: IEEE ICC (2011)