Computer Standards & Interfaces 36 (2014) 480–488

Contents lists available at ScienceDirect

Computer Standards & Interfaces

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

An access authentication protocol for trusted handoff in wireless mesh networks

Peng Xiao [a,1], Jingsha He [b,*], Yingfang Fu [a]

[a] College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China
[b] School of Software Engineering, Beijing University of Technology, Beijing 100124, China

ARTICLE INFO

Article history:
Received 15 January 2013
Received in revised form 22 August 2013
Accepted 24 August 2013
Available online 31 August 2013

Keywords:
Wireless mesh network
Seamless handoff
Security
Access authentication
Trusted network connect

ABSTRACT

WMNs (Wireless Mesh Networks) are a new wireless broadband network structure based completely on IP technologies and have rapidly become a broadband access measure to offer high capacity, high speed and wide coverage. Trusted handoff in WMNs requires that mobile nodes complete access authentication not only with a short delay, but also with the security protection for the mobile nodes as well as the handoff network. In this paper, we propose a trusted handoff protocol based on several technologies, such as hierarchical network model, ECC (Elliptic Curve Cryptography), trust evaluation and gray relevance analysis. In the protocol, the mobile platform's configuration must be measured before access to the handoff network can proceed and only those platforms whose configuration meets the security requirements can be allowed to access the network. We also verify the security properties through formal analysis based on an enhanced Strand model and evaluate the performance of the proposed protocol through simulation to show that our protocol is more advantageous than the EMSA (Efficient Mesh Security Association) authentication scheme in terms of success rate and average delay.

1. Introduction

WMNs are a new wireless network structure that is expected to set free the restrictions of Ad Hoc networks, WLANs (wireless local area networks), WPANs (wireless personal area networks) and WMANs (wireless metropolitan area networks), and will be used to establish commercial wireless mobile networks. Combining the advantages that WLANs and Ad Hoc networks can offer, WMNs are a wireless broadband network structure based completely on IP technologies, and become a growing effective broadband access measure that can provide high capacity, high speed and wide coverage. To some extent, WMNs are mainly a network design idea with features including no-center, self-organization, multi-hops, best routing-judgment, etc. [1]. Since a WMN does not rely on fixed infrastructure and is operated in an open space, any user within the coverage area of the radio waves can access the network. Therefore, secure access authentication is the first provision to prevent unauthorized users from accessing the network [2,3,4]. For handoff in WMNs, it is required that mobile nodes complete access authentication not only with a short delay, but also with the protection for the mobile nodes as well as the handoff network.

Past practice in the areas of information security has shown that most security problems just come from the network but more from terminal nodes [5,6,7]. Thus, the original idea of trusted computing was proposed to ensure the security of network terminals. Moreover, trusted computing is relied upon to secure the entire computer system through successive steps. First, a root of trust is established to construct a chain of trust, namely, from the root to the hardware platform to the operating system and finally to applications. Thus, trust can spread to the entire system through graded trusted authentications. For handoff in a WMN, the platform's configuration must be measured before access to the network can proceed and only those platforms whose configuration meets the security demands of the network can be allowed to access the network. Consequently, a terminal with potential threat cannot gain access to the network directly. Moreover, the terminal can verify the security of the AP (Access Point) with which it is associated and will only connect to the network when it satisfies the terminal's security demands [8].

Based on the current 802.1× authentication scheme and trusted computing technologies, we present a trusted handoff protocol in this paper to ensure security and trust in WMNs. Our goal in the design of the protocol presented in this paper is to ensure that only a legitimate user operated on a trusted platform can complete handoff to a new secure network without too much sacrifice on performance. In addition to proposing a trust-based authentication protocol to achieve the above goal for secure handoff from one network zone to another, our other contributions in this paper include the following. We propose a trust model for the trust evaluation of both starting and runtime system states, prove the security properties of the protocol through formal analysis based on an enhanced Strand model, evaluate the performance of the protocol in terms of success rate and handoff delay using simulation, and compare our protocol to a comparable scheme to demonstrate the advantages of our protocol over the other scheme.

The rest of this paper is organized as follows. Section 2 reviews some related work on handoff protocols in WMNs. Section 3 provides some

* Corresponding author. Tel.: +86 10 67396061.
E-mail addresses: xp4523@emails.bjut.edu.cn (P. Xiao), jhe@bjut.edu.cn (J. He), fuyingfang@bjut.edu.cn (Y. Fu).
[1] Tel.: +86 13552992403.

0920-5489/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.csi.2013.08.016

background information on TPM (trusted platform module) and TNC (trusted network connect). Section 4 contains a zone-based hierarchical network model for hybrid WMNs and a universal handoff model in WMNs. Section 5 describes the method for evaluating the trust degrees of both the starting and the runtime states in a trusted system. Section 6 presents our handoff protocol, which is based on several technologies such as the hierarchical network model, ECC, trust evaluation and gray relevance analysis. Then, a formal analysis of the security properties of the protocol based on the strand space model and a demonstration of the security performance based on experiment results are provided in Sections 7 and 8, respectively. Finally, Section 9 concludes the paper, which also contains a description of our future work.

2. Related work

The IEEE 802.11 [9] protocol outlines the basic steps of the handoff process. Unfortunately, the handoff latency of the original protocol is several hundred milliseconds [10] while real-time applications require that MAC layer handoff latency be 50 ms or lower. As the result, a lot of work has been done to reduce the handoff latency in recent years. However, most of the work has failed to consider a complete authentication process which is useful in real scenarios.

MIP (Mobile IP) is the most widely known mobility management proposal and has, thus, become the most common solution that can offer seamless handoff to mobile devices on the Internet [11]. Essentially, MIP uses two addresses to handle the movement of the user. Every time the MN (Mobile Node) connects to a foreign network, it obtains a temporary address called CoA (care-of-address) from a mobile agent called FA (foreign agent) through the exchange of ASAA (agent solicitation and agent advertisement) messages. However, MIP is originally designed to operate at L3 (Layer 3) only regardless of the underlying link layer (L2). This approach thus implies a clear separation between L2 and L3 handoff functionality, which may lead to unacceptable handoff latency. Actually, the messages generated by the registration process need some time to propagate through the network and the MN is unable to send or receive packets during that time [12].

IEEE P802.11 s™/D1.01 [13] provides an EMSA (efficient mesh security association) authentication scheme based on the IEEE 802.11i standard where the 802.1× scheme and four handshakes are adopted to implement access authentication and key establishment. EMSA can be used to achieve efficient establishment of link security between two MNs in a WMN. It relies on a mesh key hierarchy in which keys are derived through the use of a PSK or when a MN performs IEEE 802.1× authentication. EMSA makes use of EAP (extended authentication protocol) just like EAP-SIM (subscriber identity module), EAP-TLS (transport layer security), EAP-TTLS (tunneled transport layer security) and PEAP (protected extensible authentication protocol). However, handoff in WMNs is not adequately addressed in EMSA due primarily to the reason that EMSA cannot meet the requirement of performance and identity protection in handoff.

A predictive authentication scheme is proposed in [14] using FHR (frequent handoff region). In the scheme, a statistical method is used to modulate the mobility pattern of the mobile terminal. A set of access points are selected as the FHR access points with which the mobile terminal may be associated in the near future. Before handoff, the mobile terminal sends an authentication request to the authentication server and the authentication server sends the authentication response to the FHR access points with authentication information. During handoff, the mobile terminal only needs to exchange a few messages with the new access point. However, how to select an appropriate FHR member and establish a secure connection with the FHR is not adequately addressed in the paper.

A scheme for efficient mobility management in WMNs was presented in [15]. In the scheme, a new model of location service is proposed based on several design principles. First, the proposal distinguishes between an allotted address, which changes according to the geographical location of the node, and a persistent identifier, which remains unchangeable despite the movement. This requirement thus needs the presence of a mapping service to locate each station and can be carried out by installing "Distributed Location Service", resulting in additional centralized equipment in the network. In addition, the scheme causes additional resource consumption and great computation latency.

An efficient and robust identity-based handoff authentication in wireless networks was proposed in [16] in which a special double-trapdoor chameleon hash function is the key. Compared to other existing identity-based handoff schemes, the main advantage of this scheme is to remove the assumption that PKG (private key generator) must be fully trusted, which could result in high security and simply deployment. However, this scheme is more suitable for WLAN since in a multi-hop WMN, there may not be any PKG in a more complicated environment.

3. TPM and TNC

A TPM (Trusted Platform Module) is usually implemented on a chip and is hence integrated into the hardware of a platform, such as a PC, a laptop, a PDA or a mobile phone. A property of TPM is that it owns shielded locations, meaning that only TPM itself can access the storage inside the TPM, as well as protected functionality, meaning that the functions computed inside the TPM cannot be tampered with and can only be accessed directly via TPM commands or via higher layer application interfaces TSS (TCG Software Stack).

In order to verify the configuration of a platform, all parts engaged in the boot process of the platform, e.g. BIOS and master boot record are measured using some integrity measurement hash values and the final result of the accumulated hash values is stored inside the TPM in an area called PCR (platform configuration registers). An entity that needs to verify if the platform is in a certain configuration will require TPM to sign the content of the PCR using its AIK (attestation identity key) that is generated specifically for this purpose. Then, the verifier would check the signature, compare the PCR values with some reference values to verify that the platform is indeed in a desired state and to verify the trustworthiness of an

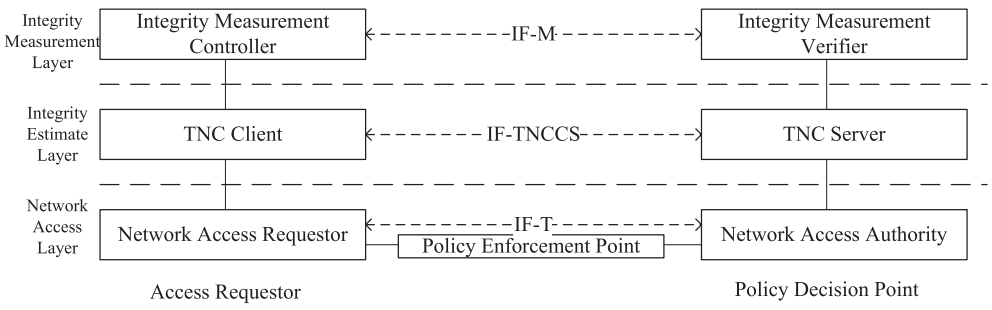

Fig. 1. The TNC architecture.