International Journal of Wireless Networks and Broadband Technologies
Volume 6 • Issue 2 • July-December 2017

Robust Secured Roaming in Wireless Local Area Networks

Shaldon L. Suntu, University of Science and Technology, Beijing, China
Nickson H. Odongo, University of Science and Technology, Beijing, China
Samwel M. Chege, University of Science and Technology, Beijing, China
Obadia K. Bishoge, University of Science and Technology, Beijing, China

ABSTRACT

This article describes how wireless local area networks are the prime way of accessing the internet nowadays. A secure roaming of information between the mobile stations moving through vertical or horizontal domains need to be swift, to reduce the delays which degrade video streaming and voice-over-wireless local area networks. In this article, various roaming schemes are researched with a goal of reducing the long delays. These are exhibited particularly in mobile internet protocol schemes which suffer from the triangular routing of information via the home agent during handover of the session keys from the original access point to the targeted access point. In this article, opportunistic key caching forwards pairwise keys ahead of the mobile station prior to subsequent association. On the hand, pair-wise master key caching plays backward roaming where the cached keys available on both devices are utilized, thus, skipping reauthentication and only performing a four-way handclasp to legitimize the roaming client

INTRODUCTION

Nowadays wireless local area network (WLAN) is the fundamental way of connecting to the internet. Wi-Fi has become an imperative element in our day-to-day life. Wi-Fi Alliance and various vendors are working up to ensure there is high speed and secured mobility in WLANs for roaming users. Real-time applications exchange in offices, health facilities, education sector etcetera are larger photo files, voice over the internet protocol (VoIP), internet of things(Yan, Zhang, & Vasilakos, 2014) and video streaming (Shi, Shen, & Jon, 2002). These services require a high-speed internet connection and fast roaming within the user's vicinity. To achieve these ingredients, robust roaming and efficient handover between the clients and the access points (APs) through a wireless environment with multiple APs. Security is a challenge in the wireless environment due to the imposters' ego to intercept and eavesdrop sensitive data while in transit to the receiving end. Wireless Gigabit (WiGig) based devices

DOI: 10.4018/IJWNBT.2017070102

are expected to sprout vigorously into the market to occupy the uncongested 60GHz frequency band with the aim of decongesting 2.4GHz and 5GHz frequencies.

To ensure interoperability, triband emerged to ensure that there is a fast handover of security keys exchange and frequencies roaming or band roaming in the 2.4GHz, 5GHz, and 60GHz devices.

Wireless LAN is the backbone of today's wireless communication. Clients can only be concomitant to one AP at a time, roaming from AP to AP must be swift for the user to have a seamless experience. Users exchange huge files, converse using voice over internet protocol (VoIP) and streaming of the videos. Mobility is one of the challenging factors in the infrastructure network (Mustafa, Mahmood, Chaudhry, & Ibrahim, 2005; Sánchez-Carmona, Borrego, Robles, & Garcia-Vandellós, 2017) for intra-domain and inter-domain clients. Users need to roam through the building seamlessly to avoid service disruption. Long delays degraded the quality of services on demand that requires a minimal handoff latency while the user is roaming. Another critical problem is the security while exchanging the handover keys during the association and dissociation from prior AP to posterior AP. IEEE 802.1X/EAP mechanism is pragmatic in an enterprises network for mutual authentication. WPA2- Enterprise is widely used for scrambling information while in transit.

The study aimed to put into play a secured handoff with minimal latency during the forward and backward roaming process for both horizontal and vertical handovers.

Handoff Process

Handover is the process by which mobile station (MSTA) moves from one access point (AP) to another when the signal network ratio falls below the expected threshold. A successful handoff process must portray these crucial features; low latency perceived during the handover process and the security of the buffered data transmitted to the new AP.

In a wireless environment, the primary objective is to ensure that there is a secure handing over of buffered data during the transition process. To ensure secure roaming enterprise network employs IEEE 802.1X/EAP authentication scheme. RADIUS servers securely transport EAP types between the Authentication server (AS) and the authenticator (Access point (AP)). Figure 1 shows a logical handoff summary in a three-step process.

In the above scenario, the AP scans for the availability of MSTA by sending a preconfigured passive scanning stipulated beacon frames at an interval of 102.4msec. The MSTA can perform an active scan by listening to a wireless broadcasting channel to detect the presence of APs beacons within its proximity. Upon successful scanning of the environment, the MSTA enters in the authentication phase. In the verification phase, the MSTA sends authentication requests to the AP, which in turn replies with an authentication feedback. The re-association process is the last step. In this phase, the AP associates with the MSTA. The time difference between scanning and re-association phases is known as the handoff latency.

The user can walk away from the associated AP coverage area and this may decreases signal strength to a certain level. This pushes the MSTA to scan for the APs with an auspicious received

Figure 1. Handoff Process between MS in a Multiple APs Scenario