



Secured Vertical Handoff between 802.16a and 802.16m for Fourth Generation (4G) Wireless Networks using PKM (Public Key Management)

Sachin Marke¹ S.S Shriramwar²

¹M.Tech(comm.), ²Asst.Prof

Department of Electronics and Telecom. Engg,
Priyadarshini College of Engineering,
Nagpur, INDIA

Abstract: The modern communication system is aimed to reach the real world one environment from virtual world via connecting resources of one with another through social network system. In Fourth generation wireless network (4g) , increasing demand of wireless networks, to provide seamless and secure handoff has become an important factor in wireless networks. To monitor unauthorized access, modification, misuse and network-accessible resources various provisions and policies are adopted by the network in network security process. Some wireless products have weaker security features so to attain the higher levels of integrity, authenticity, and confidentiality, network security features need to be embedded in the handoff policies. For security purpose we will present a Secured Vertical Handoff Decision (Sec-DVHD) scheme using PKM(Public Key Management).

Keywords-Handoff decision, 4G, public key Management, Mobile Node, Wireless network

I. Introduction

One of the main issues in the Fourth Generation (4G) wireless networks is the vertical handoff decision. The handoff mechanism in order to used to let a Mobile Node (MN) switches from a network to another without remarkable service disconnection. In future heterogeneous 4G network there may be several available networks at the same time and location. During this process i.e.(If a mobile terminals need to switches from one wireless system to another), how to execute the vertical handoff at the right time and how to satisfy the entire applications working on mobile terminal are still exciting research fields. The handoff is the mechanism used in order to let a Mobile Node (MN) switches from a network to mobile node .The major issue which generally degrades the Quality of Service (QoS) is the delay required to choose suitable network to which the MN may connect .

In this context and in order to provide continuous service we proposed in a Distributed Vertical Handover Decision (DVHD) scheme. DVHD main goals is to reduce the processing delay at the Mobile Node (MN) side and the number of exchanged information between MN and neighbor networks, by delegating the user profiles and the computing task among networks Briefly, DVHD process is as follow; the MN initiates the handoff process and sends its reference to all available neighbor networks and computes its Network Quality Value (NQV). NQV is passed to the MN, which compares all received NQVs and chooses the network with the highest NQV as the network to which it will redirect its connections.

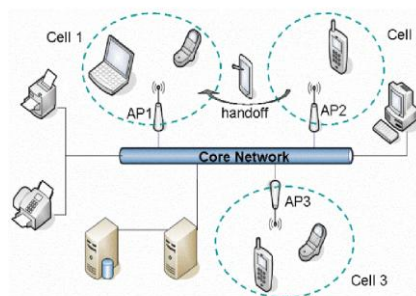


Figure 1: Vertical Handoff in heterogeneous networks

Vertical handovers:

A. Supervision of handover processes and vertical handovers

Handover is the process of maintaining a user's active sessions when a mobile terminal changes its connection from one network to another access network, There are two types of handover i.e. horizontal and vertical. A horizontal handover is the handover between points of attachment supporting the same network technology. for example, two neighboring base stations of a cellular network. On the other hand, a vertical handover is the handover when points of attachment supporting different network technologies.

A handover process can be divided into three stages: hand-over decision, channel assignment and radio link transfer. Handover decision involves the selection of the target point of attachment and the time of the handover.

channel assignment deals with the allocation of channel resources and Radio link transfer is for forming links to new point of attachment.

While choosing the best network VHD(Vertical Handover decision) algorithms has to take care of not only the efficiency but also criteria's such as service cost and power so that maximum user satisfaction is achieved. For Horizontal Handover Decision measure parameter of concern is RSS.

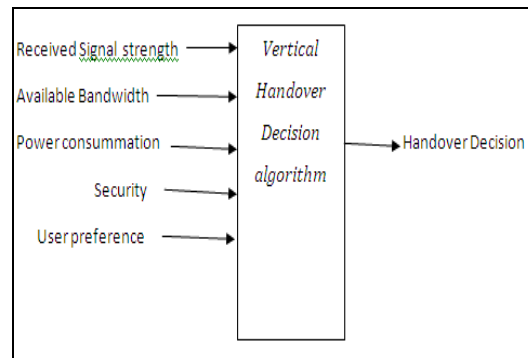


Figure 2: Parameters used for making VHD decisions

B. Key Management Issues for Public Key Cryptography

The public key cryptography has one interesting concept which solves the problem of distributing secret keys. The message send by user1 is received only by user2 without agreeing on secret key, because encryption & decryption keys are totally different. In practice, the methods that have been developed for realizing public key encryption are comparatively slow, and public key cryptography is generally used for encrypting "session keys" that are then used for a faster traditional single-key encryption method such as the Data Encryption Standard (DES).

Digital signatures are also implemented in Public key cryptography. As public and private keys are different, without disclosing secret key users can sign their data & allow others to verify their signatures with the help of public key. Public key cryptography provides two schemes to encrypt messages:

- i. Users can "sign" messages by encrypting them with their private keys. Since any message recipient can check that the user's public key can decrypt the message, and also prove that the user's secret key was used to encrypt it.
- ii. Users can send secret messages, by encrypting them with the recipient's public key. In this case, only the intended recipient can decrypt the message, since only that user should have access to the required secret key.

For a scalability reason, we use in our proposal the first scheme. The public key or the asymmetric cryptography allows each user (sender) to have a pair of public/private key. Once user-1 wants to send a message to user-2, it encrypts the message with its private key. Then, at the reception of this message user-2 decrypts the message using the user-1 public key.

To manage the creation and liberation processes of the pairs public/private key we need a key management system, which implements the Public Key Infrastructure (PKI).

This PKI covers several jobs:

- (i) Generates pairs of keys (public / private keys).
- (ii) Insures the correspondent between public key and user.
- (iii) Certifies the association between each user and its public key.
- (iv) Revokes key (in case of loss by its owner, expiration date of its validity or compromise).

C. Vertical Handoff Decision

Here we describe how the Vertical Handoff Algorithm was implemented and how the simulation was carried out. It is important that we test the performance of the algorithm by simulating it over a wide range of simulation parameters. This is true not only for the Vertical Handoff Algorithm but as a matter of fact, for any algorithm. Simulation firstly, helps us determine whether the algorithm is performing correctly as required by the standards and the user. Before the algorithm is implemented in real time systems, its performance has to be carefully studied so that, the system in which the algorithm is implemented performs according to the users expectations. Secondly, this simulation also helps us determine the right values of the parameters that need to be set so that the algorithm attains a satisfactory performance level. If the parameters are not appropriately set then it may happen that the algorithm might be switching too often between the two networks without any real necessity for doing it and thus, causing a sub-optimal performance of the system/device; or it might also happen that the algorithm does not switch the device connection between networks even though the device might perform better in the other network.

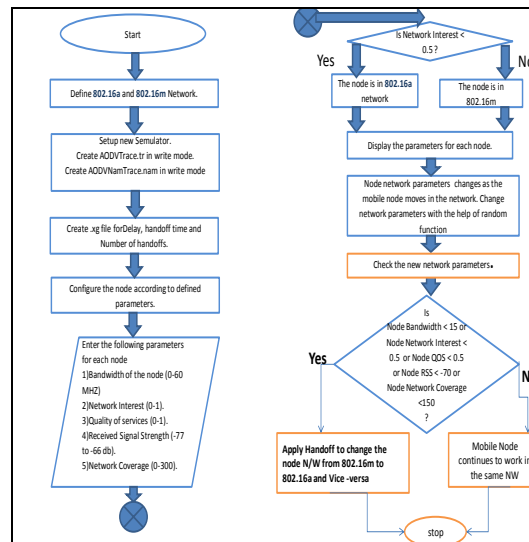


Fig. 3 Vertical Handoff Procedure between 802.16a and 802.16m

II. Simulation Result:

In figure 4.1, we have plotted the delay in handoff by the node against the time spent in network. It shows that as the node under goes handoff mechanism the delay in transmission of packets increases. This is because all the layers in the communication protocol stack contribute to the delay in a handoff. Depending on the access technology, a mobile node may go through several steps with each step adding its contribution to the overall delay before a new link is established.

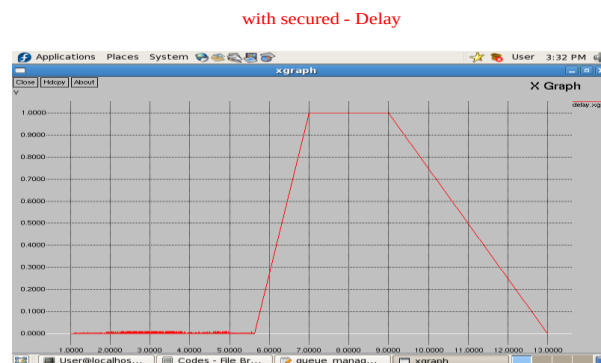


Fig. 4.1. Plot of Delay in handoff (vs) Time Spent in Network with secured

In Figure 4.2 shows that as the device spent more time in network, the handoff delay remains the same. The delay increases suddenly at the time when the device undergoes handoff mechanism. This is because as the device moves away from the tower the threshold value of various parameters like network bandwidth, node network interest, network coverage, RSS of a node and QoS decreases.

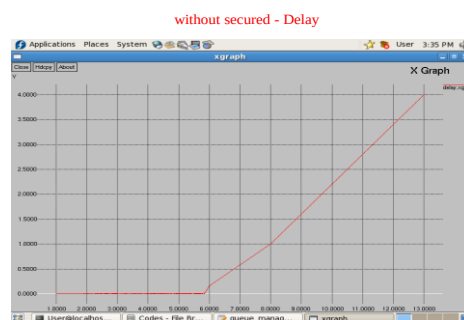


Fig. 4.2 Plot of Delay in handoff (vs) Time Spent in Network without secured

In Figure 4.3, we have plotted the delay in handoff by the node against the time spent in network without security. It shows that as the node under goes handoff mechanism the delay in transmission of packets increases.

From the above graphs we can compare Handoff delay in network i.e. Secured vertical handoff and without Secured vertical handoff.

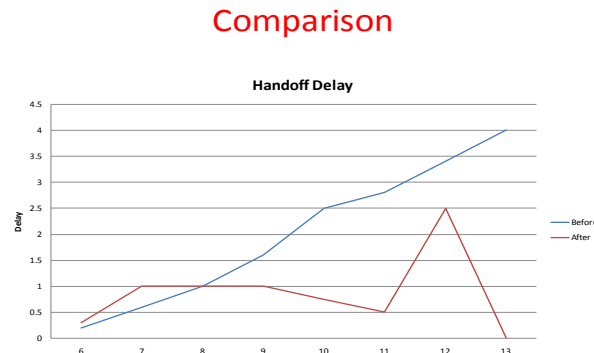


Figure4.3: Comparison between SVH with security and SVH without security

References:

- [1]. Ram tawil, Jacques Demarjien and Guy Pujolle, "Secured Vertical Handoff Decision Scheme for the fourth Generation wireless network", International conference ,IEEE 24-27 nov.-2008.
- [2]. Yaw Nkansa-Gyekye and Johnson I. Agbinya, "Driven Vertical Handoff Decision scheme Algorithm for 4G wireless network", AusWireless 2007, IEEE computer A society.
- [3]. Enrique Stevens-Navarro and Vincent W.S.Wong, "Providing security in fourth Generation wireless network", IEEE-VTC 2006.
- [4]. McNair, J., Zhu, F., 2004. Vertical handoffs in fourth-generation multinet network environments. IEEE Wireless Communications 11, 8–15.
- [5]. G.Mapp, D.N Cotingham, F. Shaikh, P. Vidales,L. Patanapongpibul, J. Crowcroft, "An Architecture Framework for Heterogeneous Networking" International conference on wireless information network and system(WINSYS), pp 5-10, august 2006.
- [6]. Y. Park and T. Park "A Survey of Security Threats on 4G Network" in Communication & Networking Lab. Samsung Adv. Inst. Of TechnologyGlobecom. Workshops, IEEE Washington, DC pp 1-6. 22-01-2008.
- [7]. Mandeep Kaur Gondara and Dr. Sanjay Kadam" Requirements of Vertical Handoff mechanism in 4G wireless networks" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 2, April 2011.