© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Secured Vertical Handoff between 802.16a and 802.16m for Fourth Generation (4G) Wireless Networks

Prajwalsingh C. Parihar[1], Meghna R. Patil[2], Sachin Marke[3], Parul Sahare[4]
[1,2]Electronics & Communication Engineering Department, Dr. Babasaheb Ambedkar College of Engineering, Maharashtra, Nagpur, India
[3]Electronics & Telecommunication Engineering Department, PIGCE, Nagpur
[42]Electronics & Communication Engineering (Center for VLSI & NANO technology) Department, VNIT, Nagpur, India

ABSTRACT

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. In a wireless environment, data is broadcast through the air and people do not have physical controls over the boundaries of transmissions. 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. In order to provide continuous service we proposed in a Distributed Vertical Handover Decision (DVHD) scheme, 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 use 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.

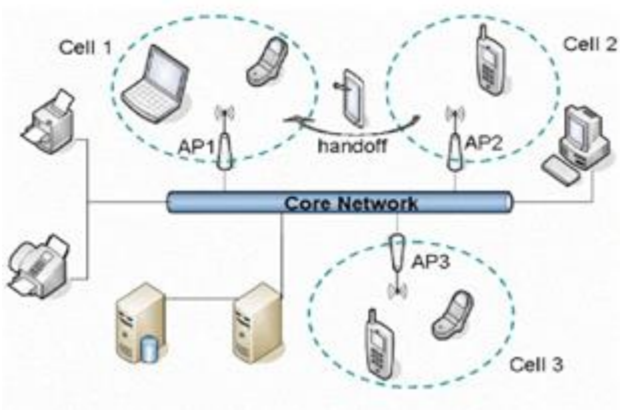


Figure 1. Vertical Handoff in heterogeneous networks

II. METHODS AND MATERIAL

1. Vertical Handoff

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.

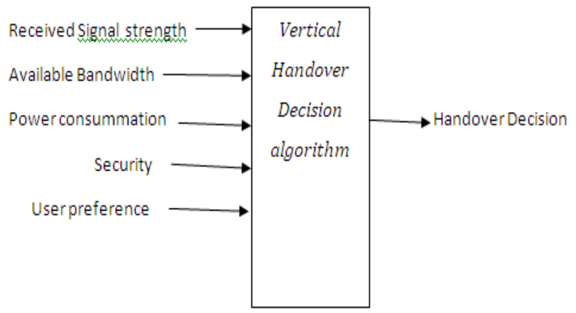


Figure 2. Parameters used for making VHD decisions

2. 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:

1. 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.
2. 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

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

3. Secured-Distributed Verticalhandoff Decision (SEC-DVHD)

The provision of seamless vertical handover requires the design of a robust Vertical Handover Decision (VHD) scheme. we assume that the MN is moving in an area covered by different networks, managed by one or different operator(s).Networks involved in the mobility area are divided into two categories:

- Serving Network (SN):
  SN is the network to which the MN is actually connected.
- Target Network (TN):
  TN is the available network to which the MN may connect.

These networks consist of Point of Attachments (PoAs) implementing different technology types, such as UMTS, WiMax, WiFi, etc.Handoff events occur when QoS degradation appears at the SN. Thus, the MN switches to the appropriate TN using the DVHD scheme, this TN will be the MN's SN.

In the process of sec-DVHD, The MN initiates the handoff process basing on QoS degradation at the SN. Then, the MN sends its Mobile Node Identity (MNID) to each TN, encrypts the NQV using the PoA's PrK (the TN's PoA to which the MN may connect) and sends the encrypted NQV to the MN. The MN receives the encrypted NQV from all TNs, decrypts the received messages using the corresponding PoA's PuK. After creating a list of confidence PoAs' NQVs (by eliminating the NQVs coming from malicious PoA) the MN picks up the highest NQV value and redirects its connection to the chosen network.

4. SEC-DVH Decision Making Parameters

A) Bandwidth

Bandwidth is a measure of the width of a range of frequencies. Higher the bandwidth, lower the call dropping and call blocking probability.

B) Handoff Latency

The time elapses between the last packet received via the old access router and the arrival of the first packet along the new access router after a handoff. This is known as handoff latency. Handoff Latency affects the QoS and it is essential to consider handoff latency while designing any handoff technique.

C) Power Consumption

During handoff, frequent interface activation can cause considerable battery drainage. It is also important to incorporate power consumption factor during handoff decision.

D) Network Cost

A multi criteria algorithm for handoff should also consider the network cost factor. Different charging policies are followed for different type of traffic. So that in some situation cost should also be consider as a factor for decision making.

E) User Preferences

Based on the application requirements like (real time, non-real time), service types (Voice, data, video), Quality of service etc. the user may prefer different network according to the network performance which is the important benefit of heterogeneous networks.

F) Network Throughput

Network throughput refers to the average data rate of successful data or message delivery over a specific communications link. Handover to the network which has higher throughput is desirable.

G) Network Security

It consists of the provisions and policies adopted by the network to prevent and monitor unauthorized access, misuse, modification, and network-accessible resources.

H) Received Signal strength (RSS)

The performance of a wireless network connection depends in part on signal strength. The wireless signal strength in each direction determines the total amount of network bandwidth available along that connection. A signal should be strong enough between mobile unit and base station to maintain signal quality at receiver.

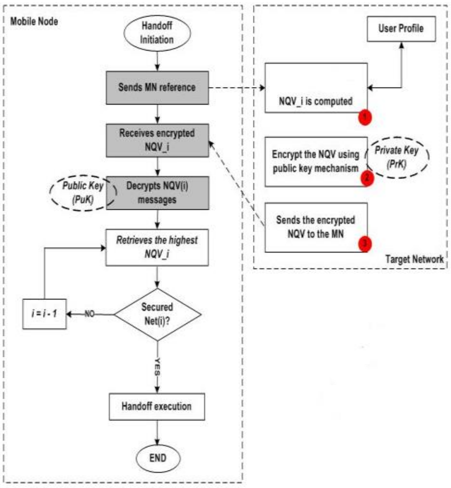


Figure 3. Sec-DVHD Process

III. RESULTS AND DISCUSSION

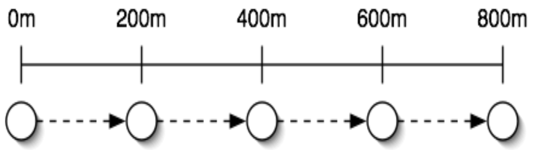
1. Workflow

- (Optional) Create custom ns2 object.
- Create TCL scenario file.
- Run the scenario to produce a trace file.
- Process the trace file to get results.

2. Basic Wireless Scenario

- Chain of 5 nodes, spaced 200m apart
- Use DSDV routing
- FTP transfer from one end to the other

Want to measure the throughput



3. Options

```
# ===============
# Define options
# ===============
set val(chan) Channel/WirelessChannel ;# channel type
set val(prop) Propagation/TwoRayGround ;# radio-propagation model
set val(ant) Antenna/OmniAntenna ;# Antenna type
set val(ll) LL ;# Link layer type
set val(ifq) Queue/DropTail/PriQueue ;# Interface queue type
set val(ifqlen) 50 ;# max packet in ifq
set val(netif) Phy/WirelessPhy ;# network interface type
set val(mac) Mac/802_11 ;# MAC type
set val(rp) DSDV ;# ad-hoc routing protocol
set val(nn) 5 ;# number of mobilenodes
```

4. Set Up Simulator

```
# Create simulator
set ns_ [new Simulator]

# Set up trace file
$ns_ use-newtrace
set tracefd [open simple.tr w]
$ns_ trace-all $tracefd

# Create the "general operations director"
# Used internally by MAC layer: must create!
create-god $val(nn)

# Create and configure topography (used for mobile scenarios)
set topo [new Topography]
# 1000x1000m terrain
$topo load_flatgrid 1000 1000
```

5. Configure Nodes

```
$ns_ node-config -adhocRouting $val(rp) \
 -llType $val(ll) \
 -macType $val(mac) \
 -ifqType $val(ifq) \
 -ifqLen $val(ifqlen) \
 -antType $val(ant) \
 -propType $val(prop) \
 -phyType $val(netif) \
 -channel [new $val(chan)] \
 -topoInstance $topo \
 -agentTrace ON \
 -routerTrace ON \
 -macTrace OFF \
 -movementTrace OFF
```

6. Creat Nodes

```
for {set i 0} {$i < $val(nn) } {incr i} {
 set node_($i) [$ns_ node]
 $node_($i) random-motion 0 ;# disable random motion
 $node_($i) set X_ 0.0
 $node_($i) set Y_ 0.0
 $node_($i) set Z_ 0.0
}
```

$node_(0) set X_ 0.0
$node_(1) set X_ 200.0
$node_(2) set X_ 400.0
$node_(3) set X_ 600.0
$node_(4) set X_ 800.0

7. Source And Destination

1500 - 20 byte IP header - 40 byte TCP header = 1440 bytes
Agent/TCP set packetSize_ 1440 ;# This size EXCLUDES the TCP header

set agent [new Agent/TCP]
set app [new Application/FTP]
set sink [new Agent/TCPSink]

$app attach-agent $agent

$ns_ attach-agent $node_(0) $agent
$ns_ attach-agent $node_(4) $sink
$ns_ connect $agent $sink

8. Run It

120 seconds of running the simulation time
$ns_ at 0.0 "$app start"
$ns_ at 120.0 "$ns_ halt"
$ns_ run

$ns_ flush-trace
close $tracefd

9. Trace File

s -t 0.000000000 -Hs 0 -Hd -2 -Ni 0 -Nx 0.00 -Ny 0.00 -Nz 0.00 -Ne -1.000000 -Nl AGT …
r -t 0.000000000 -Hs 0 -Hd -2 -Ni 0 -Nx 0.00 -Ny 0.00 -Nz 0.00 -Ne -1.000000 -Nl RTR **…**
Each line represents a message being transferred
Common fields:

- Event type (s = send, r = received, d = drop)
- Time stamp
- Source and destination
- XYZ co-ordinates of the node
- Network layer (AGT = agent, RTR = router, …)
- … many many others

10. Result

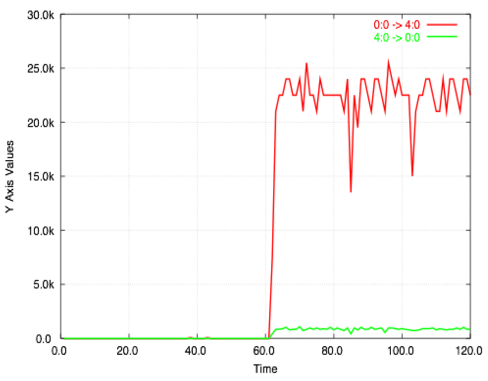


Figure 4. Simulation output

IV. REFERENCES

[1] Ram tawil, Jacques Demarjien and Guy Pujolle," Secured Vertical Handoff between 802.16a and 802.16m fourth Generation wireless network using parameter thresholding protocol",

[2] 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

[3] Yaw Nkansa-Gyekye and Johnson I. Agbinya," Driven Vertical Handoff Decision scheme Algorithm for 4G wireless network", AusWireless 2007, IEEE computer A society

[4] Enrique Stevens-Navarro and Vincent W.S.Wong," Providing security in fourth Generation wireless network", IEEE-VTC 2006

[5] Mcnair, J., Zhu, F., 2004. Vertical handoffs in fourth-generation multinetwork environments. IEEE Wireless Communications 11, 8–15.

[6] 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, augest 2006

[7] 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

[8] 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