1

Optimization of IPV$_6$ over 802.16e WiMAX Network Using Policy Based Routing Protocol

David Oluwashola Adeniji
University of Ibadan
Nigeria

1. Introduction

Internet application needs to know the IP address and port number of the remote entity with which it is communicating during mobility. Route optimization requires traffic to be tunneled between the correspondent node(CN) and the mobile node (MN).). Mobile IPv6 avoids so-called triangular routing of packets from a correspondent node to the mobile node via the Home Agent. Correspondent nodes now can communicate with the mobile node without using tunnel at the Home Agent..The fundamental focal point for Optimization of IPv6 over WiMAX Network using Policy Based Routing Protocol centered on the special features that describe the goal of optimization mechanism during mobility management. To reiterate these features there is need to address the basic concept of optimization as related to mobility in mobile IPv6 Network. WiMAX which stands for Worldwide Interoperability for Microwave Access, is an open, worldwide broadband telecommunications standard for both fixed and mobile deployments. The primary purpose of WiMAX is to ensure the delivery of wireless data at multi-megabit rates over long distances in multiple ways. Although WiMAX allows connecting to internet without using physical elements such as router, hub, or switch. It operates at higher speeds, over greater distances, and for a greater number of people compared to the services of 802.11(WiFi).A WiMAX system has two units. They are WiMAX Transmitter Tower and WiMAX Receiver. A Base Station with WiMAX transmitter responsible for communicating on a point to multi-point basis with subscriber stations is mounted on a building. Its tower can cover up to 3,000 Sq. miles and connect to internet. A second Tower or Backhaul can also be connected using a line of sight, microwave link. The Receiver and antenna can be built into Laptop for wireless access.This statement brings to the fact that if receiver and antenna are built into the laptop, optimization can take place using a routing protocol that can interface mobile IPv6 network over WiMAX 802.16e.However the generic overview of optimization possibilities most especially for a managed system can be considered.

What then is Optimization? Basically optimization is the route update signaling of information in the IP headers of data packets which enable packets to follow the optimal path and reach their destination intact. The generic consideration in designing route optimization scheme is to use minimumsignaling information in the packet header. Furthermore the delivery of managed system for optimization describes the route optimization operation and the mechanism used for the optimization. In order for

optimization to take place, a protocol called route optimization protocol must be introduced. Route optimization protocol is used basically to improve performance. Also route optimization is a technique that enables mobile node and a correspondent node to communicate directly, bypassing the home agent completely; this is based on IPv6 concept.

The use of domains enables a consistent state of deployment to be maintained. The main benefits of using policy are to improve scalability and flexibility for the management system. Scalability is improved by uniformly applying the same policy to large sets of devices , while flexibility is achieved by separating the policy from the implementation of the managed system. Policy can be changed dynamically, thus changing the behavior and strategy of a system, without modifying its implementation or interrupting its operation. Policy-based management is largely supported by standards organizations such as the Internet Engineering Task Force (IETF) and the Distributed Management Task Force (DMTF) and most network equipment vendors.However the Architectures for enforcing policies are moving towards strongly distributed paradigms, using technologies such as mobile code, distributed objects, intelligent agents or programmable networks.

Mobile IP is the standard for mobility management in IP networks. New applications and protocols will be created and Mobile IP is important for this development. Mobile IP support is needed to allow mobile hosts to move between networks with maintained connectivity. However internet service driven network is a new approach to the provision of network computing that concentrates on the services you want to provide. These services range from the low-level services that manage relationships between networked devices to the value-added services provided to the end-users. The complexity of the managed systems results in high administrative costs and long deployment cycles for business initiatives, and imposes basic requirements on their management systems. Although these requirements have long been recognized, their importance is now becoming increasingly critical. The requirements for management systems have been identified and can be facilitated with policy-based management approach where the support for distribution, automation and dynamic adaptation of the behaviour of the managed system is achieved by using policies. IPV6 is one of the useful delivery protocols for future fixed and wireless/mobile network environment while multihoming is the tools for delivering such protocol to the end users. Optimization of Network must be able to address specific market requirements, deployment geographical, end-user demands, and planned service offerings both for today as well as for tomorrow.

2. IP mobility

The common mechanism that can manage the mobility of all mobile nodes in all types of wireless networks is the main essential requirement for realizing the future ubiquitous computing systems. Mobile IP protocol V_4 or V_6 considered to be universal solutions for mobility management because they can hide the heterogeneity in the link-specific technology used in different network. Internet application needs to know the IP address and port number of the remote entity with which it is communicating during mobility. From a network layer perspective, a user is not mobile if the same link is used, regardless of location. If a mobile node can maintain its IP address while moving, it makes the movement transparent to the application, and then mobility becomes invisible. From this problem the basic requirement for a mobile host is the

Mobile IP works in the global internet when the mobile node (MN) which belong to the home agent (HA) moves to a new segment, which is called a foreign network (FN). The MN registers with the foreign agent (FA) in FN to obtain a temporary address i.e a care of address(COA).The MN updates the COA with the HA in its home network by sending BU update message. Any packets from the corresponding node (CN) to MN home address are intercepted by HA. HA then use the BU directly to the CN by looking at the source address of the packet header.

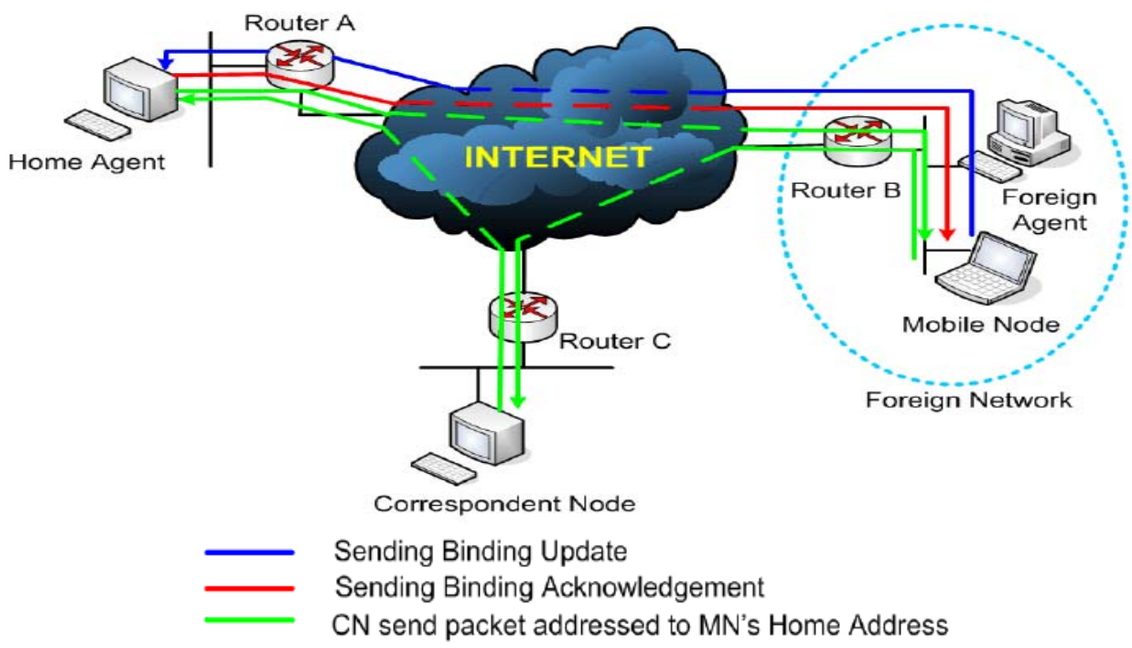

Fig. 1. Mobile IP Network

The most critical challenges of providing mobility at the IP layer is to route packets efficiently and securely. In the mobile IP protocol all packets are sent to a mobile node while away from home are intercepted by its home agent and tunneled to the mobile node using IP encapsulation within IP.

2.1 Limitation of mobile IP

Mobile IP can only provide continuous Internet connectivity and optimal routing to a mobile host, and are not suitable to support a mobile network. The reasons is that, not all devices in a mobile network is sophisticated enough to run these complicated protocols.Secondly, once a device has joined a mobile network, it may not see any link-level handoffs even as the network moves.

2.2 Detailed description of NEMO

Network Mobility describes the situation of a router connecting an entire network to the Internet dynamically changes its point of attachment. The connections of the nodes inside the network to the Internet are also influenced by this movement. A mobile network can be

connected to the Internet through one or more MR, (the gateway of the mobile network), there are a number of nodes (Mobile Network Nodes, MNN) attached behind the MR(s). A mobile network can be local fixed node, visiting or nested. In the case of local fixed node: nodes which belong to the mobile network and cannot move with respect to MR. This node are not able to achieve global connectivity without the support of MR. Visiting node belong to the mobile network and can move with respect to the MR(s).Nested mobile network allow another MR to attached to its mobile network. However the operation of each MR remains the same whether the MR attaches to MR or fixed to an access router on the internet. Furthermore in the case of nested mobile network the level mobility is unlimited, management might become very complicated. In NEMO basic support it is important to note that there are some mechanism that allow to allow mobile network nodes to remain connected to the Internet and continuously reachable at all times while the mobile network they are attached to changes its point of attachment.Meanwhile, it would also be meaningful to investigate the effects of Network Mobility on various aspects of internet communication such as routing protocol changes, implications of real-time traffic, fast handover and optimization. When a MR and its mobile network move to a foreign domain, the MR would register its care-of-address (CoA) with it's HA for both MNNs and itself. An IP-in-IP tunnel is then set up between the MR and it's HA. All the nodes behind the MR would not see the movement, thus they would not have any CoA, removing the need for them to register anything at the HA. All the traffic would pass the tunnel connecting the MR and the HA. Figure 2.3 describes how NEMO works.

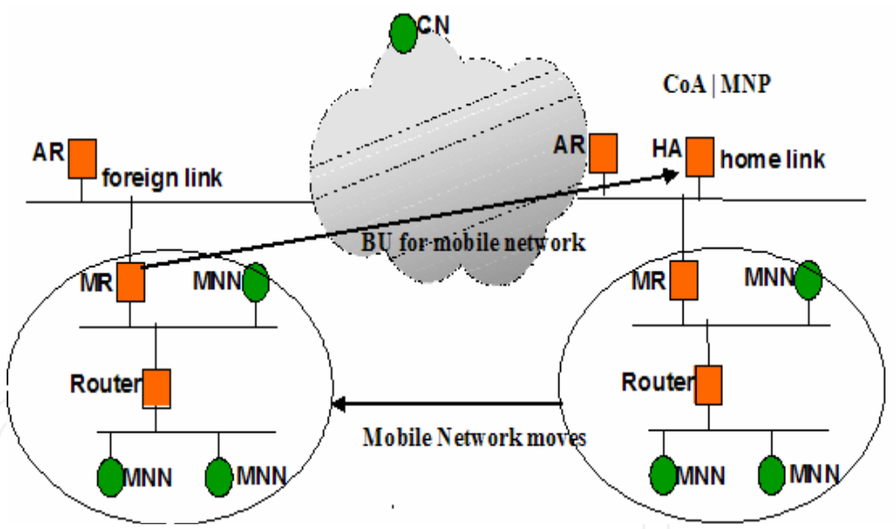

Fig. 2. Network Mobility

2.3 Micro mobility and Macro mobility

This discussion on Micromobility and Macromobility is centered on wireless communication architecture that focuses on the designed of IP Micromobility protocol that compliment an IETF standard for Macromobility management which is usually called Mobile IP. From this point of view, Macro-mobility concerns with the management of users movements at a large scale, between different wide wirelesses accesses networks connected to the Internet. Macro-mobility is often assumed to be managed through Mobile IP. On the

other hand, Micro-mobility covers the management of users movements at a local level, inside a particular wireless network.The standard Internet Protocol assumes that an IP address always identifies the node's location in the Internet. This means that if a node moves to another location in the Internet, it has to change its IP address or otherwise the IP packets cannot be routed to its new location anymore. Because of this the upper layer protocol connections have to be reopened in the mobile node's new location.

The Technologies which can be Hierarchical Mobile IP,Cellular IP,HAWAII at different micro mobility solutions could coexist simultaneously in different parts of the Internet. Even at that the Message exchanges are asymmetric on Mobile IP. In cellular networks, message exchanges are symmetric in that the routes to send and receive messages are the same. Considering the mobile Equipment the appropriate location update and registration separate the global mobility from the local mobility. Hence Location information is maintained by routing cache. During Routing most especially in macro mobility scenario a node uses a gateway discovery protocol to find neighboring gateways Based on this information a node decides which gateway to use for relaying packets to the Internet. Then, packets are sent to the chosen gateway by means of unicast. With anycast routing, a node leaves the choice of gateway to the routing protocol.

The routing protocol then routes the packets in an anycast manner to one of the gateways.In the first case, a node knows which gateway it relays its packets to and thus is aware of its macro mobility.

The comparative investigation of different requirement between Micro mobility and Macro mobility are based on following below:

- ***Handoff Mobility Management Parameter***:The interactions with the radio layer, initiator of the handover management mechanism, use of traffic bicasting were necessary. The handoff latency is the parameter time needed to complete the handoff inside the network. Also potential packet losses were the amount of lost packets during the handoff must be deduced. Furthermore the involved stations: the number of MAs that must update the respective routing data or process messages during the handover are required.
- ***Passive Connectivity*** with respect to paging required an architecture that can support via paging order to control traffic against network burden.This architecture is used to support only incoming data packet.Therefore the ratio of incoming and outcoming communication or number of handover experienced by the mobiles are considered for efficiency support purposes.To evaluate this architecture an algorithm is used to perform the paging with respect to efficiency and network load.
- ***Intra Network Traffic*** basic in micro mobility scenario are the exchanged of packet between MNs connected to the same wireless network. This kind of communication is a large part of today's GSM communications and we can expect that it will remain an important class of traffic in future wireless networks.
- **Scalability and Robustness**: The expectation is that future large wireless access networks will have the same constrains in terms of users load. These facts are to be related to the increasing load of today's Internet routers: routing tables containing a few hundreds of thousandsentries have become a performance and optimization problem.

The review of micromobility via macromobility of key management in 5G technology must addressed the following features:

- 5G technology offer transporter class gateway with unparalleled consistency.
- The 5G technology also support virtual private network
- Remote management offered by 5G technology a user can get better and fast solution.
- The high quality services of 5G technology based on Policy to avoid error.

5G technology offer high resolution for crazy cell phone user and bi-directional large bandwidth shaping.

2.4 Concept of Multihoming

Mobile networks can have multiple points of attachment to the internet, in this case they are said to be multihomed. Multihoming arises when the MR has multiple addresses, multiple egress interfaces on the same link, or multiple egress interfaces on different links. Basically the classification of configuration can be divided into :***Configuration-Oriented Approach, Ownership-oriented Approach*** and ***Problem-Oriented Approach.*** The multihoming analysis classifies all these configuration of multihomed mobile networks using (x, y, z) notation. Variables x, y, and z respectively mean the number of MRs connected to the Internet (so called root MRs), the number of HAs, and the number of Mobile Network Prefix (MNP) s. In case of 1, each variable implies that there exists a single node or prefix. If the variable is N, then it means that one or more agents or prefixes exist in a single mobile network. From different combinations of the 3-tuple (x, y, z), various types of multihoming scenarios are possible. For example the (N, 1, 1) scenario means there is multiple MRs at the mobile network, but all of MRs are managed by single HA and use same MNP.

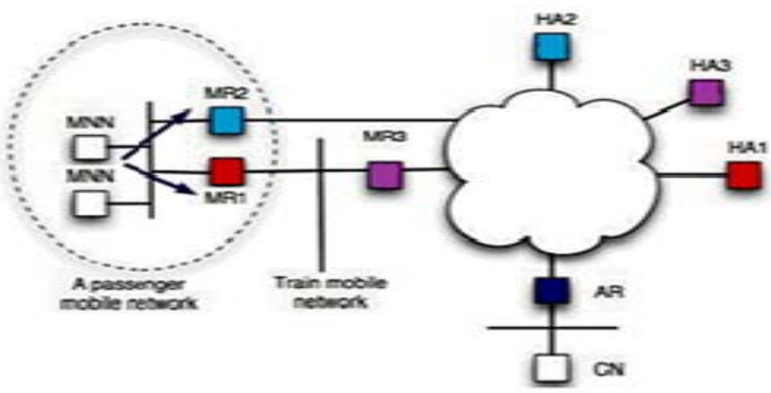

Fig. 3. A Multihoming of Nested Mobile Network

The Figure above shows how a train provide a Wifi network to the passengers with MR3, the passenger could connect to MR3 with MR1 (for example his Laptop). The passenger could also connect directly to Internet with MR2 (his Phone with its GPRS connectivity).The train is connected to Internet with Wimax connectivity. The MNNs can be a PDA and some sensors.

Multihoming from the above nested mobile network provides the advantages of session preservation and load sharing. During optimization the key data communication that must be taking into consideration are:

- Session preservation by redundancy.-the session must be preserved based on the available stable mobile environment either via wireless or wired.

- Load balancing by selecting the best available interface or enabling multiple interfaces simultanously.Traffic load balancing at the MR is critical since in mobile networks, all traffic goes through the MR.

The apprehension from the above can be justified by specifying the mobile message notification mobile node as well as the procedure for node joining. A mobility notification message contains two important information:(i) the notification interval for multihoming; and (ii)the prefix of the access network that the sending gateway belongs. The optimal choice of the notification interval depends on the mobility of the nodes as well on the amount of traffic sent.

Processing of packets from multihomed nodes is more complex and requires the gateway to perform two tasks. First,the gateway has to verify if a node has recently been informed that its packets are relayed through this access network. If this does not take place, the gateway sends a mobility notification message to the mobile node to inform it about the actual access network. For reducing the amount of mobility notification messages, the gateway records the node address combined with a time stamp in a lookup table. After a notification interval, the gateway deletes the entry and if it is still relaying packets for this node, notifies the mobile node again.Secondly the gateway substitutes the link-local address prefix of the IP source address of the packet with the prefix of the access network it belongs to and forwards the packet to the Internet. When a multihoming node receives a mobility notification message, it adjusts its address prefix to topologically fit the new access network. Subsequently,it informs about its address change using its IP mobility management protocols. In the case where packets of a node are continuously forwarded over different access networks,multihoming support is an advantage to prevent continuous address changes. When a multihoming node receives a mobility notification message, it checks if it already is aware of X or Y access network.

2.5 Requirement of Multihoming configuration

The requirement for Multihomed configurations can be classified depending on how many MRs are present, how many egress interfaces, Care-of Address (CoA), and Home Addresses (HoA) the MRs have, how many prefixes (MNPs) are available to the mobile network nodes, etc. The reader of this chapter should note that there are eight cases of configuration of multihomed mobile network. The 3 key parameter associated to differentiate the configuration are referred to 3-tuple X, Y, Z. To describe any of this requirement configurationin respect to macro mobility, a detection mechanism and notification protocol is required. The below table present the most significant features of the eight classification approach for NEMO. Although there are several configuration but NEMO does not specify any particular mechanism to manage multihoming.

	Configuration	**Class**	**Requirement**	**Prefix Advertisement**
1	Configuration 1, 1, 1	Class 1,1,1	MR, HA, MNP	1 MNP
2	Configuration 1, 1, 1	Class 1,1,n	1 MR, 1 HA, More MNP	2 MNP
3	Configuration 1, 1, 1	Class 1,n,1	1 MR, More HA, 1 MNP	1 MNP
4	Configuration 1, 1, 1	Class 1,n,n	1 MR, More HA, More MNP	Multiple MNP
5	Configuration 1, 1, 1	Class n,1,1	More MR, 1 HA, 1 MNP	MNP
6	Configuration 1, 1, 1	Class n,1,n	More MR, 1 HA, More MNP	Multiple MNP
7	Configuration 1, 1, 1	Class n,n,1	More MR, More HA, MNP	1 MNP
8	Configuration 1, 1, 1	Class n,n,n	More MR, More HA, More MNP	Multiple MNP

Table 1. Analysis of Eight cases of multihoming configuration

What then about the reliability of these configurations during NEMO? Internet connection through another interface must be reliable. The levels of ***redundancy*** cases can be divided into two: if the mobile node's IP address is not valid any more, and the solution is to use another available IP address; the order is that the connection through one interface is broken, and the solution is to use another. If one of the interfaces is broken then the solution is to use another interface using a ***Path Exploration***. However in the case of multiple HAs, the redundancy of the HA is provided, if one HA is broken, another one could be used. The important note here is the broken of one interface can also lead to failure. ***Failure Detection* in** all the cases in which the number of MNP is larger than 1, because the MNN could choose its own source address, if the tunnel to one MNP is broken, related MNNs have to use another source address which is created from another MNP. In order to keep sessions alive, both failure detection andredirection of communication mechanisms are needed. If those mechanisms could not perform very well, the transparent redundancy can not be provided as well as in the cases where only one MNP is advertised.

The only difference between using one MR with multiple egress interfaces and using multiple MRs each of which only one egress interface is ***Load sharing.*** Multiple MRs could share the processing task comparing with only one MR, and of course it provides the redundancy of the disrupting of the MR. Therefore the mechanisms for managing and cooperating between each MRs are needed.Also the common problem related to all the configuration is where the number of MNP are larger than 1 and at the same time the number of MR or the number of HA or both is larger than one. So a mechanism for solving the ***ingress filtering*** problem should be used. In most cases the solution is to use second binding on the ingress interface by sending a Prefix-BU through the other MRs and then the HA(s) get(s) all other CoAs.

How do we then distinguish between CoAs.? We use ***Preference Settings*** One solution is to use an extra identifier for different CoAs and include the identifier information in the update message. This kind of situation exists a lot, except for the cases in which one MNP is only allowed to be controlled by one CoA.

2.6 Policy Based Routing Protocol

Policy is changing the behavior and strategy of a system, without modifying its implementation or interrupting its operation. Policy-based management is largely supported by Standards organizations such as the Internet Engineering Task Force ***(IETF)*** and the Distributed Management Task Force ***(DMTF)*** and most network equipment vendors. The focal point in the area of policy-based management is the notion of policy as a means of driving management procedures. Although the technologies for building management building management systems are available, work on the specification and deployment of policies is still scarce.Routing decisions and interface selection are based entirely on IP/network layer information.In order to provide adequate information the level of hierarchy must be considered.The specific information during optimization and deployment is based on the following approach:

Link Layer Information: Interface selection algorithm should take into account all available information and at the same time minimize resource consumption and make decisions with

as light computation as possible .However , link quality must be constantlymonitored and the information must be made available for the network layer and user applications in a form that suits them best.

IP layer Information: Several attributes can be retrieved from the IPv6 header without looking into the data, e.g., source address and destination address etc.Some attributes can also be retrieved from IPv6 extension headers (e.g. HOA) only transport protocols like TCP and UDP can be identified directly from the IP header.

Network Originated Information: A service provider may disseminate information about cost, bandwidth and availability of the Internet access in an area using WiMax,WLAN, GPRS and Bluetooth. To advertise such information the default gateway or the access router can send information on cost and bandwidth. The mobile users could then have preferences for connections, like maximize bandwidth or minimize price and the host would select the appropriate interface satisfying these preferences.

This section of the chapter considered the below Algorithm for message notification of mobile node.

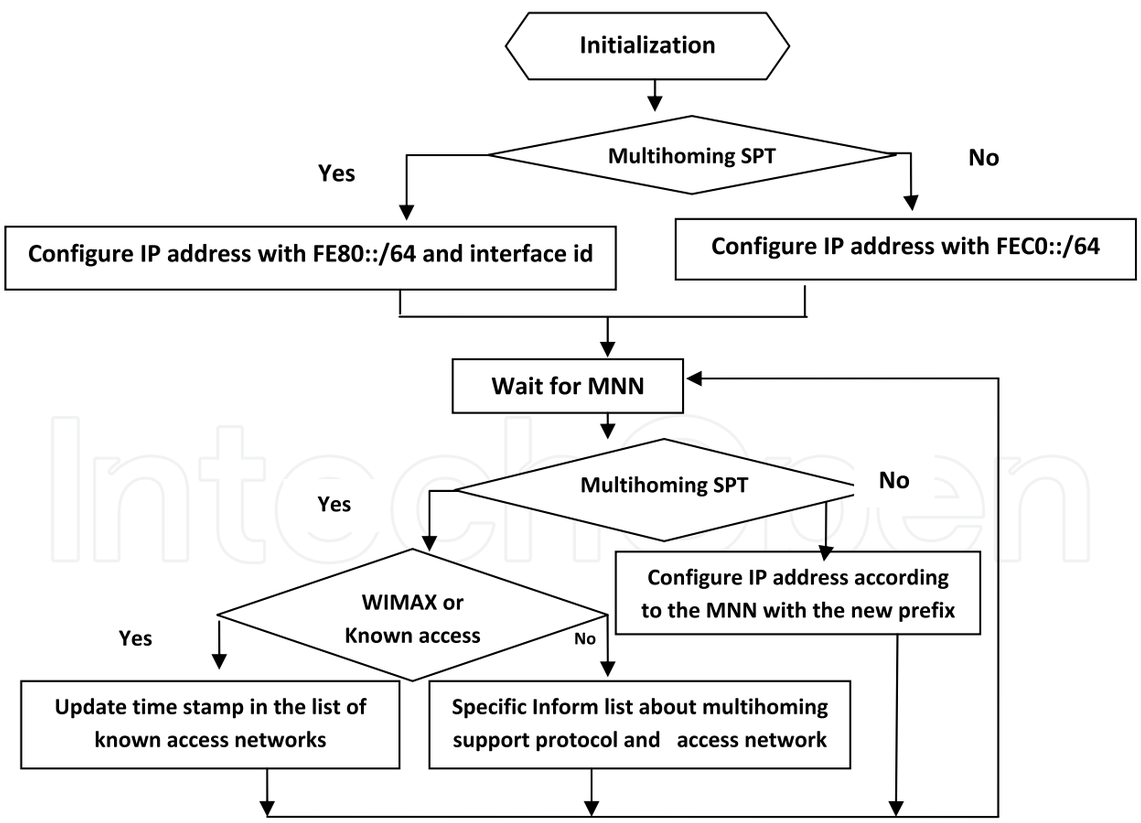

Fig. 4. Algorithm for mobility notification messages at a mobile node during optimization.

2.7 Mechanism for interface selection

The separation of policy and mechanism makes it possible to implement a dynamic interface selection system. The mechanism evaluates connection association and transport information against the actions in policies, using principles.The interface selection system is based on four basic components, ***entities, action, policy and mechanism***. ***Entities*** define actions. ***An entity*** may be a user, peer node or 3rd party, e.g., operator. Action is an operation that is defined by an entity and is controlled by the system. ***Actions*** specify the interfaces to be used for connections on account of entity's requirements. Actions can be presented as conditional statements. Policy governs the actions of an entity. Only one action can take place at a time in a policy. ***A policy*** set contains several policies possible defined by different entities. ***Mechanism*** evaluates actions against connection related information and decides which interface is to be used with a specific connection.

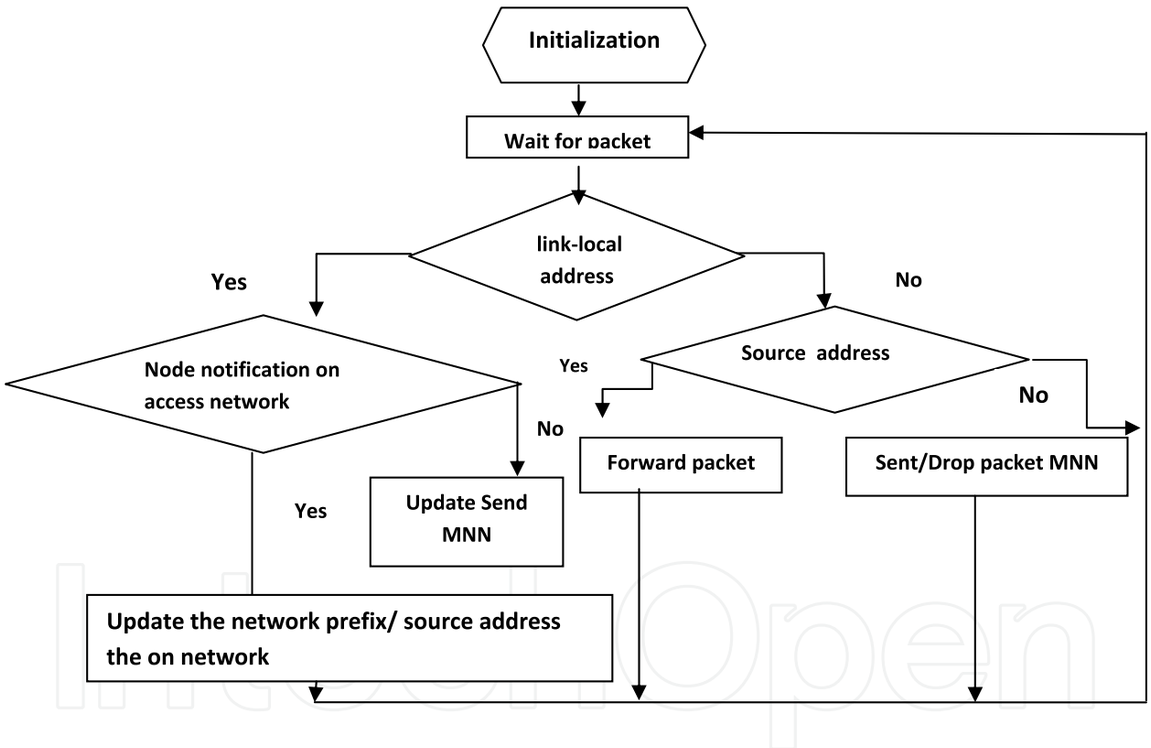

Fig. 5. Algorithm to optimizing the interface selection mechanism.

2.7.1 Network model and optimization

Network model topology to be optimized must contain futures that addressed parameter such as assurance of service delivery and security. Since Wimax is a Flexible Access Point System that delivers on the promise of personal broadband and rich service delivery. Paired with a converged IP core and communicating with feature-rich, multimodal devices combining one network, one service delivery platform and seamless experience that is

transparent to the end users. The below fig 6 consider the network model topology for optimization of IPv6 over wimax.

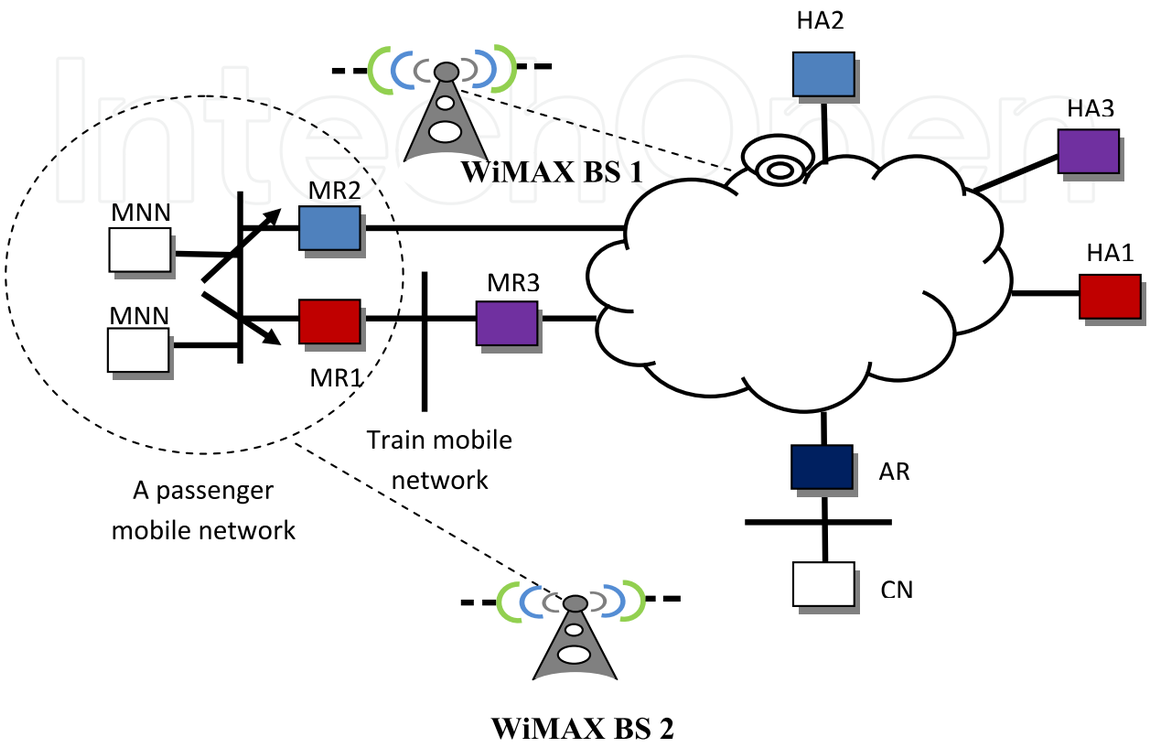

Fig. 6. Network Model Topology For Optimization of IPv6 over WIMAX

From the Network model the wimax BS1, wimax BS2,AR was coined from the architectural specification that depict the concept of Wimax deployment. The access Service Network (ASN) mainly was used for regrouping of BS and AR.The connectivity service Network (CSN) offers connectivity to the internet. To optimize using policy based routing protocol. The link layer information,IP layer information,Network originated information are initialized.

2.8 Standard for WiMAX architecture

WiMAX is a term coined to describe standard, interoperable implementations of IEEE 802.16 wireless networks, similar to the way the term Wi-Fi is used for interoperable implementations of the IEEE 802.11 Wireless LAN standard. However, WiMAX is very different from Wi-Fi in the way it works. The architecture defines how a WiMAX network connects with other networks, and a variety of other aspects of operating such a network, including address allocation, authentication. An overview of this specification for different architectures in order to deploy IPv6 over WiMAX is depicted below in Fig 7 by WiMAX forum .

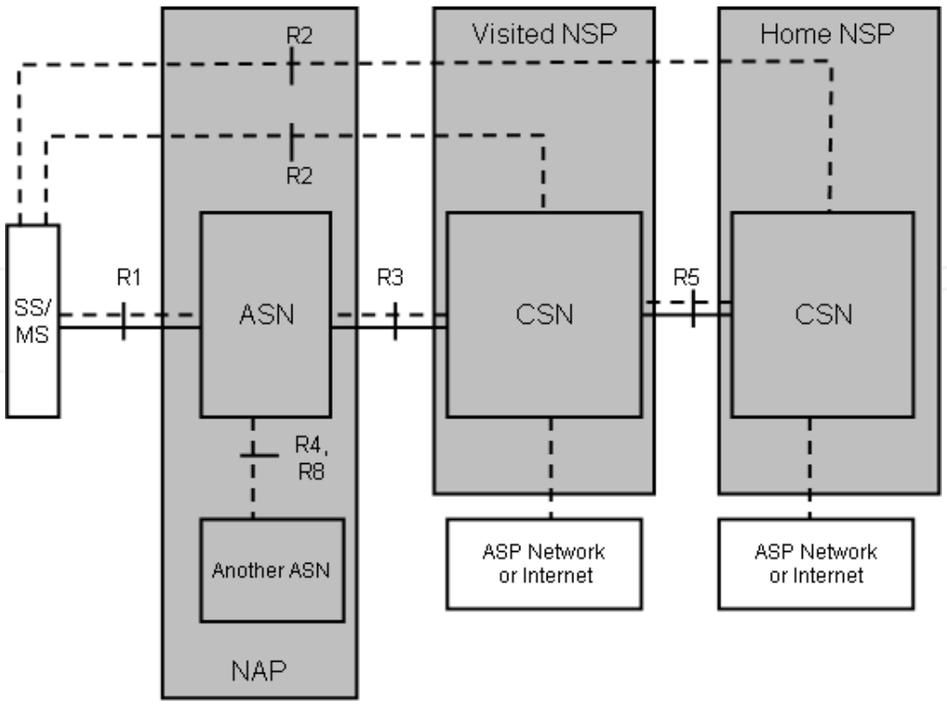

Fig. 7. Architectural Specification for Deployment of IPv6 over WiMAX.

In the proposed network model and optimization the reminder should note that : Regrouping of BS and AR into one entity is named the Access Service Network (ASN) for WiMAX. It has a complete set of functions such as AAA (Authentication, Authorization, Accounting), Mobile IP Foreign agent, Paging controller, and Location Register to provide radio access to a WiMAX Subscriber. The Connectivity Service Network (CSN) offers connectivity to the internet. In the ASN, the BS and AR (or ASN-Gateway) are connected by using either a Switch or Router. The ASN has to support Bridging between all its R1 interfaces and the interfaces towards the network side; forward all packets received from any R1 to a network side port and flood any packet received from a network side port destined for a MAC broadcast or multicast address to all its R1 interfaces. The SS are now considered as mobile (MS), the support for dormant mode is now critical and a necessary feature. Paging capability and optimizations are possible for paging an MS are neither enhanced nor handicapped by the link model itself. However, the multicast capability within a link may cause for an MS to wake up for an unwanted packet.

The solution can consist of filtering the multicast packets and delivering the packets to MS that are listening for particular multicast packets. To deploy IPv6 over IEEE 802.16, SS enters the networks and auto-configure its IPv6 address. In IEEE 802.16, when a SS enters the networks it gets three connection identifier (CID) connections to set-up its global configuration. The first CID is usually used for transferring short, sensitive MAC and radio link control messages, like those relating to the choice of the physical modulations. The second CID is more tolerant connection, it is considered as the primary management connection. With this connection, authentication and connection set-up messages are exchanged between SS and BS. Finally, the third CID is dedicated to the secondary management connection.

2.8.1 WiMAX security

WiMAX Security is a broad and complex subject most especially in wireless communication networks. The subject mechanism of Wimax Technology must meet the requirement design for security architecture in Wimax. Each layer handles different aspects of security, though in some cases, there may be redundant mechanisms. As a general principle of security, it is considered good to have more than one mechanism providing protection so that security is not compromised in case one of the mechanisms is broken. Security goals for wireless networks can be summarized as follows. Privacy or confidentiality is fundamental for secure communication, which provides resistance to interception and eavesdropping.

Message authentication provides integrity of the message and sender authentication, corresponding to the security attacks of message modification and impersonation. Anti-replay detects and disregards any message that is a replay of a previous message. Non-repudiation is against denial and fabrication. Access control prevents unauthorized access. Availability ensures that the resources or communications are not prevented from access by DoS attack. The 802.16 standard specifies a security sub layer at the bottom of the MAC layer. This security sub layer provides SS with privacy and protects BS from service hijacking. There are two component protocols in the security sub layer: an encapsulation protocol for encrypting packet data across the fixed BWA, and a Privacy and Key Management Protocol (PKM) providing the secure distribution of keying data from BS to SS as well as enabling BS to enforce conditional access to network services. The model below was adapted based on security in wimax. This chapter is still investigating the protocol in the sub layer that can mitigate encapsulation of packet data.

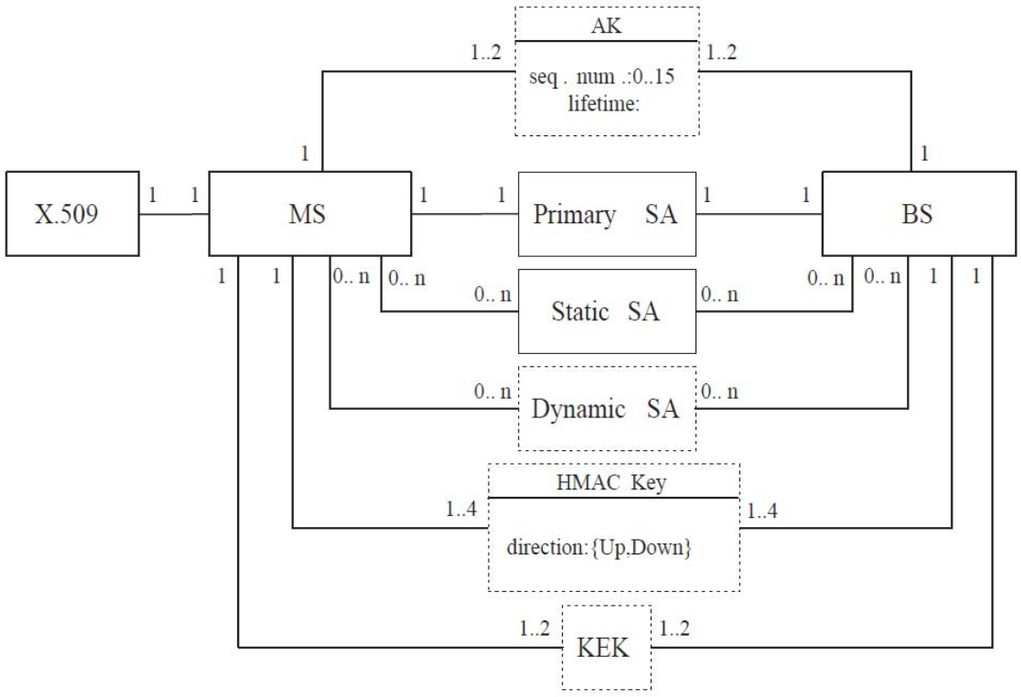

Fig. 8. Security model

2.8.2 Authentication in WiMAX

Basically in WIMAX/802.16 there are three options for authentication: device list based, X.509 based or EAP-based. If device list-based authentication is used only, then the likelihood of a BS or MA masquerading attack is likely. Impact can be high. The risk is therefore high and there is a need for countermeasures. If X.509-based authentication is used, the likelihood for a user (a MS) to be the victim of BS masquerading is possible because of the asymmetry of the mechanism.

There are specific techniques that identify theft and BS attack. Identity theft consists of reprogramming a device with the hardware address of another device. This is a well know problem in unlicensed services such as WiFi/802.11, but in cellular networks because it had been made illegal and more difficult to execute with subscriber ID module (SIM) cards. The exact method of attack depends on the type of networks.

The proposed policy based routing protocol for optimization evaluates connection association and transport information against the actions in policies, using the following principles:

- The mechanism must allow dynamic management of policies such as add, update and remove operations.
- The evaluation of policies should always result in exactly one interface for any traffic flow or connection. This is reached by having a priority order for actions.
- All attribute-value pairs in an action must match for a traffic flow or connection for the action to take place.
- The mechanism selects an interface based on the priority order of interfaces in an action.
- The mechanism uses default actions which match to all flows and connections if no other matching action is found. The mechanism should support distributed policy management and allow explicit definition of priorities. The below table consider our model for optimization during Authentication of WIMAX/802.16.

Threat	DoS on BS or MS
Kind	Mechanism
Device	Device List : RSA / X.509 Certificate
User Level	EAP + EAP – TLS (X.509) or EAP – SIM (subscriber ID module)
Data Traffic	AES-CCM CBC-MAC
Physical Layer Header	None
MAC Layer Header	None
Management messages	SHA – 1 Based MAC AES Based MAC

Table 2. Authentication in WIMAX 802.16

The intended proposed concept is to mitigate and prevent Dos on the BS or MS by introducing **Policy Repository.** In a WiMax/802.16 network, it is more difficult to do these because of the time division multiple access model. The attacker must transmit while the

legitimate BS is transmitting. The signal of the attacker, however, must arrive at the targeted receiver MS(s) with more strength and must put the signal of the legitimate BS in the background, relatively speaking. Again, the attacker has to capture the identity of a legitimate BS and to build a message using that identity. The attacker has to wait until a time slot allocated to the legitimate BS starts. The attacker must transmit while achieving a receive signal strength. The receiver MSs reduce their gain and decode the signal of the attacker instead of the one from the legitimate BS.

2.8.3 Key management in Wimax for 5G technology

5G technology has a bright future because it can handle best technologies. The primary concern that should be focused on in 5G is the automated and optimization capability to support software. Although the issue of handover is being address since the Router and switches in this Network has high connectivity capability. Security is under studied in this regard. The knowledge base for the key management for 5G technology centered on physical layer, privacy sub layer threat, mutual Authentication, Threat of identity theft, water Torture and Black hat threat in wimax technology. The protocol used is not rolled out because some flexible framework created by the IETF (RFC 3748), allows arbitrary and complicated **authentication protocols** to be exchanged between the supplicant and the authentication server. **Extensible Authentication Protocol** (**EAP**) is a simple encapsulation that can run over not only PPP but also any link, including the WiMAX link. A number of **Extensible Authentication Protocol** (**EAP**) methods have already been defined to support authentication, using a variety of credentials, such as passwords, certificates, tokens, and smart cards. For example, **Protected Extensible Authentication Protocol** (**PEAP**) defines a password- based EAP method, EAP-transport-layer security (EAP-TLS) defines a certificate-based **Extensible Authentication Protocol** (**EAP**) method, and EAP-SIM (subscriber identity module) defines a SIM card–based EAP method. EAP-TLS provides strong mutual authentication, since it relies on certificates on both the network and the subscriber terminal.(Chong li).

3. Conclusion

Considering the complex issues and areas that have been addressed in this book chapter. The main focus of the chapter is how to provide techniques on automation and optimization using Algorithm based on policy based routing protocol. However, the various issues on this subject matter have been addressed. Analysis of micro mobility via Macro mobility based on comparative investigation and requirement was advanced. Furthermore the key optimization and data communication of IPv6 over wimax deployment must consider: *session preservation and interface selection mechanism*. The account of policy based routing protocol must provide: *link layer information, IP layer information and network originated information.* Our network model topology for optimization evaluates connection association and transport information against the actions in the policies using the aforementioned Algorithm. The remainder of this report should note that there are limitations in wimax deployment such as: low bit rate, speed of connectivity and sharing of bandwidth.

Finally, the chapter provides the basic Algorithm for optimization of IPv6 over wimax deployment using policy based routing protocol.

4. References

[1] Mobile IPv6 Fast Handovers over IEEE 802.16e Networks H. Jang, J. Jee, Y. Han, S. Park, J. Cha, June 2008
[2] IPv6 Deployment Scenarios in 802.16 Networks M-K. Shin, Ed., Y-H. Han, S-E. Kim, D. Premec, May 2008.
[3] Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks B. Patil, F. Xia, B. Sarikaya, JH. Choi, S. Madanapalli, February 2008.
[4] Mobility Support in IPv6 D. Johnson, C. Perkins, J. Arkko,RFC 3775. June 2004.
[5] Analysis of IPv6 Link Models for 802.16 Based Networks S. Madanapalli, Ed. ,August 2007.
[6] Threats Relating to IPv6 Multihoming Solutions E. Nordmark, T. Li, October 2005.
[7] Koodli, "Fast Handovers for Mobile IPv6", IETF RFC- 4068, July 2005.

IntechOpen