International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 2, February- 2013

Fast and Secure Inter-ASN Handovers in Mobile Wimax Networks in Car GPS

N. Stalin M.Sc.,CT.,(ME.,CSE), Mr. S. Sathish, M.E., MISTE(Ph.D)[A], Mr. K. Sathaseelan.,M.Tech [B]
[A] HOD,Department of Electronic & Communication, Mahendra Institute of Engineering &Technology
[B] HOD,Department of Computer Science & Engineering Mahendra Institute of Engineering &Technology

***Abstract*— Mobile WiMAX is an expectation from mobile users to give secured and seamless services. EAP with Enhanced Extensible Authentication Protocol based pre-authentication (EEP) method to overcome the vulnerability of the above-mentioned scheme with much fewer requirements on the computation and communication resources. Mobile WiMAX system supports give up processes to create a mobile station find another base station from the same or different access service network to establish connection when moving out of coverage of the present serving base station. Long delay in the time-consuming verification procedure is a well-known bottleneck of handover scheme, causing service disturbance when a mobile user moves between base stations.**

***Index Terms*— Mobile WiMAX, formal verification, security,handover, pre-authentication.**

I. INTRODUCTION

Over the past ten years mobile communications have transitioned from a luxury item to a utility as critical as electricity and water. With this rapid expansion of subscribers and services, the operators of the wireless networks are making money today and adding subscribers at rapid rates. India for example has growth between 20% and 30% year over year growth in mobile subscribers.

However, this very success carries the seeds of potential crisis as these subscribers begin expecting, demanding and consuming ever-increasing amounts of data over these same networks. 3G networks-from the RAN architecture to the synchronous transport-were designed primarily to support increased voice capacity with a modicum of data support. They were never intended to support the multiple terabytes being transported today. HSPA and HSPA+, while definitely providing enhancements, are still bound by the 3G architecture and can be considered mere Band-Aids as opposed to long term solutions.

At this time there is little controversy over the fact LTE (Long Term Evolution) will become the dominant global 4G wireless technology over the next ten years. The only real issue at this point is when most carriers will opt to migrate to LTE and how long HSPA+ and CDMA EVDO Rev A will delay LTE deployments.

Many areas within these regions are also severely lacking in broadband infrastructure due to the same lack of spending power among the potential subscriber audience. This is changing however due to government efforts, falling prices on broadband access and cheaper access devices, such as the ultra-low-cost PC.

The wireless industry made it clear over the last year or so that 4G technology is a short-term necessity in mature markets, and the long-term answer to broadband connectivity worldwide. In mature markets, consumers are beginning to find ubiquitous access to medium or higher-rate broadband a necessary part of their communications capabilities.

In developing markets, wireless will continue to be the only affordable way to deliver broadband and governments will foster those services to promote economic growth. Thus, it is clear that the experience with voice services over the last two decades-in which it overtook and caused the decline of wire line-will repeat itself with broadband. That is, wireless will become the dominant method to deliver broadband services to users. This process may take a while, but it will happen.

When a MS handovers from one BS to another in different ASNs, which is referred as an inter-ASN handover, the MS will perform a full EAP authentication with the AS and Security Association's traffic encryption key (SA- TEK) 3-way handshake with the BS to distribute the TEK. The handover process should be fast to maintain a seamless service connection. However, an EAP-based authentication has been well known to be costly due to its time-consuming public key cryptography operations and the delay of several round-trips between the MS and the AS. A full EAP authentication takes about 1000ms, while the recommended maximum handover latency for streaming applications is only 150 ms [3].

In order to reduce the handover latency, mobile WiMAX supports handover optimization, allowing users to reduce handover latency by reusing key materials from previous authentication [1]. However, it creates critical security holes such as a lack of valid entity authentication

leading to Man- in-the-Middle (MITM) attacks. Alternative solutions in [4]- [9] have focused on reducing the delay incurred in the EAP authentication, which is the majority of the handover latency, without compromising security requirements. The current proposed techniques mainly fall into two categories, namely the re-authentication and the pre-authentication.

Re-authentication can avoid a full EAP-based authentication in handover by reusing the information exchanged between the MS and the AS in the previous authentication. In [4], the HOKEY working group has proposed the EAP re-authentication protocol (ERP) which allows a MS and the AS to use the extended master session key (EMSK) from previous EAP authentication for master session key (MSK) derivation. Thus, instead of carrying out a full EAP authentication, the MS and the AS will only need a single round trip to exchange the ERP messages. In [5], a re-authentication scheme has been proposed that can be applied for handover between heterogeneous networks. The protocol makes use of an encrypted credential, which is given to a MS as a proof of its past honest behaviors and should be presented to the tBS for the handover. The main idea is to let the MS to have instant access to the network through a weak but fast authentication first followed by a stronger and more costly authentication. Base on the similar idea, the proposal in [6] has used the truncated 192 bits of the MSK in the subsequent EAP authentication as a temporary authentication root key for an inter-ASN handover. By reducing the number of messages exchanged and simplifying the cryptographic operations, re-authentication techniques can lower the authentication signaling latency.

By pre-authentication techniques in [7]-[9], a MS and the AS pre-compute the shared secret keys before a handover.

Thus, the handover delay could be effectively reduced to the same amount of the time used by a 3-way handshake, resulting in the shortest authentication signaling delay. The main advantage of the pre-authentication is that the cryptographic material will not be reused, hence it becomes more secure. The HOKEY working group has proposed an EAP- based pre-authentication model in [7] which has been adapted to Mobile IPv6 network in [8] and is called Handover Early Authentication (HOEA) protocol. HOEA utilizes proactive signaling to discover candidate access network where the MS potentially moves to and performs a full EAP authentication before it attaches to the candidate network. However, it only works when the link layer supports proactive signaling and there is a possibility that the handover has already started before the pre-authentication phase has completed, resulting in a failed pre-authentication. An EAP-based pre-authentication scheme (EPA) has been proposed to reduce the authentication delay in inter-ASN handovers [9]. By the EPA scheme, a MS exchanges the key materials with different neighbor ASN- GWs (nASNs) of the serving ASN-GW, home ASN-GW or hASN, so that when it handovers to one of those nASN- GWs, instead of performing a full EAP authentication, it can proceed directly with the 3-way handshake. The EPA has some advantages over the HOEA. Proactive signaling is not required in order to use EPA. Besides, the pre-authentication with the nASN-GWs is done right after the MS attaches to the current hASN-GW. As a result, the possibility that the pre-authentication completes before the handover is much higher compared to that by the HOEA. However, the EPA is vulnerable to DoS attacks and replay attacks, which greatly degrades its security level. Another drawback is the wastage of unnecessary effort for key exchange between the MS and those nASN-GWs that the MS never roams to. The HOEA also faces the same problem since proactive signaling can only be provided to the possible candidate networks. In this paper, in order to enhance the security functionality and the efficiency of the EPA, as our major contribution, we propose an Enhanced EAP-based, or specifically, the EAP-Transport Layer Security (EAP-TLS) based pre-authentication (EEP) scheme which can prevent DoS and replay attacks with much less computational and communication resources and at the same time, can overcome the abovementioned drawbacks incurred in the EPA and the HOEA schemes.

II. SYSTEM BACKGROUND

A. WiMAX Network Model

The IEEE 802.16e-2005 standard provides the air interface for WiMAX but does not define the full end-to-end WiMAX network. The WiMAX Forum's Network Working Group (NWG), is responsible for developing the end-to-end network requirements, architecture, and protocols for WiMAX, using IEEE 802.16e-2005 as the air interface. The WiMAX NWG has developed a network reference model to serve as an architecture framework for WiMAX deployments and to ensure interoperability among various WiMAX equipment and operators. The network reference model envisions unified network architecture for supporting fixed, nomadic, and mobile deployments and is based on an IP service model. Below is simplified illustration of IP-based WiMAX network architecture.

The overall network may be logically divided into three parts:

a. Mobile Stations (MS) used by the end user to access the network.
b. The access service network (ASN), which comprises one or more base stations and one or more ASN gateways that form the radio access network at the edge.

c. Connectivity service network (CSN), which provides IP connectivity and all the IP core network functions.

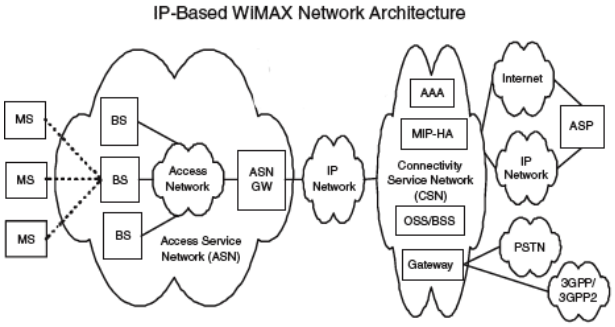


Figure 1

B. ITS (Intelligent Transportation System)

Telematics is called ITS for short. Transport use the Internet is the trend of development of mobility communication in the future. The current development of ITS main objective is to combine the communications technology provided by industry. It has become the country's main transport system in the development of logistics. Car connected to internet to construct the Ubiquitous computing will be most popular of information communication and business in the future.

C. GPS (Global Positioning System)

GPS is the most popular positioning system technology, developed by the U.S. Department of Defense. In the past, GPS only was used in some high-tech areas, for example: for military, aviation or maritime, it's for public usage now. The "car navigation systems" now is an example of practical application. GPS is constructed from 24 satellites, including three preparatory satellites .The overall operation of the satellite positioning system can be divided into three parts: Space Segment, Control Segment and User Segment. It uses the simultaneous signal with the satellite and its relationship between relative positions to detect the exact location.

In fact, there has been a combination of GPS and handoff of wireless networks design proposed in the literature, it mainly integrates 802.11 wireless networks, Mobile IP and GPS systems constitute the entire structure of the environment, but simply through the GPS to locate the current location of MS, to choose an AP database from all APs around current position. Then, by telling MN of Mobile IP that it can use the database as a handoff list, but it does not have the designated base stations to process the handoff. Overall, this is a network environment architecture which is decided by end users to make handoff.

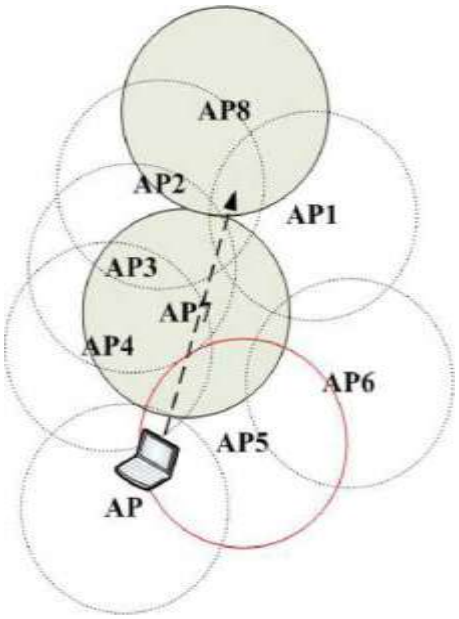
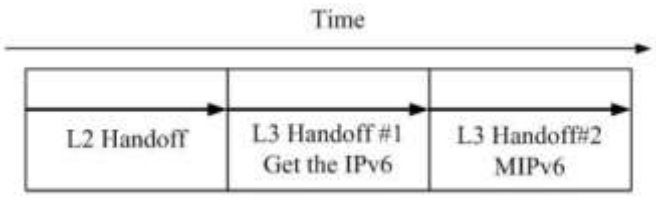


Figure 2. GPS combine with 802.11

D. Handoff Procedure

Handoff is disconnected from the connection to stop receiving the packet from Correspond Node, until MN move to a new subnet and received the packet from Corresponding Node again. For Wireless internet handoff, its main purpose is providing the handoff of Layer 3, IP layer, but besides the Layer 3, the Layer 2 is also included in the overall handoff of total time. When MN (Mobile User) left the scope of Serving BS (Serving Base Station), in order to avoid any disruption in service, it would search the available a Target BS (Target Base Station) which can handoff. MN will set a Neighbor BS Scanning RSSI value (Here's a example by 802.16e's MS), once Serving BS signal strength below this value, it will start this process to find the base station, MN according to the channel from backbone or it own allow list to scan and measure the signal strength, once the Serving BS value lower than the Handover RSS Target value, it will start handoff procedures, disconnect the original connection, and connect to the base station it scanned, waiting for receive or request a new network Prefix. To form IPv6 address according to automatically formed address and deliver exchange message to HA for register and complete the overall handoff process. Figure 2 is handoff architecture. L2 Handoff contains the scan channels and choices BS, L3#1 includes the getting a new IP of new network and verification IP, L3#2 is the message of handoff.



III. *INTELLIGENT MOBILE NETWORK HANDOFF MECHANISM*

In this section we will explain our system and how to provide services, explains how Telematics indicative handoff without modifying the 802.16e standard through MOB_NBR-ADV.

A. Through MOB_NBR-ADV control Telematics handoff

L2 handoff mechanism includes three steps:

1. Discovery
2. Re-association
3. Re-authentication

Whether a handoff decision will be made is based on the Discovery, and Discovery is used for scanning BS for handoff. The convention handoff mechanism is based on strength of signal which is getting high enough to threshold for determining to begin handoff. The protocol of WiMAX add a mechanism that back-end network provides BS information around itself (MOB_NBR-ADV includes BS information which can be linked) coordinate scanning, search base station. MOB_NBR-ADV is sent by our system which one includes only one indicative BS to handoff.

MS is moving between two BS, it will be affect by them. However, when the signal strength fluctuates within the default level value of handover, it would create the mechanism for starting handoff, resulting in constant change Hand, this situation known as the Ping-Pong-Effect. How to choose BS is the question we want to explain here.

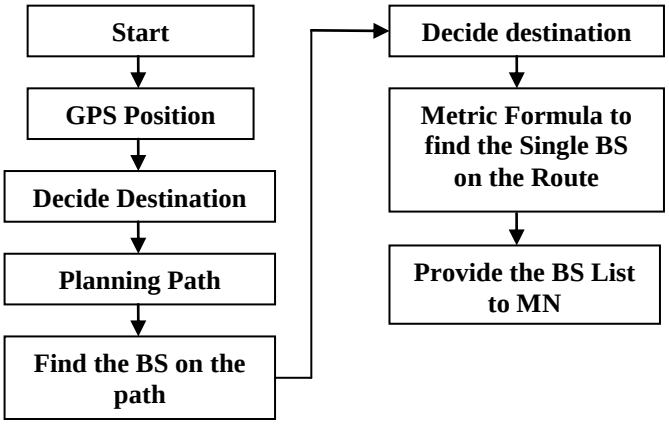


Figure 3. Flowchart of WiMAX combines GPS

First GPS will use Triangulation Method to find the current location and label the values of longitude and latitude. After user deciding the destination, user should point the destination clearly in GPS. Map software using own algorithms calculate the path between source and destination. Map Software will deliver path information to Serving BS through network and deliver to Handoff Management Server which in ASN. According to this information, HMS will calculate the amount of BS which affected the coordinative value respectively

In Figure 4

, After HMS has calculated completely, it will deliver BS-indication message to Serving BS through ASN, and forward the user using GPS. Next step, user wills handoff BS chosen which is indicated. Once user arrived at the location which needs handoff, user will scan and process handoff according to the indicated BS frequency. Finally, we can find that the method we introduced does not modify the standard.

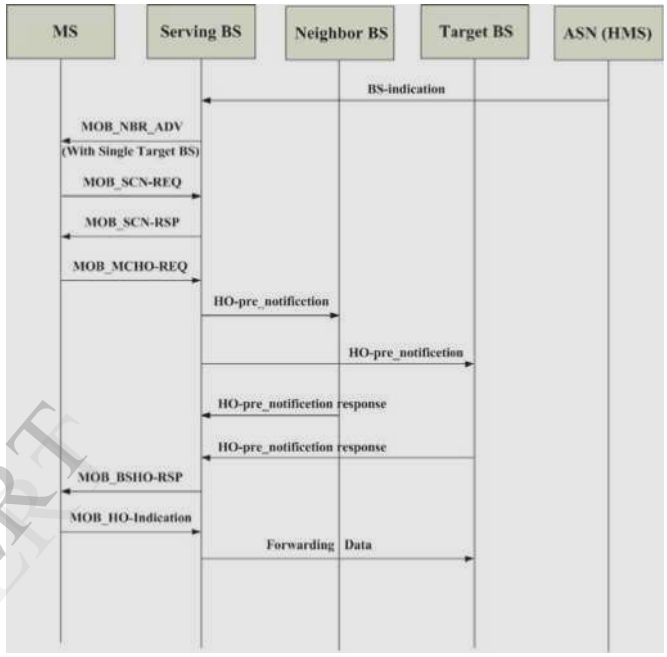


Figure 4:

IV. REVIEW OF THE WIMAX NETWORK

A. WiMAX Network Configure Setting

WiMAX network used to create the no of nodes. The packets to send and receiving through the source to destination. It's based the scheme of packets delivered for ACK packet drop on the nodes. In this network to creating the source and destination node of the network and transmit the data to processing on their whole networking.

B. Topology Design

This module is developed to Topology design all node place particular distance. Without using any cables then fully wireless equipment based transmission and received packet data. Node and wireless between calculate sending and receiving packets. The sink is at the center of the circular sensing area. Intermediate the sender and receiver of this networking performance on this topology.

C. Node Creating

This module is developed to node creation and more than 10 nodes placed particular distance. Wireless node placed intermediate area. Each node knows its location relative to the sink. The access point has to receive transmit packets then send acknowledge to transmitter.

D. Dos Attacks

The neighbor list message sent by the access service network to a mobile station without a freshness indication and a proof of the origin, it can produce a security hole for a DoS attack. The lack of the message authentication allows an adversary to forge its own neighbor list message and send it to the mobile station, claiming that it is sent by the access service network.

E. Replay Attacks

Pre-authentication process, an adversary can eavesdrop the pre authentication request message and retransmit it later, pretending to be a legitimate MS. Since the message does not have a freshness indicator, they will consider it as a new request message, verify its signature and relay it to the network.

F. EAP Framework And Authentication

EAP- Transport Layer Security based authentication can provide strong mutual authentication it has been selected by the WiMAX forum as one of the options for the specification of the authentication procedure between the mobile station and the authentication server. The EAP authentication is executed between a mobile station and the base station in the key management system.

G. Pre-Authentication Latency

The pre-authentication latency consists of the delay of computing process and the transmission and propagation delays of the total messages. To evaluate the delay of computing process, which is the time used for the cryptographic operations. The processing powers of the base station, the access service networks as well as the authentication server are the same.

H. Graph Design Based Result

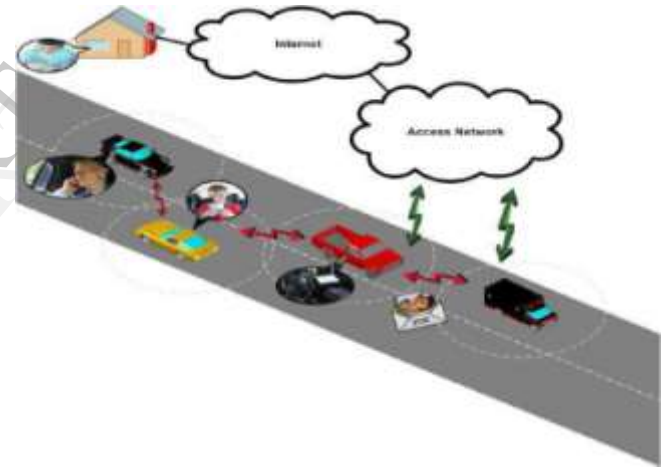
Graph is an essential part of display a result, so we plot a graph to show a various result comparison with packets, throughput, energy efficient and etc.

V. WORKING OF WiMAX combine GPS with EAP

GPS permits users to obtain real-time location information. However, expanded communications among vehicles and with roadside infrastructure can substantially expand services drivers currently enjoy in the areas of traffic flow, safety, information (Internet), communications (VoIP) and comfort applications, among others [2].According to Sichitiu et al. applications for vehicular communications include the following:

a. Proactive safety applications: geared primarily to improve driver reaction and decision making to avoid possible accidents (e.g. broadcast warnings from a vehicle that has ignored red stop light) or minimize the impacts of an imminent crash (automated braking systems).
b. Traffic management applications: mainly implemented to improve traffic flow and reduce travel time, which is particularly useful for emergency vehicles.
c. Traffic coordination and traffic assistance: principally concerned with improving the distribution and flow of vehicles by helping drivers pass, change lanes, merge and form columns of vehicles that maintain constant relative speeds and distances (platooning).
d. Traveler Information Support: mainly focused on providing specific information about available resources and assistance persons require, making their traveling experience less stressful and more efficient.
e. Comfort Applications: primarily designed to improve the travel experience of the passengers and the driver (e.g. gaming, internet, automatic tolls, etc.)

Figure 5 shows some potential applications.



In order to provide greater passenger safety, convenience and comfort, protocols and equipment must provide more timely and reliable data transfer between network nodes for them to effectively share vital information. In the case of WiMAX, network nodes must efficiently transmit and receive data in a instantaneously changing network environment, characterized by the constant entry and exit of nodes. In addition, mobile nodes must handle handoffs between different clusters, all while functioning within very strict technical parameters regarding packet loss, delay, latency, and throughput, among others.

Sichitiu and Kihl in [3] construct a taxonomy based on the way nodes exchange data. Their work involves two forms of vehicular communication: vehicle to vehicle (IVC) and vehicle to roadside (RVC). IVC can employ either a one hop (SICV) or

multi-hop (MIVC) strategy. On the other hand, RVC can be ubiquitous (URVC) or scarce (SRVC). Figure 2 schematizes these authors' taxonomy [3]. The following three figures explain this taxonomy and provide examples of IVC, RVC and HVC.

Communications within VANETs can be either inter-vehicular or vehicle to roadside and each type of communication imposes its specific requirements. For example, highway collision warning systems can more easily be implemented using multi-hop communications between vehicles (without infrastructure). On the other hand, traveller information requires fixed infrastructure to provide connectivity between the vehicles and an information center. IVC deployment is significantly less expensive than RVC because it is infrastructure less. This kind of architecture allows vehicles to send information between each other via multi-hop communication, even with vehicles that are beyond their immediate radio coverage area. IVC internet access is much more complicated than with RVC.

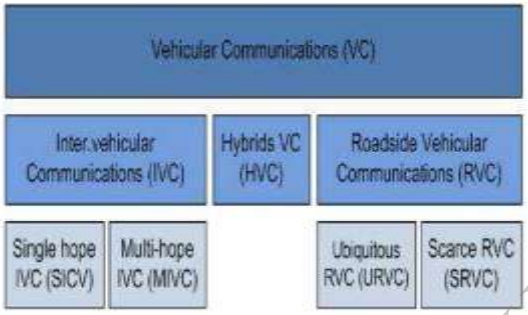


Fig. 6. Vehicular communications Taxonomy

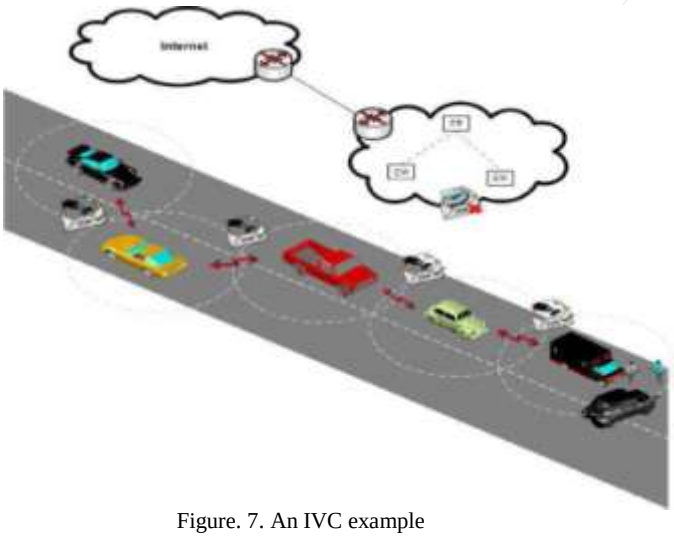


Figure. 7. An IVC example

As a result, IVC can only provide a reduced number of applications. However, IVC is better suited for safety applications because the vehicles can almost immediately detect collision or congestion warning that is transmitted within the affected area. Figure 7 provides an example of inter vehicular communication, where a vehicle approaching an accident detects the crash and informs the vehicles behind it that it is about to brake suddenly. This forewarning could help avoid other accidents caused by drivers who cannot apply their brakes opportunely and allows vehicles further behind to change lanes to lessen traffic congestion.

RVC can offer a wider range of applications because of its more stable and robust access to the Internet, which allows ready availability of information about specific places and the services they provide. RVC, however, has two important drawbacks when considered for safety applications:

- ✓ The cost of deployment of base stations (BS) makes it difficult to provide full coverage for so many vehicles over such a large area as vehicles leaving the BS coverage area lose connectivity.
- ✓ The delay caused by sending packets through a base station can prove disastrous in time sensitive safety applications.

Different technologies have been tested to enable RVC, including cellular, WiFi (IEEE 802.11p) and WiMAX (IEEE 802.16e), but no standard has been established as of yet. Presently, authors believe that WiMAX best fits VCN requirements because of its high bandwidth, robust medium access control (MAC), versatility (i.e. wide range of compatible standards) and QoS support. Importantly, it meets the already existing standard for mobile nodes (IEEE 802.16e). Figure 4 illustrates examples of some RVC applications, which include broadcasting the location of specific businesses and providing information about goods and services offered by them.

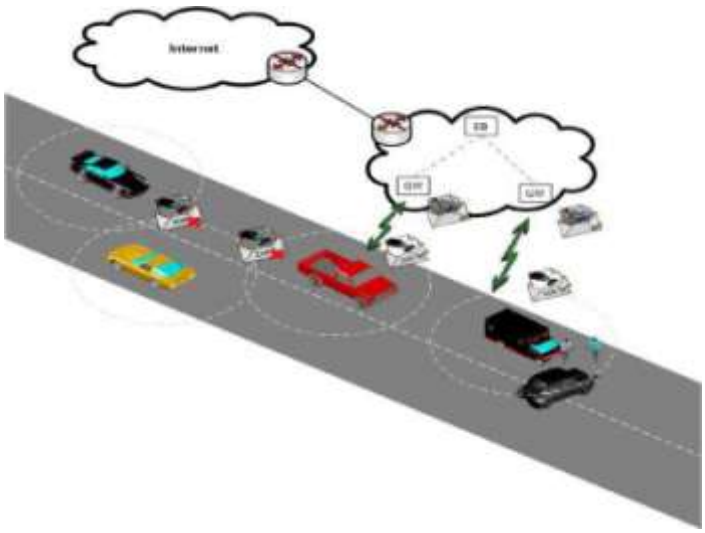


Fig. 8. A RVC network example

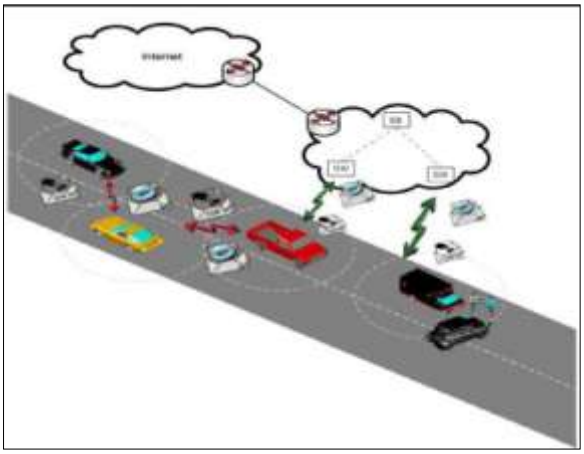


Fig. 9. A mixture of IVC and RVC (HVC)

Both IVC and RVC have desirable benefits; while with IVC users can form groups practically anywhere, with RVC persons can have access to internet and extend the vehicular applications. Importantly, combining both of these architectures into a hybrid vehicular communications (HVC) network can maximize benefits. HVC, however, is more complex in various aspects: HVC need more complex routing protocols, a robust physical layer and a medium access layer that is sufficiently dynamic to fully exploit the short duration of links and organized enough to minimize interference.
Figure 9 illustrates a hybrid vehicular communication network where vehicles inside the coverage area of a RVC can act as gateways for vehicles outside the coverage area. HVC networks are very desirables because they can provide virtually any kind of service. Importantly, however, as previously mentioned, research must first overcome many technical challenges before HVC networks can be implemented in real-world applications. This is primarily because of the incompatibility of technologies (e.g. WiFi was developed for WLANs, while cellular communications were designed for WANs).

As previously mentioned, each type of vehicular communications (IVC, RVC or HVC) has different technological requirements, although they all must meet several common demands inherent in VCN (see Table 1 and Figure 6). Three of these network requirements include [4]:

- radio transceiver technology that provides omni-directional coverage
- rapid vehicle-to-vehicle communications to keep track of dynamic topology changes
- highly efficient routing algorithms that fully exploit network bandwidth

Fig. 10. Types of scenarios for VCN

	Rural	Urban	City	Highway
Speed	Low	Medium/ High	Low/Very Low	Very high
Vehicles Density	Low	Medium	Very high	Med/Low
Interference	Low	Medium	Very high	Low
Infrastructure	Low	Medium	Very high	Med/Low

Table 1. Features of Vehicular Scenarios

Numerous researchers have worked to overcome issues related to vehicular communications (e.g. [5-9, 10-12]). In 2004, the IEEE group created the IEEE 802.11p (wireless access in vehicular environments-WAVE) task force [13]. The workforce established a new standard that essentially employs the same PHY layer of the IEEE 802.11a standard, but uses a 10 MHz channel bandwidth instead of the 20 MHz used in IEEE 802.11a. With respect to the MAC layer, WAVE is based on a contention method (i.e. CSMA/CA), similar to other standards in this group.

The MAC layer in IEEE 802.11p has several significant drawbacks. For example, in vehicular scenarios, WAVE drops over 53% of packets sent according to simulation results [14].

✓ State of the art of WiMAX in multi-hop vehicular communication networks

The authors in propose a routing protocol called Coordinated External Peer Communications (CEPEC), whose cross-layer protocol is designed for multi-hop vehicular networks. They obtained their simulation results using a proprietary development tool which guaranteed all vehicles fair access to the Internet, even over nodes that were several hops distant from the BS. Their proposal includes organize the OSI model into three layers: PHY, MAC and Network. However, the authors do not specify the modifications they made to the IEEE 802.16-2004 standard that permitted the increased mobility and quicker registration of the MS. The authors employ TDMA to assign channels, exploiting TDMA's centralized scheduler and time division duplexing.

Finally, and very importantly, CEPEC needs to determine the geographic position of every vehicle. To do this, all vehicles must be equipped with GPS.

An important disadvantage of CEPEC is that it only allows data communication from vehicles to the BS and vice versa; therefore, it does not provide for vehicle-to-vehicle data exchange. Additionally, CEPEC's centralized scheduling mechanism reduces its scalability. Since, as previously mentioned, the authors of [11] do not specify the changes they made to the IEEE 802.16 standard, we must assume that vehicles enter the network according to standard specifications for nodes in mesh mode. Of course, this implies that network performance suffers significant deterioration. Also, the authors fail to detail the modifications they made to the standard that permitted increased mobility and topology control.

Figure 11 shows the segment configuration of a CEPEC simulation in which the green vehicles are segment subscriber stations (SSSs) and the red ones are segment heads (SH).

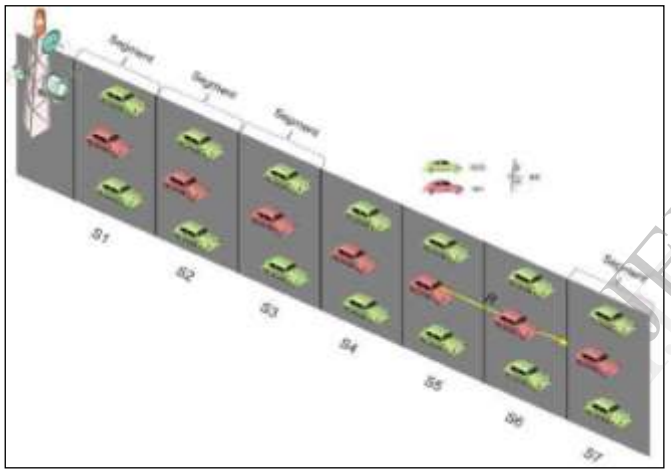


Fig. 11. CEPEC Topology

The authors in [12] do not provide simulation or test bed results and limit their work to making suggestions at a conceptual level about how to apply a hierarchical topology using WiFi hotspots (i.e. IEEE 802.11p) as access points for vehicles and WiMAX mesh stations as access points for WiFi hotspots. One major issue concerning this topology is that the IEEE 802.11p standard does not support QoS and the MAC contention-based method represents a significant disadvantage.

The topology in [12] is comprised of a point of access (PoA) consisting of a WiMAX mesh point (MP) and at least one access point (AP). The clusters are formed by several PoAs, one of which serves as a cluster head (CH) and domain, which is formed by a group of clusters. Figure 8 schematizes the described topology.

The authors in [13] propose a handoff mechanism called SWIFT, which includes modification in the MAC and network layers.

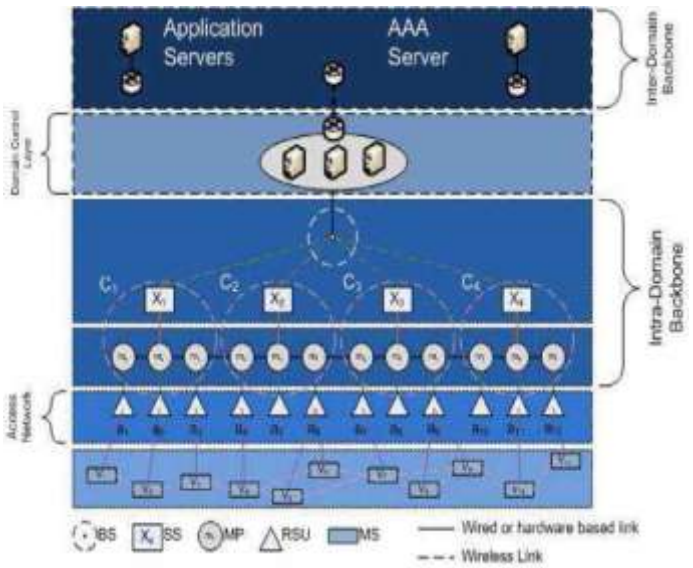


Fig. 12. Conceptual Architecture

The objective of the architecture is to provide high speed internet access in trains with a soft handoff, and having a minimum of connectivity interruptions. This proposal consists of a three layer topology: Level 0 is an access point functioning under the IEEE 802.11e standard; Level 1 uses base stations (BS) that work in conjunction with the IEEE 802.16m standard and Level 2 enables an optical backbone to interconnect with base stations located alongside the train tracks. Each train possesses two gateway interfaces that serve both as WLAN access points (i.e. IEEE 802.11e) and IEEE 802.16m subscriber stations. Results obtained using the popular NS-2 simulator show that the handoff latency of SWiFT is 52% less than with ipV6 mobile.

The SWiFT protocol can be seen as having a vehicle-to-roadside architecture where, as in

[12] , there is no possibility of inter-vehicular communications to cause a reduction in network services. Figure 12 shows the architecture of the SWiFT proposal.

In [24], the authors develop a handoff mechanism with a hybrid architecture using the IEEE 802.16e and IEEE 802.16j standards, which also includes control information of the vehicles via V2V. In this handoff mechanism, vehicles leaving their relay vehicle coverage area, called oncoming small size vehicles-OSV, directly transmit the information maintained in layers 2 and 3 to the vehicles outside the coverage area (called broken vehicles) of the relay vehicle. The information passed from OSV to

BV is necessary to synchronize communications between the oncoming vehicle and the network.

The NS-2 simulator tool was used in this work and results show that the handoff mechanism developed helped reduce the handoff latency between relay vehicles. Figure 14 shows the topology described in [14] where the relay vehicles, in this case public buses, are equipped with IEEE 802.16j, which is used to register the buses at a base station that

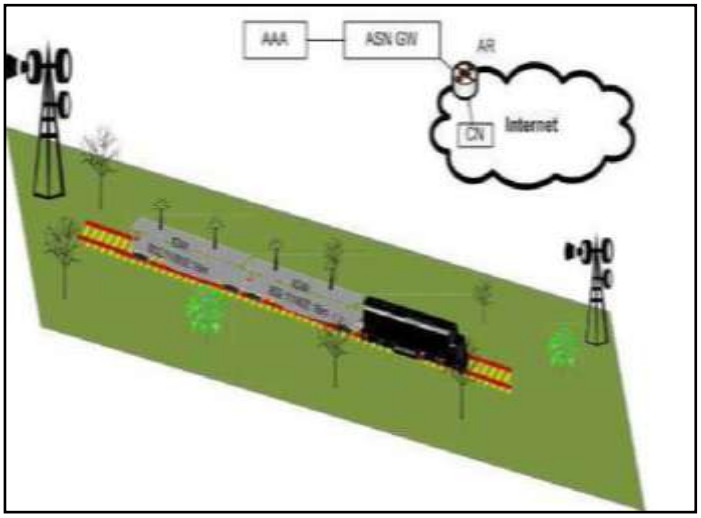


Fig. 13. Swift architecture

functions according to IEEE 802.16e. This proposal does not provide a communications solution for vehicles beyond the RS or BS coverage. Additionally, it does not recommend a routing mechanism to assist nodes select the optimal RV for overlapping coverage areas.

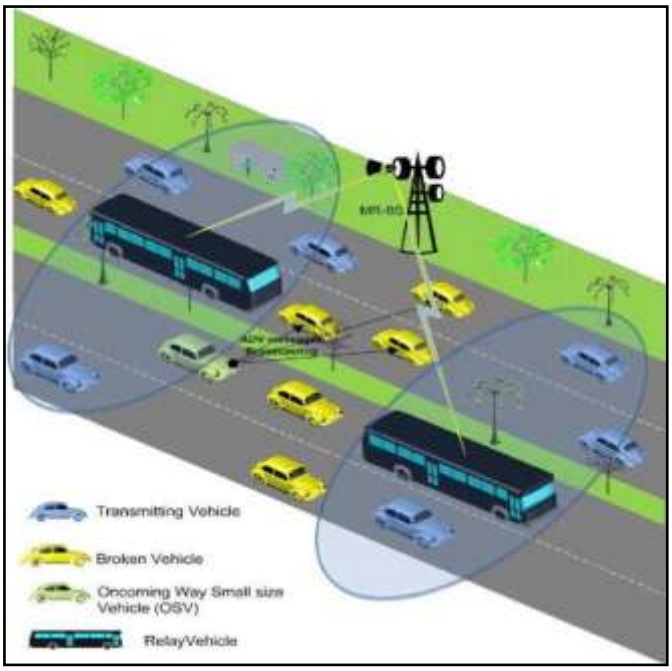
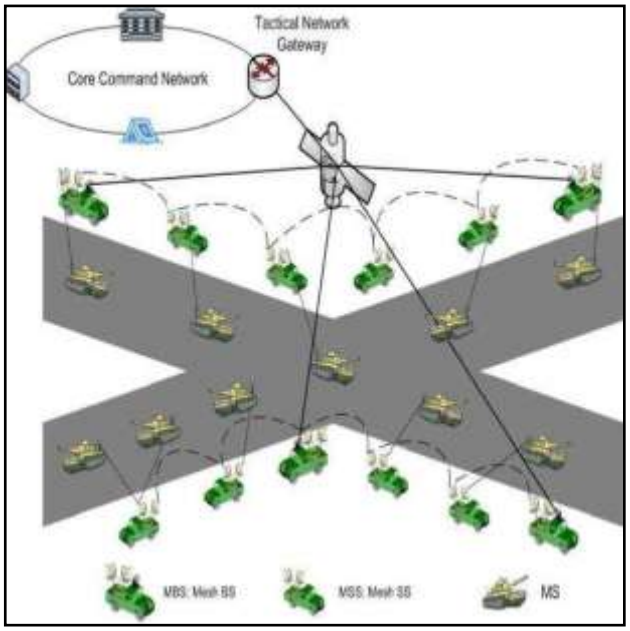


Fig. 14. A handoff with the VFHS mechanism

The authors in [15] design a scheduling mechanism called "An interference and QOS aware distributed scheduling approach for hybrid IEEE 802.16e mesh networks," which was obtained using the NS-2 simulator. Their results show that the developed scheduling mechanism facilitates efficient spectral reuse by permitting the deployment of base stations under the IEEE 802.16-2004 mesh standard. Each BS also has an IEEE 802.16e interface that provides access to mobile subscribers. Importantly, the backbone is enabled by satellite communications and their proposal does not provide a routing mechanism to improve network performance. Finally, vehicles outside the coverage area of the BS cannot access network services. Figure 11 shows the topology suggested by [15].

The authors in [16] propose a routing mechanism for Mobile Ad-hoc networks (MANET). This mechanism uses WiMAX architecture to relay routing information. After the route is enabled by a WiMAX BS, the data is sent through participating nodes.

The researchers in [16] implement their routing mechanism simulating speeds of up to 108 km/h. Their results show that packet delivery is good, but they do not mention the method used to combine the MANET and WiMAX architectures. Also, the simulations varied node



densities at a speed of 18 km/h, which is an insufficient velocity for their results to be conclusive. Another important issue concerns nodes leaving the BS coverage area, because network performance can be compromised by node mobility.

VI. CONCLUSION

Mobile WiMAX is an expectation from mobile users to give secured and seamless services. EAP with Protected based Extensible Authentication Protocol based LAP authentication method to overcome the Vulnerability of the above-mentioned scheme with much fewer requirements on the computation and communication resources. Mobile WiMAX system supports give up processes to create a mobile station find another base station from the same or different access service network to establish connection when moving out of coverage of the present serving base station. Long delay in the time-consuming verification procedure is a well-known bottleneck of handover scheme, causing service disturbance when a mobile user moves between base stations. The flexibility makes the EAP-based lightweight authentication a popular authentication method for mobile WiMAX systems. Lightweight Extensible Authentication Protocol is their proprietary method for EAP based on mutual authentication between servers and then client on the network.

The proposals analyzed in this work suggest that WiMAX can represent a viable alternative for roadside communication using present standards. Importantly, it also has the potential to be used in conjunction with radio technology for inter-vehicular communications because its strong PHY and QoS support. However, there are still significant technical challenges to be overcome before WiMAX can be implemented as radio technology for inter-vehicular communications networks.

Research provided in this chapter shows that integrating WiMAX technology into vehicular ad hoc networks is a very rich area of inquiry, although current research is somewhat limited. We believe that this is because standards for VCN are still in their infancy or have only very recently been published (i.e. IEEE 802.16j/June 2009, and IEEE 802.16m/February 20101). Consequently, we predict there will be much more research carried out in the future as these standards are more fully exploited.

REFERENCES

1. "A Novel Secure Authentication Protocol for WiMAX Network Base Stations and Subscriber Stations against Attackers using NS2", by B.Chandran Mahesh, (Research scholar) , Dr.B.Prabhakara Rao (Professor in ECE).
2. "Security Enhancement & Solution for Authentication Frame work in IEEE 802.16", by A.K.M. NAZMUS SAKIB, Chittagong University of Engineering & Technology
3. "An Enhanced Authentication Mechanism for IEEE 802.16(e) Mobile WiMAX", by Deepak Kumar Mehto, and Rajesh Srivastava.
4. "Strong Password Based EAP-TLS Authentication Protocol for WiMAX", by Anjani K.Rai, Shivendu Mishra and Vimal Kumar.
5. "Mobile WiMAX Network Security", by Rainer Falk, Christian Gunther, Dirk Kroselberg, and Avi Lior, Siemens Corporate Technology.
6. "Authentication and Privacy", by Thomas M. Chen Department of Electrical Engineering, Southern Methodist University, Dallas, Texas, USA and Nhut Nguyen Network Systems Lab, Samsung Telecommunications America, Richardson, Texas, USA
7. "Enhancing Security Using the Discarded Security Information in Mobile WiMAX Networks", by Youngwook Kim and Saewoong Bahk, School of Electrical Engineering and Computer Science, INMC.
8. "Analysis on Mobile WiMAX Security", by Perumalraja Rengaraju, Chung-Horng Lung, Yi Qu, Department of Systems and Computer Engineering Carleton University, Canada and Anand Srinivasan EION Inc. Canada.
9. "Formal Analysis of the Handover Schemes in Mobile WiMAX Networks", by Ahmed M. Taha, Amr T. Abdel-Hamid, and Sofiene Tahar, Faculty of Information Engineering and Technology German University in Cairo (GUC), Cairo, Egypt.
10. "Security Issues of IEEE 802.16 (WiMAX)", by Jamshed Hasan, School of Computer and Information Science, Edith Cowan University, Australia.
11. "WiMAX Security for Real-World Network Service Provider Deployments".
12. "Trust based authentication technique for security in WiMAX networks", by Mrs.M.Rekha and Dr.C.Chandrasekar, Department Of computer science.
13. "An enhanced Scheme for Reducing Vertical handover latency", by Mohammad Faisal, and Muhammad Nawaz Khan, Department of Computing, Shaheed Zulfikar Ali Bhutto Institute of Science & Technology (SZABIST), Islamabad, Pakistan.
14. "SPIN-based Verification of Authentication Protocols in WiMAX Networks", by Beth N. Komu, Mjumo Mzyece and Karim Djouani.
15. "Security issues and proposed solutions concerning authentication and authorization for WiMAX (IEEE 802.16e)", by Bart Sikkens Faculty of Electrical Engineering, Mathematics and Computer Science University of Twente, the Netherlands.