International Journal of Advanced Science and Research
ISSN: 2455-4227; Impact Factor: RJIF 5.12
Received: 25-07-2020; Accepted: 10-08-2020; Published: 28-08-2020
www.allsciencejournal.com
Volume 5; Issue 4; 2020; Page No. 07-13

Design and Development of quick and confident bury-asn deliveries in Portable wimax Grids in Flatcar Gps

S Ravichandran[1], R Rajkumar[2]

[1] Professor, Computer Science Department, Annai Fathima College of Arts & Science, Madurai, Tamil Nadu, India

[2] Assistant Professor, Computer Science Department, Annai Fathima College of Arts & Science, Madurai, Tamil Nadu, India

Abstract
Portable WiMAX is a desire from versatile clients to give made sure about and consistent administrations. EAP with Enhanced Extensible Authentication Protocol based pre-verification (EEP) technique to conquer the helplessness of the previously mentioned plot with many less prerequisites on the calculation and correspondence assets. Portable WiMAX framework underpins surrender procedures to make a versatile station locate another base station from the equivalent or distinctive access administration system to build up association when moving out of inclusion of the current serving base station. In the course of recent years portable interchanges have changed from an extravagance thing to a utility as basic as power and water. WiMAX is a highly scalable, long-range system, covering many kilometers using licensed spectrum to deliver a point-to-point connection to the Internet from an ISP to an end user. WiMAX can be used to provide a wireless alternative to cable and DSL for broadband access, and to provide high-speed data and telecommunications services. With this fast extension of supporters and administrations, the administrators of the remote systems are bringing in cash today and including endorsers at quick rates. Notwithstanding, this very achievement conveys the seeds of likely emergency as these supporters start expecting, requesting and expending ever-expanding measures of information over these equivalent systems. Numerous regions inside these areas are likewise seriously ailing in broadband foundation because of a similar absence of spending power among the potential endorser crowd. This is changing anyway because of government endeavors, falling costs on broadband access and less expensive access gadgets, for example, the ultra-minimal effort PC. Long deferral in the tedious check method is a notable bottleneck of handover plot, causing administration unsettling influence when a versatile client moves between base stations.

Keywords: Mobile wimax, ivc, rvc, formal verification, security, lte, hoea, pre-authentication, Gps

1. Introduction

In the course of recent years portable interchanges have changed from an extravagance thing to a utility as basic as power and water. With this fast extension of supporters and administrations, the administrators of the remote systems are bringing in cash today and including endorsers at quick rates. India for instance has development somewhere in the range of 20% and 30% year over year development in portable supporters. Notwithstanding, this very achievement conveys the seeds of likely emergency as these supporters start expecting, requesting and expending ever-expanding measures of information over these equivalent systems. 3G systems from the RAN engineering to the simultaneous vehicle were structured basically to help expanded voice limit with a small amount of information support. They were never expected to help the different terabytes being shipped today. HSPA and HSPA+, while certainly giving improvements, are as yet limited by the 3G engineering and can be viewed as minor Band-Aids instead of long haul arrangements. Right now there is little debate over the reality LTE (Long Term Evolution) will turn into the predominant worldwide 4G remote innovation throughout the following ten years. The main problem now is when most bearers will select to relocate to LTE and how long HSPA+ and CDMA EVDO Rev A will postpone LTE organizations. Numerous regions inside these areas are likewise seriously ailing in broadband foundation because of a similar absence of spending power among the potential endorser crowd. This is changing anyway because of government endeavors, falling costs on broadband access and less expensive access gadgets, for example, the ultra-minimal effort PC. The remote business made it understood throughout the most recent year or with the goal that 4G innovation is a momentary need in develop markets, and the drawn out response to broadband network around the world. In develop markets, customers are starting to discover omnipresent access to medium or higher-rate broadband an essential piece of their correspondences abilities. In creating markets, remote will keep on being the main moderate approach to convey broadband and governments will cultivate those administrations to advance financial development. Accordingly, plainly the involvement in voice administrations in the course of the most recent two decades wherein it surpassed and caused the decay of wire line-will rehash itself with broadband. That is, remote will turn into the prevailing technique to convey broadband administrations to clients. This procedure may take some time, however it will occur.

At the point when a MS handovers starting with one BS then onto the next in various ASNs, which is alluded as a between ASN handover, the MS will play out a full EAP verification with the AS and Security Association's traffic encryption key (SA-TEK) 3-route handshake with the BS to disperse the TEK. The handover procedure ought to be quick to keep up a consistent help association. Notwithstanding, an EAP-based validation has been notable

to be exorbitant because of now is the right time devouring open key cryptography activities and the deferral of a few full circle trips between the MS and the AS. A full EAP confirmation takes about 1000ms, while the suggested greatest handover dormancy for spilling applications is just 150 ms [3]. So as to diminish the handover idleness, portable WiMAX bolsters handover streamlining, permitting clients to lessen handover inertness by reusing key materials from past validation [1]. Notwithstanding, it makes basic security gaps, for example, an absence of legitimate substance verification prompting Man-in-the-Middle (MITM) assaults. Elective arrangements in [4, 9] have concentrated on lessening the postponement brought about in the EAP verification, which is most of the handover inertness, without bargaining security necessities. The current proposed procedures fundamentally fall into two classes, to be specific the re-confirmation and the pre-validation. Re-confirmation can stay away from a full EAP-based verification in handover by reusing the data traded between the MS and the AS in the past validation. In [4], the HOKEY working gathering has proposed the EAP re-validation convention (ERP) which permits a MS and the AS to utilize the all-inclusive ace meeting key (EMSK) from past EAP verification for ace meeting key (MSK) inference. Along these lines, rather than doing a full EAP verification, the MS and the AS will just need a solitary full circle to trade the ERP messages. In [5], a re-verification conspire has been recommended that can be applied for handover between heterogeneous systems. The convention utilizes an encoded accreditation, which is given to a MS as a proof of its past legit practices and ought to be introduced to the tBS for the handover. The primary thought is to let the MS to have moment access to the system through a feeble yet quick validation previously followed by a more grounded and all the more expensive confirmation. Base on the comparable thought, the proposition in [6] has utilized the shortened 192 bits of the MSK in the ensuing EAP verification as an impermanent confirmation pull key for a between ASN handover. By decreasing the quantity of messages traded and improving the cryptographic activities, re-confirmation procedures can bring down the validation flagging inactivity. By pre-confirmation procedures in [7, 9], a MS and the AS pre-register the common mystery keys before a handover. In this way, the handover deferral could be adequately diminished to a similar measure of the time utilized by a 3-way handshake, bringing about the most brief validation flagging postponement. The fundamental favorable position of the pre-validation is that the cryptographic material won't be reused, henceforth it turns out to be progressively secure. The HOKEY working gathering has proposed an EAP-based pre-confirmation model in which has been adjusted to Mobile IPv6 organize in [8] and is called Handover Early Authentication (HOEA) convention. HOEA uses proactive motioning to find up-and-comer get to organize where the MS possibly moves to and plays out a full EAP confirmation before it appends to the competitor arrange. Nonetheless, it possibly works when the connection layer bolsters proactive flagging and there is a likelihood that the handover has just begun before the pre-verification stage has finished, bringing about a fizzled pre-validation. An EAP-based pre-verification plot (EPA) has been proposed to lessen the confirmation delay in between ASN handovers [9]. By the EPA conspire, a MS trades the key materials with various neighbor ASN-GWs (nASNs) of the serving ASN-GW, home ASN-GW or hASN, so when it handovers to one of those nASN-GWs, rather than playing out a full EAP verification, it can continue legitimately with the 3-way handshake. The EPA has a few favorable circumstances over the HOEA. Proactive flagging isn't required so as to utilize EPA. Plus, the pre-validation with the nASN-GWs is done well after the MS connects to the current hASN-GW. Subsequently, the likelihood that the pre-confirmation finishes before the handover is a lot higher contrasted with that by the HOEA. Be that as it may, the EPA is defenseless against DoS assaults and replay assaults, which enormously debases its security level. Another disadvantage is the wastage of pointless exertion for key trade between the MS and those nASN-GWs that the MS never meanders to. The HOEA likewise faces a similar issue since proactive flagging must be given to the conceivable competitor systems. In this paper, so as to upgrade the security usefulness and the productivity of the EPA, as our significant commitment, we propose an Enhanced EAP-based, or explicitly, the EAP-Transport Layer Security (EAP-TLS) based pre-verification (EEP) plot which can forestall DoS and replay assaults with considerably less computational and correspondence assets and simultaneousl y, can defeat the previously mentioned disadvantages caused in the EPA and the HOEA plans.

2. Related Work

Wimax Network Model

The IEEE 802.16e-2005 standard gives the air interface to WiMAX however doesn't characterize the full start to finish WiMAX arrange respectively. This WiMAX Forum's Network Working Group is at risk for working up the through and through sort out necessities, structure, and shows for WiMAX, using IEEE 802.16e-2005 as the air interface separately. This WiMAX NWG has developed a framework reference model to fill in as a designing structure for WiMAX courses of action and to ensure interoperability among various WiMAX rigging and managers. The system reference model imagines brought together system engineering for supporting fixed, itinerant, and portable organizations and depends on an IP administration model. The following is rearranged representation of IP-based WiMAX arrange engineering.

The general system might be sensibly isolated into three sections:

(i) Portable Stations (MS) utilized by the end client to get to the system.

(ii) The entrance administration arrange (ASN), which contains at least one base stations and at least one ASN doors that structure the radio access organize at the edge.

(iii) Availability administration organize (CSN), which gives IP availability and all the IP center system capacities.

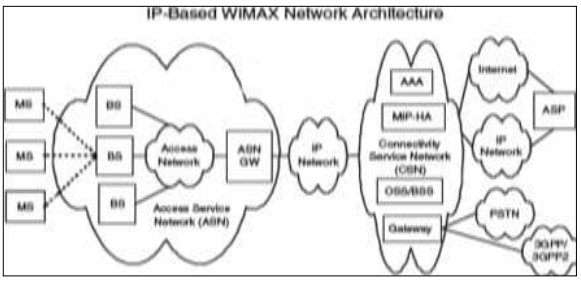


Fig 1: Conventional WiMAX Design

ITS (Intelligent Transporation System)
Telematics is called IT'S for short. Transport utilize the Internet is the pattern of advancement of versatility correspondence later on. The current improvement of ITS primary goal is to consolidate the interchanges innovation gave by industry. It has become the nation's primary vehicle framework in the improvement of coordination. Vehicle associated with web to develop the Ubiquitous registering will be generally well known of data correspondence and business later on.

GPS (Global Positioning System)
GPS is the most well-known situating framework innovation, created by the U.S. Division of Defense. Before, GPS just was utilized in some cutting edge regions, for instance: for military, aeronautics or sea, it's for open utilization now. The "vehicle route frameworks" presently is a case of down to earth application. GPS is developed from 24 satellites, including three preliminary satellites .The general activity of the satellite situating framework can be partitioned into three sections: Space Segment, Control Segment and User Segment. It utilizes the concurrent sign with the satellite and its connection between relative situations to identify the specific area.
Truth be told, there has been a blend of GPS and handoff of remote systems configuration proposed in the writing, it essentially incorporates 802.11 remote systems, Mobile IP and GPS frameworks comprise the whole structure of nature, yet basically through the GPS to find the current area of MS, to pick an AP database from all APs around current position. At that point, by telling MN of Mobile IP that it can utilize the database as a handoff list, yet it doesn't have the assigned base stations to process the handoff. By and large, this is a system situation engineering which is chosen by end clients to make handoff.

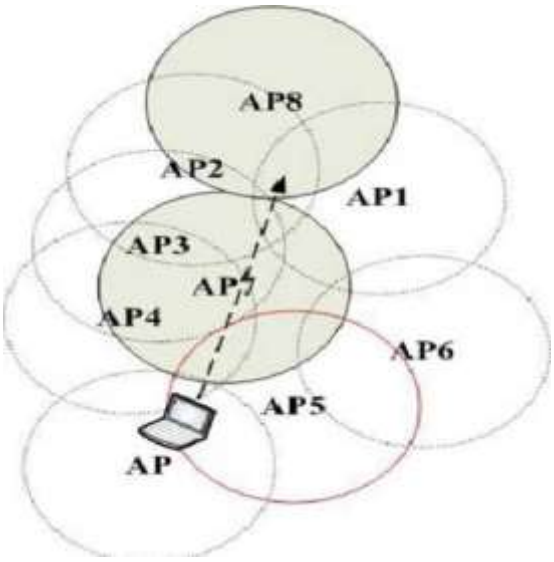
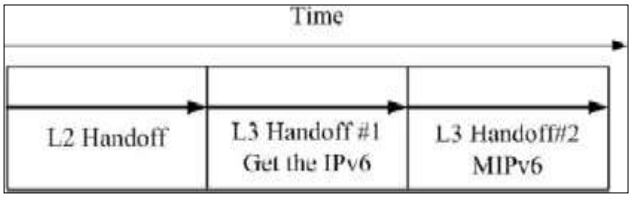


Fig 2: Conventional GPS combines with 802.11 Design

Handoff Procedure
Handoff is disengaged from the association with quit accepting the bundle from Correspond Node, until MN move to another subnet and got the parcel from Corresponding Node once more. For Wireless web handoff, its primary object is giving the handoff of Layer 3, IP layer, however next to the Layer 3, the Layer 2 is likewise remembered for the general handoff of all out time. At the point when MN (Mobile User) left the extent of Serving BS (Serving Base Station), so as to maintain a strategic distance from any interruption in administration, it would look through the accessible a Target BS (Target Base Station) which can handoff.

Table 1: Handoff format Design



MN will set a Neighbor BS Scanning RSSI esteem (Here's a model by 802.16e's MS), when Serving BS signal quality beneath this worth, it will begin this procedure to locate the base station, MN as per the channel from spine or its own permit rundown to output and measure the sign quality, when the Serving BS esteem lower than the Handover RSS Target esteem, it will begin handoff systems, disengage the first association, and interface with the base station it checked, hanging tight for get or demand another system Prefix. To frame IPv6 address as indicated by naturally shaped address and convey trade message to HA for register and complete the general handoff process. Figure 2 is handoff engineering. L2 Handoff contains the output channels and decisions BS, L3#1 incorporates the getting another IP of new system and confirmation IP, L3#2 is the message of handoff.

3. Problem Statement
In this segment we will clarify our framework and how to offer types of assistance, clarifies how Telematics characteristic handoff without changing the 802.16e norm through MOB_NBR-ADV.

Through Mob_Nbr Adv control Telematics handoff
The handoff system incorporates three stages: They are,

1. Disclosure
2. Re-affiliation
3. Re-validation

Regardless of whether a handoff choice will be made depends on the Discovery, and Discovery is utilized for filtering BS for handoff. The show handoff component depends on quality of sign which is getting sufficiently high to limit for deciding to start handoff. The convention of WiMAX include an instrument that back-end organize gives BS data around itself (MOB_NBR-ADV incorporates BS data which can be connected) arrange checking, search base station. MOB_NBR-ADV is sent by our framework which one incorporates just a single demonstrative BS to handoff.
MS is moving between two BS, it will be influence by them. In any case, when the sign quality vacillates inside the default level estimation of handover, it would make the component for beginning handoff, bringing about consistent change Hand, this circumstance known as the Ping-Pong-Effect. The most effective method to pick BS is the issue we need to clarify here:
First GPS will utilize Triangulation Method to locate the current area and name the estimations of longitude and scope. After client choosing the goal, client should point the goal obviously in GPS. Guide programming utilizing own

calculations figure the way among source and goal. Guide Software will convey way data to Serving BS through system and convey to Handoff Management Server which in ASN. As per this data, HMS will figure the measure of BS which influenced the coordinative worth individually.

4. Implementation

Wimax Network Configure Setting

WiMAX organize used to make the no of hubs. The bundles to send and accepting through the source to goal. It's based the plan of parcels conveyed for ACK bundle drop on the hubs. In this system to making the source and goal hub of the system and communicate the information to preparing on their entire systems administration.

Topology Design

This module is created to Topology plan all hub place specific separation. Without utilizing any links then completely remote hardware based transmission and got parcel information. Hub and remote between figure sending and getting bundles. The sink is at the focal point of the round detecting territory. Middle of the road the sender and recipient of this systems administration execution on this geography.

Node Creating

This module is created to hub creation and in excess of 10 hubs set specific separation. Remote hub put middle of the road zone. Every hub knows its area comparative with the sink. The passage needs to get communicate parcels at that point send recognize to transmitter.

Dos Attacks

The neighbor list message sent by the entrance administration system to a portable station without a newness sign and a proof of the cause, it can create a security gap for a DoS assault. The absence of the message validation permits an enemy to produce its own neighbor list message and send it to the portable station, guaranteeing that it is sent by the entrance administration arrange.

Replay Attacks

Pre-verification process, an enemy can listen in the pre validation demand message and retransmit it later, professing to be a real MS. Since the message doesn't have a newness pointer, they will consider it as another solicitation message, confirm its mark and hand-off it to the system.

ERP Framework and Authentication

EAP-Transport Layer Security based verification can give solid common confirmation it has been chosen by the WiMAX gathering as one of the alternatives for the determination of the validation strategy between the versatile station and the confirmation worker. The EAP verification is executed between a portable station and the base station in the key administration framework.

Pre Authentication Latency

The pre-confirmation dormancy comprises of the postponement of figuring process and the transmission and proliferation deferrals of the complete messages. To assess the postponement of registering process, which is the time utilized for the cryptographic activities. The preparing forces of the base station, the entrance administration arranges just as the validation worker are the equivalent.

Graph design based Result

Diagram is a basic piece of show an outcome, so we plot a chart to show a different outcome examination with bundles, throughput, and vitality effective and so forth.

5. Imitation Outcomes

GPS licenses clients to get constant area data. In any case, extended interchanges among vehicles and with side of the road foundation can significantly grow administrations drivers at present appreciate in the regions of traffic stream, wellbeing, data (Internet), correspondences (VoIP) and solace applications, among others [2].According to Sichitiu *et al*. applications for vehicular interchanges incorporate the accompanying.

1. Proactive wellbeing applications: outfitted basically to improve driver response and dynamic to stay away from potential mishaps (for example communicate admonitions from a vehicle that has overlooked red stop light) or limit the effects of an up and coming accident (computerized stopping mechanisms).
2. Traffic the board applications: for the most part actualized to improve traffic stream and diminish travel time, which is especially valuable for crisis vehicles.
3. Traffic coordination and traffic help: basically worried about improving the conveyance and stream of vehicles by helping drivers pass, switch to another lane, consolidation and structure sections of vehicles that keep up consistent relative speeds and separations (platooning).
4. Voyager Information Support: for the most part centered on giving explicit data about accessible assets and help people require, making their voyaging experience not so much unpleasant but rather more productive.
5. Solace Applications: fundamentally intended to improve the movement experience of the travelers and the driver (for example gaming, web, programmed tolls, and so forth.).

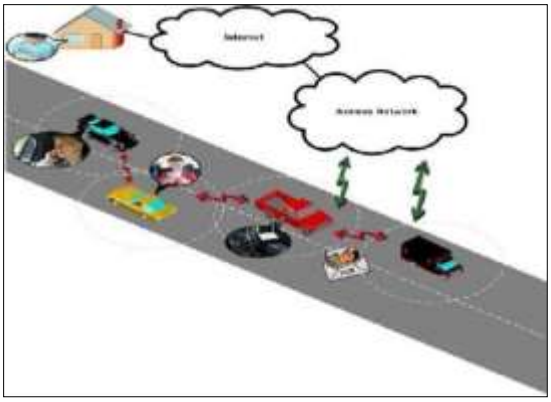


Fig 3: Potential Applications in WiMAX

So as to give more noteworthy traveler wellbeing, accommodation and solace, conventions and hardware must give all the more opportune and dependable information move between organize hubs for them to viably share indispensable data. In figure 3 shows, on account of WiMAX, arrange hubs should effectively communicate and get information in an immediately changing system condition, described by the consistent section and exit of

hubs. Furthermore, portable hubs must deal with handoffs between various groups, all while working inside extremely exacting specialized boundaries in regards to bundle misfortune, postponement, idleness, and throughput, among others. Sichitiu and Kihl in [3] build a scientific categorization dependent on the manner in which hubs trade information.

Their work includes two types of vehicular correspondence: vehicle to vehicle (IVC) and vehicle to side of the road (RVC). IVC can utilize either a one bounce (SICV) or multi-jump (MIVC) methodology. Then again, RVC can be universal (URVC) or scant (SRVC). Correspondences inside VANETs can be either between vehicular or vehicle to side of the road and each sort of correspondence forces its particular prerequisites. For instance, roadway impact cautioning frameworks can all the more effectively be actualized utilizing multi-jump correspondences between vehicles (without foundation). Then again, voyager data requires fixed foundation to give availability between the vehicles and a data place. IVC arrangement is essentially more affordable than RVC on the grounds that it is framework less. This sort of design permits vehicles to send data between one another by means of multi-bounce correspondence, even with vehicles that are past their prompt radio inclusion territory. IVC web get to is significantly more confounded than with RVC.

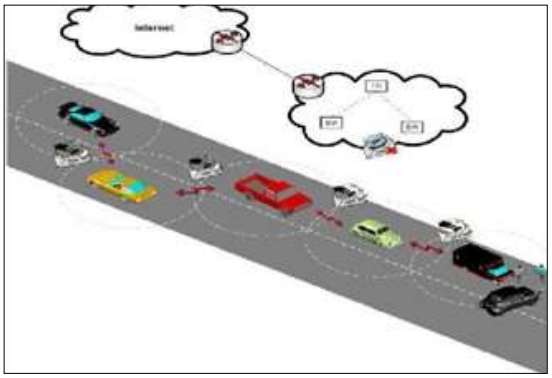


Fig 4: Example of IVC

Subsequently, IVC can just give a diminished number of uses. Nonetheless, IVC is more qualified for security applications in light of the fact that the vehicles can very quickly identify impact or clog cautioning that is communicated inside the influenced territory. Figure 7 gives a case of bury vehicular correspondence, where a vehicle moving toward a mishap identifies the accident and advises the vehicles behind it that it is going to slow down out of nowhere. This cautioning could help maintain a strategic distance from different mishaps brought about by drivers who can't make a difference their brakes ideally and permits vehicles further behind to move to another lane to decrease gridlock. RVC can offer a more extensive scope of uses as a result of its increasingly steady and strong access to the Internet, which permits prepared accessibility of data about explicit spots and the administrations they give. RVC, in any case, has two significant disadvantages when considered for security applications.

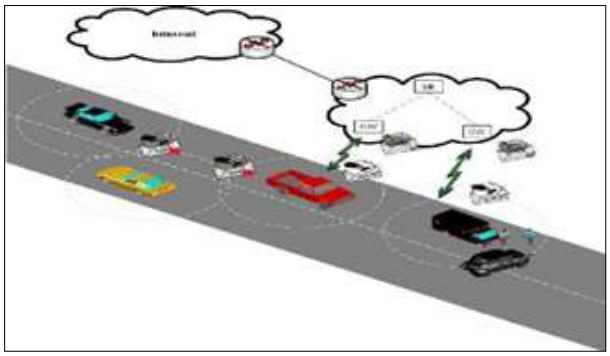


Fig 5: Example of RVC Network

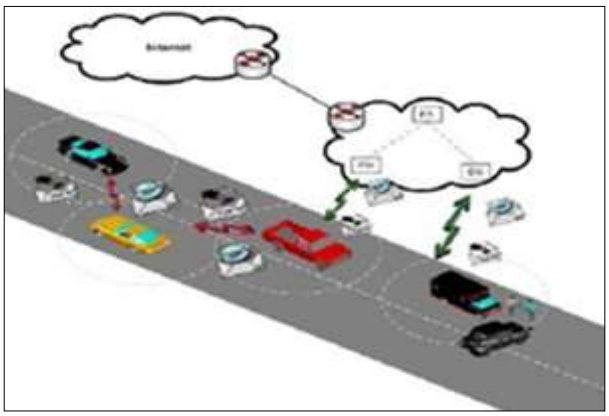


Fig 6: Mixture of IVC and RVC

Figure 6 outlines a half breed vehicular correspondence organize where vehicles inside the inclusion region of a RVC can go about as doors for vehicles outside the inclusion zone. HVC systems are very desirables in light of the fact that they can give practically any sort of administration. Critically, be that as it may, as recently referenced, research should initially conquer numerous specialized difficulties before HVC systems can be executed in certifiable applications. This is principally a result of the contrariness of advances (for example WiFi was created for WLANs, while cell interchanges were intended for WANs).

Various advances have been tried to empower RVC, including cell, WiFi (IEEE 802.11p) and WiMAX (IEEE 802.16e), however no standard has been set up starting at yet. By and by, creators accept that WiMAX best fits VCN prerequisites due to its high data transfer capacity, vigorous medium access control (MAC), flexibility (for example wide scope of perfect guidelines) and QoS support. Significantly, it satisfies the previously existing guideline for portable hubs (IEEE 802.16e). Figure 4 delineates instances of some RVC applications, which incorporate telecom the area of explicit organizations and giving data about merchandise and ventures offered by them.

Both IVC and RVC have attractive advantages; while with IVC clients can shape bunches for all intents and purposes anyplace, with RVC people can approach web and broaden the vehicular applications. Critically, joining both of these designs into a half breed vehicular correspondences (HVC) system can amplify benefits. HVC, in any case, is progressively mind boggling in different viewpoints: HVC

need increasingly complex directing conventions, a hearty physical layer and a medium access layer that is adequately powerful to completely misuse the brief length of connections and sorted out enough to limit obstruction.

The creators in propose a steering convention called Coordinated External Peer Communications (CEPEC), whose cross-layer convention is intended for multi-jump vehicular systems. They got their reproduction results utilizing an exclusive improvement instrument which ensured all vehicles reasonable access to the Internet, significantly over hubs that were a few bounces removed from the BS. Their proposition incorporates arrange the OSI model into three layers: PHY, MAC and Network. In any case, the creators don't indicate the changes they made to the IEEE 802.16-2004 standard that allowed the expanded versatility and faster enrollment of the MS. The creators utilize TDMA to dole out channels, abusing TDMA's brought together scheduler and time division duplexing. At long last, and critically, CEPEC needs to decide the geographic situation of each vehicle. To do this, all vehicles must be furnished with GPS.

A significant burden of CEPEC is that it just permits information correspondence from vehicles to the BS and the other way around; in this way, it doesn't accommodate vehicle-to-vehicle information trade. Moreover, CEPEC's unified booking component decreases its adaptability. Since, as recently referenced, the creators of [11] don't indicate the progressions they made to the IEEE 802.16 norm, we should expect that vehicles enter the system as per standard details for hubs in work mode. Obviously, this suggests arrange execution endures critical decay. Likewise, the creators neglect to detail the alterations they made to the standard that allowed expanded portability and geography control.

6. Conclusion

Versatile WiMAX is a desire from portable clients to give made sure about and consistent administrations. EAP with Protected based Extensible Authentication Protocol based LAP verification technique to conquer the Vulnerability of the previously mentioned conspire with many less necessities on the calculation and correspondence assets. Versatile WiMAX framework bolsters surrender procedures to make a portable station locate another base station from the equivalent or distinctive access administration system to build up association when moving out of inclusion of the current serving base station.

Long postponement in the tedious check strategy is a notable bottleneck of handover plot, causing administration aggravation when a versatile client moves between base stations. The adaptability makes the EAP-based lightweight verification a well-known validation technique for versatile WiMAX frameworks. Lightweight Extensible Authentication Protocol is their exclusive strategy for EAP dependent on shared validation among workers and afterward customer on the system. The proposition examined in this work recommend that WiMAX can speak to a practical option for side of the road correspondence utilizing present principles. Significantly, it likewise can possibly be utilized related to radio innovation for between vehicular interchanges since its solid PHY and QoS support.

Be that as it may, there are as yet huge specialized difficulties to be defeated before WiMAX can be actualized as radio innovation for between vehicular interchanges systems. Exploration gave in this section shows that incorporating WiMAX innovation into vehicular impromptu systems is a rich zone of request, albeit ebb and flow research is fairly restricted.

7. Acknowledgments

The authors are thankful to Ahmed M. Taha, Dr. B. Prabhakara Rao and Dr. C. Chandrasekar for providing the necessary facilities for the preparation of the paper. Also thanks to IJASR Journal staffs to publish this paper.

8. References

1. 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, 2017.
2. 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), 2018.
3. 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, 2018.
4. 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, 2018.
5. Analysis on Mobile WiMAX Security", by Perumalraja Rengaraju, Chung-Horng Lung, Yi Qu, Department of Systems and Computer Engineering Carleton Univer sity, Canada and Anand Srinivasan EION Inc. Canada.
6. "Security Enhancement and Solution for Authentication Frame work in IEEE 802.16", by A.K.M. NAZMUS SAKIB, Chittagong University of Engineering & Technology, 2019.
7. "Formal Analysis of the Handover Schemes in Mobile WiMAX Networks", by Ahmed M. Taha, Amr T. Abdel Hamid, and Sofiene Tahar, Faculty of Informatio n Engineering and Technology German University in Cairo (GUC), Cairo, Egypt, 2018.
8. David Fick, Andrew DeOrio, Gregory Chen, Valeria Bertacco, Dennis Sylvester and David Blaauw, "A Highly Resilient Routing Algorithm for Fault Tolerant NoCs", Design, Automation & Test in Europe Conferen ce, 2019.
9. "Trust based authentication technique for security in WiMAX networks", by Mrs.M.Rekha and Dr.C.Chandr asekar, Department of computer science, 2017.
10. "Security Issues of IEEE 802.16 (WiMAX)", by Jamshed Hasan, School of Computer and Information Science, Edith Cowan University, Australia, May 2018.

11. “SPIN-based Verification of Authentication Protocols in WiMAX Networks”, by Beth N. Komu, Mjumo Mzyece and Karim Djouani, 2017.
12. “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.
13. An Enhanced Authentication Mechanism for IEEE 802.16(e) Mobile WiMAX”, by Deepak Kumar Mehto, and Rajesh Srivastava, 2018.
14. Mobile WiMAX Network Security”, by Rainer Falk, Christian Gunther, Dirk Kroselberg, and Avi Lior, Siemens Corporate Technology, 2018.