Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.613 – 625

RESEARCH ARTICLE

RAPID AND PROTECTED DATA COLLECTION USING GPS FOR INTER ASN HANDOVER AND IMPROVING QOS IN MOBILE WIMAX

[1]S.Janane, [2]H.Lookman Sithic

[1]Research Scholar, Muthayammal College of Arts and science

[2]Assistant Professor, Muthayammal College of Arts science

ABSTRACT- The sink mobility along a constrained path can improve the energy efficiency in wireless sensor networks. 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. The flexibility makes the Protected EAP-based authentication a popular authentication method for mobile WiMAX systems. We have obtainable a new algorithm and used GPS (Global Position system) to perform handover faster and decrease data collection interval. WNs with following DCPs. Due to the path constraint, a mobile sink with constant speed has limited communication time to collect data from the sensor nodes deployed randomly. To address this issue, we propose a novel data collection scheme, called the Maximum Amount Shortest Path (MASP).That increases network throughput as well as conserves energy by optimizing the assignment of sensor nodes. We also develop a practical distributed approximate algorithm to solve the MASP problem. The impact of different overlapping time partition methods is used to solve the ns2.

Key Words: MASP, PEAP, DCP, Mobile WiMAX, NS2

I. INTRODUCTION

The rapid growth of wireless communication and its pervasive use in all walks of life are changing the way we communicate in all fundamental ways. WiMAX is poised to broadcast the Internet throughout the world. WiMAX which stands for "Worldwide Interoperability for Microwave Access" is about to bring the wireless and the Internet revolutions to portable devices across the globe. WiMAX is a wireless digital communications system, also known as IEEE 802.16 that is intended for wireless "metropolitan area networks".

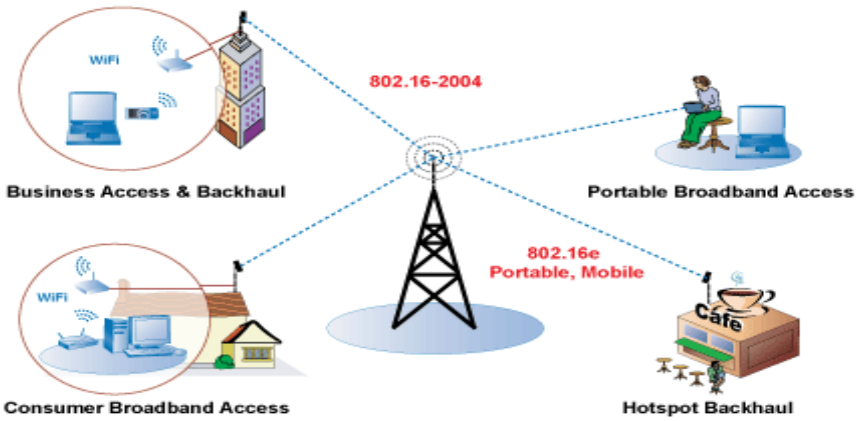

Figure 1: WiMAX Accessibility

WiMAX can provide broadband wireless access (BWA) up to 30 miles (50 km) for fixed stations, and 3 - 10 miles (5 - 15 km) for mobile stations. In contrast, the WiFi/802.11 wireless local area network standard is limited in most cases to only 100 - 300 feet (30 - 100m). With WiMAX, WiFi-like data rates are easily supported, but the issue of interference is lessened. Enhance mobility wireless access are designed such as 802.16 to operate on the move without any interfere of services.

The mobile WiMAX is a step towards the evolution of WiMAX. Mobile WiMAX, or Institute of Electronic and Electrical Engineers (IEEE) 802.16e-2005, emerged as a potential alternative to cellular technology for wide-area wireless networks. Based on Orthogonal Frequency Division Multiple Access (OFDMA) and approved by the International Telecommunication Union (ITU) as an IMT-2000 (3G technology) under the name OFDMA Time Division Duplex (TDD) Wireless Metropolitan Area Network (WMAN), mobile WiMAX gained its greatest traction in developing countries as a fixed wireless alternative to wire line deployment.

II. BACKGROUND OF MOBILE WIMAX TECHNOLOGY

Handover in mobile WiMAX:

Mobile WiMAX has three types of handover procedures in mobile WiMAX which are Micro Diversity Handover (MDHO), Fast Base Station Switch Handover (FBBS) and the hard handover (HHO). The first two types are optional handover which enables the MS to send and receive data from numerous access points simultaneously. The hard handover however is mandatory.

Handoff Support:

The mobile WiMAX standard supports three physical-layer handoff mechanisms.

- **Hard Handoff**: This is a 'break before make' handoff in which the subscriber terminal is disconnected from one base station before connecting to the next base station.
- **Fast base station switching (FBSS):** The network hands-off the subscriber between base stations while the connection with the core network remains with the original base station.
- **Macro-diversity handover (MDHO):** The subscriber maintains a simultaneous connection with two or more base stations for a seamless handoff to the base station with the highest quality connection.

Quality of Service (QoS) Support:

- Meet QoS requirements for a wide range of data services and applications
- In the MAC layer, QoS is provided via service flows as seen in Figure 2.
- The connection-oriented QoS enable the end-to-end QoS control.

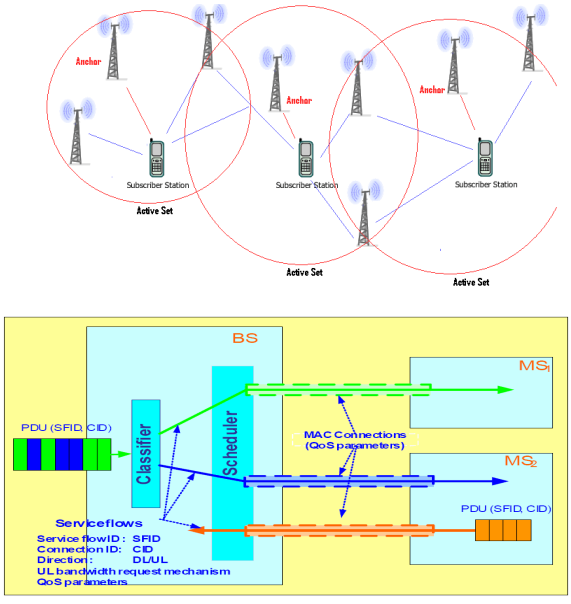

Figure 2: Mobile WiMAX QoS Support

Ends-to-End WiMAX Architecture

- Support loosely-coupled internet working with existing wireless networks such as 3GPP and 3GPP2, or wire line networks such as DSL and MSO with internetworking interfaces based on a standard IETF suite of protocols.
- WiMAX Network Reference Model (NRM) -> is logical representation of the network architecture.
- It providing unified support for functionality needed in a range of network deployment models and usage scenarios (from fixed-nomadic-portable-simple mobility-to fully mobile subscribers)

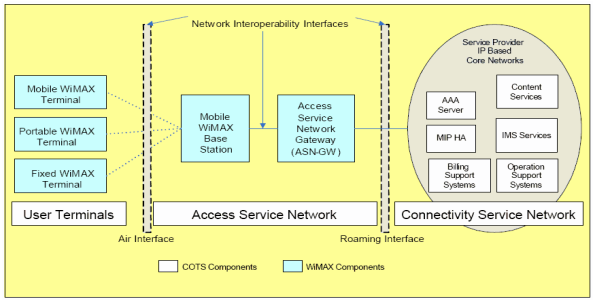

Figure 3: WiMAX Network IP-based Architecture

III. METHODOLOGY

It is mandatory for the handover process in cellular and circuit switching based wireless network to perform address re-assignment when moving from one BS to another. Mobile WiMAX considered to be IP based packet switching network, so avoiding address re-assignment is possible in case that the serving BS and the target
BS are located in the same IP subnet, such scenario can be found in high speed trains and also highways where several neighboring BSs can be lined alone the railway or the highway path.

In the standard WiMAX handover procedure, the MS is required to re-assign its address according to new subnet of the target BS. For our fast handover mechanism we propose to construct both of the serving BS and the target BS to be in the same subnet. Fortunately, nowadays increasing numbers of BS are connected within the same metro Ethernet backhaul. This fact can provide a platform for faster handover.

WORKING PRINCIPALS

The bandwidth signal is separately in OFDMA (Orthogonal Frequency Division Multiplexed Access) which is used to carry data called sub carrier. Transmitted data divided into numerous data stream where everyone is owed to another sub carrier and then transmitted at the same broadcast interval. At the downlink path the base station broadcast the data for different user professionally over uninterrupted sub-carriers. WiMAX is providing quality of service (WiMAX QoS) which enables high quality of data like VoIP or TV broadcasts.

The data communication protocol from base station is alternative of quality of service (WiMAX QoS) application and offering video streaming. These types of data translated into

parameters or sub carriers per user. All type of technique is carrying out together to speed up coverage, bandwidth, efficiency and number of users. The base station of WiMAX has ability to cover up 30 miles. WiMAX technology supports various protocols such as VLAN, ATM, and IPv4 Ethernet etc.

GLOBAL POSITIONING SYSTEM

The Global Positioning System (GPS) is a satellite based navigation system .It has revolutionized the surveying and navigation fields since stages of development. It is a civil application that grown much faster. Now GPS has used in numerous of applications in land, marine and navigation, vehicle. In network Data tracking are rapidly growing applications. GPS provides continuous positioning and timing information, anywhere in the world under any whether condition. Because it serves an unlimited number of users as well as being used for security reasons.

MAXIMUM AMOUNT SHORTEST PATH:

We proposed an efficient data collection scheme called Maximum Amount Shortest Path (MASP) for wireless sensor networks with path-constrained mobile sinks. The integer of DCPs is per unit time with no impressive extra work strike on each on its have possession of DCP. A multistage complex configuration (Genetic) algorithm is proposed to construct the proposed network structure while keeping communication distance surrounded by transmitter nodes at low values. Simulation results shows that the proposed network structure can provide significant improvements on data collection rates without increasing data collection durations. GPS permit user to achieve real-time site Information. Though, long-drawn-out communications in the middle of devices and with network infrastructure can Substantially get bigger services drivers at present enjoy in the areas of interchange flow, safety, information, communications and comfort applications, among others.

In MASP, the mapping between sensor nodes and sub sinks is optimized to maximize the amount of data collected by mobile sinks and also balance the energy consumption. A heuristic based on genetic algorithm and local search is presented to solve the MASP optimization problem.

We design a communication protocol that supports MASP and adapts to dynamic topology changes. To reduce the computational complexity, we develop two practical algorithms, a zone partitioning-based solution and a distributed solution. The proposed schemes on different scenarios with various movement trajectories of mobile sinks. Considering that minimizing the total energy consumption may not lead to the maximum network lifetime, we also plan to study the sub sink selection problem with network lifetime maximization as the optimization of this work.

GENETIC ALGORITHM

The performance of the genetic algorithm proposed in the GA is run 20 times for each scenario. The information about the number of hops and the number of nodes is obtained through the simulation environment. In our simulations, the parameter used to terminate the GA is set and the size of the initial population. Genetic algorithm is a computing search technique to find true/approximate solutions to optimization and search problems.

As genetic algorithm (GA) is a programming technique that mimics the biological evolution as a problem solving strategy. When solving a specific problem, the input to GA is a potential solutions domain, encoded with a metric titled fitness function allowing quantitative

evaluation of each candidate solution. Each candidate's evaluation is based on the fitness function. Fitness function evaluates a set of chromosomes from a population. The algorithm routinely chooses individuals for the creation of new ones. The parents produce two offspring using crossover technique. Generation of mutants is also possible. Crossover technique includes random exchange of bits between intermediate population strings. Mutation operators are new string bits.

This algorithm provides an optimal acceptable solution. Genetic algorithms (GAs) are a relatively new paradigm for a search, based on principles of natural selection. GAs is proven to be the most powerful optimization technique in a large solution space. This explains the increasing popularity of Gas applications in image processing and other fields. These GA are used where exhaustive search for solution is expensive in terms of computation time.

BEGIN
Initialize the start node and destination node
Generate randomly the initial data collection using via gps in each network
While NOT (out of range node) DO
Evaluate the distance for each node in current position using gpd
Rank the node using the coverage values
Eliminate the highest coverage area node
Apply or to collect the all data in corresponding node in network
Generate or collect the all data
END To received the destination node
END

In Mobile Ad hoc network, mobile node battery energy is limited and represents one of the important constraints for designing multicast routing protocols.

In regards to the battery lifetime limitation in supporting multicast routing, some studies have given a Genetic algorithm solution for saving power. Previously the techniques are considered only for static scenario. Here the proposed energy-efficient genetic algorithm is tested in a dynamic scenario. The simulation results are taken by considering a dynamic scenario which is appropriate for Mobile Ad hoc networks. The proposed genetic algorithm depends on bounded end-to-end delay and minimum energy cost of the multicast tree.

IV. PERFORMANCE OF PEAP (PROTECTED ENHANCED AUTHENTICATION PROTOCOL)

EXTENSIBLE AUTHENTICATION PROTOCOL

In existing they use EAP. EAP was originally created as an extension to PPP to allow for the development of arbitrary network access authentication methods. With PPP authentication protocols such as Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), and MS-CHAP version 2 (MS-CHAP v2), a specific authentication mechanism is chosen during the link establishment phase. The authentication protocol is a fixed series of messages sent in a specific order. With EAP, the specific authentication mechanism is not chosen during the link establishment phase of the PPP connection. Instead, the PPP peers negotiate to perform EAP during the connection authentication phase. When the connection authentication phase is reached, the peers negotiate the use of a specific EAP authentication scheme known as an EAP method. After the EAP method is agreed upon, EAP allows for an open-ended exchange of messages between the access

client and the authenticating server that can vary based on the parameters of the connection. The EAP method determines the length and details of the authentication conversation.

Architecturally, an EAP infrastructure consists of the following:

EAP peer Computer that is attempting to access a network, also known as an access client.

EAP authenticator An access point or network access server (NAS) that is requiring EAP authentication prior to granting access to a network.

Authentication server A server computer that negotiates the use of a specific EAP method with an EAP peer, validates the EAP peer's credentials, and authorizes access to the network. Typically, the authentication server is a Remote Authentication Dial-In User Service (RADIUS) server.

The EAP peer and the EAP authenticator send EAP messages using a supplicant-a software component that uses EAP to authenticate network access-and a data link layer transport protocol such as PPP or IEEE 802.1X. The EAP authenticator and the authentication server send EAP messages using RADIUS. The end result is that EAP messages are exchanged between the EAP components on the EAP peer and the authentication server. The following figure shows EAP infrastructure and information flow.

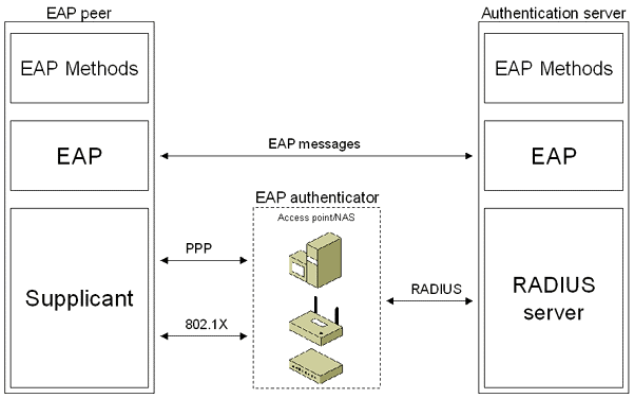

Figure.4: EAP infrastructure and information flow.

Because the logical communication of EAP messages is between the EAP components on the EAP peer and the authentication server, the EAP authenticator does not need to support any specific EAP methods. You can use EAP to support authentication schemes such as Generic Token Card, One Time Password (OTP), Message Digest 5 (MD5)-Challenge, Transport Layer Security (TLS) for smart card and digital certificate-based authentication, and future authentication technologies. The IEEE 802.1X standard defines how EAP is used for authentication by IEEE 802 devices, including IEEE 802.11 wireless APs and authenticating Ethernet switches. IEEE 802.1X differs from PPP in that only EAP authentication methods are supported. The 802.1X specification recommends EAP, a widely used and flexible authentication transport. By using EAP between the wireless client device and the back-office authentication servers, you can provide robust and scalable authentication and reuse much of the infrastructure commonly present for dial-up remote access and virtual private network (VPN) access.

After studying the available EAP-based authentication schemes, Microsoft realized that further protocol development was needed to address some security and deployment issues with

EAP. As a result, Microsoft has been instrumental in the development of PEAP, a draft standard for a common approach to wireless-network user authentication. The PEAP proposal is supported under the security framework of the IEEE 802.1X specification, and has been submitted to the IETF.

PROTECTED EXTENSIBLE AUTHENTICATION PROTOCOL (PEAP)

The Protected Extensible Authentication Protocol, also known as Protected EAP or simply PEAP, is a protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel. The purpose was to correct deficiencies in EAP; EAP assumed a protected communication channel, such as that provided by physical security, so facilities for protection of the EAP conversation were not provided.

The protocol only specifies chaining multiple EAP mechanisms and not any specific method. However, use of the EAP-MSCHAPv2 and EAP-GTC methods are the most commonly supported. The protected EAP is designed to simplify the deployment of 802.16m by using Microsoft Windows logins and passwords. PEAP is considered a more flexible EAP Scheme because it creates an encrypted channel between the client and authentication server, and the channel then protects the subsequent user authentication exchange.

PEAP is a more flexible scheme than EAP-TLS. PEAP creates an encrypted SSL/TLS channel between the client and the authentication server, and the channel then protects the subsequent user authentication exchange. To create the secure channel between client and authentication server, the PEAP client first authenticates the PEAP authentication server using digital certificate authentication. This technique is widely used to protect Web transactions (using SSL) and requires only the server to own a digital certificate. When the secure TLS channel has been established, you can select any standard EAP-based user authentication scheme for use within the channel. If you intend to use digital certificates to authenticate the client, Microsoft recommends that you use EAP-TLS rather than PEAP.

If you are not currently planning to deploy a PKI, Microsoft recommends you use PEAP-Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) user authentications because it provides a combination of security, interoperability, flexibility, and ease of deployment.

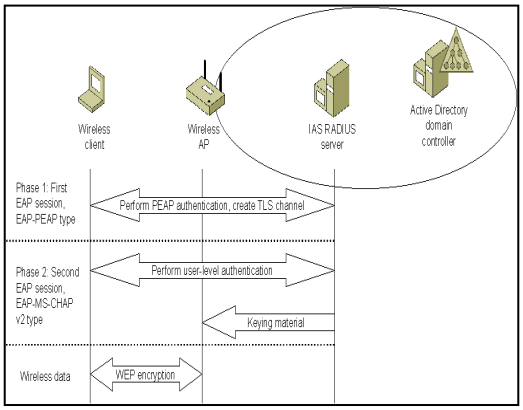

Figure 5: PEAP authentication in a wireless environment.

This combination is not offered by most other password methods available today. For Microsoft Windows products, existing EAP plug-ins written to the current EAP application programming interface (API) should work transparently with PEAP. To prevent a possible 'man-

in-the-middle' attack, Microsoft recommends that you do not use the same authentication method and credentials for PEAP and non-PEAP connections, unless the non-PEAP connections are otherwise protected by Internet Protocol security (IPSec).

PEAP AUTHENTICATION PHASE

PEAP transactions occur during the 802.1X authentication process. PEAP authentication occurs in two phases:

- Phase 1. Client authenticates the authentication server to prevent connections to rogue networks. TLS creates a robust, encrypted channel from the client to the authentication server.
- Phase 2. The TLS channel is used to protect the client authentication exchange.

After the user is successfully authenticated, dynamically generated keying material is supplied by the authentication server to the wireless AP. From this keying material, the AP creates new encryption keys for data protection.

The Robust Security Network Association (RSNA) proposed in IEEE 802.11i has emerged as the most popular method to counter the first time association problem. The RSNA technique is widely used in both WLANs and WiMAX. Although IEEE 802.16 security architecture offers sufficient protection to the wireless environment, it is up to the implementer to guarantee that all issues are addressed and the appropriate security measures are implemented for secure operation. There are two schemes for authentication during handover in Mobile WiMAX. These schemes try to avoid the MS re-authentication. In the first scheme, whenever the MS enters the network for the first time, it is authenticated by AAA through EAP authentication.

Later, whenever the MS needs to be authenticated by the AAA server, then instead of standard EAP method used in handover authentication, an efficient shared key-based EAP method is used. In the second scheme, the standard EAP method is skipped and the MS authentication is done by SA-TEK three-way handshake in PKMv2 process. This scheme is not suitable for implementation because it avoids the standard procedures. Pre-authentication mechanism that follows the least privilege principle to solve the domino effect and this handover protocol guarantees the backward and forward secrecy. But this pre-authentication scheme is not efficient and secure.

The straight forward way to deal with any attack is to verify each message before forwarding it. The fake messages should be dropped at the first-hop neighbors of the malicious nodes so that other nodes beyond do not get affected. Although this is preferable when dealing with fake messages, it has significant penalty on legitimate broadcast messages, because it takes time for nodes to conduct message authentication. For example, signature verification using 160-bit elliptic curve keys on at mega128, a processor used in Mica motes, may take as much as 1.6 seconds [9, 10]. If every node verifies the incoming packets before forwarding them, there will be a long delay for remote nodes The procedure of the EAP-Transport Layer Security (EAP-TLS) based authentication as shown in figure is one of the EAP-based authentication approaches that can provide strong mutual authentication.

It is selected as one of the options of the authentication schemes between the MS and the AS by the WiMAX forum. If you intend to use digital certificates to authenticate the client, Microsoft recommends that you use EAP-TLS rather than PEAP. Initially, the MS issues a link-up requesting message to the BS. The BS then relays the EAP message to the authenticator in the ASN. The EAP message is carried to the AS over the RADIUS. After the authentication process, the MS and the AS generate a MSK which is transferred to the authenticator in the ASN. The MSK is used by both the authenticator and the MS to generate PMK and authorization key (AK).

The AK is transferred to the hBS. It is used for SA-TEK 3-way handshake and key exchange. At the end of the authentication, both the MS and the BS share the Traffic Encryption Key (TEK) for data encryption. In a typical network connection, a MS asks a server to authenticate it.

The server returns the authentication approval to the MS, the MS acknowledges this approval, and then the MS is allowed to connect to the server. In a Denial of Service (DoS) attack, a MS sends multiple authentication requests to the server.

All the requests have false return addresses. So the server is in a predicament unable to find the MS when it tries to send the authentication approval. When the server closes the connection, the DoS attacker sends a new batch of forged requests and the process begins again causing the server to be unavailable for legitimate connections.

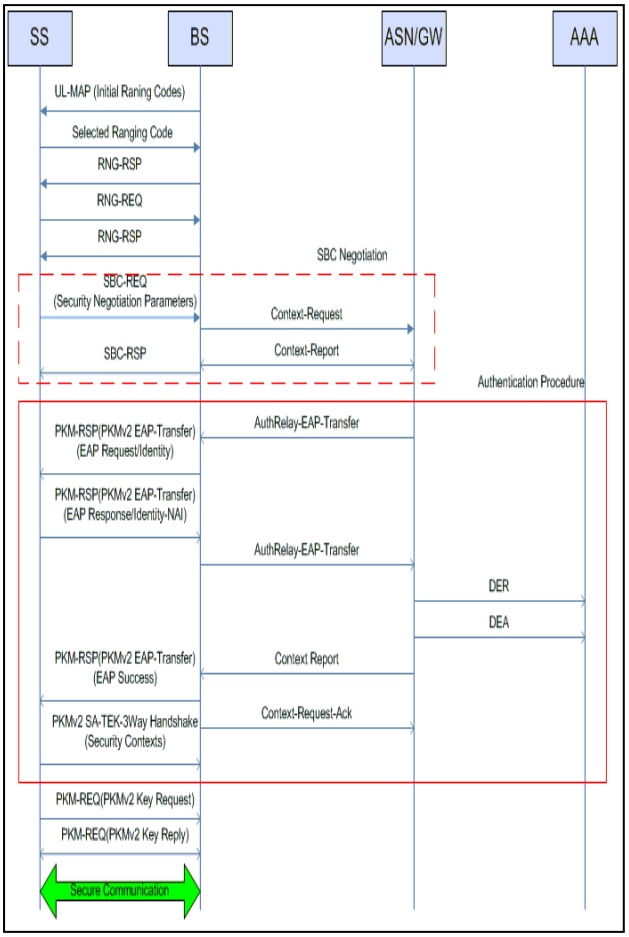

Figure 6: AUTHENTICATION PROTOCOL

A common method of blocking a DoS attack is to set up a filter in the network that looks for attacks by noticing patterns or identifiers contained in the information. If a pattern comes in frequently, the filter can be instructed to block messages containing that pattern, thus protecting the server from being overloaded by malicious attacks.

V. RESULT AND DISCUSSION

Convergence of mixed wireless networks has its own advantages and challenges. One type of network that is suitable for a particular application may not be appropriate for another type of application. A security mechanism that is effective in one environment may not be effective in the other. Also, there can be situations, where different types of networks coexist in one geographical area. The most significant of these is the first time association. Whether it is a LTE, a WLAN or a WiMAX, all wireless devices will have this setback.

The lack of physical connectivity (anchor-attachment) from the wireless device to the network makes the wireless network more vulnerable and hard to protect against authenticity, confidentiality, integrity and availability threats. Hence, to overcome this first time association problem wireless devices adopt a range of different techniques. Here we use PEAP for reduce time duration in data collection process.

COMPARISON CHART

THROUGHPUT

Throughput is the amount of data transferred in a given period of time. A higher throughput increases the network performance through improved packet delivery ratio and minimized packet delay.

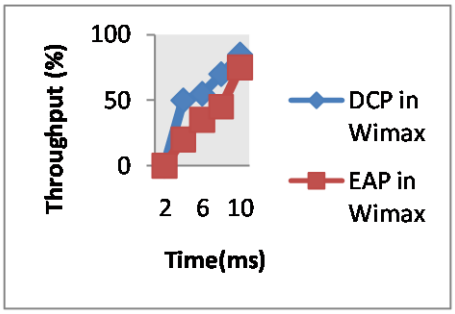

Figure.5.11 (a): Throughput

The curves in figure5.11 (a) compare the throughput of packets Vs time for the two methods; EAP and data collection process scheme (DCP). It clearly shows that the throughput of DCP method is higher than existing method for all time intervals calculated for the whole duration of 10 milliseconds. It is observed that for duration of 10 milliseconds the throughput of DCP is 90% while the throughput of EAP method is only about 75%.

The comparative analysis shows that the DCP delivers 20% more packets effectively than the existing method.

THE PACKET DELIVERY RATIO

The packets delivery fraction (PDF) refers to the ratio of packets transmitted and received from the source to destination successfully over the network. The figure compares the packet delivery fraction ratio of both the existing (EAP) and proposed (DCP) systems. As shown the PDF is 0% for the first 2 ms, since the transmission only starts after 2ms.

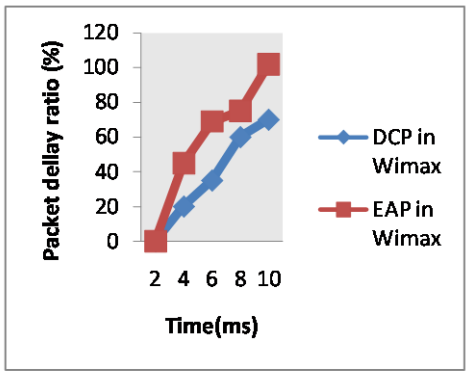

Figure.5.11 (b): The Packet Delivery Ratio

It is clearly evidenced that, for the entire duration of data transmission, the PDF values of DCP method is considerably higher than the EAP method. It shows that, through DCP method a PDF ratio up to 80% is achieved which is almost 12.5% higher than the existing method.

VI. CONCLUSION

The DCP-based Wireless networks have significantly different channel and network capacities. Using different routing protocols in wireless network by considering the realistic assault traces. To minimize the relay coil number, the MASP algorithm is provided. The MASP algorithm uses the shortest path tree to connect the entire wireless node with the optimal relay coil number. However, the network constructed by the MASP algorithm is used to reduce failure node and node displacement. We have using low propagation delay network to reduce delay and reduce relay coils in the network. To improve the network performance based on this MASP. In our future work to implement the spatial network performance and reduce delay, avoid traffic model on the network. The three metrics of PDR E2D THROUGHOUT are evaluated using AODV protocol in three density regions of low density, medium density and high density in network scene as well as in node point.

REFERENCES

[1]. Hua Cai, Dongmyoung Kim, Seunghyun Choi, "Measurement-Based Low-Level Performance Analysis of IEEE 802.16e/WiBro Networks", Feb. 2006.
[2]. Robert J. Zupko, "Introduction To IEEE Standard 802.16: Wireless Broadband Access", 2007.
[3]. Perumalraja Rengaraju,Chung-Horng Lung, Yi Qu, "Analysis on Mobile WiMAX Security", September 27-29, 2009.
[4]. Taeshik Shon, Bonhyun Koo, "Novel Approaches to EnhanceMobileWiMAX Security", 5 July 2010.
[5]. Ajay Roy and A.K.Jain, "Survey of Mobile WiMAX Networks IEEE 802.16 Standards", April 2010.
[6]. ANDREW WELLS-DANG, "Inside-Outside Advocacy And Virtual Networks In Preserving Reunification Park", 2011.

[7]. Tingting Sun, Bin Zan, Yanyong Zhang and Marco Gruteser, "The Boomerang Protocol: Tying Data to Geographic Locations in Mobile Disconnected Networks", IEEE transactions on Mobile Computing, vol 11, No.7,July 2012.
[8]. MARIO DI FRANCESCO and SAJAL K. DAS, GIUSEPPE ANASTASI., "Data Collection in Wireless Sensor Networks with Mobile Elements: A Survey", 2012.
[9]. S. MELBA, N.S. USHA. "An Effective Geocahe Collection in Mobile Networks Using Data Collection Protocol", 2013.
[10]. Vinothini.R, Sugapriya.M, Sudha.S, Srisakthi.C "Broadcasting Of Urban-Statistics via Vehicular Intellect DIAS",2013.
[11]. Pavan Mulgund1, Gayathri. "A Survey On Tying Data To Geographic Locations In Mobile-Disconnected Networks Using Data collection Protocol," 2013.
[12]. Pankaj Sharma, "Evolution of Mobile Wireless Communication Networks-1G to 5G as well as Future Prospective of Next Generation Communication Network", August 2013.
[13]. Z.H. Talukder, S.S. Islam, D. Mahjabeen, A. Ahmed, S. Rafique and M.A. Rashid, "Cell Coverage Evaluation for LTE and WiMAX in Wireless Communication System", Feb 2013.
[14]. H.F.Zmezm,S.J, S.J. Hashim, Aduwati Sali, "Fast and Secure Authentication Scheme in Mobile Wimax", January 2014.

Author's Details:

H.Lookman Sithic received his B.Sc degree from Bharathidasan University Trichy and M.S. (IT) degree from Bharathidasan University. He has completed his M.Phil at Periyar University. He is having 13 year s of experience in collegiate teaching and he is the Assistant Professor of computer science and applications in Muthayammal college of Arts and Science, Rasipuram affiliated by Periyar University. His main research interests include data mining, Network security.

S.Janane received her B.Sc., degree in Vivekanandha College of Arts and Science for Women from Periyar University, Tiruchengode (2006 - 2009) [TamilNadu (India)]. Then, did MCA degree in Vivekanandha College of Arts and Science for Women from Periyar University, Tiruchengode (2009-2012). She is the M.Phil Research Scholar of Muthayammal College of Arts and Science, Rasipuram. Periyar University, Salem. Her Area of interest is Networking.

