Distributed Security and Proliferate QoS in Handover Scheme

Jamyang Tashi, Tashi Wangchuk

Abstract— Today, the development of small cell deployment with overlay coverage or handling through coexisting heterogeneous network has worthwhile solution for 5G mobile network. The challenges faced in this is the security provisioning due to performing of more frequent mutual authentications in 5G small cells and heterogeneous network. In this article we review related studies and proposed Distributed Security in handover scheme to give Quality of Service by selecting best access point and secured routing. The best access network is chosen dynamically based on the Quality of Service parameters such as throughput, packet loss, and delay. The main purpose of this work is to provide prevention from impersonation and man-in-the-middle (MitM) attacks and to provide Quality of Service (QoS) and Quality of Experience (QoE).

Index Terms— Heterogeneous Network, WiMAX, Quality of Service, Denial of Service, Quality of Experience, Distributed Security and Proliferate, Downlink Channel Descripton.

———————————— u ————————————

1. INTRODUCTION

THE internet, Broadband Wireless Access (BWA) has been serving IT operators and enterprises for many years by providing the outmost services to the users. However, the new IP-based standard that was developed by the IEEE 802.16 is expected to speed up the adoption of the technology. According to the definition given in the IT Business Edge, the Worldwide Interoperability for Microwave Access (WiMAX) is a category of wireless communications standards originally intended to provide 30 to 40 megabit-per-second data rates with the 2011 update providing up to 1 Gbit/s for fixed stations. WiMAX is a standards-based technology, that is capable of delivering last mile wireless broadband access and it works an different to wired broadband like cable network and Digital Subscriber Line (DSL). WiMAX provides secure, roaming and portable mobile wireless broadband connectivity to the users without requiring of direct connection to the line-of-sight with a base station. In a characteristic of WiMAX, the cell radius deployment is of three to ten kilometers, The WiMAX Forum also certified TM systems can be likely to send capacity of up to 40 Mbps per channel for fixed and portable access applications. [1]

In parallel, the WiMAX platform forum, supported by industry leaders encourages the widespread implementation of broadband wireless access by introducing a brand for the technology and forwarding interoperability between products. [1]

IEEE 802 refers to a category of IEEE standards deals with the local area networks and metropolitan area networks. More specifically, the IEEE 802 standards are limited to networks transporting variable-size packets. The number, 802 was basically the next free number that IEEE could assign, though “802” is linked with the date the first meeting was held February 1980. [2]

The design of the WiMAX is one of the greatest challenges related with earlier versions of wired and wireless networks. At the same point, the backhaul connects the WiMAX system to the network, it is not an incorporated part of WiMAX system. In general, very similar to the other network, a WiMAX network consists of two parts, a WiMAX Base Station (BS) and a WiMAX receiver which we call it as Customer Premise Equipment (CPE). Backhaul is actually a connection to the system from the Access Point (AP) and back to the provider and connection back from the provider to the network. A backhaul can be placed any technology and medium provided, it connects the system to the backbone. In most of the WiMAX deployments circumstances, it is also reliable and most possible to

Jamyang Tashi and Tashi Wangchuk is currently working as Associate Lecturer in the Department of Information Technology, Jigme Namgyel Engneering College, Royal University of Bhutan, Bhutan
E-mail: jamyangtashi@jnec.edu.bt or jamyangtashi.jnec@rub.edu.bt and tashiwangchuk@jnec.edu.bt or tashiwangchuk.jnec@rub.edu.bt respectively

connect several base stations with one another by use of high speed microware links. This would permit for roaming by a WiMAX subscriber from one base station coverage area to another, similar to roaming enabled by cellular phone [3].

Man-in–the-middle attack is an intruder who gets in between the network system or network communication without the knowledge of the sender and the recipient [8]. They will try to access the traffic, modify the data and it forwards data to the other recipients in the network or sometimes drop the packets in between the network traffic. With the integration of WiFi into the worldwide coverage of a mobile operator, the mobile network architecture is as shown in Fig. 1, whereby many areas are covered with WiFi, LTE, and/or other access types. Mobile operators may confidently use WiFi as a backup network for their networks if and only if the WiFi backhaul network, or the fixed broadband connection, ensures a level of quality of service (QoS) similar to that provided by cellular networks. WiFi would indeed become a step down in performance in scenarios whereby a potential number of users simultaneously connect to WiFi while the communication path, in the backhaul [3].

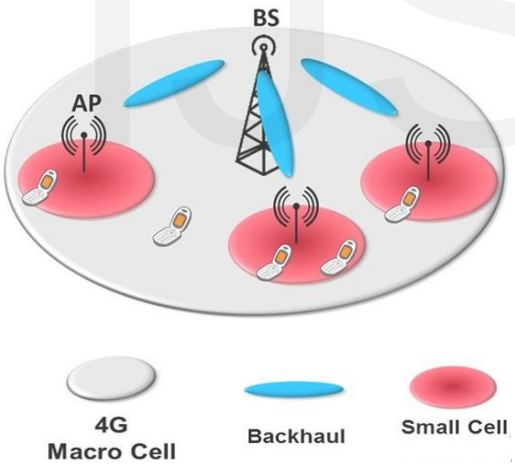

fig 1. 5G heterogeneous network

The rest of the paper is organized as follows. In Section II, some related works are described. In Section III, Proposed system and methods. In Section IV, Implementation and Expected Result. Finally Section V, concludes the works.

2. RELATED WORKS

The Framework for Quality of Service (QoS) support the Next Generation Networks (NGNs), that ensures end-to-end QoS guarantees of their point of attachment with the multi-interface terminals given. The framework supports media independent handover, triggered either user or network, to optimize network resources distribution [1]. This framework is generally providing the service guarantees, and also providing the operators the ability to reconfigure the distribution of network resources to optimize for the challenges in NGNs with a flexible and scalable solution.

A cognitive framework done by evolutionary algorithm, Swarm Intelligence, is proposed that framework using a novel approach that utilizes a cost function optimal parameters to provide a quality of service (QoS) based on the user's needs [2]. This kind of approaches makes an interoperability and scalability in different modulation methods in the physical layer and increases security against DoS attacks, jamming attacks, and signaling an attack. Modulations such as OFDM, W-CDMA, to evaluate real-time cognitive network are not incorporated in our work.

This system combining with two radio access technologies, IEEE 802.11 and IEEE 802.16 cognitive requirements [3]. Real-world handovers include responding to applications, operators, or users asking for higher data rates, lower costs, higher quality of service, or better traffic management, as well as to changes in mobility status or coverage. Voice Call Continuity (VCC) possibility to applies in 802.16m/802.11 Very High Throughput (VHT) handover. VCC increases network complexity [3]

The network selection or vertical handover procedure proposed in this paper is based on the mobility feature of a user and its prediction, and the load dynamics of the backhaul network of the available accesses and their prediction. Regarding the former, in [4], Nadembega et al. have proposed a scheme for the prediction of the entire or partial moving path of a vehicle, supported by the prediction of the final destination or intermediate points along the path based on historical records, contextual information, and spatial theoretical maps [5].

The two papers also present a brief overview on existing mobility modeling and prediction methods that can be of use in this work. Regarding the reflection of traffic dynamics of access backhaul networks in an admission control operation, a QoS/QoE predication-based admission control for deciding on handovers and flow mobility between a macro network and a small-cell network has been proposed in [6].

The network selection process has to consider attributes and criteria defined by the operator as well as the user [7]. Criteria defined by the user aim at maximizing his/her QoS (e.g., data rate and latency) and minimizing the communication cost. Criteria defined by the network operator are mainly related to network resource optimization (e.g., network utilization and load balancing between wireless networks). Sometimes, there is a conflict among these criteria; for instance, increasing user data rate may impact load balancing between networks. Several solutions have been proposed based on mathematical models or empirical solutions to find a tradeoff between user and operator requirements. Most of these solutions do not consider Quality of Experience (QoE) as a criterion for users and are based on an instantaneous sample of the criteria values to take the decision. On the one hand, it is generally agreed that Quality of Service (QoS) is not enough to model the user satisfaction; on the other hand, using instantaneous values is not efficient as these values do not reflect the long trend evolution of the criteria, which may result in wrong decisions. Combining mobility and Quality of Experience (QoE) prediction permits to create for each UE a list of APs to connect to in order to reduce exchanged messages and reduce the handover procedure, while maximizing user's QoE [6][7]

3. PROPOSED SYSTEM

The proposed modules assist in predicting the UE mobility features, predicting the available throughput of network and translating this information into a user satisfaction factor Quality of Experience(QoE) and implementing a network selection mechanism. Quality of Service enables a mobile operator to establish the list of APs a user of a User Equipments is likely going to visit during a time window of interest and to predict the mean satisfaction level the user is likely going to experience at each AP when connected to the AP. Based on these assessments, the mobile operator provides guidelines to the UE on which the AP is to connect to provide the highest Quality of Experience to the user. In proposed Distributed Security and proliferate Quality of Service framework, we consider mainly four criteria for the Multi Attribute Decision Making model, Quality of Service, Quality of Experience, Security, and Mobility.

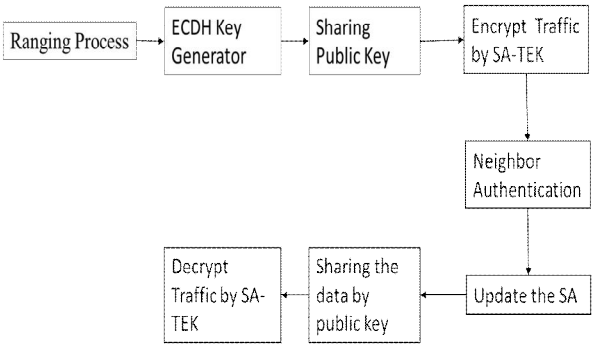

Fig 2 : Data Flow

From the above data flow diagram, it explains about network signal is captured and the flow of data in the network. Initially, it will start discovering the nearby Access Points (AP) and it generates Ecliptic Curve Deffie Hellman (ECDH) key. Then it will start sharing the public key between the neighboring nodes of the Access Points. Once it is done, then it encrypts the data by using the public key to authenticate the neighboring Access Points and it updates the Base Station. Once it reached the Base Station, the neighboring nodes will share the public key in order to decrypt the data by individual Access Points.

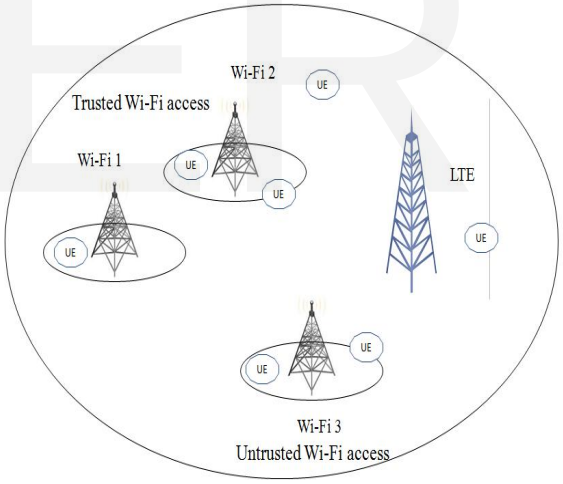

fig 3 : Network Architecture

In the figure 3, it is presenting the user an overall network architecture of mobile network system along with the other main components. We can clearly understand what are the components present in the system as every components plays a big role in it to function as a system. The mobile network system particularly consists of number of wireless domains consisting the Wireless Access Points (WAP) with same or different network technologies such as 4G or 5G. We are proposing the

Distributed Security and Proliferate QoS in Handover Scheme. We are using the centralized control system, so that the end user or Mobile device can discover the Access Point (AP) in the network and select the best network available the in the network with the policies defined dynamically or on demand by the User Equipment (UE).

In multihop Long-term Evaluation (LTE) networks, the security architecture defined by the 3rd Generation Partnership Project (3GPP) standard is a distributed scheme. On the other hand, selection of the distributed security mode in WiMAX is optional, but data transfer using the tunnel mode is still an open issue. Hence, we proposed the distributed security architecture using ECDH for multihop WiMAX networks. For multihop connectivity using ECDH, the cell-edge Radion Shack (RS) broadcasts its public key, ECDH global parameters, RS-ID, and system parameters in the Downlink Channel Descriptor (DCD) broadcast message. The MS/RS that wishes to join with access RS starts the ranging and connectivity process. After the initial connectivity, if the newly connected node is an RS, then the super ordinate RS will share the public key of the Base Station (BS) and the corresponding global parameters. The new RS will associate with the BS by sending its public key to the BS. Hence, the multihop RS can send its traffic over the tunnel mode. The SA and key management in the proposed security architecture. For multihop users, the access RS maintains the encryption and SA keys as similar to the BS, where the BS maintains the Security Association (SA) keys of single-hop MSs, RSs, and ECDH public key of multihop RSs. the BS maintains the SA and encryption keys of MS1, RS1, and RS2 as well as the ECDH public key of RS3. RS1 maintains the SA and encryption keys of MS2, MS3, and RS3. RS2 and RS3 maintain the encryption keys of MS4 and MS5, respectively. Suppose MS5 need to send an encrypted data in a tunnel mode, first, it encrypts the traffic using SA-TEK associated with RS3. Then, RS3 decrypts the traffic using SA-TEK and encrypts the data using BS's public key. Hence, the intermediate RS1 does not need to decrypt/encrypt the traffic. We propose neighbor authentication and SA for multihop WiMAX/LTE networks to avoid network coding security threats and secured pre-authentication for fast handovers. Providing fast-handover support improves the QoS performance of the vehicular networks. Consider the WiMAX network, if any new RS is connected to the network, the BS will inform the updated members list to the existing RSs group in a regular DCD message. Now, if the new RS finds another RS during channel scanning, it verifies whether the RS is genuine or not by verifying the RS-ID. Then, the new RS will send the public key and the RS-ID to the neighbor RS for establishing the SA.

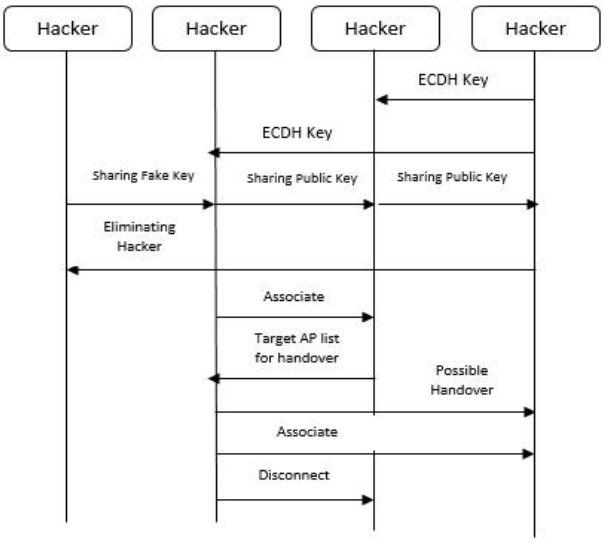

fig 4, Authentication process of Handover between same network and eliminating the hacker.

The Base Station will broadcast the signal to the open nearby nodes in which the it will send the ECDH key to Wireless LAN and User Equipments. Then Base Station will also request to share their public key in order to authenticate and establish the communication. If the Hackers comes in to the networks, then the Hacker may send the fake response to the Base Station. The Base Station will eliminate the hacker's node from the network. At the same time, the User Equipments will associate with Wireless LAN and it will request for Handoff, then Wireless LAN will list the possible Access Points to handoff. It will also associate with the Base Station and disconnect from Wireless LAN.

Coming to the Network Selection Based on Multi Dissemination Protocol (MDP), we can assume that the decision on whether to use a macro cell or a WiFi cell (if both are available) are done every t s (i.e., decision epochs = t s).

The set of decision epochs is denoted as $T = \{1, 2, 3, \ldots, K\}$.

Intuitively, when only one Radio Access Technology (RAT) is available, no decision optimization takes place. To retrieve an optimal policy for deciding to which RAT a UE has to attach, we define an MDP that associates with each state an action, corresponding transition probabilities, and rewards. Let st be the process describing the evolution of the system state. Let S denote the state space. A state s is composed by

the type of the network currently used by the UE and the current QoE perceived at the macro cell and the QoE perceived at the WiFi cell.

4. IMPLEMENTATION AND EXPECTED RESULTS

This paper, it generally discussed about the enhancing the security in terms of protecting the attack such as Man in the middle attack, impersonation attack and target based attack. We would be using the Ecliptic Curve Deffie Hellman key exchange the public key in order to avoid those attacks. In most of the current practices, it is either attacked by man in the middle attack or impersonation attack since they use the pre share key. The Heterogeneous is the techniques used in this proposed system as would enhance the mobility of the user. The study can be taken up in the broader prospective as it needs lots of time and resources to analyze the output of the work. It is expected that it would enhance the security in the mobile communication by protecting the data using the Diffie Hellman algorithm and other encryption mechanisms.

5. CONCLUSION

With the development of the small cell deployment with overlay coverage through coexisting heterogeneous network has viable solution for 5G mobile networks. Many users in the network face the different kind of problems in exchanging the mobile communication. To overcome those challenges and difficulties, the proposed work that would perform more frequent mutual authentications in 5G small cells and heterogeneous network. In this whole paper, we were discussing about the studies related to Distributed Security in handover scheme to give Quality of Service by selecting best access point and secured routing. The best access network is chosen dynamically based on the Quality of Service parameters such as throughput, packet loss, and delay. It is aimed at the providing the prevention from impersonation and man-in-the-middle (MitM) attacks and to provide Quality of Service (QoS) and Quality of Experience (QoE).

REFERENCES

[1] An End-to-End QoS Framework for cognitive Mobile Heterogeneous Environments, Miguel Almeida, Daniel Corujo, Susana Sargento, Vítor Jesus, Rui L. Aguiar.

[2] Increasing QoS and Security in cognitive Networks Using Cognitive Intelligence RajaniMuraleedharan and Lisa Ann Osadciw.

[3] Mobility using IEEE 802.21 in a heterogeneous IEEE 802.16/802.11-based,it-advanced (cognitive) network.

[4] A. Nadembega, A. Hafid, and T. Taleb, "A path prediction model to support mobile multimedia streaming," in *Proc. IEEE ICC*, Ottawa, ON,Canada, Jun. 2012, pp. 2001–2005.

[5] A. Nadembega, T. Taleb, and A. Hafid, "A destination prediction modelbased on historical data, contextual knowledge and spatial conceptualmaps," in *Proc. IEEEICC*,Ottawa, ON, Canada, Jun. 2012, pp. 1416–1420.

[6] T. Taleb and A. Ksentini, "QoS/QoE predictions-based admission control for Femto communications," in *Proc. IEEE ICC*, Ottawa, ON, Canada, Jun. 2012, pp. 5146–5150.

[7] Mathematical Modeling for Network Selection in Heterogeneous Wireless Networks.

[8] Kapil M. Jain, Manoj V. Jain, Jay L. Borade available on http://www.ijste.org/articles/IJSTEV2I9103.pdf