東海大學資訊工程學系研究所

碩士論文

指導教授：呂芳懌

Dr. Fang-Yie Leu

使用 MIH 和 CRRM 在相互信任或不信任環境下之換手機制

MIH and CRRM Assistant Handover in Mutually Trusted or Untrusted Network Environments

研究生：吳美瑜

中華民國　108　年 7 月 14 日

東海大學碩士學位論文考試審定書

東海大學資訊工程學系 研究所

研究生 吳 美 瑜 所提之論文

使用 MIH 和 CRRM 在相互信任或不信任環境下之換手機制

經本委員會審查，符合碩士學位論文標準。

學位考試委員會

召 集 人 ________________ 簽章

委 員 ________________

____

____

指 導 教 授 ________________ 簽章

中華民國 108 年 7 月 14 日

中文摘要

在跨區域的通訊系統中，當移動節點（簡稱 MN），如手機。進入一個網路的邊界時，須考慮到家網路（簡稱 H-Net），服務網路（簡稱 S-Net）和目標網路（簡稱 T-Net）三者之間相互的關係，三個移動運營商(mobile operators)之間彼此是否相互信任。在兩個相互不信任的網路之間進行無縫切換是一個巨大的工程挑戰，因為它需要即時地互通兩個網路個基地台運作狀態的信息。在這種不受信任的環境，意味著若 MN 要換手至其目標網路的過程將會更加複雜，且需花更長的時間。此外，S-Net 和 T-Net 可能是同構的或異構的網路環境。前者表示它們屬於相同的網路模型，例如，兩者都是 LTE-A 系統；後者則是它們是不同的網路環境，例如，一個是 LTE，另一個是 Wi-Fi。在換手的過程中，同質換手不管是消耗的資源或時間等都是優於異質換手。

在本研究中，我們考慮 H-Net、S-Net、T-Net 之間是信賴/不可信賴的關係時，該如何改善換手過程。並提出一個多參數演算法，所考慮的參數包括 MN 的移動方向、Received Signal Strength、同質和異質和服務品質和中延遲，單位時間之工作量及封包拋棄率等，目的是選擇合適的目標基地台，我們也使用媒體獨立換手服務(IEEE 802.21 Media Independent Handover)及 Common Radio Resource Management (CRRM)，來幫助移動過程中的移動節點(Mobile Node 簡稱 MN)順利地換手。實驗結果顯示，利用多屬性參數基地台的決策，能提升 MN 待在基地台的時間，能使 MN 獲得較好的服務品質。

關鍵字: 基地台選擇、換手服務、多屬性參數基地台決策演算法、非相互信任網路

Abstract

In a cross-region communication system, when a mobile node (referred to as MN), such as a mobile phone, reaches the boundary of a network, it is necessary to consider the relationship among the home network (H-Net), the service network (S-Net) and the target network (T-Net), and whether the three mobile operators mutually trust each other or not. Handover between two mutually untrusted networks is a huge engineering challenge because it needs to exchange base station information of the two networks in real time. In this untrusted environment, the process for MN to hand over from S-Net to its T-Net will be more complicated and take longer time than that when S-Net and T-Net are mutually trusted. Besides, S-Net and T-Net may be homogeneous or heterogeneous. The former indicates that they belong to the same network model, e.g., both are LTE-A systems; the latter is that they are different network environments, e.g., one is LTE and the other is Wi-Fi. Generally, homogenous handover consume less resource and time than heterogeneous handover does. In this study, we consider how to improve the handover process when the relationship among H-Net, S-Net and T-Net are mutually trusted/untrusted. We propose a multi-parameter algorithm, in which parameters include MN's moving direction, RSRQ, homogeneity and network (delay, throughput and drop rate are addressed, aiming to select a more appropriate target base station for MN. We also use the Media Independent Handover service (IEEE 802.21) and Common Radio Resource Management (CRRM) to help the process of MN handover. Our experimental results show that the decision of using the multi-attribute parameter base station can improve the time that the MN stays at the base station, and the MN can obtain better service quality.

Key word: Base station selection, handover, multi-attribute parameter base station decision algorithm, non-mutual trust network

Table of Contents

List of Figures

List of Tables

I. Introduction

In recent years, people rely on wireless network systems to communicate with their outside worlds, no matter whether at home or somewhere in the world. These network systems allowing users to contact their friends or business partners anytime and anywhere have gradually become a part of our everyday lives. On the other hand, due to convenient transportation, people can go to anywhere they like. It means that the places people can reach have no longer limited to their Home Networks (H-Net).

When MN moves to a network which is not its H-Net, we say the MN is roaming. Also, as MN comes to a network's boundary, the trusted relationship among H-Net, Serving Network (S-Net) and Target Network (T-Net), and whether H-Net, S-Net, and T-Net are members of the same alliance need to be addressed. If they belong to the same alliance, we call them, e.g., M and N, mutually trusted network (MT-Net), meaning that the two operators have signed a contract promising to provide network services to users of the other operators. In other words, M will provide network services to N's MN and vice versa. However, if M and N do not belong to the same alliance, we call them mutual untrusted network (MU-Net), implying that the procedure for M (N) to authenticate N' (M') MN will be more complicated, of course, spending a longer time [1].

There are many countries in the world and often there are several operators in a country. Roaming services have flourished over the past few years. Currently, if MN would like to roam to a network, i.e., T-Net, and the T-Net and MN's H-Net are MT-Net, MN can receive network services from T-Net. Otherwise, the NM may not access wireless services it requires from T -Net. Also, 5G networks (or Simply 5G) adopts small cells, the communication ranges of which are smaller than that of a macro cell. Therefore, given an area, when MN passes through this area, the handover frequency in 5G will be higher than that in 4G. For MN, this will contradict the principle of reducing the number of MN's handover. Furthermore, existing base station selection schemes during handover select base stations mostly based on Reference Signal Received Power (RSRP), Reference Signal Received Quality (RSRQ) or Signal to Interference Noise Ratio (SINR). As a result, when a group of MN, like those in a bus or a train, needs to hand over, most MNs will contact the MAG with the strongest signal. Its load is then heavy. Consequently, its QoS may be not as expected.

In this study, we propose a multi-parameter (MP) algorithm and a third-party mechanism to solve the above mentioned problems. The parameters used by the MP algorithm include MN's moving direction, MN's moving speed and the angle between the MN's moving direction and arrow from MN to the candidate MAG, RSRQ and MAG's delay, throughput, drop rate, etc. to select an appropriate target base station for MN. The purposes are to reduce the number of handover and avoid communication QoS reduction.

Further, third party acts as a bridge between two mutually untrusted operators that have individually signed a contract with the Third party. For example, operators A and B have individually signed a contract with the Third party. The users of operator A (or B) are allowed to access network services provided by B (A) with the help of a Third party.

The rest of this study is organized as follows. Chapter 2 introduces the background and related studies of this paper. Chapter 3 describes the architecture of the proposed system and the process of MN handover. Chapter 4 presents and discusses the experimental results. Chapter 5 summarizes this article and describes our future studies.

II. Background and Related work

In this section, we briefly overview background and related work of this study.

2.1 IEEE 802.21

IEEE 802.21 Media Independent Handover (MIH for short) [2] allows users to select one base station as NMAG which may be a base station of 802.3, 802.11, 802.16, 3GPP or 3GPP2 networks. The purposes of employing MIH architecture is enabling low-latency handover across multiple technology access networks, helping handover decision making, standardizing functions to gather network characteristics, formalizing command procedures for MN to seamlessly hand over and supporting both station-initiated and network-initiated handover. As shown in Figure 1, MIHF is a 2.5-layer system built in MNs, MAGs and LMAs. The Media Independent Handover Function (MIHF) is one of the features of MIH. MIH provides three services, including Media Independent Command Service (MICS), Media Independent Event Service (MIES) and Media Independent Information Service (MIIS). If MN needs to hand over, the MICS will help the MN to issue required commands. MIES monitors the network and then stores the collected information in the MIIS server.

MIH accesses other layers through Services Access Points (SAPs) [2]. MIH SAP is the interface between the MIHF layer and the upper layer. MIH LINK SAP is the interface between MIHF and its lower layers. MIH NET SAP is the interface for information exchange between MIHF and another MIHF.

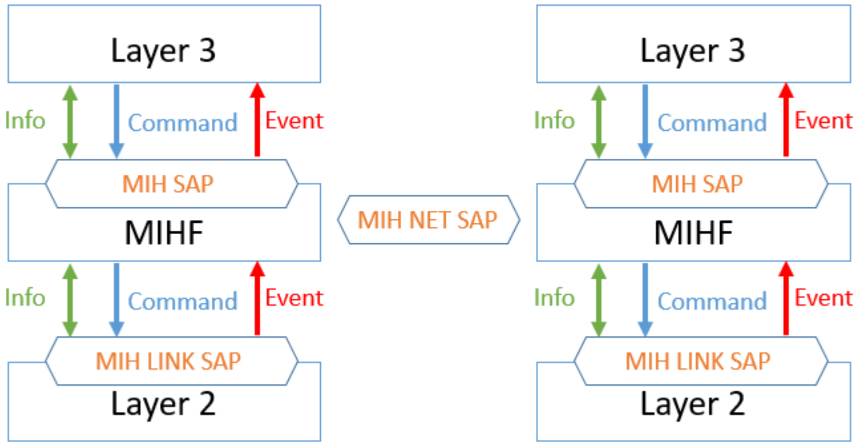

Figure 1. MIH Function [3,4,5]

2.2 The Common Radio Resource Management

The Common Radio Resource Management (CRRM) is a two-tier Radio Resource Management (RRM) model [6-8], consisting of CRRM and RRM entities, as shown in Figure 2. The RRM entity is located at a lower layer to coordinate with Remote Radio Head (RRH for short) in multiple Radio Access Technologies. CRRM entity located at the upper of the two-tier RRM model controls multiple RRM entities, communicates with other CRRM entities and manages the RRM entities for collecting information, so the CRRM entity can know the availability of RRH of multiple RATs and assign users to the most appropriate RATs.

Messages transmitted between RRM and CRRM entities provide two basic features. The first is message report that allows an RRM entity to report information to its controlling CRRM entity. The information can be delivered periodically or triggered by events [9]. The message report feature is also used for information exchange and sharing between different CRRM entities, as shown in Figure 2. The second feature is RRM decision. There are two decision methods. One is CRRM-centric, with which CRRM entity makes decisions and notifies

RRM entities to follow. The other is that CRRM entity only recommends RRM entity to do something, and the final decision is made by the RRM entity.

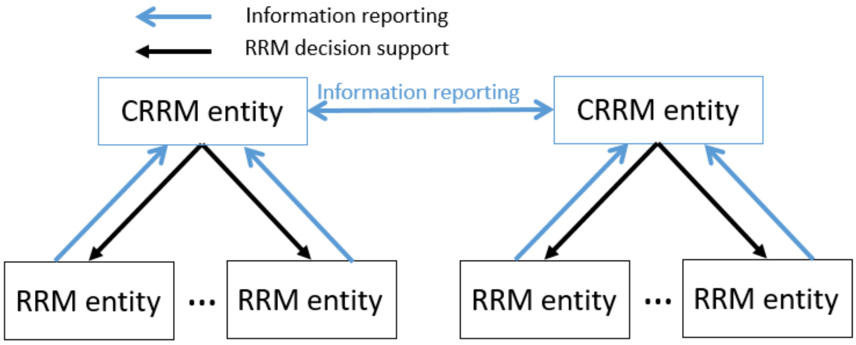

Figure 2. CRRM interaction model.

2.3 EPS-AKA

EPS Authentication and key agreement (EPS-AKA) is a security protocol for mutual authentication between users and operators. As shown in Figure 3, both MN and it's operator's HSS hold the key K of the MN. MN and the HSS/MME use EPS-AKA to authenticate each other. The procedure is as follows. Step 1: MN transmits an Attach Request (including IMSI, MN Security Capacity, KSI_{ASME}, ...) to eNB. eNB passes the message to MME; Step 2: On receiveing the Attach Request, MME processes the message and sends Authentication Data Request (containing IMSI, SN ID, Network Type, ...) to HSS; Step a: HSS retrieves MN's parameter K from its database based on the IMSI carried in the message, and checks the validation of the SN ID. If at least one of the IMSI and SN ID does not belong to the network, the HSS terminates the authentication. Otherwise, HSS generates n sets of authentication vectors (AVs for short), each of which contains RAND||XRES||AUTN_{HSS}||K_{ASME}, and transmits Authentication Data Response carrying the n AVs to MME.

The MME chooses an AV, retains XRES and K_{ASME} of the AV, and sends

User Authentication Request (including RAND, AUTN_{HSS}, KSI_{ASME}, ...) to MN. After that, MN generates the same parameters with some parameters of its own and some conveyed in the User Authentication Request message sent by MME, and compares AUTN_{HSS} with the AUTN_{MN} generated by itself, to authentiate the network. If they are not equal, MN drops the message and starts contacting other eNB. Otherwise, meaning that the netowork is valid, MN sends Authentication Data Response (carrying RES) to MME. MME checks to see whether or not RES and XRES are equal. If yes, the network completes the authentication on the MN, i.e., the entire EPS-AKA program is finished. MME informs eNB to start serving MN. In the Figure3, steps a~d are actions individually performed by HSS, MME, and MN.

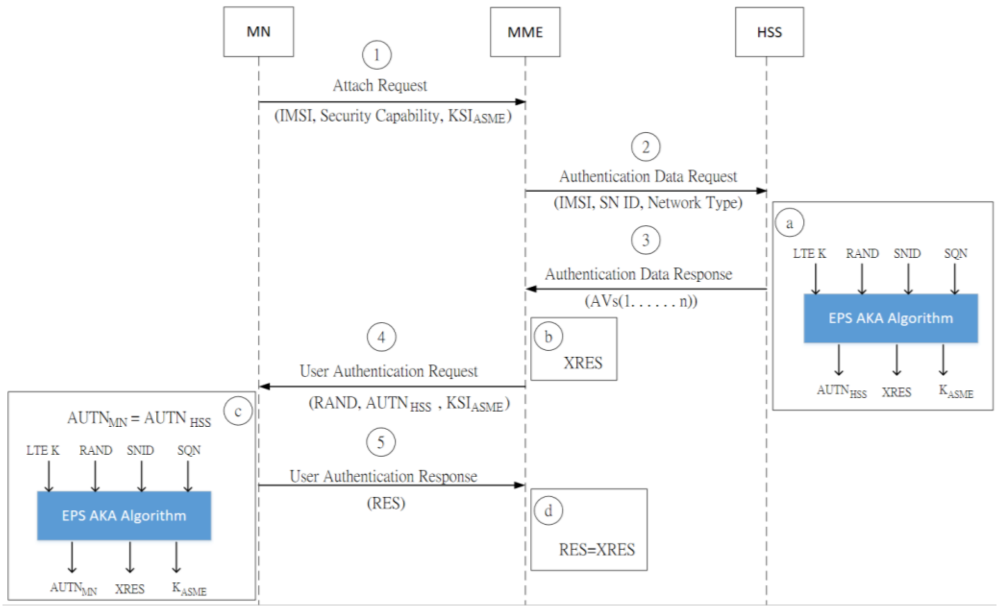

Figure 3. The sequence chart of EPS-AKA [10,11,12]

2.4 Mutually Untrusted Network

In an U-Net, S-Net, e.g., M, and T-Net, e.g., N, may be homogeneous or heterogeneous. Assume that M's MN needs to hand over to N. But M's LMA does not have the information of N's MAGs, thus unable to select an appropriate MAG for MN. Usually the handover will enter its reactive mode, and its procedure is as follows: When MN enters the communication range of an MAG, and decides to contact the MAG as its NMAG, it first disconnects its own connection with the M's MAG (PMAG) and then connects to the NMAG. Of course, N requires to authenticate MN with the help of H-Net HSS. However, in an MU-Net, the N's HSS cannot directly request H-Net HSS to authenticate the MN. Consequently, the MN will lose network services until MN moves to a network that is mutually trusted with MN's H-Net. Then, the MN can access network services again [1].

2.5 Multi-attribute Decision Making

Multi-attribute Decision Making (MADM for short) as a decision characterized by multiple attributes has been applied to a wide range of applications. There are three different multi-attribute scoring methods that have been employed by the MADM [13]. The first is including Simple Additive Weighting method (SAW), second is Weighted Product Method (WPM), and the third is Technique for Order Preference by Similarity to Ideal Solution (referred to as TOPSIS). Among them, in this study, we adopt SAW, which was proposed in 1981 [14]. It has been widely used in MADM because its content is simple and easy to operate, and does not cause too much burden on the system. Its scoring procedure consists of three steps. The first is normalizing all attributes in different units so as to integrate these attributes for further calculation. The second is multiplying each of the normalized attribute values by the attribute's own weight. Finally, adding the weighted values of the attributes as the score of the evaluated item.

2.6 Related Work

Kishida *et al*. [15] adopted the angle between the MN's moving direction and the connection connecting MN and an MAG, as one of the features for base-station selection, and compared performance of those MAGs on different angles. Due to considering the relative positions of MAGs, the probabilities of those MAGs with smaller angles for MN's handover are higher. Authors also showed that GPS error has little influence on MAG selection. Tartarini *et al*. [16] used a Software-defined mechanism to choose MAG when MN hands over in a heterogeneous environment. Authors set different SINR thresholds according to MN's different moving speeds, aiming to reduce the chance of handover failure. Leu *et al*. [1] employed MIH and third-party entities to assist base-station selection when MN hands over in an MU-Net, and proposed an algorithm to select a better MAG for MN.

Wang *et al*. [17] proposed an enhanced MIH architecture and developed seamless mobility management capabilities to enhance MIH. But this also increases the message delivery overheads. Buiati *et al*. [18] presented layered MIIS architecture to reduce MIIS response times and the delay of heterogeneous vertical handover. Zeng *et al*. [19] adopted this method to select the best network service. Ipaye *et al*. [20] utilized several MADM scoring methods to select the best base station based on QoS (delays, bandwidths, costs and jitters) of these base stations.

In contrast to these studies, to complete handover in untrusted network environment, we added a Third party to this environment, and selected the appropriate MAG for the MN with the corresponding handover algorithm.

III. Proposed Scheme

In the following, we introduce the relationship among S-Net, T-Net and H-Net.

3.1 The relationship among S-Net, T-Net and H-Net.

We first study the cases when MN hands over from S-Net (rather than from H-Net) to T-Net to continue its network access. In fact, serving, home and target network (referred to as H, S and T, respectively) have different trusted/untrusted relationships with each other. It can be summarized to 2^3 combinations, where 2 indicates the trusted and untrusted relationship. The 8 relationships are as follows:

1. ((H-T: trust), (H-S: trust), (S-T: trust))
2. ((H-T: trust), (H-S: trust), (S-T: untrusted))
3. ((H-T: trust), (H-S: untrusted), (S-T: trust))
4. ((H-T: trust), (H-S: untrusted), (S-T: untrusted))
5. ((H-T: untrusted), (H-S: trust), (S-T: trust))
6. ((H-T: untrusted), (H-S: trust), (S-T: untrusted))
7. ((H-T: untrusted), (H-S: untrusted), (S-T: trust))
8. ((H-T: untrusted), (H-S: untrusted), (S-T: untrusted))

When the MN enters the S-Net, no matter whether the relationship between H-Net and S-Net is trusted or untrusted, T-Net has to authenticate this MN and serves as MN's new S-Net to provide MN with network services. In fact, during handover the focuses are whether S-Net can directly access information and statuses of T-Net's base stations or not and whether T-Net can directly request H-Net to authenticate this MN or not. There are no needs for S-Net to contact H-Net. It means that the above eight combinations can be simplified into four since those that contain (H-S: trust) and (H-S: untrusted) are ignored and removed. Thus, only

((H-T: trust), (S-T: trust)), ((H-T: trust), (S-T: untrusted)), ((H-T: untrusted), (S-T: trust)) and ((H-T: untrusted), (S-T: untrusted)) remain. We will describe them below.

3.1.1 ((H-T: trust), (S-T: trust))

Because of (S - T: trust), when PMAG's RSRQ on MN is lower than its predefined threshold, MN needs to hand over. As shown in Figure 4,

(1) MN sends MIH_Net_Mesurement_report, which contains ($IMSI$, $RSRQ_{PMAG}$, v, $\text{Service\_charge}_{MN}$, ($MAG_1\_SNID$, $RSRQ_{MAG_1}$, $\theta_{\overrightarrow{MN}\_MAG_1}$, $R_{MAG_1\_MN}$), (MAG_2_SNID, $RSRQ_{MAG_2}$, $\theta_{\overrightarrow{MN}\_MAG_2}$, $R_{MAG_2\_MN}$), ..., (MAG_n_SNID, $RSRQ_{MAG_n}$, $\theta_{\overrightarrow{MN}\_MAG_n}$, $R_{MAG_n\_MN}$)), to PMAG, where IMSI is the MN's international mobile subscriber ID, $RSRQ_{PMAG}$ is PMAG's RSRQ on MN, v is MN's moving speed, $\text{Service\_charge}_{MN}$ is the charging policy signed by the MN and its operator, and the four parameters, (MAG_i_SNID, $RSRQ_{MAG_i}$, $\theta_{\overrightarrow{MN}\_MAG_i}$, $R_{MAG_i\_MN}$), are the features of the candidate MAG$_i$, representing MAG$_i$'s SN ID, RSRQ on MN, the angle of the MN's moving direction and the line connecting the MN and MAG_i, and the linear distance from the MN to MAG_i, respectively, for all is, $1 \leq i \leq n$. The four parameters are enough for our system because other information concerning a candidate MAG will be collected by using MIH_Link_Mesurement_report which is sent by surrounding MAGs/CRRMs and will be described in the following.

(2) PMAG sents MIH_HO_Indication_request, which carrie ($IMSI$, $PMAG\ SNID$, $CMAG\ SNID$, $RSRQ_{PMAG}$, v, $\text{Service\_charge}_{MN}$, ($MAG_1\_SNID$, $RSRQ_{MAG_1}$, $\theta_{\overrightarrow{MN}\_MAG_1}$, $R_{MAG_1\_MN}$, $\text{Service\_charge}_{MAG_1}$), ($MAG_2\_SNID$, $RSRQ_{MAG_2}$, $\theta_{\overrightarrow{MN}\_MAG_2}$, $R_{MAG_2\_MN}$, $\text{Service\_charge}_{MAG_2}$), ..., ($MAG_n\_SNID$, $RSRQ_{MAG_n}$, $\theta_{\overrightarrow{MN}\_MAG_n}$, $R_{MAG_n\_MN}$, $\text{Service\_charge}_{MAG_n}$)),

to CRRM in its LMA, and asks the CRRM to choose a suitable MAG for MN to hand over.

(a) The LMA uses the parameters sent by the MN and the parameters collected in the MIIS to calculate the scores for all candidate base stations, and then selects one, e.g., MAG X. The parameters in the MIIS are the data sent by the nearby base station periodically or on demand. The data carried in the MIH_Link_Mesurement_report includes the QoS and related information, including (SNID, LD, D, End to end delay, Throughput and Drop rate), of an candidate MAG where LD is the load of MAG X, D is the communication range of MAG X. The latter three are this MAG-X's QoS parameters.

(3) The CRRM sends MIH_HO_Indication_request2 which conveys (IMSI, PMAG_SNID, CMAG_SNID) to MAG X's LRRM, telling it that MAG X has been selected as the NMAG.

(4) The LMA/CRRM transmits MIH_HO_Indication_report to the PMAG and the CMAG, and then PMAG and CMAG can individually connect to NMAG.

(b) MN establishes L2 connection with NMAG.

(5) EPS-AKA is performed.

(c) A connection between PMAG and NMAG and one between NMAG and CNAM are established by using the information exchanged in steps (3) and (4). The former connection is utilized to transfer those packets delivered to MN by CN during MN's handover from PMAG to NMAG since before this connection is established, these packets are temporarily retained in the PMAG. The latter connection is employed to continue the communication between MN and CN after handover.

(d) NMAG then notifies its Radio Resource Control (RRC) to reserve network resources for MN.

(6) NMAG delivers MIH_HO_Indication_response2, containing (NMAG_SNID, upload/download channels reserved for MN), to CRRM.

(7) The CRRM transmits MIH_HO_Indication_response, conveying (IMSI, information of resources reserved by the PMAG for the MN), to the PMAG. PMAG then releases all these resources, and the MN starts using NMAG's network resources.

In Figure 4, steps (a), (b), (c) and (d) are internal actions, rather than messages, performed by LMA, (MN and NMAG), (PMAG and NMAG), and NMAG.

When MN is connected to the T-Net, due to (H - T: trust), T-Net HSS (T-HSS for short) asks MN's H-Net HSS (H-HSS for short) to authenticate MN. In Figure 4, the blue rectangle represents the authentication steps (steps from 5-1 to 5-6), some of which may be omitted based on required security levels. For example, if PMAG and NMAG belong to the same LMA and the connection security level required is low, authentication is unnecessary. If PMAG and NMAG belong to different LMAs, there are two cases: First, the two LMAs belong to the same operator. Then authentication is not needed after MN hands over. Otherwise, meaning that the LMAs are managed by different operators, authentication is often required.

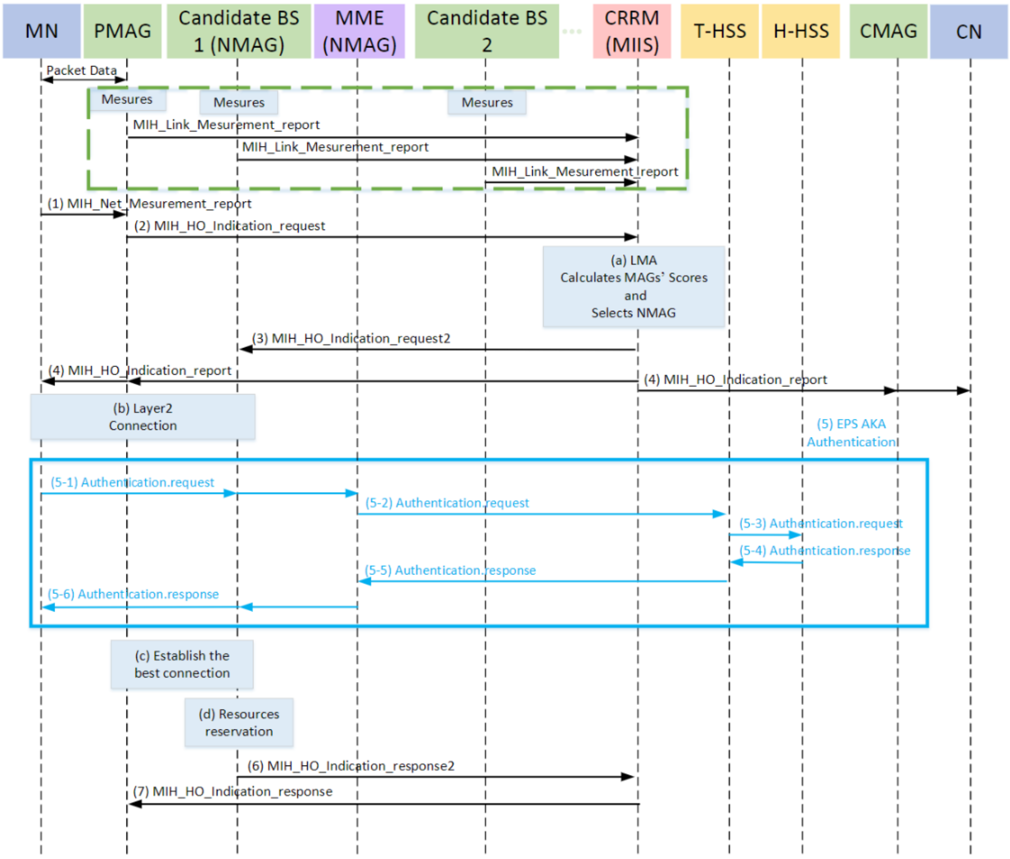

Figure 4. The sequence chart of ((H-T: trust), (S-T: trust)).

3.1.2 ((H-T: trust), (S-T: untrusted))

Because of the (S - T: untrusted), S-Net cannot directly obtain the information of nearby T-Net MAGs. The information needs to be collected by a Third party, either periodically or on demand. The green dashed box in Figure 5 shows that the MAG periodically sends messages to the Third party, without showing on-demand messages. As shown in Figure 6, if PMAG requests handover in time period A, since the data is still fresh, the Third party uses the data currently stored in MIIS. Otherwise, meaning that the request is issued in time period B, since the data is a little out of date, the Third party initiates a request for MAG to report its current status, including the base station load, the communication range of the base station and QoS data, etc. (Please also refer to step2 of ((H-T: trust),(S-T: trust)))

As in step (a) of Figure 5, the LMA of the Third party calculates the scores for all MAGs near the PMAG, and selects one as the NMAG for the MN according to the scores. In step (3), the LMA informed the NMAG that it was selected by sending MIH_HO_Indication_Request2 which carries the same information listed in step (3) of ((H-T: trust), (S-T: trust)). In step (4), LMA notifies MN that this MAG is its NMAG by sending MIH_HO_Indication_report. In step (5), after the MN is connected to the NMAG, the corresponding authentication starts.

Because of the (H - T: trust), T-HSS directly requests H-HSS to authenticate MN without passing the request through the Third party.

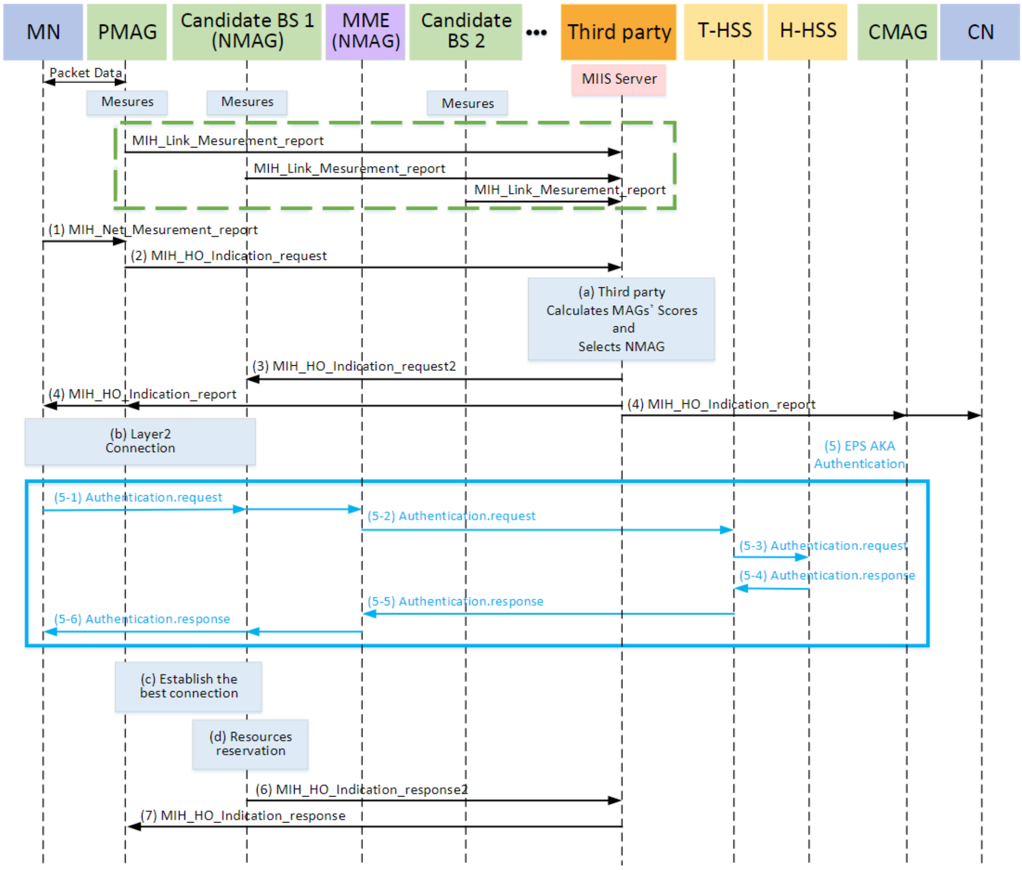

Figure 5. The sequence chart of ((H-T: trust), (S-T: untrusted)).

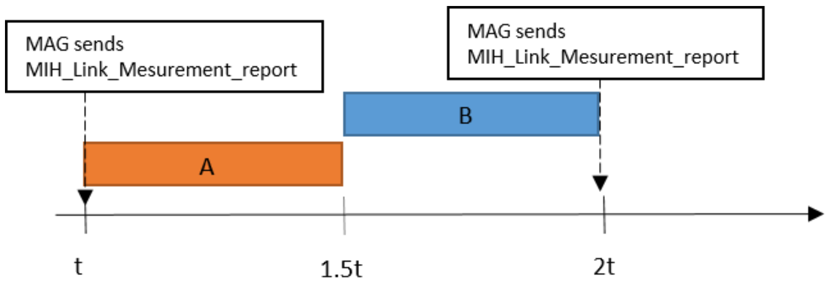

Figure 6. Timing of data collection. If handover information is requested at timing A, MIIS provides existing information; if handover is requested at timing B, MIH will request LMA/CRRM or the Third party to collect new information, store it in MIIS, calculate scores for MADs and choose NMAG for MN.

3.1.3 ((H-T: untrusted), (S-T: trust))

Because of the (S-T: trust), the methods that collect data from the base stations and select one as the NMAG are the same as those of ((H-T: trust), (S-T: trust)). In step (a) of Figure 7, the LMA calculates the scores for all base stations near PMAG, and then selects a suitable one as the NMAG for the MN based on the scores. In step (3), the LMA/CRRM informs NMAG that it is selected by sending MIH_HO_Indication_request2. In step (4), it notifies MN which base station will serve as its NMAG. Of course, if MN is connected to CN, MIH_HO_Indication_report will also transmit to CN. After that, the MN can establish L2 connection with NMAG. In step (5), HSS completes the MN authentication.

The authentication procedure of (H-T: untrusted) is a little different from that of (H-T: trust). In step (5), we need a trusted Third party to authenticate the MN. To ensure the security of the authentication process, two VPN channels are required, one between H-HSS and the Third party and the other between the Third party and T-HSS (see steps from (5-3) to (5-6) in the red box (denoted by VPN) of Figure 7). The messages delivered for authentication are passed through the two VPN tunnels.

As shown in Figure 8, when T-Net and H-Net are untrusted, meaning that there is no direct channel between them, messages exchanged between them must be delivered through the Third party, i.e., via VPN1 (VPN2) established between the Third party and the T-HSS (H-HSS). The authentication messages of ((H-T: untrusted), (S-T: trust)) and ((H-T: untrusted), (S-T: untrusted)) are all delivered with this method.

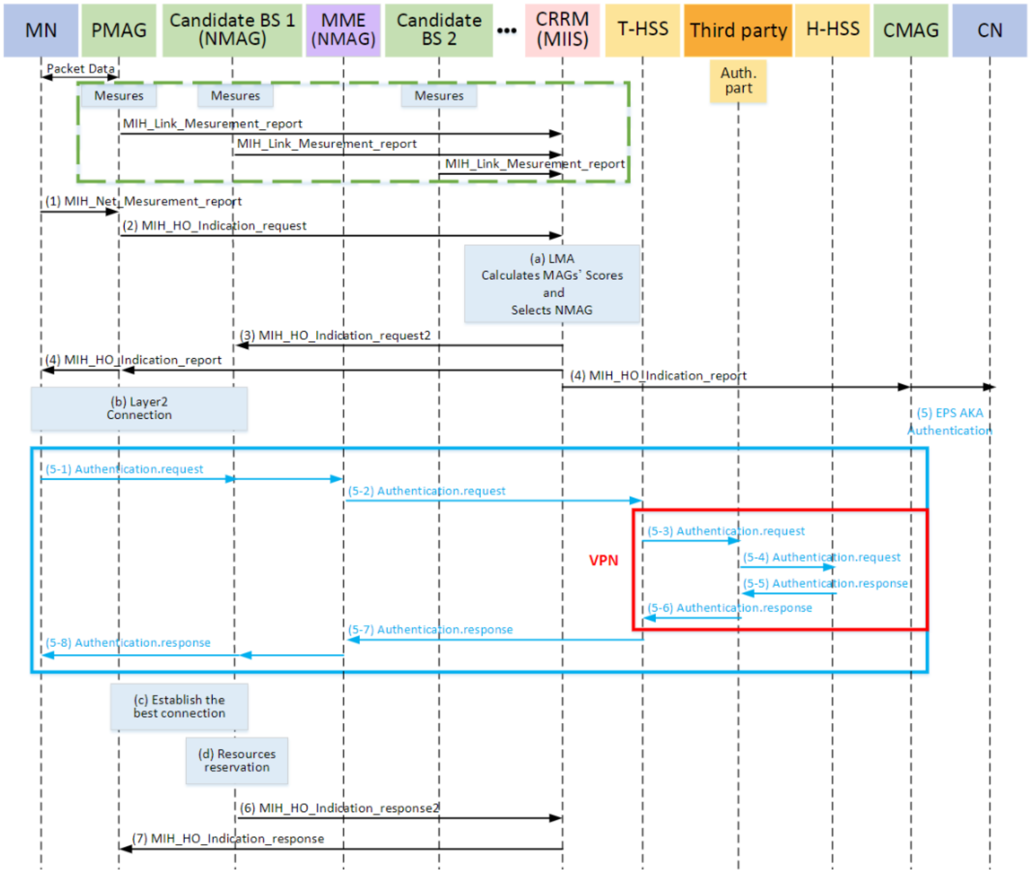

Figure 7. The sequence chart of ((H-T: untrusted), (S-T: trust)).

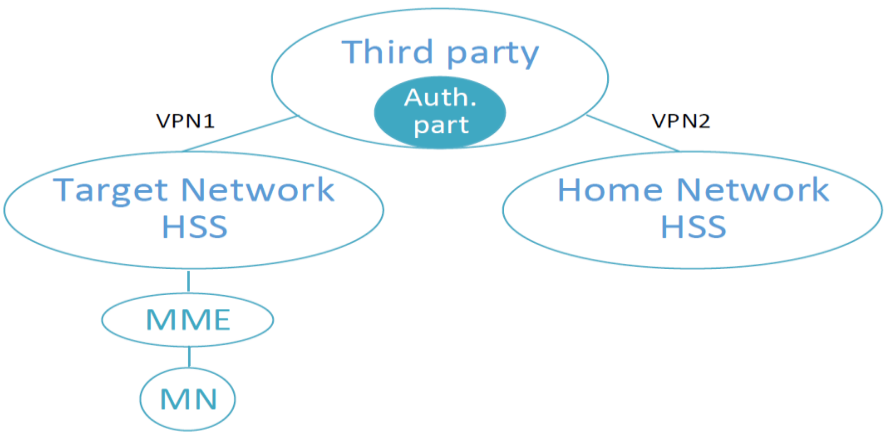

Figure 8. An architecture for MN authentication via VPN and VPN2.

3.1.4 ((H-T: untrusted; S-T: untrusted))

This is the worst case. Because of (S - T: untrusted), Third party collects data from PAMG's nearby base stations. The green dashed box illustrated in Figure 9 only shows that the MAG periodically sends messages to the Third party without illustrating the on-demand data collection from MAGs. The Third party calculates the scores for all MAGs from which to select NMAG for MN, as shown in step (a) of Figure 9. In step (3), the Third party informs NMAG that it has been selected. In step (4), it notifies MN that the selected MAG will serve as its NMAG. In step (5), because of the (H-T: untrusted), the T-HSS cannot directly request H-HSS to authenticate the MN. Therefore, those messages delivered in the steps from (5-3) to (5-6) are all transferred to the Third party through VPNs.

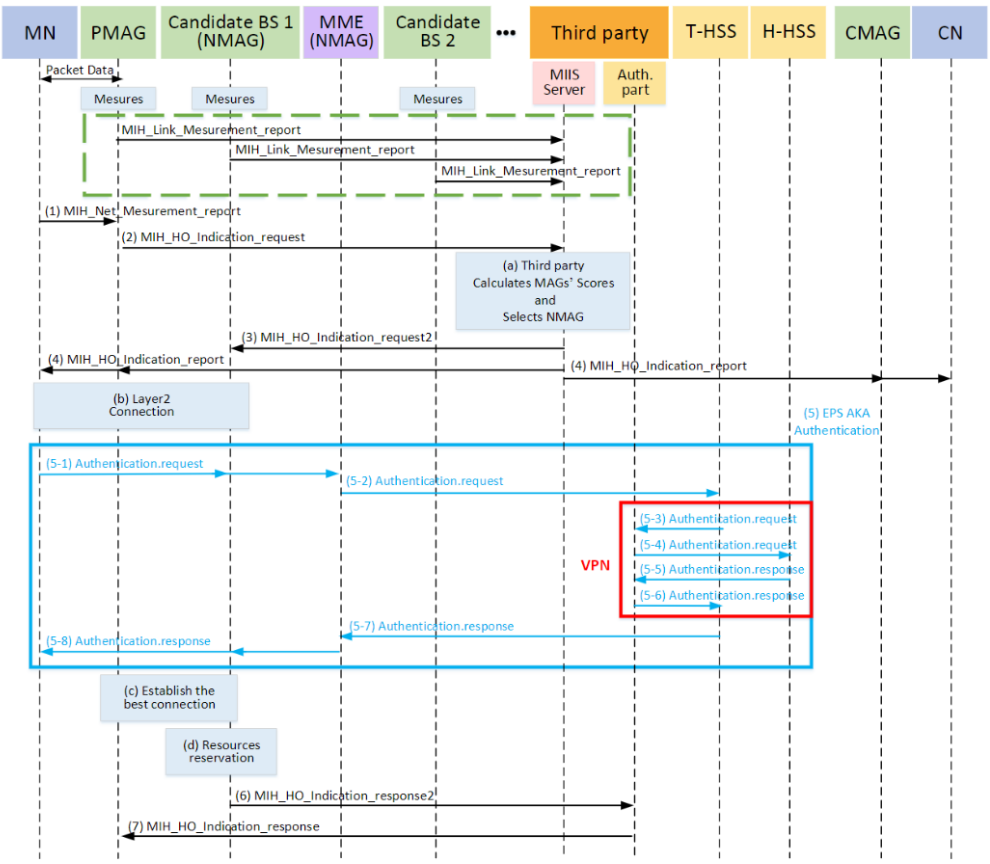

Figure 9. The sequence chart of ((H-T: untrusted), (S-T: untrusted)).

3.2 Base station selection

At present, current NMAG selection approaches, such as PMIPv6 and FMIPv6, only consider RSRQ. This study adopts three categories of parameters to select NMAG. (please refer to Table 1), including those only belonging to MN, those singly concerning MAG and those related to both MN and MAG. The first category contains MN's moving speed v, $\text{Service\_charge}_{MN}$ and $RSRQ_{PMAG}$. All are attributes of MN. The second category consists of candidate MAG's Load (LD), MAG's communication range (D), Delay to next hop, Throughput to next hop, Drop rate to next hop and $\text{Service\_charge}_{MAG}$. The third category comprises RSRQ that MN receives from the candidate MAG (denoted by $RSRQ_{MAG_n}$), $R_{MAG_n\_MN}$, θ and T, the description of which is depicted in Table 1. The goal is to reduce the number of handovers and select a suitable base station which provides better network QoS to MN. LMA is responsible for the base station selection, thereby reducing the workload of PMAG and increasing the utilization of LMA [1]

3.2.1 Parameters of MN

MN's moving speed v will affect the time T that MN stays in the communication range of the candidate MAG. In the Access network discovery and selection function (ANDSF), there is a Policy and Charging Rules Function (PCRF) responsible for charging policies represented by $\text{Service\_charge}_{MN}$. When RSS_{PMAG} is lower than its predefined threshold, MN will send MIH_Net_Mesurement_report to inform PMAG to select NMAG.

3.2.2 Parameters of MAG

The goal of considering MAG's load LD is to achieve load balance among base stations. Since when some MAGs are over loaded, they will provide poor network service quality. LD is defined as

$$LD = \frac{MAG_{use\_MN}}{MAG_{Max\_MN}} \quad (1)$$

where MAG_{Max_MN} represents the maximum number of MNs that am MAG can serve, and MAG_{use_MN} is the number of MNs currently served by the MAG.

The three parameters, Delay to next hop, Throughput to next hop and Drop rate to next hop, are used to evaluate the QoS of the candidate MAG.

3.2.3 Parameters of MN-MAG

When handing over, if $RSRQ_{MAG_n} > RSRQ_{PMAG}$, MAG_n will be preferentially selected. When the value of θ is closer to 0, it means that the MN is moving toward the candidate MAG, and the signal will become stronger. T is calculated by using $R_{MAG_n\_MN}$, θ, MN's v and MAG's D under the assumption that the MN moves linearly.

$$T = \frac{2Dsin\left(\cos^{-1}\frac{(R_{MAG_n\_MN})\sin\theta}{D}\right)}{v} \quad (2)$$

A longer T can effectively reduce the number of MN's handover.

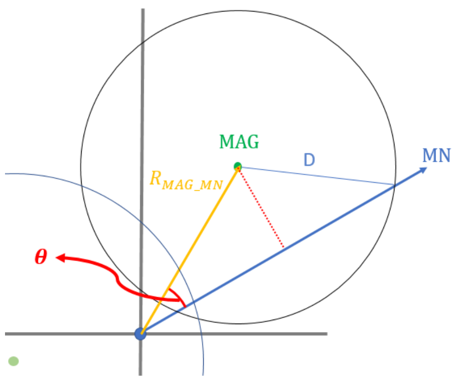

Figure 10. The expected time T in which MN stays in the communication range of a candidate MAG.

Table 1. Parameters adopted in this study to calculate scores of MAGs near PMAG.

Provider	Name	Description
MN	v	MN's moving speed
	$Service\_charge_{MN}$	Charging policies signed by MN/user and its Home operator
	$RSRQ_{PMAG}$	The quality of signal strength MN receives from PMAG
MAG	LD	MAG's current load
	D	MAG's communication range
	Delay to next hop	The time required a candidate MAG to send a packet to the next hop
	Throughput to next hop	The number of bytes received per second at the next hop of the candidate MAG.
	Drop rate to next hop	$\frac{N-M}{N}$, where N is the number of packets sent to next hop by the candidate MAG per second and M is the number of packets received by the next hop
	$Service\_charge_{MAG}$	Charging policies of candidate MAG's operator.
MN-MAG	$RSRQ_{MAG_n}$	The quality of signal strength MN receives from MAG_n
	$R_{MAG_n\_MN}$	Distance between MN and MAG_n
	θ	The angle between MN's moving direction and the connection between MN and MAG_n
	T	The time that MN stay in the MAG's communication range

3.3 Algorithm for base station selection

The base station selection algorithm can be divided into two phases, one in PMAG and the other in CRRM or Third party.

3.3.1 Algorithm in PMAG

Figure 11 shows the Flow chart with which NMAG chooses a trusted or an untrusted MAG. Let $B = \{b_1, b_2, b_3, \dots, b_x\}$, let $Bt = \{tb_1, tb_2, tb_3, \dots, tb_m\}$, let $Bu = \{ub_1, ub_2, ub_3, \dots, ub_n\}$, where $x = m + n$, and $B = Bt \cup Bu$. B represents that there are x candidate MAGs around the MN. Bt (Bu) are m (n) candidate MAGs that are mutually trusted (untrusted) with PMAG. Let $\theta = \{\theta_{b_1}, \theta_{b_2}, \theta_{b_3}, \dots, \theta_{b_x}\}$, θ_{b_i} is the angle between MN's moving direction and the connection from MN to MAG_i, i.e, b_i.

$cos\theta_{tb_i} \geq 0,\ 1 \leq i \leq m$, indicates that the *i*-th MAG, i.e., tb_i trusted with PMAG, is located in front of the MN, i.e., the MN is gradually close to this candidate MAG. $cos\theta_{ub_j} \geq 0,\ 1 \leq i \leq n$, indicates that the *j*-th MAG, i.e., ub_j mutually untrusted with PMAG, is located in front of the MN.

Algorithm 1: Selecting LMA or Third party by PMAG
Input: θ=$\{\theta_{b_1},\ \theta_{b_2},\ \theta_{b_3},\ \dots,\ \theta_{b_x}\}$
Output: a request sent to LMA or to Third party
{PMAG receives MIH_Net_Mesurement_report from MN;

If $\exists\ cos\theta_{tb_i} \geq 0\ , tb_i \in Bt, \quad 1 \leq i \leq m$
then PMAG sents a MIH_HO_Indication_request to LMA (CRRM);

else if $\exists\ cos\theta_{ub_j} \geq 0,\ ub_j \in Bu, \quad 1 \leq j \leq n,$
then PMAG sents a MIH_HO_Indication_request to the Third party;

else
choose the MAG, e.g., tb_k, with the highest RSRQ, $tb_k \in Bt$;}

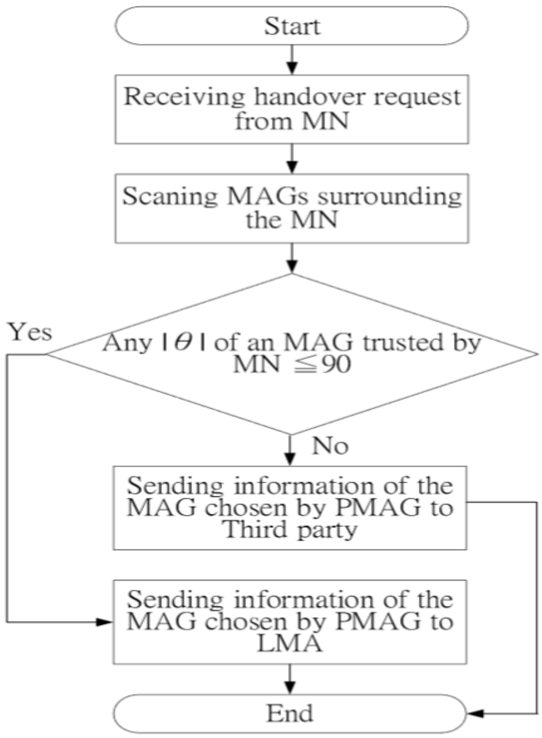

Figure 11. Flow chart for PMAG to choose a trusted or untrusted MAG.

3.3.2 Algorithm performed by CRRM or Third party

Figure 12 show the Flow chart with which CRRM or Third party can choose NMAG. The algorithm is installed in LMA and Third party. If there is a candidate MAG, e.g., MAG-X, MAG-X's home network, i.e., T-Net, and MN's S-Net are mutually trusted and MAG-X is in front of MN, the algorithm will be performed by the LMA. However, MAG-X's home network, i.e., T-Net, and MN's S-Net are mutually untrusted and MAG-X is in front of MN, the algorithm will be executed by the Third party.

Let $B' = \{B'_1, B'_2, \dots, B'_n\}$ represents that there are n candidate MAGs in front of MN, and a total of 9 parameters, i.e., B'_n=$\{term_{n,1}$, $term_{n,2}$, …, $term_{n,9}\}$, is used to evaluate all candidate base stations,. They are $\{\varphi$, $cos\theta$, T, $1 - LD_{MAG}$, $D \quad elay \ to \ next \ hop$, $Throughput \ to \ next \ hop$,

$Drop\ rate\ to\ next\ hop$, \$, $H\}$ (See Table 2). Each of these parameters has to be normalized. Let w_h be the weight of parameter h, and the weights defined for the 9 parameters are listed in the third column of Table 2. Let S_{MAG_i} be the score of the i-th candidate MAG. The base station with the highest score will be the MN 's NMAG.

Algorithm 2: Selecting a base station as NMAG by CRRM or the Third party

Input: $\{B'_1, B'_2, \ldots, B'_n\}$
Output: S_{MAG_p} /*ranking the top first MAG*/
{if (S-Net and T-Net are mutually trusted) /*MT-Net*/
    M = LMA;
else if S-Net and T-Net are mutually untrusted) /*MU-Net*/
    M = The Third party;

if M receives MIH_HO_Indication_request from PMAG
    For (i=1; i<= n; i++) {

    Retrieve $\{term_{i,1},\ term_{i,2},\ \ldots,\ term_{i,9}\} = \{\ \varphi_i\ \ cos\theta_i,\ T_i,\ 1 - LD_{MAG_i},\ Delay\ to\ next\ hop_i,\ Throughput\ to\ next\ hop_i,\ Drop\ rate\ to\ next\ hop_i,\ \$_i,\ H_i\}$ from M's database for MAG_i;

$S_{MAG_i} = \sum_{h=1}^{9} w_h \cdot term_{i,h}$;
/* $term_{i,h}$ represents the h-th parameter of the MAG_i, and S_{MAG_i} is the score of MAG_i*/}

Let $S_{MAG_p} = \max_{1 \le i \le n} \{S_{MAG_i}\}$;

Choose MAG_p as MN's NMAG;   //by M
M sends MIH_HO_Indication_request2 to NMAG;}

Table 2. The 9 Parameters used to evaluate a candidate MAG.

Term	**Description**	**Weight**
φ	$RSRQ_{MAG_n} - RSRQ_{PMAG}$	0.2
θ	The angle between MN's moving direction and the connection between MN and MAG_n	0.1
T	The time that the MN stays in the MAG's communication range	0.1
$1\text{-}LD_{MAG_n}$	Remaining bandwidth	0.1
Delay	Delay of the link from MAG_n to its next hop	0.1
Throughput	Throughput on the link from MAG_n to its next hop	0.1
Drop rate	Drop rate on the link from MAG_n to its next hop	0.1
$	$Service\ charge_{MN}$-$Service\ charge_{MAG_n}$	0.1
H	Hand over to Homogeneous/Heterogeneous Network	0.1

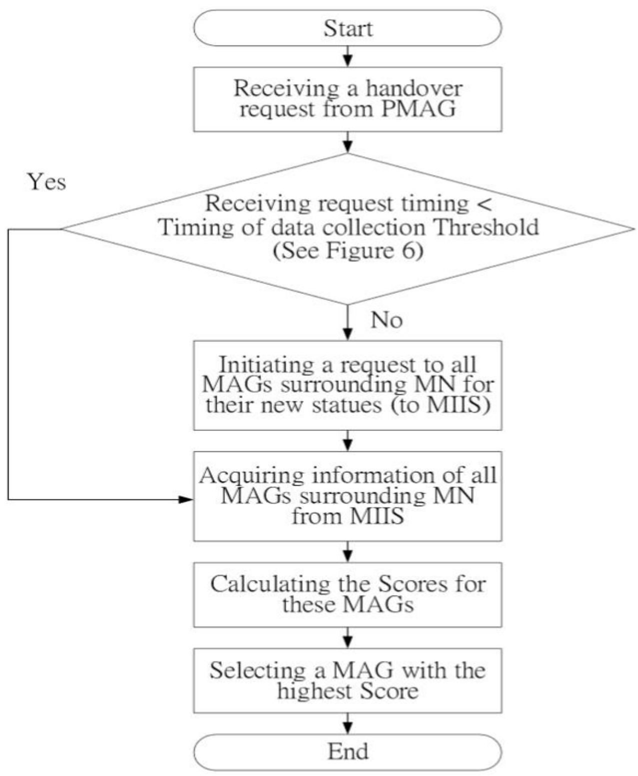

Figure 12. Flow chart for CRRM or Third party to choose NMAG.

IV. Experiments and Discussion

We use ns-3 [21 - 23] as the network simulation tool to implement our system topology. Four experiments were performed in this study. In the first experiment, different data rates on different bandwidths are given. The second experiment compares performance of different NAMG selection schemes. The third experiment compares the performance of these schemes given different θs and RSRQs. The fourth redoes the third experiment but given different RSRQs.

4.1 Experiment 1: Different Data Rates and Bandwidths

The specifications and default parameters of the first experiment are listed in Table 3.

Table 3. The specifications and default parameters of the simulation environment utilized in the first experiment.

Network parameter	Description
Communications Protocol	UDP
Bandwidth	1 to 1,000 (Kbps)
Packet size	1,024 bytes
Number of MN	1
Simulation time	2,000 sec
Operating system	Linux

In the first experiment, different data rates including 8, 40,80, 160 and 320 Kbps on different bandwidths ranging between 1 and 1,000 Kbps are given. Figure 13 to Figure 15 show end-to-end delays of the case when a packet, the size of which is the same as the data rates, is sent per second. Figure 13 shows the case in which only one packet is sent in each experiment. Figure 14 (Figure 15) illustrates the case in which one packet is transmitted per second and a total of 10 (50) packets are delivered when one packet is transmitted per second. From these two figures, we can see the average delay of a packet is very longer than that of a packet shown in Figure13 due to the head of line blocking problem, i.e., a packet can be delivered only after the delivery success of its previous packets. Please refer to Appendix of this paper.

In these figures, some curves do not exist at their low bandwidths. Because the maximum size of a packet is fixed, some packets are too long to be completely transmitted, i.e., the server is not able to receive the entire packet before sender delivers the next packet. The experimental results shown in these three figures are similar. Of course, the scales of delays are different. Take data rate of 8Kbps as an example. The Delays increase with the number of transmitted packet, even though the data rate remains unchanged. When bandwidth is 1Kbps and data rate is 8Kbps, in Figure 13, it is about 9 sec. But in Figure 14 (15), it is about 40 (200) sec.

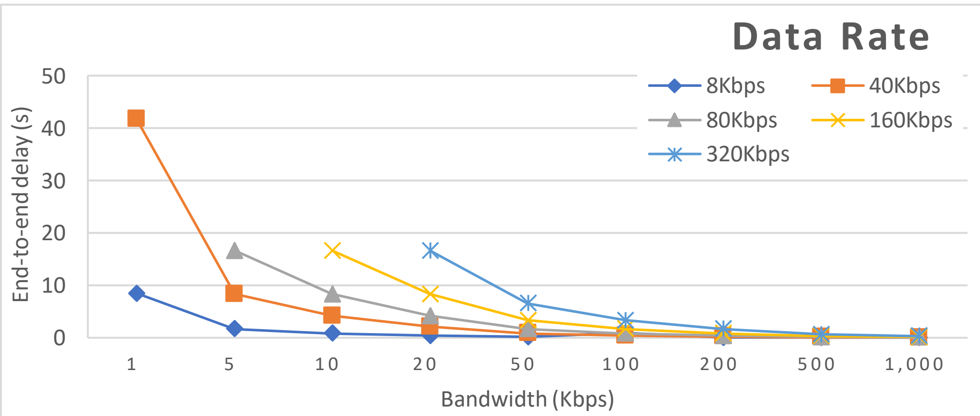

Figure 13. The delay (including transmission delay and queuing delay) of a packet when it is sent per second given different bandwidths. The size of the packet is the same as the corresponding data rate.

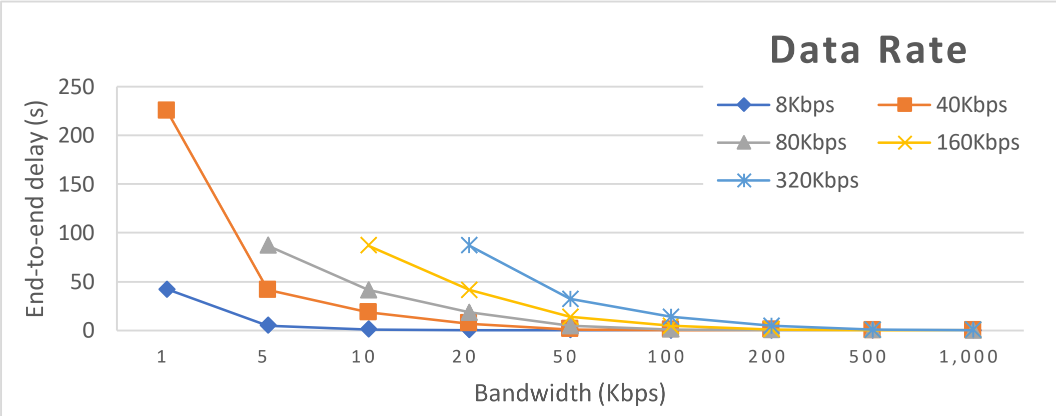

Figure 14. The delay (including transmission delay and queuing delay) of a packet when it is sent per second given different bandwidths. The size of the packet is the same as the corresponding data rate. A total of 10 packets is sent in a 10-sec time period.

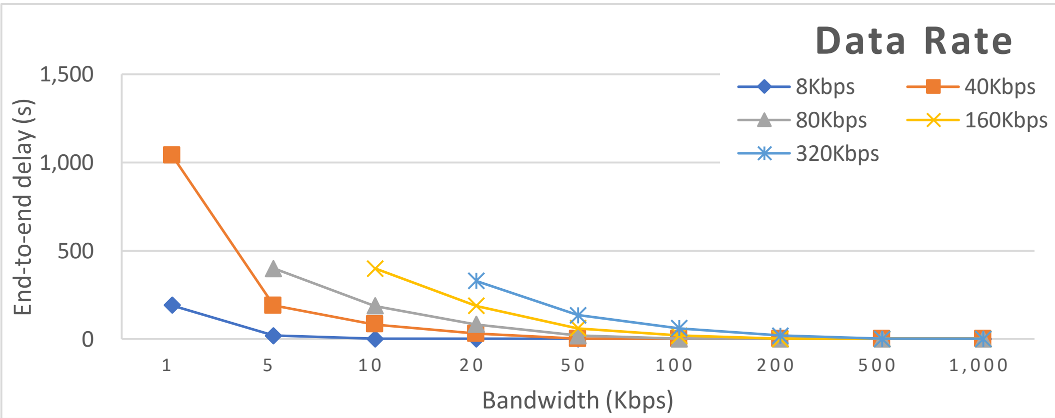

Figure 15. The delay (including transmission delay and queuing delay) of a packet when it is sent per second given different bandwidths. The size of the packet is the same as the corresponding data rate. A total of 50 packets is sent in a 50-sec time period.

In Figures 16 and 17, the packet size is fixed to 1024bytes, i.e., 8,192bits. Several packets, rather than only one packet, are sent per second to control the corresponding data rates. Basically, the curves illustrated in Figure 16 (Figure 17) on different data rates are themselves similar. When bandwidths are individually higher than data rates, the delays are almost equal, e.g., when the bandwidth is higher than or equal to 1,000Kbps the delays are almost less than 0.1s.

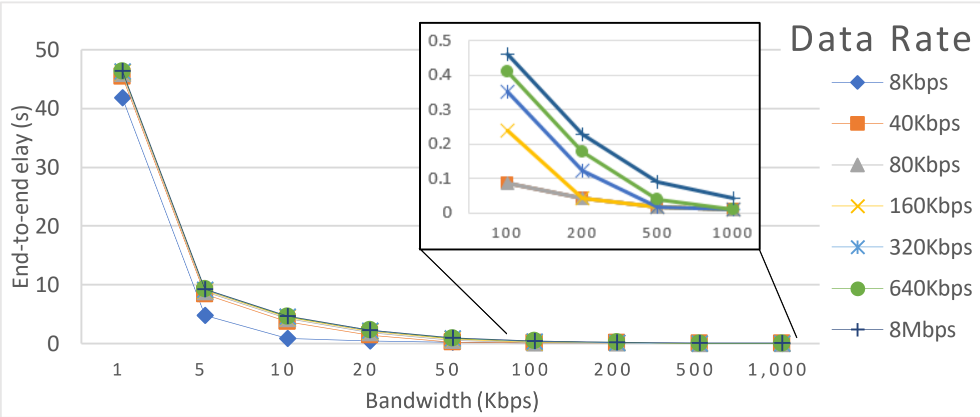

Figure 16. The delay (including transmission delay and queuing delay) of a packet when packet size is fixed to 1024 bytes given different data rates and bandwidths. A total of 10 packets is sent in different time periods.

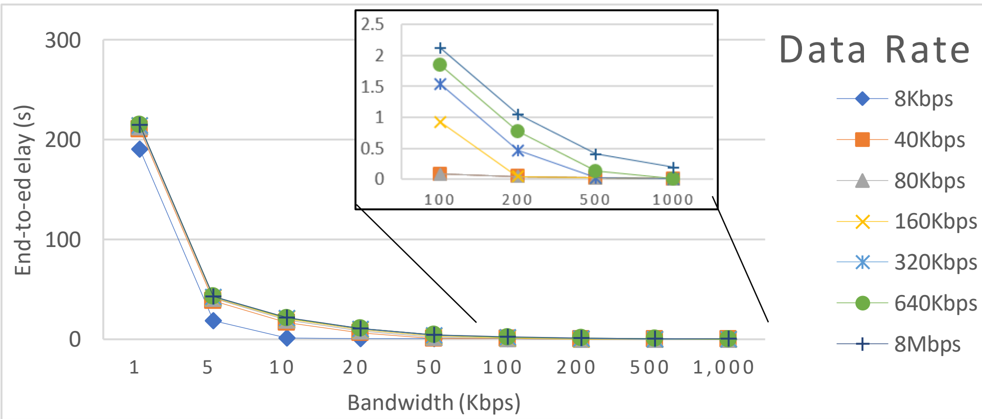

Figure 17. The delay (including transmission delay and queuing delay) of a packet when packet size is fixed to 1024 bytes given different packet rates and bandwidths. A total of 50 packets is sent in different time periods.

In this experiment, we can see that when the bandwidths are greater than 100 Kbps, the delays reduce to about 1 sec or less. The link bandwidth between MAG and each MN is higher than 100 Kbps, meaning that the wireless delays are not significant and can be ignored. This is the reason why we did not list this parameter, i.e., bandwidth of a link, in Table 2.

4.2 Experiment 2: Handover scheme comparison

In the second experiment, we compare the NAMG selection schemes including RSRQ which is used by PMIPv6, RSRQ+θ which was mentioned in [15], propose_1 which employs parameters including RSRQ+θ+ T +LD and propose_2 which adopts parameters listed in Table 2 given MN different moving speed, including 1.5 15 33 and 80 m/s, and given NMAG different communication range, containing 500, 5,000 and 25,000 m. The difference between propose_1 and propose_2 is that propose _2 considers extra parameters that represent QoS, charging, and whether or not MAG and PMAG are homogeneous networks.

When MN hands over, selecting a homogeneous network can reduce the time consumed for the handover and number of delivered messages. That is why homogeneous/heterogeneous is added in this study. We discuss the results at the end of this experiment. Before the start of this experiment, we randomly generate the position and load for an MAG and then use this position and MN’s current location to produce θ, and according to MAG's load to produce MAG's throughputs, drop rates and end-to-end delay. The topology used by this experiment is shown in Figure 18 and the specifications and default parameter of our simulation are listed in Table 4.

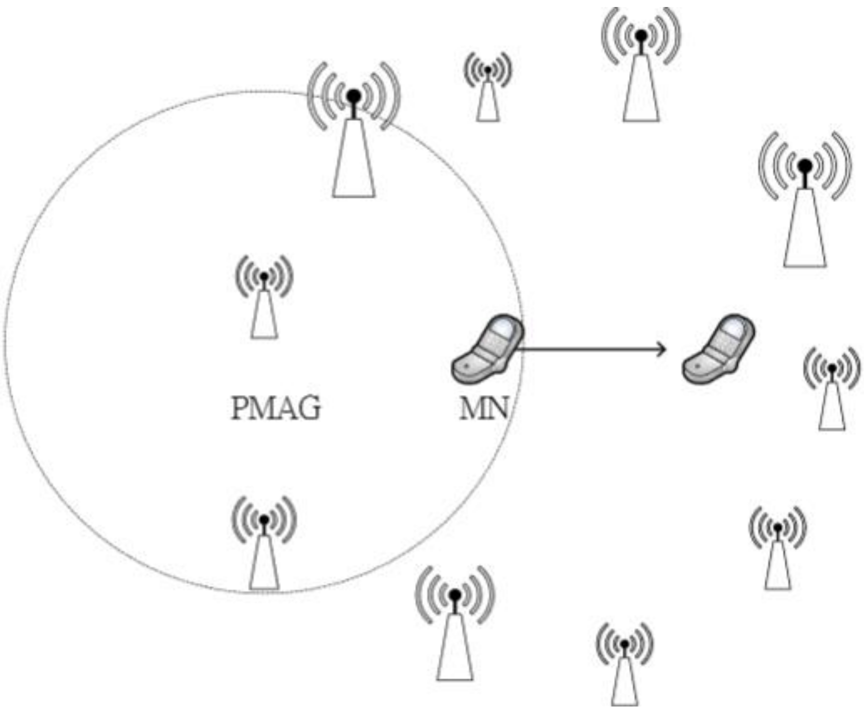

Figure 18. The topology of our second simulation.

Table 4. The specifications and default parameters of the simulation environment utilized in the following experiments.

Network parameter	Description
MAG's communication range	500, 5,000, 25,000 m
Number of candidate MAG	10
MAG_{Max_MN}	100
Number of Packets	100
Packet size	1,500 bytes
Data rate	100 Mbps
Distance between MN and MAG	0 ~ 2,5000 m
MN's moving speed	1.5, 15, 33, 80 m/s
NMAG selection schemes	RSRQ, RSRQ+ θ, propose_1, propose_2
Simulation time	100 sec
Operating system	Linux

MN at a speed of 1.5 m/s

In the first sub-experiment, MN is a pedestrian who walks with the speed of 1.5 m/s. Figures from 19 to 22 illustrate loads (number of MAG's serving MN), staying time in NMAG's communication range, throughputs (the average throughputs of all MNs currently under an MAG) and end-to-end delays (the average end-to-end delays of the link between an MAG and its next hop).

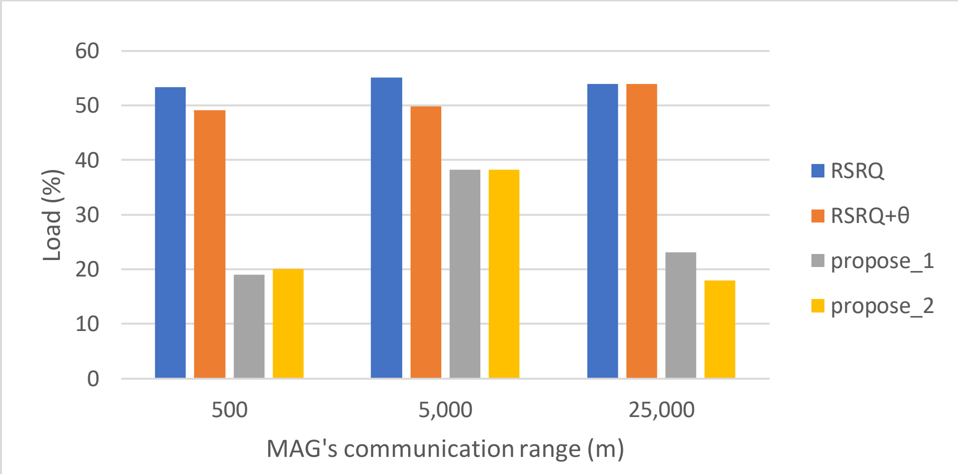

Figure 19. NMAG's loads after NMAG selection by using different NAMG selection schemes on MN's moving speed which is 1.5 m/s.

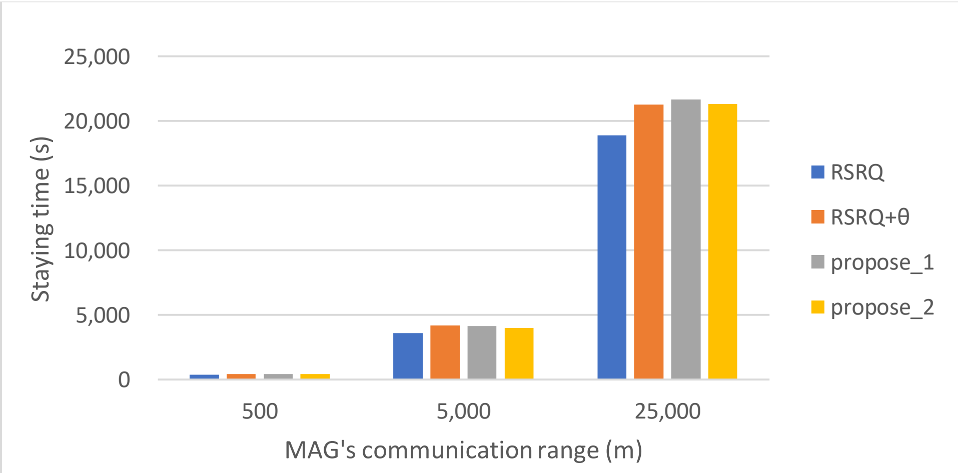

Figure 20. The time that MN can stay in NMAG's communication area after NMAG selection by using different NMAG selection schemes on MN's moving speed which is 1.5 m/s.

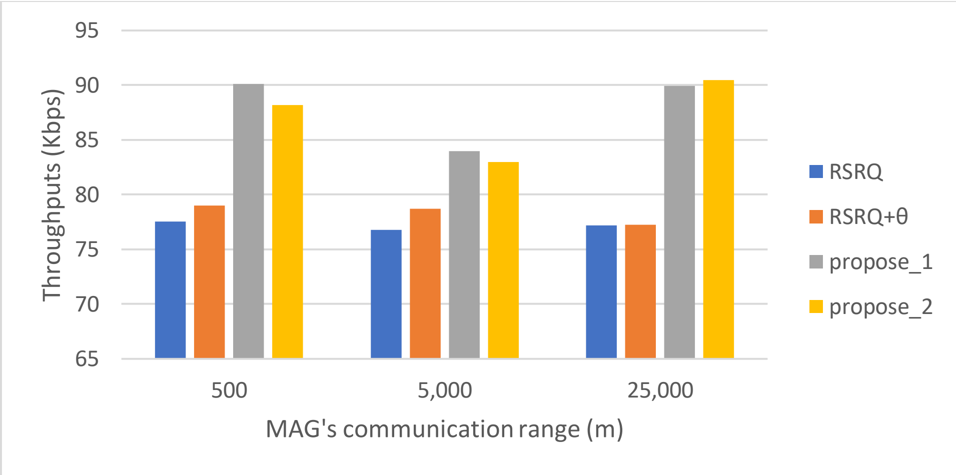

Figure 21. NMAG's throughputs after NMAG selection by using different NAMG selection schemes on MN’s moving speed which is 1.5 m/s.

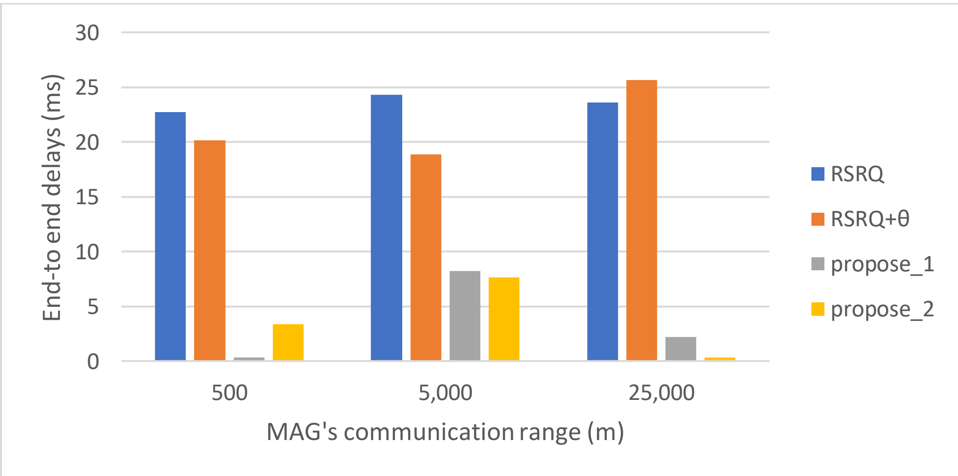

Figure 22. NMAG's end-to-end delays after NMAG selection by using different NAMG selection schemes on MN’s moving speed which is 1.5 m/s.

MN at a speed of 15 m/s

The second sub-experiment redoes the first sub-experiment, but MN is now on a car moving along a road at a speed of 15 m/s. Figures from 23 to 26 show the loads, staying time, throughputs and end-to-end delays, respectively.

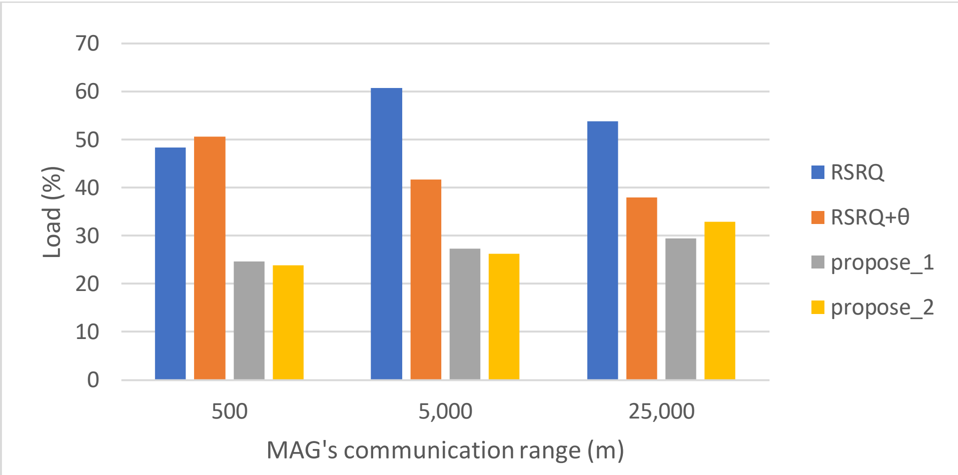

Figure 23. NMAG's loads after NMAG selection by using different NAMG selection schemes on MN’s moving speed which is 15 m/s.

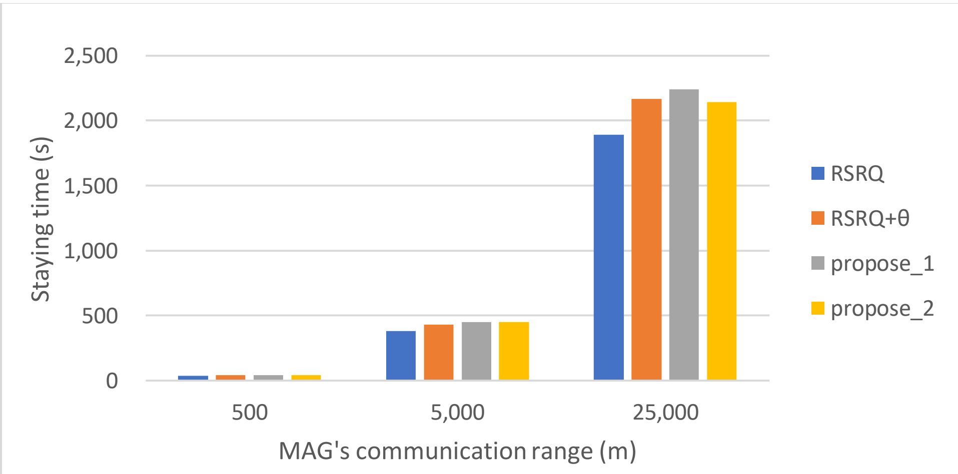

Figure 24. The time that MN can stay in NMAG’s communication area after NMAG selection by using different NMAG selection schemes on MN’s moving speed which is 15 m/s.

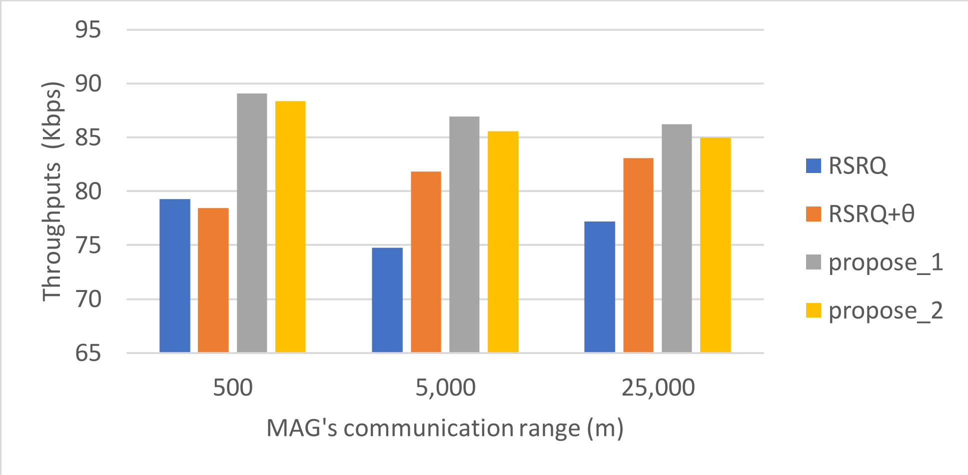

Figure 25. NMAG's throughputs after NMAG selection by using different NAMG selection schemes on MN’s moving speed which is 15 m/s.

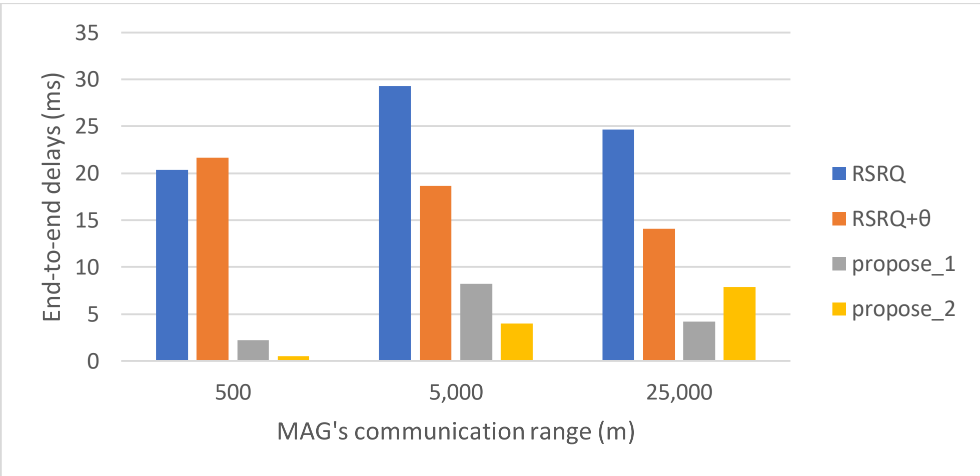

Figure 26. NMAG's end-to-end delays after NMAG selection by using different NAMG selection schemes on MN’s moving speed which is 15 m/s.

MN at a speed of 33 m/s

The third sub-experiment redoes the first sub-experiment, but MN is now in a train or a car moving at a speed of 33 m/s. Figures from 27 to 30 show the loads, staying time, throughputs and end-to-end delays, respectively.

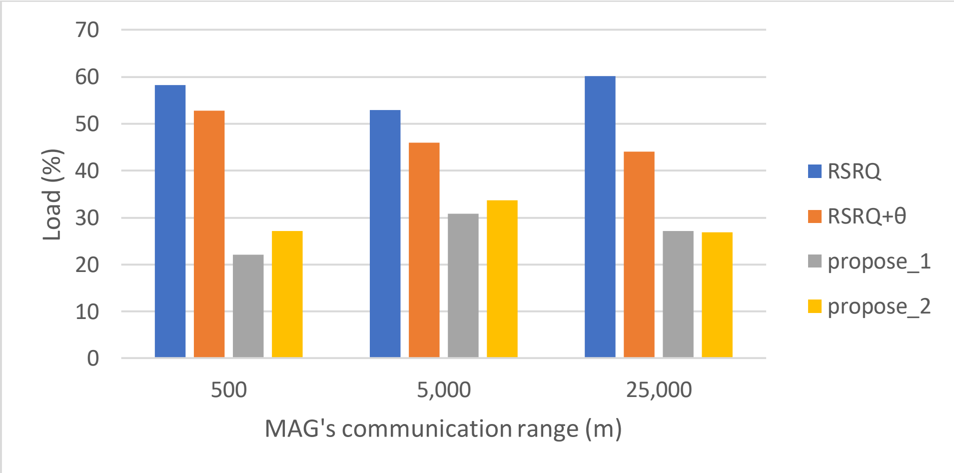

Figure 27. NMAG's loads after NMAG selection by using different NAMG selection schemes on MN’s moving speed which is 33 m/s.

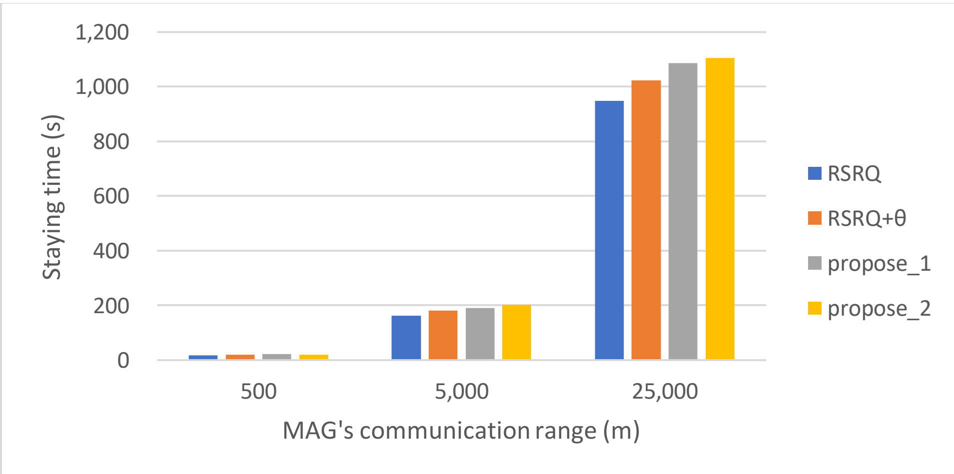

Figure 28. The time that MN can stay in NMAG’s communication area after NMAG selection by using different NMAG selection schemes on MN’s moving speed which is 33 m/s.

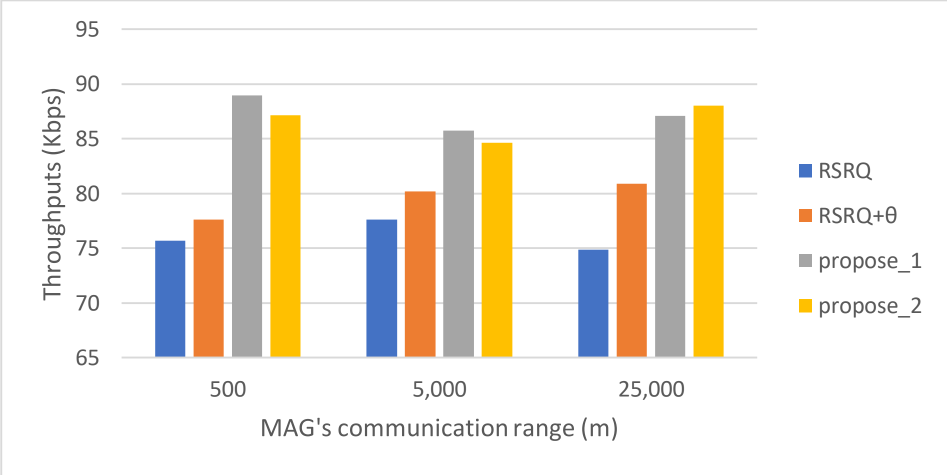

Figure 29. NMAG's throughputs after NMAG selection by using different NAMG selection schemes on MN’s moving speed which is 33 m/s.

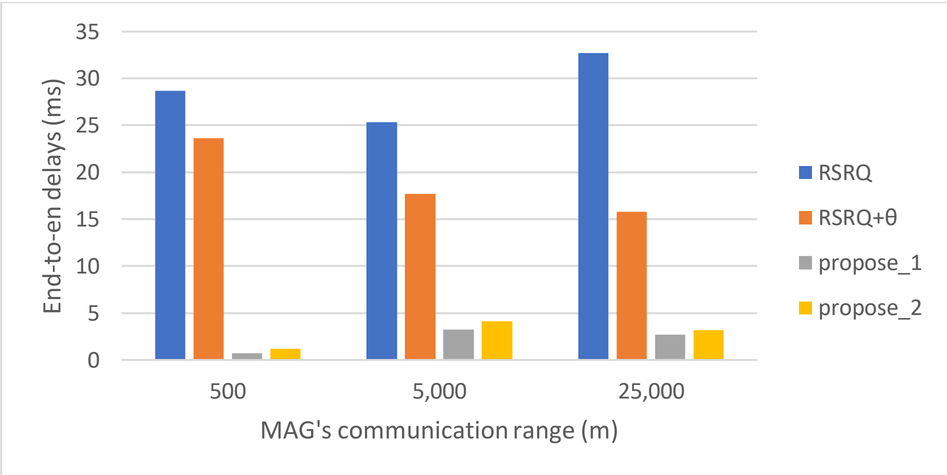

Figure 30. NMAG's end-to-end delays after NMAG selection by using different NAMG selection schemes on MN’s moving speed which is 33 m/s.

MN at a speed of 80 m/s

The fourth sub-experiment redoes the first sub-experiment, but MN is now on a high speed vehicle that moves at a speed of 80 m/s. Figures from 31 to 34 show the loads, staying time, throughputs and end-to-end delays, respectively.

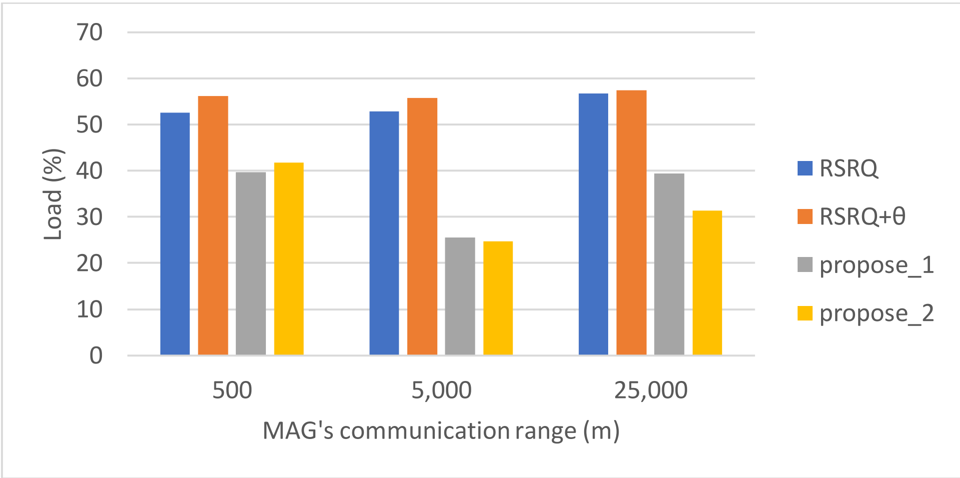

Figure 31. NMAG's loads after NMAG selection by using different NAMG selection schemes on MN’s moving speed which is 80 m/s.

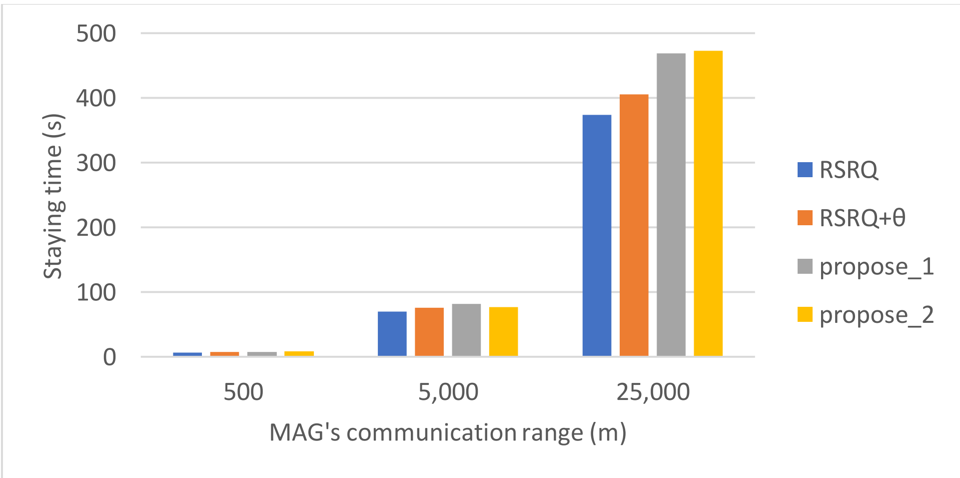

Figure 32. The time that MN can stay in NMAG’s communication area after NMAG selection by using different NMAG selection schemes on MN’s moving speed which is 80 m/s.

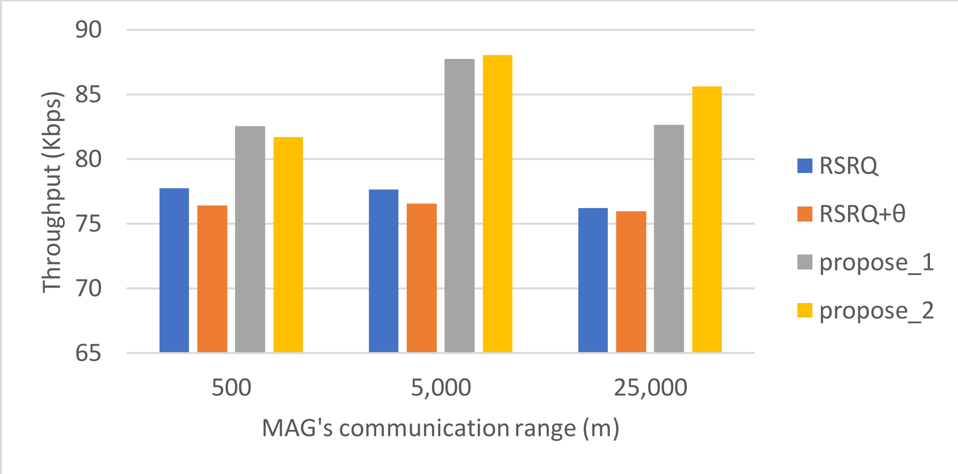

Figure 33. NMAG's throughputs after NMAG selection by using different NAMG selection schemes on MN’s moving speed which is 80 m/s.

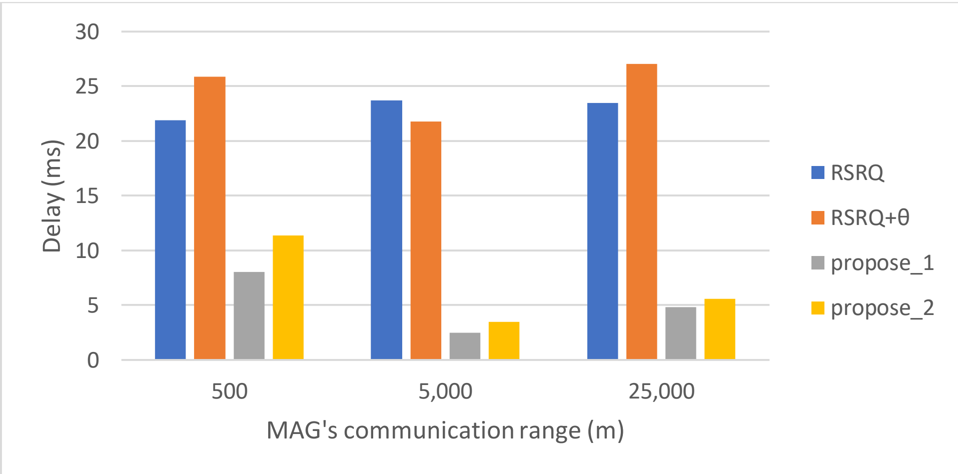

Figure 34. NMAG's end-to-end delays after NMAG selection by using different NAMG selection schemes on MN’s moving speed which is 80 m/s.

About the loads of NMAG (see Figures 19, 23, 27 and 31), it is clear that the loads of propose_1 and propose_2 are all lower than those of PMIPv6 and RSRQ+θ because the latter two do not consider MAG’s load during NMAG selection. Even through the MAG is one with high load, RSRQ and RSRQ+θ may still select it as the NMAG for MN. In this case, after MN hands over to this MAG, it may further worsen this MAG’s load and lower this MAG’s service quality.

About the MN's staying time in NMAG's communication range (see Figures 20, 24, 28 and 32), when MAG's communication range is 25,000m, it is clear that the time that MN can stay in communication range of the NMAGs selected by using propose_1 and propose_2 is longer than the time selected by using PMIPv6 and RSRQ+θ, indicating that when MN's moving distance is fixed, the number of required handover will be lower. But when MN moves at specific speed under an MAG with shorter communication range, the time difference among the four tested schemes is not significant, no matter what the MN's moving speed is. The reason is that low communication range indicates that the time MN stays under an MAG is short, their difference among the four tested schemes is insignificant. Propose_2 considers some extra parameters than propose_1 does, like serving charge and homogeneous/heterogeneous. But propose_2's experimental results, i.e., staying time, are not always better than those of propose_1, showing that the weights of the parameter, i.e., MN's moving speed, are very low. That is why it is not listed in Table 2.

About throughputs (see Figures 21, 25, 29 and 33) and end-to-end delays (see Figures 22, 26, 30 and 34), propose_1 and propose_2 choose NMAGs which provide better QoS for MN than the QoS of those NMAGs selected by the other two tested schemes.

4.3 Experiment 3: Parameter θ

In the third experiment, we compare the four tested schemes on different θs (recall, θ is the angle between MN's moving direction between MN and MAG.). We only consider MN at a speed of 80 m/s and do not compare parameter T, because T is a function of MN move speeds v, NM moving direction and $\overline{MNMAG}$ angle θ and MAG communication range R, i.e.,

$$T(t) = f(v, \theta, R) \quad (3)$$

θ is 0°

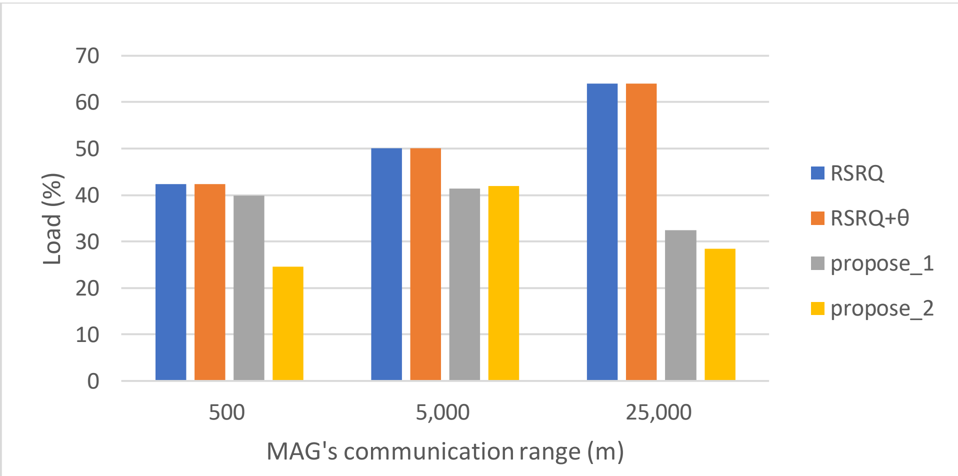

Figure 35. NMAG's loads when θ is 0°.

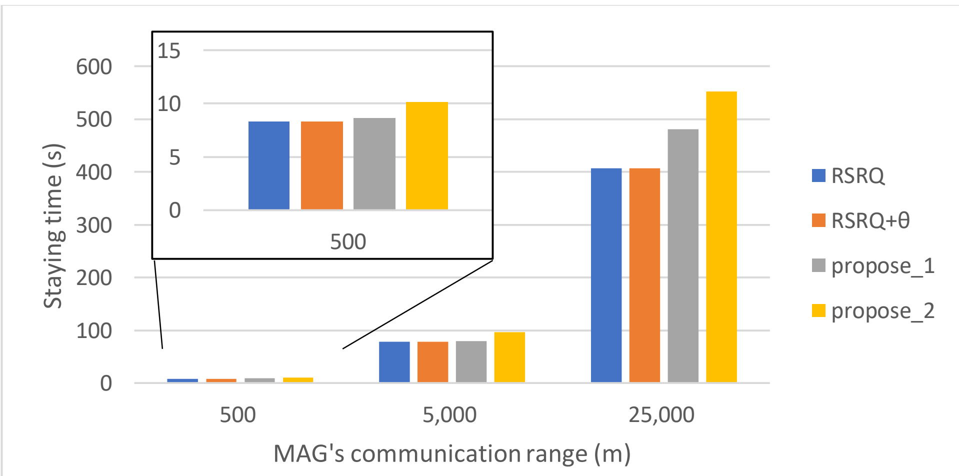

Figure 36. The time that MN can stay in NMAG's communication area when θ is 0°.

θ is 45°

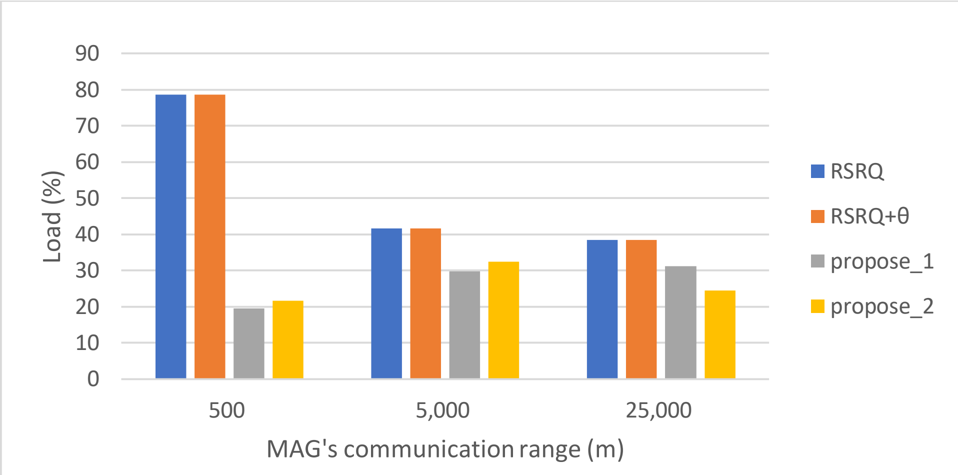

Figure 37. NMAG's loads when θ is 45°.

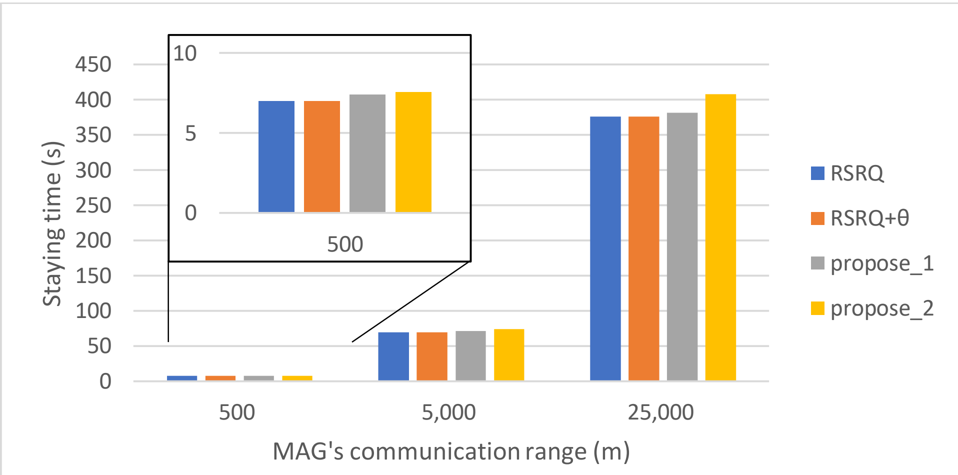

Figure 38. The time that MN can stay in NMAG's communication area when θ is 45°.

θ is 90°

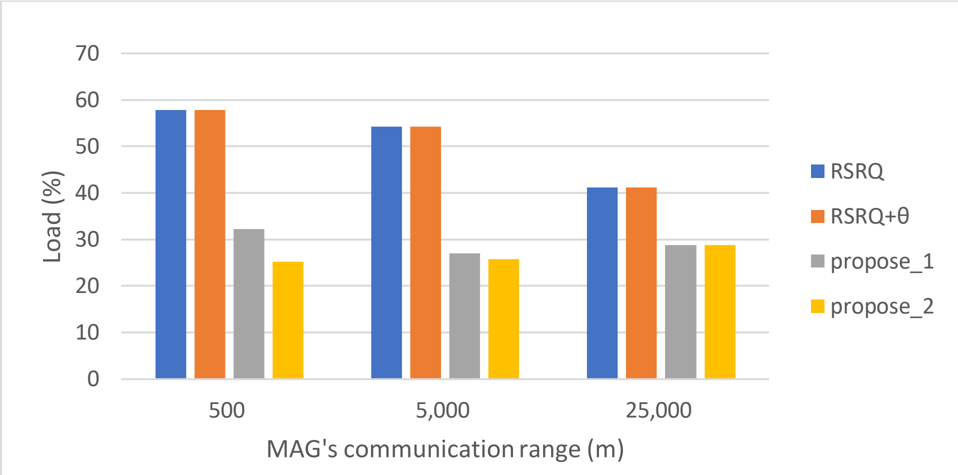

Figure 39. NMAG's loads when θ is 90°.

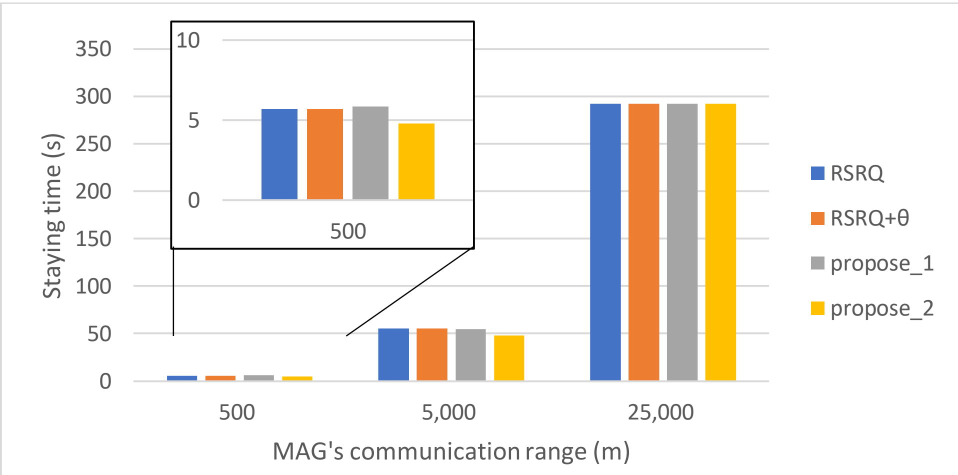

Figure 40. The time that MN can stay in NMAG’s communication area when θ is 90°.

In this experiment, we can see that the NMAG's loads (see Figures 35, 37 and 39) on propose_1 and propose_2 are better than those on PMIPv6 and RSRQ+θ because PMIPv6 and RSRQ+θ do not consider MAG’s *LD*. Also, the time that MN can stay in NMAG’s communication area (see Figures 36, 38 and 40) on PMIPv6 and RSRQ+θ is shorter, as mentioned above, increasing the number of handover when the path length is fixed.

4.4 Experiment 4: Parameter RSRQ

In the fourth experiment, we evaluate the four tested schemes given different RSRQs, including RSRQ_33, RSRQ_17 and RSRQ_1. In the experiment, the mapping of the measured quantities is defined in the table shown in Appendix B.

RSRQ_33

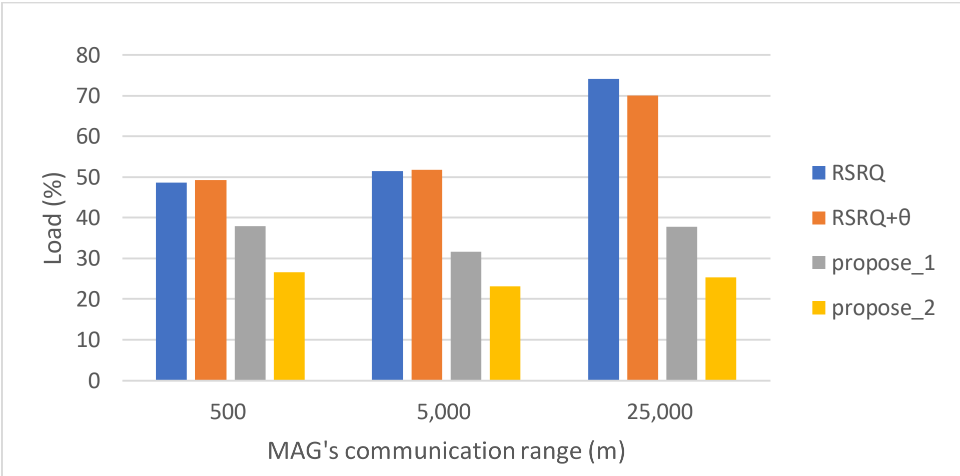

Figure 41. NMAG's loads when RSRQ is RSRQ_33.

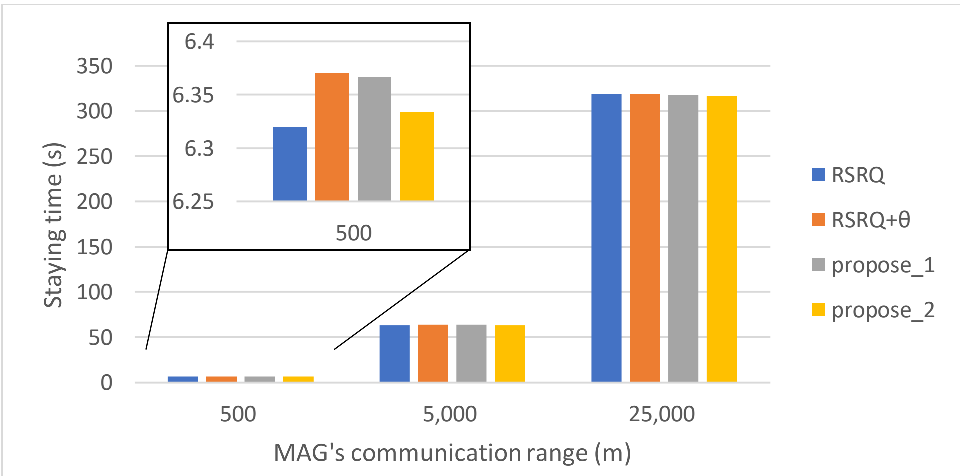

Figure 42. The time that MN can stay in NMAG’s communication area when RSRQ is RSRQ_33.

RSRQ_17

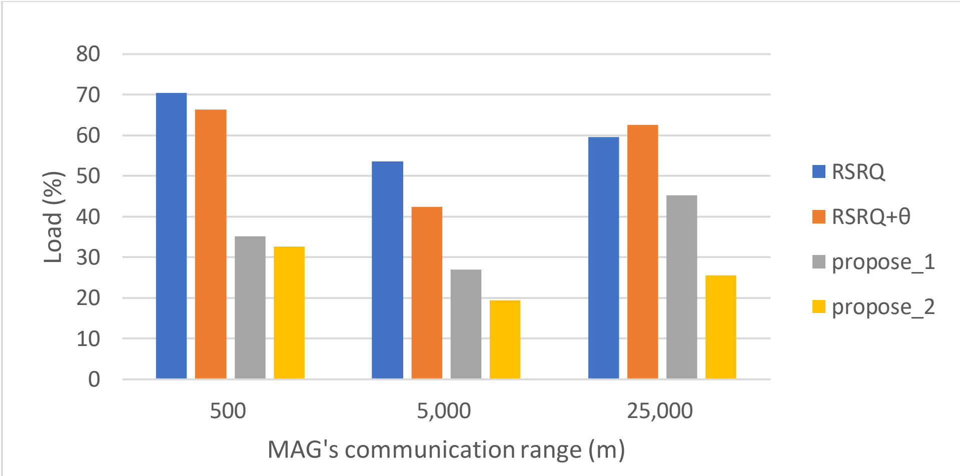

Figure 43. NMAG's loads when RSRQ is RSRQ_17.

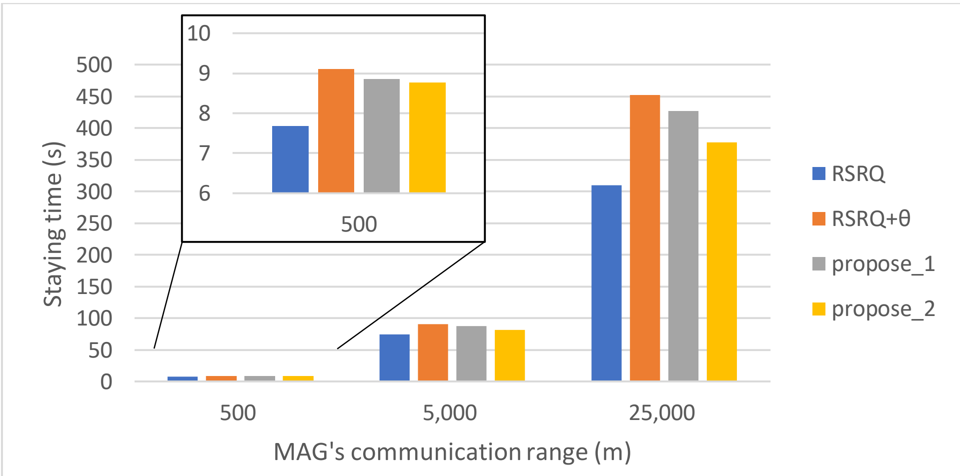

Figure 44. The time that MN can stay in NMAG's communication area when RSRQ is RSRQ_17.

RSRQ_1

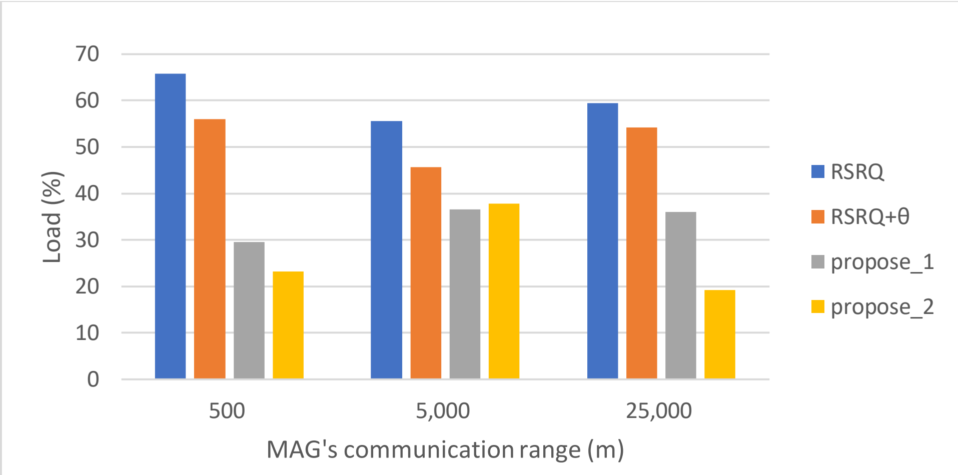

Figure 45. NMAG's loads when RSRQ is RSRQ_1.

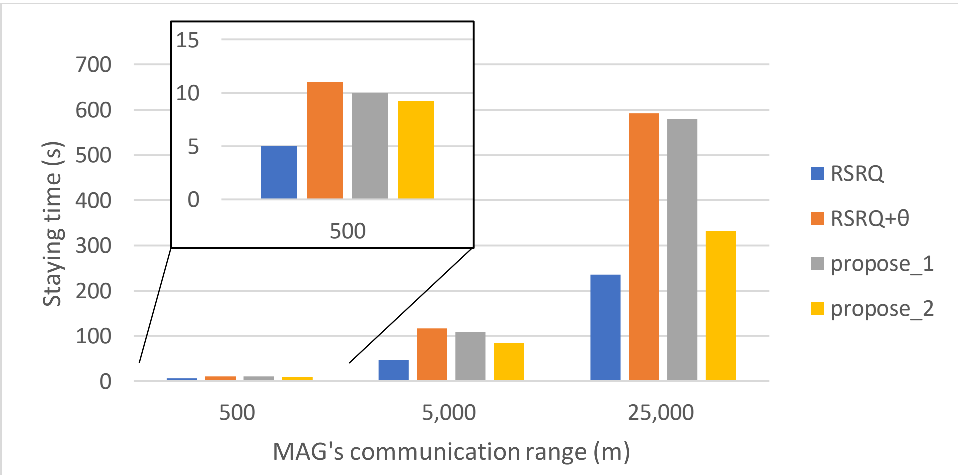

Figure 46. The time that MN can stay in NMAG’s communication area, when RSRQ is RSRQ_1.

In this experiment, we can see that the loads of NMAG selected by using propose_1 and propose_2 are all lower than those selected by employing only RSRQ and RSRQ+θ (see Figures 41, 43 and 45). Further, due to fixing RSRQ, the distance s between a MN and two arbitrary candidate MAGs are exactly the same. Thus the scores of all candidate MAGs are the same, i.e., θ can be ignored. In this study, we choose the first one, the score of which is calculated. That is why sometimes, blue bars are higher and sometimes they are lower.

About the time that MN can stay in NMAG's communication area (see Figures 42, 44 and 46), we can see that in Figure 42, the heights of the four tested schemes are almost the same because MN is very close to MAG, i.e., RSRQ=RSRQ_33. In Figure 46, the height's difference between gray bar and orange bar is limited since most MAGs selected by these two schemes are the same. But propose_1 considers the parameter *LD*, causing its MN's staying time in NMAG is shorted than that of MAG selected by RSRQ+ θ. But the loads of propos_1 are lower than those of $\mathrm{RSRQ} + \theta$.

4.5 Signaling costs

In this study, we consider the signal costs required by the four combinations mentioned in Section 3.1. We divide the signal costs into three categories. The first category is the costs for collecting an MAG's status. The second category is the costs of authentication. The third is the costs of the remaining signals.

4.5.1 Costs for collecting MAG's status

We divide the MAG-status collection of the first category into two types. One requires the help of a Third party, i.e., PMAG and NMAG are now in an MU-Net, while the other requires no Third party, i.e., PMAG and NMAG are in a MT-Net. Let T(TC) be the signal costs of an MAG-status collection requiring the help of a Third party. The signal costs of the four combinations listed in Section 3.1 belong to this type. Even ((H-T: trust), (S-T: trust)), ((H-T: untrusted), (S-T`: trust)), it is possible that Third party's help is required when |θ|<90° there are no MAGs that are trusted by the PMAG. In these cases, we need the Third party to provide MAG-statuses. Let T(C) be the signal costs of an MAG data collection requiring no help from the Third party. T(C) and T(TC) refer to the green dashed frames in Figures 4, 5, 7 and 9.

$$\mathrm{T(TC)} = 2\mathrm{T(MAG, CRRM)} \qquad (4)$$

$$\mathrm{T(C)} = \mathrm{T(MAG, CRRM)} \qquad (5)$$

$\mathrm{T(TC)} - \mathrm{T(C)} = \mathrm{T(MAG, CRRM)}$ because MAG needs to send extra message to the Third party for MAG-status collection. If the CRRM collects n MAGs' status, the signal costs requiring the help of Third party, denoted by T'(TC) and requiring no help from Third party, represented by T'(C), are

$$\mathrm{T'(TC)} = n \times 2\mathrm{T(MAG, CRRM)} \qquad (6)$$

$$\mathrm{T'(C)} = n \times \mathrm{T(MAG, CRRM)} \qquad (7)$$

4.5.2 Authentication costs

In an MU-Net, a Third party is required. Let T(TA) be the authentication costs of an MU-Net, and let T(A) be the authentication costs of a MT-Net. ((H-T: trust), (S-T`: trust)) in Section 3.1.1 and ((H-T: trust), (S-T: untrusted)) in Section 3.1.2 belong to T(A), which refers to step (5) in Figures 4 and 5. ((H-T: untrusted), (S-T`: trust)) in Section 3.1.3 and ((H-T: untrusted), (S-T: untrusted)) in Section 3.1.4 are T(TA), which refers to step (5) in Figures 7 and 9.

$$\mathrm{T(TA)} = 2\mathrm{T(MN, MAG)} + 2\mathrm{T(MAG, MME)} + 2\mathrm{T(MME, HSS)} + 4\mathrm{T(HSS, HSS)} \qquad (8)$$

$$\mathrm{T(A)} = 2\mathrm{T(MN, MAG)} + 2\mathrm{T(MAG, MME)} + 2\mathrm{T(MME, HSS)} + 2\mathrm{T(HSS, HSS)} \qquad (9)$$

$\mathrm{T(TA)} - \mathrm{T(A)} = 2\mathrm{T(HSS, HSS)}$. Due to MU-Net, H-HSS cannot directly authenticate the MN, messages exchanged between T-HSS and H-HSS need to be transmitted via a Third party, consuming 2T (HSS-HSS).

4.5.3 Costs of remaining signals

Concerning costs of remaining signals, we also divide consider the two cases, with a Third party and without a Third party. Let T(TR) be the cost of remaining signals in an MU-Net, and let T(R) be the cost of remaining signals in a MT-Net. T(TR) and T(R) refer to the steps shown in Figures 4, 5, 7 and 9 except the green dashed and blue rectangles.

$$\mathrm{T(TR)} = 2\mathrm{T(MN, MAG)} + 6\mathrm{T(MAG, CRRM)} \quad (10)$$

$$\mathrm{T(R)} = 2\mathrm{T(MN, MAG)} + 6\mathrm{T(MAG, CRRM)} \quad (11)$$

T(TR) and T(R) are the same, owing to relating to no Third party.

V. Conclusion and Future studies

In this study, we propose a Third party to choose NMAG for an MU-Net to mitigate the network handover problems for two untrusted networks. Third party helps the two networks to communicate with each other, to mutually exchange their network information and to provide authentication channels. We also propose a target base station selection algorithm for LMA/Third party which adopts parameters, like angle, time, and QoS…etc, to ensure that a network can provide MN with better service quality and reduce the number of MN handover.

During experiments, we can see that if the packet size is fixed, the bandwidth is larger, even if the data rate is larger, the delays decrease and we can find that adding the parameter T can lengthen the time in which MN stays in the communication range of NMAG. In addition, we also add the parameter "Service charge". This may conduct our system close to the reality when that MN hands over to an untrusted network. The costs requiring the help of Third party are higher than the costs consumed without a Third party. Although the case with a Third party, the proposed schemes consume extra signal costs, i.e.,$\mathrm{T(MAG, CRRM)} + 2\mathrm{T(HSS, HSS)}$, the schemes can choose more suitable MAG for MN handover.

In the future, we wish to use Artificial Intelligent techniques to adjust weights for all employed parameters, aiming to derive more accurate weighs for different parameters based on users' needs. We also like to derive the behavior and reliability models for this proposed scheme so that user can realize the behaviors and reliabilities before using it. These constitute our future studies.

References

[1] F.Y. Leu, C.C. Cheng, “MIH-based Congestion Control with Seamless Handover in Untrusted Heterogeneous Networks,” The 11th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, July 2017, pp. 502-510.

[2] IEEE Standard for Local and metropolitan area networks, Part 21: Media Independent Handover Services. January 2009. [online]. Available: http://ieeexplore.ieee.org/document/4769367/ [Accessed: 04-Dec-2016]

[3] S. M. Faccin, "IEEE 802.21 Media Independent Handoff: Overview of services and scenarios for 3GPP2," Liaison to 3GPP2, Jul 2005, pp31.

[4] Y. Ohba, “Media-Independent Handover Security Tutorial,” IEEE 802 meeting, March 2008, pp,36.

[5] K.Taniuchi, Y.Ohba, V.Fajardo, et al, "IEEE 802.21: Media Independent Handover: Features, Applicability, and Realization," IEEE Communications Magazine, January 2009, pp. 112-120,

[6] A. Tolli, P. Hakalin, H. Holma, “Performance evaluation of common radio resource management (CRRM),” IEEE International Conference on Communications 2002, New York, USA, May 2002, pp. 3429–3433.

[7] H. Mzoughi, F. Zarai and L. Kamoun, “Interference – Limited Radio Resources Allocation in LTE_A System with MIH Cooperation,” 2016 22nd Asia-Pacific Conference on Communications (APCC) pp. 174-179, August 2016.

[8] N. Passas, S. Paskalis, A. Kaloxylos, F. Bader, R. Narcisi, E. Tsontsis, A.S. Jahan, H. Aghvami, M. O’Droma, I. Ganchev, “Enabling technologies for the always best connected concept,” Wirel Commun Mob Comput Vol. 6, 2006, pp. 523–540.

[9] J. Pérez-Romero, O. Sal1ent, R. Agustí, P. Karlssont, A. Barbaresit, L. Wang, F. Casadevall, M. Dohler, H. Gonzfilezt, F. Cabral-Pintot, “Common radio resource

management: functional models and implementation requirements," IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications, Berlin, Germany, Sept 2005, pp. 2067–2071.

[10] M. Purkhiabani and A. Salahi, "Enhanced Authentication and Key Agreement Procedure of next Generation 3GPP Mobile Networks," International Journal of Information and Electronics Engineering, Vol.2, No.1, January 2012, pp.69-77.

[11] F.Y. Leu, I. You, Y.L. Huang, K. Yim, C.R. Dai "Improving security level of LTE authentication and key agreement procedure," IEEE Globecom Workshops 2013, pp.1032-1036.

[12] F.S. Azar, "Multiattribute Decision-Making: Use of Three Scoring Methods to Compare the Performance of Imaging Techniques for Breast Cancer Detection," January 2000. [online]. Available: https://repository.upenn.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1121&context=cis_reports

[13] R.V. Rao, "Introduction to Multiple Attribute Decision-making (MADM) Methods", Decision Making in the Manufacturing Environment, Springer Series in Advanced Manufacturing, 2007 pp. 27-41.

[14] S. Meng, F. Arbab, "QoS-Driven Service Selection and Composition Using Quantitative Constraint Automata," Fundamenta Informaticae, Vol. 95, January 2009, pp. 103-128.

[15] A. Kishida, Y. Morihiro, T. Asai, Y. Okumura "Cell selection scheme for handover reduction based on moving direction and velocity of UEs for 5G multi-layered radio access networks," International Conference on Information Networking (ICOIN), Jan 2018, pp.362-367.

[16] L. Tartarini, M.A. Marotta, E. Cerqueira, J. Rochol, C.B. Both, M. Gerla, P. Bellavista "Software-defined handover decision engine for heterogeneous cloud

radio access networks," Computer Communications, Vol. 115, January 2018, pp.21-34.

[17] Y. Wang, J. Yuan, Y. Zhou, G. Li, F. Liu and P. Zhang, "Handover Management in Enhanced MIH Framework for Heterogeneous Wireless Networks Environment," Wireless Personal Communications, Vol. 52, No. 3, February 2010, pp. 615-636.

[18] F. Buiati, L.J.G. Villalba, D. Corujo, S. Sargento, R.L. Aguiar, "IEEE 802.21 Information Services deployment for heterogeneous mobile environments," IET Communications, Vol.5, No. 18, December 2011, pp. 2721-2729.

[19] L. Zeng, B. Benatallah, A. H. H. Ngu, M. Dumas, J. Kalagnanam, H. Chang, "QoS-aware middleware for Web Services Composition," IEEE Transactions on Software Engineering, Vol. 30, No. 5, May 2004, pp311-327.

[20] A.A.A. Ipaye, A.M.A. Ibrahim, I.I.O. Ahmed, S.A. Nagar, D.N.G. Mitropoulos "Mathematical Model Implementation of Vertical Handover Network Decision Algorithms in Heterogeneous Network Based On QoS Parameters," International Conference on Computer, Control, Electrical, and Electronics Engineering, Nov. 2018, pp.1-6.

[21] https://www.nsnam.org/ns-3-26/

[22] https://www.nsnam.org/wiki/Installation

[23] https://www.nsnam.org/docs/models/html/animation.html

[24] http://anisimoff.org/eng/rsrp_rsrq.html

Appendix A

As shown in Figure 14, when data size is smaller than the bandwidth, a packet's transmission time plus its queuing delay is less than 1s. The real average transmission delays for higher bandwidths present higher errors than those of lower bandwidths compared to their the oracle values, e.g., the error of 5Mbps is 131% ((0.0037-0.0016)/0.0016) but the error of 50Kbps is 6.6% ((0.1706-0.16)/0.16).

Table A. Packets' delivery information where x/y/z represents the packet's sending time/ queuing time/ transmission delay when data rate is 8Kbps (please refer to Figure 14) (sec)

Bandwidth	1Kbps	5Kbps	10Kbps	20Kbps	50Kbps
First packet	2 / 0/ 8.434	2 / 0/ 1.6884	2 / 0 / 0.8452	2 / 0 / 0.4236	2 / 0 / 0.1706
Second packet	3 / 7.434 / 8.432	3 / 0.6884 / 1.6864	3 / 0 / 0.8452	3 / 0 / 0.4236	3 / 0 / 0.1706
Third packet	4 / 14.866 / 8.432	4 / 1.3748 / 1.6864	4 / 0 / 0.8452	4 / 0 / 0.4236	4 / 0 / 0.1706
Fourth packet	5 / 22.298 / 8.432	5 / 2.0612 / 1.6864	5 / 0 / 0.8452	5 / 0 / 0.4236	5 / 0 / 0.1706
Fifth packet	6 / 29.73 / 8.432	6 / 2.7476 / 1.6864	6 / 0 / 0.8452	6 / 0 / 0.4236	6 / 0 / 0.1706
Sixth packet	7 / 37.162 / 8.432	7 / 3.434 / 1.6864	7 / 0 / 0.8452	7 / 0 / 0.4236	7 / 0 / 0.1706
Seventh packet	8 / 44.594 / 8.432	8 / 4.1204 / 1.6864	8 / 0 / 0.8452	8 / 0 / 0.4236	8 / 0 / 0.1706
Eighth packet	9 / 52.026 / 8.432	9 / 4.8068 / 1.6864	9 / 0 / 0.8452	9 / 0 / 0.4236	9 / 0 / 0.1706
Ninth packet	10 / 59.458 / 8.432	10 / 5.4932 / 1.6864	10 / 0 / 0.8452	10 / 0 / 0.4236	10 / 0 / 0.1706
Tenth packet	11 / 66.89 / 8.432	11 / 6.1796 / 1.6864	11 / 0 / 0.8452	11 / 0 / 0.4236	11 / 0 / 0.1706
Avg	- / 33.4458 / 8.4322	- / 3.0906 / 1.6866	- / 0 / 0.8452	- / 0 / 0.4236	- / 0 / 0.1706

Bandwidth	100Kbps	200Kbps	500Kbps	1Mbps	5Mbps
First packet	2 / 0 / 0.0863	2 / 0 / 0.0442	2 / 0 / 0.0189	2 / 0 / 0.0104	2 / 0 / 0.0037
Second packet	3 / 0 / 0.0863	3 / 0 / 0.0442	3 / 0 / 0.0189	3 / 0 / 0.0104	3 / 0 / 0.0037
Third packet	4 / 0 / 0.0863	4 / 0 / 0.0442	4 / 0 / 0.0189	4 / 0 / 0.0104	4 / 0 / 0.0037
Fourth packet	5 / 0 / 0.0863	5 / 0 / 0.0442	5 / 0 / 0.0189	5 / 0 / 0.0104	5 / 0 / 0.0037
Fifth packet	6 / 0 / 0.0863	6 / 0 / 0.0442	6 / 0 / 0.0189	6 / 0 / 0.0104	6 / 0 / 0.0037
Sixth packet	7 / 0 / 0.0863	7 / 0 / 0.0442	7 / 0 / 0.0189	7 / 0 / 0.0104	7 / 0 / 0.0037
Seventh packet	8 / 0 / 0.0863	8 / 0 / 0.0442	8 / 0 / 0.0189	8 / 0 / 0.0104	8 / 0 / 0.0037
Eighth packet	9 / 0 / 0.0863	9 / 0 / 0.0442	9 / 0 / 0.0189	9 / 0 / 0.0104	9 / 0 / 0.0037
Ninth packet	10 / 0 / 0.0863	10 / 0 / 0.0442	10 / 0 / 0.0189	10 / 0 / 0.0104	10 / 0 / 0.0037
Tenth packet	11 / 0 / 0.0863	11 / 0 / 0.0442	11 / 0 / 0.0189	11 / 0 / 0.0104	11 / 0 / 0.0037
Avg	- / 0 / 0.0863	- / 0 / 0.0442	- / 0 / 0.0189	- / 0 / 0.0104	- / 0/ 0.0037

Table A2. Packets' delivery information where x/y/z represents the packet's sending time/ queuing time/ transmission delay when data rate is 40Kbps (please refer to Figure 14) (sec)

Bandwidth	1Kbps	5Kbps	10Kbps	20Kbps	50Kbps
First packet	2 / 0 / 41.73	2 / 0 / 8.3476	2 / 0 / 4.1748	2 / 0 / 2.0884	2 / 0 / 0.8366
Second packet	3 / 40.73 / 41.728	3 / 7.3476 / 8.3456	3 / 3.1748 / 4.1728	3 / 1.0884 / 2.0864	3 / 0 / 0.8366
Third packet	4 / 81.458 / 41.728	4 / 14.6932 / 8.3456	4 / 6.3476 / 4.1728	4 / 2.1748 / 2.0864	4 / 0 / 0.8366
Fourth packet	5 / 122.186 / 41.728	5 / 22.0388 / 8.3456	5 / 9.5204 / 4.1728	5 / 3.2612 / 2.0864	5 / 0 / 0.8366
Fifth packet	6 / 162.914 / 41.728	6 / 29.3844 / 8.3456	6 / 12.6932 / 4.1728	6 / 4.3476 / 2.0864	6 / 0 / 0.8366
Sixth packet	7 / 203.642 / 41.728	7 / 36.73 / 8.3456	7 / 15.866 / 4.1728	7 / 5.434 / 2.0864	7 / 0 / 0.8366
Seventh packet	8 / 244.37 / 41.728	8 / 44.0756 / 8.3456	8 / 19.0388 / 4.1728	8 / 6.5204 / 2.0864	8 / 0 / 0.8366
Eighth packet	9 / 285.098 / 41.728	9 / 51.4212 / 8.3456	9 / 22.2116 / 4.1728	9 / 7.6068 / 2.0864	9 / 0 / 0.8366
Ninth packet	10 / 325.826 / 41.728	10 / 58.7668 / 8.3456	10 / 25.3844 / 4.1728	10 / 8.6932 / 2.0864	10 / 0 / 0.8366
Tenth packet	11 / 366.554 / 41.728	11 / 66.1124 / 8.3456	11 / 28.5572 / 4.1728	11 / 9.7796 / 2.0864	11 / 0 / 0.8366
Avg	- / 183.2778 / 41.7282	- / 33.057 / 8.3458	- / 14.2794 / 4.173	- / 4.8906 / 2.0866	- / 0 / 0.8366

Bandwidth	100Kbps	200Kbps	500Kbps	1Mbps	5Mbps
First packet	2 / 0 / 0.4193	2 / 0 / 0.2106	2 / 0 / 0.0855	2 / 0 / 0.0437	2 / 0 / 0.0103
Second packet	3 / 0 / 0.4193	3 / 0 / 0.2106	3 / 0 / 0.0855	3 / 0 / 0.0437	3 / 0 / 0.0103
Third packet	4 / 0 / 0.4193	4 / 0 / 0.2106	4 / 0 / 0.0855	4 / 0 / 0.0437	4 / 0 / 0.0103
Fourth packet	5 / 0 / 0.4193	5 / 0 / 0.2106	5 / 0 / 0.0855	5 / 0 / 0.0437	5 / 0 / 0.0103
Fifth packet	6 / 0 / 0.4193	6 / 0 / 0.2106	6 / 0 / 0.0855	6 / 0 / 0.0437	6 / 0 / 0.0103
Sixth packet	7 / 0 / 0.4193	7 / 0 / 0.2106	7 / 0 / 0.0855	7 / 0 / 0.0437	7 / 0 / 0.0103
Seventh packet	8 / 0 / 0.4193	8 / 0 / 0.2106	8 / 0 / 0.0855	8 / 0 / 0.0437	8 / 0 / 0.0104
Eighth packet	9 / 0 / 0.4193	9 / 0 / 0.2106	9 / 0 / 0.0855	9 / 0 / 0.0437	9 / 0 / 0.0104
Ninth packet	10 / 0 / 0.4193	10 / 0 / 0.2106	10 / 0 / 0.0855	10 / 0 / 0.0437	10 / 0 / 0.0103
Tenth packet	11 / 0 / 0.4193	11 / 0 / 0.2106	11 / 0 / 0.0855	11 / 0 / 0.0437	11 / 0 / 0.0103
Avg	- / 0 / 0.4193	- / 0 / 0.2106	- / 0 / 0.0855	- / 0 / 0.0437	- / 0 / 0.0103

Appendix B [24]

Reported value	Measured quantity value	Unit
RSRQ_00	RSRQ < -19.5	dB
RSRQ_01	-19.5 ≤ RSRQ < -19	dB
RSRQ_02	-19 ≤ RSRQ < -18.5	dB
…	…	…
RSRQ_32	-4 ≤ RSRQ < -3.5	dB
RSRQ_33	-3.5 ≤ RSRQ < -3	dB
RSRQ_34	-3 ≤ RSRQ	dB