東 海 大 學 資 訊 工 程 學 系 研 究 所

碩士論文

指導教授：呂芳懌 博士

Dr. Fang-Yie Leu

在非信賴的異質網路中基於 MIH 的壅塞控制與無縫換手

MIH-based Congestion Control with Seamless Handover in Untrusted Heterogeneous Networks

研究生：鄭治中

中 華 民 國 一 〇 六 年 七 月

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 鄭 治 中 所提之論文

在非信賴的異質網路中基於MIH的壅塞控制與無縫換手

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 106 年 7 月 5 日

摘要

現今行動裝置(如:手機、筆記型電腦等)通常會安裝一種以上的無線接入協定，以適應各種異質網路環境。而兩相鄰網路(如:網路 M 和網路 N)之間，除了同質/異質性存取技術的關係之外，兩者之間也可能是可信賴或不可信賴的關係。如果 M 和 N 之間是可信賴的關係，意味著他們屬於同一聯盟，意即，兩者之 LMA(CRRM)可以相互溝通，並取得對方之網路資訊來幫助對方網路之 UE 進行換手。在本研究中，我們考慮的情況是當 M 和 N 互相之間是不可信賴的關係時，該如何改善換手過程。我們提出一個位於 Local Mobility Anchor (LMA)用以選擇目標基地台的演算法，和使用媒體獨立換手服務(IEEE 802.21 Media Independent Handover)來幫助 UE 於異質網路中順利地換手，另外，使用 Common Radio Resource Management (CRRM)機制也可以預先分配基地台資源，來保持網路的負載平衡。

關鍵字: 媒體獨立換手服務、CRRM、untrusted network、LTE-A、無線網路

Abstract

Recently, a user equipment (UE) is often equipped with more than one RAT (Radio Access Technology) to adapt itself to a heterogeneous network environment which comprises network systems of different models. On the other hand, besides the homogeneous/heterogeneous relationship between two adjacent network systems, e.g., M and N, the relationship between M and N can also be trustable and untrusted. We say M and N are trustable when they belong to the same alliance group, meaning they have signed a contract promising to provide network services to users of the other network. Basically, during handover, it would be better if we can choose a suitable base station to serve UE, balance network load and support session QoS. In fact, Common Radio Resource Management (CRRM) as a network resource management mechanism can help us to achieve this. In this study, we propose a target network selection mechanism for two adjacent untrusted networks, e.g., M and N, to select an appropriate base station in N when UE needs to hand over from M, i.e., source network (S-Net) to N, i.e., target network (T-Net). The base station selection algorithm is installed in Local Mobility Anchor (LMA). In order to enable the communication between the different types RATs, such as Long Term Evolution Advanced (LTE-A) and Wireless Local Area Network (WLAN) in a heterogeneous wireless environment, we adopt IEEE 802.21 Media Independent Handover (MIH) to help UE's vertical handover. With the CRRM, the load balance in a heterogeneous network environment can be also maintained. In our simulation, the performance of this scheme in an untrusted network handover case is better than that of PMIPv6 and FMIPv6.

Keywords－MIH; CRRM; untrusted networks; LTE-A; WLAN

Table of Contents

List of Figures

List of Tables

I. Introduction

Recently, a user equipment (UE) is often equipped with more than one RAT (Radio Access Technology) to adapt itself to a heterogeneous network environment which consists of network systems of different models. A typical example is that one is 802.16 Wimax [1] and others are 802.11 (WLAN) [2] and Long Term Evolution Advanced (LTE-A) [3]. When UE would like to move from one wireless system to another, due to requiring performing a series of network activities, the handover delay is often long [4].

On the other hand, besides homogeneous/heterogeneous relationship between two adjacent network systems, e.g., M and N, their relationship may also be trustable and untrusted. We say that M and N are trustable when they belong to the same alliance group, meaning they have signed a contract promising to provide network services to users of the other network. Here, we also assume that UE belongs to M and UE will hand over to N (i.e., target network, T-Net) from M (i.e., source network, S-Net). Also assume that, UE's serving MAG (called S-Net MAG or previous MAG, (PMAG)) can access the information provided by N. On the other hand, M and N are untrusted networks if they do not belong to the same alliance group. In this case, UE's serving MAG, i.e., PMAG, cannot access the information of the MAGs under the T-Net LMA which is the LMA in the target network, i.e., N [5]. Often their handover is performed in a reactive mode [6]. When UE enters the T-Net, i.e., N, N's AAA server will authenticate UE under the help of M's home AAA server [7]. After that, N starts serving UE.

In 2008, the IEEE 802.21 (Media Independent Handover, MIH) protocol [8] was proposed to help UE to hand over so as to shorten the handover delay and reduce packet loss rates. However, MIH works only when S-Net and T-Net are trustable. The handover based on MIH has been discussed in many studies [9-11].

Basically, during handover, it would be better if we can choose a suitable base station as NMAG to serve UE, and this choice truly balances network load [12] and supports session QoS. In fact, Common Radio Resource Management (CRRM) [13] as a network resource management mechanism can help us to achieve this. Houda *et al*. [14] proposed a scheme to optimize handover decision in an LTE-A network by using MIH and CRRM. The advantage of this scheme is that the selection of a target network is performed by CRRM based on load balancing. But CRRM entity and MIIS server need to exchange information frequently. Also, CRRM is applicable only when S-Net and T-Net are trustable.

The ANDSF [15], as a network entity assisting UE to hand over between 3GPP and non-3GPP base stations, collects information from MAGs belonging to a non-3GPP network and provides S-Net with the information for choosing a suitable MAG. But ANDSF can be applied also only when the two networks are trustable. To the best knowledge of ours, none studies have addressed untrusted network cases.

On the other hand, Leu *et al*. in [7] and Rasem *et al*. in [16] mentioned that the capability utilization of LMA is only 20%, which in fact can be further maximized. Furthermore, if S-Net and T-Net are two trustable networks, the MIIS server in S-Net stores the information of all base stations under both S-Net and T-Net and UEs under S-Net. So it is easy for UE or PMAG in S-Net to acquire the statuses of all base stations in T-Net. But if the two networks are untrusted, MIIS server in S-Net cannot collect the information of those base stations under T-Net. Therefore, it is hard for UE or PMAG in S-Net to choose an appropriate target base station when UE needs to hand over to T-Net.

Therefore, in this study, we propose a target network selection mechanism, named Target-MAG Selection in an Untrusted System (TMSUS for short), for two adjacent untrusted networks, e.g., M and N, to select an appropriate base station in N when UE needs to hand over from M to N. The base station selection algorithm is installed in LMA. Once S-Net MAG (i.e., PMAG) discovers that UE's signal is weak, it requests S-Net LMA to autonomously choose one of its MAGs in T-Net as the UE's NMAG.

The contributions of this study are as follows

(1) We have reduced the burden of MAG, and maximize the utilization of LMA.

(2) The signaling costs of the TMSUS are lower than those of FMIPv6 and PMIPv6 and its handover delay is also shorter than the two schemes'.

(3) A network entity (MAG-discovery Entity) is proposed to help two untrusted LMA communicate with each other.

(4) With the CRRM, an appropriate base station in an untrusted-heterogeneous network system can also be chosen.

Often, different names are given to one thing in different systems or protocols. For example, in FMIPv6, PMIPv6 and MIH, a mobile node is called MN. But in LTE, MN is named user equipment (UE). In FMIPv6 and PMIPv6, the name of a base station is AR and MAG, respectively. In MIH and LTE, it is called Point of Attachment (PoA) and eNodeB, respectively. In this study, we unify these names, e.g., mobile node as MN, base station as MAG, and CRRM/MIIS Server as LMA as illustrated in Table 1. In this study, we assume that MN hands over from home network to a neighbor untrusted network.

The rest of this paper is organized as follows. Section 2 introduces the background and related studies of this paper. Section 3 describes our scheme. The simulation results are shown and discussed in Section 4. Section 5 concludes this study and outlines our future studies.

Table 1. Names of network entities in FMIPv6, PMIPv6, MIH and LTE-A.

	FMIPv6	PMIPv6	MIH	LTE-A	This study
Mobile node	MN	MN	MN	UE	MN
Base station	AR	MAG	PoA	eNodeB	MAG
Local Mobility Anchor		LMA		MME	LMA

II. Background and Related studies

2.1 IEEE 802.21

In 2006, Internet Engineering Task Force (IETF) proposed the IEEE802.21 Media Independent Handover (MIH) which helps MN to exchange information for handing over in a homogeneous or heterogeneous wireless environment. Media Independent Handover Function (MIHF) as one of the features of MIH shown in Figure 1 is a 2.5-layer system built in MNs, MAGs and LMAs. MIH provides three services, including Media Independent Event Service (MIES), Media Independent Command Service (MICS) and Media Independent Information Service (MIIS). MIES is used to monitor a network, and then the information it collects is stored in MIIS Server. If MN needs to hand over, MICS assists users to issue required commands.

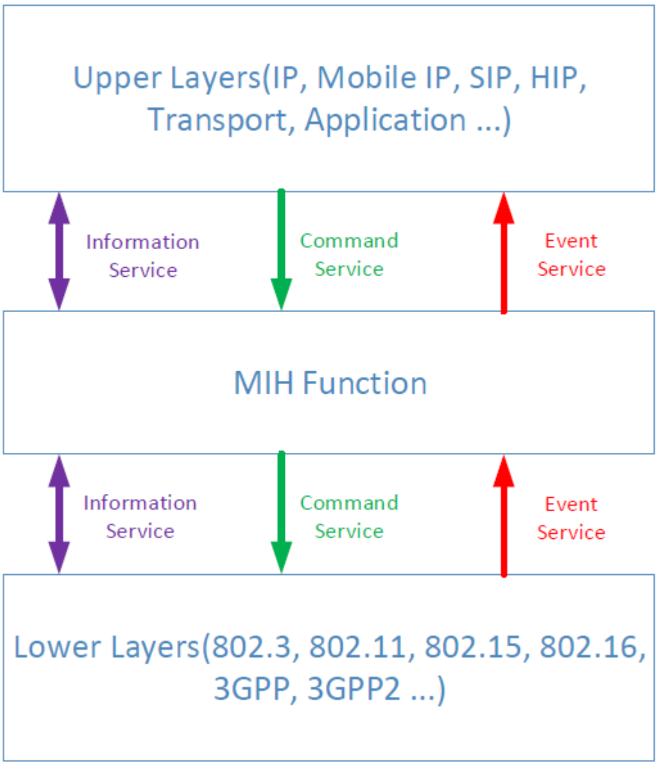

Figure 1. MIH Functions [8].

The communication between MIH and its upper layers as shown in Figure 2 goes through the Services Access Points (SAPs) which is a set of primitives defined in [8]. MIH_SAP is the interface between MIHF layer and MIHF users. The interface between the MIH and its lower layers in the protocol stack is MIH_LINK_SAP. MIH_NET_SAP supports information exchange between MIHF and remote MIHF entities.

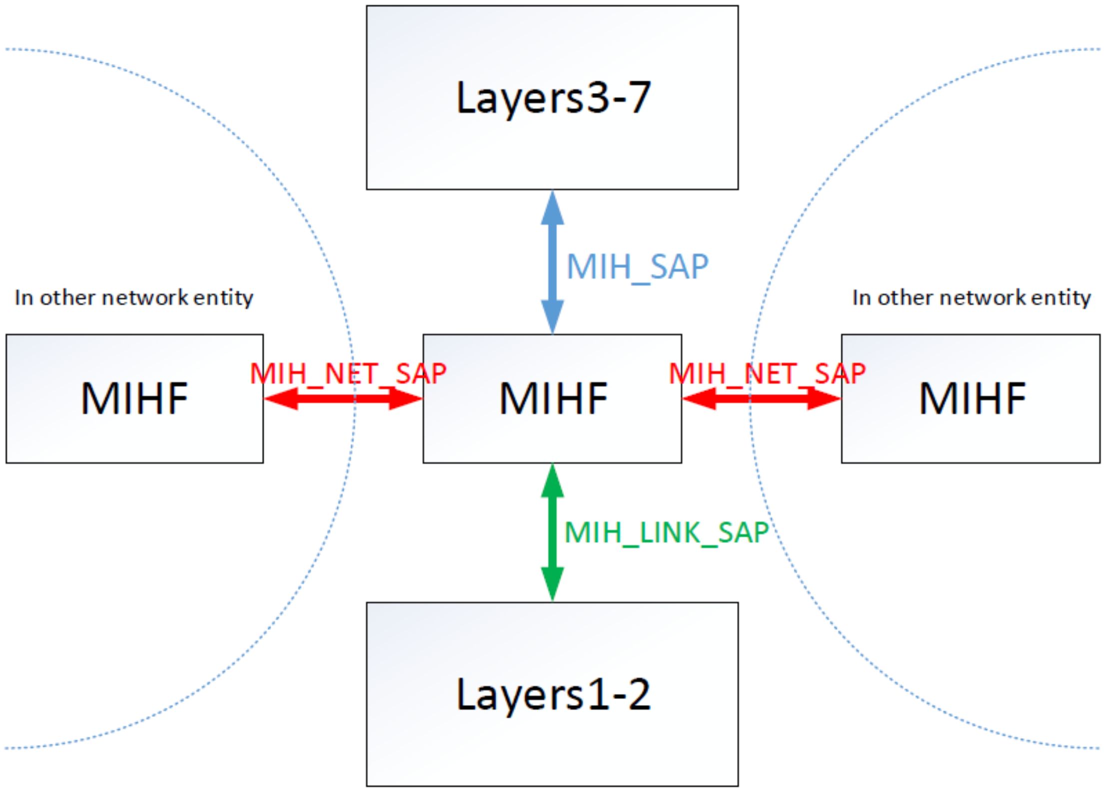

Figure 2. MIH_SAPs.

The handover procedure under MIH's assistance consists of three steps, including handover initiation, handover preparation, and handover execution, in which handover initiation is the process executed when MN's RSSI is lower than the threshold of RSSI. MN's MIHF will send a primitive MIH_Link_Going_Down to MIH user. Handover preparation is the process in which NMAG reserves network resources for MN's handover. Handover execution is the procedure performed by MN and NMAG when MN enters the communication range of NMAG and attaches to NMAG. The responsibility of MIH is handing the first two, i,e., handover initiation and handover preparation.

2.2 SCTP

The Stream Control Transmission Protocol (SCTP), defined in RFC 4960 [17] by IETF Signaling Transport (SIGTRAN) working group in 2000, has been maintained by the IETF Transport Area (TSVWG) working group. SCTP has two features, multi-homing and multi-streaming. Multi-homing is a specific characteristic of an association. The association between two nodes consists of K links, i.e., each of the two nodes has K IP addresses, $K \geq 1$. One of the links will be chosen as the primary path and others are called backup paths or alternate paths. When primary path fails or its transmission quality is poor, one of the backup path will be chosen to take over for the primary one. This connection policy provides high qualities of transmission and reliability. The multi-streaming reduces the latency due to the Head of Line (HOL) blocking [18], thus speeding up multi-process communication.

2.3 The Common Radio Resource Management (CRRM)

CRRM [19], i.e., Joint Radio Resource Management (JRRM), as shown in Figure 3 is a two-tier RRM model. It has been proposed to balance network load. The CRRM entity as the upper tier of the model is installed in LMA. It manages a number of Radio Resource Management (RRM) (or called local RRM, LRRM) entities installed in MAGs and is able to communicates with other CRRM entities.

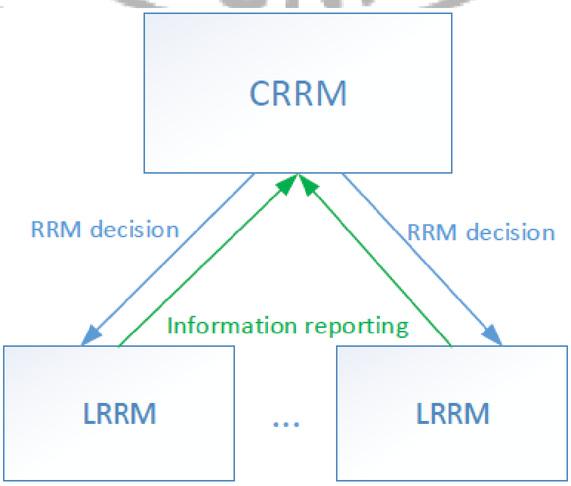

Figure 3. Two-tier RRM model.

In fact, the RRM mechanism provides Power Control (PC), Handover Control (HC), Packet Scheduling (PS), Congestion Control (CC) and Admission Control (AC) functions. The interaction between RRM and CRRM entities is implemented by using two basic functions, i.e., report function and LRRM decision function. The former allows RRM entities to report recent status of its MAG to CRRM. The status contains static information, including cell capabilities, QoS, etc., and dynamic information, including cell load, signal strength received (RSS), interference strength, etc.

The LRRM decision function, as shown in Figure 4, defines how LRRM and CRRM entities interact with each other for selecting base stations. There are two models that can help UE or PMAG to achieve this. One is that CRRM makes a decision and informs an LRRM entity to follow. The second is that the CRRM only provides related information and advises an LRRM entity to make a decision, i.e,. selecting a base station (i.e., NMAG) by LRRM itself.

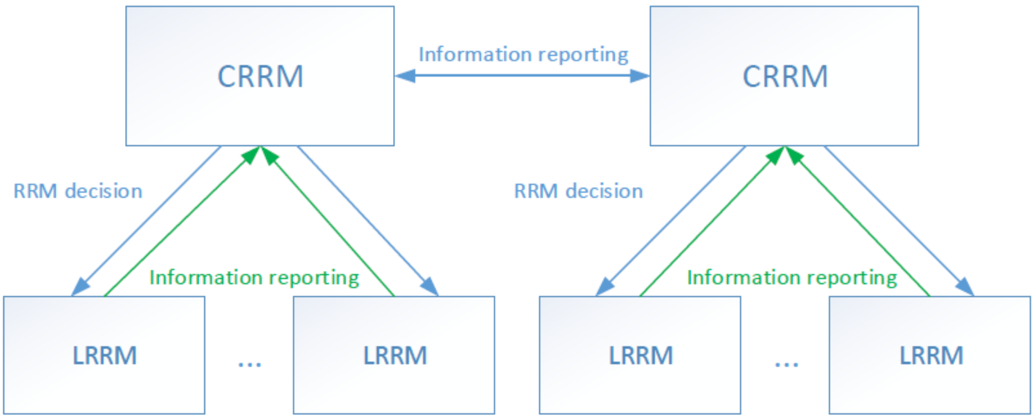

Figure 4. CRRM interaction model.

The degree of an interaction as shown in Table 2 can be divided into four levels: Low, Intermediate, High, and Very High. Low interaction degree means that most of the functions are performed by LRRM, whereas Very High interaction degree indicates that most of the functions are done by CRRM. A higher interaction between CRRM and LRRM often results in higher efficiency of radio resource management since the information is newer, of course, consuming higher signaling costs.

Table 2. The degrees of interaction between CRRM and LRRM.

Degree of Interaction	Time Scale	CRRM Functions	LRRM Functions
Low	Hours/days	Policy translations and configuration	Initial RAT selection, vertical handover, admission control, congestion control, horizontal handover, packet scheduling, power control
Intermediate	Minutes	Policy translations and configuration, initial RAT selection, vertical handover	Admission control, congestion control, horizontal handover, packet scheduling, power control
High	Seconds	Policy translations and configuration, initial RAT selection, vertical handover, admission control, horizontal handover	Packet scheduling, power control
Very High	Milliseconds	Policy translations and configuration, initial RAT selection, vertical handover, admission control, horizontal handover, packet scheduling	Power control

2.4 Related Work

Recent researchers have tried to improve handover performance for a heterogeneous environment by using IEEE 802.21 MIH standard. Mussabbir *et al*. [20] proposed a scheme to optimize FMIPv6 in a vehicular network. They designed a cross-layer mechanism for making an intelligent handover decision and creating a repository to store neighbor-network information. Its advantage is reducing network-prediction time. But MN's power consumption is high because the prediction is done by MN. This may seriously shorten the available time of battery. The scheme proposed by Ha *et al*. in [21] balanced network loads by using a traffic balancing architecture for heterogeneous wireless networks. But serious interference among base stations cannot be avoided. Wang *et al*. [22] proposed a framework which enhances MIH by developing a function providing seamless mobility management. Nevertheless, it may bring heavy signaling overheads to users. Buiati *et al*. [23] proposed a hierarchical MIIS architecture to diminish MIIS response time and reduce the latency of heterogeneous vertical handover.

2.5 Untrusted Networks

Figure 5 shows the signals exchanged in current untrusted network handover. We assume that when MN needs to hand over to T-Net, the S-Net LMA does not have the information of T-Net MAGs. So S-Net LMA is unable to choose a suitable T-Net MAG for MN. MN must disconnect itself from S-Net MAG (PMAG) before it can connect to T-Net MAG (i.e., NMAG). When MN enters the communication range of NMAG, it sends primitive MIH_MN_HO_Commit.request to NMAG to request network services. NMAG then passes this primitive to T-Net LMA. Then T-Net LMA delivers authentication.request to T-Net AAA server to request it authenticating MN.

After the authentication, T-Net AAA server sends authentication.response to T-Net LMA to tell it the completion of the authentication procedure. When T-Net LMA receives this primitive, it sends MIH_HO_Indication to PMAG through S-Net LMA to tell PMAG the IP of NMAG so as to establish the bidirectional tunnel between PMAG and NMAG. T-Net LMA also sends MIH_Resource_Allocation.request to T-Net MAG (i.e., NMAG) to allocate the resources for MN. Then NMAG internally delivers resources-allocation primitive (not shown) to its MIH to allocate resources. After the allocation, NMAG reports T-Net LMA with a MIH_Resource_Allocation.response. Following that, NMAG also sends two primitives, i.e., MIH_MN_HO_Commit.response to MN for committing the service request, and MIH_Resource_Report.request to T-Net LMA telling it the status of this MAG after the MN connects to NMAG successfully. Finally, T-Net LMA sends MIH_Resource_Report.response as an acknowledgement to NMAG.

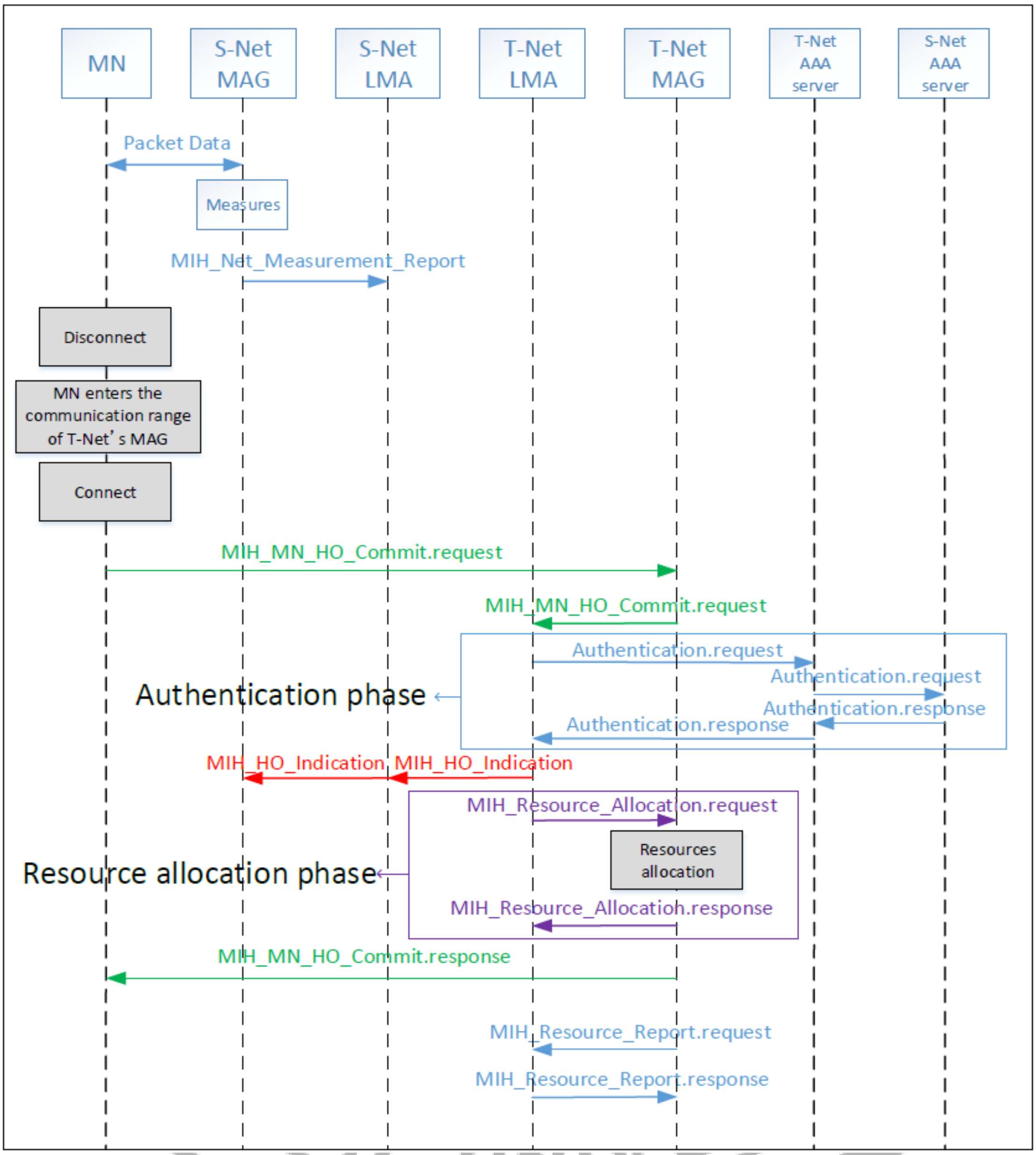

Figure 5. The primitives exchanged in current untrusted network handover (i.e., in reactive mode).

2.6 Signals of FMIPv6 Handover

The primitives exchanged in FMIPv6 [24] for handover are shown in Figure 6. At first, each MN and MAG in the system periodically send their information, such as Signal-to-Interference-plus-Noise Ratio (SINR), Received Signal Strength Indication (RSSI), etc., to CRRM. The information is conveyed in some primitives defined in IEEE802.21 MIH standard. MN's MIHF sends MIH_Get_Information.request (see dashed rectangle in Figure 6) to CRRM to acquire the statuses of neighbor base stations. CRRM replies MN with MIH_Get_Information.response. When MN's RSSI is lower than $RSSI_{th}$, MN's MIHF sends MIH_Link_Going_Down to the mobile user to indicate that there will be an event. The user then sends MIH_MN_HO_Candidate_Query.request back to its MIHF. MN's MIHF passes this primitive to MIIS Server through AP MIHF to enquire nearby base-station information which is then conveyed in the MIH_MN_HO_Candidate_Query.response sent by MIIS server to MN's MIHF through AP's MIHF. With this information, MN chooses the next MAG (NMAG for short). After that, MN sends MIH_MN_HO_Commit.request to CRRM through the serving MAG (in Figure 6, it is an AP) to request handover. On receiving this primitive, CRRM sends MIH_Resource_Reservation.request to NMAG (in Figure 6, it is eNodeB) to reserve the required resources (e.g., wireless uplink and downlink channels, backhaul transmission bandwidth, etc.) for MN. When NMAG receives this primitive, it internally delivers MIH_Resource_Allocation.request to its own RRC for resources allocation since in an eNodeB, wireless resources are managed by RRC. After that, MIH_Resource_Allocation.response will be sent to eNodeB's MIHF by RRC. Then the NMAG sends a MIH_Resource_Reservation.response primitive to CRRM. CRRM replies MN with MIH_MN_HO_Commit.response. When MN enters the communication area of the NMAG and attaches to it, NMAG sends a MIH_Resource_Report.request to CRRM telling CRRM the arrival of this MN and

CRRM replies NMAG with MIH_Resource_Report.response as an acknowledgement.

2.7 Signals of PMIPv6 Handover

In PMIPv6 [25], the primitives exchanged among network entities are shown in Figure 7. Those primitives originally designed for handover and sent by MN in FMIPv6 are now delivered by previous MAG (i,e., PMAG), since PMAG is the proxy of MN. The main difference between FMIPv6 and PMIPv6 is which network entity decides to hand over. When MN's RSSI is lower than $RSSI_{th}$, PMAG will sends MIH_MN_HO_Candidate_Query.request (see the dashed rectangle in Figure 7) to CRRM to acquire the statuses of neighbor base stations with which to choose a suitable NMAG for MN. CRRM will deliver MIH_MN_HO_Candidate_Query.response, which carries the statuses of neighbor base stations, to PMAG. In FMIPv6, this primitive is issued by MN. The remaining sections of resources reservation are almost the same as those of FMIPv6. We do not redundantly describe them.

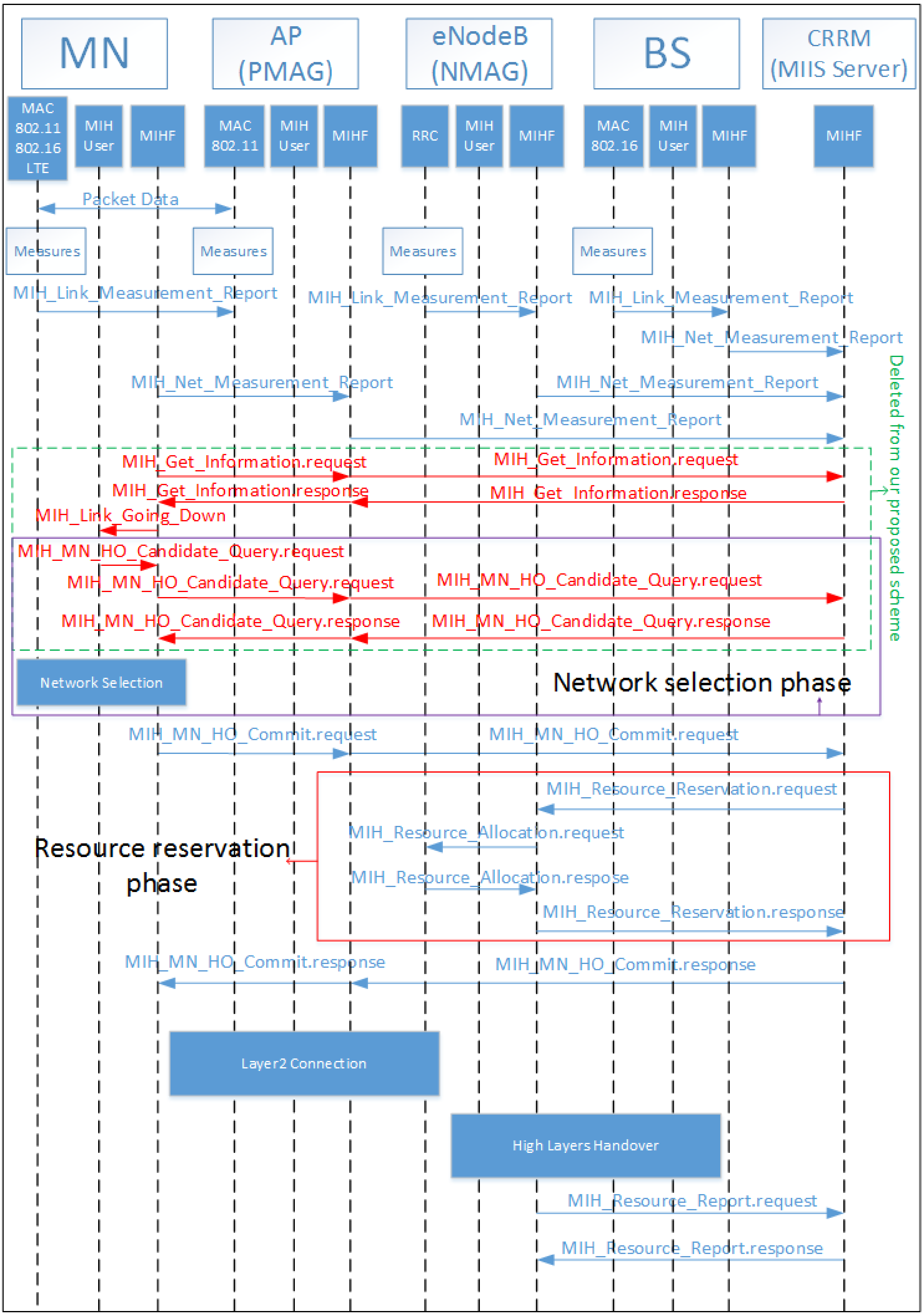

Figure 6. The primitives exchanged based on MIH in the handover procedure of FMIPv6.

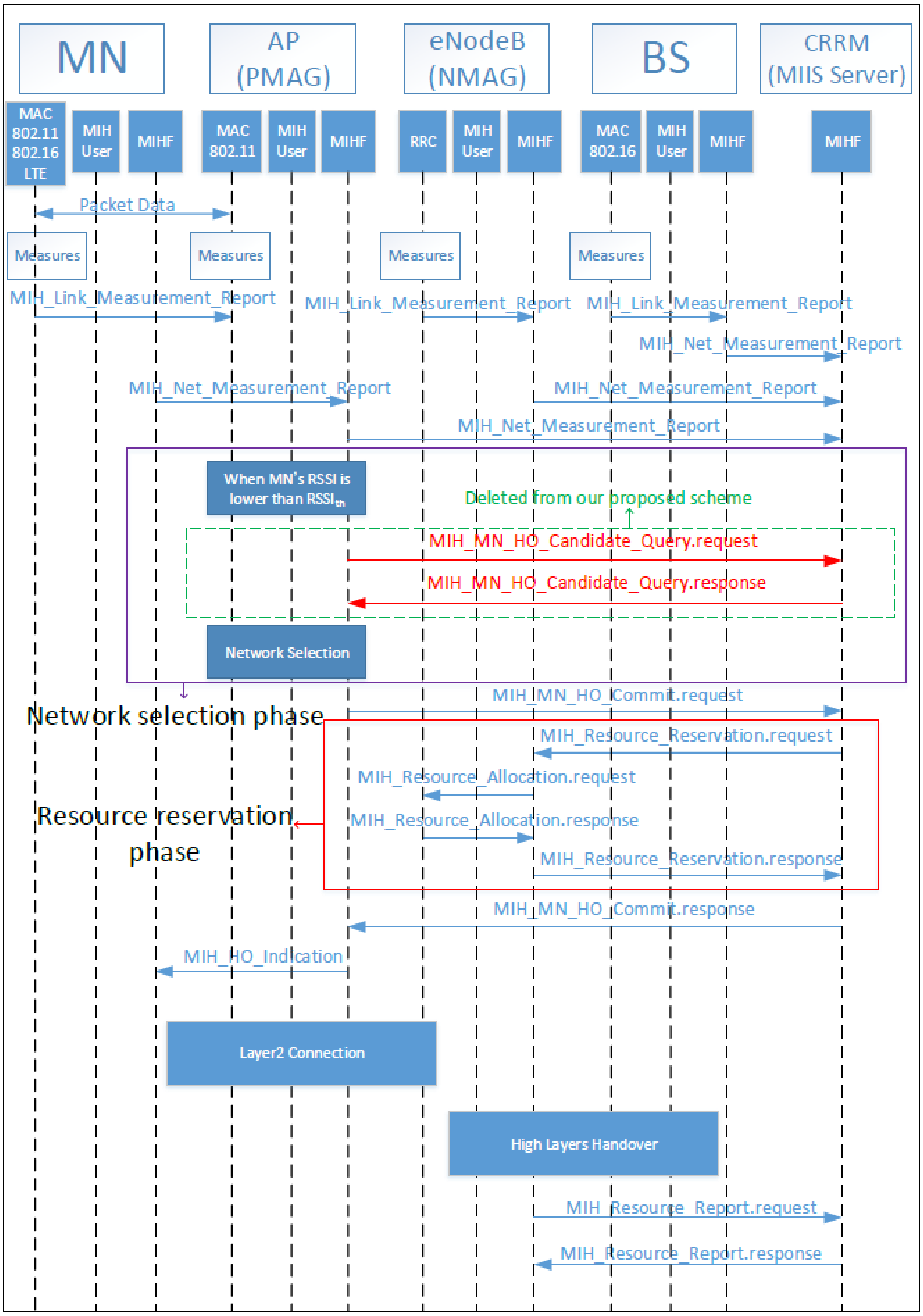

Figure 7. The primitives exchanged based on MIH in the handover procedure of PMIPv6.

III. Proposed Scheme

As mentioned above, in this study, the TMSUS is proposed to solve the handover problem in an untrusted environment. In order to diminish handover delay and signaling cost, our handover decision algorithm is installed in LMA. MIH is also employed to help heterogeneous network handover and CRRM mechanism is utilized to balance network load.

If S-Net and T-Net are two adjacent untrusted networks, the primitives exchanged among network entities are shown in Figure 8, in which MN is now in S-Net. An MIH-enabled network entity, called MAG-discovery Entity, which helps S-Net LMA to acquire the information of T-Net MAGs through MIH is developed. At first, MN's serving MAG (i.e., S-Net MAG, also known as PMAG) periodically sends MIH_Net_Measurement_Report which carries the status of the link between MN and PMAG (also called an active link) to S-Net LMA. When MN needs to hand over to T-Net, the S-Net LMA will send the MIH_HO.Indication.request to MAG-discovery Entity to request a suitable MAG for MN. (once MAG is determined, the T-Net follows) After receiving this request, MAG-discovery Entity passes this primitive to T-Net LMA. Then T-Net LMA delivers Authentication.request to T-Net AAA server which will in turn request S-Net AAA server to authenticate MN. After the authentication, on receiving Authentication response from S-Net AAA server, T-Net AAA server passes this primitive to T-Net LMA. T-Net LMA then selects a suitable MAG for MN and sends MIH_Resource_Reservation.request to T-Net MAG (i.e., NMAG). When NMAG receives this primitive, it internally delivers a MIH_Resource_Allocation.request primitive (not shown, but please refer to the second step of the Resource reservation phase in Figure 7) to its MAC layer to allocate resources for MN. After the allocation, NMAG reports T-Net LMA with a MIH_Resource_Reservation.response primitive. T-

Net LMA sends MIH_HO_Indication.response which carries IP of NMAG to MAG-discovery Entity. MAG-discovery Entity passes this primitive to CRRM in S-Net LMA. S-Net LMA sends MIH_HO_Indication.response which carries IP of NMAG to S-Net MAG (PMAG). PMAG in turn delivers MIH_HO_Indication to MN. When MN enters the communication area of the NMAG and attaches to it, NMAG sends a MIH_Resource_Report.request primitive to T-Net LMA telling it the arrival of this MN. Finally, T-Net LMA sends MIH_Resource_Report.response as an acknowledgement back to NMAG to end this handover.

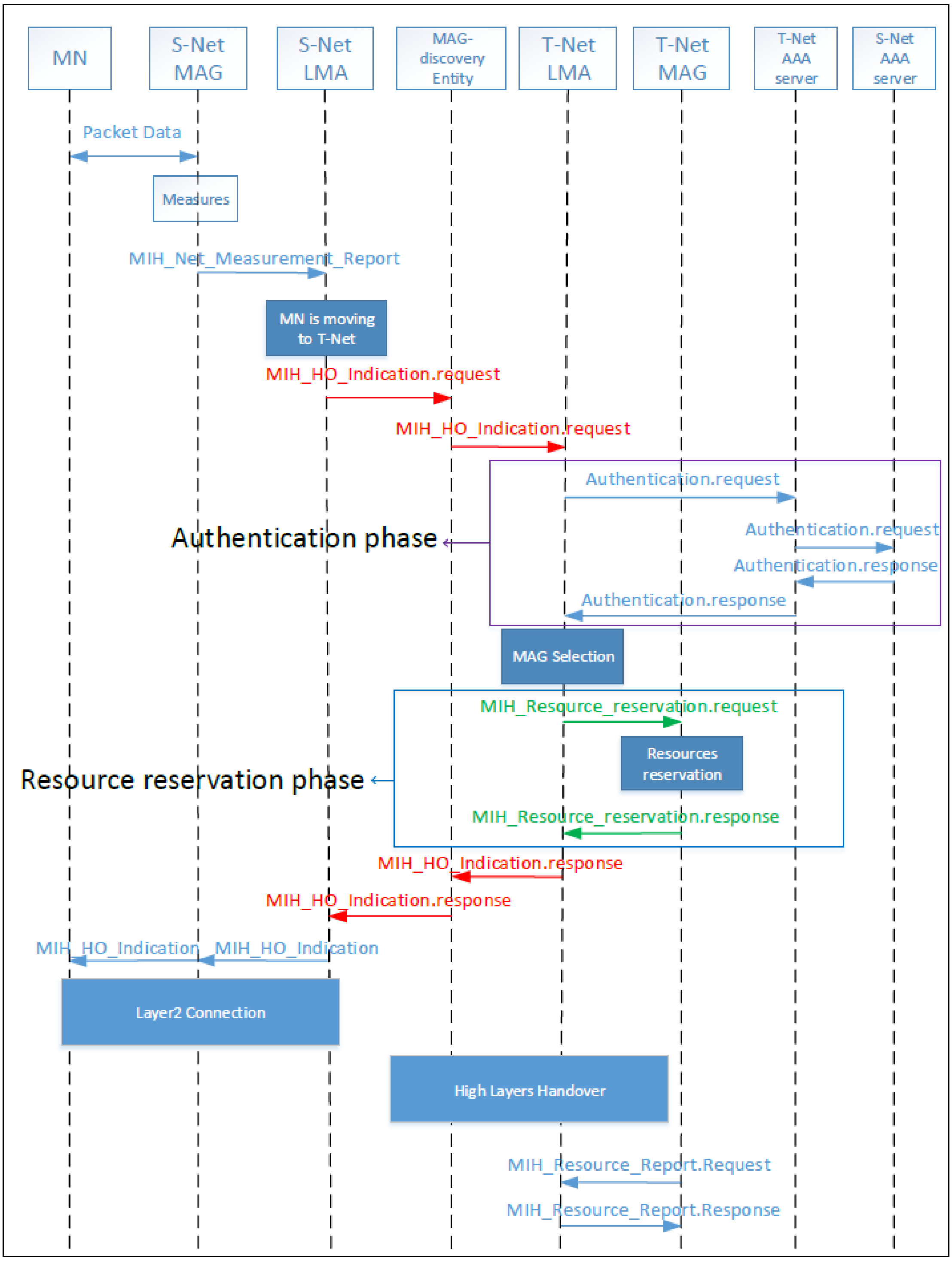

Figure 8. The primitives exchanged in untrusted networks handover case (MN hands over from S-Net to T-Net).

3.1 MAG-discovery Entity

The main function of MAG-discovery Entity is mediating the working processes of two untrusted networks, i.e., T-Net LMA and S-Net LMA. This entity basically is created by a trustable third party. Figure 9 shows an example topology, in which there are 4 untrusted networks. S-Net LMA cannot enquire the information of T-Net MAGs. With the help of MAG-discovery Entity, when MN needs to hand over from network 1 (i.e., S-Net) to network 2 (i.e., T-Net), S-Net LMA will communicate with T-Net LMA to request the information of T-Net MAGs and then notify MN with this information.

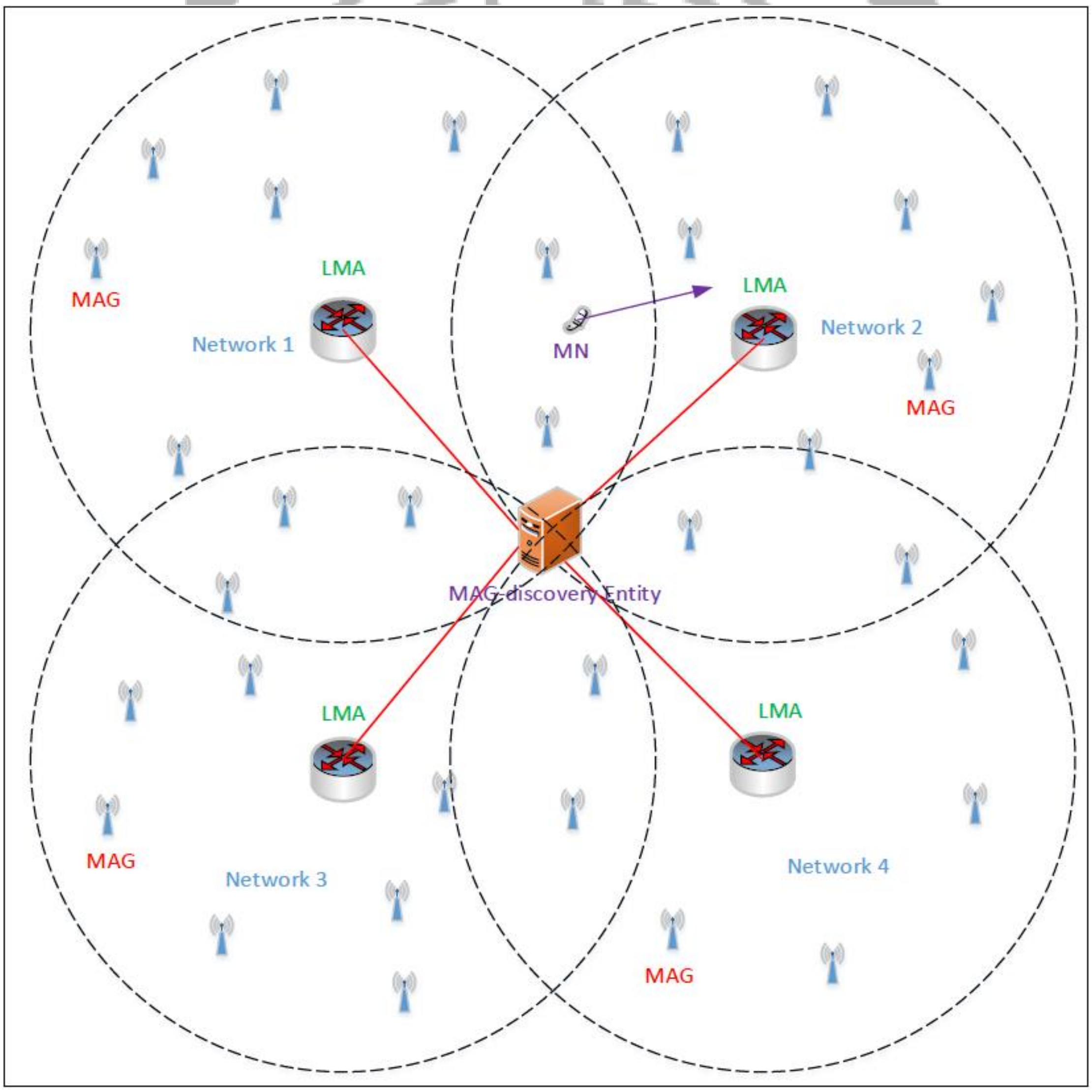

Figure 9. The topology of untrusted networks with the help provided by the MAG-discovery Entity.

3.2 MN Connection

Basically, MIH has five connections, denoted by MIH-R1to MIH-R5 [8] as shown in Figure 10. MIH-R1 is the connection between MN and previous S-Net MAG (PMAG), also called an active link. MIH-R2 is the connection between MN and a candidate MAG in one of S-Net's neighbor networks. With MIH-R2, MN is able to access the statuses of nearby MAGs from CRRM/MIIS Server via the PMAG, no matter whether these nearby MAGs belong to S-Net or other neighbor networks. Consequently, when MN has to hand over to another MAG, it chooses a nearby MAG as the NMAG based on the received statuses without the requirement of scanning candidate MAGs. In this study, we only use MIH-R1 and MIH-R2. The functions of MIH-R3 to MIH-R5 are defined in MIH standard [8].

In our scheme, when discovering that the PMAG is too busy to effectively serve MNs or MN's RSSI is lower than $RSSI_{th}$, CRRM autonomously notifies MN to build a MIH-R2 connection to one of the neighbor network's MIHF entities (i,e, NMAG) through MIH_NET_SAP (see Figure 2) by using the second IP of SCTP. After handover and the MIH-R2 connection is built (i.e., now active link), the MIH-R1 will be disconnected. This is a make-before-break feature of MIH. In the offloading case, MIH-R1 and MIH-R2 connections need to be kept until current session finishes since we assume that offload can be performed only when MN stays at its current position without handing over to other MAG. How to make sure that MN is still so that offload can be performed will be another topic which is out of scope of this study. In fact, we focus on how to choose a suitable NMAG for MN by CRRM to build the MIH-R2 connection.

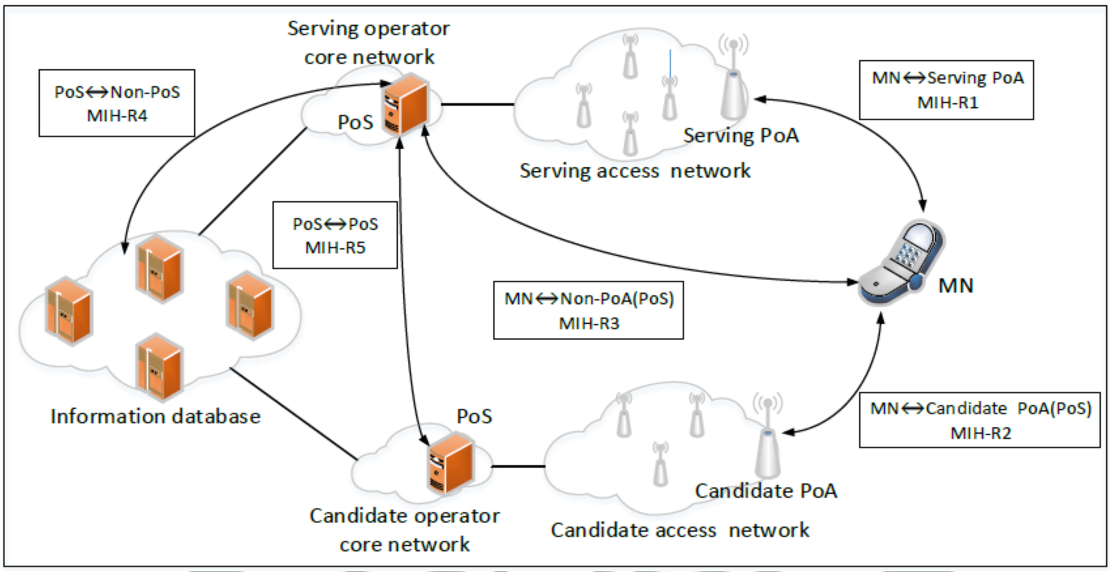

Figure 10. MIH Connections [8].

3.3 Signaling cost

In our scheme, several primitives originally defined by MIH standard, including MIH_Get_Information, MIH_Link_Going_Down, and MIH_MN_Candidate_Query.request and MIH_MN_HO_Candidate_Query.response (see Figure 6) used in FMIPv6 or PMIPv6 system, are deleted to reduce MN's handover cost and delay without losing the functions of handover and traffic offload.

Figure 11 shows the primitives exchanged in the handover procedure of the TMSUS. They can be divided into network selection and resources reservation phases. Here we assume that a mobile node, i.e., MN, will hand over from WiFi AP (i.e., PMAG) to LTE-A eNodeB (i.e., NMAG). When S-Net CRRM discovers that MN's RSSI value is lower than the predefined $RSSI_{th}$, it chooses a NMAG based on the information collected in its database, and sends our proposed new primitive MIH_Resource_Reservation.request to MIHF of NMAG (i.e., eNodeB). The purpose is requesting NMAG to reserve resources for the MN. The MIHF sends MIH_Resource_Allocation.request to its RRC. After reserving required resources, RRC replies the MIHF with MIH_Resources_Allocation.response. NMAG's MIHF then delivers MIH_Resources_Reservation.response to S-Net CRRM. Then the CRRM sends MIH_HO_Indication which carries the IP of NMAG to MN through PMAG (i.e., AP in Figure 11).

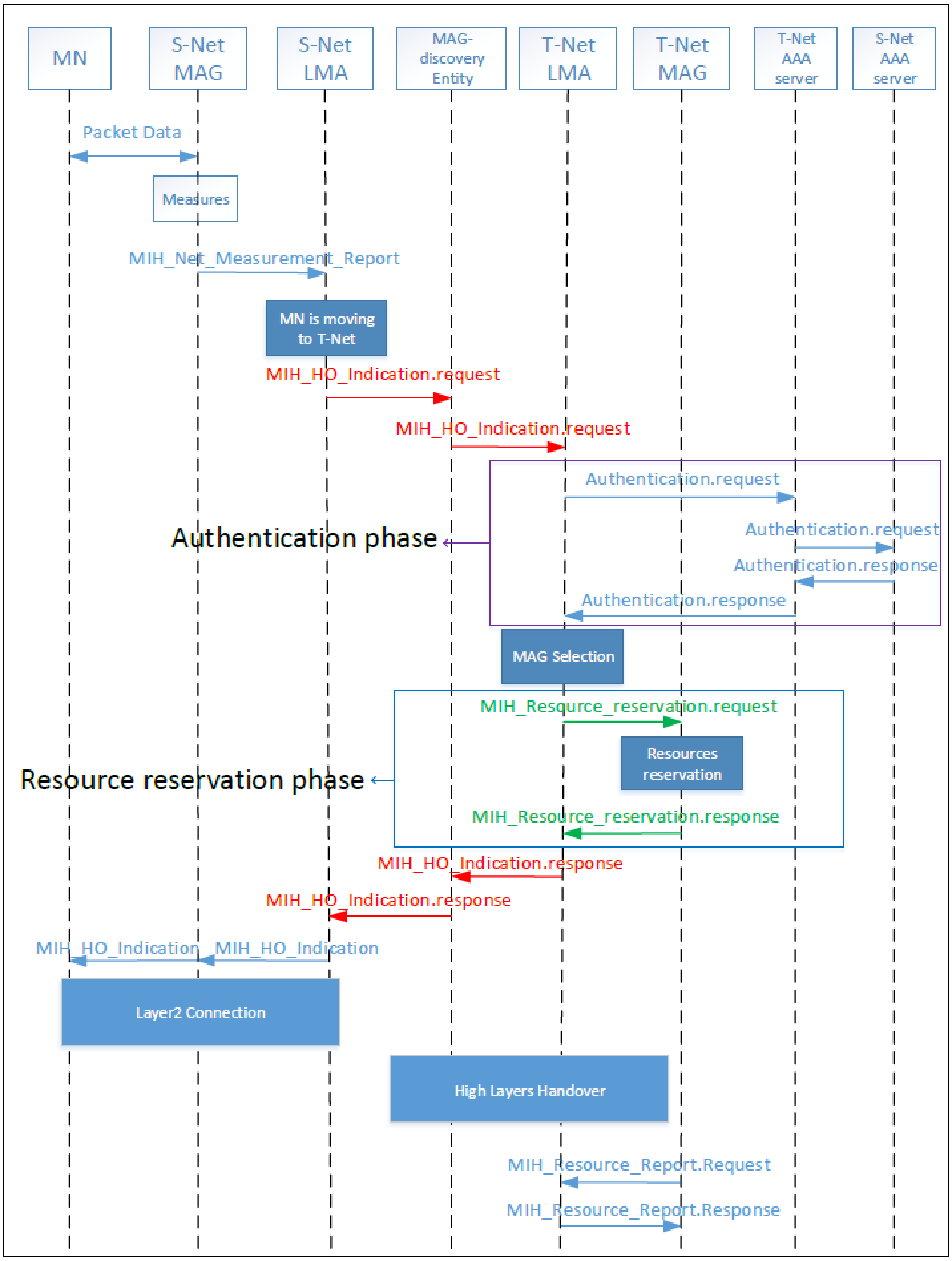

Figure 11. The primitives exchanged during the handover procedure of the TMSUS.

3.4 MIH / CRRM Database

The MIH database is one of the components of MIIS Server. We integrate the CRRM and MIIS Server in the LMA. To find a suitable MAG for MN, CRRM calculates the parameter data reported by LRRMs. Assume that there are m base stations $B = \{b_1, b_2, b_3, \ldots, b_m\}$, including those under the CRRM in S-Net and those near the boundary of S-Net but in the T-Net. Where b_i is a base station, $b_i \in B$, $1 \leqq i \leqq m$. Of course, if S-Net has K direct neighbors, these neighbors' MAGs near the S-Net will be collected in B. We further assume that each base station, i.e., b_i, provides n parameters, $T_i = \{term_{i,1}, term_{i,2}, term_{i,3}, \ldots, term_{i,n}\}$, where $term_{i,k}$ is the k^{th} parameter of b_i. Each parameter needs to be normalized to real number between 0 and 1, i.e., $term^u_{i,k} = \frac{term_{i,k} - Min(term_{i,k})}{Max(term_{i,k}) - Min(term_{i,k})}$ in which $term_{i,k}$ is the original value of this parameter, and $Max(term_{i,k})$ ($Min(term_{i,k})$) is the maximum (minimum) value in $term_{i,k}$'s domain. The purpose is to avoid parameters from large recessive weights, e.g., a parameter x's value is between 100 and 1000, and another, e.g., y's value, is between 1 and 10. Basically, the former's recessive weight is 100 times that of the latter. In other words, even x's value is the minimum (i.e., 100), y's value is the maximum (i.e., 10) and their weights are the same, e.g., 0.5, x is the dominate parameter since 0.5*100 is very large than 0.5*10, i.e., the result is almost determined by x. After normalization for all $term_{i,j}$, $1 \leqq j \leqq n$, $1 \leqq i \leqq m$, we can obtain a matrix $T=\{T_1, T_2, \ldots, T_m\}^{\mathrm{T}}$ for B. Let $W = \{w_1, w_2, w_3, \ldots, w_n\}$ be the weights of T_i, and let w_h be the weight of $term_{i,h}$, $1 \leqq h \leqq n$, $\sum_{h=1}^{n} w_h = 1$.

In fact, from available bandwidth consideration, the highest priority is homogeneous MAG since before and after handover, the bandwidth reserved for MN is the almost the same. This may reduce the narrow bandwidth effort which is the case when S-Net provides a higher bandwidth, e.g., BW_S and T-Net can only provide bandwidth, e.g., BW_T and $BW_S >> BW_T$. If MN is watching streaming TV or movie program, after it hands over to T-Net, the streaming speed will be lower, particularly when $B_T < |B_{str}|$ where B_{str} is the bandwidth for streaming such a TV / movie program.

The target MAG's ranking score on b_i, denoted by S_i, is calculated as

$$S_i = \sum_{h=1}^{n} w_h \cdot term_{i,h}^{u} \qquad (1)$$

where $1 \leqq i \leqq m$, $1 \leqq h \leqq n$. Let

$$S_p = \max_{1 \le i \le m}\{S_i\} \qquad (2)$$

The MAG b_p will be chosen as the target MAG. These two equations can also be used to select an AP for WiFi offload.

If there is no homogeneous MAG for MN. The LMA will calculate the score of candidate MAGs and select the highest one to be NMAG. The information recorded in the MIIS Server for a base station (MN) is shown in Table 2. (Table 3).

Table 3. Information recorded in the MIIS Server for a base station.

Parameters	Weight
Location	**0**
Bandwidth	**0.3**
End-to-end delay	**0.1**
Throughput	**0.1**
Drop rate	**0.1**

Table 4. Information recorded in the MIIS Server for MN.

Parameters	Weight
RSS	**0.1**
MN's moving direction	**0**
Angle$_{MN,MAG}$	**0.2**
Distance$_{MN,MAG}$	**0.1**

3.5 The angle between MN's moving direction and $\overrightarrow{MNMAG}$

The location of MN and MAG are expressed by (Longitude, Latitude), i.e., GPS format [26]. Note that the coordinate system of a GPS is different from the Cartesian coordinate system [27] and Polar coordinate system [28]. To simplify the coordinate calculation, we transform the MN's and MAG's location from GPS coordinate system into the Cartesian system. The results are expressed as (X_{MN} , Y_{MN}) and (X_{MAG} , Y_{MAG}).

The distance between MN and MAG, denoted by $D(MN, MAG)$ can be expressed by the Polar coordinates.

$$D(MN, MAG) = \sqrt{(|X_{MN} - X_{MAG}|)^2 + (|Y_{MN} - Y_{MAG}|)^2} \qquad (3)$$

The unit vector of $\overrightarrow{MNMAG}$, denoted by $\vec{V}(MN, MAG)$, is

$$\vec{V}(MN, MAG) = (X^{vector}_{(MN,MAG)}, Y^{vector}_{(MN,MAG)}) = (\frac{X_{MAG} - X_{MN}}{D(MN, MAG)}, \frac{Y_{MAG} - Y_{MN}}{D(MN, MAG)}) \qquad (4)$$

which is equal to $(\cos\theta', \sin\theta')$ where θ' is the counterclockwise angle between X-axis and $\overrightarrow{MNMAG}$ expressed by Polar coordinates. Let θ be the counterclockwise angle between X-axis and MN's moving direction. Table 4 indicates the moving direction of MN in the 4 quadrants of a Cartesian coordinate system.

Table 5. The moving directions of MN in the different quadrants of a Cartesian coordinate system [29].

$\cos\theta$	$\sin\theta$	Quadrant	MN's moving direction
>0	≥ 0	1	North and East
≤ 0	≥ 0	2	North and West
≤ 0	≤ 0	3	South and West
>0	≤ 0	4	South and East

Figure 12 shows that the angle between MN's moving direction and $\overrightarrow{MNMAG}$, denoted by α, is $\cos\alpha = \cos|\theta - \theta'|$.

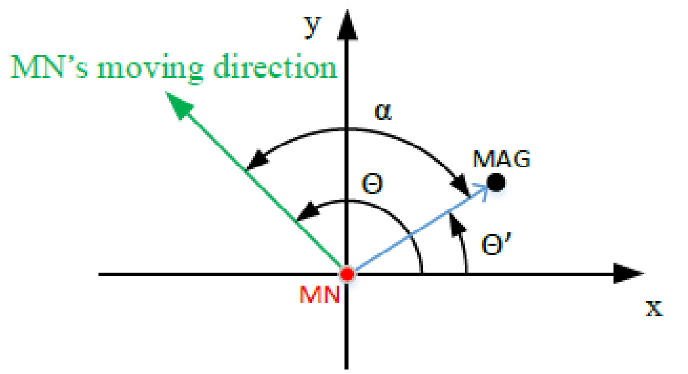

Figure 12. The angle between MN's moving direction and $\overrightarrow{MNMAG}$, denoted by $\alpha = |\theta - \theta'|$, $\alpha \leq 180^{\circ}$.

Note that the angle useful to us is $0^{\circ} \sim 180^{\circ}$ since $\cos\alpha = \cos(360^{\circ} - \alpha)$, i.e., when $\alpha > 180^{\circ}$, we let $\alpha = 360^{\circ} - \alpha$, as shown in Figure 13. The value of $\cos\alpha$ is between -1 and 1. When the value of $\cos\alpha$ is lower than 0, it means that the MN is moving away from, rather than approaching, the MAG. $\alpha = 180^{\circ}$, i.e., $\cos(180^{\circ}) = -1$ is the worst case since the moving direction is right opposite that of $\overrightarrow{MNMAG}$. Of course,

$\alpha = 0^{\circ}$, i.e., $\cos(0^{\circ}) = 1$ is the best case since MN is moving straight toward MAG. The RSSI will be stronger when MN moves forward.

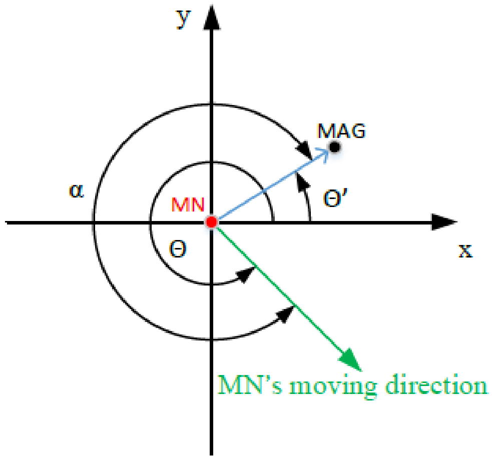

Figure 13. $\alpha > 180^{\circ}$, we let $\alpha = 360^{\circ} - \alpha$.

IV. Simulation and Discussion

In the study, five experiments were performed and the signaling costs of FMIPv6, PMIPv6 and TMSUS were analyzed. We simulate the TMSUS and current untrusted-network handover scheme (i.e., reactive mode) by using NS-2 and its mobility extension developed by National Institute of Standards and Technology (NIST) [30]. In the first experiment, the three tested schemes were analyzed given two untrusted heterogeneous networks, including LTE-A and WLAN. An MN is equipped with two network interface cards, one for LTE-A and the other for WLAN, each of which is assigned a unique IP and channel. MN hands over from LTE-A to WLAN. The second redid the first but in an untrusted-homogeneous environment. The third evaluated the signaling costs of the three tested schemes all under a trustable environment and an untrusted environment. The fourth experiment is calculating the times the three schemes spend for predicting NMAG under a trustable and an untrusted environment. The fifth compared the performance of TMSUS algorithm and current algorithm (based on RSS).

Three test metrics are employed, including throughput defined as the bit rate received over the data rate, end-to-end delay defined as the time required by a packet to travel from sender to receiver, and drop rate defined as the number of packets received over the number of packets sent. The specifications and network parameters of the test-bed used are illustrated in Table 6. Figure 14 shows the simulation topology.

Table 6. The specifications and default parameters of our tested.

Network parameter	Value
LTE-A bandwidth	200Mbps
WLAN bandwidth	54Mbps
Bandwidth of a wired link	500Mbps
Data rate	100Mbps
MN's moving speed	1 m/s
Simulation time	10 sec

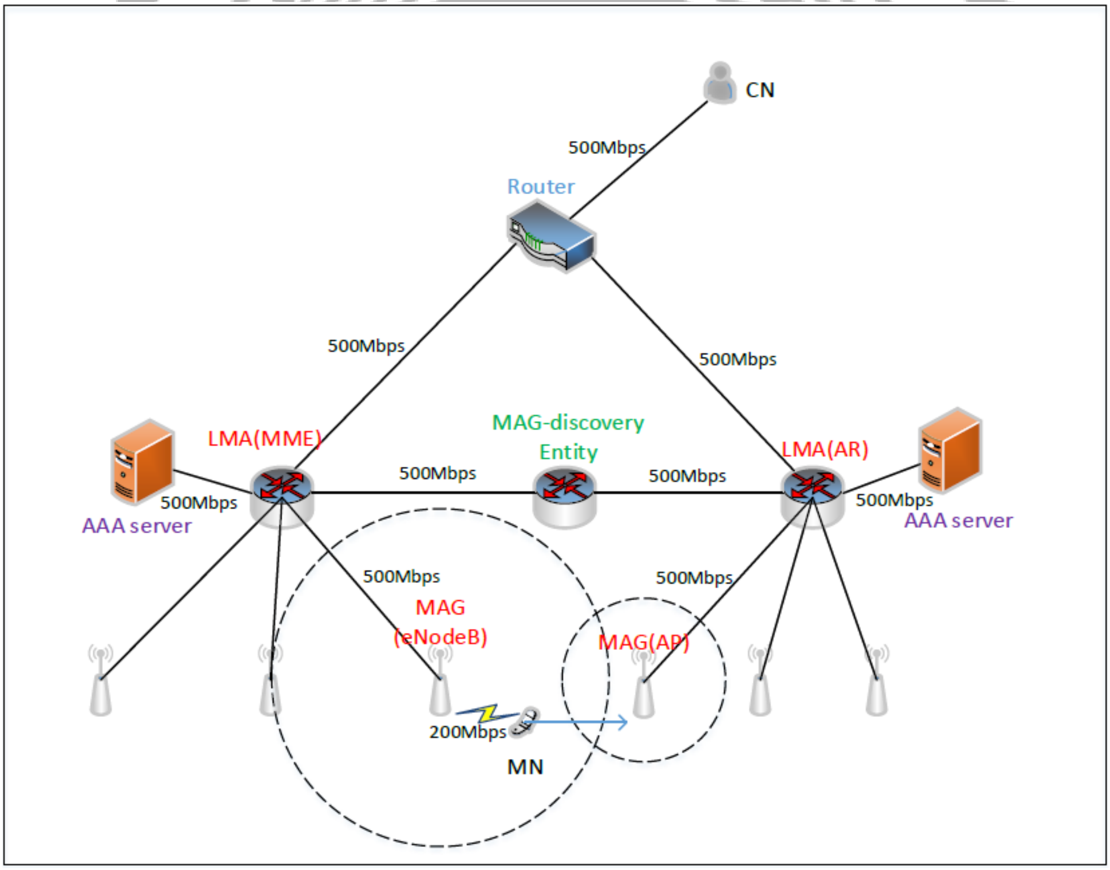

Figure 14. The topology of our simulation.

4.1 The First Experiment in a Heterogeneous Network

In the first experiment, MN is now being served by an LTE-A MAG and would like to hand over to a WLAN at the 5^{th} sec. After that, it hands over to LTE-A at the 8^{th} sec. Figure 15 shows the throughputs of the TMSUS, FMIPv6 and PMIPv6 (i.e., a reactive mode). Obviously, FMIPv6 and PMIPv6 are not better than the TMSUS since when MN of FMIPv6 and PMIPv6 hands over, it must disconnect itself from PMAG before connecting to NMAG, i.e., break-before-make. So FMIPv6's throughputs in the time periods between 5^{th} and 5.15^{th} sec and between 8^{th} and 8.15^{th} sec are 0. PMIPv6s throughputs between 5^{th} and 5.1^{st} sec and between 8^{th} and 8.1^{st} sec are also 0.

It is also clear that PMIPv6 is better than FMIPv6. The key reason is that in PMIPv6, PMAG as a proxy, issues handover process. This actually reduces its signaling cost. We will show this later. Figure 16 illustrates the drop rates. Because of active link disconnection, the drop rates of FMIPv6 and PMIPv6 during handover are 100% where an active link is the wireless link between MN and PMAG. Furthermore, the bandwidth of WLAN (i.e., 54 Mbps) is smaller than that of LTE-A (i.e., 200 Mbps). The drop rates during its stay in WLAN are about 53 % since data rate is 100 Mbps. Their end-to-end delays are plotted in Figure 17. Due to link disconnection during handover, the end-to-end delays of FMIPv6 and PMIPv6 are longer. Owing to the bandwidth of WLAN, the end-to-end delays in WLAN are about 1.8 msec and in LTE-A are about 0.1 msec.

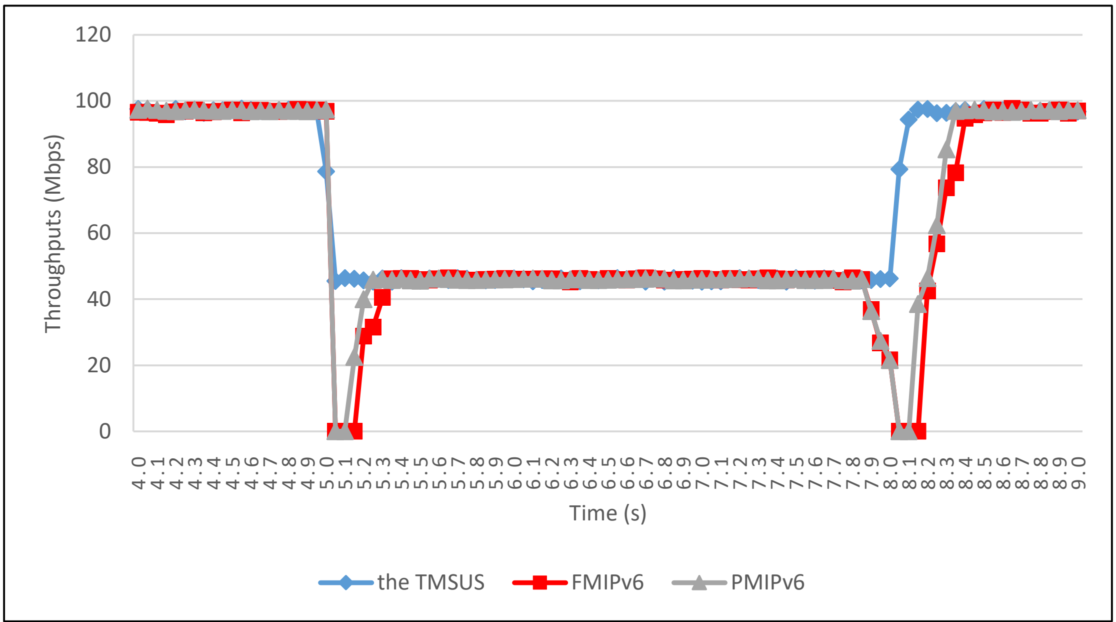

Figure 15. The throughputs between the 4th and 9th sec when MN hands over from LTE-A to WLAN and then from WLAN to LTE-A.

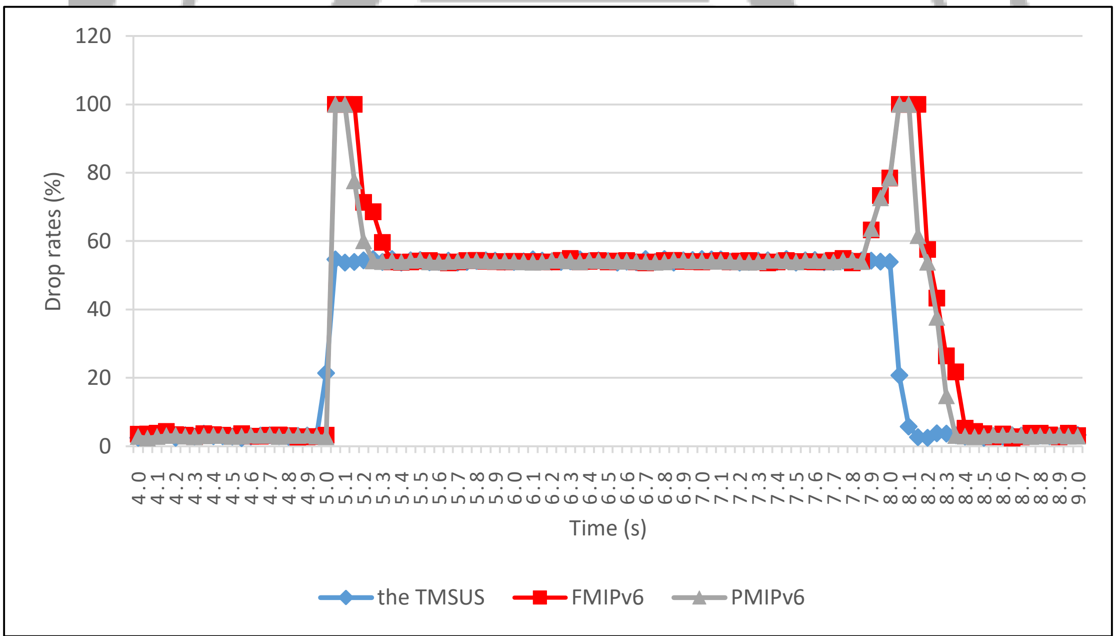

Figure 16. The drop rates between the 4th and 9th sec when MN hands over from LTE-A to WLAN and then from WLAN to LTE-A.

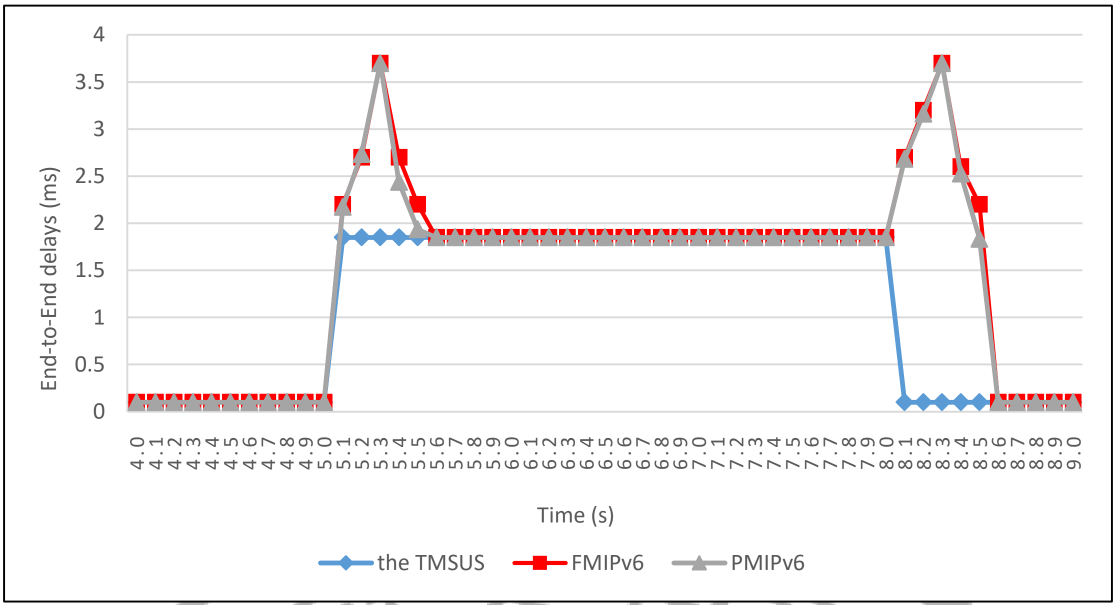

Figure 17. The end-to-end delays between the 4th and 9th sec when MN hands over from LTE-A to WLAN and then from WLAN to LTE-A.

4.2 The Second Experiment in a Homogeneous Network

In the second experiment, the three schemes are evaluated in an untrusted-homogeneous environment. This time, the bandwidth of LTE-A is set to 80 (rather than 100) Mbps and wired-link bandwidth is 100 (rather than 500) Mbps. At the beginning, MN is connected to an LTE-A, and it hands over to another LTE-A network at the 10th sec. Figure 18 shows the throughputs. Owing to the employment of MAG-discovery Entity and SCTP's multi-streaming and multi-homing characteristics, the performance of the TMSUS is better than those of FMIPv6 and PMIPv6. Figure 19 illustrates the drop rates. Because of active link disconnection, the drop rates of FMIPv6 (PMIPv6) are 100% between the 10th and 10.15th (between 10th and 10.10th) sec. The end-to-end delays are illustrated in Figure 20. Because before connecting to NMAG, MN must disconnect the active link. It is the reason why the end-to-end delays of FMIPv6 and PMIPv6 are higher than those of the TMSUS.

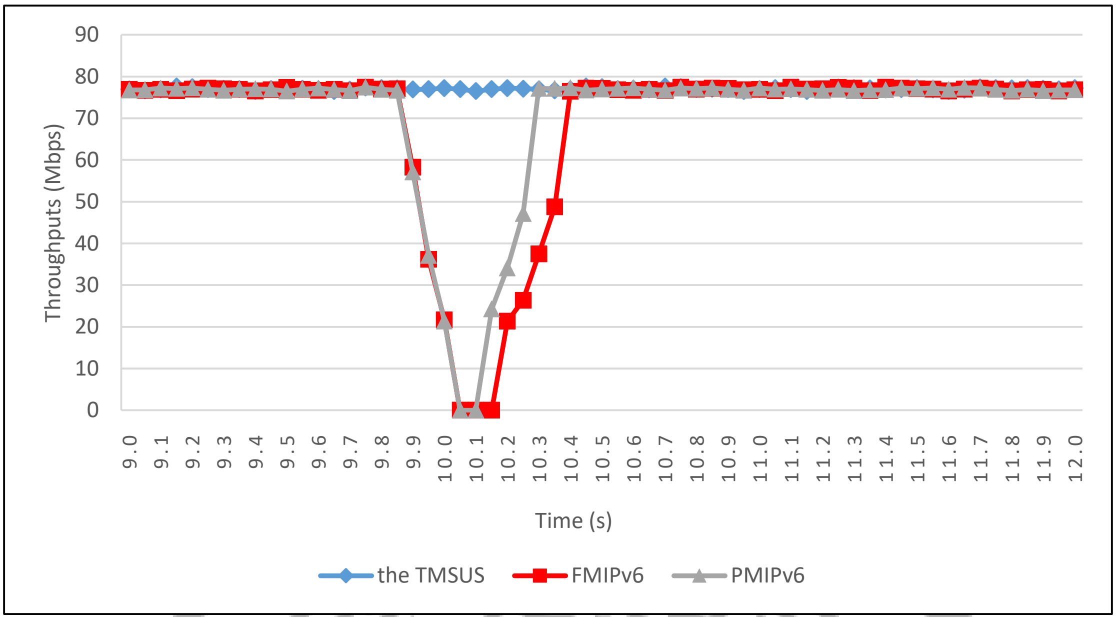

Figure 18. The throughputs between the 9th and 12th sec when MN hands over from LTE-A to LTE-A in an untrusted-homogeneous network environment.

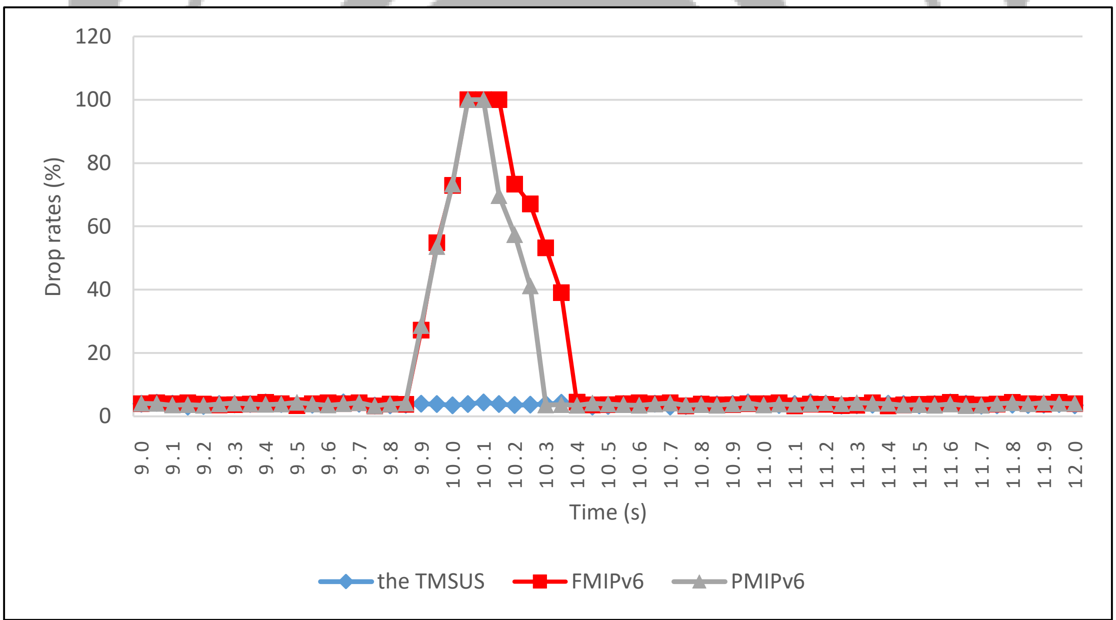

Figure 19. The drop rates between the 9th and 12th sec when MN hands over from LTE-A to LTE-A in an untrusted-homogeneous network environment.

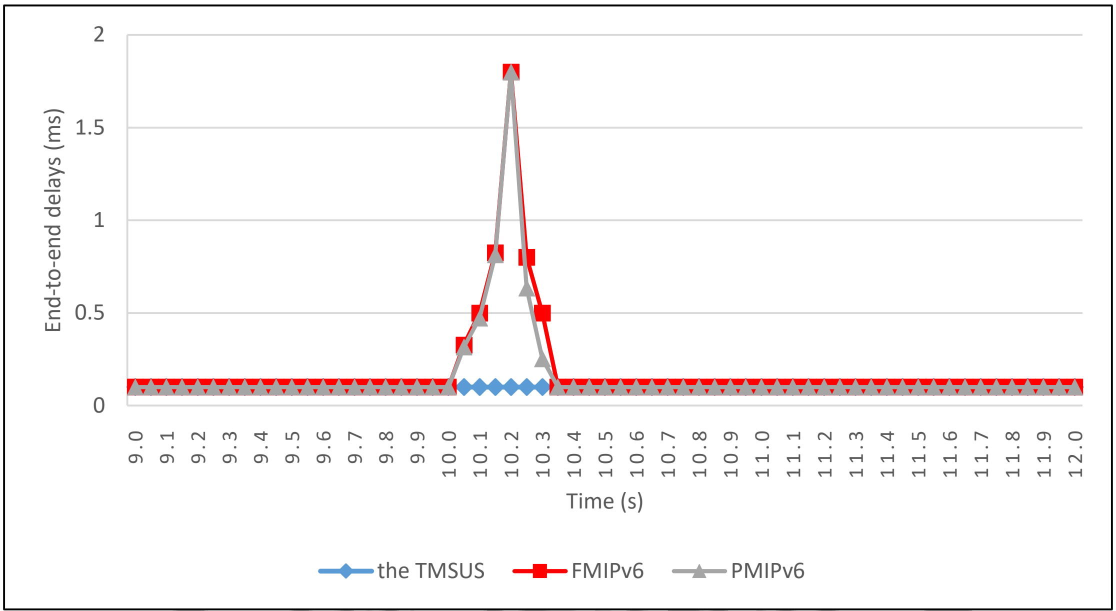

Figure 20. The end-to-end delays between the 9th and 12th sec when MN hands over from LTE-A to LTE-A in an untrusted-homogeneous network environment.

4.3 The Third Experiment-Signaling Costs of Different Schemes

The third experiment evaluates signaling costs of the TMSUS, PMIPv6 and FMIPv6 in a trusted environment and in an untrusted environment given different numbers of MNs, i.e., different network loads. The experimental results are shown in Figure 21. In the untrusted environment, the handover strategy of reactive mode is break-before-make, and no base station prediction is performed. So its signaling costs are lower than those of the untrusted-TMSUS. Also, in PMIPv6 and FMIPv6, after the disconnection, MN needs to wait for the accomplishment of authentication performed by T-Net's AAA server with the help of S-Net AAA server. Thus, their overall performance is lower than that of the TMSUS both in the trustable and the untrusted environments.

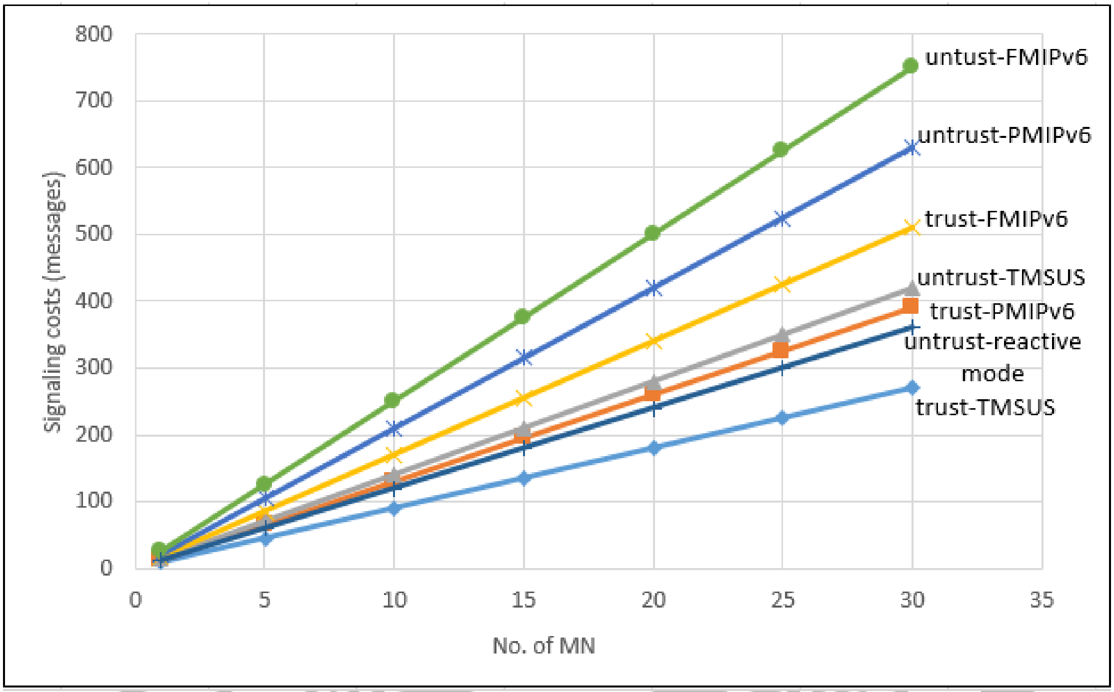

Figure 21. The signaling costs of different schemes on different numbers of MN.

4.4 The Times Consumed for predicting NMAG

In the fourth experiment, we simulate the time consumed by a scheme to predict NMAG in a trustable network environment and in an untrusted network environment. In the following, T(L2) denotes the time consumed by layer 2 to trigger corresponding handover. The time consumed by a network entity V to deliver a message (primitive) to another network entity W through wired links is denoted by T(V-W) under the assumption that T(V-W) = T(W-V) where V and W may be MAG, LMA, MAG-discovery Entity or AAA server. The time consumed by MN for choosing NMAG is denoted by T(MN). T(MAG) is the time required by PMAG to choose NMAG and allocate resources for MN. T(LMA) is the time spent by LMA to select NMAG. T(AAA server) is the time for S-Net's AAA server to authenticate MN. Table 7 summaries the times consumed by network entities to perform network activities. The measured time and description are also given.

Table 7. The summary of the times consumed by network entities for sending a message, choosing NMAG or allocating resources.

T( )	Value (ms)	Description
T(L2)	25 ms	The time consumed by layer 2 to trigger corresponding handover.
T(MN-MAG) (wireless)	8 ms	The time consumed by MN to deliver a message to MAG or vice versa.
T(V-W) (wired)	5 ms	The time consumed by network entity V to deliver a message to another network entity W or vice versa, where V and W may be MAG, LMA, MAG-discovery Entity or AAA server.
T(MN)	5 ms	The time consumed by MN for choosing NMAG.
T(MAG)	5 ms	The time consumed by PMAG for choosing NNAG or by NMAG for allocating resources.
T(LMA)	5 ms	The time consumed by LMA for choosing NMAG.
T(AAA server)	5 ms	The time consumed by S-Nets AAA server for authenticating MN.

Note that the time required to deliver a message through a wireless link is 8ms and via a wired link is 3 ms.

The time consumed by PMAG to choose NMAG in a trustable network environment is as follows.

(A) FMIPv6 [24]

$$T(FMIPv6) = T(L2) + 4T(MN\text{-}MAG) + 6T(MAG\text{-}LMA) + 4T(LMA\text{-}LMA) + T(MAG) + T(MN) \quad (5)$$

(B) PMIPv6 [25]

$$T(PMIPv6) = T(L2) + T(MN\text{-}MAG) + 6T(MAG\text{-}LMA) + 4T(LMA\text{-}LMA) + 2T(MAG) \quad (6)$$

(C) The TMSUS

$$T(TMSUS) = T(L2) + T(MN\text{-}MAG) + 3T(MAG\text{-}LMA) + 4T(LMA\text{-}LMA) + T(MAG) + T(LMA) \quad (7)$$

The time required by PMAG to predict the NMAG in an untrusted network environment by employing MAG-discovery Entity is as follows.

(D) FMIPv6

T(FMIPv6) = T(L2) + 4T(MN-MAG) + 6T(MAG-LMA) + 8T(MAG-discover Entity-LMA) + 2T(LMA-AAA Server) + 2T(AAA Server-AAA Server) + T(AAA Server) + T(MAG) + T(MN) (8)

(E) PMIPv6

T(PMIPv6) = T(L2) + T(MN-MAG) + 6T(MAG-LMA) + 8T(MAG-discovery Entity-LMA) + 2T(LMA-AAA server) + 2T(AAA server-AAA server) + T(AAA server) + 2T(MAG) (9)

(F) The TMSUS

T(TMSUS) = T(L2) + T(MN-MAG) + 3T(MAG-LMA) + 4T(MAG-discovery Entity-LMA) + 2T(LMA-AAA server) + T(AAA server) + T(LMA) + T(MAG) (10)

Table 8. The primitives delivered by network entities to other network entities in FMIPv6, PMIPv6 and TMSUS.

T( )	Primitives	FMIPv6	PMIPv6	TMSUS
T(MN-LMA)	MIH_HO_Indication		✓	✓
T(MN-LMA)	MIH_Get_Information.request	✓		
	MIH_Get_Information.responce	✓		
T(MAG-LMA)	MIH_MN_HO_Candidate_Query.request	✓	✓	
	MIH_MN_HO_Candidate_Query.responce	✓	✓	
T(MAG-LMA)	MIH_MN_HO_Commit.request	✓	✓	
	MIH_MN_HO_Commit.responce	✓	✓	
T(MAG-LMA)	MIH_Resource_Reservation.request	✓	✓	✓
	MIH_Resource_Reservation.responce	✓	✓	✓
T(LMA-MAG-discovery Entity)	MIH_HO_Indication.request			✓
	MIH_HO_Indication.responce			✓
T(LMA-AAA server), T(AAA server-AAA server)	Authentication.request	✓	✓	✓
	Authentication.responce	✓	✓	✓

T(MN-MAG) is the time required for deliver one of the following messages (primitives) from MN to MAG or vice versa, including MIH_HO_Indication (PMIPv6 and TMSUS), MIH_Get_Information.request (FMIPv6), MIH_Get_Information.responce (FMIPv6), MIH_MN_HO_Candidate_Query.request (FMIPv6 and PMIPv6), MIH_MN_HO_Candidate_Query.responce (FMIPv6 and PMIPv6), MIH_MN_HO_Commit.request (FMIPv6 and PMIPv6), MIH_MN_HO_Commit.response (FMIPv6 and PMIPv6), MIH_Resource_Reservation.request (FMIPv6, PMIPv6 and TMSUS) and

MIH_Resource_Reservation.responce (FMIPv6, PMIPv6 and TMSUS).

The time required by MAG and LMA to transport primitives and their processing time is denoted by T(MAG-LMA), including primitives that are MIH_MN_HO_Candidate_Query.request (FMIPv6 and PMIPv6), MIH_MN_HO_Candidate_Query.responce (FMIPv6 and PMIPv6), MIH_MN_HO_Commit.request (FMIPv6 and PMIPv6), MIH_MN_HO_Commit.response (FMIPv6 and PMIPv6), MIH_Resource_Reservation.request (FMIPv6, PMIPv6 and TMSUS) and MIH_Resource_Reservation.responce (FMIPv6, PMIPv6 and TMSUS). The time required for LMA and LMA to transport primitives is denoted by T(LMA-LMA), including MIH_HO.Indication.request (TMSUS), MIH_HO.Indication.responce (TMSUS), MIH_MN_HO_Commit.request (TMSUS) and MIH_MN_HO_Commit.response (TMSUS). The primitives in T(LMA-MAG-discovery Entity) are MIH_HO_Indication.request (TMSUS) and MIH_HO_Indication.responce (TMSUS). The primitives in T(LMA-AAA server) and T(AAA server- AAA server) are Authentication.request (FMIPv6, PMIPv6 and TMSUS) and Authentication.responce (FMIPv6, PMIPv6 and TMSUS). Table 8 summaries the primitives and the schemes that use them.

Figure 22 shows the results of the fourth experiment. Obviously, the time consumed by the TMSUS is shorter than that required by FMIPv6 (PMIPv6), no matter whether in the trustable or the untrusted environment. Note that the time spent by the TMSUS for predicting NMAG in an untrusted is even shorter than that of FMIPv6 in a trustable handover. The phenomenon can also be seen in Figure 21. Since in the FMIPv6, NMAG is chosen by MN. The information of MAGs needs to be transported to MN. After MN chooses NMAG, it also needs to inform LMA.

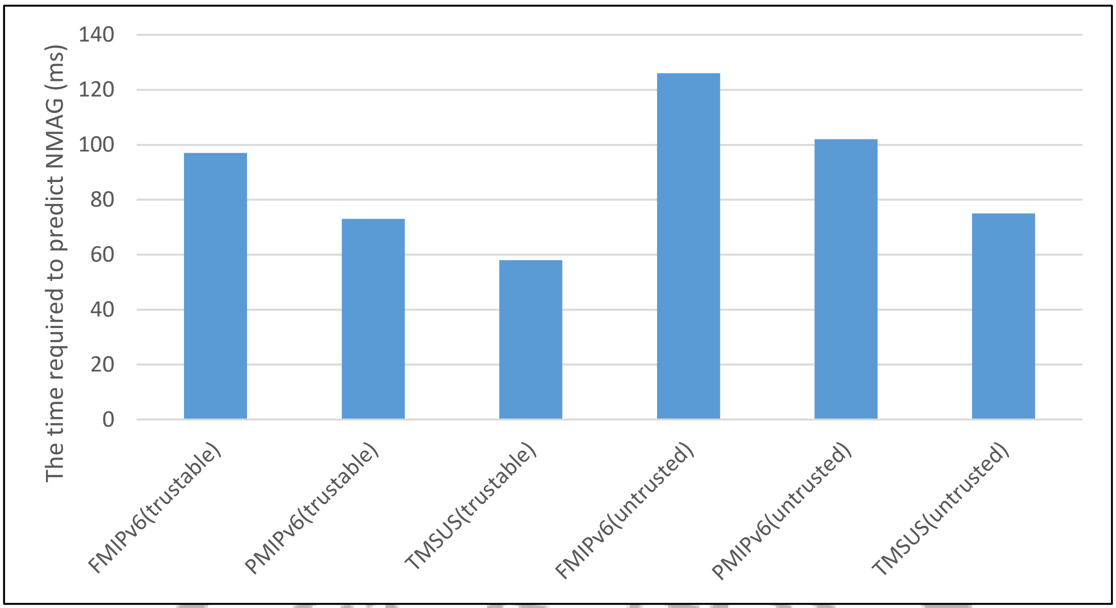

Figure 22. The times required by FMIPv6, PMIPv6 and TMSUS to predict NMAG in a trustable network environment and an untrusted network environment.

4.5 The Performance of TMSUS and Current Scheme

In the fifth experiment, MN will hand over from S-Net to T-Net and there are 10 MAGs in T-Net. The topology of this experiment is shown in Figure 23. Every MAG has multiple parameters and the values are setting randomly in every times. We do this experiment ten times. Each time the direction of MN is randomly chosen and the scores of the 10 MAGs are calculated. The parameters of all MAGs are shown in Appendix of this paper.

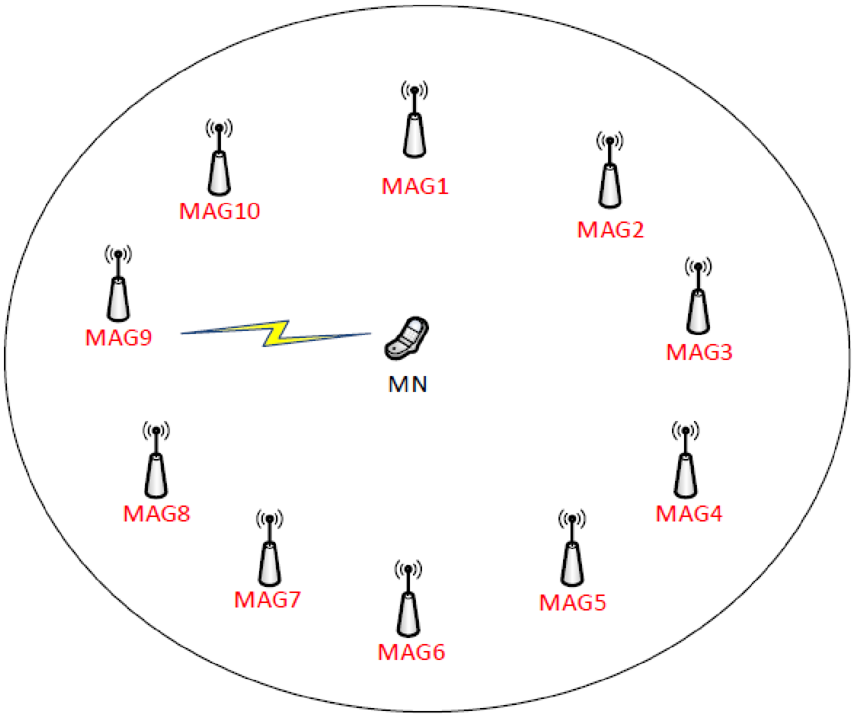

Figure 23. The topology of performance test.

Table 9 shows the average throughputs, average drop rates and average end-to-end delays of the TMSUS and current scheme (used by PMIPv6 and FMIPv6) in this experiment. The average throughputs of TMSUS is better than those of the current scheme which selects NMAG only based on RSS. But the TMSUS will calculate multiple parameters for all MAGs and then choose the one with the highest score as NMAG. TMSUS's average drop rates is lower than the current scheme's. End-to-end delays is one of parameters considered by the TMSUS. It is clear that the TMSUS outperforms current scheme. In other words, multi-parameters reflecting current statuses of candidate MAGs are helpful in choosing an appropriate NMAG.

Table 9. The performance of the TMSUS and current scheme.

	TMSUS	Current scheme (PMIPv6/FMIPv6)
Throughput (Mbps)	94.25219	87.36214
Drop rates (%)	5.74781	12.63786
End-to-end delay (ms)	0.16011	0.22818

V. Conclusion and Future work

In this study, we propose a scheme to mitigate the network handover problem for two adjacent untrusted networks by introducing the MAG-discovery Entity which constructed by a trustable third party is the mechanism helping two networks' LMAs to communicate with each other and mutually exchange network information. Due to the help of MAG-discovery Entity and the feature of SCTP, the link between MN and NMAG will be established before handover starts. The association between MN and network will not be disconnected during the handover. With the CRRM, a target base station can allocate resources required by MN before MN connects to it. CRRM can also help us to accomplish congestion control and network load balance. Considering homogeneity of two adjacent networks and the angle between MN and MAGs, we can choose an appropriate MAG as NMAG. We also proposed a target base station selection algorithm for LMA to decrease handover delays and signaling costs.

In the future, we consider another situation. Our proposed scheme only considers the case in which S-Net is MN's Home network. When stays in a foreign network and MN needs to hand over to another network, the problem is that T-Net's AAA server should communicate with S-Net's AAA server and MN's AAA server. The relationship among the three AAA servers may be heterogeneous/homogeneous and/or trustable/untrusted. In fact, the relationship among them is complicated. We hope we can propose a mechanism to solve this problem. Also, we would like to derive the behavior and reliability models so that users can predict its behaviors and reliability before using it. These constitute our future studies.

References

[1] K. Leung, "WiMAX Forum / 3GPP2 Proxy Mobile IPv4," IEFT RFC 5563, February 2010. [online]. Available: https://tools.ietf.org/html/rfc5563 [Accessed: 15-Jan-2017]

[2] D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11," IETF RFC 5416, March 2009. [online]. Available: https://tools.ietf.org/html/rfc5416 [Accessed:27-Nov-2016]

[3] F. Xia, "DHCPv6 Prefix Delegation in Long-Term Evolution (LTE) Networks," IETF RFC 6653, July 2012. [online]. Available: https://tools.ietf.org/html/rfc6653 [Accessed:10-Dec-2016]

[4] P. Begerow, S. Krug, A.A. Rubaye, K. Renhak and J. Seitz, "Delay Tolerant Handover for Heterogeneous Networks," *39th Annual IEEE Conference on Local Computer Networks*, pp. 370-373, September 2014.

[5] F.Y. Leu and 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 (IMIS 2017)*, pp. 502-510, July 2017.

[6] Y.H. Han, J.H. Choi and S.H. Hwang, "Reactive Handover Optimization in IPv6Based Mobile Networks," *IEEE Journal on Selected Areas in Communications*, September 2006, pp. 1758-1772.

[7] F.Y. Leu, C.Y. Liu, J.C. Liu and F.C. Jiang, "S-PMIPv6: an Intra-LMA model for IPv6 Mobility," *Journal of Network and Computer Applications,* Vol. 58, pp. 180-191, December 2015.

[8] 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]

[9] 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.

[10] G. Wang and L. Chen, “Performance Comparison between Utility Based and MIH Schemes in Vertical Handover,” *2014 9th IEEE Conference on Industrial Electronics and Applications*, pp. 203-207, June 2014.

[11] P.S. Kim, M.S. Jang and E.H. Lee, “An IEEE 802.21 MIH Functionality Assisted Proxy Mobile IPv6 for Reducing Handover Latency and Signaling Cost,” *2013 10th International Conference on Information Technology: New Generations*, pp.692-695, April 2013.

[12] D.M. Chiu and R. Jain, “Analysis of the Increase and Decrease Algorithms for Congestion Avoidance in Computer Networks,” *Computer Networks and ISDN Systems,* Vol. 17, No. 1, June 1989, pp. 1-14.

[13] L. Wu and K. Sandrasegaran, “A Survey on Common Radio Resource Management,” *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, August 2007.

[14] M. Houda, F. Zarai, M.S. Obaidat and L. Kamoun, “Optimizing Handover Decision and Target Selection in LTE-A Network-based on MIH Protocol,” *IEEE International Conference on Communications,* pp. 299-304, June 2014.

[15] S. Das, “DHCPv4 and DHCPv6 Options for Access Network Discovery and Selection Function (ANDSF) Discovery,” IETF RFC 6153, February 2011.

[16] A. Rasem, C. Makaya and M. St-Hilaire, “O-PMIPv6: Efficient Handover with Route Optimization in Proxy Mobile IPv6 Domain,” *2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp.47-54, October 2012.

[17] R. Stewart, "Stream Control Transport Protocol," IETF RFC 4960, September 2007. [online]. Available: https://tools.ietf.org/html/rfc4960 [Accessed: 15-Dec-2016]

[18] M. Happenhofer and P. Reichl, "Measurement-Based Analysis of Head-of-Line Blocking for SIP over TCP," *18th Annual IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, pp. 244-253, August 2010.

[19] S. Tarapiah, K. Aziz and S. Atalla, "Common Radio Resource Management Algorithms in Heterogeneous Wireless Networks with KPI Analysis," *International Journal of Advanced Computer Science and Applications*, Vol. 6, No. 10, pp. 53-58, November 2015.

[20] Q.B. Mussabbir, W. Yao, Z. Niu and X. Fu, "Optimized FMIPv6 Using IEEE 802.21 MIH Services in Vehicular Networks" *IEEE Transactions on Vehicular Technology*, Vol. 56, No. 6, November 2007, pp. 3397-3407.

[21] J. Ha, J.Y. Kim, J.U. Kim, and S.H. Kim, "Dynamic Load Balancing Architecture in Heterogeneous Wireless Network Environment," *The 9th International Symposium on Communications and Information Technology (ISCIT 2009),* pp. 248-253, September 2009.

[22] 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.

[23] 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.

[24] R. Koodli, "Mobile IPv6 Fast Handovers," IETF RFC 5568, July 2009. [online]. Available: https://tools.ietf.org/html/rfc5568 [Accessed: 09-Dec-2016]

[25] V. Devarapalli, "Proxy Mobile IPv6," IETF RFC 5213, August, 2008. [online].

Available: https://tools.ietf.org/html/rfc5213 [Accessed: 09-Dec-2016]

[26] “Global Positioning System.” [online]. Available: https://en.wikipedia.org/wiki/Global_Positioning_System. [Accessed: 10-Feb-2017]

[27] “Cartesian coordinate system.” [online]. Available: https://en.wikipedia.org/wiki/Cartesian_coordinate_system. [Accessed: 10-Feb-2017]

[28] “Polar coordinate system.” [online]. Available: https://en.wikipedia.org/wiki/Polar_coordinate_system. [Accessed: 10-Feb-2017]

[29] F.Y. Leu and K.C. Liang, “A Location-based Handoff Scheme Based on IEEE 802.21 in Heterogeneous Wireless Networks,” *2011 Fifth International Conference on Innovative Mobile and Internet Service in Ubiquitous Computing*, pp. 571-576, July 2011.

[30] “Seamless and Secure Mobility.” [Online]. Available: https://www.nist.gov/publications/seamless-and-secure-mobility [Accessed: 17-Mar-2017].

Appendix: The parameters of all MAGs in the fifth experiment

Data of first time.

	throughputs	drop rates	delays	RSS	Angle	score
MAG1	95.3542	4.6458	0.1328	-72	23	0.565968
MAG2	96.2154	3.7846	0.1174	-87	56	0.438427
MAG3	77.5342	22.4658	0.3384	-65	68	0.395932
MAG4	95.2485	4.7515	0.1264	-70	21	0.57471
MAG5	92.5254	7.4746	0.1684	-90	97	0.292331
MAG6	95.6641	4.3359	0.1246	-82	127	0.207148
MAG7	88.2145	11.7855	0.2354	-75	26	0.541359
MAG8	90.2785	9.7215	0.1836	-85	62	0.41126
MAG9	67.2485	32.7515	0.4271	-80	134	0.139567
MAG10	85.2483	14.7517	0.2684	-77	45	0.470693

Data of second time.

	throughputs	drop rates	delays	RSS	Angle	score
MAG1	95.3542	4.6458	0.1328	-80	55	0.449302
MAG2	72.5752	27.4248	0.3851	-77	36	0.479237
MAG3	84.2685	15.7315	0.2751	-95	114	0.216457
MAG4	95.2148	4.7852	0.1247	-61	17	0.59917
MAG5	92.2145	7.7855	0.1638	-71	51	0.468639
MAG6	64.2585	35.7415	0.4685	-82	67	0.3558
MAG7	88.2451	11.7549	0.2169	-90	138	0.14872
MAG8	74.2148	25.7852	0.3782	-90	106	0.232703
MAG9	82.5412	17.4588	0.2685	-86	27	0.514032
MAG10	86.2835	13.7165	0.2285	-79	46	0.4656

Data of third time.

	throughputs	drop rates	delays	RSS	Angle	score
MAG1	81.2575	18.7425	0.2538	-62	54	0.450975
MAG2	89.2453	10.7547	0.2135	-88	157	0.089774
MAG3	91.8547	8.1453	0.1912	-71	68	0.412166
MAG4	67.2149	32.7851	0.4381	-78	38	0.462366
MAG5	97.2586	2.7414	0.1285	-80	19	0.572967
MAG6	95.2487	4.7513	0.1367	-85	126	0.206304
MAG7	83.2147	16.7853	0.2538	-90	45	0.449889
MAG8	94.2871	5.7129	0.1421	-81	72	0.389561
MAG9	83.2164	16.7836	0.2598	-73	61	0.418009
MAG10	78.2485	21.7515	0.3295	-77	31	0.505397

Data of fourth time.

	throughputs	drop rates	delays	RSS	Angle	score
MAG1	86.2574	13.7426	0.2267	-78	73	0.376738
MAG2	97.6421	2.3579	0.1246	-61	34	0.547354
MAG3	90.6548	9.3452	0.1982	-90	66	0.392916
MAG4	85.2147	14.7853	0.2354	-72	92	0.319109
MAG5	77.3685	22.6315	0.3385	-58	58	0.437687
MAG6	68.2198	31.7802	0.4289	-81	27	0.496986
MAG7	88.2853	11.7147	0.2135	-86	156	0.093687
MAG8	79.2854	20.7146	0.3145	-94	53	0.412387
MAG9	95.2587	4.7413	0.1432	-80	167	0.076124
MAG10	81.2584	18.7416	0.2835	-92	42	0.454467

Data of fifth time.

	throughputs	drop rates	delays	RSS	Angle	score
MAG1	90.2581	9.7419	0.1985	-62	61	0.4438
MAG2	87.2561	12.7439	0.2251	-72	83	0.352849
MAG3	95.2145	4.7855	0.1564	-71	33	0.534392
MAG4	76.2185	23.7815	0.3495	-84	165	0.046587
MAG5	94.2588	5.7412	0.1682	-90	126	0.199124
MAG6	77.2581	22.7419	0.3354	-73	27	0.521946
MAG7	68.6215	31.3785	0.4219	-81	67	0.364223
MAG8	88.3268	11.6732	0.2168	-57	60	0.45013
MAG9	92.8514	7.1486	0.1826	-75	77	0.378873
MAG10	93.5814	6.4186	0.1735	-66	62	0.441279

Data of sixth time.

	throughputs	drop rates	delays	RSS	Angle	score
MAG1	92.2854	7.7146	0.1865	-65	27	0.557037
MAG2	88.2654	11.7346	0.2268	-82	73	0.375757
MAG3	67.2485	32.7515	0.4356	-77	134	0.1436
MAG4	79.2585	20.7415	0.3195	-68	72	0.381667
MAG5	95.2658	4.7342	0.1584	-92	69	0.388312
MAG6	92.8541	7.1459	0.1862	-84	33	0.514415
MAG7	86.2547	13.7453	0.2493	-58	64	0.432486
MAG8	82.9542	17.0458	0.2841	-90	118	0.207045
MAG9	92.8541	7.1459	0.1835	-72	48	0.479325
MAG10	91.6854	8.3146	0.1984	-66	55	0.461651

Data of seventh time.

	throughputs	drop rates	delays	RSS	Angle	score
MAG1	67.8521	32.1479	0.4368	-85	133	0.138181
MAG2	92.5841	7.4159	0.1825	-66	53	0.469585
MAG3	95.8451	4.1549	0.1568	-65	33	0.543167
MAG4	81.2584	18.7416	0.2985	-72	62	0.4133
MAG5	88.2448	11.7552	0.2257	-75	51	0.457763
MAG6	93.5421	6.4579	0.1723	-56	45	0.510328
MAG7	77.2458	22.7542	0.3358	-80	113	0.226518
MAG8	85.2145	14.7855	0.2514	-75	72	0.382559
MAG9	91.2568	8.7432	0.1984	-70	85	0.355794
MAG10	79.2581	20.7419	0.3185	-72	64	0.4033

Data of eighth time.

	throughputs	drop rates	delays	RSS	Angle	score
MAG1	77.5124	22.4876	0.3368	-72	116	0.227085
MAG2	83.5268	16.4732	0.2756	-68	65	0.412074
MAG3	92.5741	7.4259	0.1862	-62	24	0.571355
MAG4	79.2561	20.7439	0.3184	-81	147	0.115376
MAG5	95.2481	4.7519	0.1568	-67	36	0.529473
MAG6	93.5417	6.4583	0.1764	-66	33	0.537963
MAG7	90.2548	9.7452	0.2054	-59	68	0.42444
MAG8	84.2685	15.7315	0.2687	-75	61	0.41791
MAG9	79.2518	20.7482	0.3194	-79	53	0.431234
MAG10	83.5217	16.4783	0.2791	-68	48	0.468847

Data of ninth time.

	throughputs	drop rates	delays	RSS	Angle	score
MAG1	91.2584	8.7416	0.1984	-72	62	0.429963
MAG2	95.3642	4.6358	0.1563	-71	85	0.361355
MAG3	72.6598	27.3402	0.3842	-81	103	0.251043
MAG4	69.2487	30.7513	0.4168	-86	154	0.069057
MAG5	92.5846	7.4154	0.1862	-64	16	0.595543
MAG6	86.2147	13.7853	0.2485	-74	64	0.412379
MAG7	79.2158	20.7842	0.3164	-78	71	0.372312
MAG8	93.2168	6.7832	0.1758	-56	57	0.469794
MAG9	86.2147	13.7853	0.1495	-68	71	0.393246
MAG10	77.2158	22.7842	0.3385	-66	43	0.477382

Data of tenth time.

	throughputs	drop rates	delays	RSS	Angle	score
MAG1	82.1654	17.8346	0.2854	-72	65	0.404677
MAG2	95.2146	4.7854	0.1532	-75	51	0.469286
MAG3	93.2145	6.7855	0.1765	-71	48	0.481062
MAG4	81.6254	18.3746	0.2963	-76	92	0.308961
MAG5	88.6542	11.3458	0.2248	-62	15	0.594802
MAG6	73.5412	26.4588	0.3765	-82	132	0.154632
MAG7	95.6532	4.3468	0.1584	-66	58	0.458253
MAG8	82.6532	17.3468	0.2846	-72	67	0.39896
MAG9	66.8421	33.1579	0.4462	-90	157	0.050224
MAG10	90.6512	9.3488	0.2068	-57	34	0.541112