Global Information Assurance Certification Paper

Secure rekeying with different MS's Velocities for MBS during Handover in IEEE 802.16e

GIAC (GSEC) Gold Certification

Author: Ibrahim A.Gomaa, Eng_Ibrahim@nti.sci.eg
Advisor: Rick Wanner

Accepted: October 19, 2010

Abstract

The IEEE 802.16e-2005 forms the basis for the WiMAX solution for nomadic and mobile applications and is often referred to as mobile WiMAX. It supports optimized handover schemes with latencies less than 50 milliseconds to ensure real-time applications. More importantly, when mobile stations (MSs) frequently handover from one multicast broadcast services (MBS) group to others, this will trigger exhaustive rekeying procedures at each MBS group. Therefore, vehicles travelled at high speeds causing many unnecessary multicast group rekeying procedures. The presented paper will investigate the effect of using different MBS group cluster sizes, different MS's velocities in different environments. The rest of paper will analyze the relation between rekeying and MS's Velocities to ensure that Enhanced Delayed Feedback Rekeying algorithm (EDFRA) obviate most of rekeys due to member handover, while still maintains backward and forward secrecy for the MBS group.

1. Introduction

The Worldwide Interoperability for Microwave Access technology, under its trade name of WiMAX (Ergen, 2009), has been elected as one of the most promising wireless communications system in the industry for the past ten years. It is a technology that aims to provide wireless long-distance broadband access for a variety of applications.

The NWG (Network Working Group) has conceptualized a WiMAX network (Figure 1) and its application environment as being comprised of three distinct entities.

- **A network access provider (NAP)** is an entity that operates one or more access service networks (ASNs). Typically, a NAP is a WiMAX operator which operates access networks in one or more areas.
- **A network service provider (NSP)** is an entity which provides connectivity and services to network access providers. In effect, NAPs need only to connect to NSPs (one or more) and expect all services and applications to be delivered through these connections. The NSPs provide connectivity to NAPs via connectivity service nodes (CSN). NSPs would be responsible for providing mobility between their own nodes as well as nodes of other NSPs.
- **Applications service providers (ASPs)** which provide services such as HTTP, video streaming, file download, e-mail, etc. These services fall above the network layer in the protocol model. Figure 1 exhibits one more "functional entity" of the WiMAX network architecture, i.e., the connectivity service network (CSN). As shown in the diagram, a CSN has AAA servers, policy functions (PF) for QoS, and provides connectivity to external networks such as a managed IP network or the public internet. It also provides the security and authentication framework through the AAA servers and the policy functions for each device, user, and service on the network. Being able to authenticate at multiple levels is a key feature of the WiMAX network architecture.

This separation between NAP, NSP, and ASP is designed to enable a richer ecosystem for WiMAX service business, leading to more competition and hence better services (Kumar, 2008). Figure 1 illustrates the Network architecture of Mobile WiMAX.

Ibrahim A.Gomaa, Eng_Ibrahim@nti.sci.eg

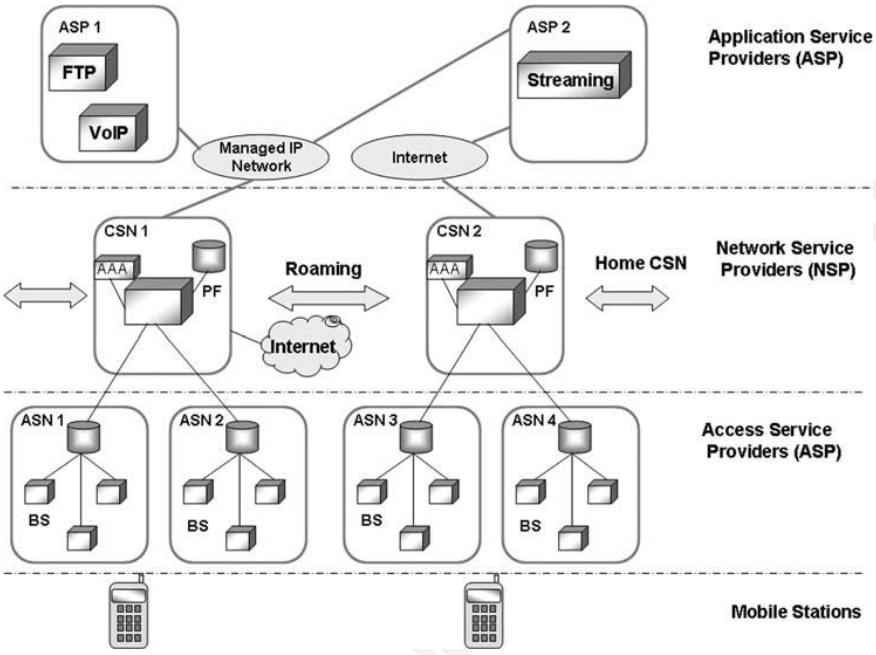

Figure 1: Network architecture of Mobile WiMAX (Kumar, 2008)

The recently released IEEE 802.16e adds mobility features and some other functions including multicast (IEEE, 2005). Multicast in WiMAX is a promising service, suitable for many applications, such as stock option bidding, pay per view TV broadcasting, video conferencing, etc., for both fixed and mobile subscribers.

The previous mentioned applications usually require access control and privacy to secure communication within MBS groups. To secure group communication we have to ensure that the messages exchanged within a group without interception by an intruder which known as group privacy. Therefore, all MBS messages should be encrypted by a secret key shared by only authorized group members. In addition, leaving members cannot access the future communication sessions to maintain forward secrecy among MBS groups. So, if an attacker compromises the current group keys, he cannot compromise any future group keys. Consequently, the group key used in current session should be updated when a member leaves the group. Lastly, joining members cannot know the group key used in previous communication sessions to achieve backward secrecy. Therefore, if an attacker compromises the current group keys, he cannot obtain preceding group keys. Similarly, the group key used in current session should be updated when a new member joins the group. For convenience, the updating operations for forward and backward secrecy called rekeying (Sun, 2007).

Many protocols dealing with secure multicast have been proposed (Harney, 1997). Logical Key Hierarchy (LKH) tree algorithms which was proposed in (Waldvogel, 1999), requires O (log n) messages where n is the number of members in certain group to update keys which needed to trigger rekeying procedure. One-way Function Tree is proposed in (Canetti, 1999), this method reduces most of the rekeying messages when compared to logical key hierarchy (it may be reached to half rekeying messages). (Sun, 2007), propose adaptive rekeying scheme, which can introduce different levels of complementary keys according to application needs.

Handover will occur often for high-speed vehicles (Lee, 2010), causing many unnecessary group rekeying procedures. The rekeying procedures are not necessary because the MS is still in the MBS group and should be allowed to access the multicast session (Xu, 2007), (Xu, 2008).

Enhanced Delayed Feedback Rekeying Algorithm (EDFRA) was implemented and designed to reduce the number of triggered rekeying procedures in the same multicast group (Gomaa, Badawy, & Saad, 2010). Therefore, EDFRA can efficiently reduce the number of forward and backward updates by recording certain data about MS and Base Station (BS) behaviors. The simulated results were published before in (Gomaa, Badawy, & Saad, 2010) proving that the EDFRA gets better performance when handover rates increase while still keeping forward and backward secrecy. In this work the following results are enhanced and a lot of parameters and environments added to ensure the basic idea and confirmed the results obtained before. In addition, the relation between maximum rekeying procedures and different MS's velocities are studied and resulted a lot of curve in each velocity which ensure the results obtained in this paper and previous one.

The simulation was done via MATLAB coding for each phase and in each case. This obtains enhanced outcomes as a number of rekeying procedures versus number of handovers were performed. This was done with different MS distributions; different BS's cluster size and different environments are added in this paper. Lastly, the maximum numbers of rekeying procedures versus MS's velocities are shown to ensure that EDFRA obviates most of rekeying procedures due to MS handover.

The rest of the paper is organized as the follows: in Section 2, the problem statement will be presented and reviewed. Section 3 presents EDFRA. Section 4 simulations & analysis. Section

5 introduces rekeying versus MS's different velocities. Finally, Section 6 will provide the conclusion and future research in this direction.

2. Problem Statement

Multicasting services in most cases require the mobile station to be authenticated for receiving the multicast services and maintain the authentication while using the service as well as while handover from one cell area to another. When the handover member exits from the serving group and enters the target group, both Serving group and target group need to update their Subgroup Traffic Encryption Key (SGTEK) due to the intra-Base Station subgroup member changes.

The range of BS is up to 6 km, and the mobile speed support is up to 120km/h. That means, even if the vehicle travels from exactly one end of the SBS cell to the other end via the diameter, it could take as little as 3 minutes or so. Considering the cases of multiple groups, the rekeying procedure will be triggered frequently. When a handover member moves from a group to another group, most schemes require two rekeying procedures. One is for forward secrecy at serving group and the other is for backward secrecy at targeting group. We can infer that the overhead of rekeying will be extremely large when there are multiple large dynamic groups in vehicular environment. (Xu, 2007),(Xu, 2008), (Gomaa, Badawy, & Saad, 2010).

3. EDFRA

DFRA (Delayed Feedback rekeying Algorithm) was proposed in (Xu, 2007), (Xu, 2008). (Gomaa, Badawy, & Saad, 2010) was suggested some enhancements to the regular DFRA. Different from (Xu, 2007), (Xu, 2008), (Gomaa, Badawy, & Saad, 2010) constructed and implemented an EDFRA that aimed to minimize the number of required rekeying procedures, while achieving the same or more security for the multicast services. The regular DFRA starts from the handover operation without taking into account the logging-in operation which has direct effect on the number of triggered rekeying procedures in overall operation. EDFRA proposes that there are three phases when dealing with multicast services, which are logging in the Multicast session, logging off the Multicast session and handover among different multicast sessions at different BSs. Moreover, the regular DFRA considers backward update at TBS during HO operation, causing not much trouble despite that it will increase the number of triggered

rekeying procedures. However EDFRA proposed that the MBS server (group manager) will make a record for each joining MS and pass it to later TBSs.

The design and construction of the EDFRA was illustrated in (Gomaa, Badawy, & Saad, 2010). The implementation process is divided into three phases according to MS's behaviors and was introduced in the form of flow chart which appears in figure 2.

The three phases are:

- **Phase1:** logging into multicast session, which enforce BS to trigger rekeying procedure to ensure backward secrecy. Then, BS made a new record in current handover subgroup member list (CHSML) for MS's SGTEK. Afterwards, MS decided that MBS session ended at this point or it should handover to another BS.
- **Phase2:** MS handover from current BS to another one. Therefore, serving BS (SBS) update its past handover subgroup member list (PHSML) by make a new record for leaved MS. Consequently, target BS (TBS) sent current SGTEK to the new MS by unicast through its primary management connection encrypted by key encryption key (KEK). Moreover, TBS update its CHSML to record the SBS from which MS left.

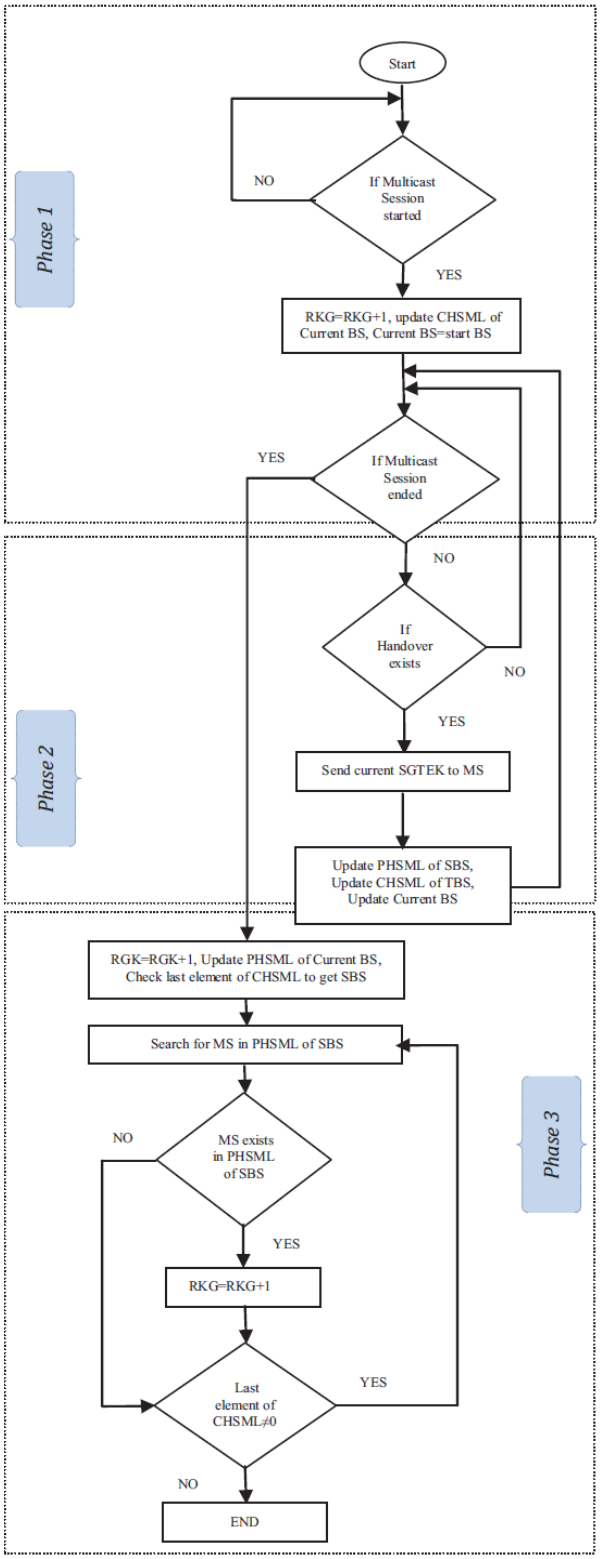

Figure 2: Flowchart of EDFRA (Gomaa, Badawy, & Saad, 2010)

- **Phase3:** logging off MBS session, which enforce BS to trigger rekeying procedure to ensure forward secrecy. The current BS made a record for leaved MS by updating its PHSML. According to the record in BS's CHSML, the BS notify leaved MS's previous SBS to make sure that leaved MS couldn't access the MBS session from that SBS. Lastly, the rekeying procedure triggered according to SBS's PHSML if contained leaved MS or not.

4. Simulations & Analysis

EDFRA and its phases were simulated in (Gomaa, Badawy, & Saad, 2010). The simulation is done using MATLAB coding for each phase obtaining the outcomes as a number of rekeying procedures versus how many HO processes are made. This will be done with different MS distributions and different BS's cluster size. Then, different environments added in this paper.

The results are outlined later and divided into two sub sections according to the measurement scenarios. The first sub section shows the number of rekeying procedures versus the number of handover processes. It was made in a pedestrian environment with low velocity. The measurements are recorded in order to compare the results with a vehicular environment. The next sub section shows the results of medium and high velocities within a vehicular environment.

The following Smart Art representing the enhanced results (Figure 3):

The outcomes of first stage are appearing as a number of rekeying procedures versus number of handover made. The results obtained in (Gomaa, Badawy, & Saad, 2010) for BS cluster size 15Km and 150Km/hr MS's velocity. In this work we are used different BS cluster sizes for different MS's velocities in different environments. The presented work uses pedestrian and vehicular environments for single and dual MS scenarios. In each environment the paper uses four different BS cluster sizes 1 Km, 3 Km, 5 Km and 15 Km. for each BS cluster size the paper uses four different distributions uniform, Gaussian, binomial and Poisson to simulate random MS movements among group of BSs.

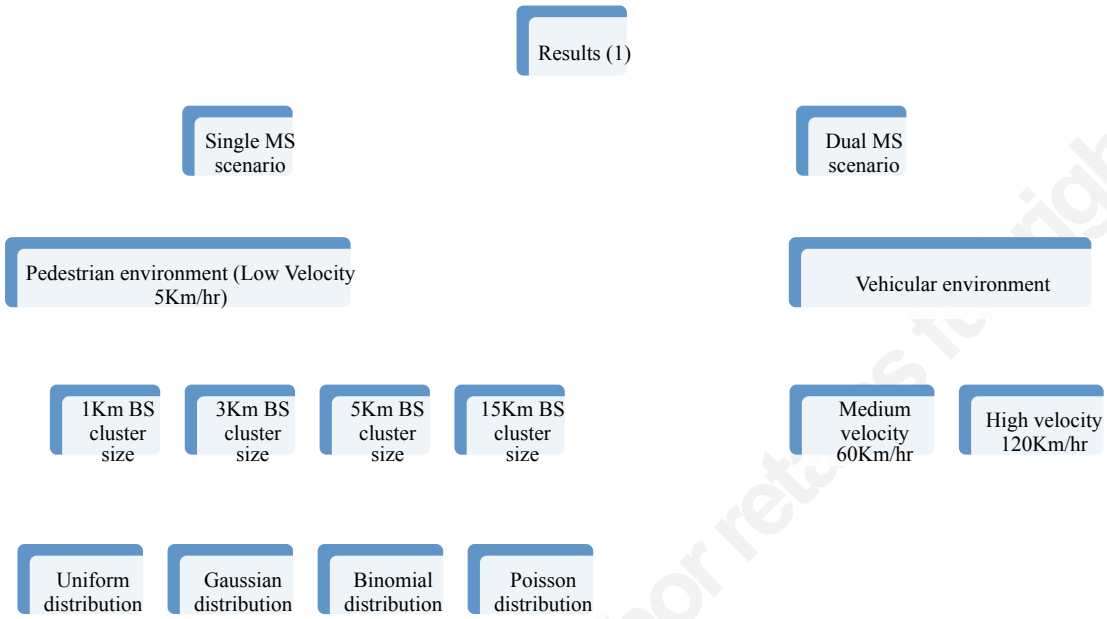

Figure 3: The outcomes of first stage

The paper will show only a sample of the results because it is impossible to show all results in the two scenarios in the same paper.

4.1.Single MS scenario

The simulation parameters are taken as constants as with (Xu, 2007), (Xu, 2008), with some practical details (Gomaa, Badawy, & Saad, 2010).The simulation model has different stimulus values at each run according to random distribution used. so in order to predict most sustainable system performance, the average of 1000 run operations are calculated to obtain the final results in each case. Therefore, our simulation model not only uses the aforementioned settings in with (Xu, 2007), (Xu, 2008) but also cooperates with the Gaussian distribution, Binomial distribution, Poisson distribution and random techniques (Gomaa, Badawy, & Saad, 2010).

Accordingly, the number of normal rekeying procedures will be calculated based on the number of HO's made. Then we compare it with the number of rekeying procedures after deploying EDFRA. Finally, the relationship between the number of handover's and rekeying are resulted in each case.

4.1.1. Pedestrian

Table 1 outlines the pedestrian measurement parameters, as we mentioned before our simulation model not only uses the following measurement parameters but also cooperates with the Gaussian distribution, Binomial distribution, Poisson distribution and random techniques to simulate MS random movements.

Table 1: Pedestrian measurement parameters

Parameter	Value
Number of BSs	9
Number of Multicast groups	1
Number of SGTEK	9
Number of CHSML	9
Number of PHSML	9
BS cluster sizes	1 Km, 3 Km, 5 Km, 15 Km
Number of MS	1
MS speed	5 Km/hr
Resolution time (Observation time)	10 Sec.
Initial position	Xn=0, Yn=0

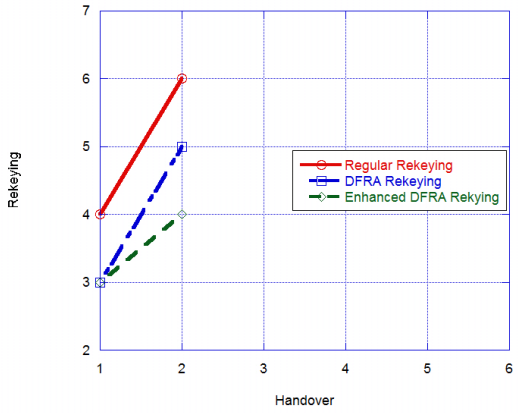

Figure 4: Random movements according to binomial distribution

MS movements according to binomial distribution were made two values for handover where BS cluster size is 1Km. No handover was occurred when the MS was moved according to the same distribution when BS cluster sizes are changed to 3, 5 and 15Km. It is near to actual scenarios.

4.1.2. Vehicular

Vehicular environments are the main target of the measurements since the thesis scope is to study Handover which will occur repeatedly for vehicles travelling at higher speeds causing many unnecessary multicast group rekeying procedures. Therefore, the paper introduced EDFRA to obviate most of the rekeys due to member HO, while still maintains backward and forward secrecy for this MBS group.

Table 2: Vehicular measurement parameters

Parameter	Value
Number of BSs	9
Number of Multicast groups	1
Number of SGTEK	9
Number of CHSML	9
Number of PHSML	9
BS cluster sizes	1 Km, 3 Km, 5 Km, 15 Km
Number of MSs	1
MS speed	60 Km/hr, 120 Km/hr
Resolution time (observation time)	10 Sec.
Initial position	Xn=0, Yn=0

Table 2 outlines the vehicular measurement parameters, as we mentioned before our simulation model not only uses the following measurement parameters but also cooperates with the Gaussian distribution, Binomial distribution, Poisson distribution and random techniques to simulate MS random movement. In addition we used different cluster sizes for the nine BS we used in our vehicular environment. First cluster size we used is 1 km then 3 km, 5 km and lastly we used 15 km to test real and theoretical BS cluster sizes.

For vehicular traffic we used two speeds for the MS, the first one is 60 Km/hr and the second one is 120 km/hr. for each speed the cluster size of the BS is changed from 1km to 15km.

In our simulation the MS makes 100 movements, we draw the last one. Moreover, the simulation model has different stimulus values at each run, so in order to predict most sustainable system performance, the 1000 run operations are averaged to obtain the final results. Finally, we repeat the overall operation 100 times to take 100 values for our results. The four distributions introduced in the two cases for MS speed's 60 km/hr and 120 km/hr.

1. Vehicular speed 60 Km/hr

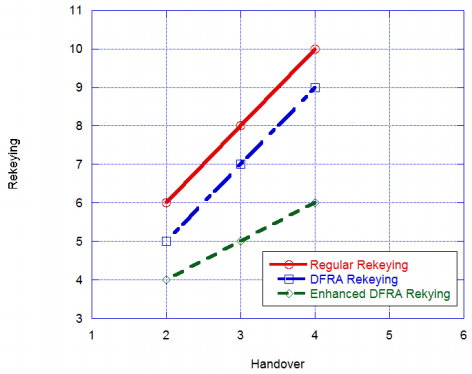

Figure 5: Binomial distribution for 3Km and 5Km BS cluster size

MS movements according to binomial distribution are the same at BS cluster sizes 3Km and 5Km and number of handover was made decreased at 15Km BS cluster size and increased at 1Km BS cluster size. Which it is make sense, so the MS movements according to binomial distributions were introduced results which are more similar to practical speech. Table 3 introduces the number of handover versus regular rekeying, DFRA rekeying and EDFRA rekeying.

Table 3: Binomial distribution for 1Km BS cluster size

Number of handover	Regular Rekeying	DFRA Rekeying	EDFRA Rekeying
30	62	61	32
25	52	51	27
28	58	57	30
31	64	63	33
⋮	⋮	⋮	⋮
28	58	57	30
31	64	63	33
30	62	61	32
32	66	65	34
32	66	65	34
30	62	61	32

2. Vehicular speed 120 Km/hr

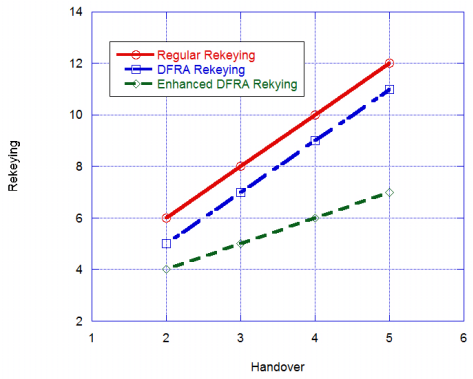

Figure 6: Binomial distribution for 3 km, 5 km BS cluster size

The MS movements according to binomial distribution are the same for the BS cluster sizes which are 3 km, 5 km. Moreover, the number of handover is large for the 1 km BS cluster size and small when the BS cluster size changed to 15 km. The MS movements according to Binomial distribution always return results closer to the real scenarios so it considered the best distributions to simulate MS movements. EDFRA triggered rekeying procedures less than the others introducing better performance.

In the case of MS movements according to Gaussian distribution the first BS triggered out of proposed boundary so the program return that can't find the first BS. And to solve this issue we have to decrease resolution time to be the half used before, so it should be 5 sec. instead of 10 sec. to get results and MS movements are observed each 5sec instead of each 10sec.

5. Rekeying versus MS's velocities

As we mentioned before, we have to study and analyze the relation between trigger rekeying procedures versus the three MS's velocities we are used. To ensure that EDFRA can efficiently reduce the number of forward and backward updates by recording and reviewing some data about MS and BS behaviors.

This section introduces the second stage of our enhanced results. The outcomes of second stage are showing as a number of rekeying procedures versus MS velocities. Figure 7 represents Smart

Art of second stages of outcomes. In this case, the paper uses the four different distributions uniform, Gaussian, binomial and Poisson for the single and dual MS scenarios.

In each distribution the paper uses four different BS cluster sizes 1 Km, 3 Km, 5 Km and 15 Km. The outcomes from stage two are maximum triggered procedures versus MS's velocities 5 km, 60 km and 120 km.

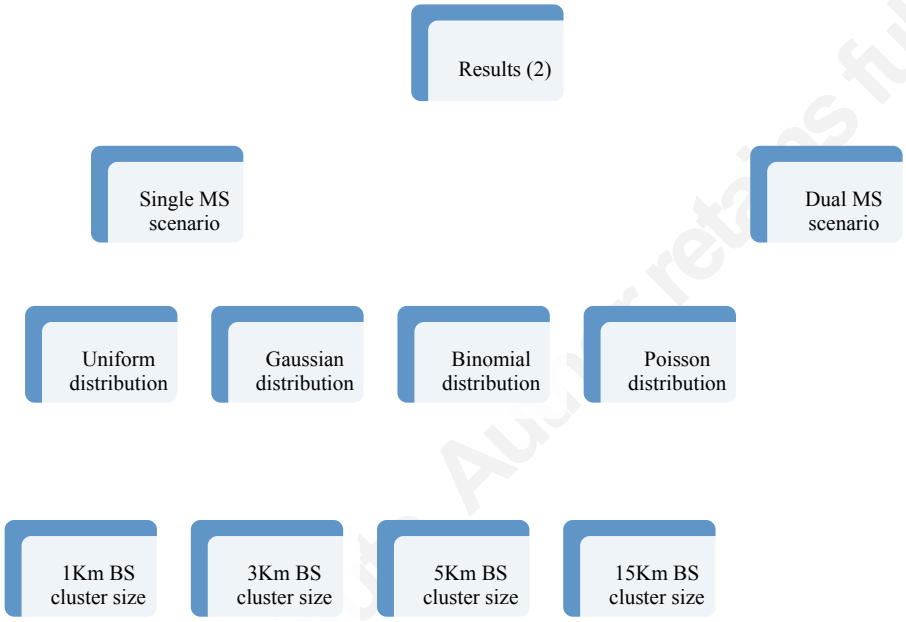

Figure 7: The outcomes of first stage

The following tables and figures show the final results for maximum number of handover and maximum number of triggered rekeying procedures in the three cases regular, DFRA and EDFRA. The cross between the DFRA and EDFRA caused because the DFRA didn't trigger the rekeying procedures when the MS entered the MBS session which was considered one of the improvements introduced by EDFRA. As we explained before, the EDFRA take into account the three cases of the mobile movements logging in, logging off and handover.

The paper will show only a sample of the results because it is impossible to show all results in the two scenarios in the same paper.

1. Single MS movements according to Uniform distribution

Table 4 will show the obtained final results for maximum numbers of handover and triggering rekeying procedures according to MS's velocities 5 km, 60 km and 120 km.

Table 4: Obtained results according to uniform distribution

BS cluster size	velocity	Max. No. of Handover	Max No. of triggered rekeying procedures		
			Regular	DFRA	Enhanced DFRA
1Km	5Km/hr	0	2	1	2
	60Km/hr	24	50	49	26
	120Km/hr	43	88	87	45
3Km	5Km/hr	0	2	1	2
	60Km/hr	4	10	9	6
	120Km/hr	4	10	9	6
5Km	5Km/hr	0	2	1	2
	60Km/hr	2	6	5	4
	120Km/hr	4	10	9	6
15Km	5Km/hr	0	2	1	2
	60Km/hr	0	2	1	2
	120Km/hr	2	6	5	4

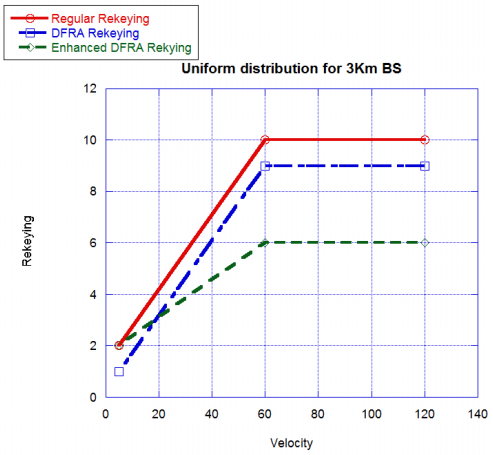

Figure 8: Uniform distribution for 3Km BS cluster size

2. Single MS movements according to Binomial distribution

Table 5 shows the final results for the maximum number of handovers and maximum number of triggered rekeying procedures in the three cases regular, DFRA and enhanced DFRA.

MS movements according to Binomial distribution are considered one of the best MS movements near to practical issues. So, the binomial distribution is considered one of the best distributions used to simulate MS movements among groups of BSs.

The number of triggered rekeying procedures in the case of DFRA is less than enhanced DFRA because the DFRA didn't take into account the logging-in operation in the MBS session.

Table 5: Obtained results according to Binomial distribution

BS cluster size	velocity	Max. No. of Handover	Max No. of triggering rekeying procedure		
			Regular	DFRA	Enhanced DFRA
1Km	5Km/hr	2	6	5	4
	60Km/hr	37	76	75	39
	120Km/hr	50	102	101	52
3Km	5Km/hr	0	2	1	2
	60Km/hr	4	10	9	6
	120Km/hr	6	14	13	8
5Km	5Km/hr	0	2	1	2
	60Km/hr	4	10	9	6
	120Km/hr	6	14	13	8
15Km	5Km/hr	0	2	1	2
	60Km/hr	2	6	5	4
	120Km/hr	4	10	9	6

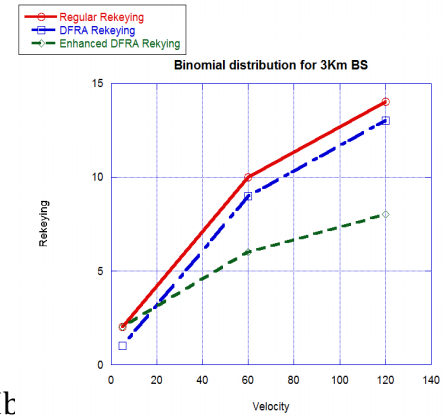

Figure 9: Binomial distribution for 3 Km BS cluster size

6. Conclusion and future research

From the obtained results, It has been verified that EDFRA decreases the number of triggered rekeying procedures; hence, minimizing the overhead on the network. The implemented algorithm is enhanced network performance, while still keeping backward and forward secrecy for the MBS session.

In this paper, EDFRA was implemented and designed to reduce the number of triggered rekeying procedures in the same MBS group. Therefore, EDFRA can efficiently reduce the number of forward and backward updates by recording some data about MS and BS behaviors. The simulated results show that the EDFRA gets better performance while handover rate gets higher. So, the current paper not only studies the DFRA but also, it proposes an adoption of the DFRA and assisted this adoption in different customer distributions. The presented work investigated the effect of using different MBS group cluster sizes, different velocities and different environments. In addition, the current paper study and analyze the relation between trigger rekeying procedures versus the three MS's velocities we are used. So, by introducing more MSs, there is an enhancement of the reduction of rekeying procedures. Finally, the paper compared the obtained performance in all scenarios in each case.

The current work may be extended via:

- LTE deployment scenario.
- Soft handover analysis for the same scenario.
- Different services classes of each MS.
- Multi MS operational scenario.

References

Canetti, R. (1999). Multicast security: a taxonomy and some efficient constructions. *Proceedings of the IEEE INFOCOM* vol. 2.

Ergen, M. (2009). *Mobile broadband including WiMAX and LTE*. ISBN: 978-0-387-68189-4. DOI: 10.1007/978-0-387-68192-4. Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA

Harney, H. (Ed.). (1997). *Group key management protocol (GKMP) architecture*. RFC 2093: Tech. Rep.

Gomaa, I., Saad, E., and Badway, H. (2010). *Adoption of Delayed Feedback Rekeying Algorithm for Secure Multicast Services during Handover in Mobile WiMAX Networks. Proceedings of the IEEE ICITIS2010. Beijing, China.474-480*

IEEE Press, Initials. (2005). IEEE std. 802.16e-2005, IEEE standard for local and metropolitan area networks, part 16, air interface for fixed and mobile broadband wireless access systems. Piscataway.

Kumar, A. (2008). *Mobile broadcasting with WiMAX: principles, technology, and applications*. ISBN: 978-0-240-81040-9: Focal Press is an imprint of Elsevier 30 Corporate Drive, Suite 400, Burlington, MA 01803, USA. Linacre House, Jordan Hill, Oxford OX2 8DP, UK

Lee, L. (2010). Design and analysis of a network-assisted fast handover scheme for IEEE 802.16e networks. *Proceedings of the IEEE transactions on vehicular technology* VOL.59 No.2.

Sun, H. Department of Computer Science, National Tsing Hua University. (2007). *An efficient rekeying framework for multiple multicast and groups in mobile WiMAX*. Taipei, Taiwan, R.O.C.: ., WiMAX Center of Networks & Multimedia Institute, Institute for Information Industry.

Sun, Y. (2007). Hierarchical group access control for secure multicast communications. *IEEE/ACM Transactions on Networking*, *15*, 1514-1526.

Waldvogel, M. (1999). The versa-key framework: versatile group key management. *IEEE Journal on Selected Areas in Communications*, *17*(9).

Xu, S. (2008). Secure multicast in WiMAX. *JOURNAL OF NETWORKS*, *3*, 48-57.

Xu, S. (2007). Secure multicast in various scenarios of WirelessMAN. *Proceedings of the 2007 IEEE southeast conference.*

Ibrahim A.Gomaa, Eng_Ibrahim@nti.sci.eg