FAST AND SECURE HANDOVER AUTHENTCATION SCHEME IN MOBILE WiMAX

[1] H. F. ZMEZM, [2] S.J. HASHIM*, [3] ADUWATI SALI
*Department Of Computer And Communication Systems Engineering, Faculty Of Engineering, University Putra Malaysia, 43400 Serdang, Selangor, Malaysia.
E-mail: [1] zmezm14@gmail.com, [2] shaiful@eng.upm.edu.my , [3] aduwati@eng.upm.edu.my

ABSTRACT

Handover is one of the essential elements that can affect the Quality of Service (QoS) and capacity of Mobile Broadband Networks. The next generation of broadband wireless networks including the IEEE802.16e standard, allow users to roam seamlessly and securely over the network. Unfortunately the current design suffers from lengthy delay between breaking of previous connection and making of next connection. This delay might not be tolerated by some of the real-time applications such as VoIP and video streaming. Therefore the need for fast and secure handover design becomes an urging necessity. This paper proposes a new handover mechanism enables fast and secure handover with minimum delay suitable for real-time applications. It should be pointed that this proposed handover protocol guarantees a forward and backward secrecy. We conducted our research using ns-2 simulation tool.

Keywords: *EAP-Authentication, Hard Handover, Mobile WiMAX, NS-2*

1. INTRODUCTION

Mobile WiMAX (Worldwide Interoperability Microwave Access) is a wireless networking system based on the IEEE 802.16e, standard, the standard has a number of capable features that can provide high bandwidth, extended coverage area and low cost. This has led to its fast rise as one of the most popular last mile broadband access technologies and as a likely component in the 4G networks [2].

IEEE 802.16e has satisfied all the needs for greater data rates and efficient spectral efficiencies in supplying a qualified mobile broadband access. Mobile WiMAX Base Station (BS) has the ability to support both fixed and mobile broadband wireless access. The latest version of Mobile WiMAX IEEE 802.16m can support mobility that can reach up to (350 km/h), which makes it a suitable candidate for high speed mobility environment such as high-speed express trains [16].

However, providing secure and fast connection for this kind of environment has proven to be a challenge. Handover latency considered being one of the major issues that is facing Mobile WiMAX network. Users receiving mobile services demand a very fast handover process, so they will not suffer any connection interruption leading to degrading in the quality of the service.

Address re-assignment and user authorization considered to be the main cause of the high handover delay in any mobile broadband access networks, including Mobile WiMAX. Extensible Authentication Protocol (EAP) used in Mobile WiMAX as an authentication procedure, because of its unique capability to cooperate with Authentication, Authorizing, Accounting (AAA) infrastructures. But unfortunately EAP could not support high speed mobility environment or have the ability to extend the authorization session before the initially authorized session ended. As a full EAP authentication latency requires about 1000*ms* every full authentication per handover [4, 8], where the encryption and decryption of the key material cause the highest delay in the EAP authentication [5].

Therefore its clearly cannot support real time application such as voice over IP and video streaming, which according to the International Telecommunication Union (ITU), should be less than 150 ms. In this paper we propose a method that target the main cause of the high handover delay and try to solve it .

2. BACKGROUND AND RELATED WORKS

2.1 Handover in mobile wimax

Mobile wimax has three types of handover procedures in mobile WiMAX which are Micro Diversity Handover (MDHO), Fast Base Station Switch Handover (FBBS) and the hard handover (HHO). The first two types are optional handover which enables the MS to send and receive data from numerous access points simultaneously. The hard handover however is mandatory. Hence we are going to consider it as a default handover in our paper of research [1, 16].

2.2 Basic hard handover procedure

HHO occur when the MS terminate its connection with the serving base station SBS and link itself to the target base station TBS, this process called break-before-make. In case handover happened and the new connection is not secure, authorization is required for a successful connection. There are two essential authorization levels in MAC layer of mobile WiMAX which are the Privacy Key Management protocol for key generation and the 3-way handshakes [2, 6].

In table 1 and 2 shown all the steps at the initial entry and the normal HHO operation and the delay associated with each step, all the statistic in table 1 and 2 was based on real measurement [16].

Table 1: Delays At The Initial Entry Steps[16].

Steps (ms)	IEEE 802.16e
Downlink Scanning Synchronization Obtain parameters	880.83 ms
Initial Ranging	148.33 ms
SBC_REQ	65 ms
SBC_RSP	43.33 ms
PKM (EAP - Authentication)	1238.33 ms
REG_REQ	25 ms
REG_RSP	50 ms
Obtain IP Address	178.39 ms
Total	2629.32 ms

2.3 Privacy key management protocol (PKM)

IEEE 802.16e security sub-layer includes two component protocols: an encapsulation protocol for securing data packet and a privacy key management (PKM) protocol providing the secure distribution of keying material from the BS and the MS.

There are two privacy key management protocols supported in IEEE 802.16e: PKMv1 and PKMv2. PKMv1 is a subset of PKMv2 in function. PKMv2 offers more enhanced features such as new key hierarchy, AES-CCM, AES key wrap algorithm, and multicast and broadcast service (MBS). Thus, the security of the IEEE 802.16e is introduced in term of the PKMv2 in this paper.

There are two main authentication schemes defined in PKMv2 of IEEE 802.16e, one based on RSA and the other based on EAP. Thus, there are two primary sources of keying material defined in PKMv2. To choose both or one of them as the authorization mechanism is decided by basic capabilities negotiation procedure at the initial network entry. In this paper, we focus on the EAP-based authentication, especially single EAP mode for simplicity [6].

Table 2: HHO Process Steps And The Delay For Each Step.

HHO Process steps	Delay for each step
Cell reselection	Probing delay = 67.41 ms
HO decision & Initiation	
Synchronize with new downlink and obtain parameters	
Obtain up link parameters	
Ranging and uplink parameter adjustment	
MS re-authorization (PKMV2 EAP-Based authentication)	Authentication delay = 1238.33 ms
MS Re-entry/registration (Obtain IP Address)	Re-association delay = 178.39 ms
Termination with the serving BS	
	Total HHO delay = 1484.13 ms

2.4 Related works

Significant volume of research have been conducted worldwide regarding Handover in Mobile WiMAX, the objective of many researcher in that aria was to find a way that can achieve fast Handover procedure and in the same time maintaining a reliable level of security .

The author in [1] was focusing on the issue of the authentication delay during the handover operation. His main goal was to speed up the handover operation by lessen the authentication period, which may suggest overlooking few authentication steps. In the author approached, the link security keys were transfer from serving BS to the target BS.

Therefore, the major key material were shared among the BSs, his approached was not able to satisfy the backward and forward secrecy concept.

The concept of forward secrecy is to disable the current BS from accessing communication line between target BS and MS while the backward secrecy is to disable the target BS from accessing communication line between the current BS and MS.

Based on [13], the author emphasized to decrease the overhead link with the security key entry and exit for fast handover, he purpose that the serving BS to transfer Key Association along with the information regarding the master key to the target BS. The PKMv2 or the 3-way handshake protocol can be ignore once the target BS obtain the information from the serving BS in order to accelerate the network re-entry operation.

The final result sadly, does not match the requirement needed for a perfect forward secrecy. In addition, the user may suffer from domino effect. This means that if the security of one BS is compromised, it can lead to the security breach of the communication in all of the BSs. The difficulties in backward secrecy is subtler, therefore the serving BS can easily derive the master key of the targeted BS

In [15], two capable authentication methods were proposed to improve the performance of the authentication procedure when the handover takes place. The goal of the proposed schemes was to enable the user to skip the re-authentication procedure when handover occur.

In the first scheme the user (MS) authentication at the initial entry is done by the authentication server AS through EAP authentication protocol, after that instead of using the standard EAP protocol to authenticate the user, an efficient shared key-based EAP method was proposed to authenticate the user when handover happens.

In the second scheme the default EAP authentication protocol was ignored and the user authentication is only done by SA-TEK three way handshake in the PKMv2 protocol. The proposed schemes is clearly not fit for implementation because its overlook the standard procedures

In [6], a promising solution for secure handover in Mobile WiMAX network was proposed. The author proposed an efficient pre-authentication scheme that follows the least privilege principle to solve the domino effect and handover protocol guarantees the backward and forward secrecy while giving little burden over the previous researched handover protocols.

But this pre-authentication scheme is proven to be impractical since it has no regards for the overhead of EAP authentication procedure for the subsequent HO to new BSs therefore the performance of the system will be crippled [7].

Our objective in this paper was to find an acceptable balance of fast handover process and a good level of security, so we proposed an enhanced handover scheme based on pre-authentication in [6] along with simple changes to the pre-authentication scheme. Our proposal target the main cause of delay in the handover process, and provide a suitable solution to the handover problem, therefore the user will enjoy a fast connection with a minimum interruption in a secure environment.

3. METHODOLOGY

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

For our fast handover mechanism we propose to construct both of the serving BS and the target BS to be in the same subnet. Fortunately, nowadays increasing numbers of BS are connected within the same metro Ethernet backhaul. This fact can provide a platform for faster handover. It also enables fast handover between BSs. This is because, the address of the MS remain the same in adjacent target BS inside the same subnet. All the delay associated with the IP layer procedure for building a new address association with the BS is avoided [9, 10].

Our strategy is to avoid address re-assignment hence, minimizing handover delay of the MS between the BSs. In conjunction to our proposal, for more secure handover, we have modified the pre-authentication scheme proposed in [6], to be used in our experiment. We proved by simulation that the merge of our fast handover mechanism and the modified pre-authentication scheme can provide not only low handover delay but superior level of security protection as well.

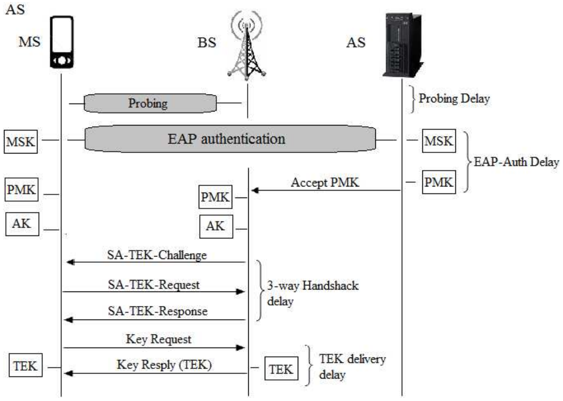

Figure 1: The Modified Message Exchange And Key Derivation At Initial Network Entry

3.1 Pre-authentication scheme

Mobile WiMAX approved the use of pre-authentication approach. A minor modification to the key management of the PKMv2 as well as pre-authentication mechanism based on the modified key hierarchy was proposed in [6]. The proposed pre-authentication mechanism enables the MS to establish a distinctive authorization key with each neighbor BS. The proposed scheme, guarantees the forward and backward secrecy. The pre-authentication mechanism manufactures the AK in the MS and the target BS before the handover occurs.

For efficient pre-authentication during initial network entry, a distinctive key namely the PMK need to be created. The key will then combine the MAC address of the MS and the BSID. This distinctive key structured by Authentication Server (AS) and delivered to the related BS instead of the MSK that commonly occurs during initial network entry in the default scenario. Construction of the PMK and AK, obtained as following.

$$PMK = Dot16KDF(MSK, MS\ MAC\ Address|BSID|\text{“PMK”}, 160), \qquad (1)$$

$$AK = PRF(PMK, 160), \qquad (2)$$

The *PRF* (PMK, 160) in the equation is a cryptographically secure pseudo-random number function that generates an output of 160-bit length on the input of PMK. Thus, a BS receives a unique PMK which no other than the MS and the AS can derive.

Distinctive PMKs created by AS for neighbor BSs during the pre-authentication phase, and AS help delivering them to the related BSs so that the neighboring BS may derives their AKs for MS. Similarly, the MS derives the PMKs and the AKs for its neighbor BSs.

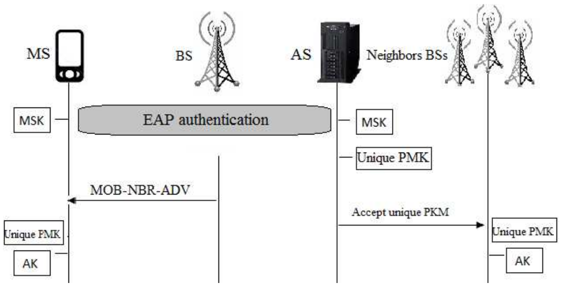

Figure 2: Pre-Authentication Phase

Unfortunately the frequent use of this pre-authentication scheme upon subsequent handover proven to be impractical, since it has no regards for the overhead of EAP authentication procedure for the repeated handover to new BSs therefore the performance of the system will be crippled [7].

In our approach the EAP-Authentication will preformed at the pre-authentication phase shown in Figure 2, resulting in the establishment of the unique PMK in the AS.

Since our approach assume that the SBS and the TBSs located in the same IP subnet the EAP-authentication for the subsequent HO will be avoided and only 3-way handshake needs to be preformed, as shown in Figure 3.
In our scheme the unique key created at the pre-authentication phase, will be stored in the AS and re-used for the subsequent handover. But in order to maintain the authenticity of the key for all the subsequent handover, the AS needs to update the

unique according to the target BS. This step can be done by including the BSID for the TBS and the MAC address of the MS as shown in equation (1) and (2).

Since the AS already maintain the MAC Address of the MS from the initial network entry, and by default the AS keeps a list of the entire neighbor BSs and there ID, so such update is possible.

On the other hand, in case that the MS cross from one BS to the next, where the BSs located in different IP subnet, the MS performs the first authentication step to register in the network. Subsequently, it must obtain a new IP address since the current IP address is not valid for the new IP subnet.

This forced the network to perform the remaining of the security procedure that required for safe communication as shown in Figure 1. Due to these, the network entry need more times, therefore the handover delay time will be longer as well [10].

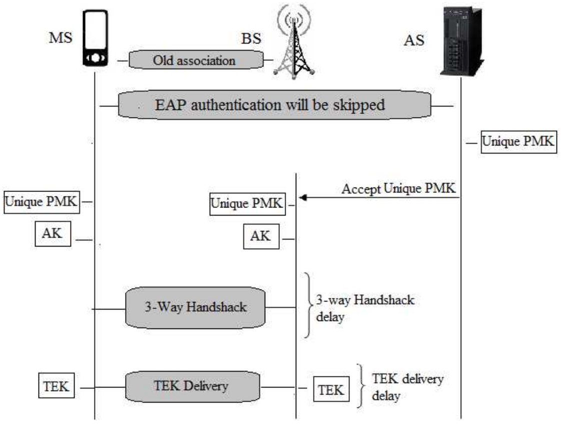

Figure 3: Message Exchange And Key Derivation at Network Re-entry For The Subsequent Handover in The Same IP Subnet Environment

4. PROTOCOL ANALYSIS

In this section, the handover delay and security analysis of the proposed handover and authentication scheme are given compared with those of the IEEE 802.16e and the ones proposed in [6]. All statistics and delay values were cited from a real world measurement study based on Mobile WiMAX in [14]. Corresponding analysis results are shown in Table 3.

In the Table 3 we can see all the hard handover steps mentioned in Table 2, we have compared the Handover delay of our proposed scheme with the IEEE 802.16e standard and the proposed approach in [6].

Table 3: Delay For The Subsequent Handover

HO Steps (ms)	802.16e	Hur *et al.*[6]	Our approach
Probing (≈68)	yes	yes	yes
EAP-Authentication(≈1000)	yes	no	no
Pre-Authentication (≈100)	no	yes	no
3-way handshake (≈100)	yes	yes	yes
TEK key REQ/REP (≈120)	yes	yes	yes
IP association (≈180)	yes	yes	no
Total Delay	≈1468 ms	≈568 ms	≈288 ms

We notice that the IEEE 802.16e standard suffer from enormous handover latency , mainly because of the delay associated with the EAP–based authentication and the IP reassignment stage , therefore the use of real-time application can be unlikely.

Hur *et al.* propose an efficient pre-authentication scheme which enables the user to reduce the delay associated with the EAP authentication protocol, but still the overall handover delay is can't be forgiven by real-time application.

Lastly our scheme proven to be very effective in reducing handover delay compared to the standard and the pre-authentication scheme proposed by [6]. And that's mainly because we were able to avoid most of the steps in hard handover process that cased the highest delay.

Users in our approach will enjoy the services of real-time application with minimum interruption.

Table 4 Security Performance [6]

	IEEE802.16e Std	Hur *et al.*[6]	Our approach
Domino Effect	No	yes	yes
Forward/Backward Secrecy	yes	yes	yes

As for the security performance we can see clearly that all schemes have the ability to provide forward and backward secrecy. Unfortunately IEEE802.16e standard will does not have the ability to protect against domino effect; meanwhile our approach does provide efficient protection against domino effect.

For further verification we tried to simulate our approach alone with Hur *et al* [6] for comparison to see if its matches the result of the real world measurement studies.

5. THE SIMULATION ENVIRONMENT AND LIMITATION

We perform simulation using ns-2 (version 2.29) simulation tool with Seamless and Secure Mobility Module which is designed and developed by the National Institute Standards and Technology (NIST) [11, 12]. We were able to insert some of the security features that are required by the Mobile WiMAX specifications to simulate the proposed pre-authentication scheme in [6].

In order for the simulation to have a reliable result, we constructed a database system that work as AAA (Authentication, Authorization and Accounting) server, there is some limitation in our handover scenario where we only conducted our simulation for layer 2 handover and did not considered the use of Mobile IP and layer 3 handover.

5.1 Simulation scenarios

There are two scenario to be shown in our simulation scenario one, have two base stations located in each scenario that place within one straight line, set for about 750 meters distance from one another, where the coverage areas for each base station encompasses as wide as 500 meters in radius.

As for the MSs, the source node fixed to produce packet size of 1500 each. In the simulation, we test the handover delay at a different MS velocity Start from 72 km/h to 252 km/h, the simulation time 180 sec.

During the simulation, handover most likely will occurs within the ambit of 500 meters from the serving BS.

In scenario one (our approach) the serving base station and the target base station are located within the same IP subnet and connected through wired connection to the backhaul network and then to the server.
Scenario two (Hur *et al.*[6]) is the same as scenario one except, the serving base and the target base station are located within different IP subnet .

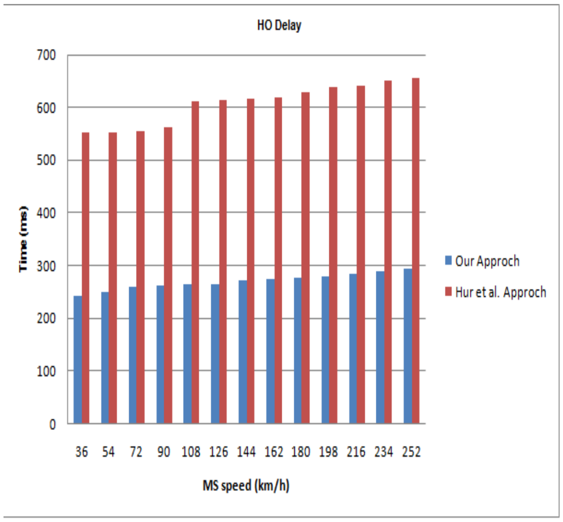

Figure 4: Average HO Delay

6. SIMULATION RESULT AND ANALYSIS

In Figure 4 we can see the average handover delay been measured in different speed velocity. Based on Figure 4, we can see that scenario 1 (our approach) has a significant low handover delay compare to the scenario 2 (Hur *et al.*[8]), in which the handover delay for scenario 1 is only 294 milliseconds compare to 655 milliseconds for scenario 2.

These numbers were taken when the MS handover from one BS to the next at a maximum speed of 252 km/h.

The reason behind this significant decrease in the handover delays of scenario 1 is that, in this scenario both SBS (serving BS) and the TBS (Target BS) are located in the same IP subnet. Therefore, all address re-assignment and procedures for IP layer handover are eliminated, and only the initial authentication step needs to be performed [9, 10].

Conversely in scenario 2 (Hur *et al.*[6]) longer handover time needed, due to the SBS and the TBS were in different IP subnet. The MS always have to notify the backbone network of its location and the CoA (Care of Address) if the handover occurs. When the MS migrated to a new IP subnet domain, it needs to re-assignment its address to the new BS. The Link layer handover followed by IP layer handover therefore, need to be preformed along with all the authentications steps required by [6]. As the results, the time needed will be longer than the scenario 1 case.

7. CONCLUSION

In this paper we proposed a design for secure and fast handover mechanism in IEEE 802.16e. The proposed handover approach gives a simple but effective solution. It solves the problem of the lengthy delay in the current handover design and protect against domino effect. From the result analysis, we can see that the highest handover delay in our approach is 294 ms, and that is clearly more than adequate to satisfy most, if not all real-time application such as VoIP and Video streaming. Parallel to the fast handover, the proposed pre-authentication scheme proven to be a fine addition to our approach to achieve fast handover with backward/forward secrecy characteristic.

REFERENCES

[1] C. K. Chang and C. T. Huang, "Fast and Secure Mobility for IEEE 802.16e Broadband Wireless Networks,"Proceedings of ICPPW 2007,Xian, China, Sept. 2007, pp.46-46.

[2] IEEE 802.16e-2005 – Amendment to IEEE Standard for Local and Metropolitan Area Networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems-Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands.

[3] Ergen, M, Mobile broadband including WiMAX and LTE, Springer Science+Business Media, LLC, Boston, 2009.

[4] Bernardos, C.J., Gramaglia, M., Contreras, L.M., Calderon, M., Soto, I, “Network-based Localized IP mobility Management: Proxy Mobile IPv6 and Current Trends in Standardization,” Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 1, pp. 16–35, 2010.

[5] Shahid Hussain, Muhammad Naeem Khan and Muhammad Ibrahim, “A Security Architecture for Wimax Networks,” International Journal of Computer Applications, vol. 50 , no.9, pp. 35-39, July 2012.

[6] Junbeom Hur, Hyeongseop Shim, Pyung Kim, Hyunsoo Yoon, Nah-Oak Song, "Security Considerations for Handover Schemes in Mobile WiMAX Networks," Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE, Las Vegas, USA, March 31 2008-April 3 2008, pp. 2531 – 2536.

[7] T.Shon, B.Koo, J.Park, H.Chang, "Novel approaches to enhance mobile WiMAX security," EURASIP Journal on Wireless Communications and Networking, vol. 2010, pp. 1-11, July 2010.

[8] Nguyen, T.N.; Maode Ma, "Enhanced EAP-Based Pre-Authentication for Fast and Secure Inter-ASN Handovers in Mobile WiMAX Networks," Wireless Communications, IEEE Transactions on , vol.11, pp.2173-2181, June 2012.

[9] Chen-Hua Shih and Yaw-Chung Chen, “A FMIPv6 Based Handover Scheme for Real-Time Applications in Mobile WiMAX,” JOURNAL OF NETWORKS, vol. 5, pp. 929-936, August 2010.

[10] Christoforos Ntantogian, Christos Xenakis, and Ioannis Stavrakakis, "A generic mechanism for efficient authentication in B3G networks", Computers & Security, vol. 29, pp. 460-475, 2010.

[11] The Network Simulator - ns-2, http://www.isi.edu/nsnam/ns/.

[12] Seamless and Secure Handover, http://www.nist.gov/itl/antd/emntg/ssm_tools.cfm.

[13] Kihun Hong, Souhwan Jung, Ki Jun Lee, Brian Lee, Jungwook Wang, "Secure Roaming of Key Association for Fast handover," IEEE C802.16e-04/407, 2004.

[14] Hua Cai, et al., “Measurement-Based Low-Level Performance Analysis of IEEE 802.16e/WiBro Networks," Proc. International Conference on Information Networking, Busan, Korea, Jan. 27-29, 2010.

[15] Hung-Min Sun; Shih-Ying Chang; Yue-Hsun Lin; Shin-Yan Chiou, "Efficient Authentication Schemes for Handover in Mobile WiMAX," *Intelligent Systems Design and Applications, 2008. ISDA '08. Eighth International Conference*, Kaohsiung., 26-28 Nov. 2008, pp.235,240.

[16] Ray, S.K.; Pawlikowski, K.; Sirisena, H., "Handover in Mobile WiMAX Networks: The State of Art and Research Issues," *Communications Surveys & Tutorials, IEEE* , vol.12, no.3, pp.376,399, Third Quarter 2010.