INTERNATIONAL JOURNAL ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 1st June 2017. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-4

Title: ECC Based Security Architecture For LTE Multihop Wireless Networks.

Volume 06, Issue 04, Page No: 1414 - 1422.

Paper Authors

*** L ANUSHA, K GOVINDARAJULU.**

* Eluru College of Engineering and Technology.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Ecc Based Security Architecture For Lte Multihop Wireless Networks

*L ANUSHA, ** K GOVINDARAJULU
*PG Scholar, Eluru College of Engineering and Technology.
**Associate Professor, Eluru College of Engineering and Technology.
anusha.2054@gmail.com grk.elr@gmail.com

ABSTRACT

Vehicular communications have received a great deal of attention in recent years due to the demand for multimedia applications during travel and for improvements in safety. Safety applications often require fast message exchanges but do not use much bandwidth. On the other hand, multimedia services require high bandwidth for vehicular users. Hence, to provide mobile broadband services at a vehicular speed of up to 350 km/h, Long-Term Evolution (LTE) are considered the best technologies for vehicular networks. LTE are Fourth-Generation (4G) wireless technologies that have well-defined quality of service (QoS) and security architectures. However, some security threats, such as denial of service (DoS), an introduction of rogue node, etc., still exist in LTE networks, particularly in multihop networks. Therefore, strong security architecture and hasty authentication methods are needed to mitigate the existing security threats in 4G multhop wireless networks. Conversely, the network QoS should not be degraded while enhancing security. Thus, we propose security architecture using the elliptic curve Diffie–Hellman (ECDH) protocol that has proven security strength and low overhead for 4G wireless networks. In this paper, we first describe the current security standards and security threats in LTE networks. Then, the proposed distributed security architecture for 4G multihop wireless networks is presented. The proposed scheme provides strong security and hasty authentication for handover users without affecting the QoS performance.

Index Terms—QR barcode, secret sharing, cryptography, RSA algorithm

I. INTRODUCTION

IN general, vehicular applications can be divided into two groups: safety and nonsafety applications. Safety applications often require fast message exchanges but do not use much bandwidth. In order to support safety applications, such as colli sion avoidance, hard-braking warnings, accident reporting, and intersection announcements, etc., vehicles are enabled to com municate with one another via (vehicle-to-vehicle communica tions) or via roadside access points (vehicle-to-roadside com munications). These vehicular communications are expected to contribute to safer roads by providing timely information to drivers and to make travel more convenient. Conventionally, vehicular ad hoc networks are used to implement dedicated short-range communications (DSRC) for safety applications. The DSRC standard, i.e., IEEE 802.11p, is probably the best positioned technique to provide safety services.On the other hand, the nonsafety applications require high bandwidth and strong security to support multimedia services for vehicular users. To support multimedia services for vehicular users, the networks that have high bandwidth, such as cellular and satellite networks, are considered. When comparing cellular and satellite networks, satellite networks are more expensive but provide lower quality-of-service (QoS) performance. On the contrary, the telecommunication industry landscape for cellular networks is rapidly growing from second-generation (2G) to fourth-generation (4G) to accommodate the increasing usage of multimedia applications and users mobility. In 4G networks, Long-Term Evolution (LTE) IS THE emerging broadband wireless technologies aimed at providing high-speed Internet of 100 Mb/s at a vehicular speed of up to 350 km/h. Further, 4G wireless standards provide well-defined QoS and security architecture. For this reason, 4G cellular networks are considered up-and-coming technologies for vehicular multimedia applications.

LTE resemble each other in some key aspects, including operating frequency spectrum, high capacity, mobility, strong QoS mechanisms, and strong security with a similar key hierarchy from the core network to the access network. However, LTE also differ from each other in certain aspects, as they have evolved from different origins. LTE has evolved from 3rd Generation Partnership Projects (3GPP); thus, the LTE network has to support the existing 3G users' connectivity, the LTE authentication process uses the EAP Authentication and Key Agreement (EAP-AKA) procedure that authenticates only the International Mobile Subscriber Identity (SIM) burned in a subscriber identity module (SIM) card. Consequently, the LTE security does not meet the enterprise security requirement, as LTE does not authenticate enterprisecontrolled security.

In wireless communications, security threats may occur in both the physical (PHY) and the medium access control (MAC) layers. The attacker can attack the radio frequency (RF) channel for the PHY-layer threats. For the MAC-layer threats, the attackers can spoof, modify, and replay the MAC-layer control messages. In one of the worst case scenarios, the attackers take total control of the network by knowing the confidential details in control messages. Nevertheless, in practice, Internet service providers may use the Internet Protocol Security (IPSec) approach at Layer 3 for their wireless access due to its popularity in wired networks. Usually, IPSec will affect the QoS performance, because the IPSec header in each packet consumes additional bandwidth. To mitigate the security threats and performance degradation, we propose a distributed security scheme using a protocol—elliptic curve Diffie–Hellman (ECDH)—that has lower overhead than that of IPSec. ECDH is a Layer-2 key agreement protocol that allows users to establish a shared key over an insecure channel. ECDH was investigated, and the results showed that it did not affect the QoS performance much in 4G single-hop WiMAX networks. Therefore, ECDH is adopted in this research in dealing with the existing Layer-2 security threats for 4G multihop networks. Further, we also compare the security and QoS performance of the IPSec and the default security scheme as defined in the WiMAX standards, using a testbed implementation.

This paper is an extension of our previous effort, as presented, which was simply an initial theoretical study based on the proposed ECDH scheme.

In available LTE chipsets, we were unable to implement our proposed scheme in a real-time testbed. For this reason, the second objective of this paper is to perform simulations to evaluate the QoS performance of the proposed scheme using ECDH. Moreover, there is a lack of an integrated study and QoS-aware solutions for multihop LTE security threats in existing research efforts. Therefore, the third objective of this paper is then to analyze LTE for network convergence that may be useful or even crucial for service providers to support high-speed vehicular applications. In short, we are motivated to fill those research gaps, and we have made the following contributions in this paper.

II. BACKGROUND

ECC is performed over one of two underlying Galois fields: prime order fields GF(p) or characteristic two fields GF(2^m).Both fields are considered to provide the same level of security, but arithmetic in will be the focus of this paper because it can be implemented in hardware more efficiently using modulo-2 arithmetic.

An elliptic curve E over the field GF(2^m) is the set of solutions to the equation

$$\mathrm{Y}^2 + \mathrm{XY} = \mathrm{X}^3 + \mathrm{AX}^2 + \mathrm{B} \tag{1}$$

$$\text{Where } \mathrm{A}, \mathrm{B} \in \mathrm{GF}(2^{\mathrm{m}}), \mathrm{B} \neq 0$$

Let $\mathrm{P}_1 = (\mathrm{X}_1, \mathrm{Y}_1) \in \mathrm{E}\ \&\ \mathrm{P}_2 = (\mathrm{X}_2, \mathrm{Y}_2) \in \mathrm{E}$, then summing the two points is $\mathrm{P}_1 + \mathrm{P}_2 = \mathrm{P}_3 = (\mathrm{X}_3, \mathrm{Y}_3) \in \mathrm{E}$, Where,

$$\mathrm{X}_3 = \begin{cases} \left(\dfrac{\mathrm{Y}_1 + \mathrm{Y}_2}{\mathrm{X}_1 + \mathrm{X}_2}\right)^2 + \dfrac{\mathrm{Y}_1 + \mathrm{Y}_2}{\mathrm{X}_1 + \mathrm{X}_2} + \mathrm{X}_1 + \mathrm{X}_2 + \mathrm{A}, \mathrm{P}_1 \neq \mathrm{P}_2 \\ \mathrm{X}_1^2 + \dfrac{\mathrm{B}}{\mathrm{X}_1^2}, \mathrm{P}_1 = \mathrm{P}_2 \end{cases} \tag{2}$$

$$y_3 = \begin{cases} \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1 + x_3) + x_3 + y_1, & P_1 \neq P_2 \\ x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right)(x_3) + x_3, & P_1 = P_2. \end{cases} \tag{3}$$

Hence, when $\mathrm{P}_1 = \mathrm{P}_2$ we have the point-doubling operation (DBL), and when $\mathrm{P}_1 \neq \mathrm{P}_2$ we have the point-adding operation (ADD). These operations in turn constitute the crux of any ECC-based algorithm, known as point multiplication or scalar multiplication KP.

Due to the computational expense of inversion compared to multiplication, several projective coordinate methods have been proposed, which use fractional field arithmetic to defer the inversion operation until the end of the point multiplication. No precomputations or special field/curve properties are required. Procedures to perform DBL and ADD are derived from efficient formulas which use only the x-coordinate of the points. In the projective coordinate version of the formulas, the x-coordinate of is represented by $\mathrm{X_i/Z_i}$, for $\mathrm{i} \in \{1,2,3\}$; the corresponding DBL and ADD computations are shown in (4) and (5), respectively, and are used in the projective coordinate point multiplication algorithm.

$$\begin{aligned} x(2P_i) &= X_i^4 + b.Z_i^4 \\ z(2P_i) &= Z_i^2.X_i^2 \end{aligned} \tag{4}$$

$$\begin{aligned} Z_3 &= (X_1.Z_2 + X_2.Z_1)^2 \\ X_3 &= x.Z_3 + (X_1.Z_2) \cdot (X_2.Z_1). \end{aligned} \tag{5}$$

III. SECURITY THREATS IN LONG TERM EVOLUTION NETWORKS

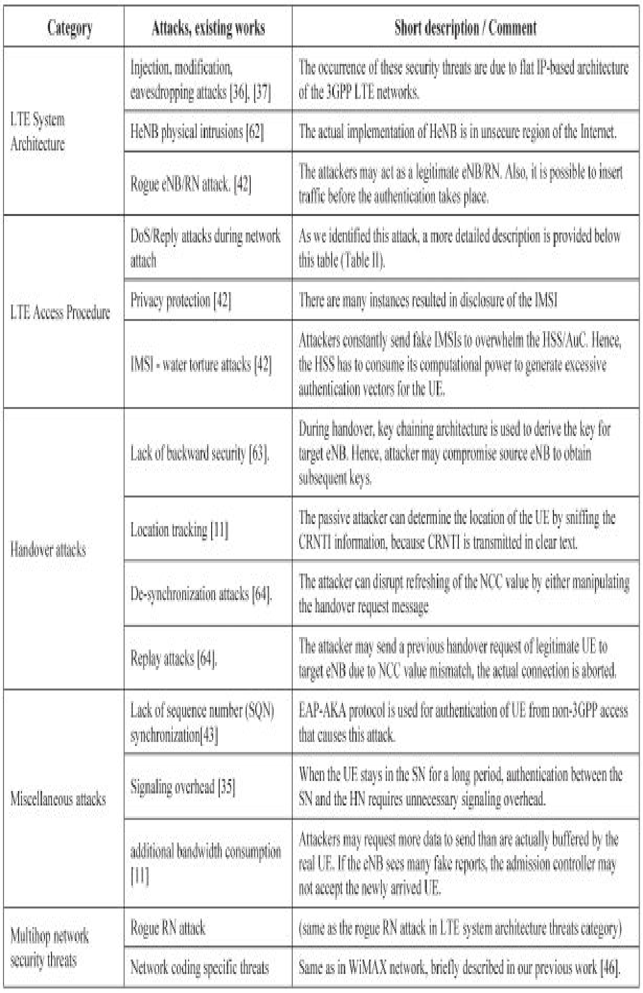
To understand the concept of security threats in LTE, Cao et al presented a comprehensive survey of various attacks and solutions in LTE networks.

The major categories are vulnerabilities in 1) access network; 2) IMS domain; 3) HeNB; and

4) MTC domain. However, due to the page limit, we only focused on the access network. The various security threats in LTE access networks have been studied and summarized in Table II. As we have identified the DoS/Reply attack in LTE, which is one of the major security threats in LTE, a detailed description of the attack is also presented.

DoS Attack During Initial Attachment: In LTE networks, DoS attacks may be possible during the initial attachment because the UE is sending MAC messages in plain text to eNB. DoS attack during the initial attachment is very critical as the UE cannot register with the home network. This is similar to the DoS attack in WiMAX networks during initial network entry. During the random-access process, the UE sends the randomaccess preamble to eNB and waits for the response until the predefined time limit. eNB responds to UE for timing adjustments and bandwidth allocation by sending an Attach Request message along with the PreambleID. If the received randomaccess PreambleID does not match the transmitted randomaccess preamble, the random-access response is considered not successful, and the UE continues the random-access process until the count reaches the maximum limit. Since the response is in plain text, an attacker can easily change the PreambleID continuously. As a result, the UE cannot register with the home net ork, which leads to the DoS attack.

TABLE II
SECURIY THREATS IN LTE NETWORKS



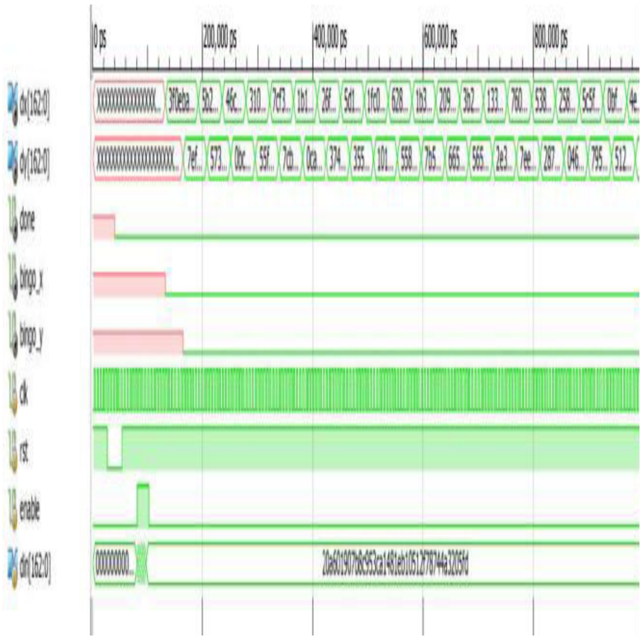
Category	Attacks, existing works	Short description / Comment
LTE System Architecture	Injection, modification, eavesdropping attacks [36], [37]	The occurrence of these security threats are due to flat IP-based architecture of the 3GPP LTE networks.
	HeNB physical intrusions [62]	The actual implementation of HeNB is in unsecure region of the Internet.
	Rogue eNB/RN attack. [42]	The attackers may act as a legitimate eNB/RN. Also, it is possible to insert traffic before the authentication takes place.
LTE Access Procedure	DoS/Reply attacks during network attach	As we identified this attack, a more detailed description is provided below this table (Table II).
	Privacy protection [42]	There are many instances resulted in disclosure of the IMSI
	IMSI - water torture attacks [42]	Attackers constantly send fake IMSIs to overwhelm the HSS/AuC. Hence, the HSS has to consume its computational power to generate excessive authentication vectors for the UE.
Handover attacks	Lack of backward security [63].	During handover, key chaining architecture is used to derive the key for target eNB. Hence, attacker may compromise source eNB to obtain subsequent keys.
	Location tracking [11]	The passive attacker can determine the location of the UE by sniffing the CRNTI information, because CRNTI is transmitted in clear text.
	De-synchronization attacks [64].	The attacker can disrupt refreshing of the NCC value by either manipulating the handover request message
	Replay attacks [64].	The attacker may send a previous handover request of legitimate UE to target eNB due to NCC value mismatch, the actual connection is aborted.
Miscellaneous attacks	Lack of sequence number (SQN) synchronization[43]	EAP-AKA protocol is used for authentication of UE from non-3GPP access that causes this attack.
	Signaling overhead [35]	When the UE stays in the SN for a long period, authentication between the SN and the HN requires unnecessary signaling overhead.
	additional bandwidth consumption [11]	Attackers may request more data to send than are actually buffered by the real UE. If the eNB sees many fake reports, the admission controller may not accept the newly arrived UE.
Multihop network security threats	Rogue RN attack	(same as the rogue RN attack in LTE system architecture threats category)
	Network coding specific threats	Same as in WiMAX network, briefly described in our previous work [46].

I. RESULT ANALYSIS

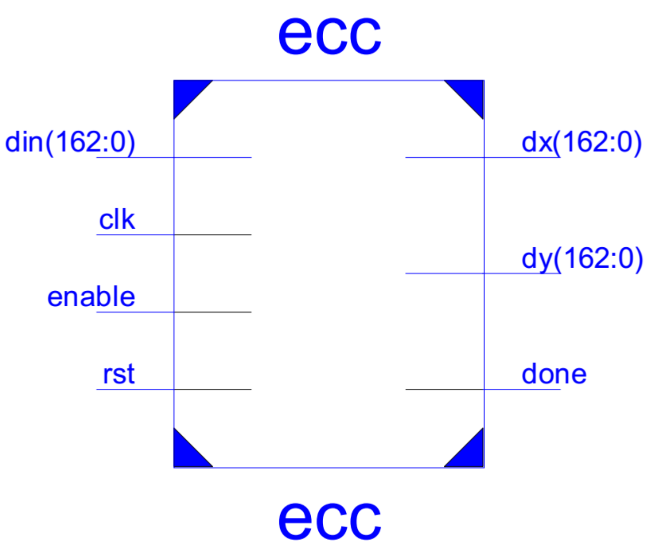
In this paper we have further presented the originator of public key cryptosystems, the Diffie-Hellman key exchange algorithm. In the following we looked at the complexity theoretic problems this algorithm was based on.

Then we explained a cryptosystem that was derived from the one presented before, but could be seen as an improvement. This Cryptosystem can be used for encryption and signing messages without direct interaction. Not only the cryptosystem itself can be compromised. As public key systems are designed for the populace, a bigger security issue is in handling the private keys. Many people do not secure their private keys as would be necessary. And to be correctly applied, a private key that was accessible by a malicious user, even if it was not, has to be declared compromised. This is due to attackers being able to cover his tracks and steal the private key undetected.

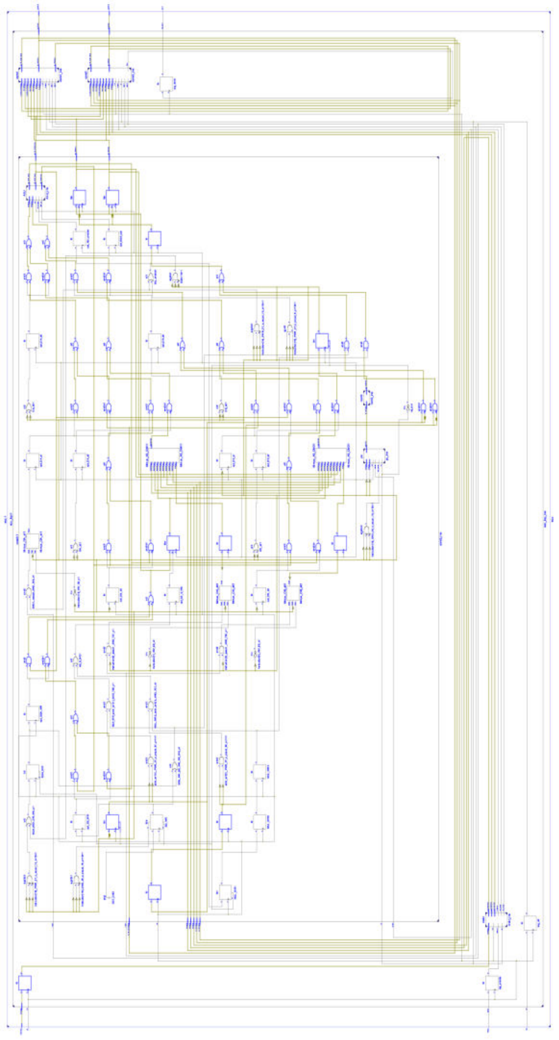
Unfortunately, the complexity of the issues involved in dealing with cryptographic systems and software keeps many people from using them. In nowadays world, where all Internet communication is supervised by several authorities, encryption offers the possibility to get at least some privacy back.



ECC_Simulation



ECC_RTL1



ECC_RTL2

II. CONCLUSION AND FEATURE RESEARCH

As the increase in demand for multimedia applications and for the safety of mobile users, providing Internet that supports QoS-aware and safe multimedia services for vehicular networks is mandatory for service providers. To provide high bandwidth support at the vehicular speed of up to 350 km/h, the LTE networks are the preferred candidates. 4G networks have well-defined QoS and security architectures. However, some major security threats such as DoS attack still exist in 4G multihop networks, because certain MAC messages are transmitted only in plain text. For this reason, we have proposed a distributed security architecture using the ECDH algorithm in Layer 2 for 4G multihop wireless networks. In the proposed scheme, the wireless nodes are initially authenticated by the home network and then authorized by the access node. In addition, the proposed scheme requires only a slightly higher bandwidth and computational overhead than the default standard scheme.

Nevertheless, there are still threats to the LTE system architecture, i.e., disclosure of IMSI due to rogue RN, lack of backward secrecy, rogue RN attack, and synchronization attack. For disclosure of IMSI, the enterprise authentication protocol, e.g., EAP-TTLS, secures the identity protection of the user. The other threats previously mentioned warrant further investigation. Currently, we are also working on other security threats in the LTE system architecture and security threats, such as IMS security, HeNB security, and MTC security, in other domains or layers of LTE networks.

III. REFERENCES

1. EEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE 802.16- 2009, 2009.
2. Amendment to IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems—Multiple Relay Specification, IEEE 802.16j, 2009.
3. Amendment to IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Broadband Wireless Access Systems—Advanced Air Interface, IEEE 802.16m, 2011.
4. “WiMAX end-to-end network systems architecture (Stage 3: Detailed protocols and procedures) Release 1, V.1.3.0,” WiMAX Forum, Clackamas, OR, USA, 2008.
5. “Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description, Stage 2, Release 11,” 3GPP, Sophia-Antipolis, France, 3GPP TS 36.300 V11.3.0, 2011.
6. “3GPP System Architecture Evolution (SAE); Security architecture,” 3GPP, Sophia-Antipolis, France, 3GPP TS 33.401, v12.5.0, 2012, Release 12.
7. “Feasibility study on LTE relay node security, Release 10,” 3GPP, SophiaAntipolis, France, 3GPP TS 33.816 v10.0.0, 2011.
8. E. Dahlman, S. Parkvall, and J. Skold, LTE–LTE-Advanced for Mobile Broadband. Oxford, U.K.: Elsevier, 2011, pp. 301–322.
9. N. A. Ali, A.-E. M. Taha, and H. S. Hassanein, LTE, LTE-Advanced and WiMAX: Towards IMT-Advanced Networks. Chichester, U.K.: Wiley, 2012.

10. P. Rengaraju, C-H. Lung, and A. Srinivasan, "An analysis on mobile WiMAX security," in Proc. IEEE Toronto Int. Conf. Sci. Tech. Hum., 2009, pp. 439–444.
11. N. Seddigh, B. Nandy, and R. Makkar, "Security advances and challenges in 4G wireless networks," in Proc. 8th Annu. Conf. Privacy, Security, Trust, 2010, pp. 62–71.
12. L. Yi, K. Miao, and A. Liu, "A comparative study of WiMAX and LTE as the next generation mobile enterprise network," in Proc. 13th Int. Conf. Adv. Comm. Tech., 2011, pp. 654–658.
13. T. Shon and W. Choi, "An analysis of mobile WiMAX security: Vulnerabilities and solutions," in Lecture Notes in Computer Science, T. Enokido, L. Barolli, and M. Takizawa, Eds. Berlin, Germany: Springer-Verlag, 2007, pp. 88–97.
14. H. Jin, L. Tu, G. Yang, and Y. Yang, "An improved mutual authentication scheme in multi-hop WiMax network," in Proc. Int. Conf. Comput. Elect. Eng., 2008, pp. 296–299.
15. T. Han, N. Zhang, K. Liu, B. Tang, and Y. Liu, "Analysis of mobile WiMAX security: Vulnerabilities and solutions," in Proc. 5th Int. Conf. Mobile Ad Hoc Sensor Syst., 2008, pp. 828–833.
16. H-M. Sun, S-Y. Chang, Y-H. Lin, and S-Y. Chiou, "Efficient authentication schemes for handover in mobile WiMAX," in Proc. 8th Int. Conf. Syst. Des. Appl., 2008, pp. 235–240. D. Johnston and J. Walker, "Overview of IEEE 802.16 security," IEEE Security Privacy Mag., vol. 2, no. 3, pp. 40–48, May/Jun. 2004.
17. C-T. Huang and J. M. Chang, "Responding to security issues in WiMAX networks," IEEE Comput. Soc. IT Prof. Mag., vol. 10, no. 5, pp. 15–21, Sep./Oct. 2008.
18. H-M. Sun, Y-H. Lin, and S-M. Chen, "Secure and fast handover scheme based on pre-authentication method for 802.16-WiMAX," in Proc. IEEE Region 10 Conf., 2007, pp. 1–4.
19. J. Hur, H. Shim, P. Kim, H. Yoon, and N.-O. Song, "Security considerations for handover schemes in mobile WiMAX networks," in Proc. Int. Conf. Wireless Comm. Netw., 2008, pp. 2531–2536.
20. Y. Kim, H-K. Lim, and S. Bahk, "Shared authentication information for preventing DDoS attacks in mobile WiMAX Networks," in Proc. 5th IEEE Conf. Consum. Comm. Netw., 2008, pp. 765–769.
21. F. Liu and L. Lu, "A WPKI-based security mechanism for IEEE 802.16e," in Proc. Int. Conf. Wireless Comm., Netw. Mobile Comput., 2006, pp. 1–4.
22. B. Sikkens, "Security issues and proposed solutions concerning," presented at the 8th Twente Student Conf. Information Technology, Enschede, The Netherlands, 2008.
23. Y. Lee, H. K. Lee, G. Y. Lee, H. J. Kim, and C. K. Jeong, "Design of hybrid authentication scheme and key distribution for mobile multi-hop relay in IEEE 802.16j," in Proc. Euro Amer. Conf. Telematics Inf. Syst., 2009, p. 12.
24. A. DeCarlo, J. Porthy, S. Tyler, B. Xie, R. Reddy, and D. Zhao, "Distributed trust relationship and polynomial key generation for IEEE 802.16m network," in Proc. Mobile WiMAX Symp., 2009, pp. 111–116.
25. J. Donga, R. Curtmolab, and C. N. Rotarua, "Secure network coding for wireless mesh networks threats challenges

and directions," J. Comput. Commun., vol. 32, no. 17, pp. 1790–1801, Nov. 2009.

26. G. Kambourakis, E. Konstantinou, and S. Gritzalis, "Revisiting WiMAX MBS security," Int. J. Comput. Math. Appl., vol. 60, no. 2, pp. 217–223, Jul. 2010.

27. A. Deininger, S. Kiyomoto, J. Kurihara, and T. Tanaka, "Security vulnerabilities and solutions in mobile WiMAX," Int. J. Comput. Sci. Netw. Security, vol. 7, no. 11, pp. 7–15, Nov. 2007.

28. S. Kumar, M. Girimondo, A. Weimerskirch, C. Paar, A. Patel, and A. S. Wander, "Embedded end-to-end wireless security with ECDH key exchange," in Proc. IEEE Midwest Symp., Circuits Syst., 2003, pp. 786–789.

29. K. Lauter, "The advantages of elliptic curve cryptography for wireless security," IEEE Wireless Commun. Mag., vol. 11, no. 1, pp. 62–67, Feb. 2004.

30. K. Byoung-Jo and S. Srinivasan, "Simple mobility support for IPsec tunnel mode," in Proc. 58th IEEE VTC Conf., 2003, pp. 1999–2003.

31. E. Barka, K. Shuaib, and H. Chamas, "Impact of IPSec on the performance of the IEEE 802.16 wireless networks," in Proc. Int. Conf. New Tech., Mobility Security, 2008, pp. 1–6.

32. L. Nazaryan, E. Panaousis, and C. Politis, "IPSec provisioning in WiMAX networks," IEEE Veh. Technol. Mag., vol. 5, no. 1, pp. 85–90, Mar. 2010.

33. C. B Sankaran, "Network access security in next-generation 3GPP systems: A Tutorial," IEEE Commun. Mag., vol. 47, no. 2, pp. 84–91, Feb. 2009.

34. M. Purkhiabani and A. Salahi, "Enhanced authentication and key agreement procedure of next generation evolved mobile networks," in Proc. 3rd Int. Conf. Commun. Softw. Netw., 2011, pp. 557–563.