Enhanced CRA Protocol For Seamless Connectivity In Wireless Networks

Elankayer Sithirasenan, Khosrow Ramezani, Vallipuram Muthukkumarasamy
School of Information and Communication Technology
Griffith University, Gold Coast, Australia
{e.sithirasenan, k.ramezani, v.muthu}@griffith.edu.au

***Abstract*–**The "post-PC" era is longing for the convergence of heterogeneous wireless communication technologies to enable seamless data connectivity. Wireless Technologies such as Wireless Local Area Networks (WLAN), Worldwide Interoperability for Microwave Access (WiMAX), Long Term Evolution (LTE) etc., attract new opportunities for collaborative and complementary usage. In the post-PC era more and more applications are emerging to benefit from the ubiquitous nature of the mobile devices. However, with the range of approaches that are used to validate the mobile devices in heterogeneous wireless networks, the need for a user friendly, flexible and reliable method to interconnect and utilize the different classes of wireless networks is becoming inevitable. In this paper, we present and analyze the different authentication mechanisms that are available for wireless networks and evaluate their advantages and limitations. We then propose an enhancement to the Coordinated Robust Authentication (CRA) protocol that can be encapsulated within the RADIUS protocol utilizing the advantages of public key infrastructure. We also present a security and cost evaluation on the proposed enhanced protocol.

Keywords– Wireless Networks, Authentication, Access Control, Heterogeneous Networks.

I INTRODUCTION

Today we are moving into a "post-PC" world! Not many people sit in front of custom built PCs to do their businesses any more. Hand held wireless devices such as iPod Touch, iPhone, Galaxy S3, iPad, Galaxy Tab, Airbook, Notepad etc. are bringing in a new paradigm as to how people use and communicate information. However, the mobility of these post-PC wireless devices is restricted to some extent due to the limitations in wireless data connectivity. A wireless device at home should preferably get its data connectivity through the wireless router, while on the move from the 3G or 4G network and while at work from the office wireless network. To achieve this interoperability the wireless devices must be recognized by the various networks as it roams from one network to another.

Due to the inherent nature of the wireless communications, wireless networks encounter numerous security problems compared to its wired counterpart. The most significant of these is the first time association. Whether it is a WLAN [1], WiMAX [2] or a 4G LTE [3], all wireless networks will have this setback. The lack of physical connectivity (anchor-attachment) from the wireless device to the network makes the wireless network more vulnerable and hard to protect against authenticity, confidentiality, integrity and availability threats [4][5]. Hence, to overcome this first time association problem wireless devices adopt a range of different techniques.

The Robust Security Network Association (RSNA) proposed in IEEE 802.11i [6] has emerged as the most popular method to counter the first time association problem. The RSNA technique is widely used in both WLANs and WiMAX. Although IEEE 802.11i security architecture offers sufficient protection to the wireless environment, it is up to the implementer to guarantee that all issues are addressed and the appropriate security measures are implemented for secure operation. A single incorrectly configured station could lead the way for a cowardly attack and expose the entire organizational network [7][8].

Notwithstanding the configuration issues, RSNA is the most preferred first time association method for wireless networks. The use of IEEE 802.1x port based access control [9] makes it more flexible for mutual authentication and key distribution. However, RSNA does not provide options for coordinated authentication in a heterogeneous network environment. This results in the wireless users having to use different credentials to authenticate in the different wireless networks. Therefore, a Coordinated Robust Authentication (CRA) Mechanism with the ability to use a single set of credentials with any network, wireless or wired would be of immense significance to both network users and administrators.

In this paper we first examine the various authentication mechanisms proposed by other researchers for similar applications and then illustrate our proposed mechanism. In section four we present a security and cost evaluation and conclude the paper in section five.

II INTEGRATING WIRELESS NETWORKS

Iyer et al. [10] assert that WLAN and WiMAX are particularly interesting in their ability towards mobile data oriented networking. They confirm that a scheme enabling mobility across these two would provide several advantages to end-users, wireless operators as well as wireless internet service Providers. Distributed authentication scheme proposed by Machiraju et al. [11] relies on Base Stations (BS) to collectively store authentication information. However, the study does not clarify how the base stations will initiate contact with each other. The security approach to establish a secure connection between the BS is not provided. The paper falls short to provide enough details for elimination of traditional backend authentication servers.

EAP-FAMOS [12] and OSNP [13] both use the Kerberos based authentication within existing EAP framework. Apart from the high administrative costs in Kerberos based methods;

their solution is mainly targeted at specific wireless networks and authentication mechanisms.

Narayanan et al. [14] propose ERP, an extension to the EAP framework and an EAP key hierarchy to support Re-authentication. As specified in RSNA, MSK is generated on successful completion of the authentication phase (phase 2 of RSNA). Subsequently MSK is passed to the authenticator to generate the TSK (phase 3 of RSNA). The TSK is then used for data encryption between the supplicant and the authenticator. However, the EAP framework proposed by Narayanan et al. suggests two additional keys to be derived by all EAP methods: the Master Session Key (MSK) and the Extended MSK (EMSK) which forms the EAP key hierarchy. They make use of the EMSK for re-authentication and successive key derivations.

ERP defines two new EAP messages EAP-Initiate and EAP-Finish to facilitate Re-authentication in two round trip messages. At the time of the initial EAP exchange, the peer and the server derive an EMSK along with the MSK. EMSK is used to derive a re-authentication Root Key (rRK). The rRK can also be derived from Domain-Specific Root Key (DSRK), which itself is derived from the EMSK. Further, a re-authentication Integrity Key (rIK) is derived from the rRK; the supplicant and the authentication server use the rIK to provide proof of possession while performing an ERP exchange. After verifying proof of possession and successful authentication, re-authentication MSK (rMSK) is derived from the rRK. rMSk is treated similar to MSK obtained during normal EAP authentication i.e. to generate TSK [15].

Apart from the few modifications to the EAP protocol due to the introduction of two new EAP codes, ERP integrates with the existing EAP framework very well. However, EAP-ERP requires a full EAP authentication at first when a user enters a foreign network. Further, if one supplicant for any reason has not been able to extract domain name of the foreign network then it should solicit it from its home server, this can result in long authentication delays. In the next section we briefly describe the CRA protocol and present our proposed enhancements to it.

III ENHANCED CRA PROTOCOL

The principal notion behind the CRA authentication mechanism is that every wireless device will primarily be associated with one wireless network, which can be referred to as its HOME network. The credentials used by a wireless device to associate with its HOME network are assumed to be robust and specific to that network. Therefore, a wireless device must be able to use its authority in the HOME network to reliably associate with any other FOREIGN network. In this context, the AAA server that authorizes the wireless device in its home network is called as the HOME AAA Server (HAS) and the AAA server in a foreign network is called as the FOREIGN AAA Server (FAS). Hence, our authentication mechanism will require only one set of credentials that it uses in the home network to access any foreign network. We are considering both different types networks and different authentication mechanisms that may be specific and effective to that type of network. Further details of our CRA protocol can be found in [16].

The Enhanced CRA protocol provides authentication in two modes; Full Authentication and Re-Authentication. With regard to mutual authentication CRA uses RADIUS servers as suggested in IEEE 802.1x [17]. RADIUS protocol exhibits better performance compared to other mutual authentication protocols [18]. CRA suggests direct communication between radius servers by pre-arranged agreement or the servers could find each other dynamically. In case the RADIUS servers do not have a pre-arranged agreement they can use their CA-signed PKI certificates to ascertain trust between servers.

All AAA servers that participate in the CRA must possess a CA-signed PKI certificate and be capable of obtaining the CA-signed PKI certificates of other participating AAA servers. Assuming that all AAA Servers that participate in the CRA are in possession of their CA-signed PKI certificates, the CRA protocol can communicate between FAS and HAS securely.

A. Full EAP-CRA authentication:

Initial assumption of the CRA protocol is that each mobile Node is primarily associated with one Network, which in this context is referred to as the Home network. The security of the Home network and the authentication mechanism used must be robust. We anticipate that an EAP method such as EAP-TLS, EAP-PEAP or EAP-TTLS is used in the Home network. Therefore the values for MSKName, MSK, EMSK and the Time To Live (TTL) for these keys are available for the Peer. Since some of the EAP methods utilize CA-signed PKI certificates to authenticate and secure the communication, CRA extends it to add more flexibility to certificate based authentication. In this paper WLAN has been chosen as the medium to illustrate the components and messaging of EAP-CRA. Firstly, both the peer and the Foreign Access Point (FAP) discover their capabilities and decide on a suitable protocol to authenticate each other. If both parties are capable of EAP-CRA then the FAP will compose an EAP request message to solicit the identity of the Peer. It should be mentioned that the key for hashing function is generated from the EMSK.

In an unknown network, the peer will first check if the TTL of MSK is still valid. Expired MSK will lead to a failed authentication and will prompt a full authentication. The peer will be responsible to do a full authentication with its Home Network to obtain a fresh MSK. On the other hand, if the MSK is valid, the peer generates a random sequence number and encrypts the MSKname of the home network and the sequence number by the public Key of its HAS. The composed EAP-Response message will be sent to the FAP, which contains the encrypted message, Message Authentication Code, the realm of the home network and the random identity of the peer (message 2 in Figure 1).

FAP will encapsulate this EAP-Response message inside a RADIUS Packet and forward it to the foreign authentication server. The FAS will also utilize RADIUS for server-to-server communication. However before sending the received message, the FAS will add its domain name and encrypt the

MSKname with its Private Key (message 3 in Figure 1). This enables the HAS to authenticate the FAS.

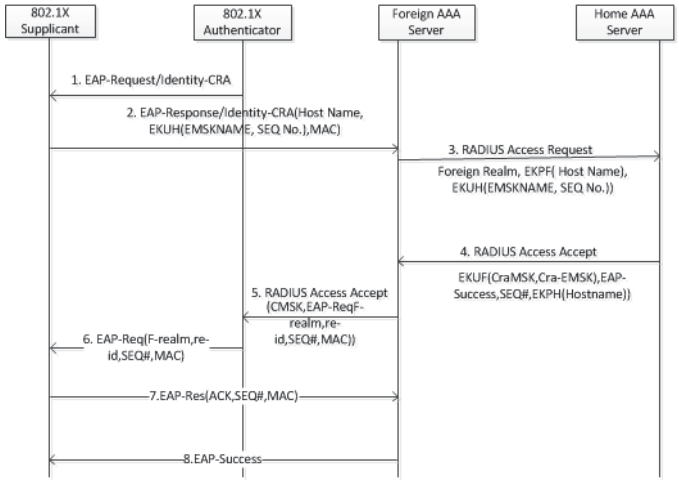

Fig. 1. Coordinated Robust Authentication (CRA) Full Authentication Protocol.

Upon receiving the message from a foreign network, HAS is able to check if the FAS is authorized based on the domain name of the FAS. The HAS can authenticate the FAS by verifying the contents of the signed message. Peer authentication will be managed by matching the MSKname with MSK, EMSK, Validation of key timer and the number of re-authentication of the peer. If the MSK is valid, the HAS can combine the foreign domain name, sequence number and the previous EMSK to generate new domain specific CRA-MSK and CRA-EMSK.

After updating the timer and counter values of the MSKname the HAS creates a RADIUS message which holds Access Accept, encrypted values of CRA-MSK and CRA-EMSK (with FAS's Public Key), MAC and privately signed message of domain name – MSKname (message 4 in Figure 1).

FAS first checks the signed MSKname to validate the HAS, and then stores the MSKname and CRA keys. In addition to these it calculates a new timer, counter and random re-authentication ID for local re-authentication in case the peer stays for longer time in the foreign network. These values are CRA_timer, CRA_counter, and CRA_RND. The value of the CRA_timer must be less than the validity time of the initial MSK. Next, the FAS sends CRA_counter, re_id, EMSKname signed with HAS's private key, Foreign realm and CRA-MSK inside a RADIUS packet to FAP (message 5 in Figure 1). The CRA-MSK will be utilized for future communication to provide privacy. The rest of the message is sent to the peer (message 6 in Figure 1). The peer will be able to authenticate its home server by verifying the signature and can generate CRA-MSK and CRA-EMSK. It then creates a EAP-Response as an acknowledgment with MSKname. The FAS can then compose a EAP-Success message and send it back to the peer.

On receiving the EAP success message, the peer generates rMSK independently leading to the key distribution phase. The key distribution phase will be similar to that of the RSNA where the supplicant and the authenticator will use the MSK to derive the Temporal Session Key (TSK). Once the TSKs are derived normal data communication can commence.

B. EAP-CRA Re-authentication:

In the previous section we described a roaming-enabled authentication mechanism for users who wish to get connected to a new network, using the security credentials they use in their home network. Although we anticipate relatively faster CRA authentication, in situations where the user continues to work on a foreign network the need for re-authentication is anticipated.

This section will explain the re-authentication process that can occur due to handover within the same network, i.e. when a user moves from one access point to another. The Enhanced CRA full authentication generates CRA-MSK and CRA-EMSK for a secure communication. Possession of these keys by the supplicant and the FAS can quicken the process of re-authentication. The FAS, after the successful authentication of a supplicant distributes the re-authentication identity and the CRA_Counter to the peer. The counter determines the number of re-authentications which can be acceptable.

The process of re-authentication will be initiated by the authenticator with EAP-Request for supplicant ID. In response the supplicant will check the time since last logon to verify the validity of CRA-MSK. In case the key is expired, a valid peer will fall back to request a full EAP-CRA authentication. On the other hand, the supplicant sends its re-authentication ID and realm inside Kname-NAI, a random sequence number with a hashed value of the message. The key for the hash can be generated from the CRA-EMSK and sequence number. Here, the need for the sequence number arises to provide immunity against replay attacks. The authenticator will then forward the EAP-Response encapsulated as a RADIUS packet to the FAS (message 3 Figure 2).

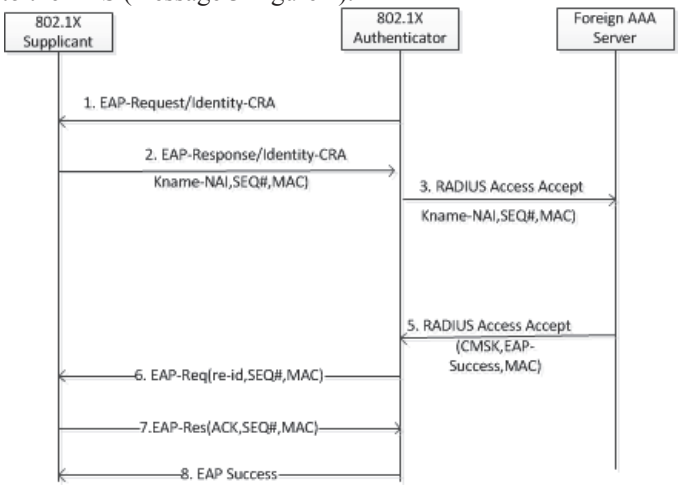

Fig. 2. EAP-CRA Re-authentication

Upon receiving the message the FAS checks the Kname-NAI with its stored authentication information. If there is a match, the server generates the hash value to verify the validity of the message and update the CRA_counter and CRA_timer values. The FAS will then send MSK, MAC, SEQ number to the authenticator. The authenticator retains the MSK and sends the rest to the peer. In the final step, the peer sends an EAP-

Response as an acknowledgment. At this point the client is able to calculate the keying material, however to start secure communication the peer waits until it received the EAP-success from the authenticator.

Two sequence numbers, one with HAS and other with FAS are maintained for replay protection of EAP-CRA messages. The sequence number maintained by the supplicant and HAS is initialized to zero on generation of EMSK. The server sets the expected sequence number to the received sequence number plus one on every successful Re-authentication request, i.e. on generation of DSRK. Similarly, the supplicant and the FAS maintain a sequence number with the generation of rMSK while the supplicant is in the FAS's domain.

IV EVALUATION

To substantiate the effectiveness our proposed protocol we first examine the key security features of Enhanced CRA and then compare the cost involved in communication and computing between Enhanced EAP-CRA and its close competitor EAP-ERP.

A. Security Consideration

RFC-3748 [17] indicates mandatory properties and security constraints of an EAP method. These features can be used as a reference to analyze our proposed protocol in compliance with the EAP frame work. In this section we present our analysis of our protocol against this criterion.

Replay attacks:

Generally replay attacks are initiated by re-using captured PDUs. The captured PDUs have authentic ingredients and can be replayed influencing legitimate nodes to respond. The CRA responds to this threat by the use of sequence numbers that enables both the sender and the receiver to have a record of the received datagram. If a packet is out of order it can be dropped. In case of re-authentication the sequence number is generated by the peer. For the rest of the session the peer and the foreign server will increment the value of this sequence number. In the process of full authentication the peer and HAS can benefit from the same procedure to protect against reply attacks.

Man In The Middle (MitM) attacks:

In this category of attacks a rogue node introduces itself as a legitimate member in the communication. If there is no security mechanism in place the malicious node can continue to remain in between two legitimate nodes and subsequently masquerade as a legitimate node. During the EAP-CRA re-authentication process, MitM attacks are shunned with a Message Authentication Code (MAC). The MAC is simply a hash of the entire message that is attached to the original message. In this situation an attacker needs to have the knowledge of the hash key to revise the message and to re-calculate the hash. In case of full authentication, the use PKI certificate provides immunization against modification of messages.

Hiding User identification:

The proposed method uses KeyName value as user's id during the full CRA process. This prevents from the real identity being revealed to an outsider. During the full authentication process, just before the EAP-Success message the FAS pass a re-authentication ID to the Peer in a secured message. Therefore when the peer requests for re-authentication there is a new random identifier for the peer.

Mutual Authentication:

EAP-ERP may satisfy the condition of mutual authentication between Home server and the supplicant, but it is lacking of bilateral proof of identity between the supplicant and a foreign server. More importantly it relies on the security of RADIUS for server-to-server authentication. In contrast, EAP-CRA reaps the advantages of PKI to satisfy this need during the full authentication process.

As both EAP-CRA and EAP-ERP extend the scope of authentication process, the mutual authentication issue can be explored in three areas; between peer and home server, peer and foreign server, and the foreign and home servers. During full EAP-CRA authentication, the proof of possession of MSK (or a key generated from MSK) from the prior EAP authentication process validates the mutual identity between the peer and the home server. The mutual identity between the peer and the foreign server is realized by the foreign server generating a MAC from a key derived from the EMSK which both the foreign server and the peer are in possession. In return the peer also calculates a MAC value to place it inside the final message. This same model is valid for re-authentication phase as well.

Mutual authentication between servers is realized by each server using its private key to encrypt their hostnames. In this view, both servers sign the MSKname to authenticate each other.

B. Cost Consideration

In this section we compare the cost of communication and computation between Enhanced EAP-CRA and EAP-ERP. It should be noted that EAP-ERP performs a full authentication with the home server every time it enters a foreign network. For this purpose we use EAP-TLS as the home authentication method.

EAP-CRA exchanges eight messages between the supplicant and the servers during full authentication. It also utilizes seven messages during the re-authentication process. In the case of ERP, a minimum of sixteen messages are exchanged between the supplicant and the servers. This is made up of seven messages that are specific to ERP and at least nine messages from EAP-TLS, since we consider EAP-TLS as the home authentication method. For simplicity we are considering the size of the messages during these exchanges. Table 1 lists the number of messages used in each authentication methods.

Table1: Communication Cost.

Authentication Method	No. of Messages
CRA Full Authentication	7
CRA Re Authentication	8
ERP Initial	16
ERP Re Authentication	5

When entering a foreign network, a station that uses EAP-ERP performs a full authentication with its home server. This

process will be very time consuming due to the fact that all message exchanges should take place over the internet. This is a significant weakness of EAP-ERP compared to EAP-CRA for two reasons; 1) the number of messages and 2) the size of the messages. With regards to re-authentication, ERP re-authentication should take place much quicker as it uses only five messages. However, the actual time differences must be determined after the real setup of both protocols.

Table 2: Computational Cost

	CRA Full-auth	**CRA Re-auth**	**ERP Initial**	**EAP Re-auth**
Peer	Hash(2) Encrypt(1) Decrypt(1)	Hash(2) Encrypt(0) Decrypt(0)	Hash(0) Encrypt(0) Decrypt(0)	Hash(2) Encrypt(0) Decrypt(0)
FAS	Hash(2) Encrypt(1) Decrypt(1)	Hash(2) Encrypt(0) Decrypt(0)	Hash(0) Encrypt(0) Decrypt(0)	Hash(2) Encrypt(0) Decrypt(0)
HAS	Hash(0) Encrypt(2) Decrypt(2)	Hash(0) Encrypt(0) Decrypt(0)	Hash(0) Encrypt(0) Decrypt(0)	Hash(0) Encrypt(0) Decrypt(0)

To evaluate the computational cost of the protocols we investigate the number of Hashing, Encryption and Decryption operations performed. Table 2 presents these values for EAP-CRA and EAP-ERP. In case of EAP-CRA full authentication there are four hashing operations and eight encryption operations. Initial EAP-ERP does not involve any encryption or decryption but it should be noticed that there will be at least 16 message exchanged while there are just 8 messages for full EAP-CRA authentication. Moreover the encryption involved in the process will ensure the security of the supplicant while it is roaming to a foreign network. In case of Re-authentication, cost of both protocols will be very similar as they both will perform four hash operations.

From the above comparisons we can say that EAP-ERP has high communication costs and Enhanced EAP-CRA has high computing costs. Therefore, we are expecting reasonable performance for Enhanced EAP-CRA due to the fact that communication overheads are normally more costly compared to the computational overheads.

V CONCLUSION

The influence of wireless hand held devices in the "post-PC" era demands persistent connectivity to the Internet for a number of good reasons. The hand held devices, as they roam from one wireless network to the other should be capable of both legitimately associating and uninterruptedly connecting to the new network. In this paper we have presented an improved version of the CRA protocol that can facilitate the association of a hand held device in a foreign wireless network. This is made possible with the credentials that it uses in its home wireless network and therefore does not warrant to acquire a new set of credentials in the foreign network. The smooth operation of the proposed protocol is sustained by the reliability and maturity of PKI certificates.

At its conceptual level the proposed protocol appears to be promising and reasonable. As the next step we intend to carry out a detailed security analysis. The success of the security analysis will guide us through to implementation.

REFERENCES

[1] IEEE Std. 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999.

[2] IEEE Std. 802.16-2004, IEEE Standard for Local and metropolitan area networks: Part 19: Air Interface for Fixed broadband wireless access systems.

[3] A. Ghosh, R. Ratasuk, B. Mondal, B. N. Mangalvedhe and N. T. Thomas "LTE-advanced: next-generation wireless broadband technology", in *IEEE Wireless Communications*, Vol. 17 , Issue 3, pp 10 - 12, Aug. 2010.

[4] C. He and J. C. Mitchell, "Security Analysis and Improvements for IEEE 802.11i", in *Proceedings of the 12th Annual Network and Distributed System Security Symposium*, NDSS 2005, pp. 90-110.

[5] A Perrig, J Stankovic, and D Wagner, "Security in wireless sensor networks", Wireless Personal Communications, vol 37, no 3-4, 2006.

[6] IEEE Standard 802.11i Part 11, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 6: Wireless Medium Access Control (MAC) Security Enhancements," July 2004.

[7] M. Lynn and R. Baird. Advanced 802.11 attack, Black Hat Briefings, July 2002.

[8] N. Asokan, V. Niemi, and K. Nyberg. Man-in-the-Middle in tunneled authentication protocols. Technical Report 2002/163, IACR ePrint archive, United Kingdom, Cotober 2002.

[9] IEEE Std 802.1X-2001, "Local and Metropolitan Area Networks – Port-Based Network Access Control", June 2001.

[10] A.P. Iyer, and J. Iyer. "Handling mobility across WiFi and WiMAX", in *Proceedings of the 2009 international Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, IWCMC 2009, pp. 537-541.

[11] S. Machiraju, H. Chen, and J. Bolot. "Distributed authentication for low-cost wireless networks", in *Proceedings of the 9th Workshop on Mobile Computing Systems and Applications*, HotMobile 2008, pp. 55-59.

[12] H. Almus, E. Brose and K. Rebensburg, "A Kerberos-based EAP method for re-authentication with integrated support for fast handover and IP mobility in wireless LANs", in *Proceedings of the 2nd international conference on communications and electronics,* ICCE 2008, pp 61–66.

[13] Y.L. Huang, P.H. Lu, J.D. Tygar and A.D. Joseph, "OSNP: Secure Wireless Authentication Protocol using one-time key", in *Proceedings of Computer and Security* 2009, pp. 803-815.

[14] V. Narayanan and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)," RFC 5296, Internet Eng. Task Force, 2008.

[15] J. Salowey, L. Dondeti, V. Narayanan and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)," RFC 5295, Internet Eng. Task Force, 2008.

[16] E. Sithirasenan, S. Kumar, K. Ramezani, and V. Muthukkumarasamy. "An EAP Framework For Unified Authentication in Wireless Networks". In TrustCom'11: *Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pages 92-99, Nov. 2011.

[17] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)," RFC 3748, Internet Eng. Task Force, 2004.

[18] Stanke, M., & Sikic, M. (2008). *Comparison of the RADIUS and Diameter protocols.* Paper presented at the Information Technology Interfaces, 2008. ITI 2008. 30th International Conference.

[19] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol," http://tools.ietf.org /wg/pppext/draft-ietf-pppext-eaptls/draftietf-pppext-eaptls-06.txt, August 1999.