

# An EAP Framework for Unified Authentication in Wireless Networks

Elankayer Sithirasenan

School of ICT

Griffith University

Gold Coast, Australia

+61 (0)7 5552 8252

e.sithirasenan@griffith.edu.au

Saurabh Kumar

School of ICT

Griffith University

Gold Coast, Australia

+61 (0)4 0551 0063

Saurabhkumar@live.com

Khosrow Ramezani

School of ICT

Griffith University

Gold Coast, Australia

+61 (0)4 4848 8600

kramzy@kbttek.com.au

V. Muthukumarasamy

School of ICT

Griffith University

Gold Coast, Australia

+61 (0)7 5552 8256

v.muthu@griffith.edu.au

**Abstract**—Rapid convergence of heterogeneous wireless communication technologies such as Wireless Local Area Networks (WLAN), Worldwide Interoperability for Microwave Access (WiMAX), Long Term Evolution (LTE) etc., attract new opportunities for collaborative usage. More and more applications are emerging to benefit from their advantages. However, with the range of approaches that are used to authenticate the wireless devices in such heterogeneous environments, users are skeptical and looking for more user friendly, flexible and reliable ways to interconnect and utilize these different classes of wireless networks. Wireless network users access the different types of wireless networks either independently or cooperatively. In either case, adequate security provision is critical for the successful operation of the networks. Moreover, emerging technologies should provide seamless transition / migration between these networks. Hence the ability to use a single but unique set of credentials to authenticate the wireless devices in heterogeneous wireless network environments would be an anticipated desire of most users. In this paper a number of authentication mechanisms are examined and evaluated for their advantages and limitations. We then propose a unified authentication protocol that can be encapsulated within the RADIUS protocol utilizing the advantages of public key infrastructure. The preliminary experimental results demonstrate that the proposed protocol is feasible and relatively fast.

*Keywords*— *Wireless Networks, Authentication, Access Control, Heterogeneous Networks.*

## I Introduction

Convergence of heterogeneous wireless networks has its own advantages and challenges. One type of network that is suitable for a particular application may not be appropriate for another type of application. A security mechanism that is effective in one environment may not be effective in the other. Also, there can be situations, where different types of networks coexist in one geographical area. However, due to the inherent nature of the radio 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 LTE [1], a WLAN [2] or a WiMAX [3], all wireless devices 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. For example, if no authentication mechanisms are implemented an adversary could establish two separate connections to the supplicant and the authenticator to construct a Man-in-the-Middle (MitM) attack as reported in [7]. Furthermore, if mutual authentication mechanism is not appropriately implemented an adversary will be able to launch a MitM attack and learn the Primary Master Key (PMK) as illustrated in [8].

Notwithstanding the configuration issues, RSNA is the most preferred first time association method for wireless networks. The use of IEEE 802.1x [9] port based access control 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 with different wireless networks. Hence, a wireless device will have to repeatedly authenticate itself as it traverses from one network to another operator's network, be it the same type of network or different. 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.

The next section briefly describes the RSNA process and provides an overview of the different approaches to coordinated authentication. Section III illustrates our proposed model and Section IV provides details of our proposed protocol. In Section V we discuss the proposed extension to the RADIUS protocol. Details of the experimental setup and the results are given in Section VI. Discussion on the results is given in Section VII and Section VIII concludes the paper.

## II Authentication and Authorization

Authentication and authorization is especially significant in wireless networks as opposed to wired networks. In wired networks clients are strongly associated with a network switch by the physical link. Lack of this physical link in the wireless networks makes it vulnerable to various security threats and hence fails to win the confidence of the wireless clients. In the following section we describe the most popular first time association techniques that are used to secure wireless networks.

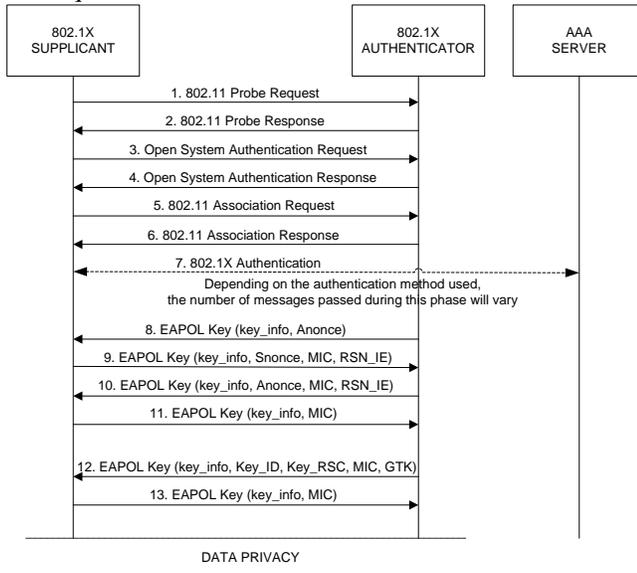


Fig. 1. RSN Association

RSNA is a three phased association mechanism that can be used to mutually authenticate wireless devices and to generate the data encryption keys for secure communication. Figure 1 shows the three phases of the RSNA, the discovery phase (messages 1 to 6), the authentication phase (number of messages depends on the type of authentication used) and the key distribution phase (messages 8 to 13). During the discovery phase, both the supplicant and the authenticator will agree on a common set of security parameters. In the authentication phase, the supplicant and the Authentication, Authorization and Accounting (AAA) server will mutually authenticate each other. If this mutual authentication is successfully completed, they both will generate a master key called the Master Session Key (MSK). The AAA server will eventually pass the MSK to the authenticator. The third phase of RSNA is the key distribution phase (Message 8 to 11). During this phase, Temporary Session keys (TSK), and the data encryption keys are generated using the MSK. Once the TSK is established the Group Keys are generated and distributed for broadcast messages.

During the authentication phase of the RSNA, a number of authentication mechanisms can be used. However, the most reliable and popular mechanisms are the EAP-TTLS

[10] and the EAP-TLS [11]. Out of the two schemes, EAP-TLS offers high level of security; however, a decrease in efficiency is noted due to the high computational needs. It is also the most inefficient and costly of all of the EAP methods because of its requirement for both the client and the server side CA-signed PKI certificate [12]. In contrast, EAP-TTLS offers very good security facilitating a tunneled connection between the client and the server. The client can, but not necessarily need to be authenticated via a CA-signed PKI certificate. This immensely simplifies the setup procedure as a certificate is not needed to be installed on every client. The server can securely be authenticated to the client via its CA-signed certificate and both the client and the server can establish a secure connection (“tunnel”). The server can then use this established connection to authenticate the client. It can use an existing and widely deployed authentication protocol and infrastructure, incorporating legacy password mechanisms and authentication databases such as Active Directory, NT Domains, LDAP, SQL etc., while the secure tunnel provides protection from eavesdropping and man-in-the-middle attack [13].

RSNA does not provide options for coordinated authentication in a heterogeneous network environment. The authentication of users in inter-domain environments will be a key issue to be addressed as the use of wireless devices in mobile context increases [13]. The following section provides a survey of the responses to the distributed authentication mechanism.

### A. Authentication Approaches

Iyer et al. [14] assert that Wi-Fi 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 (WISP). Further, they propose a technique with a common Wi-Fi/WiMAX mobility service agent for use across Wi-Fi and WiMAX access. By incorporating an acceptable mapping mechanism between Wi-Fi and WiMAX, they interface a Wi-Fi Access Point with the WiMAX Access Service Network (ASN) gateway. The mapping function inside Wi-Fi access point maps all 802.11 events to the R6 events. For example the event association request will be mapped to WIMAX pre-attachment request.

In their architecture the problem of handling mobility across Wi-Fi and WiMAX comes down to the problem of handling mobility across WiMAX base stations that already have concrete solutions. Also, the mapping function consumes 1.82 seconds for EAP-TLS authentication in comparison to few milliseconds as shown in section VI. Further, their proposed architecture enables the same IP address to be used across both the Wi-Fi and the WiMAX network interfaces, and keeps it seamless from an application perspective.

Distributed authentication scheme proposed by Machiraju et al. [15] relies on Base Stations (BS) to collectively store authentication information. To achieve the goal of single point of access they introduce the notion of tokens. However, the paper does not clarify how the base stations will initiate contact with each other. The security approach to establish a secure connection between BSs is not determined. Moreover the details to establish trust between base stations and actions taken in case of base stations being compromised are not provided. The capabilities required to perform the expected functionality of a BS are not addressed. Furthermore, the paper falls short to provide enough details for elimination of traditional backend authentication servers.

The EAP-FAMOS authentication method developed by Almus et al. [16] use the Kerberos based authentication in the existing EAP framework. It allows secure and true session mobility and requires the use of another EAP method, only for the initial authentication. It uses the keying material delivered by the other EAP method during the initial authentication for its Kerberos-based solution for fast re-authentication. Mobility is based on Mobile IPv4 and a sophisticated handover supported by a so-called Residential Gateway together with a Mobility Broker located in the ISP's backend network. Their performance studies show that Wi-Fi technology can be used in mobile scenarios where moving objects are limited to speeds below 15kmh. Further, they state that applications requiring very low delay and allowing only very short service interruptions can be supported by their technique.

Apart from the high administration required in Kerberos based methods, their solution is mainly targeted at specific wireless networks and authentication mechanisms. Wireless service providers use different authentication schemes on their diverse types of wireless networks. For example, a WiMAX service provider may use the EAP-TLS authentication scheme on their custom AAA server, whereas corporate entities may want to use EAP-TTLS authentication mechanism facilitating the use of their authentication databases such as Active Directory, LDAP, and SQL. Hence, considering the convergence of networks it is significant to develop an authentication mechanism that is versatile and simple so that it can be effectively used under any type of network.

Another practical approach is edu-roaming which has been designed and implemented by European educational institutes. This service allows users to secure internet access in participating academic institutions when they roam between the member institutions. To authenticate a user education roaming uses a series of hierarchical authentication servers. The authentication servers are all RADIUS based servers and each institution has its own RADIUS server which is connected to the federation level RADIUS server. The Federation level authentication servers are connected to the global level RADIUS server. When a user enters a foreign network the RADIUS server of the

foreign network checks the user credentials and then if the user does not belong to the local network then requests the federation level RADIUS server, which includes a directory of all RADIUS servers under its control and also has connection to the ROOT RADIUS server. If the federation level server cannot find the Home RADIUS server for supplicant then it will forward the authentication request to the Root RADIUS server. The Root RADIUS server will then forward request to the appropriate federation level RADIUS server and consequently redirects the request to the Home authentication server. The response to the authentication request assumes the same route in the opposite direction from Home RADIUS server to the Foreign RADIUS server [17].

Narayanan et al. proposed an EAP extension to the EAP framework and the EAP key hierarchy to provide support for Re-authentication [18]. As described in the section II, MSK is generated on the successful completion of the authentication phase (phase 2). Subsequently MSK is passed to the authenticator for the generation of TSK, phase 3 of RSNA. The TSK is used further for data encryption between the supplicant and the authenticator. However the EAP framework suggests two keys to be derived by all EAP methods: the Master Session Key (MSK) and the Extended MSK (EMSK) which forms the EAP key hierarchy [19]. Narayanan et al. makes use of the EMSK for re authentication and successive key derivations, as mentioned in [20].

ERP defines two new EAP messages, EAP-Initiate and EAP-Finish to facilitate Re-authentication in a single round trip messages. At the time of the initial EAP exchange, the peer and the server derive an EMSK along with MSK. EMSK is used to derive a re-authentication Root Key (rRK). 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) from the rRK is derived. rMSK is treated similar to MSK obtained during normal EAP authentication i.e. to generate TSK.

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. To demonstrate the possession, supplicant uses rIK to compute the integrity checksum over the EAP-Initiate message. The algorithm used to compute integrity checksum is selected by the peer and on occasion of server's policy not allowing the use of cipher suite selected by the peer; the server sends a list of acceptable cipher suites in the EAP-Finish/Re-auth message. In this case the peer has to re-start the ERP process by sending the EAP-Initiate message and the integrity checksum using the acceptable cipher suites.

Furthermore ERP also recommends use of IPsec or TLS to protect the keying materials in transit.

### III Proposed Technique

The principal notion behind our proposed 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 and the AAA server in a foreign network is called as the FOREIGN AAA Server. Hence, as for our proposal, a wireless device will require only one set of credentials that it uses to access the home network to access any type of foreign networks. We are considering both different types networks and different authentication mechanisms that may be specific and effective to that type of network. We have proposed and developed an efficient mechanism to utilize the credentials in a heterogeneous network environment.

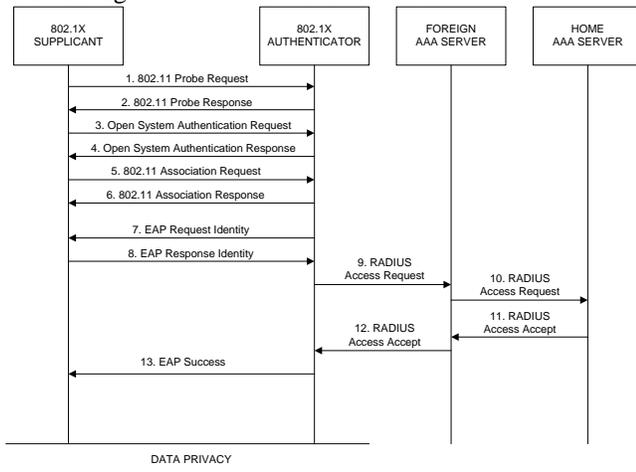


Fig. 2. Coordinated authentication message exchange

Therefore, in our perception a wireless device will deal with one HOME network and a number of FOREIGN networks. We also assume that the security mechanism used in the HOME network is the most effective that can be adapted to the type of wireless devices using the network. Further, it is assumed that the HOME AAA server will have pre-arranged agreements with the FOREIGN AAA servers for secure communications by other means such as IPsec, SSL etc.

Figure 2 outlines the messages exchanged in our proposed method. In order to facilitate this authentication mechanism we introduce a new EAP authentication protocol called the EAP-CRA (Coordinated Robust Authentication). As in the RSNA, the EAP-CRA also includes a discovery

phase that comprises of the six 802.11 open system association messages. During this phase a wireless device that is in the FOREIGN network will advertise that it is capable of EAP-CRA together with other allowed EAP methods. Hence, an authenticator in the FOREIGN network can initiate EAP-CRA if it is capable of managing it. Once they both agree on the CRA authentication mechanism, the authenticator can initiate the EAP-CRA authentication by sending the EAP Request / Identity message to the supplicant (message 7 in Figure 2). The supplicant in return will reply with the EAP Response / Identity message (message 8). The Response / Identity message is passed to the FOREIGN AAA server as a RADIUS Access Request message. At this stage unlike in the other EAP authentication methods the AAA server will pass the Access Request message to the relevant HOME AAA server for validation. If the HOME AAA server successfully validates the Identity information sent by the wireless device, it then responds with an Access Accept message with the necessary keying material to the FOREIGN AAA server. The keying material, in-turn, is passed to the authenticator with the RADIUS Access Accept message. The authenticator can then use the keying material to initiate the 4-way handshake process to generate the TSK. Further details of the CRA protocol are explained in the next section.

### IV Proposed CRA Protocol

With regard to mutual authentication EAP-CRA proposes using RADIUS servers as suggested in IEEE 802.1x [19]. RADIUS protocol exhibits better performance compared to other mutual authentication protocols [21]. EAP-CRA proposes 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 then they can use their CA-signed PKI certificates to ascertain trust between servers.

All AAA servers that participate in the EAP-CRA must have some pre-arranged agreement for secure communication. Assuming that all AAA Servers that participate in the EAP-CRA are in possession of their CA-signed PKI certificates, the CRA protocol, in this instance relies on the CA-signed PKI certificates to communicate between the FOREIGN and the HOME AAA servers.

However, other options for secure communications such as a virtual private network (VPN) or SSL can also be explored. In the protocol details shown in Figure 3, we can use the already available CA-signed PKI certificates of the FOREIGN and the HOME AAA servers for secure communication. Message 3 can be encrypted using the private key of the FOREIGN AAA server ( $E_{KP_F}[HostName, E_{KU_H}[EMSKname, SeqNo.]]$ ) and message 4 can be encrypted using the public key of the FOREIGN AAA server ( $E_{KU_F}[DSRK]$ ). However, in Figure 3, we have left the issue of secure communication

between the FOREIGN and the HOME AAA server open, to confirm that other options are possible.

According to our proposed EAP-CRA protocol, in response to the EAP-CRA Request Identity message (message 1 in Figure 3), the supplicant sends an EAP Response message with its *Identity* (EMSKname and Sequence number) encrypted with the public key of the HOME AAA server (message 2 in Figure 3) along with the unencrypted host name of the HOME AAA server. EMSKname is used to identify the corresponding EMSK and Sequence Number for Replay protection by the Home AAA server. The authenticator, having received the encrypted *Identity* will pass it to the FOREIGN AAA server as it is. The FOREIGN AAA server uses the fully qualified *Host Name* provided in EAP-CRA Response message to determine the Home AAA server. The FOREIGN AAA server will append its *Domain name* to the received message (EAP-CRA Response) and pass it to the HOME AAA server using the secure method described above (message 3).

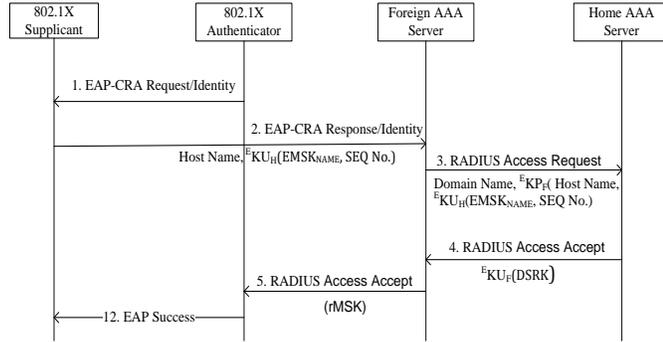


Fig. 3. Coordinated Robust Authentication (CRA) Protocol.

The HOME AAA server will then have to do a double decryption to find the identity of the HOME wireless device. If the wireless device is positively identified, the HOME AAA server calculates *DSRK* (Domain Specific Re-authentication key). *DSRK* is calculated using *Domain Name* as an optional data in the key derivation specified in [20]. HOME AAA server will then send the *DSRK* to the FOREIGN AAA server after encrypting the message using the public key of the FOREIGN AAA server (message 4). The process is illustrated in Figure 4. The FOREIGN AAA server can use its private key to decrypt the received message to discover the *DSRK* and generate *rMSK* (Re-authentication Master Session Key). *rMSK* is calculated using a sequence number as an optional data specified in [18]. The *rMSK* can then be transferred to the authenticator with the RADIUS Access Accept message (message 5). Finally the authenticator sends the EAP success message to the wireless device indicating the completion of the CRA authentication and the beginning of the key distribution phase.

Two sequence numbers, one with HOME AAA server and one with FOREIGN AAA server is maintained for replay protection of EAP-CRA messages. The sequence

number maintained by the supplicant and HOME AAA server is initialized to zero on the 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 FOREIGN AAA server maintain a sequence number with the generation of *rMSK* until the supplicant is in the FOREIGN AAA server's domain.

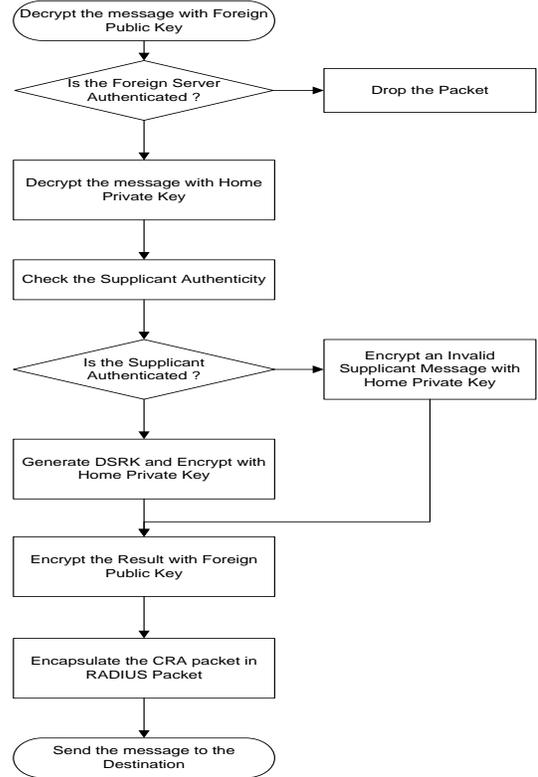


Fig. 4. EAP-CRA on Home Server

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 *TSK*. Once the Temporary Session keys (*TSK*) are derived normal data communication can commence. In the next section we discuss the server side communication of our proposed authentication mechanism.

## V Proposed Extensions to RADIUS

EAP-CRA uses RADIUS as the transportation protocol between the Home and Foreign servers. However the RADIUS protocol is a client-server protocol. The RADIUS server, when forwarding the authentication packet to another RADIUS server, designates the sender as client. Hence, the foreign server's only responsibility is to fulfill the role of a proxy server and to forward the RADIUS packets to the Home server. In the proposed protocol, EAP-CRA takes advantage of RADIUS communication and

encapsulates the EAP-CRA messages inside the RADIUS packets. There are two viable approaches to designing the security methods that were discussed in the previous section.

The first approach is to implement the security features inside the attribute field of the RADIUS packet (Figure 5). The attribute field of each RADIUS Packet includes at least three fields that enable the RADIUS packet to carry EAP messages or other information for Dial in user. The attribute field can be used to encapsulate EAP-CRA messages inside the RADIUS packet. Extensions to RADIUS protocol so far proposed have been for the purpose of modifying or creating new attributes such as EAP or apple extensions for RADIUS, each of which has particular attributes.

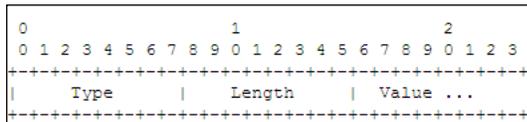


Fig. 5. Attributes in a RADIUS packet

Type 79 is for EAP messages and 92-191 are Unused. If the value is string or text type then the length can be from 1 to 253 octets. Therefore the type value can be between 92 to 191 octets for the EAP method. The type of the value will be string and as with other EAP methods data is encapsulated inside the RADIUS packet. The foreign server can encapsulate the encrypted message inside the RADIUS packet, so that the home server must first decrypt the message and then respond by a proper RADIUS message to the foreign server.

The second approach is to use a dependent VPN over a SSL connection between the two servers prior to RADIUS communication. The RADIUS packets can then be sent in a secure channel. This research did not investigate this method because it entails extra network administration. It also creates a connection delay prior to the EAP-CRA message transmission. The second reason preventing the separate link investigation is that the use of PKI actually provides a more secure channel by which the EAP-CRA message can be sent and received.

### A. EAP-CRA Message and Process details

The proposed EAP-CRA packet is depicted in Figure 6. The explanations for each field are given in the next paragraphs. The reasons for designing each of the fields are illustrated based on the associated requirements. The fields are transmitted from left to right.

The first influencing factor of EAP-CRA is that it is based on the EAP protocol. Therefore, the fields, code, identifier and length are inherited from an EAP structure. The explanation of each field is listed below.

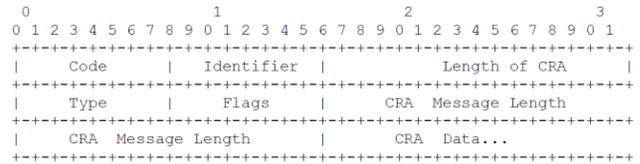


Fig. 6. Proposed CRA packet

The Code field is one octet and identifies the type of EAP packet. EAP Codes are assigned as 1 for Request, 2 for Response, 3 for Success and 4 for Failure. The Identifier field is one octet and aids in matching responses with requests. The Length field is two octets and indicates the length of the EAP packet including the Code, Identifier, Length and Data fields. Octets outside the range of the Length field should be treated as Data Link Layer padding and should be ignored on reception. The Flags field includes the following fields:



L = Length included  
S = EAP-CRA start  
T = Source Type

M = More fragments  
R = Reserved,

### B. Two Kinds of RADIUS Packets in EAP-CRA

In EAP-CRA, RADIUS packets are divided into two categories, based on their content. The first category includes those messages sent from an access point to the foreign server and the second type is those exchanged between a Home and Foreign server. In the first scenario, the supplicant encrypts the EAP-CRA message using the Home server public key and sends it to the foreign server. Between the home server and the client, the authenticator encapsulates the message inside a RADIUS packet and sends it to the foreign server. On the other hand, when the two servers are in communication with each other they sign the EAP-CRA message first using their own private key and then by encrypting the message using the other server's public key. Therefore, the content of the RADIUS packets differ depending on whether they are received from an authenticator or from an authentication server. The field T in the fragmentation field is for source type of the packet. If the packet is from or is sent to an authenticator then the value will be set to 0. Otherwise, if the source is a server, then the value will be set to 1.

### Retry behavior

It is possible during peer communication that a response will not occur within the expected time. In which case, there must be a way to specify how many messages will be sent to make sure that another peer is not present. The time to resend the message is another parameter which

needs to be determined. The exact number for the time and trials will be decided in the actual implementation and depends on the protocol process time, line traffic and other unforeseen factors. One of the issues present in retry is the duplicate packets which must be handled by the receiving peer. Three retries will be performed, forming the base configuration for the EAP-CRA.

### Fragmentation

EAP-CRA message may span multiple EAP-packets due to the multiple public and private key encryptions; hence there must be a method, to be engineered in the servers, for handling the fragmentation. As a base for work on the fragmentation, the length of the TLS record can be up to 16384 octets, while the TLS message may be 16 MB if it carries the PKI certificate of a server. However, to protect against denial of service attacks and reassembly lockup there must be maximum size set for the group of the fragmented messages. An example can be seen in what was implemented for EAP-TLS[11]. The exact numbers will be determined during implementation of the protocol, and will reveal the average length of long EAP-CRA messages. For the purposes of initial configuration, this number can be borrowed from EAP-TLS which is 64 KB.

Since EAP is an uncomplicated ACK-NAK protocol, fragmentation support can be provided according to a relatively simple process. Damage or loss of fragments during transit is an inevitable risk for any communication. In EAP, these fragments will be retransmitted, and because sequencing information is included in EAP's identifier field, a fragment offset field like that of IPv4 is not necessary.

EAP-CRA fragmentation support will be provided by adding flag fields to the EAP-CRA packets inside the EAP-Response and EAP-Request. Flags include the Length (L), More fragments (M), and Start (S) bits. The L flag indicates the presence of the four octet Message Length field. It *must* be set in the first piece of a fragmented EAP-CRA message or set of messages. The M flag will be set in all except the last fragment showing that there are more frames to follow. The S flag will only be for the EAP-CRA start message sent from the EAP server to the peer. The T flag refers to the source type of the EAP-CRA message; whether it is coming from an 802.1x authenticator or from an authentication server. If there is a fragmented message, both server and the other peer must acknowledge the receipt of a packet with the flag set to M. The response can be an empty message to the other peer showing that the message has not been received.

## VI Experiments and Results

For our experiments we setup three different scenarios to compare the time taken to authenticate a user. Edu-roaming, EAP-CRA and direct authentication with a single RADIUS authentication server were considered. RADIUS servers were installed on Windows 2003 Server standard

edition and all platforms had 2 GB RAM and 2GHz dual core CPU.

Microsoft Internet Authentication Service (IAS) with Microsoft EAP-PEAP was used in these experiments. IAS is the Microsoft implementation of a Remote Authentication Dial-In User Service (RADIUS) server and proxy in Windows Server 2003. As a RADIUS server, IAS performs centralized connection authentication, authorization and accounting for many types of network access including wireless and VPN connections. As a proxy, the IAS forwards authentication and accounting messages to other RADIUS servers.

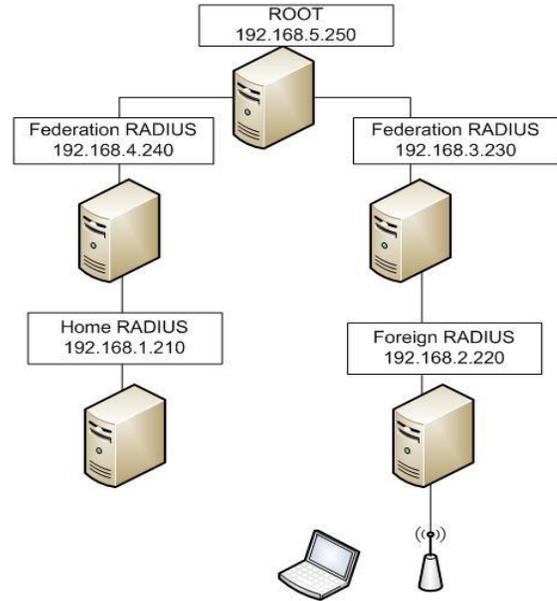


Fig. 7. Experimental Edu-roam Setup on LAN

To start with fair baselines both EAP-CRA and Edu-roaming were implemented in LAN but in different IP subnets. Moreover to magnify the delay of authentication for Edu-roaming another setup on Internet was also implemented. The first topology is the Edu-roaming model. Since this is a proprietary model it was implemented on five Microsoft IAS that was installed on the Java virtual box. Because the Edu-roaming has federation level RADIUS servers and one root RADIUS server, we implemented five RADIUS servers in all. Two of the RADIUS servers were for the home and the foreign networks, two as the federation level RADIUS servers and the last one as the Root authentication server. Figure 7 shows the topology for Edu-roaming that was implemented by us.

The second scenario was an implementation of Edu-roaming and EAP-CRA servers on the Internet. Five servers were installed at various remote sites in Brisbane Australia. In all scenarios, the time difference between the first RADIUS request message and the last RADIUS accept message was used for comparing the time taken for authentication.

Tables 1 and 2 lists the average times obtained on the LAN and Internet implementations over forty different trials.

Table 1. Average Authentication Time on LAN

Topology	Edu-roam	EAP-CRA	Direct
Average Time (ms)	259	148	119

Table 2. Average Authentication Time on Internet

Topology	Edu-roam	EAP-CRA
Average Time (ms)	4176	750

According to Table 1 there is a 111 milliseconds time difference in the authentication times between Edu-roaming and the EAP-CRA. As explained earlier the EAP-CRA directly communicates with the foreign RADIUS server. Moreover, the difference in authentication times between the CRA approach and direct authentication with the RADIUS server is 29 milliseconds.

Table 2 shows the authentication times over the Internet. Here, the RADIUS servers are located at different locations and are connected over the Internet. In this case there is a significant difference in authentication times between Edu-roaming and EAP-CRA approaches. The Eduroaming approach is almost three times slower than the EAP-CRA approach in this case.

## VII Discussion

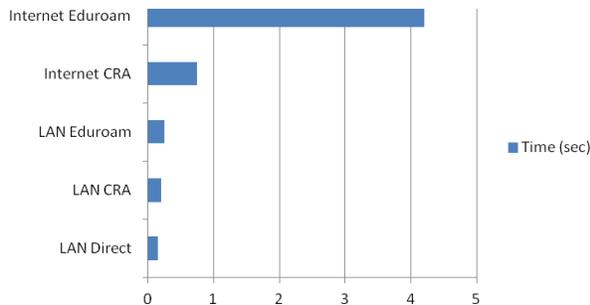


Fig. 8. Comparison of Authentication Times

Figure 8 confirms the viability of the EAP-CRA approach compared to the other methods. The main advantage of the EAP-CRA authentication mechanism is the use of only two messages to authenticate a wireless device in a FOREIGN network. Although the time taken between the FOREIGN AAA server and the HOME AAA server may vary depending on the traffic and/or capacity of the wired network, the use of only two messages in a FOREIGN network makes our authentication mechanism very much reliable compared to other available techniques. Further, even if the foreign network uses a less secure authentication mechanism, it still will not affect the EAP-CRA supplicants since their PMKs are supplied by the

HOME AAA servers notwithstanding the limitations of the foreign network.

Another significant advantage of the EAP-CRA is its reliance on the HOME security credentials to secure its clients in the foreign network. Hence, it can be assured that the EAP-CRA clients will have the same security guarantee as in their home network in the foreign network. Further, in the case of EAP-TLS authentication with CA-signed PKI certificates, clients will need only a single set of certificates signed by the CA accepted by the HOME AAA server. There will be no need for clients to carry a number of different certificates to authenticate with different networks. Hence, in this context, the EAP-CRA facilitates EAP-TLS authentication and makes it more practical and viable.

Although there are many other techniques proposed for distributed authentication, the advantages of the EAP-CRA technique is its simplicity, robustness and versatility. Unlike many other systems that require additional components such as a token management system [15] or a [16] federation of RADIUS servers [17], the EAP-CRA system depends only on the existing infrastructure, hence, assuring simplicity. The use of existing CA-signed PKI certificates without necessitating other authentication mechanisms such as tokens or smart cards enables the EAP-CRA system to be confined. Further, our proposed system is not limited to WLAN or WiMAX, it can be effectively used with any wireless network, harnessing the unique security features of that particular wireless network. Furthermore, the authentication mechanism (EAP-TLS, EAP-TTLS, EAP-PEAP etc.) used by the wireless network does not influence the EAP-CRA system because it does not use any form of mappings between these protocols and the proposed EAP-CRA protocol.

The above discussions illustrate the significance of the CRA approach and emphasize the need for a fast authentication mechanism as opposed to a hierarchical mechanism like the Edu-roam. Although Microsoft IAS provides a similar infrastructure to that of EAP-CRA, it is restricted to only Microsoft EAP-PEAP authentications. In contrast our proposed protocol does not rely on any particular authentication protocol. It is designed to reap the maximum leverage of the authentication mechanism that is best for the particular home environment. Hence, when a hand-held device roams in a foreign network it will have the same security guarantee as in the home network.

EAP-CRA is differentiated by other EAP methods in the aspects of communication scope by covering both the foreign and the home authentication servers. Other EAP methods such as EAP-TLS or EAP-TTLS do not consider server to server communication. The EAP-CRA provides authentication and communication privacy between the foreign and the home authentication servers based on public key infrastructure. The home and foreign servers have got the public certificates of each other. EAP-CRA encrypts the authentication message twice and then sends it to the other foreign server ensuring privacy and authenticity of the

message. Any message from home server will first be signed by the home server's private key and then by the foreign server's public key. Same process happens if the foreign server sends a message to the home server. The signature of a server by the private key authenticates the server to the other server and the public key encryption ensures privacy of the transmitted message.

To implement the transmitting of the messages between two authentication servers EAP-CRA suggests using of RADIUS protocol by creating a new attribute field which encapsulates the EAP-CRA message. The EAP-CRA message is the double encrypted message which will be located in the value field of the RADIUS attribute.

On the negative aspect, the effectiveness of the proposed protocol will depend on the mutual trust established between the participating AAA servers. If the AAA servers do not have any form of prior agreement, it will be up to the discretion of a FOREIGN AAA server whether to accept or deny an EAP-CRA request.

## VIII Conclusions

Securing wireless devices in an efficient way is a real challenge due to the unique characteristics of the wireless communication and the environment that they operate. Therefore, wireless devices use authentication mechanisms that are tailored to meet the specific characteristics and requirements of the wireless network that they operate. Hence, it is expected that a wireless device that roam from one network to another requires the same kind of security guarantee as in its home network. In this regard we have developed and proposed an efficient mechanism that can provide almost the same level of security guarantee both in the home network and in a foreign network. Our mechanism is simple and robust and does not require any additional infrastructure or security arrangements to provide this security guarantee. The results from our preliminary experiments demonstrate that our proposed protocol is fast compared other methods that require additional infrastructure.

In this study we have not considered IP mobility between wireless networks. We have decided to leave it as a secondary requirement since we believe that providing effective security with minimal changes to the existing infrastructure is vital in achieving robust security in a foreign environment. Furthermore, interoperability between wireless and GSM networks is not considered at this stage. As of now our main aim is to facilitate unified authentication between wireless, WiMAX and LTE networks using a single set of credentials.

## REFERENCES

[1] H. Ekstrom et al., "Technical Solutions for the 3G Long-term Evolution", IEEE Communications Magazine, March 2006.  
 [2] IEEE Std. 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999.

[3] IEEE Std. 802.16-2004, IEEE Standard for Local and metropolitan area networks: Part 19: Air Interface for Fixed broadband wireless access systems.  
 [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, October 2002.  
 [9] IEEE Std 802.1X-2001, "Local and Metropolitan Area Networks – Port-Based Network Access Control", June 2001.  
 [10] P. Funk and S. Blake-Wilson. EAP Tunneled TLS Authentication Protocol (EAP-TTLS). <http://tools.ietf.org/wg/ppext/draft-ietf-pppext-eap-ttls/draftietf-pppext-eap-ttls-05.txt>, July 2004.  
 [11] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol," <http://tools.ietf.org/wg/pppext/draft-ietf-pppext-eap-ttls/draftietf-pppext-eap-ttls-06.txt>, August 1999.  
 [12] D.Q. Liu, and M. Coslow, "Extensible authentication protocols for IEEE standards 802.11 and 802.16", in *Proceedings of the international Conference on Mobile Technology, Applications, and Systems*, Mobility 2008, pp. 1-9.  
 [13] R. Dantu, G. Clothier and A. Atri, "EAP methods for wireless networks", *Comput. Stand. Interfaces*, vol. 29, no. 3, pp. 289-301, 2007.  
 [14] 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.  
 [15] 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.  
 [16] H. Almus, E. Brose and K. Rebenburg, "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.  
 [17] M. Milinović, J.Rauschenbach, S.Winter, L. Florio, D.Simonsen, J.Howlett, "eduroam Service Definition and Implementation Plan", GN2-07-327v2,2008  
 [18] V. Narayanan and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)," RFC 5296, Internet Eng. Task Force, 2008.  
 [19] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)," RFC 3748, Internet Eng. Task Force, 2004.  
 [20] 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.  
 [21] 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.