Low-latency Secure Mobile Communications

Vinod Kumar Choyi and Michel Barbeau, *Member, IEEE*

\

***Abstract*— On the one hand, the challenge of meeting various security requirements in the mobile and wireless environment is difficult, compared to the fixed and wired environment, because of the very nature of radio communications. On the other hand, wireless networks such as GSM, PCS and CDMA, which are predominantly circuit-switched voice networks, have been shielded from the vulnerabilities that exist in the Internet. With the introduction of the IP multimedia subsystems (IMS) solutions, data, voice and video will be accessible using UMTS and CDMA2000 networks via the Internet. The current mobile equipment has the capability to work with multiple radio interfaces using heterogeneous radio access networks. Mobile subscribers have also become truly mobile since they are not constrained by mobile equipment, networks and applications. However, information between individuals has to be protected. Therefore, there will exist always the notion of private and public communications. In the mobile and wireless environment, the challenge is private communications between peers over non private domains. This paper describes schemes offering secure communications between mobile nodes using virtual private networking technologies based on IP security (IPSec). In addition, mobility management is done using mobile IP along with route-optimization techniques. This paper also describes how latencies suffered by real-time traffic when traversing IPSec and mobile IP tunnels can be reduced so that real-time delay constraints can be meet.**

***Index Terms*— Mobility, VPN, IPSec, Mobile IP**

I. Introduction

THIS paper addresses the problem of providing IP payload traffic confidentiality to mobile nodes (MNs) belonging to the same domain. The challenge is to provide MNs visiting outside the corporate environment the same level of communications confidentiality and integrity offered by the corporate environment. This paper proposes mechanisms for providing secure and seamless session continuity between MNs when roaming between corporate networks and public networks. Our approach consists of optimizing routes taken by virtual private network (VPN) tunnels and avoiding renegotiation of IP security (IPSec) security associations (SAs) after handoffs.

Vinod Kumar Choyi is a researcher with the Research and Innovation group at Alcatel Canada Inc., Ottawa, ON, Canada K2K 2E6 (phone: (613) 784-1071; email: vinod.choyi@alcatel.com).
Michel Barbeau is a Professor with the School of Computer Science, Carleton University, Ottawa, ON, Canada K1S 5B6 (phone: (613) 520-2600; email: barbeau@scs.carleton.ca).

Avoidance of triangle routing is at the core of our solution. Given two MNs belonging to the same corporate network, i.e. MN1 and MN2, we address the following scenarios:

1. Both MN1 and MN2 are within the corporate network.
2. MN1 is within the corporate network and MN2 is outside the corporate network.
3. Both MN1 and MN2 are outside the corporate network.

Scenario 1 is straightforward. Communications between MNs within the private domain are protected by firewalls, network address translation (NAT) and intrusion detection and prevention mechanisms. Besides, mobility within the corporate network can be supported using mobile IP (MIP). In Scenario 2, secure communications can be provided using an IPSec tunnel between MN1, in the corporate network, to MN2, in the visited network, via a VPN gateway (VPN-GW), while MIP can be used to support mobility. A challenge is to ensure that renegotiation of IPSec SAs is not done each time a network-layer handoff is performed by a MN. This challenge has been addressed in the past (see Section II), but the solutions so far are not optimized in terms of routing. Scenario 3 in itself is not much more complex than Scenario 2, but offering route-optimized and low-latency communications, between MN1 and MN2, are challenging. To the best of our knowledge, past solutions have not been explicitly addressed this scenario.

We propose three different protocol extensions to address Scenarios 2 and 3. The proposed solutions are based on the secure universal mobility (SUM) architecture [10]. In Scenario 2, SUM suffers from a double triangle routing problem. We overcome this problem by integrating an adapted MIP route optimization technique to the SUM architecture. In Scenario 3, we found that mobility and VPN management need to be co-coordinated in order to achieve a certain degree of optimization. Therefore, we combine the VPN-GW and external home agent (HA) roles into a single entity that we call the mobility aware VPN gateway (MAG). This enables the MAG to perform mobility management in conjunction with VPN functions. We have two solutions that exploit the MAG functionality. In the first solution, the MAG is completely involved in the communications between the two MNs. In short, the MAG is involved in the setup and operation of the VPN tunnels and MIP tunnels. In the second solution, which is an optimization of the first, the MAG is only involved in key distribution and tunnel setup. In contrast to the first solution, the user traffic flows through route-optimized paths.

The rest of this paper is organized as follows. Related work is reviewed Section II. The protocol extensions are described in Section III. We conclude with Section IV.

0-7803-9182-9/05/$20.00 ©2005 IEEE.

II. Related Work

The combination of traffic confidentiality and mobility has received attention in the scientific literature. On the one hand, the Internet key exchange (IKE) protocol can be used for negotiating the SAs required by tunnels of VPNs [1]. On the other hand, the MIP can be used to support mobility of IP nodes [2]. When used together, the following issue arises. A SA of a VPN tunnel is bound to two IP addresses, one for each end-point participants to the tunnel. A MN has a dual identity, a permanent home address (HoA) and a temporary care-of address (CoA), as a function of its geographical location. When a MN participates to a VPN tunnel, either the HoA or CoA can be used as MN's identity. If the HoA is used to identify the MN's end-point of the VPN tunnel, then a mechanism is required to redirect the traffic to the current location of the MN. If the CoA is used as the MN's end-point of the VPN tunnel, then a mechanism is required to change or update the SA whenever the CoA is changed. Here is a review of work that addresses the aspects of this problem in one way or another.

Rejeb et al. proposed an extension to IKE to establish SAs over insecure wireless channels [4]. The authors stress the absence of confidentiality of identities and hashes used for authentication. Consequently, SAs over insecure wireless channels are vulnerable to passive dictionary attacks. They guess pre-shared keys using eavesdropped hashes. The authors propose an extension where IKE is modified to provide identity and hashes confidentiality using encryption. Resilience to passive dictionary attacks is claimed. Encryption is achieved using a pre-shared key identified by a user name.

Kivinen drafted an extension to the IKE protocol to address the problem of key establishment in a mobile environment [3]. The protocol provides mechanisms for updating the IP addresses bound to SAs.

Barton et al. introduced wireless link confidentiality for a MN using an integration of MIP with IPSec encryption [5]. Their solution relies on a wireless security gateway (SGW) and HA (SGW/HA), located in the home network, trusted by the MN and integrated with the HA. A MN to SGW/HA IPSec tunnel is established. Traffic from a correspondent node (CN) is sent to the home network, intercepted by the SGW/HA, encrypted using encapsulating security payload (ESP) and tunneled (using MIP tunneling) to the foreign agent (FA). The FA de-capsulates the traffic and forwards the encrypted packets to the MN. Traffic from the MN is encrypted using ESP and destined to the SGW/HA. The SGW/HA decrypts the packets and forwards them to the CN. In this solution, trust of foreign networks is not required. IPSec is required in the MN and SGW/HA. MIP support is required.

Bhagvathula et al. compare the performances of three different approaches to offer VPN services to MNs [6]. The first uses MIP, but does not offer any security or QoS. The second is similar to the first except that IP-in-IP tunneling is replaced by an IPSec tunnel. The third approach uses a multi-protocol label switching (MPLS) based mobile VPN. The results obtained show that the end-to-end packet delay is less for the MPLS-based VPN solution while the voice quality is acceptable for all the three options.

Khatavkar et al. compared the performances (throughput) of MIP combined with different authentication and encryption algorithms used in IPSec [7]. When reverse tunneling is used, the performance is de-graded. The ESP mode combined with DES is the worst performing. They expected a drop of 12 K bps at the most when using MIP in real-time and using ESP when compared to not using IPSec.

As a countermeasure to IP-spoofing, routers block packets with source addresses not belonging to the network of the interface on which they are received. This is termed ingress filtering. It blocks particular packets of MNs visiting foreign networks and using their HoA as a source address. To address this issue, Gupta and Montenegro define the concept of mobile VPN (MVPN) and simple key-management for Internet protocols (SKIP) [8]. Using public-key cryptography, the role of SKIP is to establish shared secret keys used to encrypt and authenticate the traffic. A firewall controls the access to the home network using a list of allowed hosts. Each node allowed to enter the home network from a foreign network has an entry in the list. A MN directs its packets to the home network encapsulating them with an outer header using the CoA, as source address, and the address of the HA, as destination address. The firewall de-capsulates inner headers to recover the HoAs of the MNs. The firewall then performs a lookup for their rights in the access list.

MIP establishes a tunnel between a MN's location and it's HA. There is a difficulty when the HA is behind firewalls, which must be able to insure consistency of tunneled traffic (outer headers and inner headers inspection is required). A MIP aware firewall is proposed by Park et al. [9]. The portion of the MIP tunnel from the firewall to the MN is protected using IPSec tunneling. When a MN changes its location, the old IPSec tunnel is released and a new IPSec is established from the new location to the firewall.

Dutta et al. introduced an architecture termed secure universal mobility (SUM) [10] addressing both confidentiality and mobility. Three distinct areas are defined. The intranet, which is a trusted area guarded by a firewall. The de-militarized zone (DMZ), which is accessible outside the intranet through another firewall with relatively weak filtering rules. The third area is the public Internet. SUM is MIP-based. The MIP protocol is not changed, but it is used differently with respect to its original definition. Each MN has two HoAs, an internal HoA (i-HoA) and an external HoA (x-HoA). The i-HoA serves as identity in the private address space of the intranet. The x-HoA serves as identity in the public address space of the Internet. There are two kinds of HAs, namely, an internal HA (i-HA) and an external HA (x-HA). The i-HA deals with intranet mobility and keeps track of i-CoA to i-HoA bindings. The x-HA deals with external mobility and keeps track of x-CoA to x-HoA bindings. The x-HA is located in the DMZ. There is a VPN gateway (VPN-GW) which bridges the intranet and DMZ. While a MN is in the Internet, confidentiality and integrity of data traffic are provided using an IPSec tunnel. The endpoints of the IPSec tunnel are the

VPN-GW's public address and MN's x-HoA.

A total of three tunnels are established to provide intranet private access to a MN visiting a foreign network. Following the acquisition of an x-CoA, a MN registers the x-CoA to x-HoA binding with the x-HA. This results in the establishment of an MIP tunnel which endpoints are the x-HA's address and MN's x-CoA. Then the MN initiates the establishment of an IPSec tunnel with the VPN-GW, using its x-HoA. This results in the creation of an entry on the private intranet to the MN. The MN then registers a binding consisting of the intranet address of the VPN-GW paired with the MN's i-HoA. This results in the creation of a third tunnel between i-HA and VPN-GW.

Intranet traffic destined to the MN is intercepted by i-HA then tunneled to the VPN-GW. The latter securely redirects the traffic, using a VPN tunnel, to the x-HoA of the MN. The traffic is intercepted by the x-HA which in turn tunnels it to the current location of the MN.

Since the x-HoA is the identity of the IPSec tunnel ending at the MN, there is no need for a protocol for updating addresses in SAs after a handoff. The MIP protocol is used as is, but the actual way it is being used is extended. Setup time requires a minimum of four round-trip times (RTTs): one RTT for the external registration, a minimum of two RTTs for the IPSec tunnel establishment (the use of the IKE protocol is assumed) and one RTT for the external registration. The intranet traffic destined to the MN must go trough two HAs.

This approach, although, suffers from double triangle routing. While visiting a foreign network, the traffic from a CN to a MN is first delivered to the home network. In the home network, the HA is aware of the fact that the MN is away. It intercepts the traffic destined to MN and tunnels it to the current location of MN. Hence, traffic destined to the MN is subject to double network latency. This problem is termed triangle routing and has been addressed with extensions to MIP called route optimization [11]. Using route optimization, the CN is made aware of the current location of the MN. The HA and MN sends binding update messages to the CN for that purpose. The CN can send traffic directly to MN hence avoiding triangle routing.

III. Protocol Extensions

A. Extension I

The Extension I addresses the Scenario 2, i.e. one node is inside the corporate network, termed the internal CN (i-CN) in the sequel, and a MN is outside the corporate network. In the SUM architecture, in order to provide a secure network connection to a MN visiting a foreign network, two MIP tunnels are used. Traffic from i-CN is intercepted by i-HA, (MIP) tunneled to the VPN-GW, forwarded by the VPN-GW, intercepted by the x-HA and (MIP) tunneled to the MN. There is an i-HA to VPN-GW MIP tunnel and a x-HA to MN MIP tunnel. Note that the flow of traffic in the opposite direction doesn't need MIP tunneling. That is the traffic from the MN destined to the VPN-GW and traffic from the VPN-GW to i-CN is not subject to interception and redirection. Hence, the result is two triangle routes. For the first route, the vertices of the triangle are i-CN, i-HA and VPN-GW. For the second route, the vertices of the triangle are the VPN-GW, x-Ha and MN. We use route-optimization techniques to eliminate the intermediaries and resulting MIP triangle routes.

When intercepting packets destined to the MN from i-CN, i-HA informs i-CN about the need to redirect the traffic destined to MN to the VPN-GW. The packets destined to the MN are then sent through the VPN-GW, which is shorter than going through both i-HA and VPN-GW.

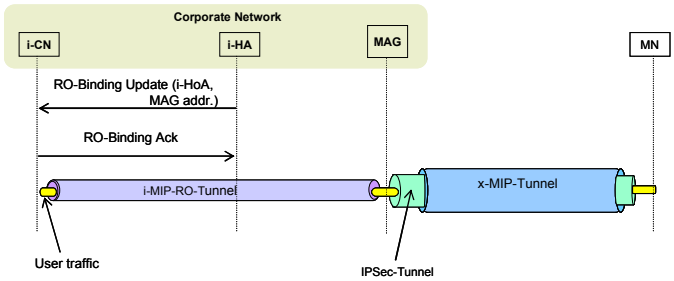

Figure 1: Extension I using route optimization.

The setup of this shorter path is achieved using the route-optimization messages defined by Perkins and Johnson [11]. Following the exchange of route-optimization messages, the i-CN forwards all the packets destined to the i-HoA directly to the VPN-GW instead of sending them to the i-HA, which then forwards to the VPN-GW. This avoids triangle routing between i-CN, i-HA and VPN-GW. Packets are delivered relatively faster. We describe the required protocol extension in detail hereafter. In our scheme the VPN-GW and x-HA are combined in to a single entity called the mobility-aware VPN gateway (MAG). Upon intercepting packets destined to i-HoA, i-HA sends a binding update message to the i-CN binding the i-HoA to the internal address of the MAG. This makes i-CN aware of a shorter path to MN via the MAG, instead of going through i-HA. I-CN then creates a binding entry for i-HoA paired with the MAG's internal address. Thereafter, packets destined to i-HoA are tunneled to the MAG, for the corporate network part. I-CN forwards all packets directly to the MAG using i-MIP-RO-tunnel as pictured in Fig. 1. It is mandatory that i-CN and MAG support MIP route optimization.

B. Extension II

The Extension II addresses the Scenario 3. Two MNs, both outside their corporate network, communicate with one another. This scenario has not been addressed by prior work. Hereafter, we present a scheme that addresses the scenario. Secure communications is provided between two MNs outside their corporate network. This is achieved by establishing a bridge between two separate VPN tunnels and two separate MIP tunnels (see Fig. 2). The establishment of the bridge is accomplished by the MAG.

When two MNs are outside their corporate network and wish to communicate with one another, the following steps are performed:

1. The MNs perform MIP registration with the MAG.

2. A secure VPN tunnel is established between each individual MN and the MAG.
3. The MNs perform MIP registration with their respective i-HAs.

The Steps 1 to 3 are performed by any MN which is outside the corporate network and with a desire to communicate securely with other nodes belonging to the corporate network. Table 1 represents the structure of the information maintained by the MAG after Steps 1 to 3 are performed by MN1 and MN2.

TABLE I
BINDING TABLE ENTRIES AT THE MAG

MN	x-HoA	i-HoA	x-CoA	$SAiD_{to\text{-}MN}$	$SAiD_{from\text{-}MN}$
MN1	192..9	10..6	198..8	1387	1388
MN2	192..1	10..12	133..7	2076	2078

When Step 1 is performed, the MN's addresses, x-HoA and x-CoA, are entered into the table. After Step 2, SA identifiers (SAids) are added for each direction. The $SAiD_{to\text{-}MN}$ is the identifier for the IPSec SA that is negotiated for the traffic from the MAG to the MN while $SAiD_{from\text{-}MN}$ is the IPSec SA from the MN to the MAG. Note that the table always has a row mapping the x-HoA to the i-HoA. The values for the x-CoA and SAids are the only ones entered after completion of Steps 1 and 2. Step 3 has no effect on the table. A row with a non-empty x-CoA field indicates to the MAG that the corresponding MN is outside the corporate network.

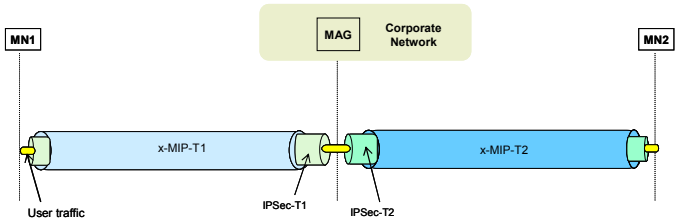

Fig. 2: Extension II with tunnels bridging by MN1 and MN2.

The key feature of this extension is that, when a packet destined to a i-HoA is received by the MAG, the MAG checks to see if the i-HoA is paired with a corresponding x-CoA. If a x-CoA does exist for a particular i-HoA, then it implies that the MN, which has a private address i-HoA, is visiting outside the corporate network. Therefore the packets destined to i-HoA are not forwarded into the corporate network. An example is pictured in Fig. 2. The traffic from MN1 to MN2 goes as follow:

- MN1 sends a packet to MN2. The source address is i-HoA1 (internal source address of MN1) and destination address is i-HoA2 (internal address of MN2).
- The VPN application on MN1 is invoked (since the packet has an internal source address and internal destination address). The packet undergoes all the necessary steps to conform to the IPSec SA that was negotiated with the MAG (e.g. encryption and integrity value computation). Then the packet is encapsulated with an IP header using the x-HoA of MN1, as the source address, and the external address of the MAG as destination address. The tunnel IPSec-T1, connecting MN1 to the MAG, is used to transport the packets. IPSec-T1 is identified by the endpoints x-HoA and address of the MAG.
- The MIP client application on MN1 encapsulates the secure packets with another IP header, using x-CoA1 as the source address and external address of the MAG as destination address. The tunnel x-MIP-T1, connecting MN1 to the MAG, is used to transport the MIP packet. Note that the original packet now has three IP headers.
- Since the outermost header is destined to the MAG, the MAG is the first to receive the packet. It processes and discards the MIP header.
- The MAG then checks the inner header and packet body for conformance to the appropriate IPSec SA. The IPSec SA is obtained from by the MAG using the appropriate $SAiD_{from\text{-}MN}$ value (1388) from Table I for MN1. The $SAiD_{from\text{-}MN}$ value is used to fetch the SA from a security association database maintained by the MAG.
- If the packet meets the IPSec SA, then the MAG discards the IPSec header and then processes the inner-most header. Since the destination address of the packet is the internal address of MN2, it looks for a row for MN2 in Table I. If there is a row, then it checks if there is a value for the x-CoA field.
- If there is a x-CoA value, then the $SAiD_{to\text{-}MN}$ is used to obtain the IPSec SA. The $SAiD_{to\text{-}MN}$ for MN2 is 2076. The $SAiD_{to\text{-}MN}$ is used to fetch the SA, from the security association database. The required security functions are applied to the packet. A new IP header is appended. The source address is the MAG external address and destination address is the x-HoA of MN2. This achieves the IPSec-T2 tunneling.
- The secure packet is then tunneled using x-MIP-T2. The source address is the external address of the MAG and destination address is the x-CoA of MN2.

With respect to prior work, our solution has the following advantages:

- The decision of whether to send the packet into the corporate network or not is performed at the MAG itself, unlike the prior work where the packets have to travel all the way to the i-HA to realize that the MN is outside the corporate network. This not only causes high latency but also high packet overhead.
- Prior work does not offer solutions for MNs wanting to communicate with one another that are outside the corporate network. Even if the solutions are tweaked they do not offer low latency communications.
- The SAs don't have to be renegotiated when the location of the MN, outside of the corporate network, is updated.

C. *Extension III*

The Extension III also addresses Scenario 3. With Extension II, there is inefficiency at the MAG. The MAG has to unnecessarily decrypt and re-encrypt the user traffic in order to conform to two different IPSec SAs.

In Extension III, a new end-to-end secure tunnel, between MN1 and MN2, and a new end-to-end MIP route-optimized tunnel, between MN1 and MN2, are created. The improvements, over Extension II, are the route-optimized paths and avoidance of decryption and re-encryption at the

MAG. Another advantage is that the signaling messages required to create new SAs and MIP tunnels are transported over already established secure VPN tunnels.

The communications between MN1 and MN2 are route-optimized so that the new MIP tunnel x-MIP-RO-Tunnel now runs between MN1 and MN2 without being terminated at the MAG (see Fig. 3). Following the setup presented in Extension II, this optimization is initiated by the MAG. Upon realizing that the MNs are communicating via split IPSec tunnels, the MAG initiates the optimization procedure. The optimization procedure consists of the following steps:

1. The MAG generates shared keys.
2. The MAG distributes shared keys via the secure tunnels to both MNs and also instructs the MNs to start IPSec negotiation between them.
3. The MNs initiate the procedure, using the newly obtained keys to establish the IPSec SAs, and create the new IPSec-Tunnel (see Fig. 3).
4. The MAG sends a MIP route optimization message to both the MNs to setup the x-MIP-RO-Tunnel.
5. Each MN updates their binding table entries to reflect the change in MIP tunnel endpoints.

When the MAG realizes that the MNs are communicating via split tunnels that traverse via the MAG, the MAG generates shared keys which are used to set-up a secure peer-to-peer VPN connection between the MNs. In Step 2, the MAG distributes these keys to the MNs and also instructs the MNs to create IPSec SAs between them. The MAG also sends the external addresses of MNs to one another. In Step 3, the MNs initiate a procedure between themselves and new IPSec SAs are created (the IKE protocol can be used for that purpose).

These SAs are negotiated between the MNs and do not involve the MAG. Communications between the MNs are now protected by the new SAs. In Step 4, the MAG sends a route optimization message containing each of the MNs current x-CoA. The MNs on receiving the route optimization message update their internal binding entry. An example is illustrated in Fig. 3. The flow of traffic from MN1 to MN2 goes as follows:

- MN1 sends a packet to MN2. The source address is i-HoA1 (internal address of MN1) and destination address is i-HoA2 (internal address of MN2).
- The VPN application on MN1 is invoked and the packet undergoes all the necessary steps to conform to the IPSec SA that was negotiated with MN2. Then the packet is transported using the IPSec-Tunnel which has x-HoA1 as source address and x-HoA2 as destination address. In Extension II, the destination address is the external address of the MAG.

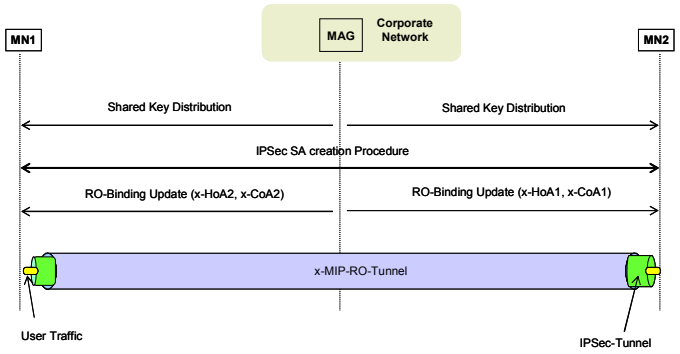

Fig. 3: Extension III.

- The MIP client application on MN1 encapsulates the secured packet using the x-MIP-RO-Tunnel which has x-CoA1 as source address. The destination address of the tunnel is x-CoA2 (care-of address of MN2). In Extension II, the destination address is the external address of the MAG.
- Since x-CoA2 is the destination, MN2 receives the packets and discards the outer MIP header.
- The MN2 then checks the inner header and the packet body for conformance to the appropriate IPSec SA.
- On conformance to the SA, the IPSec header is discarded and the original packet, having i-HoA1 as source address and i-HoA2 as destination address, is processed by the application.

The following advantages can be observed when compared to all the prior solutions:

- Unlike Extension II or the SUM solution, the MAG does not decrypt and re-encrypt to conform to the SAs. The load on the MAG is very much reduced since the MAG may be serving a number of CNs and MNs.
- The latency incurred by user traffic because of decryption, re-encryption and re-tunneling of packets at the MAG is completely avoided.
- The tunnel that is established is generally the shortest path possible since it avoids triangle routing.

When one of the MN moves back to the protected corporate network, the MAG updates the table to reflect the absence of x-CoA value for the particular MN. The table is updated based on MIP registration or binding update message sent by the MN. The message can be sent by the MN to the MAG before handoff happens or after it. For session continuity, it is recommended that the MIP registration message is sent before the actual layer-2 handoff occurs. Layer-2 triggers to the network layer can be used as an indication of imminent handoff so that a network layer handoff can be performed thus providing make-before-break.

IV. Conclusion

In this paper, we presented solutions to reduce the latency incurred by real-time user traffic when using secure tunnels in a mobile environment. The mechanisms we have discussed decrease traffic latency when a MN in a public Internet communicates with another MN in a protected Intranet. We also provide solutions for the case where both communicating MNs are outside the protected Intranet, but demand the same

level of secure communications as when inside the corporate network. For real-time applications, the latency incurred by intermediaries and triangle routes and their effects; namely, decryption, re-encryption and re-tunneling at the MAG; is not acceptable. This latency is further magnified when session continuity is required between heterogeneous radio accesses or in a highly mobile environment. By providing secure connections over route-optimized paths, as described in Extension III, unnecessary computation and latency are avoided.

REFERENCES

[1] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," Request for Comments: 2409, November 1998.

[2] C. Perkins (Editor), "IP Mobility Support," Request for Comments: 2002, October 1996.

[3] T. Kivinen, "Design of the MOBIKE Protocol," Internet-Draft, June 2004.

[4] J. Rejeb, M. Vohra, and T.T. Le, "IKE-based Secure Wireless and Mobile Networks," IEEE 6th CAS Symp. On Emerging Technologies: Mobile and Wireless Comm., Shanghai, pp. 567-570, June 2004.

[5] M. Barton, D. Atkins, J. Lee, S. Narain, D. Ritcherson, K.E. Tepe, and K.D. Wong, "Integration of IP Mobility and Security for Secure Wireless Communications," IEEE International Conference on Communications (ICC), vol. 2, pp. 1045–1049, April-May 2002.

[6] R. Bhagvathula, N. Thanthry, W. Lee, and R. Pendse, "Mobility: A VPN Perspective," The 45th Midwest Symposium on Circuits and Systems (MWSCAS), vol. 3, pp. III-89 - III-92, Aug. 2002.

[7] D. Khatavkar, E. Rena Hixon, and R. Pendse, "Quantizing the Throughput Reduction of IPSec with Mobile IP," The 45th Midwest Symposium on Circuits and Systems (MWSCAS), vol. 3, pp. III-505 - III-508, Aug. 2002.

[8] V. Gupta and G. Montenegro, Secure and Mobile Networking, Mobile Networks and Applications, vol. 3, pp. 381-390, 1998.

[9] J.-M. Park, M.-J. Jin, and K. Chae, "Secure Firewall Traversal in Mobile IP Network," in: P.M.A. Sloot et al. (Eds.):ICCS 2003, LNCS 2660, Springer-Verlag, Berlin Heidelberg, pp. 535-544, 2003.

[10] A. Dutta, T. Zhang, S. Madhani, K. Taniuchi, K. Fujimoto, Y. Katsube, Y. Ohba, and H. Schulzrinne, "Secure Universal Mobility for Wireless Internet," First ACM International Workshop on wireless Mobile Applications and Services on WLAN Spots (WMASH), Philadelphia, pp. 71-80 October 2004.

[11] C. Perkins, D. Johnson, Route Optimization in Mobile IP, Internet Draft, 2001.