Mobile Multilayer IPsec protocol

T.Gayathri[1], S.Venkadajothi[2], S.Kalaivani[3], C.Divya[4] and Dr.C.Suresh Gnana Dhas[5]

Final year Computer Science and Engineering[1, 2, 3, 4] and Professor[5]

tgayathri88@gmail.com[1],venkadajothipandian@yahoo.in[2],kalai_s4@yahoo.co.in[3],

divi8901@yahoo.co.in[4],sureshc.me@gmail.com[5]

Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering college,Avadi

Abstract : A mobile user moves around and switches between wireless cells, subnets and domains, it needs to maintain the session continuity. At the same time security of signaling and transport media should not be compromised. A multi-layer security framework involving user authentication, packet based encryption and access control mechanism can provide the desired level of security to the mobile users. Supporting streaming traffic in a mobile wireless Internet is faced with several challenges due to continuous handoff experienced by a mobile user. These challenges include dynamic binding, location management, quality of service and end-to-end security for signaling and transport. Mobile users will use heterogeneous radio access networking technologies. Mobile multilayer IPsec protocol (MML IPSec) extends ML-IPSec to deal with mobility and make it suitable for wireless networks. MML-IPSec is integration of ML-IPSec and mobile IP.

Keywords : Mobile multilayer IPsec protocol, MML IP-Sec

1. Introduction:-

Data confidentiality and integrity are two critical issues for wireless, mobile networks. These issues are of growing importance as wireless service providers attempt to increase wireless data traffic by providing mobile VPN services. The most widely accepted method for ensuring data confidentiality and integrity is to pass encrypted data end-to-end using a mechanism such as IPsec. MML-IPsec[2] allows a mobile access router, for example a Mobile IP Foreign Agent (FA) to decrypt and operate on packet headers to enable performance enhancing algorithms to execute, while protecting the packet payload end-to-end.

However, these services cannot be provided if end-to-end encryption is used, such as in IPsec, because the information needed by these algorithms resides inside the portion of the packet that is encrypted, and can therefore not be used by mobile routers. Multi-layered IPsec (ML-IPsec) applies a modified version of IPsec so that certain portions of the user information may be exposed to particular intermediate network elements in a route. In this way, portions of a datagram may be encrypted end-to-end, while portions may be read and operated upon by network elements providing performance enhancements. However, the ML-IPsec is designed for static environments and does not examine mobility.

Several studies have shown that the performance of classic data communication protocols can be quit poor when used over wireless links. In particular the performance of TCP, the reliable Internet transport protocol, can be degraded by the loss and delay characteristics of a wireless link. Consequently, there have been several efforts aimed at improving the performance of TCP on wireless links.

2. IP-Sec Protocol:-

IPSec[4] is a framework for security that operates at the Network Layer by extending the IP packet header (using additional protocol numbers, not options). This gives it the ability to encrypt any higher layer protocol, including arbitrary TCP and UDP sessions, so it offers the greatest flexibility of all the existing TCP/IP cryptosystems. Flexibility, however, often comes at the price of complexity, and IPsec is not an exception. Configuring which addresses and ports to encrypt using which IPsec options often begins to look like configuring packet filtering, then add in the additional complexities of key management.

2.1 Modes:-

There are two modes of IPSec operation: transport mode and tunnel mode

I. Transport mode: - In transport mode, only the payload of the IP packet is encrypted and/or authenticated. The routing is intact, since the IP header is neither modified nor encrypted; however, when the authentication header is used, the IP addresses cannot be translated, as this will invalidate the hash value. The transport and application layers are always secured by hash, so they cannot be modified in any way. Transport mode is used for host-to-host communication.

II. Tunnel mode: - In tunnel mode, the entire IP packet (data plus message headers) is encrypted and or authenticated. It must then be encapsulated into a new IP packet for routing to work. Tunnel mode is used for network-to-network communication or host-to-network and host-to-host communication over Internet.

2.2 IPsec uses two protocols to provide traffic security - Authentication Header (AH) and Encapsulating Security Payload (ESP).

The IP Authentication Header (AH) provides connectionless integrity, data origin authentication, and an optional anti-replay service. The Encapsulating Security Payload (ESP) protocol may provide confidentiality (encryption), and limited traffic flow confidentiality. It also may provide connectionless integrity, data origin authentication, and an anti-replay service.

These protocols may be applied alone or in combination with each other to provide a desired set of security services in IPv4 and IPv6. Each protocol supports two modes of use: transport mode and tunnel mode. In transport mode the protocols provide protection primarily for upper layer protocols; in tunnel mode, the protocols are applied to tunneled IP packets

2.3How does IPSec works:-

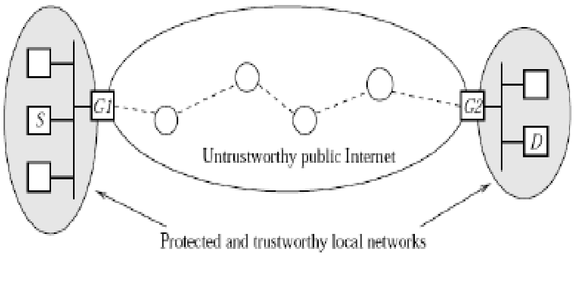
S
G1
G2
D
Untrustworthy public Internet
Protected and trustworthy local networks

Fig1.IPSec

-It is standard protocol for secure communication[4] over the Internet

-It protects the entire IP datagram of a packet from end-to-end

-It is used for VPNs and secures remote access

-No intermediate node can access information above the IP layer

Path between source and destination consists of three parts:

1. Protected and trusted LAN at the source

2. Untrusted public Internet

3. Protected and trusted LAN at the destination

G1 establishes a security association with G2 using shared secrets

G1 encrypts a datagram with an IPsec protocol (e.g.: 3DES, AES256)

G2 decrypts the datagram before forwarding it to the destination

2.4 Limitations of IPSec protocol:-

With IPSec the following is not possible:-

I. Internet traffic engineering:

The internet is moving towards active traffic engineering to meet increasing demand for bandwidth a rich services. Depending upon granularity used in defining a “flow,” certain nodes in the middle of the network may need access to the information to the upper layer protocols, such that TCP/UDP ports numbers, to classify packets into flows before applying discriminating operations.

II. Transport-aware link layer mechanisms:

Link layer mechanism for TCP performance improvement require intermediate node to access and sometimes modify the upper layer protocol header.

III. Application-layer proxies/agents:

Some internet router can provide application layer service for performance gains. For example an intermediate router can become a transparent web proxy when it snoops through the TCP and HTTP header of a bypassing IP datagram to determine the URL request, and serves it with the web page from the local cache. It is transparent to end user but boosts responsiveness because the delivery paths for web requests and data between the intermediate router and the web site server are eliminated.

IV. Active networks:

The active network architecture is a new networking paradigm in which router performs customized computation on the data flowing through them. A number of experimental active network systems have been developed and they can be run over the internet. In this architecture, a single IP datagram carries not only upper-layer protocol headers and user data, but also a "method" – a set of executable instructions to be interpreted by the intermediate routers, for describing, provisioning, or tailoring network resources and services order to achieve the delivery and management requirements.

V. Traffic Analysis

Many network operators actively monitor the traffic for accounting or for intrusion detection purposes. Usually, such monitoring requires logging of certain upper layer protocol information, like TCP/UDP ports. Many firewalls that protect local network also depend on such information to deny unauthorized traffic

3. Multi-Layer IPsec (ML-IPsec)

ML-IPsec uses multi-layer protection model to replace the single end-to-end model. Unlike IPsec where the scope of encryption and authentication apply to the entire IP datagram payload (sometimes IP header as well), this scheme divides the IP datagram into zones. Each zone has its own sets of security associations, its own set of private keys (secretes) that are not shared with other zones, and its own sets of access control rules(defining which nodes in the network have access to the zone).

When ML-IPsec protects a traffic stream from its source to its destination, the first IPsec gateway (or source) will re-arrange the IP datagram into zones and apply cryptography protection. When the packet reaches the last IPsec gateway (or destination), ML-IPsec defines a complex security relationship that involves both the sender and the receiver of a security service, but also selected intermediate nodes along the traffic stream.

For example, a TCP flow that desires link-layer support from the network can divide the IP datagram payload into two zones: TCP header and TCP data. The TCP data part can use an end-to-end protection with key shared only between the source and destination (host or security gateway). The TCP header part can use a separate protection scheme with keys shares among the source, the destination, and certain trusted intermediate node. This way, no other than the source, the destination and the trusted intermediate nodes has access to TCP header or TCP data, and no one other than source and destination (not even trusted intermediate node) has access to TCP data.

The identity of the intermediate nodes must be authenticated to prevent any man-in-middle attack. After authentication, keys or shared secrete corresponding to the authorized IP datagram zones must be distributed to the intermediate nodes.

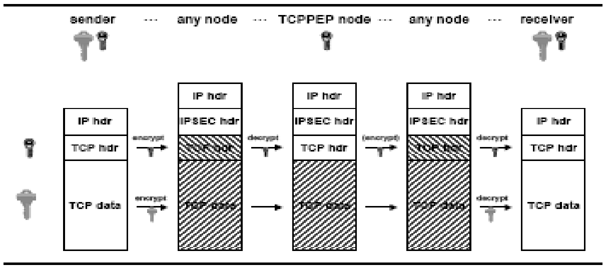

Fig.2 Multi-layer IPSec

4. Mobile IP

IP version 4 assumes that a node's IP address uniquely identifies its physical attachment to the Internet. Therefore, when a correspondent host (CH) tries to send a packet to a mobile node (MN), that packet is routed to the MN's home network; independently of the current attachment of that MN (this is because CHs do not have any knowledge of mobility). When the MN is on its home network, and a CH sends packets to the mobile node, the Mobile Node obtains those packets and answers them as a normal host (this is one important requirement in Mobile IP), but if the MN is away from its home network, it needs an agent to work on behalf of it. That agent is called

Home Agent (HA). This agent must be able to communicate with the MN all the time that it is “on-line”, independently of the current position of the MN. So, HA must know where the physical location of the MN is.

In order to do that, when the MN is away from home, it must get a temporary address (which is called care-of address), which will be communicated to the HA to tell its current point of attachment. This care-of address can be obtained by several ways, but the most typical one is that the MN gets that address from an agent. In this case, this agent is called Foreign Agent (FA). Therefore, when a MN is away from home, and it’s connected to a foreign network, it detects is on a different network and sends a registration request through the FA to the HA requesting mobile capabilities for a period of time. The HA sends a registration reply back to the MN (through the FA) allowing or denying that registration. This is true when the Mobile Node is using a Foreign Agent for the registration. If the Mobile Node obtains the care-of address by other meanings, that step (registration through the FA) is not necessary. If the HA allows that registration, it will work as a proxy of the MN. When MN’s home network receives packets addressed to the MN, HA intercepts those packets (using Proxy ARP), encapsulates them, and sends them to the care-of address, which is one of the addresses of the FA. The FA will decapsulates those packets, and it will forward them to the MN (because it knows exactly, where the MN is). Encapsulation is the method used by the HA to deliver information to the MN putting an extra IP header on top of the packet and tunneling that packet to the MN (when it's on a foreign network). Tunneling and encapsulation are defined in IP tunneling and IP encapsulation within IP.

So, when the MN is on a foreign network, it uses its home agent to tunnel encapsulated packets to itself via FA. This occurs until the lifetime expires (or the MN moves away). When this happens (time out) MN must register again with its HA through the FA (if the MN obtains its care-of address for other meanings, it acts as its own FA).

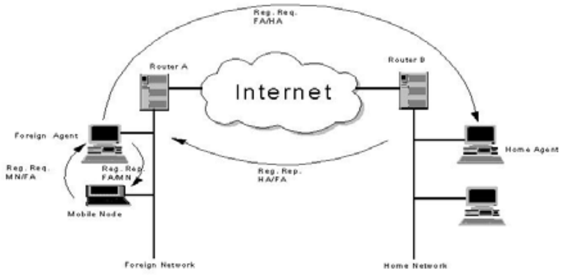

Fig.3 Mobile IP

When the MN moves to another network and it detects so, it sends a new registration request through (one more time) the new FA. In this case, HA will change MN’s care-of address and it will forward encapsulated packets to that new care-of address (which, usually, belongs to the FA). Some extensions of Mobile IP allows to a MN to have several care-of addresses. Then, HA will send the same information to all the care-of addresses. This is particularly useful when the MN is at the edgesof cells on a wireless environment, and it is moving constantly. MN bases its movement detection basically looking at periodic adverts of the FA (and HA), which sends to its local net. Those messages are one extension of the ICMP router discovery messages and they are called Agent Advertisement (because they advertise a valid agent for Mobile Nodes).

4.1 There are two different methods to detect network movement:

a) The first method is based on network prefixes.

b) The second method is based upon the Lifetime field within the main body of the ICMP Router Advertisement portion of the Agent Advertisement. Mobile nodes keep track of that Lifetime and if it expires, it sends an Agent Solicitation (asking for a new Agent Advertisement) and it presumes that it has been moved.

When the MN returns to its home network, it does not require mobility capabilities, so it sends a deregistration request to the HA, telling it that it’s at home (just to deactivate tunneling and to remove previous care-of address (es)). At this point, MN does not have to (de)register again, until it moves away from its network. The detection of the movement is based on the same method explained before.

5. Mobile Multilayer IP sec

ML-IPsec protocol allows a user to define zones within an IP packet. Each zone is encrypted and authenticated with its own security association **(SA).** Each zone may be accessed (decrypted) by different network elements. This requires **SAS** to be established between a client and several nodes in a network, each of which can decrypt a certain portion of the IP packet while being unable to view the entire packet.

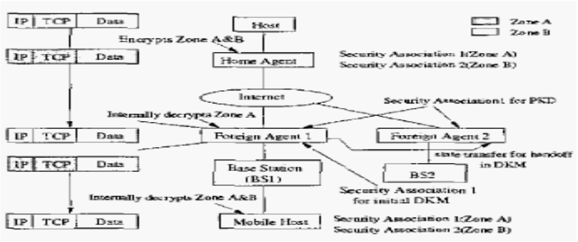
IP
TCP
Data
Host
Zone A
Zone B
Encrypts Zone A&B
Home Agent
Security Association 1(Zone A)
Security Association 2(Zone B)
Internet
Security Association1 for PKD
Internally decrypts Zone A
Foreign Agent 1
Foreign Agent 2
state transfer for handoff in DKM
Base Station (BS1)
BS2
Security Association 1 for initial DKM
Internally decrypts Zone A&B
Mobile Host
Security Association 1(Zone A)
Security Association 2(Zone B)

Fig. 4 Wireless Network

For example, consider the wireless network of Fig 4. In this example the corporate firewall acts as a Mobile IP Home Agent (HA). Foreign Agent (FA) 1 requires access to TCP/IP header information to perform smart packet processing. Using IPSE, secure communication would entail running an IPsec tunnel between the HA and Mobile Host IMH), in which case FA1 would not have access to the TCP/IP header information. Using ML-IPsec, this header information would be included in Zone A which is accessible to FA 1. However, the user payload would be placed in Zone B which is not accessible to FA1. In this way, the user information is protected end-to-end and the TCP/IP header information is protected from all nodes except FA1 which may perform smart packet processing. While ML-IPsec is a promising Start, it has limitations and several unknowns.

First, it requires that SAS (secret keys, algorithms, parameters, etc.) be established between multiple elements for a single data session. This requires an efficient key distribution algorithm which has yet to be defined.

Second, mobility is not supported. The mobility requires that new SAS be established as a mobile host moves during a data session. For example, in Fig. 4, if the mobile host moves from base station 1 (BS1) to BS2, SA1 must move from FA1 to FA2. These modifications must be performed quickly so that sessions are not disrupted during a handoff.

Third, there is no data available on the performance tradeoffs between the overhead of supporting multiple zones versus the benefits of packet classification or smart packet process- ing. Specifically, mobile access routers,

The original ML-IPsec is defined to allow network layer packets to be segmented into zones, each of which is protected, i.e., encrypted, authenticated. or both, independently. Corresponding hosts have access to all zones and can therefore authenticate and decrypt the entire packets. Selected intermediate nodes are given access to one or more selected zones, and may therefore decrypt and authenticate only these portions of the packet, Before communication can commence, a set of SAS, called a composite security association (CSA), must be established, one for each zone in each node for which access to the zone is permitted. The FA routes this data traffic into the Mobile IP tunnel based on the reverse tunnel of the Mobile IP Next. Traffic from the CN to the MH is intercepted by the HA. The HA encrypts the traffic and encapsulates it within the Mobile IP tunnel, which has the outer header source address as the HA IP address, and the destination address as the FA IP address, If IPsec is used. When receiving the encapsulated traffic, the FA decapsulates the Mobile IP outer header and transmits the encrypted traffic to the MH. If ML-IPsec is used, the intermediate node decrypts the first zone (packet header), performs some processing, re-encrypts this zone, and forwards the data.

5.1 Key Distribution and Mobility Management:-

The key management protocols have two phases. In the first phase, a MML-IPsec[1] session is initialized using ML-IKE. This includes determining if a FA will be involved in the secure session, and hence requires the use of MML- IPsec. The second phase of the protocols supports mobility. There are two protocols, the first, called Proactive Key Distribution (PKD), pre-establishes SA's with not only the current FA, but its neighbors as well. Therefore, when a MH moves to a new FA, the SA already exists. The second called Dynamic Key Migration (DKM), requires SA's to migrate between FAs as a user moves.

I. Initialization

When a MH leaves its home network, it executes Mobile IP registration procedures. In addition, ML-IKE is invoked. Figure 6 shows the initialization flows between the HA, FA and MH with the Mobile IP registration. The initialization phase begins after the HA has sent the Mobile IP registration reply to the FA. First, the HA establishes an ISAKMP SA with the FA and MW so that session key information may be exchanged securely. The establishment of the ISAKMP SA between the FA and HA occurs in parallel with sending the Mobile IP registration reply to the MH. The second step of the initialization is to establish the CSAs in the MH, HA and FA. The CSA has two elements, a zone map and a zone list.. The source and destination (HA and MH) store a complete list of SAS. On the other hand, the FA has a non-null SA in the zone list for the zone that it supports, and a null SA for the zone that it does not support.

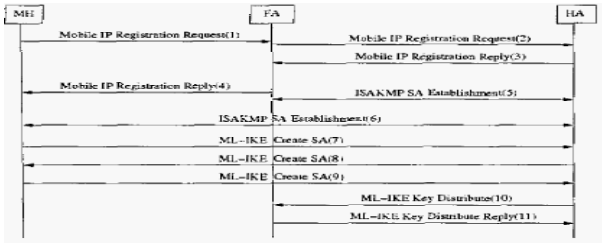
MH
FA
HA
Mobile IP Registration Request(1)
Mobile IP Registration Request(2)
Mobile IP Registration Reply(3)
Mobile IP Registration Reply(4)
ISAKMP SA Establishment(5)
ISAKMP SA Establishment(6)
ML-IKE Create SA(7)
ML-IKE Create SA(8)
ML-IKE Create SA(9)
ML-IKE Key Distribute(10)
ML-IKE Key Distribute Reply(11)

Fig. 6 HA and MH setup

The HA and MH setup a MML-IPsec CSA using the MLIKE Create SA Exchanges (flows (7)-t9) in Fig. 6). During these exchanges, the MH and HA exchange the complete zone map and SAS to compose a CSA. We define a new payload type called “Zone Map” which delivers the zone map information. In addition, we modify the key exchange protocol to allow for multiple SAS to be included. The secret key values for all zones are decided in the MML-IPsec Create SA Exchanges. Once the CSA is established between the MH and HA, the HA delivers the CSA to the FA, using the ISAKMP SA with the FA. For the zone to which the FA has access, i.e. the zone covering the TCP/IP header, the HA sends the corresponding non-null SAS to the FA (flow (10) - (11) in Fig. 6 with the corresponding symmetric key values. A new payload, called “SECRET’, delivers the symmetric key values. Upon completion of the ML-IKE procedure, data transmission using MML-IPsec may take place.

II. Proactive key Distribution (PKD)

The goal of PKD is to enable a fast handoff by pre-distributing keys in FAs that are neighbors of the current FA, so that very little overhead is incurred during the real time handoff. The distribution of the CSA information to the neighboring FAs is performed after the ML-IKE exchange is complete, so initialization overhead will not be increased. The disadvantage of this approach is that the active key information must be stored in more nodes than are actively being used, thus creating a higher chance of the session key being compromised. Fig. 7 shows the PKD protocol flow. The FA, when finished initialization, notifies the HA of its neighbor FAs (flow (1) in Figure 7). The HA distributes the MML-IPsec CSA information established via ML-IKE to the neighbor FAs. The HA establishes an ISAKMP SA to each neighboring FA *to* transmit ML-IPsec CSA securely (flow *(2)* and (5) in Figure *7)*

PKD can be performed in two ways: (a) point-to-point sequential key distribution; (b) multicast key distribution. When the MH moves to a new FA, the handoff latency is low because the MML-IPsec CSA information is already loaded in the new FA. When the new FA receives a Mobile IP registration reply from the HA, the FA internally activates the MML-IPsec CSA.The HA only changes the internal binding of the Ma-IPsec tunnel to the new Mobile IP tunnel with the neighbor FA.

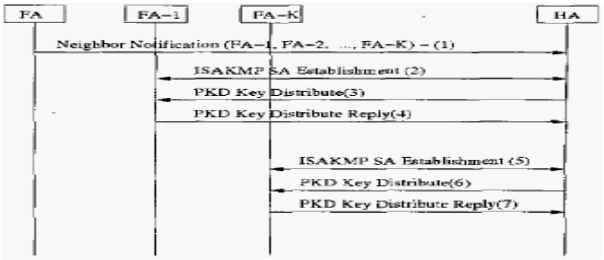
FA
FA-1
FA-K
HA
Neighbor Notification (FA-1, FA-2, ..., FA-K) - (1)
ISAKMP SA Establishment (2)
PKD Key Distribute(3)
PKD Key Distribute Reply(4)
ISAKMP SA Establishment (5)
PKD Key Distribute(6)
PKD Key Distribute Reply(7)

Fig. 7 PKD protocol flow

III. Directed Key Migration (DKM)

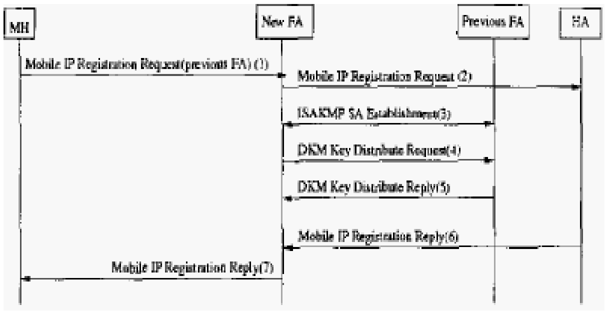
MH
New FA
Previous FA
HA
Mobile IP Registration Request(previous FA) (1)
Mobile IP Registration Request (2)
ISAKMP SA Establishment(3)
DKM Key Distribute Request(4)
DKM Key Distribute Reply(5)
Mobile IP Registration Reply(6)
Mobile IP Registration Reply(7)

Fig. 8 Mobile Ip registration

For example, in Fig.4, SA1 must be moved from FA1 to FA2. This method only requires that the CSA be stored in a single intermediate node, but incurs a higher latency than PKD because more signaling is required during he handoff. Figure 8 shows the DKM protocol flow. When a MH moves to a new FA, it detects the movement using standard Mobile IP techniques. We modify the Mobile IP Registration by adding an extension to include the previous FA address, as is done in Mobile IP with Route Optimization.

First, the MH transmits a Mobile IP registration message with the previous FA information to the new FA (flow (1) in Figure 8). The new FA uses the previous FA information to decide where to retrieve the MML-IPsec CSA information. The new FA initiates the DKM protocol, and relays the Mobile IP registration message to the HA simultaneously.

In DKM, if there is no ISAKMP SA established between the previous FA and the new FA. The new FA establishes an lSAKMP SA with the previous FA so the key information is transferred securely. Once this ISAKMP SA is established, the new FA transmits the MML-IPsec CSA information request to the previous

FA (flow (41 in Figure 6). The previous FA authenticates the new FA and sends the response to the new FA (flow (5) in Figure 6). The response message includes the ML-IPsec CSA including the secret key values, Note that the DKM protocol is processed in parallel with the Mobile IP registration between the new FA, HA and MH.

D. Rekeying and Revocation

There are several reasons why rekeying or key revocation may take place when using MML-IPsec. For example, if a CSA lifetime expires, or a CSA is determined to be insecure, it may be revoked, or if secure communication is still desired, rekeying may take place during which a new CSA is established. Further, key revocation may take place when a Mobile IP tunnel is deleted, for example when a MH returns to its home network or powers off. Finally, rekeying may take place when using MML-IPsec if the number of FAs that share the CSA exceeds a threshold value due to mobility.

Once the new CSA is established, the MH, FA and HA change to use the new CSA for data transfer, and the old CSA is deleted.

6. Conclusion

This paper describes a simplified version of ML-IPsec, an efficient key distribution protocol for initializing secure wireless sessions, and two protocols for managing mobility for these secure sessions. This suite of protocols are called MML-IPsec. MML-IPsec enables performance enhancing algorithm to be introduce into wireless network.

7. References

[1] Heesook Choi, Hui Song, Guohong Cao. and Tom La Porta Department of Computer Science & Engineering The Pennsylvania State University "Mobile Multi-Layered IPsec", 2005 IEEE.

[2] Yongguang Zhang and Bikramjit Singh HRL Laboratories, LLC, "A multi layer IPsec protocol".

[3] Ashutosh Dutta, Subir Das, Peter Li, Anthony McAuley Telcordia Technologies Inc. Yoshihiro Ohba, Shinichi Baba Toshiba America Research Inc, Henning Schulzrinne Computer Science Department, Columbia University, New York. "Secured Mobile Multimedia Communication for Wireless Internet".

[4] S. kent BBN corp "Security Architecture for the Internet Protocol" RFC 2401.