Analysis of Mobile IP Protocols Security

Amit Gupta
Student, ME (CSE)
Thapar University,
Patiala (Punjab), India

Sumit Miglani
Assistant Professor
Thapar University,
Patiala (Punjab), India

Maninder Singh
Associate Professor
Thapar University,
Patiala (Punjab), India

ABSTRACT
This paper describes the route optimization between Mobile IPv6 nodes which introduced several vulnerabilities in mobile environment. We first explain all the possible threats evolved due to route optimization technique and then possible defense mechanism to counter them. We have analyzed all that defense mechanism through comparative discussion and tried to find out best solution which may be more efficient and less complex.

General Terms
Security of mobile network, Analysis of mobile IP, Network design of mobile devices.

Keywords
Mobile IPv6, Network Security, Route Optimization, Mobility Protocol, Denial of Service, Return Routability, Internet key exchange protocol.

1. INTRODUCTION
After the evolution from 2G to 3G and now 3G to 4G, 4G will be based on the transmission of IP packets only, using an architecture known as mobile IPv6. Mobile IP [1] was introduced first to support mobility environment, it's a protocol that co-ordinates among different components of mobility environment such as home agent, foreign agent for mobility management to facilitate reachability of mobile nodes. Initially one mobile node couldn't communicate directly with another mobile node because all traffic passed through the home agent and then to the foreign agent. But as Mobile IPV6 [2] was introduced, the communication among mobile node and correspondent node had gone directly and thus improving the performance of mobility protocols by reducing delay with direct communication. Because 4G require a fast response, so IPv6 will feature many advantages, however security is still a fundamental issue to be resolved. One major security issue involves the route optimization (RO) technique, which deals with binding updates. This allows the corresponding node to communicate directly with the mobile node by passing the home agent router. Before route optimization, binding updates are exchanged between mobile node, home agent and correspondent node which causes a variety of security vulnerabilities. Binding updates include the interception of data packets, which would allow an attacker to eavesdrop on its contents or to modify transmitted packets for the attacker's own malicious purposes. There are other possible vulnerabilities with mobile IP like address spoofing, IP redirection and denial of service attacks. But to perform these attacks, all the attacker needs to know is the IPv6 addresses of the mobile's home agent and the corresponding node.

To implement route optimization the mobile host sends a Binding Update (BU) to the correspondent node for direct communication by informing the current location of the mobile host, thereby a Binding Acknowledgement (BA) message sent by correspondent node starts direct communication among mobile node and correspondent node. Here an attacker can send the false Binding Update message to fool mobile host, home agent or the correspondent node. And so route optimization has introduced new scope for an attacker by sending malicious Binding Update and thus produced security vulnerabilities to mobility protocols.

To prevent these attacks two of the main solutions are cryptography and authentication. Cryptography allows the transmitted data to be in encrypted form resulting in non-readable form of the intercepted packets. Only the authorized party possessing keys will be able to decrypt the message. Second solution is authentication to verify the identity of the user or device one is in communication with. There are different authentication schemes exist however many of them rely on a certification authority and consumes resources. So decentralized authentication mechanisms would be more appropriate for the nature of mobile IP. But in spite of all these facts, the main focus of true communication will be either cryptography or authentication or mixing of both.

Thus the objective of this paper is to analyze the existing security threats and possible security threats that may arise due to existing solutions and compare the existing defense mechanisms to these threats and propose some future solutions that are less complex and concrete. Effort of this work is to remove or reduce the limitation of existing defense mechanism and discuss their pros and cons upon previous solutions. That is the focus of this paper is on authenticating the binding updates.

1.1 Related Work
Major threats which are possible in mobile environment as bombing attack, man–in–middle attack, traffic redirection attack, replay attack, reflection and amplication, home agent poisoning etc. These attacks may be serious for data, resources of mobile nodes as well as network resources and thus can break the main principle of network security and also degrades the performance of network and network components.

Different researchers have tried to find the solution for these security threats for example P. Nikander et al. [3] explain the Mobile IP version 6 route optimization security design background. J. Arkko et al. [4] discusses how to authenticate unknown principals without trusted parties. D. Hu et al. [5] describes the security threats in mobility environment and propose solution with a public Key Infrastructure (PKI) and secret key based approach for it. But there is a lack of concrete solution to mitigate the attacks (existing as well as new possible or identified threats).

All solutions are based either on encrypting the packet or to authenticate the user identity. There are several schemes are proposed to mitigate these threats against the vulnerabilities of mobility protocols, such as cryptographic generated address provide the user identity to authenticate user and similarly for binding update (BU) authentication, return routability protocol is used to reconfirm authentication from different routes. IPSec protocol used in mobile environment requires true relationship between communicating entities and thus provide secure tunnel. But these protocols do not provide a complete solution and have several limitations. Cryptographic generated address does not verify whether the authenticated node is reachable or not and whether the fresh packets are coming or not and also does not any cookie type security for fast access, so only cryptographic generated address technique can't be the only solution. The return routability protocol can be breached if the attacker is on the path between the HA and CN. Instead of these techniques if asymmetric key cryptography (which provides public, private key combination and digital signature as security between communicating nodes) is used it takes high processing power and requires certification authority with infrastructure. And asymmetric key cryptography also causes latency problems due to its slow speed. IPSec protocol works securely but that has a limitation and works if the nodes have a true relationship in between them. So there is a need of computationally less expensive and low latency solutions to mitigate security attacks with low processing power in the way that objective for seamless connectivity of mobility protocol is not affected. But still there is a hope in which only the advantages of the protocols can be taken into account means protocols combination can be used as a complete and concrete solution.

In this paper, Section 2 describes the Mobile IP protocol architecture in brief. In Section 3, we illustrate the possible security vulnerabilities and threats relating to mobility protocol. In Section 4, existing defense mechanisms are analyzed critically, followed by some proposed changes to the existing mechanism. Section 5 describes the comparative analysis of different protocols with their advantages and limitations. Finally, Section 6 has the concluding remarks.

2. NETWORK ARCHITECTURE FOR ROUTE OPTIMIZATION

When a mobile node starts communication by sending packets to the correspondent node, Home Agent (true relationship between mobile node and its home agent) intercepts the packets through an IPSec secure tunnel and forwards them to the correspondent node. When the mobile node moves to a new location, mobile node tells about its new current location called as care-of address (CoA) to the home agent (HA). It causes HA to update the secure tunnel so that packets are routed to and from the new CoA. Authentication and encryption of the binding update (BU) and the following binding acknowledgement (BA) are possible due to preconfigured IPSec security association in tunnel-mode between the mobile and the home agent. But this routing is not optimal and so Route Optimization (RO) technique is used in which MN sends BU directly to correspondent node (CN) and tells CN about its CoA. But there is a need to authenticate that BU among them. To implement this Internet Engineering Task Force (IETF) proposed Mobile IP which aims mainly two problems [6] at the same time:

i. First, Mobile IP allows transport layer sessions (TCP or UDP) and IPSec security associations to continue between the mobile and other hosts even if the underlying host(s) are roaming and changing their IP addresses.
ii. Second, it allows a host to be reached through a static IP address (home address) for new connections.

The first problem matters in case if protocol is stateful, but does not affect stateless protocols such as HTTP. Since stateful protocol saves the state and important parameters for ongoing session to make communication fast. The second problem is most important for servers but not client computers. The route optimization [8] protocol is shown in Figure 1(b). BU may be sent either when the mobile has data to send to CN or when mobile receives the data from CN and mobile node moves from one network to another. When a mobile node changes its current location, it sends BU initial message to CN which contains mobile's home address (HoA) [9] and current care-of address (CoA). The CN node then verifies the initial update message is sent by authenticated user or not, if it is authenticated CN sends some keygen token to MH. MH then generates a binding secure symmetric key and hashes the BU and device information with that binding key and send it to CN. CN after confirmation sends the binding acknowledge (BA) and stores the new location information in its binding cache for future communication but cache may not be updated, so cache needs to be refreshed after every few minutes to continue communication even if the mobile stays at the same CoA. In case if cache entry expires then the same procedure of BU and BA will start again and it continues in this way.

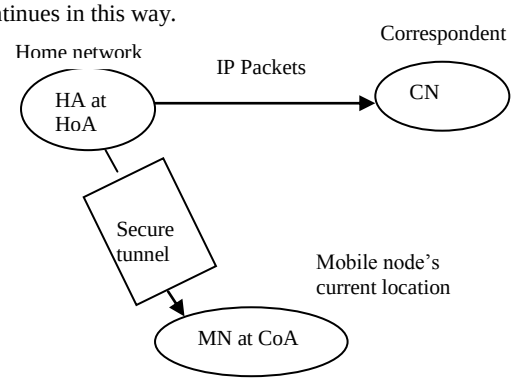

Figure 1(a) Before Mobile IPv6

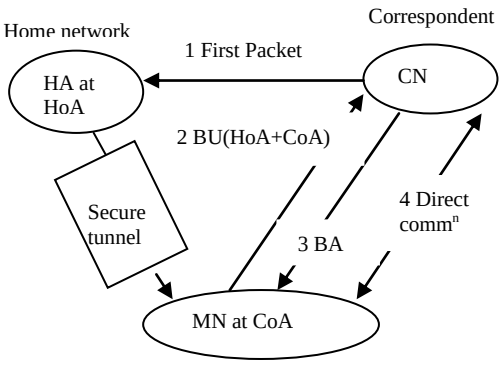

Figure 1(b) after route optimization

The transparent mode of Mobile IPv6 operation is shown in Figure 1(b). Only one packet is sent via the unoptimized route. But after the binding has been created, the mobile node and the correspondent node can communicate directly. A mobile that is about to send a packet to a correspondent uses the CoA as the source IP address and inserts the home address destination option (HAO), which contains HoA in it, in a type-2 routing header (RH) after IP header. When the CN receives the packet, it overwrites the source IP address with the HoA from the HAO, and thus re-creates the original packet. But actual current address is CoA so when CN sends the packets to the mobile it contains the HoA in a type-2 routing header (RH), it compares this destination address against the HoA in its binding cache. If a binding entry exists in the cache memory, it replaces the destination IP address with the actual destination CoA and inserts the RH after the IP header. The mobile node after receiving the packet, copies the HoA from the RH header back into the destination address field and removes the RH, thus re-create the original packet. In this way, upper layers in OSI network model including IPSec and the transport layer are made transparent for mobility. And upper layers always see HoA for mobile node. That is, the source address of outermost IP header always belongs to the subnet from which the packet is sent and thus packet is not dropped by ingress filtering. Thus HAO and RH provides the tunneling header for direct communication among MN and CN.

3. ATTACK ON MOBILE IP PROTOCOL

Mobility protocols, because of lack of secure infrastructure, may lead to so many threats that must be checked out for mobile nodes communication. All attacks are concerned with false binding updates sent in route optimization. An attacker who is in path between MH and CN can take advantage to spoof the address and he either can redirect the traffic or can hijack the session which results in Denial-of-Service attacks. So there are so many attacks are possible but those major attack which should be prevented in network for traditional networks are discussed here as Traffic Redirection Attack, Connection Hijacking or Man-in-the-Middle Attack, Bombing Attack, Replay Attack, Reflection and Amplication Attack, Home Agent Poisoning, Resource Exhaustion and State Storage Exhaustion.

3.1 Traffic Redirection Attack

An attacker sends a false BU to the CN while CN is communicating with the authenticated mobile node and claims in BU that current location of MH has changed to a fake receiver IP or a non existing receiver. In this case if CN accepts the BU considering it authenticated due to lack of security measures, it will redirect all the ongoing packets to the address of fake receiver considering that address as CoA of MH and MH will get response as denial of service. In case, if the redirected node does not exist, then the message "destination host not reachable" is sent to the correspondent node and so correspondent node will stop to send the traffic further to the mobile node. But still there are some servers as correspondent node that will continue to send the traffic to the non existing mobile node. Even if the data is encrypted by any means, an attacker can redirect the traffic, because BU is transparent to upper layer and only thing is required the IP addresses of the communicating nodes. Therefore, nodes with well-known IP addresses, such as public servers, DNS servers or file servers are more vulnerable to such attacks. Figure 2 shows how the communication is redirected towards the third user by sending false BU.

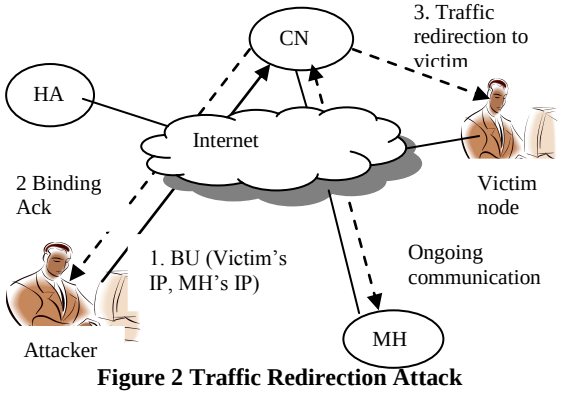

Figure 2 Traffic Redirection Attack

3.2 Connection Hijacking Attack

An attacker sends a false BU to the CN while CN is communicating with the authenticated mobile node and claims in BU that current location of MH has changed to its own IP. If such malicious BU is accepted by the CN, it will start sending packets to the attacker's IP. The attacker now will be able to learn the information of the message if message is not encrypted and so can modify the information before forwarding it to the MH. Such intermediate attacker called as man-in-middle getting all-important private data which was for the victim (MH) without the knowledge of the CN and the MH. Even if the data is encrypted an attacker can change or redirect the encrypted data while it is not able to learn the data. In traffic redirection if victim node is also an attacker and after intercepting the packets, sends them to MH and similarly to CN, then it becomes a connection hijacking attack.

3.3 Bombing Attack

Bombing attack may cause due to false change in current location through BU from attacker's actual IP to victim's (MH) IP. In this attack, an attacker is MH itself, first starts to download the data from server (CN) after performing TCP handshake and note down the sequence number of ongoing communication. And then he sends a forge BU involving victim address as care-of address. If this BU is accepted by CN a huge amount of unsolicited data traffic are redirected to the victim node (or a network) to degrade its performance as well as to waste its bandwidth. Thus while the BU is authenticated, but still it is a fake one because of lack of verification of care-of address. So an attacker may exploit real-time streaming servers which are very common and known for this kind of attack. Fig. 3 shows the bombing attack on a MH which overwhelms MH with unsolicited data packets and degrades its performance.

But when data packets are forwarded towards the victim node, victim node will not accept those (streaming data) packets which are unknown for the victim's machine and so no acknowledgement will be sent by victim to the server or CN for those unnecessary packets, thereby the communication is stopped. But because it was an attacker that had made the connection so he knows the sequence number of ongoing communication and by taking the advantage of this it can spoof an acknowledgement towards the server making a continuous flow of data streams sent to the victim. One TCP Window (may consist

huge data) requires only one acknowledgement and so requires less spoofed acknowledgement to send a large data stream to victim node. Still there is a facility at the transport layer to stop the unnecessary data streams, victim node can send a TCP RESET signal. But it may not work because when the victim node reads the routing header of data packets at the network or IP layer then it encounters a strange address of an attacker as home address, so victim node will not allow to flow the packet up in transport layer and so victim can't change or reset TCP sequence number. So no TCP reset signal will be sent to the server and victim can't stop to coming data streams.

The bombing attack is a very serious and dangerous attack since an attacker may force the server to send a huge amount of unwanted data to any Internet node, the target node also have nothing to stop the data stream, thereby losing its resources along with bandwidth without knowing about the attack. If an attacker does not know an individual address, it may target a network by redirecting the data to one or more IP addresses within its address range. And thus attack becomes severer and called as distributed denial-of-service (DDoS) attack.

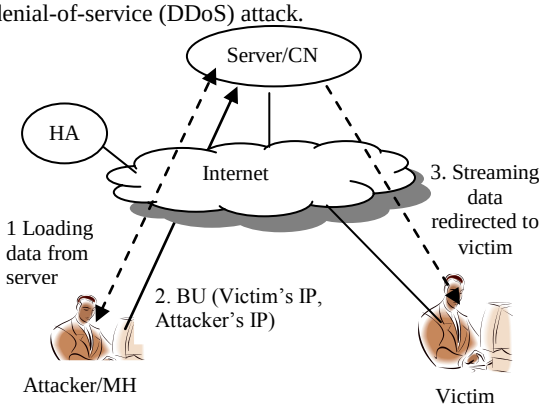

Figure 3 Bombing Attack

3.4 Replay Attack

In this type of attack, an attacker first intercepts the authenticated BU sent by MH to CN and then stores it. Now attacker replays this stored BU later on when MH moves in future to a new location. And thus misguides the CN by interrupting the ongoing communication in between MH and CN. But an attacker may capture the packets for binding update (BU) only if the attacker and the MH are in the same network. BU here is authenticated but replayed and so there is a need to confirm the freshness of packets for BU. Packets start to flow towards another host may be still IP address of another node or not. Though replay attack can be mitigated by introducing time stamping but because time clock for mobile devices may be different, so it is not so useful. Further it was thought that sequence numbered BUs may be used to prove the freshness of packet but still an attacker can intercept the sequence number and delayed for later attack. So to mitigate replay attack there should generate a random number as nonce index in RR protocol that may be known at both sides and so can signify the freshness of packet.

3.5 Reflection and Amplication Attack

In reflection attack, an attacker takes the advantage of the BU security protocol in some earlier design (earlier design of return routability test), because in the earlier design of BU security protocol, to validate the BU authentication CN sends two messages to the MH, one through home agent via secure tunnel and another one directly . CN could initiate route optimization signaling whenever CN receives spoofed initial BU message packet through an attacker, and this can lead to reflection attack. But since packet headers contain home address in original packets, route optimization is initiated at home address that is included in the Home Address option. Fig. 4 shows the reflection attack. When an attacker sends a false BU message to the CN, MH receives every packet sent by the attacker twice due to BU security protocol action. Thus an attacker may amplify a packet flooding attack against a target MH by double. And because attacker address means CoA is not involved in CN messages so MH does not know about the attacker's identity, instead MH thinks about the CN's address as the source address.

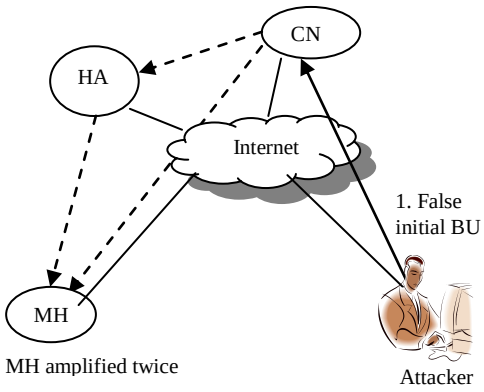

Figure 4 Reflection and Amplication Attack

To mitigate this attack RR protocol was improved in which one additional initial parallel messages as cookie are sent by MH to CN directly as well as through HA which will be discussed in detail in RR protocol.

3.6 Home Agent Poisoning

HA can be made poison if there is no secure tunnel in between the HA and MH .HA keeps the mapping of Home address to CoA for MH. So if a MH moves to a new location, updates are sent to HA to update the database entry, here an attacker may send the fake BU to HA to corrupt its database entry if the tunnel between HA and MH is not secure. Now all the subsequent messages will be sent to the wrong IP address and thus MH will not be reachable by any means through any internet node. Therefore, whenever any CN will ask to HA for the current address of MH, HA will redirect the communication to a wrong address and so communication may be stopped or interrupted by an attacker.

3.7 State-storage Exhaustion

In a stateful protocol, whenever an attacker sends an initial BU message, the CN responds with two secret values by storing them in its memory cache until it receives the authenticated BU. An attacker takes the advantage of this and sends initial BU message so many times to exhaust the state storage and thus prevent the legitimate mobiles from using route optimization with the CN. This attack can be mitigated by making CN stateless and CN stores only the master key value Kcn (as in RR protocol) which is used to compute two secret keygen token values send to HA and MH. CN recomputes the keygen token when it receives authenticated BU. And thus no state-storage exhaustion takes place. It is very difficult to find which end of communication should be stateless, but responder or CN (more often server) is necessitating being stateless.

3.8 Attacks on Access Network or Resource Exhaustion

An attacker first establishes a number of connections with MH by changing its IP address. Therefore, whenever a victim node moves to a new location, it has to send BU to all these imaginary IP addresses to inform them about its current new location and so MH involves itself into huge processing to deal with this unnecessary BUs and all of the resources become busy to handle them. Instead of this an attacker also starts to send fabricated keygen tokens to MH and HA, thus make it busier. By doing this, an attacker makes MH so busy that all the legitimate BU may be blocked which has to be sent by MH to CN. At this time, the attacker can send fabricated BUs to the CNs and the HA, thereby can redirect MH's traffic either to itself or to any other victim. By this attack, an attacker can easily perform traffic redirection attack and session hijacking and all other attacks.

4. SECURITY MECHANISM AGAINST THREATS

Different mechanisms are used to secure the mobile network against threats but all of them should have particular goals to make a secure communication with low resources consumption and infrastructure less authentication. Security in mobile environment can be achieved by cryptography and authentication so that an attacker can't forge BU with false address and also can't look upon the contents of packets.

4.1 Consideration for Designing Protocol against Threats

The goal of the IETF working group was that the Mobile IPv6 protocol should be *at least as secure as the current non-mobile IPv4 Internet*.

First consideration is that in mobile environment every node has its home agent (HA) which has all the information of all the devices in its home network, information of device also includes device sim number, phone number, IMEI number and so on. A static binding is there among the mobile node and HA and so End-to-end encryption and integrity protection with authenticated SSL or IPSec can be provided between them. So there is always assumed a secure tunnel between MH and HA in the analysis of security protocols in route optimization. But in route optimization, the main goal is to focus the direct communication between MH and CN, and since these are mobile nodes, MH and CN do not have static true relationship, so there is a need of infrastructure less secure protocol for authenticating the communication. To implement that some shared key like symmetric or asymmetric key cryptographic algorithms techniques are required, but asymmetric key cryptographic is a slow and power consumption process, symmetric key cryptography approach should be used without infrastructure.

So the first approach should be to validate the user, whether the initiator is authenticated user or a fake user. Secondly binding update should be the valid one and this again reconfirms the user identity. And third approach is to find whether an attacker is not attempting to make CN or MH busy by involving them into fake BUs authentication, since inclusion of home-address destination option (HAO) (it hides the CoA address), mobility is transparent to the upper layers including IPSec and transport layer. Firstly in this paper, the security in between mobile node and home agent will be discussed and then security in between mobile and correspondent node will be considered.

4.2 IP Security Protocol (IPSec protocol)

An IP packet consists of two portions: IP header and the actual data. IPSec [5] defines two IP extension headers: one for authentication and another for confidentiality. So IPSec consist of two protocols mainly as Authentication Header protocol (AH), Encapsulating Security Payload protocol (ESP) and a supporting protocol as Internet Key Exchange Protocol (IKE).

4.2.1 IKE Protocol

IKE [10] is the initial phase of IPSec, where the algorithms and keys are decided. The output of the IKE phase is a Security Association (SA). SA is an agreement between the communicating parties about factors such as the IPSec protocol version in use, mode of operation (transport mode or tunnel mode), algorithms, keys, lifetime of keys etc. once this is done, both major protocols of IPSec (i.e. AH and ESP) make use of SA for their actual operation. Moreover, an SA is simplex, i.e. unidirectional. Therefore, at a second level, we need two sets of SA per communication party that is one for incoming and another for outgoing transmission. Thus if two communicating parties use both AH and ESP, each one will require four sets of SA. So Security Association Database (SAD) is maintained at both communicating node which contains active SA entries.

4.2.2 IPSec key Management Scheme

This key management in IPSec consists of two aspects: Key agreement and distribution. The protocol used in IPSec for key management is called Oakley protocol. Oakley is based on the Diffie-Hellman key exchange protocol, with a few variations. It fulfills our aim for mobility protocols:

a) To create secret keys as and when required.
b) It has features to defeat Replay Attack.
c) It implements a mechanism called as cookies to defeat resource exhaustion (attack by sending forge BU) at victim node.
d) It provides authentication mechanisms to thwart man-in-the-middle attacks.

But there should be true relationship between the communicating nodes to implement key management through this mechanism. So we can ensure key management in between mobile node and its home agent, while not between mobile node and correspondent node. We can use IPSec tunnel mode to provide security between MN and HA. And to provide authentication, integrity, confidentiality of packets IPSec is used with AH protocol or ESP protocol or both.

4.2.3 Authentication Header protocol

AH [11] protocol provides connectionless integrity and data origin authentication of IP packets and anti-replay service using sequence number if required. This protocol consist a cryptographic checksum similar to message digest for the content of binding updates, so Internet Key Exchange (IKE) infrastructure with certificate authentication is required. On receipt of an IP packet, receiver processes the AH first to know about content of packet whether it is tampered or not. AH protocol can be used in tunnel mode or transport mode, but it needs a true relationship between MH and CN. Therefore, use of AH protocol to authenticate the BUs between the MH and CN

is not feasible. But MH has a prior relationship with HA, so IPSec AH protocol is suitable to be used to authenticate BU between MH and HA. Figure 5 shows the use of AH protocol for securing BUs from MH to the HA and to achieve this first Security Associations (SA) are performed between them.

By establishing security associations between MH and HA, both nodes know the IPSec protocol version, mode of operation (tunnel or transparent) and algorithms used with keys etc. And thus a secure tunnel is formed in between MH and HA and these nodes are ready to use AH protocol. Therefore, when MH moves to a new network, it sends BU message to HA either in transport mode in which the authentication header is inserted after the IP header and before the next layer protocol header or in tunnel mode in which AH is inserted between CoA and HoA addresses. This is AH which ensures MH node and it is possible due to the public key infrastructure (PKI).

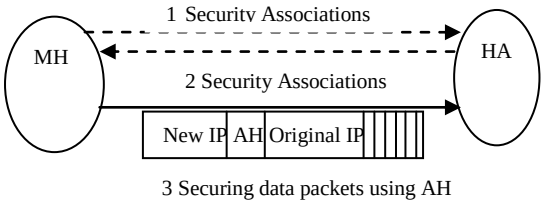

Figure 5 Security association and AH in Tunnel Mode

4.2.4 Encapsulating Security Payload protocol

AH protocol is used between the HA and MH to authenticate the BU and was possible due to a relationship between them. But AH protocol cannot provide confidentiality of data contents. Therefore, Encapsulating Security Payload (ESP) [12] protocol can be used alone to provide confidentiality of data or within AH protocol to provide authentication also. When ESP is used in conjunction with AH, receiving node first check authentication, data integrity and then decrypt the content by extracting keys and algorithm (chosen during SAs were established) associated with ESP. At the time of security association establishment the set of services can be chosen ESP protocol or ESP with AH protocol or simply AH protocol depending on requirement. An encryption algorithm is used to encrypt the data packet by using a key to form a special format with ESP header, trailer and authentication data is combined into a packet and transmitted to the destination as shown in figure 6. ESP protocol can also be used in tunnel or transport mode.

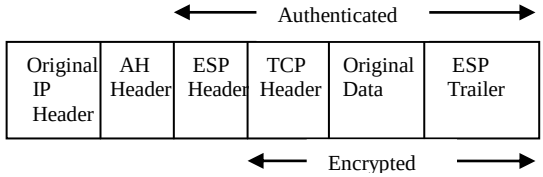

Figure 6 ESP with AH in Transport mode

Therefore, MH and HA can communicate securely for the binding updates because of true relationship between them and so IPSec with AH and ESP can be used between them. Now the main concern is for MH and CN because of no true relationship, so there should be a need to authenticate both of the nodes first and then the data should be encrypted by some binding key through binding update. Return Routability protocol is designed for this purpose as explained in next section.

4.3 Cryptographically Generated Address

Cryptographically Generated Address (CGA) [13] is a suitable use of public key technique without any PKI infrastructure. The use of Cryptographically Generated Address authenticate the user identity by integrating public key of user with the machine IP address and so reduces the chance of attack on a victim node. It is intermediate level security which is above no authentication. This idea was first introduced in a BU authentication protocol known as CAM [14]. In this approach, the least significant 64-bits of user's IP address act as interface identifier which is selected by computing a 64-bit one-way hash of node's public signature key. The main focus of this approach was to bind the IP address of node with its public key to provide authentication of BU. Therefore, whenever a mobile node moves to a new location, mobile host signs the binding update with its private key and sends the public key along with the signed data. The recipient of the binding update it means CN or home agent of CN (to reduce the processing load on CN) hashes the public key which is equivalent to least significant 64-bits of IP address for HoA of MH node. Thus the CN node accepts the BU message if these both values matches and so this technique authenticates both the user identity and BU. But there is a limitation to verify CoA means no checking for the location of CoA in this scheme and may cause bombing attack.

4.4 Return Routability Protocol

Routing in the mobile environment is semi-reliable. Security can be achieved using IPSec between the nodes of trusted relationship. Now this protocol is designed to implement the security between the nodes which don't have true relationship that is between MH and CN. But in order to sniff or intercept a packet, the attacker needs to be on its route. This test is performed to authenticate the BU. This is shown in figure 7.

Message 1(a):
Initially HA receives the Home Test Init (HoTI) as home init cookie C1 (random generated 64-bit number) message sent by the MH and then forwards it to the CN.

Message 1(b):
MH also sends a Care of Test Init (CoTI) as care of init cookie C2 (random generated 64-bit number) to CN directly. Both HoTI and CoTI should be returned back to MH to authenticate the communication.

Message 2(a):
Each correspondent node is assumed to maintain a secret key (20 bytes) Kcn and a key generating function as HMAC SHA1() involving parameters as Kcn, Home (or Care-of) address and some nonce index and a byte index (0 for HoA and 1 for CoA) to calculate a MAC (message authentication code) involving a secure cryptographic hash function SHA-1. The first 64-bit output of function is used as keygen token k1 as h(Kcn,HoA,0) and k2 as h(Kcn,CoA,1) send by CN in HoT and CoT as return messages to MN. So CN sends HoT (home init cookie C1+ home keygen token K1 + home nonce index) to HA and HA forward it to MH.

Message 2(b):
CN also sends CoT (care-of init cookie C2 + care-of keygen token K2 + care-of nonce index) to MH directly. Nonce (random generated number) in HoT and CoT is

used to prevent the replay attack to tell the freshness of packet.

Message 3:
MH, after matching the received cookies as send by it in HoTI and CoTI, hashes both the home keygen and care-of keygen tokens together and results in a 20-byte Kbm (binding management key) using the SHA-1 function. Then MH records the value of Kbm as h (K1, K2) and the nonce indices correspond to HoT and CoT messages sent by CN, and use them in the binding update.

Message 4:
After getting authenticated binding update (BU) from MH, CN sends a binding acknowledgement (BA) using same key as in BU to MH and communication starts among them at optimized path.

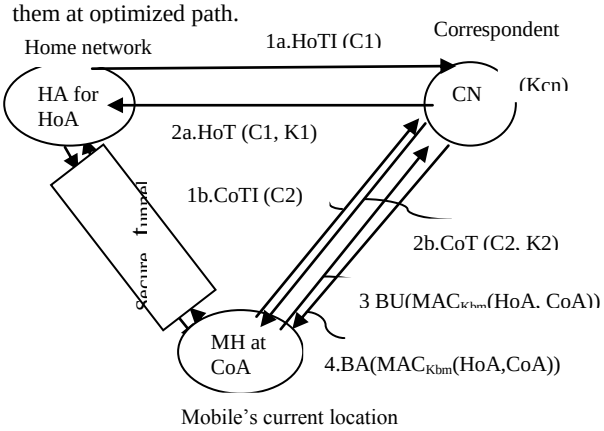

Figure 7: Return Routability Test Protocol Working

Because the key sent by the CN is again used by MH to send binding update to the CN so it is called return routability test. In this way, the CN node verifies that the mobile is able to receive messages at the home address.

Limitations-

1. Because the nodes are mobile so there is no prior relationship or security association exists between these nodes. An Attacker which is in path between CN and HA can act as a mobile node and can sniff all the packets and it can capture the keys in between path and can send his fabricated keys to CN and HA and thus can harm the reliability of this protocol by spoofing the BU.
2. Vulnerability for spoofing BU is also possible when the CN is also another mobile node at an access network which is insecure. For that case, an attacker in such network may capture the keygen tokens to spoof BU. Channel between the HA and MH is assumed to be secure to send the right key to the MH.
3. Key sent in communication as plain text that is not encrypted and so attacker in between path can read them easily.
4. The two reachability tests can lead to a handoff delay unacceptable for many real-time or interactive applications such as Voice over IP (VoIP) and video conferencing.
5. Finally, periodically refreshing a registration at a correspondent node implies a hidden signaling overhead.

There are some advantages:

1. The number of potential attackers and targets are reduced. The attacker must be on the route of the hijacked connection. That is in between path of CN and HA.
2. The RR protocol uses less CPU processing power since it uses inexpensive encryption and light one-way hash function unlike other complex authentication method.
3. It does not store the state until CN has authenticated the MH, while it stores the key of their communication.
4. The RR protocol uses nonce (home keygen token) to avoid replay attack since nonce (random generated) in token also tells the freshness of the BU. On the other hand, sequence numbered BUs can be interrupted by an attacker after looking on sequence number.
5. The RR protocol also verify the location of CoA to authenticate BU, this can be used to overcome the Bombing Attack in which authenticated mobile node can send false care-of address in forge BU.
6. Initial messages are directed by MH as cookie (without init cookies anyone could spoof the HoT and CoT messages and thus can determine the value of the binding management key) prevents the reflection and amplication attack because MH initiates BU authentication to avoid reflection and the correspondent sends as many as messages as it receives to prevent amplication.
7. Correspondent node is stateless (prevents stage-storage exhaustion) because it responds according to received messages as HoTI with a HoT and CoTI with a CoT.

4.4.1 Mitigation of vulnerability:

Vulnerability in Return Routability protocol is due to the presence of an attacker in between the path of CN and HA, but this vulnerability can be mitigated if the correspondent is also another Mobile IPv6 mobile node. That is CN also has a secure tunnel with it's HA and correspondent node's HA will communicate to the mobile node's HA. So in this case, CN should tunnel the HoT message through its own home agent. Thus it prevents the attacker to spoof the packets or BU at the correspondent node's local network and also correspondent network is also assumed to be secured (Note that IPSec tunneling can be used between nodes to router as well as router to router provided they have a true relationship). But it will produce latency problems and delay will become a problem. It is shown in figure 8.

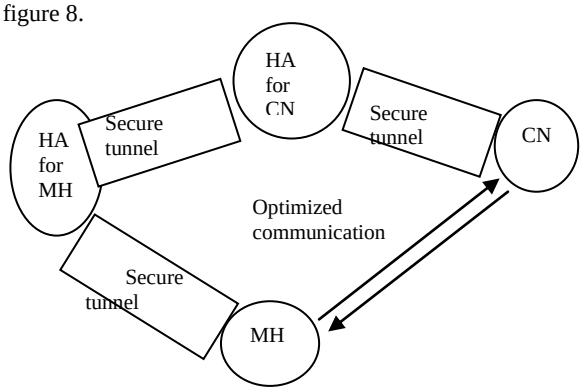

Figure 8: RR protocol through secure tunneling on both sides

4.5 Ingress Filtering:

Ingress filtering means to deploy a gateway or router which checks upon all the ongoing traffic to and fro from the local network. It act as a firewall that checks the source addresses of all packets that are leaving the local network and drops those ones which are not originated from the local network. This can limit the number of potential attacker and their targets. But ingress filtering to be effective if it is applied on the attacker's local network because an attacker's false BU will be filtered out by the gateway in this case. But it can't protect attack targets to victim's network. Also there is a problem in Mobile IPv6 that it uses care-of address as sub-option means sending a false care-of address without spoofing source address. Such an address is not subject to inspection by ingress filtering and would have to be verified through other means. But still ingress filtering can be used to reduce the potential attacks.

4.6 Stateless Mobile Nodes (CN)

CN node should be stateless for receiving and replying to BU messages, otherwise an attacker can exhaust the memory or resources containing legitimate states and then can send fake BU to take advantage of exhaust memory. Therefore stateless [15] approach can prevent the corresponding node from Denial of Service attacks by malicious agents. But to make CN stateless, the BU will have to contain enough information so that accounting can be done for legitimate BUs which on the other hand may delay the communication process.

4.7 Time Bound Binding Update

It is better to limit the binding entry lifetime to mitigate the attack based on the spoofed binding update, rather than complete stateless or stateful binding cache of CN. This approach may reduce the delay as it was in case of stateless protocol. As a result, binding entry is removed from the cache of the CN, if it is not refreshed after some time or any further BU is not received. Therefore, the attacker cannot perform replay attack and can't take advantage of the old binding entry when the MH is inactive for some time. But still refreshing binding cache again and again causes the wastage of bandwidth and network resources of the MH and the CN or HA, and sometimes in legitimate situations.

5. Analyses of Security Protocols

Security protocols discussed above focus security between MH and CN, MH and HA. Because MH and HA have true relationship, they use IPSec protocol security which provides them authentication of data origin, integrity of data, confidentiality of data using AH and ESP protocol in transparent mode or tunnel mode. While the security between MH and CN uses less complex protocol with less computation using one way hash function known as return routability protocol. To mitigate the different kind of attacks, there is a need of different approach, but there is a need a concrete less complex protocol which can mitigate all kind of attacks. Based on above discussed protocol, an analyses is made to security protocol whether they are able to mitigate different possible threats, this is shown in table 1 given below.

From the analysis of above table, it was analyzed that no one protocol is suitable to secure network from all the possible threats, but deep analyses tells that if we combine the advantages of two or more protocols, a concrete solution may be achieved. If we combine CGA approach with return routability protocol, then both the user identity is authenticated and also CoA is verified during the return routability binding update authentication. So CGA + Return Routability Protocol after combination providing the less complex, PKI infrastructure less solution which is suitable for low end devices. It is the best possible solution till now.

6. Conclusions

Today all the electronic gadgets for communication are becoming mobile day by day. So to compete this time, we need to design mobility protocols that are more reliable, secure and too fast. So in this paper, we have explained different mobility protocols and security threats available in mobile node environment. So on the basis of analysis of security of mobility protocols, it is concluded that infrastructure less mobile node requires the mobility protocols which are less complex and efficient, consumes low power that is less complex algorithms and have a low latency solutions. Instead of this we should also consider the factor as dual identity on one mobile node as well as static node along with mobile node, but all of these concerns should have a balance with security and efficiency of device.

Table 1 Comparison of different protocols for mobile security

Security protocol	Threats mitigated	Advantage	Limitations
IPSec protocol	Attack on BU, Home Agent Poisoning and all kind of threats	Authentication of data origin, Integrity and Confidentiality of data using AH and ESP, provides secure tunnel between MH and HA	Requires true relationship between nodes, so MH and CN can't use this protocol to authenticate BU.
CGA protocol	Spoofed BU, Traffic Redirection attack, Connection Hijacking	Public key is associated with IP address of MH	Do not check for CoA, so vulnerable to Bombing Attack
Ingress Filtering	Spoofed BU	Filter spoofed BU if applied attacker's network, reduces potential attackers	IPV6 uses CoA as sub option, so ingress filtering not effective
Stateless Mobile Nodes	Resource exhaustion, Spoofed BU blocking legitimate BU, DoS attack by resource exhaustion	Attacker have to send legitimate BU after some time again and again and can't take advantage of previous stored state	Bandwidth wastage, Mobile node have to keep information about legitimate BU.
Time Bound BU	Resource exhaustion, Spoofed BU blocking legitimate BU, DoS attack by resource exhaustion	Attacker can't take advantage of previous stored cache entry when MH is inactive for some time.	Bandwidth wastage, sometimes entry expires for legitimate user also.
Return Routability Protocol	Redirection Attack or Connection Hijacking Attack on BU (MH-CN), Replay Attack, Bombing Attack, Reflection and Amplication Attack.	Reduces the potential attackers, requires less computational algos, stateless CN, verify location of CoA.	Can't ensure security if attacker is on path between CN and HA

7. ACKNOWLEDGEMENTS

I would like to thank my supervisors for helping me and putting up with Dr. Maninder Singh, HOD, CSE Dept. and Mr. Sumit Miglani, Assistant Professor, CSE Dept., Thapar University, thank you for taking me on as your student and guiding me to this point. Special thanks to my parents and friends who supported me and guided me as I need any kind of help.

8. REFERENCES

[1] D. Johnson, C. E. Perkins, and J. Arkko, "Mobility support in IPv6," IETF RFC 3775, June 2004.

[2] Hesham Soliman. Mobile IPv6: Mobility in a Wireless Internet. Addison-Wesley, 2004.

[3] P. Nikander, J. Arkko, T. Aura, G. Montenegro, and E. Nordmark, "Mobile IP version 6 route optimization security design background," IETF RFC 4225, Dec. 2005.

[4] J. Arkko and P. Nikander, "How to authenticate unknown principals without trusted parties," in Proc. of the 10th International Workshop. Security Protocols. Cambridge, UK. Springer, Apr. 2002, pp. 5–16.

[5] D. Hu, D. Zhou, and P. Li, "PKI and secret key based mobile IP security," in International Conference on Communications, Circuits and Systems, Guilin, China, June 2006, pp. 1605–1609.

[6] Tuomas Aura, Michael Roe," Designing the Mobile IPv6 Security Protocol", Vol. 61 no. 3-4, March-April 2006, Network and information systems security.

[7] S. Thomn and T. Narten. 1Pv6 Stateless Address Autoconfiguration. Internet Engineering Task Force, Dccember 1998.

[8] Pekka Nikander, Tuomas Aura, Jari Arkko and Gabriel Montenegro, Mobile IPversion 6 (MIPv6) route optimization security design. In Proc. IEEE VehicularTechnology Conference Fall 2003, Orlando, FL USA, October 2003. IEEEPress.

[9] Christian Huitema, Routing in the Internet. Prentice Hall, 1995.

[10] C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)," IETF RFC 5996, September 2010.

[11] S. Kent, "IP Authentication Header," IETF RFC 4302, Dec 2005.

[12] S. Kent, "IP Encapsulating Security Payload (ESP)," IETF RFC 4303, Dec 2005.

[13] T. Aura, "Cryptographically Generated Addresses (CGA)," IETF RFC 3972, March 2005.

[14] G. O'Shea and M. Roe, "Child-proof authentication for MIPv6 (CAM)," ACM Computer Communications Review, vol. 31, no. 2, April 2001.

[15] Thomas Narten and Richard Draves. Privacy extensions for stateless address auto configuration in IPv6. RFC 3041, IETF, January 2001.