Security Vulnerabilities and Protection Mechanisms of Mobility Management Protocols

Md. Shohrab Hossain
Mohammed Atiquzzaman
School of Computer Science
University of Oklahoma, Norman, OK 73019
shohrab@ou.edu, atiq@ou.edu

William D. Ivancic
NASA Glenn Research Center
Cleveland, OH 44135.
wivancic@grc.nasa.gov

Abstract—Mobility protocols are originally proposed to support ongoing Internet connectivity of hosts or networks in motion. However, the requirement of seamless connectivity in mobile environment and use of route optimization between the communicating nodes have introduced several security vulnerabilities to mobility protocols. In this paper, we explain with illustrative examples major security threats on various components of the network involving the mobility protocol. We have analyzed critically several existing security solutions that have been proposed to prevent or mitigate security attacks on mobility protocols. We have also identified additional security holes of these existing solutions and propose some simple mechanisms to counter them.

TABLE OF CONTENTS

1. INTRODUCTION

Mobility protocols are originally proposed to support ongoing Internet connectivity of hosts or networks in motion, such as in bus, train, aircrafts, and satellites. Mobile IP [1] is an example of such a mobility protocol that requires signaling among the mobility agents, such as home agent, foreign agent for mobility management to facilitate reachability of mobile nodes. Originally, Mobile IP had no route optimization between the mobile host and the correspondent node. All traffic passed through the home agent and the foreign agent. However, recent mobility protocol, such as Mobile IPv6 has incorporated route optimization between the mobile host and the correspondent node, by informing the current location of the mobile host through updates (known as binding updates), thereby improving the performance of the mobility protocol. However, these binding updates are vulnerable to various attacks since malicious agent might send fabricated binding updates to fool mobile host, home agent or the correspondent node. In short, the requirement of seamless connectivity in mobile environment and use of optimized route between the mobile host and the correspondent node have introduced several security vulnerabilities to mobility protocols.

There have been several earlier attempts to identify potential threats arising from mobility protocols to the public Internet. Kempf et al. [2] outlines the security threats to Mobile IPv6 and explain how the security features of Mobile IPv6 protocol mitigate them. Hu et al. [3] discusses and outlines the security threats for network mobility architecture and propose a public Key Infrastructure (PKI) and secret key based protection approach for it. Elgoarany et al. [4] present a survey on the Mobile IPv6 security through the classification of threats and possible scenarios. However, there is lack of research work that outlines all the possible security vulnerabilities caused by mobility protocols along with detailed analysis of existing defense mechanisms.

In this paper, we explain with illustrative examples major security threats on various components of the network due to the introduction of the mobility protocol. Some of the major threats are traffic redirection attack, man-in-the-middle attack, replay attack, bombing attack, denial-of-service attack, home agent poisoning, etc. These are serious threats for the integrity and confidentiality of data packets, leading to session hijacking and resource exhaustion as well as degrading performance of key network entities.

To prevent or mitigate security attacks, the defense mechanisms aim at choosing solutions that are simple enough to be implemented in mobile nodes with low processing power, computationally less expensive and low latency solutions so that the main objective (seamless connectivity) of mobility protocol is not affected.

Several defense mechanisms have been proposed to protect against the vulnerabilities of mobility protocols, such as return routability protocols for Mobile IPv6, IP security protocols, PKI and secret key-based approaches. However, the existing defense mechanisms suffer from several limitations. The return routability protocol might not work if the attacker

[1] 978-1-4244-7351-9/11/$26.00 ©2011 IEEE.
[2] IEEEAC Paper #1755, Version 2, Updated 10/01/2011.

is on the path between the MH and CN. PKI and secret key-based schemes require the existence of trusted certification authority. Other protocols involving cryptographic operations require higher processing power, resulting in higher handoff latency that may conflict with the design goals related to seamless handoff.

Our objective of this paper is to identify possible security vulnerabilities that arise due to the introduction of mobility management protocols, and critically analyze the existing defense mechanisms to these threats.

Our contributions of this work are identifying possible security vulnerabilities of mobility management protocols, and analyzing and comparing the defense mechanisms to prevent or mitigate these security threats.

The detailed analysis of the security vulnerabilities and possible protection mechanisms along with their pros and cons will help network engineers to design suitable future solutions that are simple, efficient yet powerful enough to prevent or mitigate these threats.

The rest of the paper is organized as follows. In section 2, the Mobile IP protocol is explained 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 the suggestions to protect additional security holes in section 5. Finally, Section 6 has the concluding remarks.

2. MOBILE IP

Internet Engineering Task Force (IETF) proposed Mobile IP [1] which aims at solving two problems at the same time. First, Mobile IP allows transport layer sessions (TCP or UDP) to continue even if the underlying host(s) are roaming and changing their IP addresses. Second, it allows a host to be reached through a static IP address (home address). The architecture of Mobile IPv6 is shown in Figure 1. Each Mobile Host (MH) is usually connected to a network called the home network where an MR is registered with a router called the Home Agent (HA). Each MH is identified by its home address, regardless of its current point of attachment to the Internet.

While away from its home, an MH is also associated with a care-of address (CoA), which provides its current location information. Data packets addressed to a MH's home address are transparently routed to its CoA. Mobile IP specifies how an MH registers with its HA and how the HA routes datagrams to the MH through the tunnel. Data packets from the CN follows an un-optimized route to MH (CN –> HA –> MH) which is sometimes referred as triangular routing(see Figure 1). This leads to longer routing path as well as degraded performance.

To alleviate the performance penalty, Mobile IPv6 includes

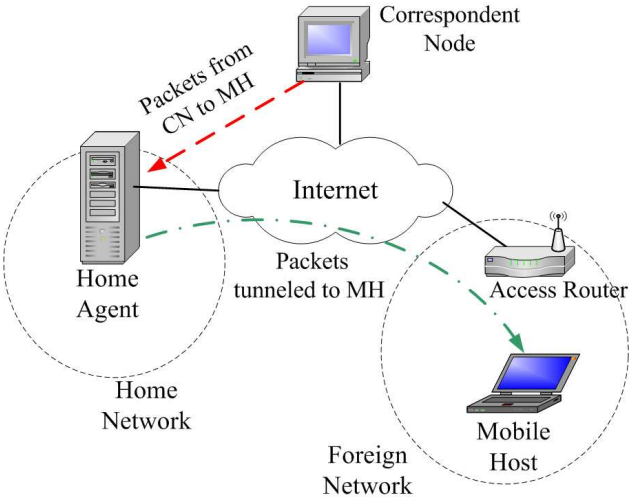

Figure 1. Mobile IPv6 Architecture.

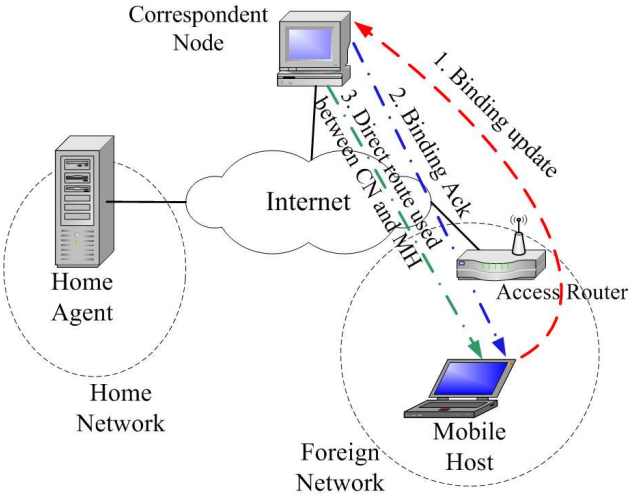

Figure 2. Mobile IPv6 Route Optimization.

a mode of operation that allows the MH and the CN, to exchange packets directly, bypassing the HA completely after the initial setup phase. This mode of operation is called route optimization (RO). Figure 2 shows the MIPv6 route optimization where MH sends Binding Update (BU) to the CN informing the newly acquired CoA along with its home address. The CN, an IPv6 node, caches the binding of the MH's home address with the CoA, and send any packets destined for the MH directly to it at this CoA. Thus using Mobile IP, an MH may change their point-of-attachment to the Internet without changing their home IP address, allowing them to maintain transport and higher-layer connections while roaming.

3. THREATS FOR MOBILE IP

Mobility protocols must protect itself against misuses of the mobility features that enables continuous Internet connectivity for ongoing communication. In Mobile IPv6, most of the potential threats are concerned with false Bindings, usually

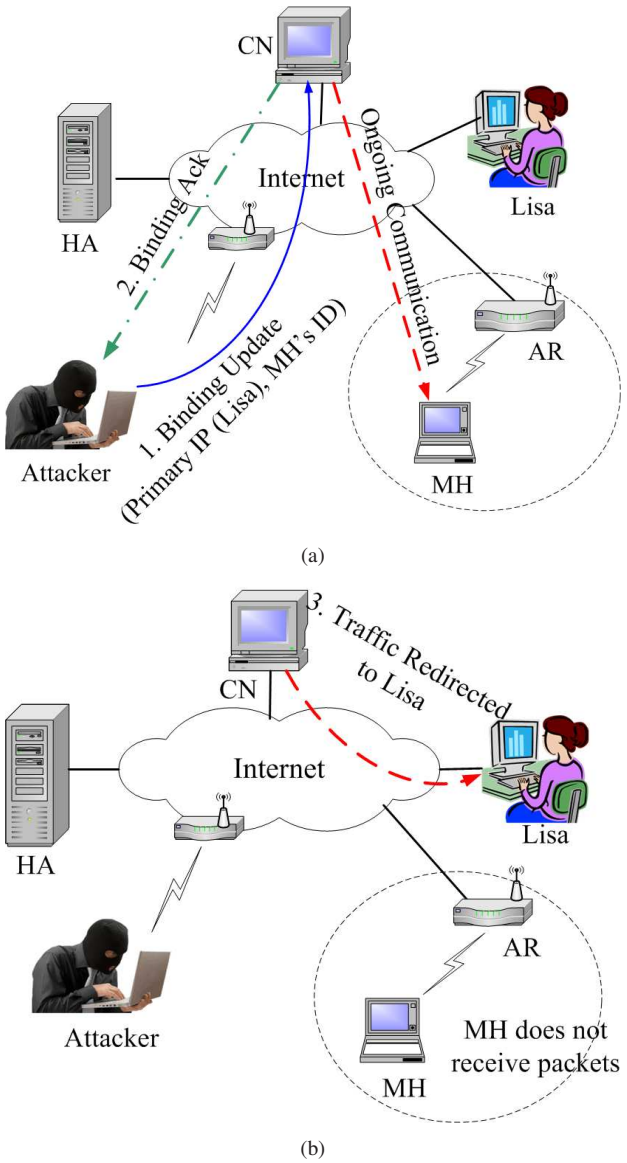

Figure 3. Traffic redirection attack (a) The attacker sends fabricated BU to the CN to modify the binding cache for the MH to some fictitious (Lisa) IP address and CN accepts the BU (b) Traffic is redirected away from the MH to Lisa's IP address.

resulting in Denial-of-Service attacks. Some of the threats include traffic redirection attack, Man-in-the-Middle attack, bombing attack, Home Agent poisoning, resource exhaustion. In this section, we explain the security threats for the Mobile IP protocol with illustrative scenarios.

The unauthenticate binding update can create serious security vulnerabilities. If the binding updates are not authenticated, then the attacker can use spoofed BU, thereby misinforming CN about the MH's current location. This may lead to traffic redirect attack as well as man-in-the-middle attacks, compromising the secrecy and integrity of data packets. These vulnerabilities are due to the fact that mobility is transparent to upper layer protocols and also due to the effort of making things simpler for the low-power mobile devices.

Traffic redirection attack

The attacker may send a fake binding update message claiming that a node (victim) has changed its care-of address due to its movement to a new location. This may happen if the BU is not authenticated. If such BU is accepted by the the CN, it will start sending packets to the new CoA and the victim node will not get any traffic. As shown in Fig. 3(a) the attacker sends fabricated BU to the CN to set the primary IP for the MH to some fictitious IP address (say Lisa's IP address) and CN accepts the BU. As the result, the ongoing session of CN with the MH has been redirected towards Lisa's location as shown in 3(b) and the MH loses all subsequent traffic of the session.

In most cases, data encryption and use of IP Security (IPSec) protocol cannot prevent such attack on data integrity and confidentiality, as route optimization signaling are transparent to IPSec, thereby redirecting the traffic even though the attacker cannot read the encrypted data.

To launch the traffic redirection attacks, the attacker has to know 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.

Remedy: Nodes with frequently changing addresses may mitigate such attacks. However, this addition of security mechanisms to the BU process makes the mobility protocol slower and more complex.

Man-in-the-middle attack

The attacker might send binding update message to the CN telling it to set the primary IP to its own (attacker's) address. If the CN accepts such binding update, CN will start sending the packets to the attacker instead of the MH. The attacker will then be able to learn the confidential contents of the message, may modify the packet before forwarding it to the MH. Thus, the attacker might act as a *man-in-the-middle* getting the all-important private data destined to the victim (MH) without the knowledge of the CN and the MH.

Fig. 4 shows the man-in-the-middle attack that is launched between the communication involving the CN and the MH. First, the attacker sends an malicious BU to the CN saying that the primary IP address of the MH has changed and it is now the attacker's IP address. If CN accepts such BU from the attacker, it will confirm with a binding acknowledgement (see Fig. 4(a)). Since the CN has updated its binding cache due to the malicious BU, it will start sending traffic towards the attacker rather than the MH as shown in Fig. 4(b). The attacker can now learn the confidential contents of the message, may modify the packet before forwarding it to the MH.

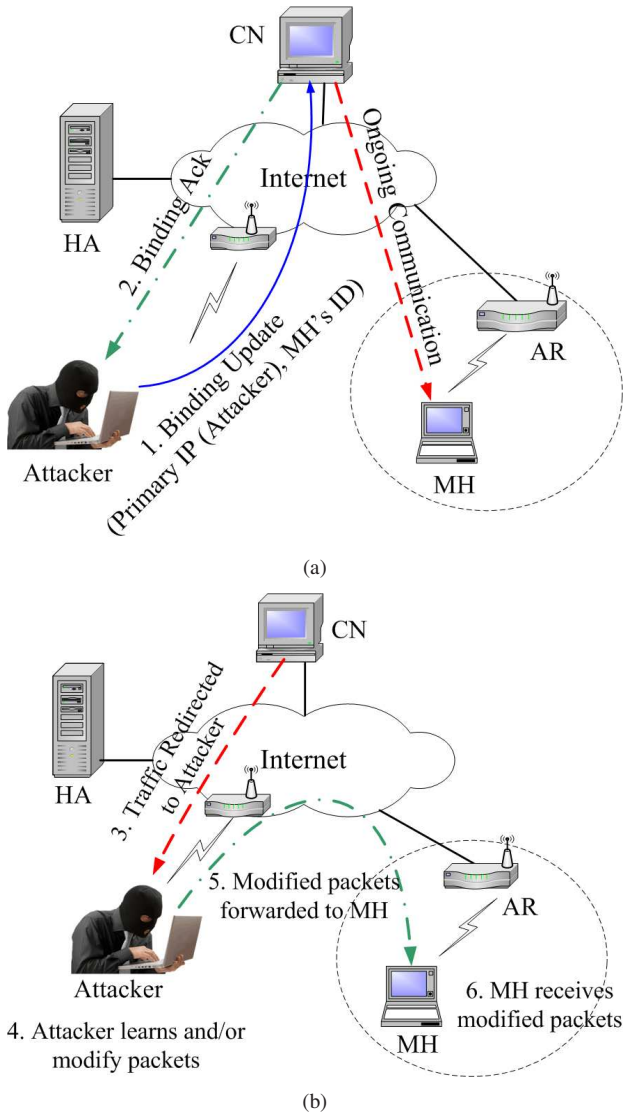

Figure 4. Man-in-the-middle attack (a) The attacker sends fabricated BU to the CN to modify the binding cache of the MH to its own (Attacker) IP address and CN accepts the BU (b) Traffic is redirected to the Attacker who learns the confidential information of the packet and may modify the packet before forwarding to the MH without the knowledge of the involved parties.

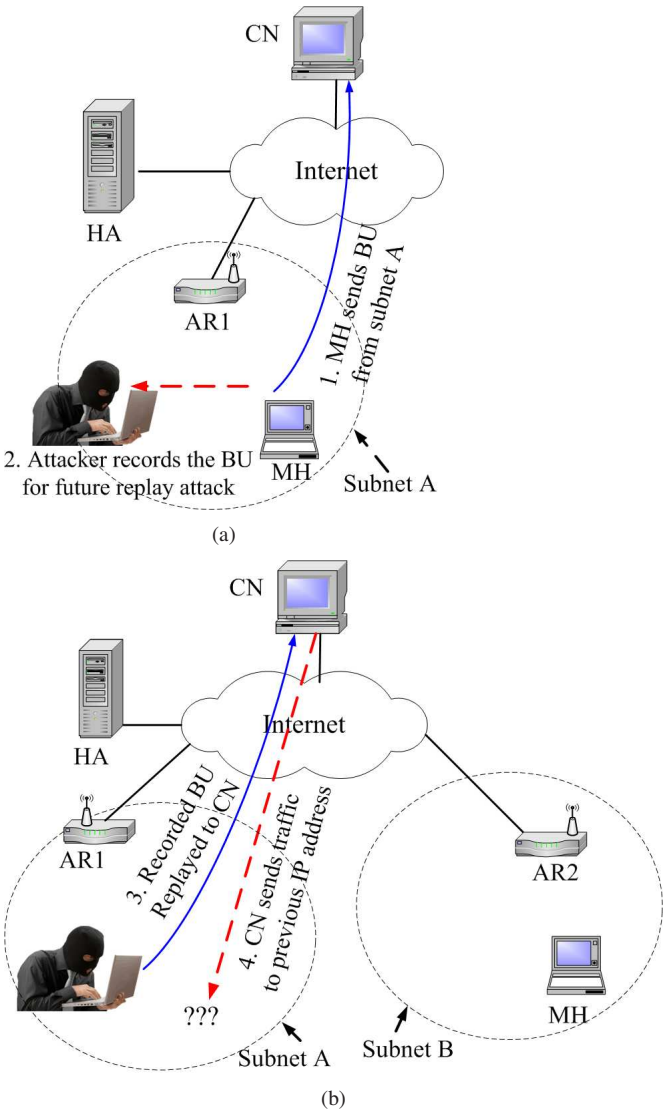

Figure 5. Replay attack (a) When the MH is in subnet A, MH sends the BU to the CN informing its newly acquired care-of address and the attacker records the BU message for prospective replay attack in the future (b) When MH moves to other subnet B, the attacker sends the recorded BU of the MH claiming that MH is in subnet A, thus disrupting traffic away from the MH to some non-existing host.

Replay attack

This kind of attack takes the advantage use of a previously sent (authenticated or unauthenticated) binding update by recording it and later on, replaying it when the victim (MH) moves to some new location, thereby interrupting the communication between the CN and the MH. The attacker may get the opportunity to receive the BU while being in the same radio access network. This attack can work on authenticated updates as well. Therefore, it is difficult to avoid such attacks.

The reply attack is shown in Fig. 5. The MH was first in subnet A in Fig. 5(a) and sends a binding update to CN to add its address to CN's binding cache. Any attacker listening to such BU can record the BU and use that for replay attack in future. In Fig. 5(b), the MH has moved to some new subnet B. Now the attacker may use the recorded BU and replay it, that is, send it to the CN to fool CN. If the CN accepts such replay message, CN would then start sending packets to the old (subnet A) address thinking that MH has again moved to subnet A which is not true. Thus, traffic from CN are redirected to a non-existing IP-address, thereby disrupting the communication.

Bombing attack

In this type of attack, huge amount of unsolicited data traffic are redirected to the victim node (or a network) to degrade

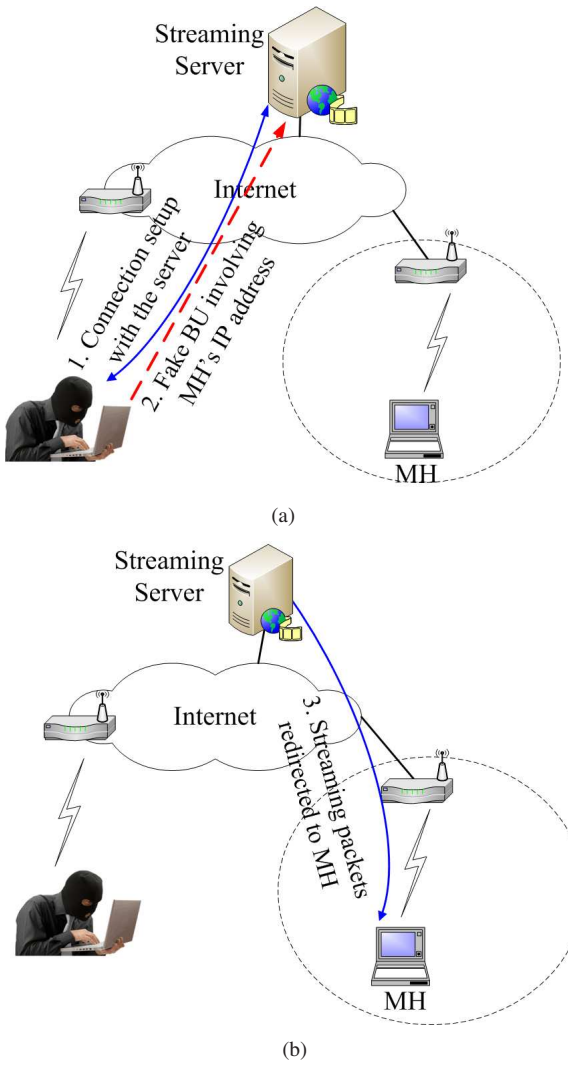

Figure 6. Bombing attack (a) The attacker establishes a connection with a streaming server, later on the attacker sends a fake BU involving the IP address of the MH, (b) The streaming data packets are redirected to the MH that the MH has not requested for.

its performance as well as bandwidth wastage. The attacker may exploit real-time streaming servers for this kind of attack. First, the attacker establishes a connection with streaming server, and starts to download a stream of data. After getting the sequence number, the attacker might claim that it has moved to a new location. The attacker might use the IP address of the victim node in the binding update. As a result, subsequent packets from the server will be directed to the victim node.

Fig. 6 shows the bombing attack on a MH which overwhelms MH with unsolicited data packets and degrade its performance. In Fig. 6(a), the attacker establishes a connection with a streaming server and after some time, it sends a false BU to the server claiming that its IP address has changed. In the BU message, the attacker uses the IP address of the victim MH. As a result, the traffic from the streaming server has

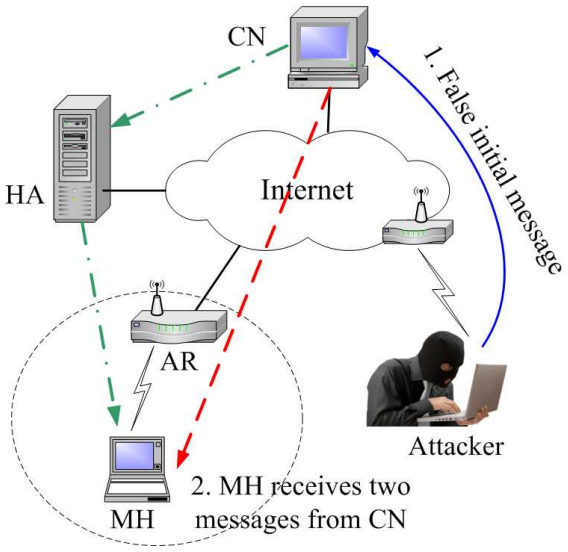

Figure 7. Reflection attack.

been redirected to the MH causing its performance degradation and bandwidth wastage of the MH.

In such attacks, the victim node will not accept those unsolicited (streaming data) packets and therefore, will not send the acknowledgement, thereby stopping the communication. However, the attacker can spoof acknowledgement (towards the server) as it knows the initial sequence number making a continuous flow of data streams sent to the victim. One possible solution of this could be to use the TCP RESET signal by the victim node to immediately stop such flow of data stream. This may not be possible since the victim will always drop the packets immediately without even processing the appropriate header to know the actual destination for which the packets are intended for.

The bombing attack can be very serious since it can target any Internet node with enormous amount of unwanted data and the target node cannot do anything to stop the data stream, thereby losing its bandwidth without any clue to such attacks. This attack may become severer and harmful to the Internet if it is used in combination with distributed denial-of-service (DDoS) attacks.

Reflection attack

In some earlier design, CN could initiate route optimization signaling whenever CN receives packet through HA, and this can lead to reflection attack. Route optimization was initiated to the address that was included in the Home Address option. An attacker can take advantage of this and can send traffic with a care-of-address of the victim and the victim's address in the Home Address option, thereby redirecting RO signaling to the victim. Fig. 7 shows the reflection attack where the attacker sends a false initial message to the CN, thereby inducing CN to send two messages to the MH. As a result, the MH receives every packet sent by the attacker twice due to the

reflection. Thus the attacker is able to amplify a packet flooding attack against a target MH by a factor of two. Moreover, the identity of the attacker of such reflection attacks remains undetected as both the messages arriving at the target have the CN's address as the source address.

Home Agent poisoning

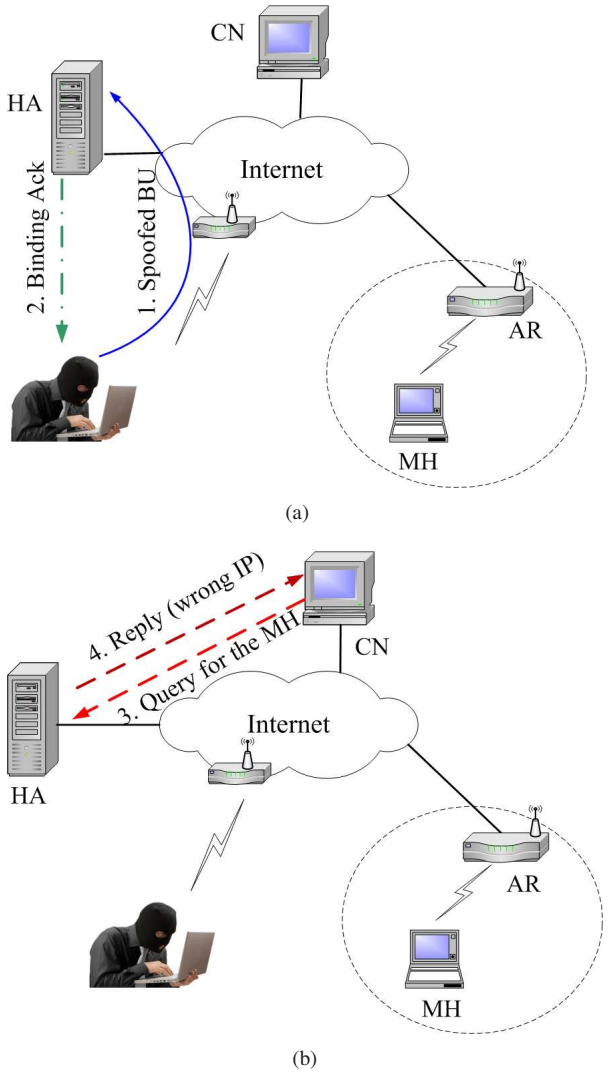

Figure 8. HA Poisoning (a) Spoofed BU send to the HA and the HA updates the entry in the location database for the MH (b) When the CN queries the HA for the IP address of the MH, it receives the wrong IP.

HA keeps the mapping of Home address to CoA of the MH. Therefore, in every subnet crossing location updates are sent to HA to update the database entry accordingly. The entry can be corrupted if spoofed BU is accepted by the HA. This will affect all subsequent communication with that host whose entry has been corrupted and no Internet node will be able to reach the victim node.

Fig. 8 shows the HA poisoning. The attacker sends spoofed BU to the HA (Fig 8(a)) and the HA accepts the BU. Therefore, the subsequent query to the HA by any CN (for the MH) will produce wrong reply as shown in Fig. 8(b).

Attack on access network to block legitimate BU

When the MH enters a new radio access network, it obtains new IP address and sends BUs to the HA and the CNs. Attacker can block MH from sending legitimate BU by launching brute-force attack on the radio link or by a flooding attack. So when the MH gives up sending BUs to the CN, the attacker can send fabricated BUs to the CNs and the HA, thereby redirecting MH's traffic towards the attacker. This could lead to man-in-the-middle attack as well.

Resource exhaustion

Attacker establishes connections with the MH with thousands of fake IP addresses. Thus whenever, the MH moves to some new location, the MH has to send to send BU to these imaginary hosts, thus huge processing power of the MH is wasted while dealing with these unnecessary BUs. This attack cannot be prevented with authenticated BUs. These fake connection will require the victim to keep states for each one of them, wasting its memory as well, resulting in denial of service attacks.

Forged tunnel packets

An attacker may forge tunnel packets between the MH and the HA, making it appear that the traffic is coming from the MH which is not the case. The attacker who is able to forge fake packets of its own, can also modify or fabricate packets that is originated from the MH. In this type of attack, the attacker can even escape detection by avoiding ingress filtering and packet tracing mechanisms.

Attack on security protocols

The attacker may trick MH to participate in unnecessary complex cryptographic operations, using up the resources of the MH. This is sometimes directed to the security mechanisms on the mobility protocols.

Another kind of flooding attack can target MH or CN to induce authentic but unnecessary binding updates and this type of attack is possible regardless of authentication protocol. The worst thing is that this attack on security protocols becomes severe for strong and expensive protocols. When a spoofed packet sent by the attacker is tunneled to the MH, the MH typically responds by sending BUs to the claimed CN. The CN then accepts the BU as it is a valid one. However, the protocol execution is completely needless and this type of attacks can be repeated for different CNs to exhaust the resources of a single MH, or with one CN address and many MHs to attack a single CN.

4. Defense Mechanisms

In this section, we explain some of the defense mechanisms that can be used to prevent the prospective attacks against mobility protocols. The goals of the defense mechanism are

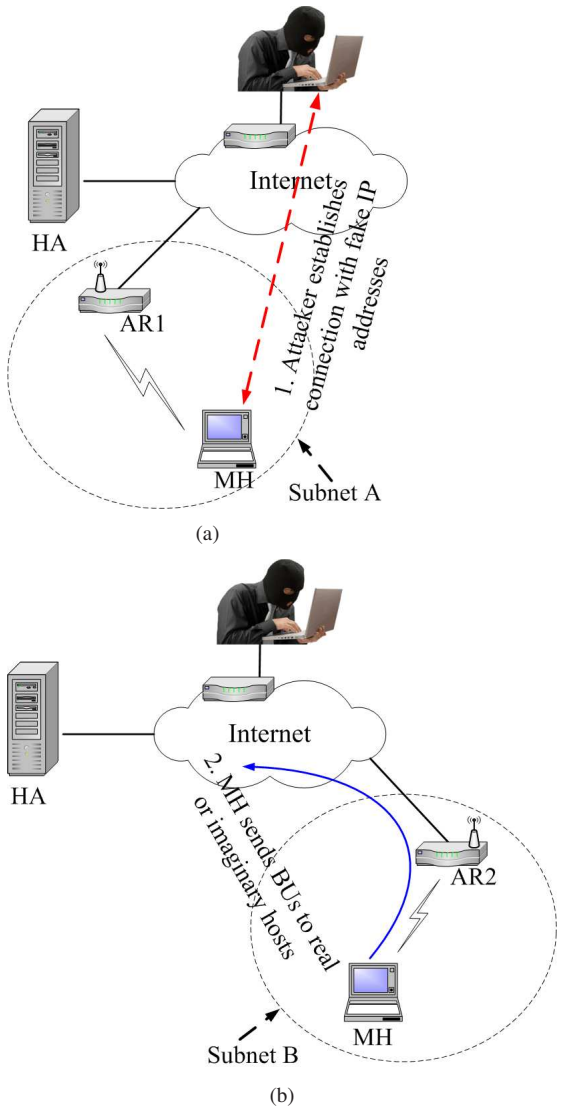

Figure 9. Resource exhaustion of MH (a) The attacker establishes unnecessary connections with the MH using fake IP addresses (b) MH sends BUs to all the fake IP addresses thus wasting its processing power as well as memory.

as follows:

- To prevent or mitigate security attacks.
- Focus on the attacks that are introduced due to mobility of nodes.
- Simple and computationally less expensive to be implemented in mobile nodes with low processing power.
- Low latency solutions.
- To prevent recursive effect due to the security protocol itself.

Design considerations

There are a few design considerations that have impacts on the selection of defense mechanism for mobility protocols. They are summarized as follows.

Infrastructure less approach: To protect against malicious BU leading to traffic redirection and man-in-the-middle attacks, authentication of BU is essential. However, use of strong cryptographic (authentication) protocols require the existence of certification infrastructure, such as IPsec or PKI. As there is no distinction between a fixed IPv6 node and a mobile node, this certification infrastructure is required to authenticate all IPv6 nodes across the public network. However, there is no such existing infrastructure that can be used to authenticate all IPv6 nodes. The deployment of such global infrastructure is neither realistic nor feasible in the current Internet. Therefore, infrastructureless approach can be suitable for authenticating purpose.

Low processing requirement: The processing overhead required for cryptographic operations and/or authentication protocols are relatively high for low-power mobile devices. Therefore, defense mechanisms that avoid such cryptographic operations can be very useful for real mobile devices.

Low latency efficient solution: The main focus of the mobility protocol is to facilitate uninterrupted ongoing communications between the MH and the CN. If the security protocols requires significant amount of time for computation, the connection between the parties may be broken. Therefore, it is desirable that the security protocols are fast enough to meet this goal.

Return Routability protocol

One major concern for security of mobility protocol is the use of unauthenticated and forged binding updates. To prevent such attacks, a node sending a binding update must prove its right to redirect the traffic. The solutions proposed in MIPv6 [1] for this kind attack is Return Routability (RR) test. This approach of RR is used before each binding update message is sent to CN, and they are exchanged among the MH, HA and CN. Fig. 10 shows the message exchange in Return Routability (RR) test. The HA receives the Home Test Init (HoTI) message sent by the MH and forwards it to the CN. It also receives the Home Test (HoT) message sent by the CN and sends it back to MH. Other two messages that are exchanged in the RR test are Care-of Test Init (CoTI) and Care-of Test (CoT) messages between MH and CN.

The first two messages of the test include two 64-bit cookies, the HoTI cookie and CoTI cookie. These cookies are randomly generated 64-bit numbers and they must be returned by the CN in the reply messages, that is, Home Test (HoT) and Care-of Test (CoT) messages. Each CN is assumed to maintain a 20-byte secret key, K_{cn} which is not shared with anyone and this Value of K_{cn} is used as a parameter for the key generating function *HMAC_SHA1()* which is a specific construction for calculating a message authentication code (MAC) involving a secure cryptographic hash function *SHA-1*. K_{cn} is the first parameter of this function and the second parameter is composed of the concatenation of the Home (or Care-of) address, nonce index and a byte x. This byte is 0 and

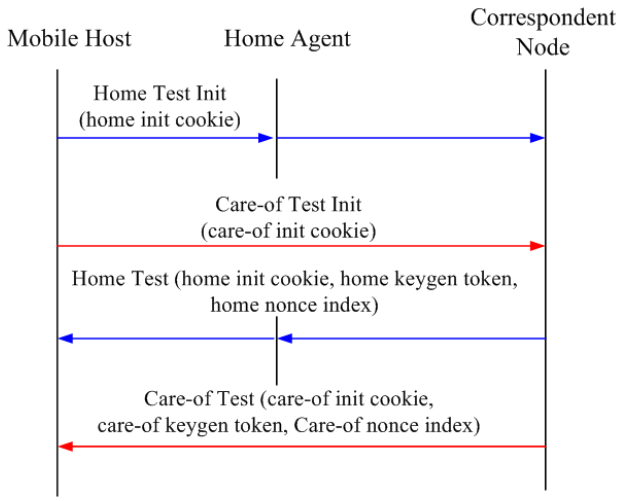

Figure 10. Return routability test in Mobile IPv6.

1 for home address and 1 for care-of address. The first 64-bit of the output of the function is used as the keygen token for the HoT and CoT message.

After receiving both the HoT and CoT messages, the MH first matches the cookies to make sure that they are same as those sent in the HoTI and CoTI messages. The mobile host then hashes both the (home and care-of) keygen tokens together and forms a 20-byte K_{bm} using the SHA1 function. The mobile host records the value of K_{bm} and the nonce indices included in the HoT and CoT messages associated with the correspondent host, for use in the binding update.

Advantages—RR protocol limits the number of potential attackers that can hijack an ongoing session. If RR is not used, any IPv6 node can spoof BUs to redirect traffic as shown in Figs. 3 and 4. The use of RR protocol can significantly scale down such damages.

The RR protocol requires less CPU processing power as it only uses relatively inexpensive encryption and one-way hash functions unlike other complex authentication methods.

The RR protocol is also stateless as the CN does not store a separate state for each mobile. Instead, it stores a single periodically-changing randomly-generated secret key K_{cn} for this purpose and remains stateless until CN has authenticated the MH.

Limitations—The vulnerabilities of the RR method exists on the path between the HA and the CN. As CN can be any node in the Internet, no prior relationship or security association exists between these nodes. Attackers who are on this path or have access to the packets sent on this path can learn the secret that is necessary for spoofing the BU. Such attacks include various DoS attacks, impersonation and eavesdropping, etc.

Another vulnerability is possible when the CN is another mobile node at an unsecured access network. In that case, an attacker in such network may learn the keygen tokens and to spoof binding updates.

The return routability may be subject to race condition though the chance is very low. Return routability process starts after the MH has sent the binding update to the HA. The race condition is possible if this binding update is delayed to reach the HA whereas the HoT message is returned by the CN to the HA. This results in tunneling the HoT message to the wrong care-of address by the HA.

Thus, RR protocol is a relatively weak routing-based authentication method and it does not protect against all possible attacks, rather aims at limiting the number of potential attackers for a particular target, and number of targets a potential attacker can threaten.

Authentication Header protocol

In order to protect against attacks that are based on spoofed binding updates, IPSec Authentication Header (AH) protocol [5] can be incorporated with the mobility protocol. AH protocol guarantees connectionless integrity and data origin authentication of IP packets. It is one of IP security protocols that can ensure that the binding update is originated from the MH, not from malicious agent or attacker. In this protocol, a preconfigured IPsec security association is established between the MH and the HA (or MH and CN) to authenticate the binding update and the following binding acknowledgement. Security associations can be established through Internet Key Exchange (IKE) [6] with certificate authentication.

It is assumed that MH has a prior trust relationship with the HA and IPSec AH protocol is suitable to be used to authenticate binding updates between MH and the HA. However, it might not be so for the BUs between the MH and the CN due to the absence of such trust relationship as the CN can be any IPv6 node in the Internet. Moreover, these exists no such global infrastructure that can be used to authenticate all IPv6 nodes. Therefore, use of AH protocol to authenticate the BUs between the MH and CN is not feasible. Alternative solutions for securing MH-CN BUs might be the use of return routability protocol of Mobile IPv6 or any other infrastructureless authentication.

Fig. 11 shows the use of AH protocol for securing BUs from MH to the HA. First, Security Associations (SA) are performed between the MH and the HA as shown in Fig. 11(a). The SA records the algorithm and parameters controlling security operations. An index parameter called the Security Parameters Index (SPI) is used in security associations. They are referenced by the sending host and established by the receiving host. SAs are unidirectional and two SAs must be established between the MH and the HA for the bi-directional tunnel required for mobility signaling. Once the security association has been performed, the MH and HA are ready to

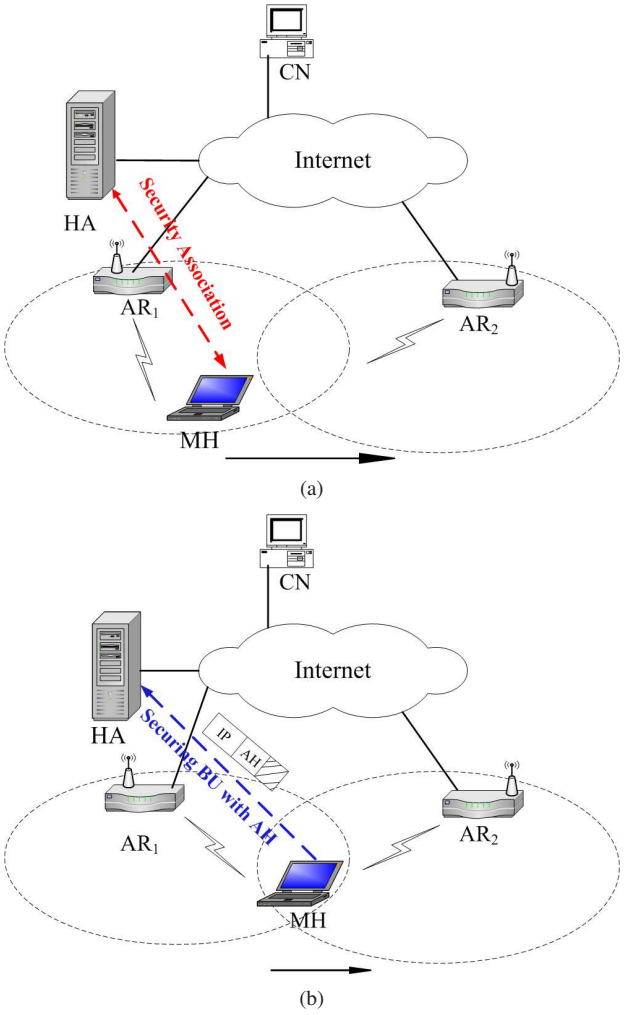

Figure 11. Protecting BU between MH and HA using AH (a) Security association performed between MH and the HA (b) The BU sent by MH is protected by AH.

use AH protocol. Therefore, when MH moves to a new subnet (Fig. 11(b)), it sends BU message. In the BU message, the authentication header is inserted after the IP header and before the next layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode). This ensures the BU is from MH itself, not from any other malicious attackers.

Encapsulating Security Payload protocol

The use of AH cannot ensure the data integrity or privacy of the contents. Therefore, Encapsulating Security Payload (ESP) protocol [7] can be used since ESP can provide confidentiality, data origin authentication, connectionless integrity, anti-replay service and traffic flow confidentiality. At the time of security association, the set of services can be chosen

ESP protocol ensures confidentiality of data by encrypting the datagram. An encryption algorithm combines the data in the datagram with a key to transform it into an encrypted form. This is then repackaged using a special format (with ESP header, trailer and authentication data) and transmitted to the destination. After receiving the encrypted packet, the destination node decrypts it using the same algorithm. ESP also supports its own authentication scheme like that used in AH, or can be used in conjunction with AH. The ESP header is inserted after the IP header and before the next layer protocol header similar to the AH protocol header.

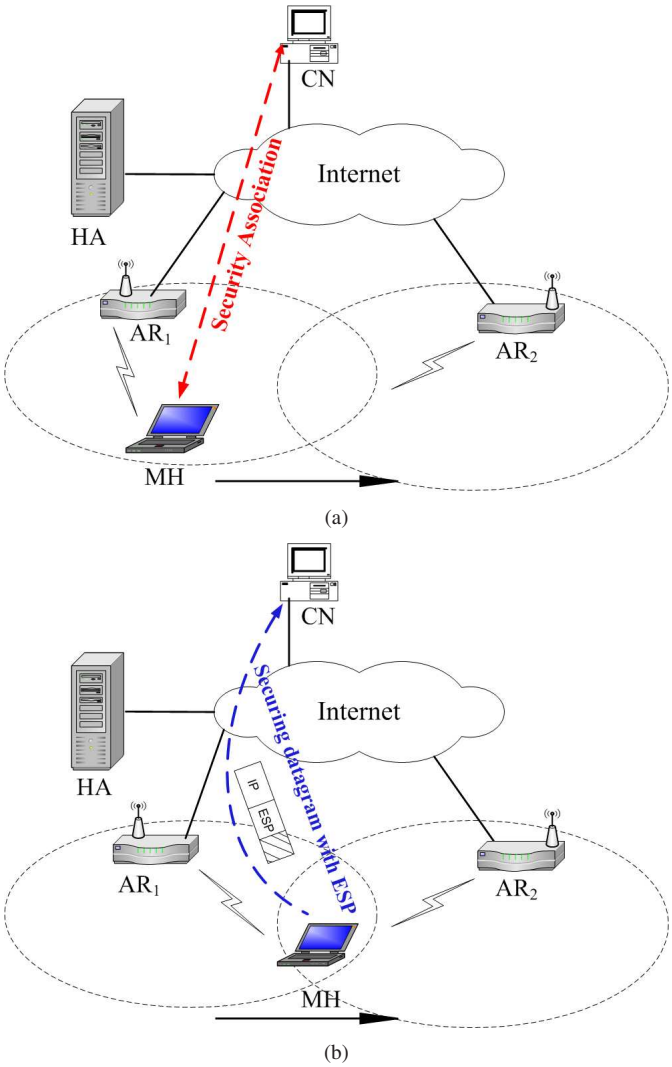

Figure 12. Protecting security and integrity using ESP (a) Security association performed between MH and the CN (b) The datagram sent by MH is protected by ESP header.

Fig. 12 shows the use ESP header for security data packets between the MH and the CN. A security association is performed between the MH and the CN to choose security algorithm and the related parameters in Fig. 12(a). After the security association, MH sends data packets to the CN with proper encryption along with the ESP header as shown in Fig. 12(a), thereby ensuring data integrity and confidentiality.

IKE based schemes

IKE or IKEv2 [6], a key distribution mechanism for Internet community, is commonly used to performing mutual au-

thentication and establishing and maintaining security associations for IPSec protocol suite. To ensure confidentiality, data integrity, access control, and data source authentication to IP datagrams, IPSec maintains state information at the two ends of the data communication. IKE helps to dynamically exchange the secret key that is used as the input to the cryptographic algorithms.

IKE uses DiffieHellman key exchange [8] to set up a shared session secret, from which cryptographic keys are derived. IKE provides very strong security though it requires very complex and power-consuming operations which may be a major concern for low-end mobile devices.

Stateless nodes

The IPv6 node may not save any state for receiving and replying to BU messages. This stateless approach can prevent the corresponding node from Denial of Service attacks by malicious agents causing resource (CPU and memory) exhaustion. To make CN stateless, the BU will have to contain enough information so that accounting can be done for legitimate BUs.

Use of Cryptographically Generated Address

The use of Cryptographically Generated Address (CGA) [9] can reduce the chance of attack on a victim node. This idea was first introduced in a BU authentication protocol known as CAM [10]. In this approach, the least significant 64-bits of the IP address (the interface identifier) is selected by computing a 64-bit one-way hash of the node's public signature key.

In CGA appraoch, the 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 hashes the public key and compares the hash to the address before verifying the signature on the location data. This prevents anyone other than the node itself from sending location updates for its address. The main advantage of this approach is that it provides public-key authentication of the IP address without any trusted third parties or PKI.

Certificate based approach

Another way of authenticating BU is the certificate based approach and it relies on digital signature to authenticate binding updates or the source of the binding update. These approach requires the existence of certification of certification authority or PKI. The CPU and memory requirement for this type approach is usually high.

Limiting binding entry lifetime

To mitigate the attack based on the spoofed binding update, one possible approach is to limit the binding entry lifetime. As a result, binding entry is removed from the cache of the CN, if any further BU is not received. Therefore, the attacker cannot take advantage of the old binding entry when the MH is inactive for some time.

The bad side of such quick expiration (of binding entry) is the wastage of bandwidth and transmission power of the MH and the CN (or HA) in legitimate situations. These messages are absolutely unnecessary resulting in overhead on the HA (or CN), sometimes leading to resource exhaustion.

5. COMPARATIVE DISCUSSION

In this section, we compare major security threats and possible defense mechanism. Table 1 lists the major security threats and corresponding defense mechanisms along with their merits and demerits. We discuss them in the following along with some simple mechanisms to mitigate them.

Among the defense mechanisms of the mobility protocols, the RR protocol is intended to authenticate the BU between the MH and the CN. The IPSec protocols (AH and ESP) can be used for securing the tunnel between the MH and the HA as they have prior trust relationship. The CGA-based scheme can reduce the chance of attack on a victim node and is also infrastructureless. There is always a need for limiting the lifetime of binding entry to restrict the potential attack by unauthenticated binding updates. Finally, the MH or the CN should not store states until authentication to avoid CPU and memory exhaustion by DoS attacks.

Attack on binding updates between MH and HA can be protected by the use of IPSec ESP protocol. This protects against certain types of traffic analysis and provides privacy. However, use of ESP does not protect against misbehaving MH that may use spoofed CoA in BU to launch DoS attacks. Attack on binding updates between MH and CN can be prevented by the return routability of Mobile IPv6. This makes sure that the MH sending the BU has the right to use the CoA. However, vulnerabilities possible if the attacker is on the path between HA and CN.

Traffic redirection attack can be prevented by IPSec AH protocol where the BUs are authenticated using this protocol though privacy and confidentiality are not ensured. This type of attaks can be mitigated if the victim node dynamically changes its IP address or uses CGA. Nodes with fixed IP addresses are more vulnerable to such attack.

Man-in-the-middle attack can be prevented by IKE or PKI-based schemes through strong mutual authentication. These approaches are difficult to break. However, it requires use of complex and expensive cryptographic operations in order to establish shared keys between the parties involved.

Replay attack is usually countered by using sequence number. However, this sequence number must be stored in stable storage between system reboots. Otherwise, replay attack is possible after reboot or turnover at 16-bit boundary.

Table 1. Security threats and corresponding defense mechanisms for mobility protocols.

Security Threats	Protection Mechanisms	Advantage	Limitations
Attack on BU (MH-HA)	IPSec ESP	Protects against certain types of traffic analysis and provides privacy	Does not protect against misbehaving MH that may use spoofed CoA in BU to launch DoS attacks
Attack on BU (MH-CN)	Return routability	Makes sure that the MH sending the BU has the right to use the CoA	Vulnerabilities possible if the attacker is on the path between HA and CN
Traffic redirection attack	AH protocol, CGA, frequently changing addresses	The BUs are authenticated using this IPSec protocol	Privacy and confidentiality are not ensured by AH protocol
Man-in-the-middle attack	PKI and secret key based approach	Difficult to break	Cryptographic operations needed to shared key
Replay attack	Sequence number	It is enough if sequence number can be stored in stable storage	Replay attack is possible after reboot or turnover at 16 bit boundary if stable storage is not available
HA poisoning	AH or ESP	strong authentication	Computationally expensive
Spoofing BU	CGA	Works with a CA or any PKI	Higher processing cost and can suffer from resource exhaustion attacks
Resource exhaustion	Keeping MH or CN stateless	Can avoid DoS attacks	May introduce delay for valid requests
Blocking legitimate BU	MH may keep on trying to send BU	Can avoid HA poisoning or session hijacking	Too much overhead on the MH

The binding entry in the HA can be prevented by authenticating and protecting data between the MH and the HA through the use of IPSec protocol suites, such as AH or ESP protocol. This will provide strong protection mechanism at the expense of CPU power.

To prevent the DoS attacks that can cause CPU and memory exhaustion, the MH or the CN can act as a stateless agent. Therefore, the MH or CN will not have to keep track of the current states of the half-open requests, thereby saving its resources. However, it might have to do more works for the valid requests and thus can increase processing delay.

To mitigate the attack on the MH's radio access network, the MH may keep on trying to send BU message in spite of failures in several attempts. This will ensure the binding entry in the HA or the CN is corrupted by the attackers. However, this will impose additional overhead on the low-end mobile devices.

6. Conclusion

In this paper, we have discussed the security issues relating to mobility protocol. We have explained in details possible security vulnerabilities on various components of the network, and their possible impacts on the Internet. We have also analyzed the existing and possible defense mechanisms that can prevent or mitigate these security vulnerabilities along with their pros and cons. Based on the analysis, several recommendation have been outlined in the comparative discussion section to improve the existing mechanisms. We conclude that the security solutions trade off among the security level, efficiency and processing requirement.

Acknowledgments

The research work reported in this paper was supported by NASA Grant NNX06AE44G.

References

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

[2] J. Kempf, J. Arkko, and P. Nikander, "Mobile IPv6 security," *Wireless Personal Communications*, vol. 29, pp. 398–414, 2004.

[3] 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.

[4] K. Elgoarany and M. Eltoweissy, "Security in Mobile IPv6: A survey," *Information Security Technical Report*, vol. 12, no. 1, pp. 32–43, 2007.

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

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

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

[8] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transaction on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

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

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

BIOGRAPHY

Md Shohrab Hossain received his B.Sc. and M.Sc. in Computer Science and Engineering from Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh in the year 2003 and 2007, respectively. Currently he is a Research Assistant, and working towards his PhD in the School of Computer Science at University of Oklahoma. His research interests include mobility of IPv6 networks, mobility models, security, scalability and survivability of mobile and wireless networks.

Mohammed Atiquzzaman obtained his M.S. and Ph.D. in Electrical Engineering from the University of Manchester. He is currently a professor in the School of Computer Science at the University of Oklahoma, and a senior member of IEEE. Dr. Atiquzzaman is the editor-in-chief of Journal of Networks and Computer Applications, co-editor-in-chief of Computer Communications journal and serves on the editorial boards of IEEE Communications Magazine, International Journal on Wireless and Optical Communications, Real Time Imaging journal, Journal of Communication Systems, Communication Networks and Distributed Systems and Journal of Sensor Networks. In recognition of his contribution to NASA research, he received the NASA Group Achievement Award for "outstanding work to further NASA Glenn Research Center's effort in the area of Advanced Communications/Air Traffic Management's Fiber Optic Signal Distribution for Aeronautical Communications" project. He is the co-author of the book "Performance of TCP/IP over ATM networks" and has over 240 refereed publications, available at www.cs.ou.edu/∼atiq. His research interests are in wireless and mobile networks, ad hoc networks, and satellite networks. His research has been funded by National Science Foundation (NSF), National Aeronautics and Space Administration (NASA), U.S. Air Force, and Cisco through grants totaling over $3.8M.

William D. Ivancic has over twenty-five years experience in network and system engineering for communication applications, communication networking research, state-of-the-art digital, analog and RF hardware design and testing. He currently is a senior research engineer at NASA's Glenn Research Center where he directs the hybrid satellite/terrestrial networking, space-based Internet, and aeronautical Internet research. He has lead research efforts to deploy commercial-off-the-shelf (COTS) technology into NASA missions including the International Space Station and Shuttle. Mr. Ivancic is also performing joint research with Cisco System on advance routing research for space-based and aeronautic-based networks. Of particular interest is large scale, secure deployment of mobile networks including mobile-ip and mobile router technology. Recent accomplishments include being first to demonstrate and deploy secure mobile networks in an operational government network, the US Coast Guard, first to deploy Mobile-IP Mobile networking on a space-based asset, the Cisco router in Low Earth Orbit (CLEO, first to deploy Internet Protocol security (IPsec) and Internet Protocol version 6 on a space-base asset, and first to deploy delay/disruption network technology bundling protocol in space.

Mr. Ivancic is also the principal of Syzygy Engineering, a small consulting company specializing in communications systems and networking as well as advanced technology risk assessment. Mr. Ivancic is currently performing research and development on Identity-based security and key and policy management and distribution for tactical networks - particularly mobile networks.