Security Issues in Space Networks

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

***Abstract*—Satellites are being used to capture real-time images, video for various purposes, such as, observing the Earth, weather data, live images for tornado, cyclones, tsunami, etc. In future, these data can be accessed by terrestrial users through the Internet. Mobility protocols aim at providing uninterrupted real-time data communication facilities through seamless Internet connectivity to hosts or networks in motion, such as in bus, train, aircraft, and satellites. Mobile IP is an example of such a mobility protocol which uses Home Agent for mobility management, and requires signaling among the mobility agents, mobile node and the correspondent node for its operation. Originally, Mobile IP had no route optimization between end hosts; all traffic passes the mobility agents. However, recent mobility protocols, such as, Mobile IPv6 incorporated Route Optimization between end hosts, by informing correspondent node and home agent about mobile node's current location through binding updates. However, these binding updates are vulnerable to various attacks as unauthorized agent might send fabricated binding updates to fool mobile node, correspondent node or home agent. In short, the requirement of seamless connectivity in mobile environment and use of optimized route between end hosts have introduced several security vulnerabilities to mobility protocols. In this paper, we explain such security threats on various components of the space networks. Some of the major threats are traffic redirection attack, man-in-the-middle attack, bombing attack, denial-of-service attack, DNS poisoning, replay attack, etc. These attacks can affect the privacy and the integrity of the data. We also discuss possible protection mechanisms to protect network components from these security threats.**

I. Introduction

Satellite communication has its vital application in telephony, weather forecasting, satellite television, in-flight Internet, navigation (GPS) and military communications. Satellite Internet can serve as an alternate means to connect aid workers and troops to coordinate rescue and recovery missions in case of catastrophic events, such as, massive earth quakes, tornados. Spacecrafts with sensing elements, such as, microwave imager, Earth radiation sensor, lightning imaging sensor, etc. are used for observing the Earth, surveillance, and monitoring. Data are periodically downloaded from the spacecrafts using dedicated links with ground stations.

Modern communications satellites use a variety of orbits including Geostationary Orbits (GEO), Medium Earth orbit (MEO) and Low Earth Orbits (MEO). A constellation of spacecrafts (such as Iridium, Globalstar, Disaster Monitoring Constellation (DMC), GPS, etc.) form space networks where the spacecrafts can communicate among themselves using inter-satellite links, and also switch data between other spacecrafts and ground stations. Spacecrafts may have IP-enabled devices or a collection of devices connecting to an onboard LAN to form a mobile network [1]. Therefore, the continuous movement of the spacecrafts relative to Earth (such as, LEO satellites) requires the IP-mobility protocols to manage the handoff of connections between ground stations on Earth.

Internet Engineering Task Force (IETF) proposed Mobile IPv6 [2], Hierarchical MIPv6 [3] to support host-mobility, NEMO Basic support protocol [1] to support network mobility, allowing a TCP connection to remain alive while mobile nodes are on the move. NASA has been investigating the use of Internet protocols for space communications [4]–[6] and handover management [7], [8] for quite some time. A number of projects including Operating Missions as Nodes on the Internet (OMNI) [9], Global Precipitation Measurement (GPM) [10], Communication and Navigation Demonstration on Shuttle (CANDOS) mission [11] studied the possible use of Internet technologies and protocols to support all aspects of data communication with spacecrafts [12]–[15].

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 protocols, (such as, SIGMA [16], Mobile IPv6 [2]) have 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 earlier attempts to identify potential threats arising from mobility protocols to the public Internet. Kempf et al. [17] outlines the security threats to Mobile IPv6 and explain how the security features of Mobile IPv6 protocol can mitigate them. Hu et al. [18] 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. [19] present a survey on the Mobile IPv6 security through the classification of threats and possible scenarios. Kota [20] discuss briefly the technical challenges for broadband sattelite networks and identifies possible solutions for mobility management, satellite IP security issues to realize heterogeneous networks. Yantao et al. [21] addresses the secu-

rity issue for satellite communication through an authenticated key-exchange protocol that uses identity-based cryptography. Chowdhury et al. [22] discuss various security attacks that are possible in hybrid satellite networks, and discuss the issues for securing communication in satellite networks Bibo et al. [23] construct a three-layer hierarchical satellite system and propose a protocol to protect the satellite network from eavesdropping, sophistication, masquerade and repudiation. They have applied asymmetric and symmetric cryptography to provide security and efficiency. However, there is lack of research work that outlines all possible security vulnerabilities caused by IP-mobility protocols in space networks.

In this paper, we explain with illustrative examples the major security threats for the space network with the possible introduction of the IP-mobility protocols. Some of the major threats are traffic redirection attack, man-in-the-middle attack, bombing attack, denial-of-service attack, home agent poisoning, resource exhaustion on the low-power IP-enabled devices in spacecrafts. 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 the satellite communication network. Moreover, the attacker may send modified control and command messages to the satellite, thereby altering the operation sequence of the satellite. This may lead to dangerous impact on the whole satellite communication systems.

Several defense mechanisms have been proposed to protect against the security vulnerabilities of IP-mobility protocols, such as return routability protocol, IP security protocols, PKI and secret key-based approaches.

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

The rest of the paper is organized as follows. In Section II, we explain the use of mobility management protocols in space networks. In Section III, we illustrate possible security threats relating to IP-mobility protocol in space networks. In Section IV, existing protection mechanisms are analyzed critically. Finally, we conclude in Section V.

II. IP-mobility in Space Networks

Mobility management protocol aims at providing essential technology to allow mobile users change their point of attachment without affecting an ongoing communication. Mobility management thus require signaling messages to be exchanged among various mobility agents to keep track of mobile nodes current locations.

Space networks include satellite communication networks and are composed of satellite constellations, in-flight mobile networks (inside aeroplanes, helicopters) can take advantage of IP-mobility protocols to maintain Internet connectivity in next generation network which is supposed to be all-IP network. IP-mobility protocols can manage host-mobility (for standalone host) and network-mobility (e.g., onboard LAN) in space networks. Satellites with IP-enabled device, transmitting or receiving data, are examples of host-mobility in space networks. In-flight Internet connectivity in commercial aircrafts is an example of network-mobility where a high capacity mobile router may communicate with satellite transponders and ground station while providing Wi-Fi in the aircraft.

A. Satellite as a Mobile Host / Network

Satellites can act as communication endpoints with onboard IP-enable device which exchange data with ground stations on earth. As shown in Fig. 1, the satellite can be considered as an Mobile Host (MH). The satellite's footprint is moving from ground station A to B, while the satellite is bound with an IP address from ground station A. During movement, the satellite should maintain continuous connectivity with ground stations on earth. Thus, the IP address of the satellite has to be changed when it is handed over to ground station B. Whenever the Satellite acquires new care-of-address from ground station B, it informs its Home Agent (HA) about the new care-of-address. So whenever any Correspondent Node (CN) wants to communicate with the satellite, it sends query message to the HA to find out the current location of the satellite. The HA replies the query message with the current Care-of-Address (CoA) of the Satellite. The CN then can send setup and data packets to the Satellite for communication.

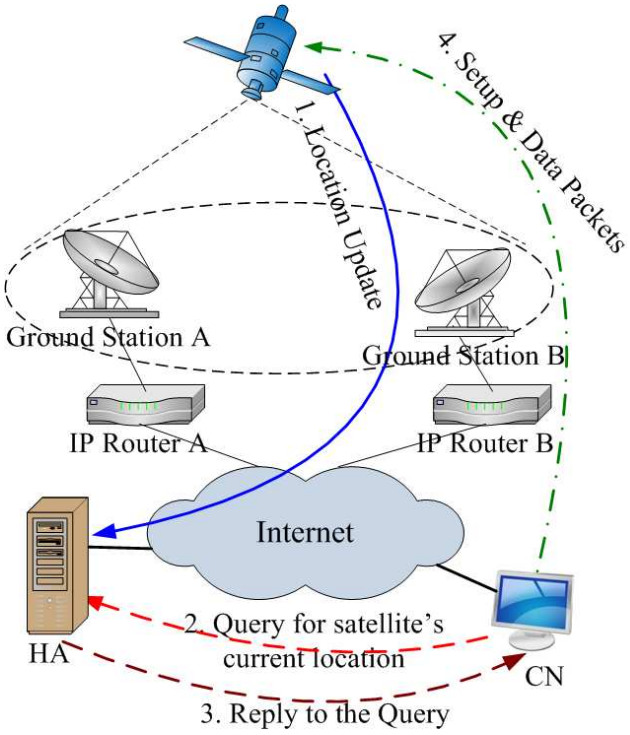


Fig. 1. Satellite as a Mobile Host.

Multiple onboard IP-enabled devices on the Satellites can form mobile network and a mobile router (with high transmission capacity) can manage the mobility of all the hosts in an aggregated way where Mobile Router (MR) act as gateways for the nodes inside the mobile network and ensures

their Internet connectivity when the MR changes its point of attachment while moving from a home network to a foreign network. As hsown in Fig. 2, a mobile network can be formed with the on-board IP-enabled devices, laptops of an aeroplane and in-flight Internet connectivity can be provided. Here MR communicates with HA via the satellite link and data is transmitted to the CN through the ground stations as shown in the figure.

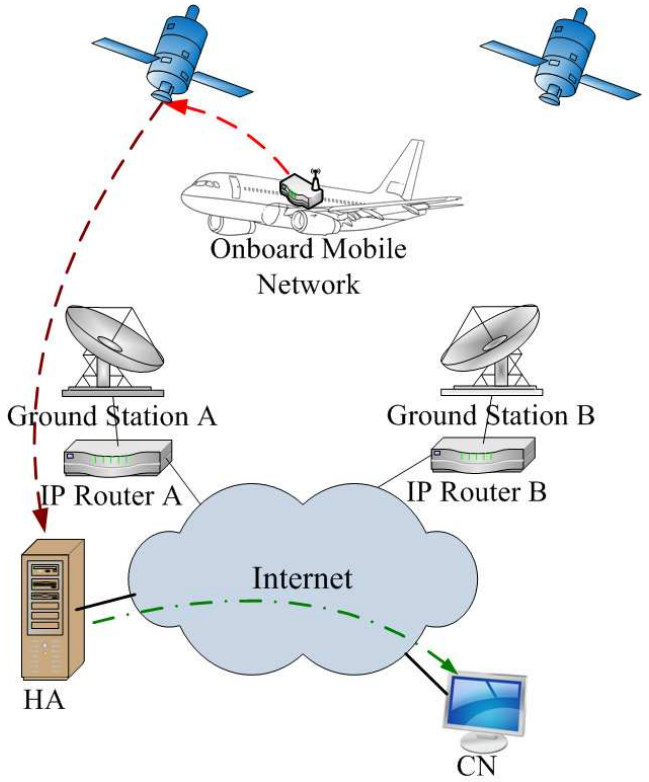


Fig. 2. In-flight Internet connectivity through satellites.

B. Satellite as a Router

As shown in Fig. 3, satellites do not have any onboard equipment to produce or receive data; rather they merely act as routers in the Internet. Each satellite can be assigned an IP address prefixes, and they can provide IP-connectivity to Mobile hosts in other spacecrafts (such as, laptops in aeroplane, helicopters, etc.) or in remote location on earth. Hosts are handed over between satellites as they come under the footprint of a new satellite.

C. SIGMA

Mobile IP protocol provides simple solution for IP-mobility support by forwarding packets through Home Agent (HA). However, base Mobile IP has several limitations: inefficient routing, high packet loss, handover latency, changes in Internet infrastructure, and low throughput.

To develop an alternative to Mobile IP, researchers at the University of Oklahoma and NASA Glenn Research Center have developed a transport layer based end to end handover

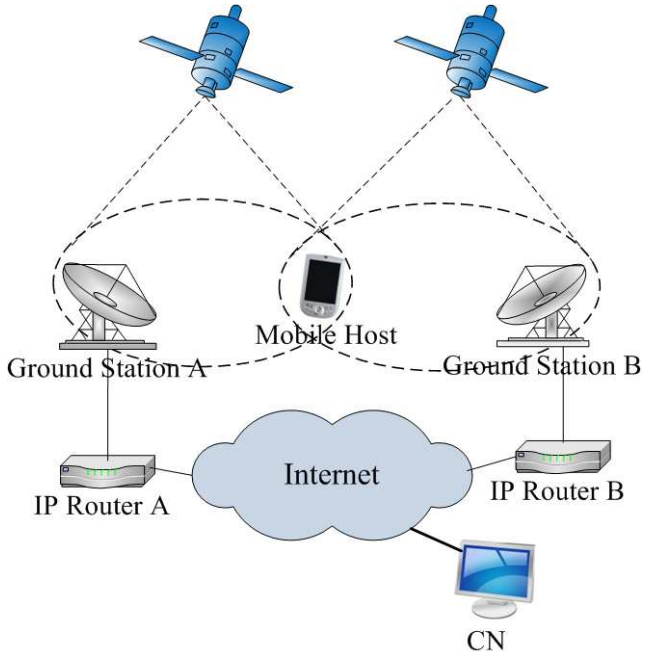


Fig. 3. User handover between Satellites where satellite act as routers.

management scheme, called Seamless IP-diversity based Generalized Mobility Architecture (SIGMA) [16]. SIGMA can be used for both space and terrestrial networks, thereby allowing easy integration between the two types of networks. SIGMA is an end to end handover management scheme and hence does not require any change in the Internet infrastructure. Moreover, it ensures uninterrupted connectivity using make-before-break strategy through its IP-diversity feature.

Cost and performance analysis of SIGMA have been done for SIGMA in [24], and survivability evaluation of SIGMA has been performed in [25]. However, we have not performed security analysis for SIGMA.

D. Route Optimization in mobility protocols

Originally, in Mobile IP, all data packets from the CN follows an un-optimized route (throught the HA) to the MH (i.e., CN –> HA –> MH) which is sometimes referred as triangular routing. This leads to longer routing path as well as degraded performance.

To alleviate the performance penalty, Mobile IPv6 includes 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 5 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.

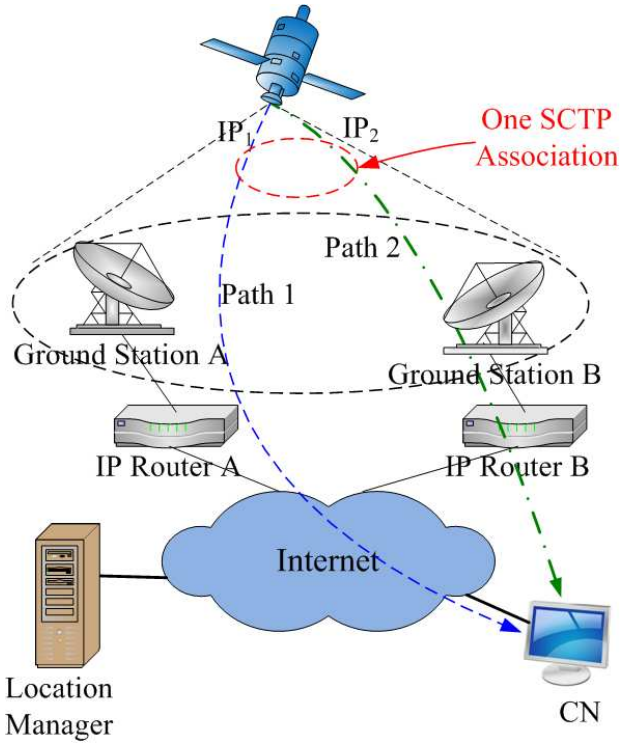


Fig. 4. SIGMA architecture.

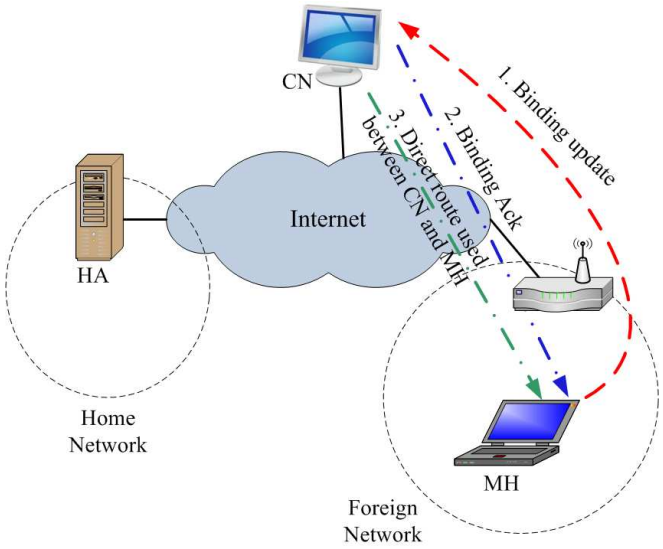
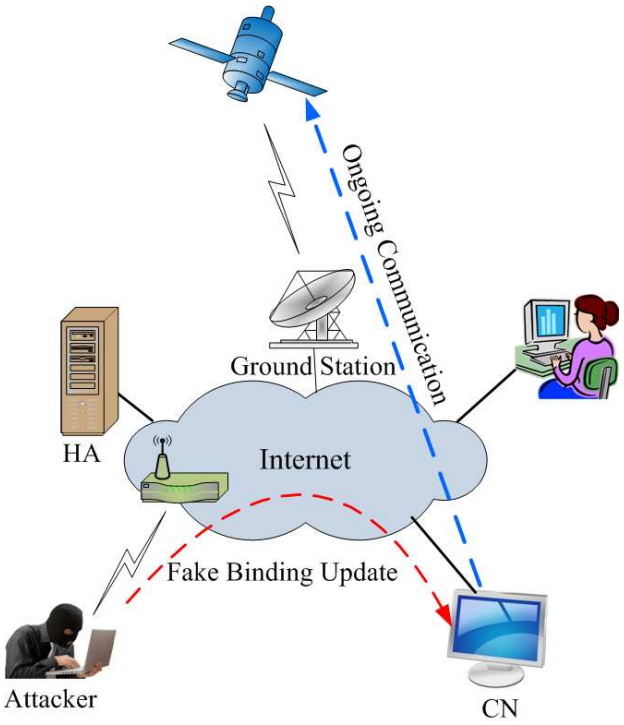


Fig. 5. Route Optimization in mobility management protocol.



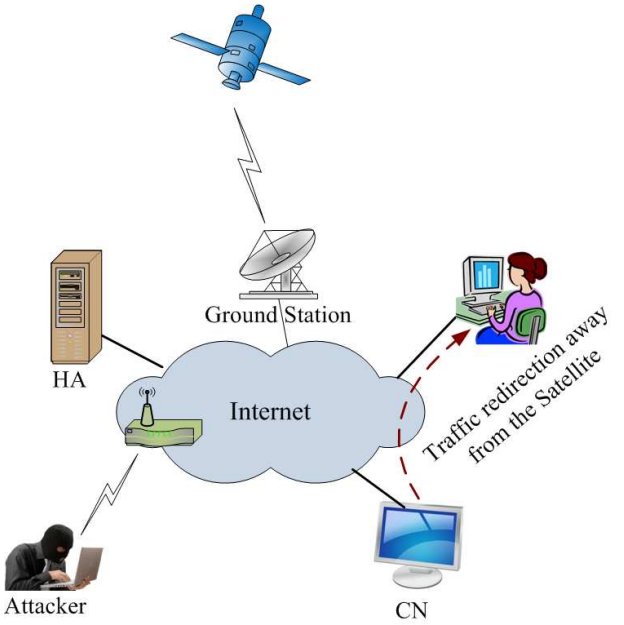


Fig. 6. Traffic redirection attack. (a) The attacker sends fabricated BU to the CN to modify the binding cache for the MH (Satellite) to some fictitious IP address (b) Traffic is redirected away from the MH (Satellite) to other location.

III. Threats for Space Networks

Mobility protocols should protect itself against misuses of the mobility related features that enables continuous Internet connectivity for end hosts. The unauthenticated 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. We explain these security threats for IP-mobility

protocols with illustrative scenarios.

A. Traffic redirection attack

The attacker may send a fake binding update message to the CN claiming that a node (victim) has changed its care-of address due to its movement to a new location. Consequently, the CN will start sending packets to the new CoA and the victim node will not get any traffic.

Fig. 6(a) shows how the traffic redirection attack hijacks an ongoing session between a Satellite (MH) and a CN on earth. The attacker sends fabricated BU to the CN to modify the binding cache (for the MH) in CN to some fictitious IP address and CN accepts the BU. As the result, the ongoing session of CN with the MH (Satellite) has been redirected towards some other location as shown in Fig. 6(b) and the Satellite device 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.

B. Man-in-the-middle attack

The attacker might send spoofed binding update message to the CN telling it to update the cache entry to its own (attacker's) IP address. Consequently, the CN will start sending the packets to the attacker instead of the Satellite. The attacker may learn the confidential information of the message, may modify the packet before forwarding it to the Satellite. Thus, the attacker might act as a *man-in-the-middle* getting the all-important private data destined to the victim satellite (device) without the knowledge of the concerned parties. Moreover, the attacker can send modified control and command messages to the satellite, thereby altering the operation sequence of the satellite. This may lead to dangerous impact on the whole satellite communication systems.

Fig. 7 shows the man-in-the-middle attack that is launched between the communication involving the CN and the Satellite. As the CN has updated its binding cache due to the malicious BU, it will start sending traffic towards the attacker rather than the MH (Satellite) as shown in Fig. 7. The attacker is able to learn and modify the confidential contents before forwarding it to the victim node.

C. Bombing attack

In this type of attack, huge amount of unsolicited data traffic are flooded towards the victim node (Satellite), resulting in the bandwidth wastage as well as performance degradation. 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 (Satellite) in the binding update. As a result, subsequent packets from the server will be directed to the victim node that has not even requested any data from the server.

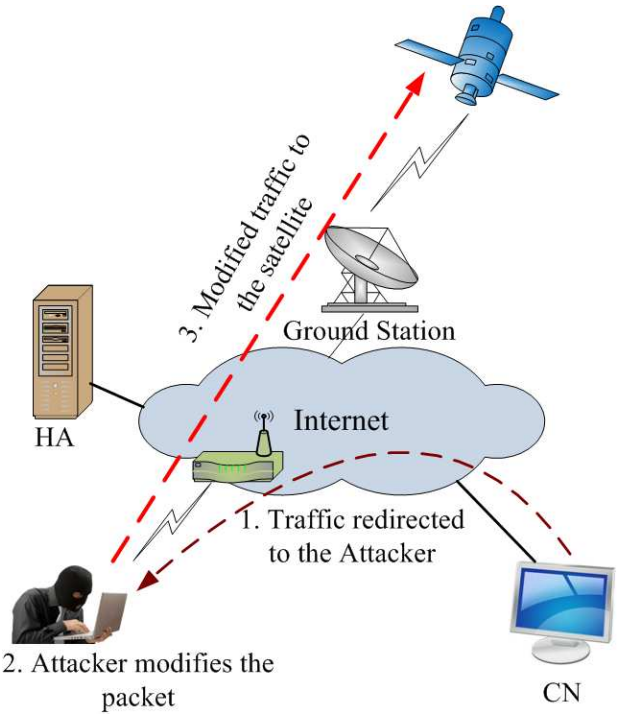
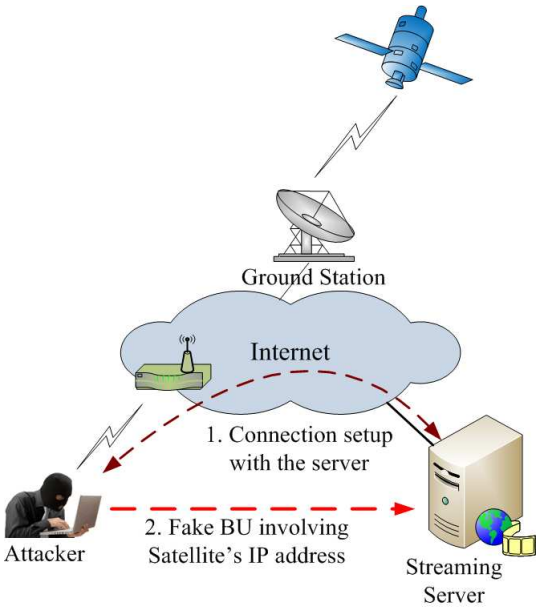


Fig. 7. Man-in-the-middle attack: traffic is redirected to the Attacker who learns the confidential information of the packet and may modify the packet before forwarding to the MH (Satellite) without the knowledge of the involved parties.

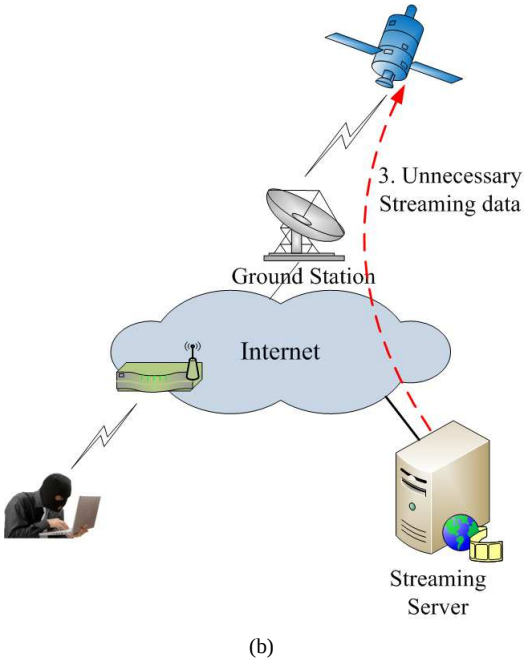
Fig. 8 shows the bombing attack on a satellite (device) which overwhelms the node with unsolicited huge amount of data packets, thereby degrading its performance. In Fig. 8(a), the attacker establishes a connection with a streaming server and after some time, it sends a spoofed BU to the server claiming that its IP address has been changed due to its movement. As a result, the traffic from the streaming server has been redirected to the victim node (see Fig. 8(b)), resulting in the bandwidth wastage.

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 packets (towards the server) as it knows the initial sequence number, thereby 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 unwanted flow of data stream. This may not be possible since the victim node 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



(a)



(b)

Fig. 8. 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 (Satellite), (b) Unwanted / unsolicited streaming data packets are flooded to the victim (Satellite).

(DDoS) attacks.

D. Reflection attack

In some earlier design, CN could initiate route optimization signaling whenever CN receives packet through HA, and this may 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 route optimization

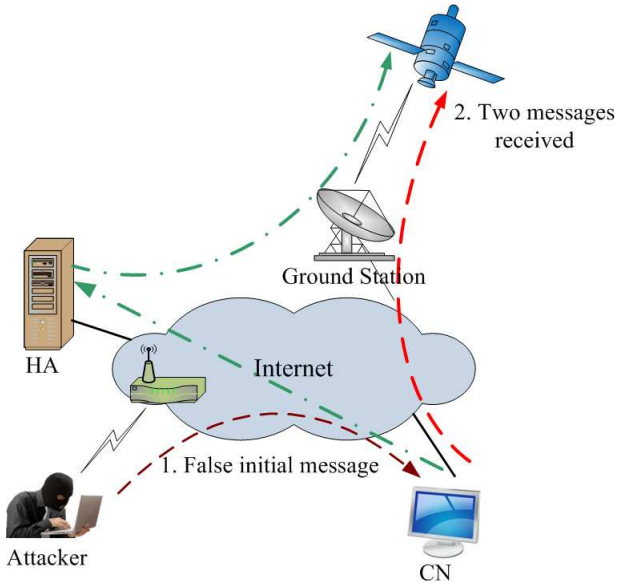


Fig. 9. Reflection attack.

signaling to the victim. Fig. 9 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 (Satellite). As a result, the Satellite 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 node 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.

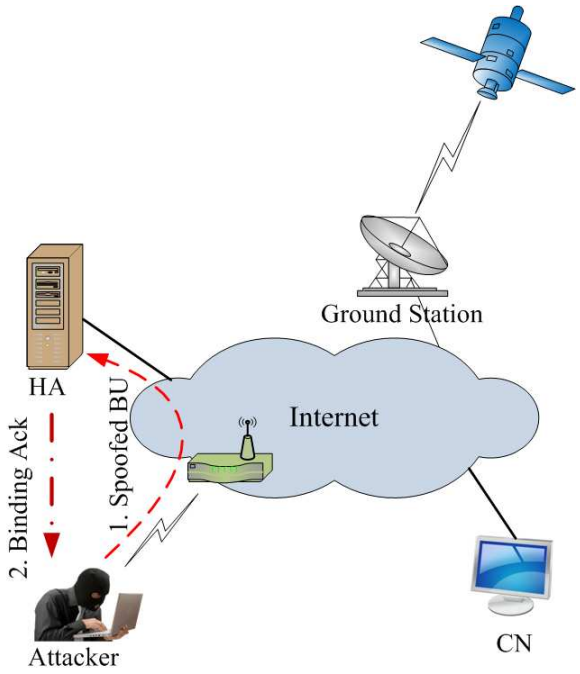
E. Home Agent poisoning

Home Agent keeps the mapping of Home address to Care-of-Address 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.

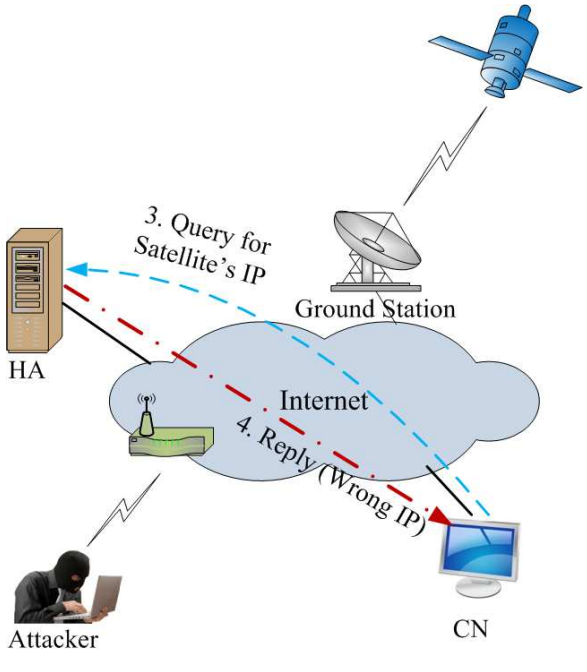
Fig. 10 shows the HA poisoning. The attacker sends spoofed BU to the HA (Fig 10(a)) and the HA accepts the BU. Therefore, the subsequent query to the HA by any CN (for the MH) will produce wrong reply as shown in Fig. 10(b).

F. Resource exhaustion

Attacker establishes connections with the IP-enabled device onboard the Satellite with thousands of fake IP addresses. Consequently, whenever the MH (Satellite) moves to some new location, it has to send to send BUs to all these imaginary hosts, thus huge processing power of the victim MH is wasted while dealing with these unnecessary BUs. This attack cannot be prevented with authenticated BUs. Fig. 11 shows the resource exhaustion attack on the satellite node. First, the attacker establishes many connections with the satellite using imaginary IP addresses while the satellite is under the coverage

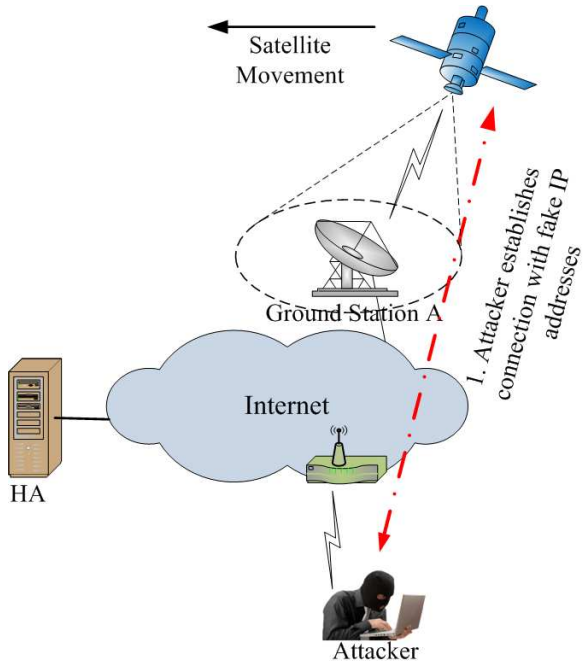


(a)

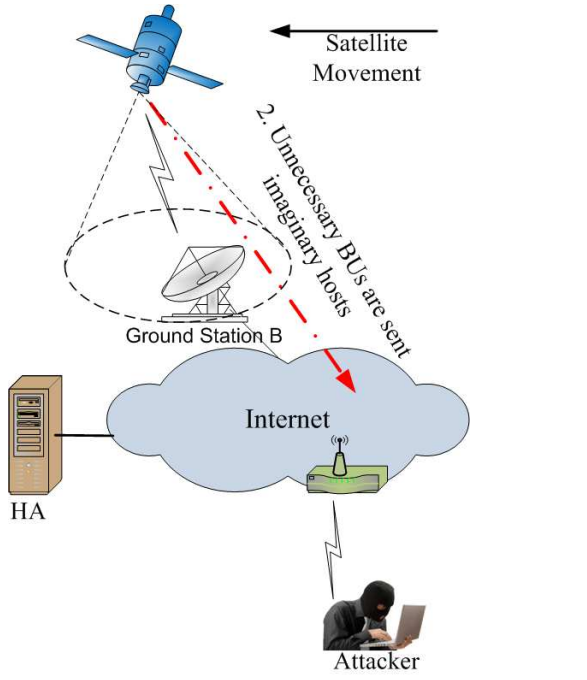


(b)

Fig. 10. HA Poisoning (a) Spoofed BU send to the HA and the HA updates the location information for the MH (Satellite) (b) When the CN queries for the IP address of the MH, it receives the wrong reply from the HA.



(a)



(b)

Fig. 11. Resource exhaustion of MH (a) The attacker establishes unnecessary connections with the MH (onboard the Satellite) using fake IP addresses (b) MH sends BUs to all the fake IP addresses thus wasting its processing power as well as memory.

area of Ground station A (Fig. 11(a)). Next, when the Satellite moves towards ground station B (Fig. 11(b)), the satellite has to inform all these imaginary nodes about its change of location through sending binding updates, thereby wasting its bandwidth and processing power.

These fake connection will require the victim to keep states for each one of them, wasting its memory as well, resulting in further denial of service attacks.

G. Attack on security protocols

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

the mobility protocols. Another kind of flooding attack can target the 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.

These kinds of attack are very harmful for spacecrafts since they have limited processing power and unnecessary strong cryptographic operations may lead to denial-of-service attacks. The satellites may not able to do legitimate operation due to the execution of such expensive operations and the satellite communication may be disrupted as the satellite may become the single point of failure.

IV. Protection Mechanisms

To prevent attacks on mobility protocols or mobile nodes, there are a few protection mechanisms that we are going to explain in this section. The defense mechanism aims at mitigating or preventing possible attacks, should be computationally less expensive so that they can be implemented in mobile nodes with low processing power. In addition, they are expected to be low latency solutions so that the seamless handover of the ongoing sessions can be ensured.

There are a few design issues to be considered while selecting the defense mechanisms for mobility protocols. They are summarized as follows.

Infrastructure less approach: To protect against malicious BU leading to session hijacking, authentication of the control messages (e.g., binding updates) is essential. However, use of strong cryptographic (authentication) protocols requires the existence of certification infrastructure as in 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, especially for low-power mobile devices. Therefore, defense mechanisms that avoid such cryptographic operations can be very useful.

Low latency 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 is bound to be broken, especially in case of space networks where the propagation delay is major concern. Therefore, it is desirable that the security protocols are fast enough to meet the main objective of the mobility management protocols.

A. Return Routability protocol

One major concern for security in space network is the use of unauthenticated and forged binding updates. To prevent such attacks, any node sending a binding update must prove its right to redirect the traffic. The solutions proposed in MIPv6 [2] 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. 12 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.

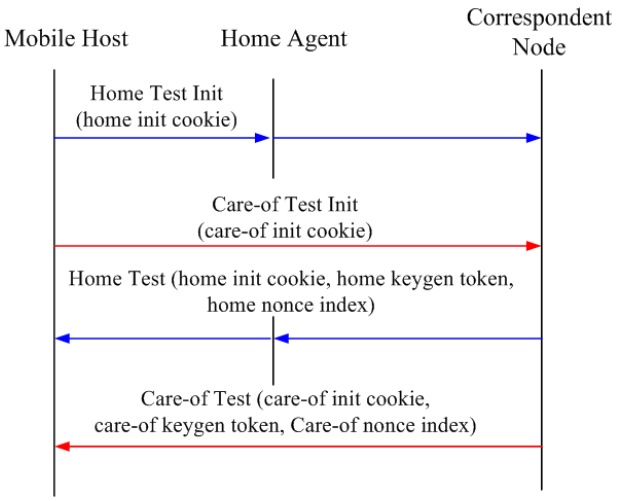


Fig. 12. Return routability test in Mobile IPv6.

RR protocol limits the number of potential attackers that can hijack an ongoing session. The use of RR protocol can significantly scale down such damages. The RR protocol is stateless as the CN does not store a separate state for each mobile node. Moreover, it requires less CPU processing power as it only uses relatively inexpensive encryption and one-way hash functions unlike other complex authentication methods. However, the security vulnerabilities exists for the RR protocol 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 which is necessary for spoofing the BU.

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.

B. IPSec

In order to protect against attacks that are based on spoofed binding updates, IPSec protocols, such as Authentication Header (AH) protocol [26] and Encapsulating Security Payload (ESP) [27] protocol can be incorporated with mobility protocols in space networks.

a) AH protocol: AH protocol guarantees connectionless integrity and data origin authentication of IP packets. It is one of the 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) [28] with certificate authentication.

b) ESP protocol: The use of AH cannot ensure the data integrity or privacy of the contents. Therefore, ESP protocol [27] can be used since ESP can provide confidentiality, data origin authentication, connectionless integrity, anti-replay service and traffic flow confidentiality. ESP ensures confidentiality of data through encryption. ESP also supports its own authentication scheme, 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.

Fig. 13 shows the use ESP header for securing 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 (Fig. 13(a)). After that, MH sends data packets to the CN with proper encryption along with the ESP header as shown in Fig. 13(b), thereby ensuring data integrity and confidentiality.

The use of IPsec can solve authentication and integrity of binding updates but cannot solve the location verification problem. As a result, using only the IPSec protocol to secure binding updates between an MN and its CN may not be enough to secure mobility protocols.

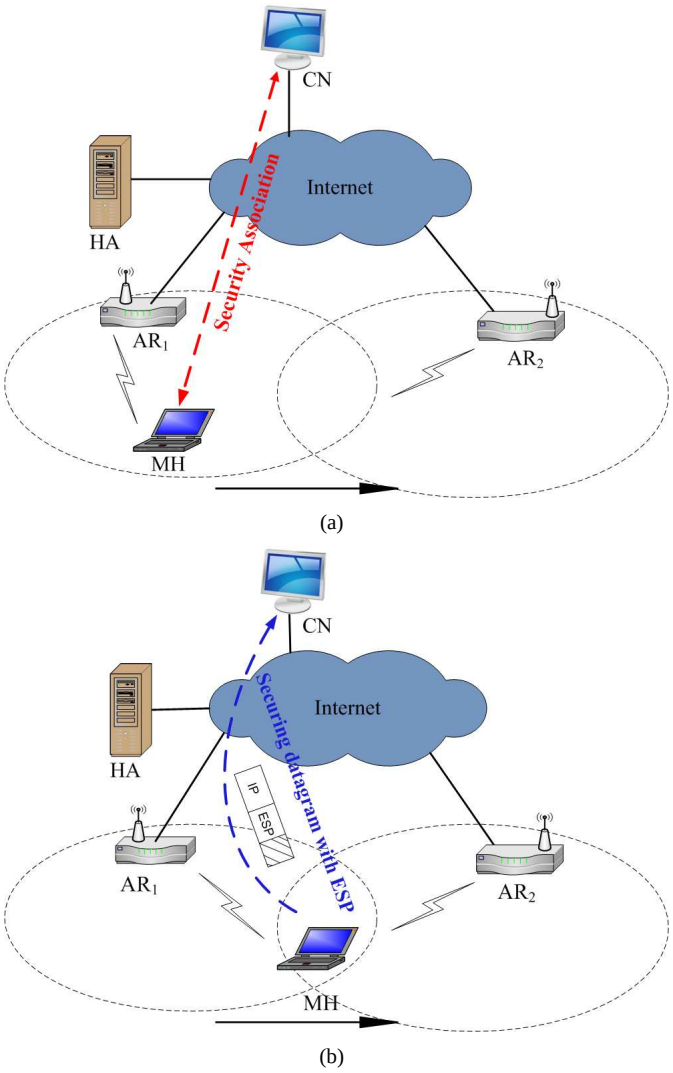


Fig. 13. ESP protocol: (a) Security association performed between MH and the CN (b) The datagram sent by MH is protected by ESP header.

C. IKE based schemes

IKE or IKEv2 [28], a key distribution mechanism for Internet community, is commonly used for mutual authentication 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. Use of this approach can ensure the confidentiality of secret key and the attacker will then be unable to learn and /or alter messages (such as, command and control messages). Therefore, man-in-the-middle attacks can be prevented.

IKE uses DiffieHellman key exchange [29] 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 IP-enabled devices in space networks.

D. Use of Cryptographically Generated Address

The use of Cryptographically Generated Address (CGA) [30] can reduce the chance of attack on a victim node (such as, IP-enabled device onboard the satellite). This idea was first introduced in a BU authentication protocol known as CAM [31]. 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 approach, 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.

E. Stateless approach

The mobile host (such as, Satellite) may not save any state for receiving and replying to BU messages. This stateless approach can prevent the CN 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.

F. 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.

G. Discussion

Table I lists the major security threats and corresponding defense mechanisms for IP-mobility in space networks along with their merits and demerits. 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 in space networks. There is always a need for limiting the lifetime of binding entry to restrict the potential attack by unauthenticated binding updates. Finally, the mobile nodes 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 CN can be prevented by the return routability protocol. This ensures that the MH sending the BU has the right to use the CoA. However, vulnerabilities are possible if the attacker is on the path between HA and CN. Attack on binding updates between MH and HA can be protected by the use of IPSec ESP protocol. This can protect against traffic analysis and privacy violation in space networks.

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 attacks in space networks can be mitigated if the victim node dynamically changes its IP address (such as, in CGA based approach). Nodes with fixed IP addresses are more vulnerable to such attack.

Man-in-the-middle attack can be very harmful, specially in space networks and can be prevented by IKE or PKI-based schemes through strong mutual authentication. However, these approaches require use of complex and expensive (CPU intensive) cryptographic operations in order to establish shared keys between the parties involved.

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 also provides strong protection mechanism at the expense of CPU power.

To prevent the DoS attacks that can cause CPU and memory exhaustion, the IP enabled devices in space networks can act as stateless agents. Therefore, they do not have to keep track of the current states of the half-open requests, thereby protecting the resources. However, higher processing may be required for legitimate connection requests.

V. Conclusion

In this paper, we have discussed the IP-security issues relating to space networks. We have explained possible security vulnerabilities that may lead to wastage of all-important bandwidth and processing power of the expensive IP-enabled devices onboard the Satellite / aircrafts. 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 to improve the existing mechanisms.

References

[1] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "NEtwork MObility (NEMO) basic support protocol," RFC 3963, Jan 2005.

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

[3] H. Soliman, C. Castelluccia, K. E. Malki, and L. Bellier, "Hierarchical Mobile IPv6 mobility management (HMIPv6)," IETF RFC 5380, Oct 2008.

[4] M. Atiquzzaman and W. Ivancic, "SIGMA for Space Sensor Web Networks," in *ESTO AIST Sensor Web Technology Meeting*, Orlando, FL, April 2-3 2008.

[5] K. Bhasin and J. L. Hayden, "Space internet architectures and technologies for NASA enterprises," *Journal of Satellite Communications*, vol. 20, no. 5, Sept 2002.

[6] W. Ivancic, P. Paulsen, D. Stewart, D. Shell, and L. W. et al., "Secure, network-centric operations of a spacebased asset - an abridged report," in *Earth-Sun System Technology Conference*, College Park, MD, June 2005.

[7] J. Noles, K. Scott, M. Zukoski, and H. Weiss, "Next generation space internet: Prototype implementation," in *NASA Earth Science Technology Conference*, Pasadena, CA, June 2002.

[8] W. Ivancic, D. Stewart, T. Bell, P. Paulsen, and D. Shell, "Use of Mobile-IP priority home agents for aeronautics, space operations and military applications," in *IEEE Aerospace Conference*, Big Sky, MT, March 2004.

[9] "Omni: Operating missions as nodes on the internet," http://ipinspace.gsfc.nasa.gov.

[10] J. Rash, E. Criscuolo, K. Hogie, and R. Praise, "Mdp: Reliable file transfer for space missions," in *NASA Earth Science Technology Conference*, Pasadena, CA, 2002.

[11] D. israel, R. Parise, K. Hogie, and E. Criscuolo, "Demonstration of internet technologies for space communication," in *The Second Space Internet Workshop*, Greenbelt, MD, 2002.

[12] G. Minden, J. Evans, S. Baliga, S. Rallapalli, and L. Searl, "Routing in space based internets," in *NASA Earth Science Technology Conference*, Pasadena, CA, June 2002.

[13] J. B. Steele, "Internet Protocol (IP) in Space," University of Maryland University College, Tech. Rep., November 28, 2004, http://home.comcast.net/∼js718/Career/".

[14] D. Israel, "Space network IP services (SNIS): an architecture for supporting low Earth orbiting IP satellite missions," in *IEEE International Conference on Networking, Sensing and Control*, Piscataway, NJ,, March 19-22 2005.

[15] W. Ivancic, D. Stewart, T. Bell, P. Paulsen, and D. Shell, "Securing mobile networks in an operational setting," in *IEEE Annual Workshop on Computer Communications*, Piscataway, NJ,, Oct 20-21, 2003.

[16] S. Fu and M. Atiquzzaman, "SIGMA: A Transport Layer Handover Protocol for Mobile Terrestrial and Space Networks," *e-Business and Telecommunication Networks, Springer*, pp. 41–52, 2006.

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

[18] 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.

TABLE I
SECURITY THREATS AND CORRESPONDING DEFENSE MECHANISMS FOR IP-MOBILITY IN SPACE NETWORKS.

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	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	PKI and secret key based approach	Difficult to break	Cryptographic operations needed to shared key
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

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

[20] S. L. Kota, "Broadband satellite networks: Trends and challenges," in *IEEE Wireless Communications and Networking Conference, WCNC*, New Orleans, LA,, March 13-17, 2005, pp. 1472–1478.

[21] Z. Yantao and M. Jianfeng, "A highly secure identity-based authenticated key-exchange protocol for satellite communication," *Journal of Communications and Networks*, vol. 12, no. 6, pp. 592–599, Dec 2010.

[22] A. R. Chowdhury, J. Baras, M. Hadjitheodosiou, and S. Papademetriou, "Security issues in hybrid networks with a satellite component," *IEEE Wireless Communications*, vol. 12, no. 6, pp. 50–61, Dec 2005.

[23] J. Bibo and H. Xiulin, "Security issues in satellite networks," in *Second International Conference on Space Information Technology*, Wuhan, China, Nov. 10-11 2007.

[24] S. Fu and M. Atiquzzaman, "Signaling cost and performance of SIGMA: A seamless handover scheme for data networks," *Wireless Communication and Mobile Computing*, vol. 5, no. 7, pp. 825–845, Nov 2005.

[25] ——, "Survivability evaluation of SIGMA and Mobile IP," *Wireless Personal Communications*, vol. 43, no. 3, Nov 2007.

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

[27] ——, "IP Encapsulating Security Payload (ESP)," IETF RFC 4303, Dec 2005.

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

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

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

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