Macrothink Institute™

Network Protocols and Algorithms
ISSN 1943-3581
2013, Vol. 5, No. 3

Security in Network Mobility (NEMO): Issues, Solutions, Classification, Evaluation, and Future Research Directions

Rohini Basak[1], Bhaskar Sardar[2]

Department of Information Technology, Jadavpur University

Saltlake Campus, Block-LB, Plot-8, Sector-III

Kolkata-700098, West Bengal, India

Tel: +91-33-23358321

Email: [1]visitrohinihere@gmail.com, [2]bhaskargit@yahoo.co.in

Received: May 31, 2013 Accepted: October 25, 2013 Published: October 31, 2013

DOI: 10.5296/npa.v5i3.3789 URL: http://dx.doi.org/10.5296/ npa.v5i3.3789

Abstract

The IETF has standardized network mobility (NEMO) basic support protocol (BSP) to extend Internet services to networks in motion such as in bus, trains etc. The NEMO BSP uses a bidirectional tunnel between the mobile router (MR) and its home agent (HA) resulting in suboptimal routing. Route optimization may be incorporated between the MR and the correspondent node (CN), by informing the HA and the CN about the MR's current location through binding updates. However, these binding updates are vulnerable to different attacks as malicious users may send fabricated binding updates to fool the MR, the HA, and the CN. Although the path between the MR and the HA is protected by IPSec tunnel, the paths between the MR and CN, between the HA and CN, and between a mobile network node and the MR remain unprotected. So the requirements of extending Internet services in NEMO and use of optimized route between the MR and the CN have introduced several security threats in NEMO. In this survey, we describe security requirements, issues, and attacks with their corresponding countermeasures in NEMO. Major attacks in NEMO include bombing attack, redirection attack, denial of service attack, man-in-the-middle attack, replay attack, home agent poisoning attack etc. These attacks can affect the integrity and privacy of data. This survey also provides an in-depth and categorized description of various security protocols and key management techniques which are specifically targeted for NEMO. Along the way we

highlight the advantages and disadvantages of existing NEMO security protocols, evaluate them, and discuss open research issues.

Keywords: Mobile IPv6, Mobile Router, Network Mobility, Route Optimization, Security.

1. Introduction

The increasing demand for ubiquitous Internet connectivity leads us towards extending the wireless communication technologies in vehicular environments. A number of devices or nodes deployed in a vehicle form a network and changes the point of attachment to the Internet as a single unit. This situation, where the entire network moves is often referred to as network mobility (NEMO) [1]. A network featuring NEMO is called a mobile network, and the nodes in this network are called mobile network nodes (MNNs). The IETF has been working for some years to develop the concept of a moving network or NEMO [2]. To provide seamless Internet connectivity to the MNNs of a mobile network the IETF has standardized NEMO basic support protocol (NEMO BSP) [1]. NEMO BSP is an extension of MIPv6 [3] and thus inherits all limitations of MIPv6 like sub-optimal routing, security etc.

To manage the mobility of the mobile network, the NEMO BSP introduces a new network component called mobile router (MR) [4] which acts as the default gateway for all inbound and outbound traffics of the mobile network. When handoff takes place, the MR performs the handoff operations on behalf of all the MNNs; hence MNNs connected to the MR feel seamless mobility. As specified in NEMO BSP, when the MR changes the point of attachment to the Internet, it acquires a care-of-address (CoA) from the foreign network and registers the new CoA with its home agent (HA) by sending a binding update (BU). To complete the registration of new CoA, the HA sends back a binding acknowledgement (BAck) to the MR. On completion of this handoff procedure, a bidirectional tunnel is established between the MR and it's HA.

Although the NEMO standards are comparatively new, various projects have already been started on implementations of the NEMO BSP. The Nautilus6 Working Group [5], a part of the Widely Integrated Distributed Environment (WIDE) Project [6], was created to improve mobility in IPv6. The SHISHA and NEMO Platform for Linux (NEPL) projects are current Nautilus6 implementations for BSD and Linux respectively. The CISCO System has supported NEMO in its CISCO IOS Software under the name Cisco Mobile Networks [7].

The mobile nodes travel on foreign and possibly untrusted networks when away from home network. Since the MNNs are unaware of mobility, it is very important that NEMO BSP provides an acceptable level of security while the MNNs are away from the home network. If a malicious attacker somehow manages to attach itself to the communication path between an MNN and a CN, it can easily modify, and/or eavesdrop all the traffic between the two nodes. An attacker can also block the communication intentionally by simply dropping the packets. In some cases, the attacker can mount flooding attack by redirecting a huge amount of unsolicited data traffic to a victim node which not at all has requested any data streams. These types of attacks introduce severe threats in the security of the overall system

of NEMO [8]. In order to prevent these attacks, a number of security protocols have been proposed in the literature for the last few years. Unfortunately, none of these proposed protocols provides complete security in the NEMO architecture. As a result, there is no widely accepted security solution for NEMO. So security remains a very critical aspect for successful deployment of NEMO.

A few existing survey on NEMO can be found in [9], [10]; however, only small sections of these surveys focus on security in NEMO. So in this paper, we make a bold attempt to survey the state-of-the-art security protocols for NEMO. First, we explore some important security metrics and compare the state-of-the-art NEMO security protocols against these metrics. Next, we describe in detail the possible attacks in NEMO while identifying the network component targeted by the attacker. We also provide some defense lists to prevent these attacks. Then we engage in thorough study on the NEMO security protocols. Most security protocols make use of some cryptography algorithms. So, managing key distribution becomes a more challenging task in NEMO. We provide a categorized and in depth description of key management techniques for NEMO.

The rest of the paper is organized as follows. In Section 2, we describe operation principle of NEMO BSP with the help of a message flow diagram, the security goals and requirements, and the various security issues. We also describe in great detail various possible attacks and corresponding countermeasures. Section 3 presents a taxonomy of NEMO security protocols. A brief description of state-of-the-art NEMO security protocols are presented in Section 4. In Section 5, we evaluate the NEMO security protocols and discuss open research issues. Section 6 presents a taxonomy of key management techniques in NEMO. Finally, Section 7 concludes the paper.

2. Security issues and requirements in NEMO

In this Section, we present security goals, requirements, issues, and attacks in NEMO. We start with an introduction to NEMO BSP.

2.1 NEMO BSP

In NEMO BSP, the MR performs mobility management functions on behalf of all MNNs in the mobile network. On moving to a new network, it receives a router advertisement and obtains a new mobile network prefix from the access router of the visited network. Then it sends a BU packet to the HA (Fig. 1). In the BU packet, the MR indicates that it is acting as an MR and includes the newly obtained mobile network prefix for registration with the HA. The HA sends back a BAck packet to the MR (Fig. 1). On successful completion of the binding update procedure, a bidirectional tunnel is created between the MR and its HA (Fig. 1, Fig. 2). It is interesting to note that the MR does not explicitly assign the newly obtained addresses to the MNNs. Instead, it advertises its home network prefix in the mobile network to keep the MNNs unaware about the mobility of the mobile network [11].

When an MNN sends a packet to a CN, the MR reverse-tunnels the packet to the HA

using the MR-HA tunnel. This reverse-tunneling is done by using IP-in-IP encapsulation. On receiving the packet, the HA decapsulates and forwards the packet to the CN. When a CN sends a data packet to an MNN, the packet is routed to the HA that currently has the binding between the MR's home address and CoA. The HA receives the data packet and tunnels it to the MR. The MR then decapsulates the packet and forwards it onto the appropriate interface where the MNN is connected. Before decapsulating the tunneled packet, the MR has to check whether the source address in the outer IPv6 header is the HA's address. This check is needed only when the packet is not protected by IPSec [12], [13]. The MR also has to make sure that the destination address in the inner IPv6 header belongs to a prefix used in the mobile network.

As provisioned in NEMO BSP, it is possible for an MR to visit another MR. So the visiting MR comes under the domain of the visited MR. This leads to a nested NEMO scenario with a hierarchy of MRs [14]. Thus, the bidirectional tunneling approach of NEMO BSP results in sub-optimal routing, increased header overhead, high handoff latency, and high data delivery delay [14]-[17]. Several route optimization techniques have been proposed in the literature [15], [16], [18]. The objective of the route optimization techniques is to update the CN about the current location of MR and thus introduces new security problems [18].

Several research efforts have been made in the recent past to measure the performance of NEMO BSP [19], [20]. It has been shown that NEMO BSP suffers from high handoff latency and high data delivery delay which directly affects the application performance. In [21], the authors have presented an implementation of NEMO BSP for low-end devices. To overcome the aforementioned problems of NEMO BSP, researchers have proposed several new NEMO protocols [22] [23]. In [22], the authors have proposed a network assisted NEMO protocol based on Proxy Mobile IPv6 (PMIPv6). An IP diversity based network mobility management protocol for satellite IP networks called SINEMO has been proposed in [23]. The difference between NEMO BSP and SINEMO is that they work in different layer of the protocol stack. The NEMO BSP works in network layer whereas SINEMO works in transport layer and makes use of stream control transmission protocol (SCTP) [24]. The SINEMO protocol has been examined in depth using simulations, experiments, and analytically, and it has been shown that it outperforms NEMO BSP [25] [26] [27] in terms of handoff latency, signaling cost, throughput, network size etc.

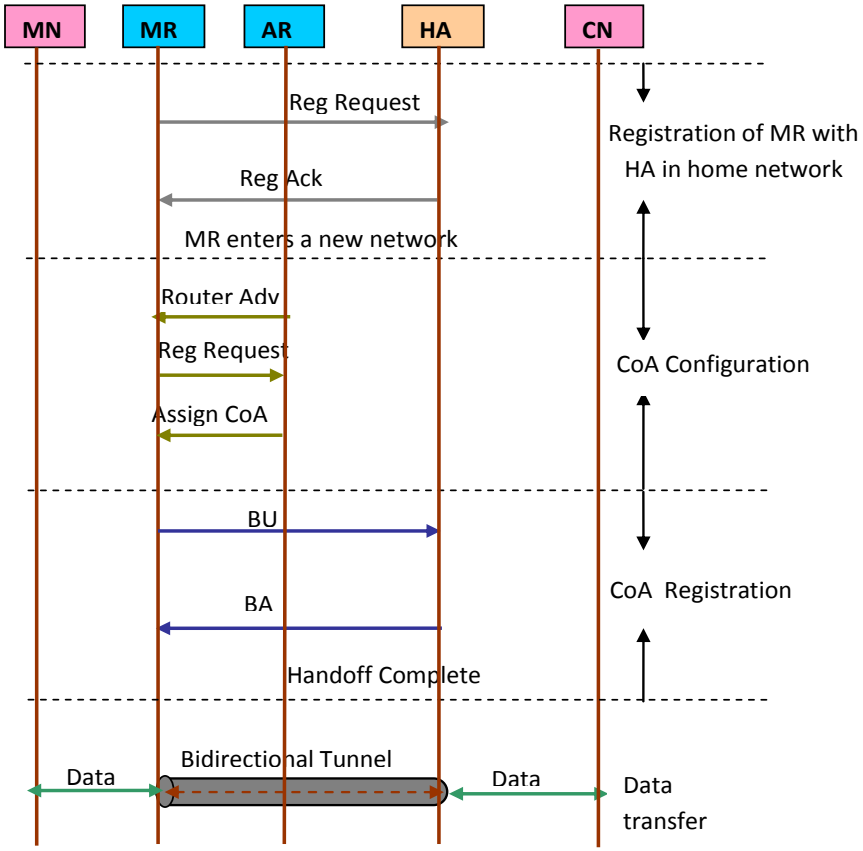

Figure 1. Message Flow Diagram of NEMO BSP.

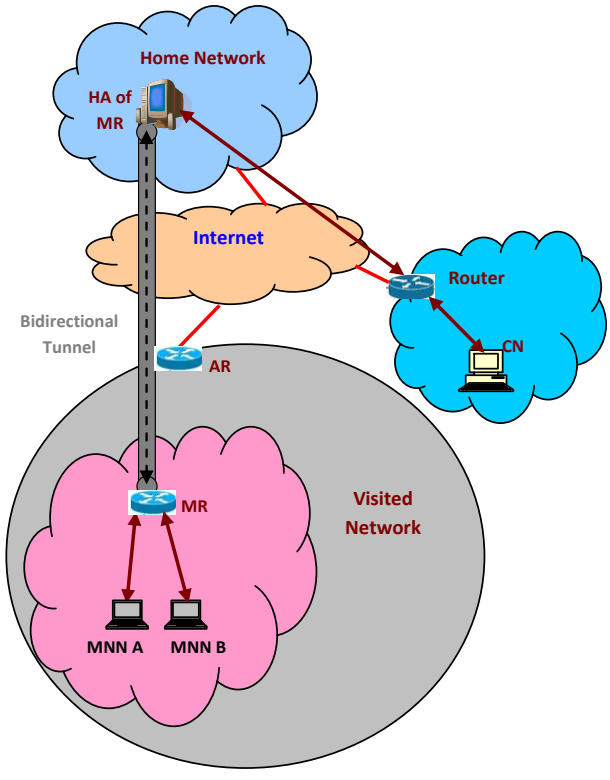

Figure 2. Operation of NEMO BSP.

2.2 Security Goals and Requirements

The objective of security services in NEMO is to protect the information and network nodes from attacks and misbehavior. In this section, we outline the security goals [28] that must be achieved while implementing NEMO BSP.

Authentication: The communications between any two legitimate nodes (e.g., between MR and HA, between MR and CN) must be authenticated, so that no malicious node will be able to generate and send any spoofed packet to a legitimate party.

Authorization: It ensures that only authorized network nodes can be involved in using the network resources or exchanging messages with the network components.

Availability: It ensures that the expected network services are available even if any node is compromised by denial-of-service attack.

Confidentiality: It ensures that the transmitted control packets like (e.g., BU, BAck, dynamic home agent discovery (DHAD) packet, router advertisement) and the data packets cannot be understood by any malicious adversary other than the legitimate recipients.

Location Privacy: This property assures that the actual location of MNNs remain hidden from third parties other than the HA.

Integrity: It assures that the contents of the transmitted messages (like mobile network prefix or source address in BU) from one legitimate party (MR or HA) to other network components (HA or CN) cannot be modified or altered by any malicious intermediate nodes.

Freshness and Anti-replay: This ensures that the control packets (e.g., BU) or data packets sent from the mobile network are recent and fresh. It means no malicious attacker should be able to capture the packets and replay them at a later time.

Robustness against leakage: There are some cases where a cryptographically strong key (generally a private key) has to be stored in tamper resistant modules. Leakage of such keys results in complete breakdown of security of the system. The tamper resistant modules are also not free from bugs and misconfigurations. So the security scheme must provide robustness against leakage of the stored secrets.

2.1 Evaluation

In addition to the above security requirements, we suggest the following security metrics to analyze the overall performance of the NEMO security protocols.

***Signaling Efficiency*:** One of the main goals of the security protocols is to keep the signaling overhead as low as possible. A security scheme is said to be efficient in terms of signaling if small number of signaling packets are used.

***Delay*:** The security scheme should not introduce high delay either in the transfer of data or in data processing at any node (CN, HA, or MR). Higher delay will cause the packets at the MRs or HAs to wait for a long time degrading the performance of the protocol.

***Computational Overhead*:** Another aim of the security schemes is to reduce the computation burden on the participating entities (HA, CN, MNN, or MR). More computations require more time which ultimately results in longer delay.

***Scalability*:** The security scheme must provide an acceptable level of security even if the network size is increased to a large extent.

***Configuration Complexity*:** This metric indicates that the participating network components need not be equipped with high level configuration for carrying out the desired task. The higher the configuration requirement, the less efficient the security scheme will be in terms of consumption of resources.

Reliability: This metric measures the degree of reliability of the security scheme. The reliability is measured in terms of the strength of the hash function used to calculate the hash digest etc. The more strong the hash function is, the more difficult it will be to regenerate the original message from the hash digest.

2.2 Security Issues

The end-to-end path between an MNN and a CN consists of three segments: a path between MNN and MR, a path between MR and **it's** HA, and a path between the HA and the CN. Each of these communication paths is susceptible to various attacks. Moreover, the control packets and data packets may be the target of attackers at any time. Some security issues of NEMO BSP are given below.

- Any malicious node can sit between the MR and the HA, and intercepts the signaling packets (e.g., BU). The contents of the packets (e.g., mobile network prefix) can be altered easily and forwarded to the HA. If the HA accepts the packet and saves it into the cache, then all the data packets will be forwarded to the attacker and the victim (legitimate MR) will not get any packets.
- If an attacker can eavesdrop the tunneled data packets and analyze the header information (e.g., CoA of MR), then it can easily identify the location of MR. Since all data packets are tunneled using the CoA of MR, the location information of the MNNs can easily be revealed which is a severe threat to location privacy.
- The MR advertises its IP network prefix periodically in the mobile network. These router advertisement packets can be easily intercepted and modified by the attckers to advertise the network prefix of its own. As a result, all subsequent packets will be redirected towards the attacker MR instead of the original MR.
- Although the data packets from an MNN to a CN are sent through the bidirectional tunnel between the MR and its HA, the paths between the MNN and the MR, and between the HA and CN are susceptible to various attacks as they are not protected by IPSec.

- Any malicious MR within the mobile network (in case of multi-homing) can register to the HA by sending a spoofed IP prefix. As a result, the MNNs which attach to the network start communicating with the malicious MR.

- Cryptographic authentication relies on the possession of a key by the party to be authenticated. Such keys are stored in tamper-resistant-modules. Leakage of such keys is enough to breakdown the security of a system. Use of IPSec does not provide enough security against leakage of stored secrets.

2.3 Threats in NEMO

Since NEMO BSP is built on the concept of MIPv6, it suffers from same kinds of attacks that MIPv6 suffers [29]. It is generally assumed that an attacker may be able to capture a node physically, compromise a node, or even it can hack the communication messages. If an attacker can compromise a node, then it may capture the packets sent by that node, modify the contents of the packets before redirecting them to the actual party. Furthermore, if the attacker is able to know the IP address of the target node (e.g., HA or CN) then it can send spoofed BUs to confuse the target node and redirect all the packets to itself or to any other node of its choice.

The goal of the attacker can be to corrupt the HA's/CN's binding cache and to cause packets to be delivered to a wrong address. This fact can compromise secrecy and integrity of packets and cause denial-of-service (DoS) both at the communicating parties and at the address that receives the unwanted packets [8], [30], [31]. The attacker may also exploit features of the BU mechanism to exhaust the resources of the MRs, the HAs, or the CNs. In this section, we describe various possible attacks and protection mechanisms in NEMO. A summary of the attacks, targeted nodes, and defense mechanism is given in Table 1.

***Bombing Attack*:** In this attack, high volume of unwanted data packets are flooded towards the victim node (MR), resulting in bandwidth wastage as well as overall performance degradation. The attacker first needs to find out the CN which wants to send data packets to any node. On getting the IP address of the CN, the attacker establishes a connection with the CN and captures all packets from the CN. In this way, the attacker gets access to the CoA of MR and sends a spoofed BU (with the CoA of MR and any arbitrary mobile network prefix) to the CN requesting it to update the cache entry. As a result, subsequent data packets will be redirected to the MR which has not at all requested any data from the CN (Fig. 3). So the MR gets overwhelmed with a high volume of unsolicited data packets.

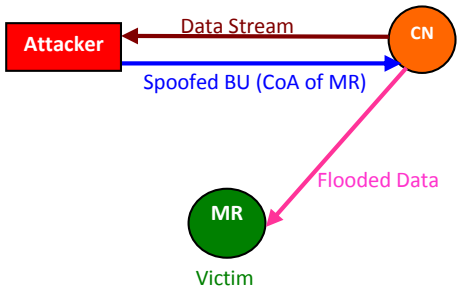

Figure 3. Bombing attack.

***Redirection/Hijack Attack*:** In this case, the attacker may send a false BU to the CN claiming that an MR (victim) has changed its location. So the CN updates the binding cache entry by replacing the old CoA with the new arbitrary CoA. As a result, the CN redirects all data packets to the new location (new CoA of an arbitrary MR specified in the false BU) (Fig. 4). So the victim (legitimate MR) will be deprived of getting the data packets.

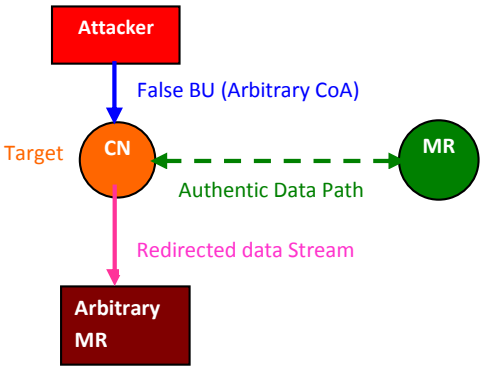

Figure 4. Redirection/Hijack attack.

***Denial of service Attack*:** A denial-of-service attack is characterized by an explicit attempt by an attacker to prevent an MR from getting packets from CN. To do so, the attacker must know the IP address of the CN. Then the attacker sends spoofed BU to the CN to redirect all the packets between the two legitimate parties (e.g., MR to CN) to a random or nonexistant address (Fig. 5). As a result, the communication between the MR and the CN may be totally stopped or disrupted.

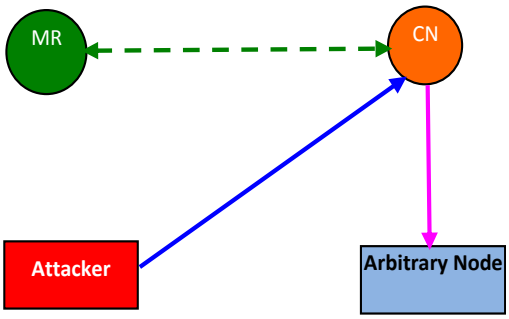

Figure 5. Denial of service attack.

***Man in the middle attack*:** In this attack, the attacker sends spoofed BU to the HA to update the binding cache entry with its own IP address. Consequently, the HA tunnels all packets to the attacker instead of the MR. As a result, the attacker gets access to the confidential information and can easily modify the contents before forwarding the packet to the actual MR (Fig. 6). In this way, the attacker inserts itself in the middle of all communications between two legitimate parties without their knowledge. This attack is also possible during route optimization between the MR and the CN.

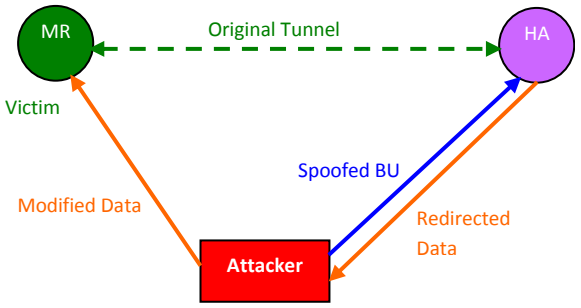

Figure 6. Man in the middle attack.

***Replay Attack*:** To launch replay attack, the attacker must connect itself to the network where the MR is connected. The MR moves so frequently that before the expiry of the previous BU at the CN, the MR sends the next BU. The attacker captures this BU and replays it to the CN when the MR moves away. So all data packets from the CN will be redirected to the previous location of MR. Also when the MR sends a BU to the HA, the attacker may capture this BU to launch replay attack.

***Home Agent Poisoning*:** The HA maintains a binding cache that maps the home address of an MR to its CoA. Therefore, in every handoff, the MR sends location updates to its HA to update the cache entry accordingly. If any malicious attacker sends a fake BU to the HA that binds the home address of the MR to its own CoA (i.e., attacker's current address), the HA will be fooled to believe that the MR is in the new location (Fig. 7). So this will severely affect all subsequent communications between the legitimate MR and its HA.

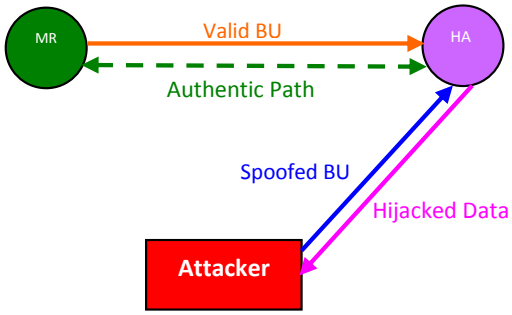

Figure 7. Home agent poisoning attack.

***Reflection and Amplification Attack*:** Sometimes, the attackers try to hide the source of a packet by reflecting the traffic from other nodes. That is, instead of flooding the packets directly to the target, the attacker sends the packet to other nodes, causing them to send same or more number of packets to the target. Such reflection hides the attacker's address. Reflection becomes more dangerous if the packets are reflected multiple times or if the nodes can be tricked into sending more packets than they receive from the attacker to amplify the throughput of the network may.

Triangle routing would easily create opportunities for reflection (Fig. 8): a CN receives packets from a malicious MR and replies to the home address given by the malicious MR in the home address option. Being unable to find the address of the attacker, the target MR assumes that the packets are actually sent by the CN.

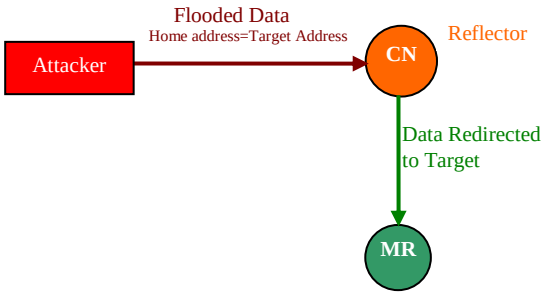

Figure 8. Reflection and amplification attack.

Table 1. Possible Attacks in NEMO.

Attacks	Victims	Degree of vulnerability	Defence List
Bombing attack	MR, HA, CN	Very severe	BU authentication, Target node may use TCP RESET signal to immediately stop unwanted flow of data stream.
Redirection attack	MR, HA, CN	Very severe	BU authentication, Target node may use TCP RESET signal to immediately stop unwanted flow of data stream.
Denial of service attack	MR, HA, CN	Very Severe	Encryption and authentication of Bus, Packet filtering, Latency examination.
Replay attack	MR, HA, CN	Severe	Use of timestamp with each BU.
Man in the middle attack	MR, HA, CN	Very severe	Strong encryption, Integrity and Authentication protection for BUs.
Home agent poisoning	HA, MR	Severe	Authenticate BUs before acceptance.
Amplification and Reflection attack	MR, CN	Medium	Use of sequence numbers in BUs.

3. Classification of NEMO security Protocols

According to our opinion, the existing NEMO security protocols can be broadly classified into two categories: control packet protection and data path protection as shown in Fig. 9. One of the main goals of the security protocols is to protect the control packets used in NEMO BSP. The attackers use these control packets intelligently to introduce severe security threads into the system. So protecting the control packets is very crucial to ensure tight security in NEMO. According to the control packets used in NEMO BSP, the protocols for control packet protection can be divided into three categories: BU protection, router advertisement protection, and DHAD message protection.

When handoff takes place, the MR sends BUs to the HA and to the CN to register the new CoA and to perform route optimization respectively. Any malicious attacker may capture these BUs, modify the CoA, and forward to the HA/CN to update the binding cache entry with his/her preferred CoA. An attacker may send a spoofed BU to the HA/CN to modify the

binding cache entry. The attacker may also capture a BU and replay it at some later time. Current NEMO BSP specification suggests the use of IPSec [12], [13] to protect BUs between the MR and its HA. On the other side, several schemes such as return routability with network prefix (RRNP) [32], Cryptographic Prefixes for Route Optimization in NEMO (CRYPTRON) [33] have been proposed to protect the BUs between the MR and the CN.

The MRs periodically broadcasts router advertisements to allow the MRs/MNNs to join the mobile network. A malicious MR may intercepts these advertisements and modify the advertisements with its own mobile network prefix. A proper authentication mechanism must be used to protect the integrity of router advertisements. When an MR moves to a foreign network, it has to look for an HA which can provide mobility support. A series of DHAD messages are exchanged between the MR and the HA. These DHAD messages are not protected by IPSec and hence it becomes very easy for the attacker to capture and modify the DHAD messages. The keyed hashed message authentication code (HMAC) [34] has been proposed to authenticate the DHAD messages.

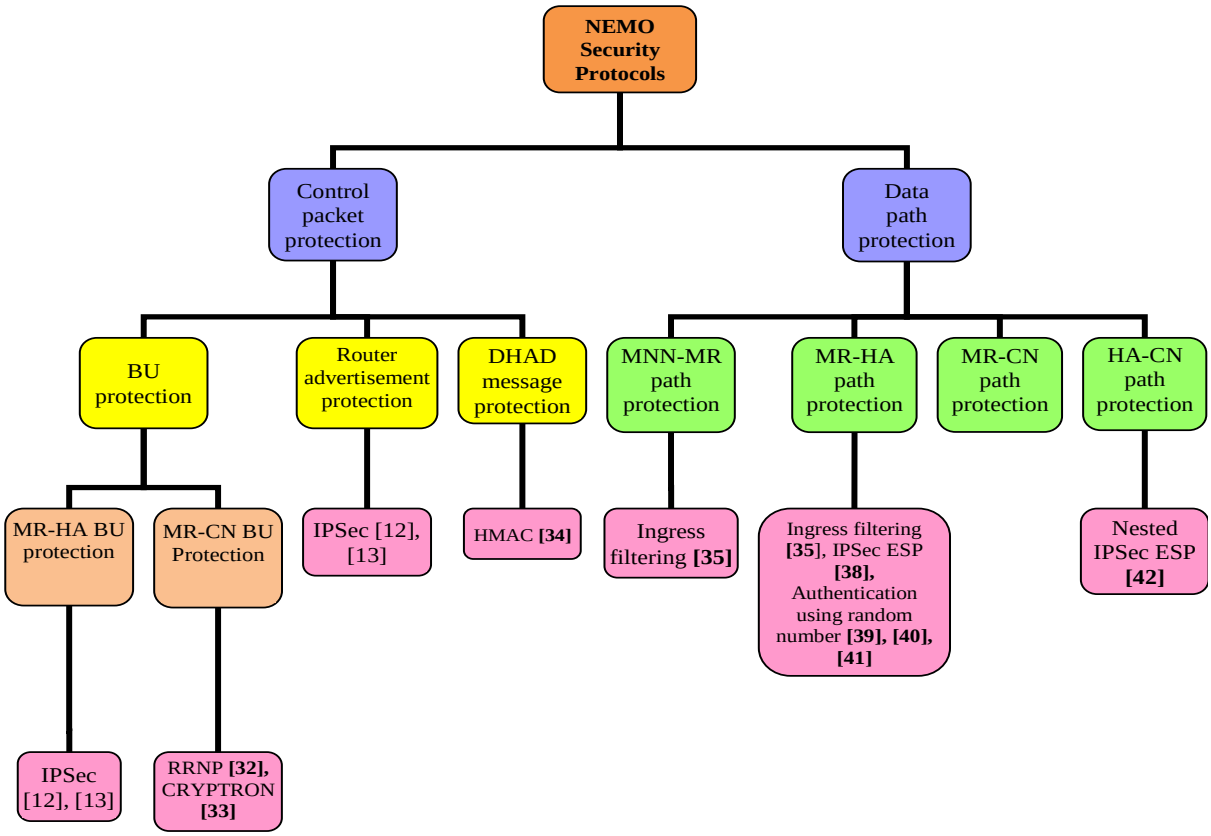

Figure 9. Security protocols in NEMO: a taxonomy.

The data path between an MNN and a CN consists of many segments. If route optimization is not used, the data path consists of three segments: MNN to MR, MR to HA, and HA to CN. If route optimization is used, the data path consists of two segments MNN to MR and MR to CN. Each of these paths is prone to several attacks and vulnerabilities. So a security protocol must provide protection to each of these paths as shown in Fig. 9. It is interesting to note that, NEMO BSP provides some level of security in the path between the

MR and the HA in the form of a tunnel but it does not take about the security of remaining paths.

In the MNN to MR path, a malicious MNN can generate a spoofed data packet by setting the source address to the home address of the MR and the destination address to the address of HA and includes the BU of the MR as payload. When the MR receives the packet, it cannot distinguish the spoofed data packet from the actual BU. So the MR forwards the spoofed packet to the HA. The HA accepts the packet and updates the binding cache. Consequently, the HA will forward subsequent data packets to the wrong CoA (attacker's address). This type of attack can be prevented by employing ingress filtering check [35] [36] at the MR.

Although the path between the MR and the HA is protected by IPSec tunnel, the tunnel itself is not free from attacks. An attacker can generate high volume of IP-in-IP packets be setting the source address and destination address of the outer header to the CoA of the MR and the address of the HA respectively. In the inner header, the attacker sets a spoofed address as the source address an arbitrary address as the destination address. The HA actively processes the tunnelled packets and forward them to the target address. The objective of the attacker is to keep the HA busy all the time. This leads to amplification attack which may be converted to denial-of-service attack in the worst case. The paths between MR and CN and between HA and CN are not protected by IPSec. As a result, all packets in these paths can be easily intercepted and modified by the attacker. This leads to sever threat to the secrecy and integrity of the data packets communicated between the MR and the CN and between the HA and the CN.

4. Descriptions of NEMO Security Protocols

In this section, we describe existing NEMO security protocols (under the heading of abovementioned broad categories) in some detail. A summary of the protocols in each category is given in Table 2 and Table 3.

4.1 Control packet protection

4.1.1 IPSec

The BU packets from an MR to its HA are the main targets of the attackers in NEMO environment. So a strong security protocol is required to protect the confidentiality, integrity, and source authenticity of these BU packets. Current NEMO specification recommends the use of IPSec [13] to protect all the signaling packets between the MR and its HA. IPSec uses two types of headers: authentication header (AH) [37] and encapsulating security payload (ESP) [38].

AH: IPSec AH is used to provide integrity checking, antireplay protection and data origin authentication for the signaling packets. But it does not provide confidentiality protection. The AH header is inserted between the IP header and the TCP header. The sequence number field in the header is used to uniquely identify the packets. Even retransmitted packets get a

different sequence number than the original packets. The sequence numbers are never cycled in order to detect replay attack. The integrity check is carried out only on the unchanging fields in the IP header including the souce address of the packet. This prevents an intruder to falsify the origin of a packet.

ESP: IPSec ESP is used to provide confidentiality, data origin authentication, connectionless integrity, and anti-replay protection. The entire IP header is encapsulated and a new IPSec header is inserted after the IP header and before the upper layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode). So the packet size is larger than AH.

4.1.2 Return Routability with Network Prefix (RRNP)

In order to secure the BUs from an MR to a CN, the original return routability test of MIPv6 is not adequate in NEMO. The return routability test provides a mean for the CN to verify whether the home address and the CoA in the BU are actually owned by the legitimate mobile node. But, in NEMO environment, in addition to the home address and CoA, the MR has to inform the CN which network prefixes are in use in the mobile network so that the data packets for the MNNs can be forwarded to the MR's CoA. So the original return routability test needs to be extended to allow the CN to ascertain whether the network prefixes specified in the BU are the actual prefixes of the mobile network. To achieve this goal, the MR has to list all the mobile network prefixes it is using in the Home Test Init packet. The CN, in addition to Home Test packet, generates a network prefix test [32] packet for each network prefix specified in the BU. The network prefix test packet containing a cryptographically generated token is addressed to any address selected at random from the mobile network prefix option. All these network prefix test packets are intercepted by the MR, the cryptographic tokens are extracted, and hashed to produce a value that will be used later in the BUs from the MR to the CN. In this way, the CN can verify that the MR really owns the mobile network prefixes which it claims as its own.

4.1.3 Cryptographic Prefixes for Route Optimization in NEMO (CRYPTRON)

CRYPTRON [33] provides BU protection from an MR to a CN. The Crypto Prefixes bind a public component of a public-private key pair to IPv6 network prefix. The binding is created by embedding the hash information of the public key in the network prefix itself. The crypto prefix allows the private key holder to claim the prefix ownership by proving its knowledge of the corresponding private key. CRYPTRON introduces two options: crypto prefix parameter and crypto prefix signature.

The crypto prefix parameter contains a public key and a random value used to compute the hash. On the other hand, crypto prefix signature carries a signature computed over the hash of MR's CoA, correspondent node's address, and the mobility header in the BU packet by using the private key associated with the Crypto Prefix.

Then the MR sends the Crypto Prefix, the crypto prefix parameter, and the crypto prefix signature together with the BU to the CN. On receiving the BU, the CN performs a set of verifications. First, it computes the hash over the public key and the random value contained

in the crypto prefix parameter option and compares it to the Crypto Prefix in the received BU. If the verification is successful, then it computes the cryptographic hash over the MR's CoA, its own address, and the mobility header and verifies the signature of the hash using the public key received in the crypto prefix parameter. Successful verification proves that the MR is the owner of the crypto prefix.

4.1.4 Hashed Message Authentication Code

The message authentication code (MAC) is used to authenticate the sender of a packet as well as to protect the integrity of its contents. MACs based on cryptographic hash functions are called HMAC. The HMAC function is used by the sender to produce a digest or MAC by condensing the input packet and a secret key that is known only by the sender and the receiver.

In NEMO, the HMAC function is applied on the dynamic home agent discovery (DHAD) packet header to produce a hash digest [34]. When the MR generates a DHADReq packet, it will apply the HMAC hashing algorithm on the packet together with the secret key to produce a digest. This digest is embedded in the DHADReq packet and sent to the HA. On receiving the packet, the HA extracts the DHADReq and apply the same HMAC hashing algorithm on the packet together with the secret key to produce a digest. Then the HA compares the computed digest and the received digest. If these two digests are identical, the HA becomes sure that the packet has come from the legitimate MR and it has not been tampered or modified. But, if digests do not match, then the HA assumes that either the packet has been corrupted or the packet has not come from a legitimate MR. So the HA has to alarm the MR about the problem and take necessary actions or just drops the packet silently. The same procedure is applied on the DHADReply packet to prove its integrity and authenticity of the HA to the MR.

Table 2. Summary of protocols for control packet protection

Protocol Name	References	Year of Publications	Proposal	Advantages	Disadvantages
IPSec	**[37],[38]**	1998, 2005	A new header containing information of integrity check, anti-replay protection, confidentiality protection is inserted into the packet.	No attacker can read or modify the contents of the packet or replay it.	The packet size is increased.
RRNP	**[32]**	2004	Introduces network prefix test packet along with home test packet to verify the validity of the mobile network prefix specified in the BU.	No attacker can send spoofed BUs with arbitrary MNPs.	Signalling overhead is increased.
CRYPTRON	**[33]**	2010	Binds the public key in a crypto prefix and allows the private key holder to provide proof of ownership.	Difficult for the attacker to hack the crypto prefixes.	Computational overhead is increased at the CN.

HMAC	**[34]**	2005	A hash digest is produced by applying hash function on the DHAD packets and appended to it.	Any modification of the packet by an attacker will be immediately detected and reported to the MR or HA.	Computational overhead is slightly increased to regenerate the hash digest.

4.2 Data Path Protection

4.2.1. Ingress Filtering

The ingress filtering is used to prevent source IP address spoofing. Any attacker disguised as an MNN can generate a spoofed BU by setting the source address to the home address of the MR and binds any arbitrary mobile network prefix to the CoA of the MR. In such cases, ingress filtering check at the MR's ingress interface will prohibit the packet to be forwarded to the HA. Otherwise, this BU will cause the HA to create a new binding cache entry binding the mobile network prefix and the CoA of the MR. As a result, the MR will be flooded with a high volume of unwanted data packets. So every MR must check that the source address in the received packets belong to the mobile network prefix and are not the same as one of the addresses used by the MR. In some cases, a malicious attacker outside of the mobile network can generate a fake IP-in-IP packet by setting the source address to the CoA of MR and sends it to the HA directly. This kind of attack generally occurs more in situations where the network supports multihoming [36]. The ingress filtering [35] employed on the ingress interface of HA will successfully pass the packet because the source address lies within a valid range of prefixes advertised by the MR. To prevent this, the access router of the outside network wherefrom the packet has come should activate ingress filtering. This would restrict the packet to pass because the source address in the packet does not belong to a valid range of prefixes supported by the access router. So ingress filtering drastically reduces the possibility of source address spoofing.

4.2.2. Authentication using Random Number

A severe problem arises for authenticating MR-HA pair in nested NEMO scenario. When an MR changes its point of attachment to the Internet, each MR-HA pair has to verify and authenticate each other by exchanging BU and BAcks. So a high protocol overhead is introduced for creating and tearing down the tunnels. To solve the problem, a new authentication mechanism for nested NEMO scenario has been proposed in [39] which use an array of random numbers. When an MR is first booted up, it generates a random number and exchanges it with its HA. The HA stores this random number and uses it later for authentication purpose. On every handoff of the MR, this random number will be exchanged with the HA and compared. If the verification is successful, the HA authenticates the MR as a genuine MR. The integrity of the random numbers during the exchange process can be secured with the help of PKI mechanism [39] [40]. Although this method avoids the need for setting up multiple tunnels, the initial set up cost is a bit high. With the completion of exchange of the random numbers secured by PKI [41], a secret key has also been securely

shared between the MR and the CN which will be used for protecting all further communications.

4.2.3. Nested IPSec ESP

In order to protect the path between the HA and the CN, a security scheme using nested IPSec ESP has been proposed in [42]. Whenever an MR is attached to some other network, it acquires several router advertisements from the MRs of the visited network. The visiting MR chooses the parent MR and implements the Internet security association and key management protocol to negotiate the security association before sending BU. In this way, several nested MRs negotiate the security association with each other for securing the BU.

When a CN wants to send packets to an MNN, the packet will be routed to the HA in the home network. Then, the HA checks its security policy database to find out the appropriate destination. Before forwarding the packet, again IPSec ESP is performed to encrypt it. All the intermediate MR will perform IPSec ESP in similar manner to encrypt the packet and finally the packet is delivered to the MNN.

Table 3. Summary of data path protection protocols.

Protocol Name	References	Year of Publication	Proposal	Advantages	Disadvantages
Ingress Filtering	**[35]**	2010	MR should check the source address of each packet received at the ingress interface.	No attacker can generate and send any spoofed packet by setting the source address to the home address of the MR.	Processing load on the MR is increased.
IPSec ESP	**[38]**	2005	An ESP header is inserted after the IP header and before the upper layer protocol header.	Difficult for the attacker to understand the contents of the packets.	Packet size is increased.
Authentication using Random Number	**[39], [40], [41]**	2007	The MR generates random number and exchanges it with the HA on every handoff to proof its identity to the HA.	It avoids the creation and teardown of several tunnels in nested NEMO.	Each node has to maintain an array of random numbers.
Nested IPSec ESP	**[42]**	2011	Multiple nested MRs negotiates security associations with each other and creates IPSec tunnels among themselves.	Provides high protection against confidentiality and integrity of the packet throughout the entire path.	Creation and tear down of multiple tunnels introduces high delay.

5. Evaluation and Open Research Issues

In this section, we evaluate the NEMO security protocols based on the metrics discussed in Section 2. The qualitative evaluation is shown in Table 4. We observe that IPSec, CRYPTRON, HMAC, and ingress filtering incur low signaling overhead whereas RRNP,

authentication by random number, and nested IPSec ESP incur high signaling overhead. Increased number of control packets introduce additional delay in communication. Moreover, computational overhead will also directly affect the delay performance of the protocol. So RRNP, authentication by random number, and nested IPSec ESP will not be acceptable in terms of signaling efficiency, computational overhead, and delay. Configuration complexity is measured in terms of consumption of hardware and software resources. Since the MR, the HA, and the CN are high-end devices, high configuration complexity does not pose huge challenge. Reliability of each of the protocol depends on certain factors which are indicated in the table. Scalability is another important metric which determines whether the protocol will function properly if the network size is increased to a large extent. Increased network size will cause extra load on all participating nodes in the protocols like authentication using random number and nested IPSec ESP. But the other protocols are not affected by the increased network size.

The ingress filtering check employed at the MR does not provide complete protection against spoofing of IP prefix. If an attacker somehow manages to spoof an IP address within another valid mobile network prefix supported by the MR, then the packet can easily pass the ingress filtering check. So the filtering method should be made more stringent in order to drop these types of false packets from the attackers.

Although authentication of BUs at the HA and CN will significantly decrease the chance of attacks listed in Table 1, but they cannot be eliminated totally. If an attacker can convince the HA and CN, by sending a spoofed BU binding its own IP address with the home address of the legitimate MR, then the binding cache entry will be updated accordingly to pass the data packets to the attacker. So more sophisticated authentication mechanisms of BUs is required to fight against these kinds of attacks.

From Fig. 9, we see that no security protocol has been proposed to protect the path between the MR and the CN. As a result this path remains susceptible to various attacks. Although nested IPSec ESP protects the path between the HA and the CN, it generates a heavy load during setup and teardown of multiple ESP tunnels. So it will introduce a high delay to transmit a data packet. So appropriate security protocols should be designed to protect the data packets from vulnerabilities in the path between the MR and the CN and between the HA and the CN.

Table 4. Evaluation of NEMO Security Protocols

Protocols	Signaling Efficiency	Computational Overhead	Configuration Complexity	Delay	Reliability	Scalibility
IPSec	Very low	Medium	Low	Medium	Highly reliable. Strongly recommended by NEMO working group.	High
CRYPTRON	Very low	Medium	Very low	Low	Depends on the proper embedment of the public key and random number in the Crypto Prefix.	High
RRNP	High	High	Low	High	Higher reliability than Return Routability Test.	High
HMAC	Very low	Medium	Very low	Medium	Depends on the strength of the hash fuction.	High
Ingress Filtering Check	Very Low	NA	Medium	Medium	Depends on the correct order of packet processing at MR.	MR may get overwhelmed with increased number of MNNs.
Authentication using Random Number	High	High	Very high	High	Depends on the proper functioning of the central authority.	High
Nested IPSec ESP	High	High	High	Very High	Depends on the negotiation of Security Associations among the communicating pairs.	High overhead if nested level increases.

6. Key-Management Techniques

Key management is one of the main issues of NEMO security protocols to ensure secured communication of data and control packets. The goal of key management is to establish required keys between the participating nodes. Fig. 10 shows a taxonomy of key management techniques in NEMO. The key management techniques in NEMO can be broadly classified into two categories: asymmetric and symmetric key management. In this Section, we present a detailed overview of key management techniques in NEMO.

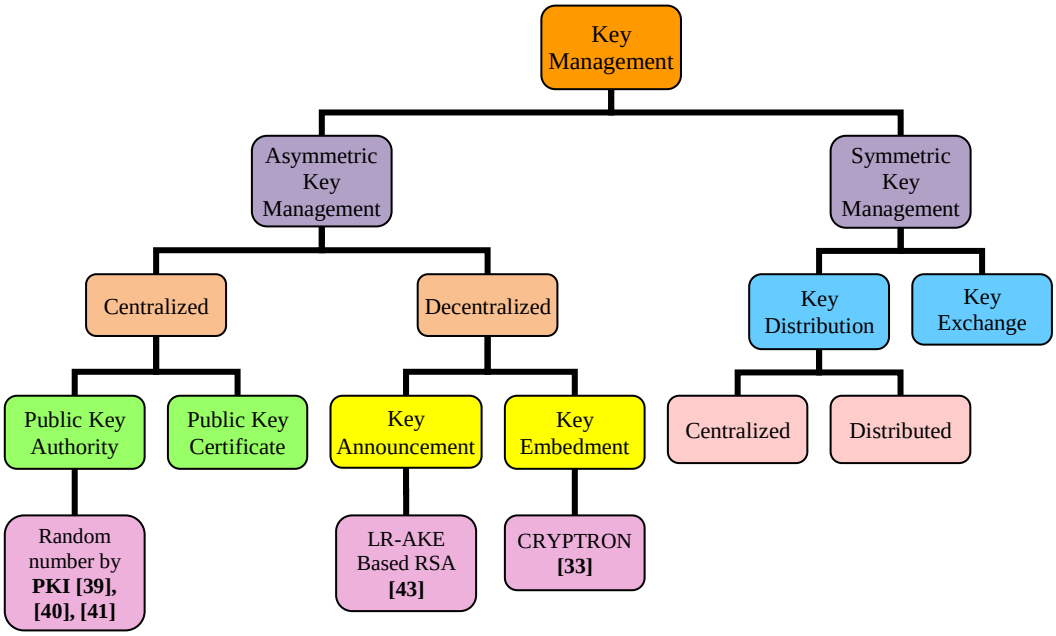

Figure 10. Key management techniques in NEMO: a taxonomy

6.1 Asymmetric Key Management

Many NEMO security protocols use a public/private key pair to protect the data and control packets. Generally, the public key is made available in the public domain and is used for encrypting packets. The corresponding private key is kept secret and is used to decrypt the ciphered packets. The distribution of public key in a secured manner is the main challenge in asymmetric key management techniques. Based on the available NEMO security protocols, we divide asymmetric key management techniques into two categories: centralized approach and decentralized approach.

6.1.1 Centralized Approach

The centralized approach uses centralized trust architecture for managing and distributing the public keys. There is only one central authority which is responsible for key generation, regeneration, and distribution. Since only one central authority is used, this approach suffers from single point failure problem. The entire NEMO security will be affected if there is a problem with the central authority. Also if the network becomes very large, then it becomes very difficult to manage the security of the entire network by a single central authority which affects scalability.

Two popular ways of distributing keys in centralized approach are public key authority and public key certificate. In [41], the authors use public key authority to distribute the public keys between the communicating nodes. The central authority maintains a dynamic directory of public keys of all nodes within a domain. Each node knows the public key of the authority with only the authority knowing its own private key. When an MR wants to communicate with a CN, it sends a time-stamped request packet to the central authority to obtain the public key of the CN. The request packet is encrypted using the public key of the MR. The central

authority sends back a reply packet which is encrypted using its own private key. The reply packet contains the public key of the CN, the original request packet and the original timestamp so that the MR can verify the freshness of the reply packet. The CN obtains the public key of MR in the same manner. The MR stores the received public key in its cache and uses it to encrypt packets for CN. The packets from MR contain the identifier of MR and a nonce. The CN copies the nonce in the reply packet which assures the MR that the sender is not an attacker.

In public key certificate approach, the central authority does not store the public key of each node. Instead, it acts as a certificate authority. The task of the certificate authority is to certify the public key of each node. Each node sends its own public key to the certificate authority in a secure manner and obtains a digitally signed certificate. The certificate contains a public key and an identifier of the key owner with the whole block signed by the trusted certificate authority. Each node uses this certificate to exchange public keys. The public key is varified using the signature of the trusted certificate authority.

6.1.2 Decentralized Approach

In this approach there is no central authority for storing the public keys. Instead, each node generates its own public/private key pair. Once the key pair is generated, the public key is made available to all other nodes and the private key is kept secret. Hence this approach eliminates single point failure problem and achieves better scalability. There are two ways, namely key announcement and key embedment, to distribute the public key of a node to all communicating nodes. In key announcement [43], a node simply sends the public key to its communicating partner or broadcasts to the community at large. Obviously, a malicious user could pretend to be a valid user and announces its own public key. Untill the valid user discovers the forgery and alerts other participants, the malicious attacker is able to read all the encrypted packets intended for the legitimate users.

In key embedment technique [33], a node binds the public component of its public-private key pair to the IPv6 network prefix. This binding is created by embedding the hash information of the public key in the network prefix. This embedded prefix allows the private key holder to claim prefix ownership by proving its knowledge of the corresponding private key. Thus key embedment technique provides security against forgery by malicious users.

6.2 Symmetric Key management

Many security protocols use only one key, known as symmetric key or shared key, to encrypt and decrypt the packets. The generation or distribution of the session key is the main challenge in symmetric key management technique. Two possible approaches are key exchange and key distribution. The key exchange algorithms are based on Diffie-Hellman algorithm key exchange algorithm [44]. The session key distribution among the senders and receivers can be managed either centrally or in a distributed fashion.

In centralized key distribution, there is a central key distribution centre and each user

shares a unique master key with the distribution centre. When two nodes want two to communicate, they obtain a one-time session key from the key distribution centre. Obviously, this approach suffers from single point failure problem.

In distributed key distribution, the session key is distributed among the users by using public key cryptography. When an MR wishes to communicate with a CN, it generates a public-private key pair and sends a packet to the CN containing its own public key and its identifier. The CN generates a secret key and sends it to the MR encrypted by MR's public key keeping it secure against eavesdropping.

6.3 Open Research Issues

Although the symmetric key cryptography is more suitable than public key cryptography in terms of computational complexity, speed and cost, no such proper key distribution scheme has been proposed yet in the literature. Diffie-Hellman algorithm was devised to generate the same private key at both communication ends so that there is no need to transfer the key over the network. But any malicious attacker can fool the legitimate parties by generating and sharing its own key. So it will cause man-in-the-middle attack even without the knowledge of the two parties. So designing efficient key distribution scheme still remains an open research area. Asymmetric key cryptography is very much expensive in terms of computational overhead. Since asymmetric key cryptography can greatly ease the design of security protocols for NEMO, it should be further studied and explored to increase the efficiency of NEMO protocols.

7. Conclusions

In this paper, we have surveyed the state-of-the-art security protocols for NEMO. We have discussed several security issues in NEMO starting with the attacks and their countermeasures. We have evaluated the existing NEMO security protocols that can prevent or mitigate the security threats along with their advantages and disadvantages. While the discussed protocols certainly add more configuration, computational, and communication overhead in NEMO, they are highly desirable. Although, these protocols can prevent attacks to some extent, none of these protocols can fully secure the system. So we have outlined few open research issues.

References:

[1] Devarapalli V., Wakikawa R., Petrescu A. and Thubert P., "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005. http://tools.ietf.org/html/rfc3963

[2] IETF Network Mobility (NEMO) Working Group. Available at: http://www.ietf.org/html.charters/nemo-charter.html

[3] Perkins C., Johnson D. and Arkko J., "Mobility Support in IPv6", RFC 6275, July 2011. http://tools.ietf.org/html/rfc6275

[4] Ernst T. and Lach H. Y., "Network Mobility Support Terminology", RFC 4885, July 2007.

http://tools.ietf.org/html/rfc4885
[5] Nautilus6 implementation. Available online: http://www.nautilus6.org/implementation/
[6] Kato A., Kusumoto H., Yamaguchi S. and Sato T., "Construction of widely integrated distributed environment", 4th IEEE Region 10 International Conference, November 1989, pp. 413-416. http://dx.doi.org/10.1109/TENCON.1989.176969
[7] CISCO IOS available at: http://www.cisco.com/en/US/products/ps6590/products_ios_protocol_group_home.html
[8] Jung S., Zhao F., Wu S. F., Kim H. and Sohn S., "Threat Analysis on NEMO Basic Operations", Internet Draft, IETF, July 2004. http://tools.ietf.org/html/draft-jung-nemo-threat-analysis-02
[9] Perera E., Sivaraman V. and Seneviratne A., "Survey on Network Mobility Support", Mobile Computing and Communications Review, vol. 8, no. 2, April 2004, pp. 7-19.
[10] Wells J. D., "A Network Mobility Survey and Comparison with a Mobile IP Multiple Home Address Extension", July 2003.
[11] Dinakaran M. and Balasubramanie P., "A Route Optimization technique for LFN-CN in NEMO", International Conference on Computer Engineering and Technology, 2009, pp. 447-451. http://dx.doi.org/ 10.1109/ICCET.2009.110
[12] Conta A. and Deering S., "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998. http://www.ietf.org/rfc/rfc2473.txt
[13] Devarapalli V. and Dupont F., "Mobile IPv6 operation with IKEv2 and the Revised IPSec Architecture", RFC 4877, April 2007. http://tools.ietf.org/html/rfc4877
[14] Sardar B. and Saha D., "Performance Analysis of Basic Support Protocol (BSP) in Nested Network Mobility (NeNEMO)", International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2013, pp. 1430-1435. http://dx.doi.org/10.1109/ICACCI.2013.6637389
[15] Shahriar A. Z. M., Atiquzzaman M. and Ivancic W., "Route Optimization in Network Mobility: Solutions, Classification, Comparison, and Future Research Directions", IEEE Communication Surveys and Tutorials, vol. 12, issue 1, 2010, pp. 24-38. http://dx.doi.org/ 10.1109/SURV.2010.020110.00087
[16] Lim H. J., Kim M., Lee J. H., and Chung T. M., "Route Optimization in Nested NEMO: Classification, Evaluation, and Analysis from NEMO Fringe Stub Perspective", IEEE Transactions on Mobile Computing, vol. 8, issue 11, November 2009, pp. 1554-1572. http://dx.doi.org/10.1109/TMC.2009.76
[17] Sirkar A., Sardar B. and Saha D., "ROTIO+: A Modified ROTIO for Nested Network Mobility", International Conference on Distributed Computing and Networking, 2010, pp. 307-322.
[18] Ng C., Thubert P., Watari M. and Zhao F., "Network Mobility Route Optimization Problem Statement", RFC 4888, July 2007. http://tools.ietf.org/html/rfc4888
[19] Hossain M. S., Atiquzzaman M. and Ivancic W., "Performance Analysis of NEMO using City Section Mobility Model", 13th International Conference on Computer and Information Technology, 2010, pp. 516-521. http://dx.doi.org/10.1109/ICCITECHN.2010.5723911
[20] Han S. and Jeong J., "Design and Performance Analysis of Cost-Effective and Fast Inter-Domain Network Mobility Schemes", 2nd International Conference on Computer

Science and Network Technology, 2012, pp. 473-476. http://dx.doi.org/10.1109/ICCSNT.2012.6525980

[21] Almodovar J. L., Oliva A. D. L., Ram C.L. and Pastor C.C., "Performance Analysis of a Lightweight NEMO Implementation for Low-End devices", TridentCom '08 Proceedings of the 4th International Conference on Testbeds and research infrastructures for the development of networks & communities, Innsbruck, Austria — March 17 - 20, 2008.

[22] Lee J. H., Ernst T. and Chilamkurti N., "Performance Analysis of PMIPv6 based Network Mobility for Intelligent Transportation Systems", IEEE Transactions on Vehicular Technology, vol. 61, issue 1, January 2012, pp. 74-85. http://dx.doi.org/10.1109/TVT.2011.2157949

[23] Chowdhury P.K., Atiquzzaman M. and Ivancic W., "SINEMO: An IP diversity based Approach for Network Mobility in Space", 2nd IEEE International Conference on Space Mission Challenges for Information Technology", 2006, pp. 115-122. http://dx.doi.org/ 10.1109/SMC-IT.2006.68

[24] Stewart R., Xie Q., Tuexen M., Maruyama S. and Kozuka M., "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration", RFC 5061, September 2007. http://tools.ietf.org/html/rfc5061 RFC 5061,

[25] Chowdhury P.K., Reaz A. S., Atiquzzaman M. and Ivancic W., "Performance Analysis of SINEMO: Seamless IP diversity based Network Mobility", IEEE International Conference on Communications, June 2007, pp. 6032-6037. http://dx.doi.org/ 10.1109/ICC.2007.999

[26] Rahman S. M., Bouidel O., Atiquzzaman M. and Ivancic W., "Performance Comparison between NEMO BSP and SINEMO", IEEE Global Telecommunication Conference, December 2008, pp.1-5. http://dx.doi.org/ 10.1109/GLOCOM.2008.ECP.461

[27] Hossain M S., Atiquzzaman M. and Ivancic W.,"Scalability analysis of a multihomed Network Mobility Protocol", IEEE GLOBECOM Workshops, December 2011, pp.513-517. http://dx.doi.org/ 10.1109/GLOCOMW.2011.6162502

[28] Ernst T., "Network Mobility Support Goals and Requirements", RFC 4886, July 2007. http://tools.ietf.org/html/rfc4886

[29] Modares H., Moravejosharieh A., Lloret J. and Salleh R., "A survey of secure protocols in Mobile IPv6", Journal of Network and Computer Applications, August 2013. In Press. http://dx.doi.org/10.1016/j.jnca.2013.07.013

[30] Petrescu A., Olivereau A., Janneteau C. and Lach H. Y., "Threats for Basic Network Mobility Support (NEMO threats)", Internet Draft, IETF, November 2003. http://tools.ietf.org/html/draft-petrescu-nemo-threats-00

[31] Atiquzzaman M. and Hossain S., "Security Issues in Space Networks", NASA Earth Science Technology Conference, June 2011.

[32] Ng C. and Hirano J., "Extending Return Routability Procedure for Network Prefix (RRNP)", Internet Draft, IETF, October 2004. http://tools.ietf.org/html/rfc3667#section-3

[33] Kukec A., Bagnulo M. and Oliva A.D.L., "CRYPTRON: CRYptographic Prefixes for Route Optimization in NEMO", IEEE International Conference on Communications, 2010, pp. 1-5. http://dx.doi.org/ 10.1109/ICC.2010.5502418

[34] Krawczyk H., Bellare M. and Canetti R., "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[35] Ferguson P. and Senie D., "Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing", RFC 2827, May 2000. http://www.ietf.org/rfc/rfc2827.txt
[36] Ng C., Ernst T., Paik E. and Bagnulo M., "Analysis of Multihoming in Network Mobility Support", RFC 4980, 2007. http://www.ietf.org/rfc/rfc4980.txt
[37] Ken S. and Atkinson R., "IP Authentication Header", RFC 2402, November 1998. http://www.ietf.org/rfc/rfc2402.txt
[38] Kent S., "IP Encapsulating security Payload", RFC 4303, December 2005. http://www.ietf.org/rfc/rfc4303.txt
[39] Tan T.K. and Samsudin A., "Fast and simple NEMO authentication via Random Number", IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, May 2007, pp. 266-271. http://dx.doi.org/10.1109/ICTMICC.2007.4448643
[40] Tan T. K. and Samsudin A., "Efficient NEMO Security Management via CA-PKI", IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, May 2007, pp. 140-144. http://dx.doi.org/10.1109/ICTMICC.2007.4448618
[41] Tan T.K. and Samsudin A., "PKI and Secret Key Cryptography Implementation for NEMO Security", International Conference on Computer and Communication Engineering, 2006, pp. 168.
[42] Li L.S., Tzeng S.S., Bai R.C. and Li M. T., "End to End Security and Path Security in Network Mobility", 40th International Conference on Parallel Processing Workshops, 2011, pp.16-21. http://dx.doi.org/ 10.1109/ICPPW.2011.35
[43] Fathi H., Shin S., Kobara K., Chakraborty S. S., Imai H. and Prasad R., "LR-AKE-Based AAA for Network Mobility (NEMO) Over Wireless Links", IEEE Journal on selected Areas in Communications, vol. 24, issue 9, September 2006, pp.1725-1737. http://dx.doi.org/10.1109/JSAC.2006.875111
[44] Stallings W., "Cryptography and Network Security", Pearson Education, Fourth Edition.

Copyright Disclaimer