Proceedings of the 2007 IEEE International Conference on Telecommunications and
Malaysia International Conference on Communications, 14-17 May 2007, Penang, Malaysia

Efficient NEMO Security Management via CA-PKI

Tat Kin Tan and Azman Samsudin
School of Computer Sciences, Universiti Sains Malaysia, 11800 Penang, Malaysia.
tatkin@cs.usm.my, azman@cs.usm.my

***Abstract*— Network Mobility (NEMO) has gained much momentum ever since being introduced. The concept of NEMO, is actually building on top of the MIPv6 and using MIPv6 as its backbone. The differences are much align at the capability of the Router being able to roam freely, hence the term Mobile Router (MR). Whereas in the MIPv6 world, there is only fix Access Router (AR). Since the NEMO is directly associated with MIPv6 as the backbones building blocks, the NEMO concepts has also inherits the security management systems of which MIPv6 is adapting. As the matter of fact, the NEMO concept has exposed greater security risks with the use of IPSec as the security design. Coupled with nested looping concept and capability that NEMO offered, the use of IPSec as the security design will no longer be sufficient from the efficiency point of view. In this paper, we will illustrate the use of IPSec on NEMO, and zooming into the instances whereby nested looping comes into picture and how security system will be at risk and finally proposing a new security design system to counter the inefficiencies.**

***Index Terms*—Network Mobility (NEMO), Mobile Network Notes (MNN), Mobile Router (MR), Mobile Internet Protocol version 6 (MIPv6).**

I. Introduction

FOR MIPv6, the basic communication model involved several mobile hosts (MH). The Mobile Network Node (MNN) communicates to Correspondent Node (CN), which in turn, is indeed another MN. The communication also involved Home Agent (HA) and Access Router (AR) [1]. The major functionality of the AR in MIPv6, will merely be a router that provides routing functionality and being the gateway routing for inbound and outbound IPv6 traffics. While the HA supports the MIPv6 protocol as playing the rule as the agent that keep tracks on the whereabouts of MNNs when MNNs roamed out away from the home network. All these protocol had been described in details in [1].

While the technology evolved everyday, the thoughts of the AR that would enjoy the mobility came into picture. The concept of "moving router" will introduce the idea of "network that moves" and hence the term NEMO is being established.

The NEMO inherited the concept of MIPv6 with the fact that, the AR is on the mobility side and hence termed as MR [2]. The functionality of HA remains the same, so as the security design of using IPSec as the core security design. Part of the MR's responsibilities will also include the subnet distribution and management, ie: prefix delegation [7]. The basic communication model for NEMO can best be illustrated in Figure 1 and the detailed protocol description can be found in [2], [5].

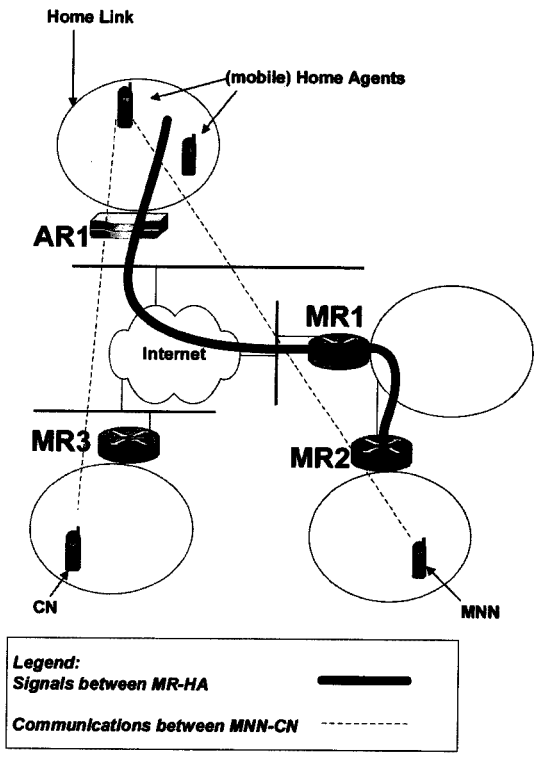

Figure 1: Simple NEMO Communication

Since the introduction of NEMO, there are more and more new design concepts being derived out from NEMO, such as the nested loop concept, prefix-delegation [7] and many more. Nested Mobility [4] and other NEMO home network models [3] are not the scope of this paper.

The NEMO protocol offers mobility and transparency

especially on the nested topology within a mobile network. Current NEMO implementation that come with and MIPv6 as the underlying carrier protocol suggested and in favor of the deployment of IPSec with Security Association (SA), and Encapsulating Security Payload (ESP) implementations. While it is not wrong, showed in various solid design specification on the usage of IPSec in MIPv6 and NEMO, still there exist many questions surrounding the use of IPSec. There are many research papers, NEMO discussion forum as well as NEMO working group already shown that the IPSec of NEMO had introduce inefficiency and design flaws [6], [8], [9]. The NEMO security threats have also been widely discussed as being pointed out in [13].

II. PROBLEM STATEMENT

For implementation of IPSec that enables MNN to exchange data to HA or CN, the appropriate Security Association Database (SAD) has to be available [10][11]. This also means that a set of security policies called Security Associations between two nodes that wish to communicate, will have to be synchronized and going thru the protocol handshake. The SAD may contain for instance a list of encryption standards from 1) Advance Encryption Standard (AES); 2) Digital Encryption Standard (DES); 3) Tripple DES (3DES) and with various encryption algorithms such as Cipher Block Chaining (CBC), Counter Mode Encryption with CBC-MAC authentication (CCM), Electronic Code Book (ECB) and many more variants [12]. For each algorithm to multiply with each encryption standards the SA database can be huge and hence for two communication nodes that wish to converse and the process of establishing and get the SA to sync up to agreeing which combination of policies to be used, the process is expensive and impact the performance of the system as a whole.

One of the problems of NEMO protocol is the performance in security encryption. For instance, MNN may have 4 sets of SA while CN could have 5 sets (or more). For MNN to be able to have conversation with CN, both sets of SA need to be synchronized. The computation overhead to synchronize between 2 sets of SA will be expensive.

When we consider the security design with these entities and topology in mind, it appears strongly that IPSec may not be the best solutions to be deployed in terms of performances. The involvement of IPSec in this case, may not yield efficiency in terms of overall performance.

Refer to Figure 2 for more illustrative example, and imagine that before MR1 detached from its current point of attachment, this mobile network contained 2 nested mobile networks within. Let us view that within these 2 nested mobile networks, each of them contained a MNN2 and MNN3.

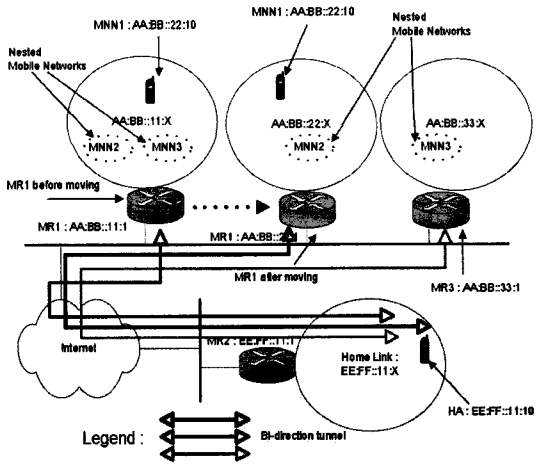

Figure 2 Potential problems in Nested Mobile Networks when changes in topologies

When the MR1 roamed into another point of attachment and being given a different CoA and hence having another different IPv6 prefixes, the nested mobile networks are separated with the first nested network staying still together with the movement and the second nested network moved into other domain. This situation is possible for instance due to the better signal strength offered by MR3, of which the second nested network physically and topologically closed to. Nevertheless, the second nested network has turned into Visiting Mobile Node (VMN) for MR3's mobile network.

Since the first nested network (MNN2) is still topologically following its original mobile networks, the session connectivity will still be similar in the sense of using similar tunnels and hence the IPSec configuration would probably have not changed too much (if IPSec is implemented). This is because the MNN2 is still working under the same MR1 prior to the movement. In short, regardless of the movement the second top level connection point (MR) is still the same. Security Association configurations of IPSec protocol processing overhead for changes may still be minimal.

However, this is not quite the same for MNN3 which is now happened to have discovered that the MR would not be the same MR of its original attached to. This discovery may in turn trigger a Fast Handover process and hence the associated overheads. If the MNN3 is in the middle of communicating with other CN, the changed of attachment will introduce even more overheads in terms of Fast Handover processing. If MNN3 was using SA of IPSec, the MNN3 will have to re-initiate association process again simply because its MR has been a different MR and hence the bi-directional tunnel will be different. Recall that the bi-directional tunneling was previously connected from MNN3-MR1 and now it seemed to be needed as for MNN3-MR3. Since the MNN3 prior to the MR changed of MR's point of attachment, has been using a trusted tunnel, the MNN3 has no way could use the tunnel in MR3 and still expecting the old security association (of the first tunnel) configurations will work for the third tunnel. The

change of attachment here possibly will trigger a protocol to detach the tunnel of MNN3-MNN1 (old tunnel) and then initiate a new attachment to MNN3-MR3. Or, establish another secure tunnel from MNN3-MR3, and with this secure tunneling (a separate set of IPSec+SA), re-tunnel back to MR1 as the access connection. So in short, the communication path from MNN3 would be like : MNN3-MR3(secure IPSec tunnel1)-MR1(Secure IPSec tunnel2)-MR2-CN. This will introduce overheads in terms of protocol and encryptions.

The CN that the MNN3 was communicating with, will have to re-negotiate a different set of security bindings, i.e.: the SA, with MNN3 again. The CN will still yet to authenticate the MNN3 (now at MR3) to ensure it is still a true MNN3 and not some malicious attacker from MR3's tunnel trying to gain access.

The situation become worsen when there is multi levels and multi layers of nested looping, where each layer of looping will introduce a sub-layer of re-tunneling when a MR roams. Simple example as : if there is n level of MR attaching each other and forming tunnels, upon detaching there will be n level of detaching as well. Performance as in overall system will hence be dropped, and end-to-end tunnels policy maintenance is expensive.

III. THE SOLUTION

Roaming from one network to another one network has been perceived to have protocol overheads as shown in the problem section.

The main culprit behind this problem is the IPSec and the Security Association. As elaborated, the grey area is still existed on the re-binding or multiple bindings of the SA after the NEMO movements at each level and typically in a multi level/layer of nested loop.

A different solution for security which do not particularly need Security Association of IPSec would much be able to resolve the issue and hence enhance the overall system performance. The solution shall look into the area of simplifying the security management area especially that can anticipate frequent roaming and movements.

Our idea is to deploy a centralized binding system eg: introducing Certificate Authority (CA) that is managed by either application layer or by Internet Service Provider (ISP). The key design concept is that, how to keep the movement mobility to the optimum without interrupting the existing protocol. It appears that every time a movement is being detected, the security portion (mainly the policy) will have to change. This is like a tight "border" or "custom" or "immigration" control. That is, if we can introduce a border-less control, by the means of using a centralized and trusted database, with the main objective for authentication purposes. By doing this, whenever there is a movement occurred, there will be no necessity of re-established tunneling.

Refer to Figure 3, the Public Key Infrastructure (PKI) concept can be deployed. The server is provided by ISP with the similar concept of today's ISP. Applying the concept into NEMO, MNN will have to register to ISP to use the service. Just like today's mobile device (eg: PDA or mobile cell phone) that wishes to use the service, the device will have to subscribe to the service. The CA/Server will then provide PKI services such as Public and Private key exchanges to the devices and storing in the central and trusted database.

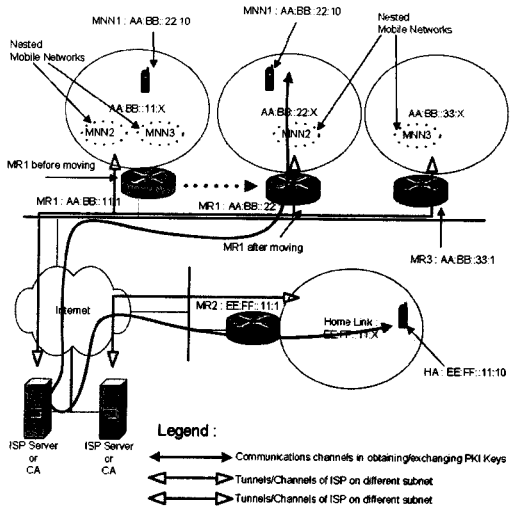

Figure 3 : ISP Server as CA to provide PKI services

Whenever a MNN roams, the MNN will need to talk to the ISP/CA only when it needs to refresh the Private Key Exchange (PKE) keys. Otherwise there is not necessary to re-establish any security policies or contacts. Without re-establishing policies or contacts, there will be lesser overheads on system protocol exchanges and hence faster communications.

IV. BENEFITS

In terms of security wise and the processing, if IPSec is deployed, stronger encryptions may be available but with the tradeoff of more expensive computing power or cycles needed on every roaming that causes new CoA being assigned. If PKI is being use, only simple block encryption is needed and this system's strength is maximizing the Public/Private Key Exchange mechanism to distribute a secret key (refer to Figure 4 on how this can be done).

Refer to Figure 4, below are the steps on how PKE mechanism can be implemented:

1) The MR will request the Public Key of CN from a trusted CA. This request will have an association to Time (t1).
2) CA responded to the MR by encrypting the message using CA's private key. This way the MR can decrypt the message using CA's public key which is openly available. The message contains CN's public key and the original request from MR,

and the time stamp. This is to allow MR compared the message and hence authenticate the integrity of the message.

3) MR can then encrypt message (which is the RN1 being generated) with CN's public key. This message will contain the MR's identifier as well.

4) CN decrypt the message using its own Private Key and retrieve the MR's identifier as well as the RN1. CN will send request to the trusted CA in order to obtain MR's Public Key. This step is similar to how MR obtained CN's Public Key.

5) CA will perform identical process (similar to step 2) which is to deliver MR's Public Key to CN.

6) CN can now encrypt a new message to MR, containing the RN1 as well as newly generated Secret Key. When the message arrived to MR,

7) By now the Secret Key has been securely shared between MR and CN and the further communications done between MR and CN will be via this symmetric encryption.

8) CN decrypt the message via the Secret Key and in return will start using this Secret Key for further communications to MR.

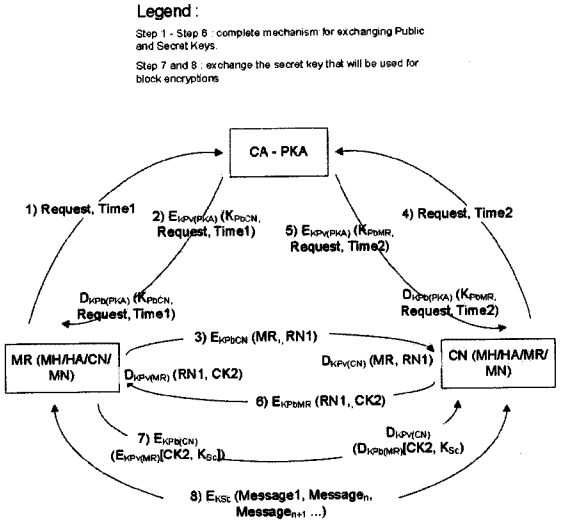

Figure 4 : PKE mechanism

In short, step 1 to step 6 of Figure 4 are the core Public and Private Key exchange mechanism. After both communication devices had established the trust between them, both can use the channel to deliver a secret key for both to perform encryption/decryption as shown in Step 6 and Step 8 of Figure 4. This cryptography is using much simpler and much faster symmetric encryptions.

Another benefits of using PKI is that, once the trust has been establish, there will be no further needs of re-establishing and re-agreeing the SA as being opposed in using IPSec; even though the initial establishment of PKI may be expensive, such as going thru the first 6 steps (as in Figure 4) to obtain Public and Private keys. However once the initial communication has established, the MR1 that roamed, do not have to re-setup or tear down tunnels in order to re-establish secure tunnels and hence this is also a big plus in nested loop scenario

As for implementation perspective, overhead on protocol processing will be lesser with this new proposal.

For software coding perspective, the new proposal only introduce several steps for initial PKI setup compared to huge and complicated IPSec implementation.

Another advantage is that this proposal is using centralize policies maintenance such as at ISP and not as proposed in the standard of maintaining security policies (SA) at tunnel-to-tunnel end point.

V. CONCLUSION

We presented the scenario of using IPSec as the security design especially with the involvement of SAD and ESP. Coupled with the scenario of nested looping with multilayer tunneling, the security design exposed the fragility from the point of efficiency and in the terms of performance.

Currently, it is recommended to be using IPSec as the primary security standards for MIPv6 and NEMO. The IPSec implementation generates a huge amount of processing overheads because IPSec requires both MN and CN (and hence Mobile Router as well) to agree upon SA (Security Association) which is a set of encryption standards. The new proposal will save the processing overhead tremendously by eliminating the need of IPSec's SA and ESP(Authentication Header as well) and by introducing a simple Secret Key Encryption methodology with PKE mechanism.

Our solution of introducing a centralize binding system such as involving CA with PKI concept, will help to eliminate the overloading computations of protocol and security performance. Our solution starts with having CA as the central point of controlling communications and authentication. Once the protocol has been established, the switch of using symmetric encryption for data integrity protection will be able to reduce the cost encryption tremendously. By eliminating the needs of re-establishment for re-tunneling, protocol encryption processing overhead can be reduced and achieving greater efficiency for overall performance.

REFERENCES

[1] Johnson, D., Perkins, C., Arkko, J., "Mobility Support in IPv6", IETF RFC3775, June 2004

[2] Devarapalli, V., Wakikawa, R., Petrescu, A. and Thubert, P., "Network Mobility (NEMO) Basic Support Protocol". IETF RFC3963. January 2005

[3] P. Thubert., R. Wakikawa., V. Devarapalli., "NEMO Home Network Models". Internet Draft, IETF. Draft-ietf-nemo-home-network-models-06.txt. February 2006.

[4] T. Ernst., H-Y. Latch., "Network Mobility Support Terminology". Internet Draft, IETF. Draft-ietf-nemo-terminology-06.txt. November 2006.

[5] T.K. Tan., A. Samsudin., "Secure Hashing of the NEMO Mobile Router Communications". MICC-ICON 2005, IEEE 05EX1235, November 2005

[6] T.K. Tan., A. Samsudin., "PKI and Secret Key Cryptography Implementation for NEMO Security". *Proceedings of the Int. Conf. on Computer and Communication Engineering, ICCCE'06* pg168, 2006.

[7] T. Kniveton., P. Thubert., "Mobile Network Prefix Delegation". Internet Draft, IETF. draft-ietf-nemo-prefix-delegation-00.txt. August 2005.
[8] Deng, R. H., Zhou, J., Bao, F., "Defending Against Redirection Attacks in Mobile IP" ACM CC @ '02 November 2002
[9] Qiu, Y,. Zhou, J., Bao, F., "Protecting All Traffics Channels in Mobile IPv6 Network" WCNC 2004 @ '02 November 2002
[10] F. Dupont., J-M. Combes. Using IPsec between Mobile Nodes and Correspondent IPv6 Nodes. Internet Draft, IETF. draft-ietf-mip6-cn-ipsec-03.txt. August 2006.
[11] J. Arkko, V. Devarapalli and F. Dupont. Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents. IETF RFC3776. June 2004.
[12] Stallings, W., "Cryptography and Network Security", Third Edition, Prentice Hall
[13] Petrescu, A., Olivereau, A., Janneteau, C. and Lach H.-Y., "Threats for Basic Network Mpbility Support (NEMO threats)" Internet Draft, IETF. Draft-petrescu-nemo-threats-01.txt. January 2004.