The Effect of Route Routability Procedure to the Route Optimization Distribution Binding Update

[1]Mohamed Y Abdelsalam, [1]Rashid A Saeed, [2*]Raed A Alsaqour

[1]Department of Electronics Engineering, Faculty of Engineering, Sudan University of Science and Technology (SUST),Khartoum, Sudan

[2]School of Computer Science, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Selangor, Malaysia

***Abstract*— With the demand of mobility by users, wireless technologies have become the hotspot developing arena. Internet Engineering Task Force (IETF) working group has developed Mobile IP (MIP) to support node mobility. The concept of node mobility indicates that in spite of the movement of the node, it is still connected to the internet and all data transactions are preserved . Network Mobility (NEMO) basic support protocol is proposed to describe the node mobility procedures, but NEMO suffers from many problems like pinball and security aspects. Route Optimization Distribution Binding Update (RODBU) is a routing mechanism proposed to eliminate these problems In this paper, we study the effect of the security aspects to RODBU mechanism and see how the performance will effect by adding RRP to the mentioned mechanism.**

Keyword- MIP, NEMO, ROBDU, RRP

I. INTRODUCTION

The Mobile IPv6 protocol [1] was introduced by the Internet Engineering Task Force (IETF) to support the host mobility (individual IP devices). The MIPv6 maintains the session continuity between the Mobile Node (MN) and its Correspondent Node (CN) regardless of the MN current point of attachment to the Internet. The MIPv6 uses the Home Agent (HA) to send or receive the packets between the current location of the MN and its CN.

The IETF has established a "NEMO Work Group" to offer a basic mobility solution based on the concept of the MIPv6 protocol to support an entire IP network instead of a single host. However, the solution has to be flexible to deal with the different mobile networks configurations, in particular, the networks that are composed from different subnets and nested mobile networks. A Mobile Router (MR) is considered to be the main mobile entity in the NEMO basic support protocol in order to manage the mobility of the entire network. The MR has two interfaces, i.e., the Egress interfaces that attach the MR to the Internet, and the Ingress interface to connect the MR to their Mobile Network Nodes (MNNs). MNNs are devices belonging to the network that obtain connectivity through the MR. All packets to/from MNN should be routed through the Bidirectional Tunnel (BT) established between the MR and its HA. The HA then encapsulates these packets and forwards them to the MR. The MR, in turn, decapsulates the packets and forwards them to the MNN.

The NEMO basic support protocol-is an extension of the MIPv6 protocol which is inherent in the limitations of suboptimal routing. The problems associated with the packet delivery, such as pinball routing problem which leads to bottle neck for traffic, latency in network and handover delay [2].

A mobile network (sub- NEMO) is said to be nested when it is attached to a larger mobile network (parent-NEMO). The aggregated hierarchy of mobile networks becomes a single Nested NEMO as pointed out in Fig. 1, such as, when multiple MRs are connected together in the nested fashion.

A Nested NEMO has limitations in routing the traffic which amplifies the suboptimal routing issues (Pinball Routing problem- as will be explained in section 4). Technically, a Route Optimization mechanism comes up with complementing solution for this pinball problem as mentioned in (Ng, 2007; Ng, 2007).

In the case of the nested NEMO networks as shown in Fig. 1, these problems and suboptimal NEMO Route Optimization (NEMO-RO) issues will be amplified.

The rest of the paper organized as follow: Section 2 presents the Pinball routing problem, section 3 introduces the NEMO network security, section 4 illustrates the return routability procedure. Route optimization distribution binding update presented in section 5. Sections 6 discuss RRP and NEMO security issues, Section 7 and 8 presents the simulation settings and simulation results and section 9 concluded the paper.

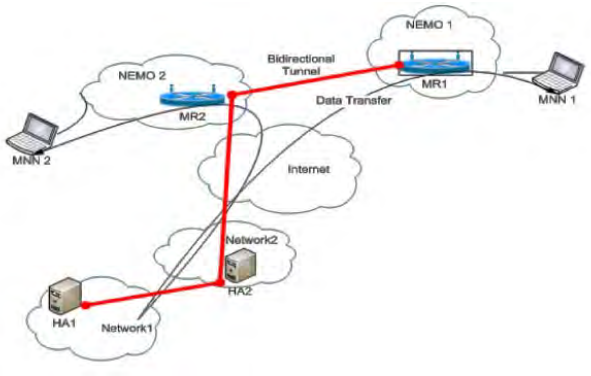

Fig. 1. Nested NEMO network

II. PINBALL ROUTING PROBLEM

In case of nested NEMO network, several tunneling occurs and this leads to several intricacies. One of the significant problems regarding the nested NEMO is the pinball routing problem. Both inbound and outbound packets will flow via the

HAs of all the MRs on their paths within the mobile network, with increased latency, less resilience and more bandwidth usage.

When a MN sends a message to a distant CN, it may pass through several MRs. On reaching each MR, a tunnel has to be established with the HA of the corresponding MR. Thus, for a single data transmission, the packet has to traverse through various MRs and their corresponding HAs. When the mobile network moves to a new location, the new location has to be informed to the HA of the mobile network. This Binding Update (BU) and Binding Acknowledgement (BA) has to pass through several MR-HA tunnels [3].

This process is called as pinball routing. This mechanism can be well described by considering a scenario in Fig. 2. In Fig. 2, three mobile networks are considered MN1, MN2, and MN3. These are managed by the routers MR, MR1, MR2 and MR3. MN1 is directly connected to its home network through internet and the Access router (AR). MN2 and MN3 access their home network through MR1and MR2 respectively; MN2 and MN3 are forming a two level nested mobile network. The packets sent in the network undergo tunneling process [4]. Fig. 2, shows the routing path between Visiting MN (VMN) (MN3) to its home agent HA3.

Fig. 2, shows the routing path between VMN to its home agent HA3. When VMN present in mobile network MN3 wants to send a data packet to it's HA, the packet is sent to MR1 then the packet is forwarded to AR, HA of MR3 followed by HA of MR1 and finally to the CN. Thus, when the router in the network receives a data packet, it is first forwarded to its home agent and then the data packets are forwarded to the destination node. This process of tunneling increases with the increase in the number of nest levels in the network.

The various problems that occur due to pinball routing are: increased processing delay, increased chances of packet fragmentation, increased susceptibility to link failure and increased packet size.

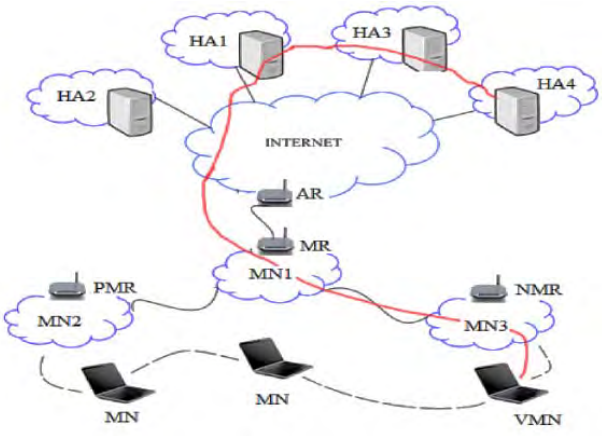

Fig. 2. Pinball routing problem

III. NEMO NETWORK SECURITY

The demand for Internet access in heterogeneous environments is keeps on increasing, especially in mobile platforms such as trains, buses. The request for connecting with Internet on the move is for entertainment, sometimes to connect with official network of the mobile users too [5]. NEMO extends the basic end-host

mobility support protocol, MIPv6 for providing mobile network support. There are various issues in terminal mobility like routing, hand-off, QoS and security. In NEMO, the security mechanisms are needed to ensure secured packet transmission between the CN and MNN. The BU provides authenticity and integrity to the packets therefore incorrect BU can lead to malicious attacks such as traffic hijacking, Denial of Service (DoS), resource consumption, black hole and man in the middle attacks [6-8]. If the MN moves out of its home network, it starts searching a new router called AR to provide service from the visited network. With the help of AR, the MN maintains connectivity with its HA. But if the MN joins with a new network, topologically it's not possible to maintain the address assigned by the home network. So a new address Care-of-Address (CoA) will be assigned by the AR, then the MN has to send an update to its HA about its new CoA. The process of updating new CoA to the respective HA or CN is BU. This process is implemented once again if the MN performs handover. The MNs duty is to update the new binding always to HA; it ensures the message integrity between these nodes and assures the HA about the legitimate MN. BA message will be a reply from HA for the update [9].

An attacker may claim spoofed information that a particular legitimate MN is in different location than where it supposes to be. If HA believes that information and works based on it, and then the respective MN may not get the traffic at all. A malicious MN may use the Home-of-Address (HoA) of a victim legitimate node in forged BU sent to a CN. These kinds of attacks generate the threats against the confidentiality, integrity and availability of the MNs.

An attacker may go through the contents of a packet destined to another node by redirecting the traffic to it. This leads to man in middle attack between MN and the CN. An attacker may also send forged BU with help of current CoA of the legitimate MN. The acceptance of such BU leads to attract the CN's reply and furthermore the DoS attack towards the victim node. An attacker may also replay the BU that the MN had sent earlier as an attempt to interrupt its communication. If the replayed old BU is accepted then the packets towards the MN will be sent to its old location, where as MN is now in new location. A malicious node related to multiple HAs can create routing loop amount the HAs. This can be attained when a MN binds one HoA located on a first HA to another HoA on a second HA. This kind of BUs will lead the HAs to route the same packets among each as they were not aware of the routing loop.

IPSec Encapsulating Security Payload (ESP) provides a secure transfer of BU and BA messages between MNs and the respective HA. As IPSec is not assuring about the correct ordering delivery of the message, sequence number can be used to ensure the correct ordering of messages. If at all dynamic keying used for data transfer, IPSec can provide anti-replay protection. Replay and reordering attacks are possible if the 16-bit MIPv6 sequence number is cycled or the HA loses the state related to the sequence number and the same is applicable if the HA reboots. So, in order to prevent such attacks it is better to use dynamic keying, IPSec anti-replay protection and sequence numbers together. A non volatile memory can be used for HA, so that the state cannot be lost [10, 11].

IV. Return Routability Procedure

The use of Return Routability Procedure (RRP) provides good support to MIPv6 without any security issues. This procedure verifies the message exchange between the HA and MN's CoA to ensure if both the nodes are reachable [12]. The BU messages are exchanged cryptographically. When symmetric attack is used always the response is sent to the node from where the request has come, which avoids the reflection attack. The CN must wait for authorized BU form the MN. The encapsulation tunnel also carried out through encryption between HA and MN with IPSec ESP. Nonce exchange through tunnel avoids the possibility of attackers to verify the nonce message, hence the attack from the visited network can also be prevented. The RRP mechanism guards the BU exchanges from all attackers, who are unable to watch the path between the MN and the respective CN. DoS attacks can also be protected through RRP.

MAC verification will identify the modifications in BU, so that the modification in BU is also protected. The exhaustion of resources against DoS attack can be protected by RRP. Keygen tokens from nonce and node keys, which are not specific to individual MN, are used to send an authentic BU from the MN to the respective CNs. The CN reconstructs the Keygen tokens based on the CoA or HoA through the BU of the MN. Thus memory exhaustion attacks can be prevented at the CN except where on path attackers are concerned. Usage of symmetric cryptography makes the CN to be safe against Control Processing Unit (CPU) resource exhaustion attack also. An attacker may try to fool the MN and CNs to request BU each other. In some scenarios if CN gets large numbers of BUs like flooding, this may lead to fail in cryptographic integrity checks. In such scenarios, CN can stop processing the BUs itself. If it finds that its spending more time and resources on processing forged binding updates, it can discard or all binding updates without even performing the cryptographic operations [13].

Generally attackers may try to break the RRP in multiple ways. Sufficient 64 bit cookies are used by RRP to protect against spoofed responses. 128 bits of information are used to provide the tokens; this can be an internal input to a hash function. The hash function uses HMAC_SHA1 algorithm [14] to produces 160 bit quantity

suitable for secured keyed hash of 96 bits length in the BU. The home Keygen token and care of Keygen token are the two pieces of 128 bit tokens. It requires very large number of messages, if an attacker tries to guess the correct cookie value. The cookies are valid for short period of time, hence attacker has to maintain high constant message rate which is not possible [15].

V. ROUTE OPTIMIZATION DISTRIBUTION BINDING UPDATE

From [16, 17], RODBU is a route optimization mechanism with the following features:

- Support route optimization for nested mobile network. The route for signaling and data transmission is optimized so that the pinball problem as well as multiple tunnels and encapsulation can be avoided.
- Support the intra-domain data communication, data transmission within the same mobile network or the root-MR can be accomplished without sending packets through any HA.
- Shorter handover delay.
- No bottleneck: packets are not necessary to pass through the HA to avoid the bottleneck of the HA.
- No binding update storm: not all MNs need to perform the BU to prevent BU storm.

In RODBU, direct tunnel to the root-MR for route optimization is employed without the BU storm. Therefore, every HA of MNs inside a mobile network is informed of the CoA of the root-MR through the packets interception by the HA, The HA tunnels the packets to the root-MR. For data transmission inside the mobile network, RODBU uses routing tables. When handover occurs, the HAs have to be informed of the CoA by distributing this message to several HAs according to the nesting level of the MR. in RODBU the following tables are utilized:

- Routing table: the routing table is used by each MR inside the mobile network for the purpose of path selection in the wireless portion. With this table, an MR can decide which path to send to one of sub-tree MRs.
- Subtree list table: this table is used by each HA of an MR inside the mobile network to record all HAs of one hop sub-tree MRs. This table is used to distribute the BU message regarding the CoA of a new root-MR.

RODBU categorizes binding update in to:

- Local Binding Update (LBU): it send by an MR to its parent MR to maintain routing table of its parent MR.
- Registration Binding Update (RBU): is send by an MR to its HA to add the HA of a new joining node into the sub-tree list.
- Distributing Binding Update (DBU): its send by an HA to all HAs in its sub-tree list to inform these HAs of a new CoA of the root-MR.
- Handover Binding Update (HBU): it's used to perform the deregistration procedure.

For RODBU, three operations are necessary, node registration, packet routing and handover.

A. Node Registration in RODBU

MNs are categorized into three types, i.e. MNN, MR and root-MR in RODBU (see Fig. 3). An MNN is a node capable to change the point of attachment to the network within the mobile network and has no capability of packet forwarding. An MR has capability to forwarding packets to its sub-tree. As shown in Fig. 3, the MR connected to the internet through ingress/egress interfaces and called root-MR. For all kind of MNs, the same registration procedure is involved. Each MR has a routing table as shown in Table I for selecting the right path to the destination. For all HAs it maintain subtree list table as shown in Table II for distributing the CoA of the root-MR.

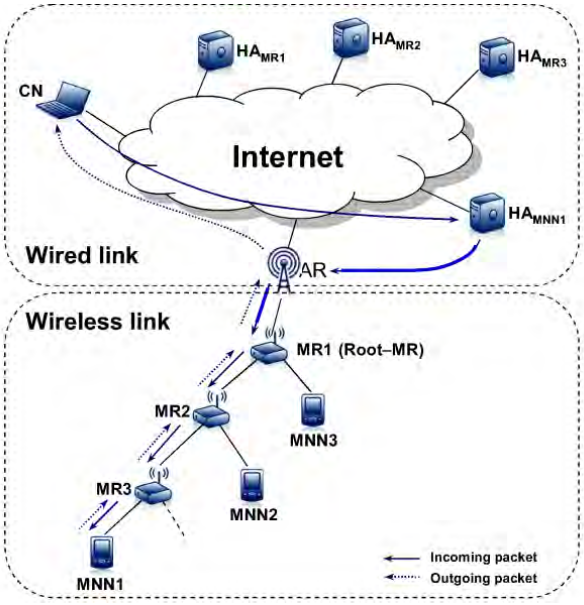

Fig. 3. The scenario for RODBU [17]

TABLE I
The Routing Tables for Nodes in Fig. 3

Node	Routing table
MR1	HoA of MR2 – CoA of MR2 HoA of MR3 – CoA of MR2 HoA of MNN1 – CoA of MR2 HoA of MNN2 – CoA of MR2 HoA of MNN3 – CoA of MNN3
MR2	HoA of MR3 – CoA of MR3 HoA of MNN1 – CoA of MR3 HoA of MNN2 – CoA of MNN2
MR3	HoA of MNN1 – CoA MNN1

TABLE II
The Subtree Routing Tables for Nodes in Fig. 3

Node	Subtree list table
HA of MR1	HA of MR2 HA of MNN3
HA of MR2	HA of MR3 HA of MNN2
HA of MR3	HA MNN1

In node registration procedure, the related information is recorded using the LBU message and DBU message in order to make routing tables and subtree list tables available. Fig. 4) depicts the message flows for the node registration procedure. All MRs periodically send a Router Advertisement (RA) message contains a Mobile Network Prefix (MNP) and the CoA of the root-MR. If a new joining node does not receive this message in certain time, it sends Router Solicitation (RS) message to its neighbor for asking of a new connection to this network. Once the new joining node receives the RA message, it creates its CoA and stores the MNP along with the CoA of the root-MR and the senders address, which the CoA of the parent MR MR_{d-1}

In Fig. 4, the MNN/MR_d sends LBU message containing its HoA along with senders address, i.e. the CoA of the MNN/MR_d (as appear in the its routing table) and then forward the LBU message to its parent-MR, i.e. MR_d, which is also stores this HoA along with the senders address, i.e. the CoA of MR_{d-1}, in its routing table and so forth until the message reaches to the root-MR.

This HoA along with the sender should be stored by all MRs. For MR_{d-1} to the root-MR to finish building routing tables. After the root-MR stores HoA, it responds with a Local Binding Acknowledgment (LBA) message containing the CoA of the root-MR to the HA of MNN/MR_d with the CoA of the root-MR so that any packet destined to MNN intercepted by the HA of MNN can be encapsulated and send it directly to the root-MR for reading MNN.

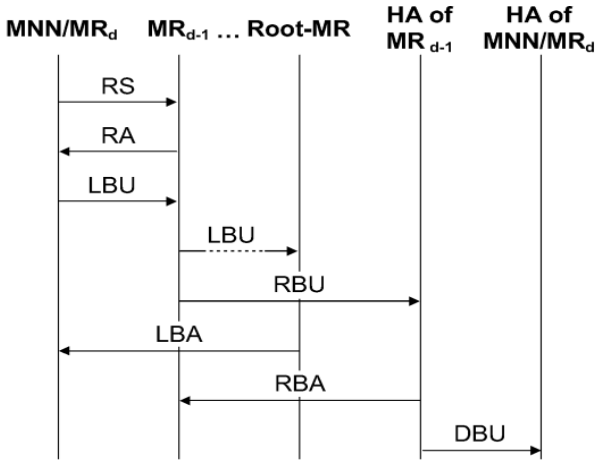

Fig. 4. Message flow for the node registration procedure

B. Packet Routing in RODBU

In this solution, different paths of incoming and outgoing packets were used. When CN needs to send packets to MN (MNN1 in Fig. 3), the HoA of MN is inserted in the field of routing header and the field of destination address. Using the binding cash of the HA of MN containing the information that MN is in the mobile network of MR. HA_{MN} encapsulate the original packet and send it to the MR1 When the packet incepted by the HA_{MN} and after receiving the packet by MR1, MR1 decapsulates the packet and checks the destination address of the packet. From its routing table, MR1 knows where MN is located under MR2. Thus, MR1 replaces the field of destination address of the packet. MR1 also decapsulates the packet and check the destination address by the CoA of MR2 and passes the packet to MR2 which also knows that the MN is located under MR3. MR2 then replaces the field of destination address by the CoA of MR3 and passes the packet to MR3 which will react similarly until the packet arrives at MN. Finally, MN finds its HoA from the routing header and the delivery of this packet is done. For the outgoing packets, the packet will be sent to the parent-MR of the MN.

C. Handover in RODBU

As shown in Fig. 5, mobile network handover in RODBU categorized into three types: intra-domain handover, inter-domain handover and root-MR handover. . The intra-domain handover occurs when mobile network moves within the same root-MR domain. The inter-domain handover occurs when a mobile network moves to a new foreign network with a different root-MR domain. The root-MR handover occurs when a mobile network moves to a new foreign network and the highest nesting level node among moving nodes (called Handover Leader Node (HLN)) becomes the root-MR in the foreign network. Note that the MNP and the CoA of the root-MR enable the HLN to differentiate these types of handover by checking the MNP of the sender and the CoA of the root-MR when a RA message is received at the new location. Once the MNP in the received RA message is found different from one saved by HLN, HLN then checks the field of the CoA of the root-MR in the RA message, if this field has the same value as the one saved by the HLN, its performs the intra-domain handover, if this field is empty. It then performs the root-MR handover; otherwise, it performs inter-domain handover. The handover mechanism RODBU informs the related HAs of the new CoA of the root-MR via wires link by using the subtree list table and DBU message to avoid the BU storm and signaling overheads.

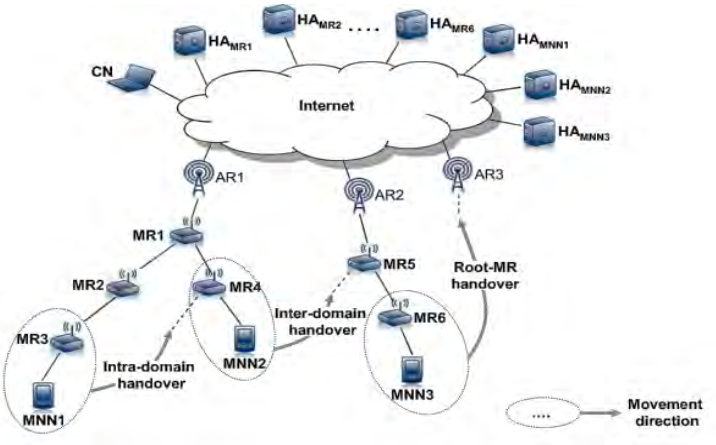

Fig. 5. Types of handover in nested mobile network

1) Intra-domain Handover in RODBU

Fig. 6 shows the procedure for the intra-domain handover, where MR_d is the HLN. Once MR_d receives an RA message from a new MR_{d-1}. It sends an LBU message containing its HoA, CoA and the HoA of the old parent-MR of the new MR_{d-1}. Since the moving network moves within the same root-MR domain, MR_d does not change its CoA. After the new MR_{d-1} receives the LBU message, it forwards the LBU message to its parent-MR and also sends an RBU message to its HA and the HBU message to the root-MR. As explained previously in the node registration procedure, the LBU message is forwarded by the new MR_{d-1} to its parent-MR until this message received by the root-MR and the RBU message is send to the HA of the new MR_{d-1} to record the HA of the new MR_d in its sub-tree list table following the node registration procedure. As for HBU message, it sends to the root-MR to perform the deregistration procedure to clean the moving nodes from the routing tables and the HA of the HLN from the sub-tree list table previously governing them. After the root-MR receives the HBU message, its first send Handover Binding Acknowledgement (HBA) message to the new MR_{d-1}, then it sends a Routing Table Deregistration (RTD) message to the old MR_{d-1} and Subtree List Deregistration (SLD) messages to all HA of the old $MR_{d-1.}$ All MRs between the root-MR to old MR_{d-1} then remove all moving nodes from their routing tables. The HA of the old MR_{d-1} then then removes the HA of MR_d from its sub-tree list table as well. Since itis not necessary for most of moving nodes to send BU message to their HAs. The BU storm can be avoided and fewer signaling overhead are required in RODBU.

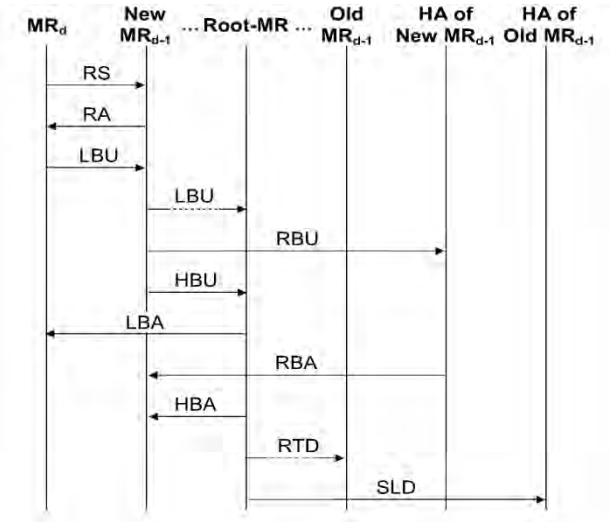

Fig. 6. Message follows for the intra-domain handover

2) *Inter-domain Handover in RODBU*

In Fig. 7 the procedure for the inter-domain handover is shown. Since MR_d and subtree MRs move to a new root-MR domain. MR_d has to create a new CoA using the new MNP in the RA message send by the new MR_{d-1} via sending an LBU message to its new parent-MR and finally to the new root-MR as the node registration procedure. As for the other moving nodes, it is not necessary to create a new CoA for them. Note that the HBU in the inter-domain handover procedure has an additional function to reduce the packet loss to be explained as follows. After the old root-MR receives HBU message, it replies with HBU message and sends a RTD SLD messages like intra-domain procedure, and forwards all packets destined to the moving network to the new root-MR. Therefore, the moving nodes can receive packets can receives the packets destined to them before the handover procedure is finished. In addition, this type of handover also uses the DBU message. After the HA of the new MR_{d-1} receives the DBU message from the MR_{d-1}, it records the HA of MR_d in its subtree list table and responds with a RBA message to the new MR_{d-1}; then it sends DBU message containing the CoA of the new root-MR to the HA of the MR_d like the node registration procedure. The HA of MR_d distributes the CoA of the new root-MR to all HAs of its subtree MRs by distribute the CoA of the new root-MR to all HAs of its subtree by forwarding DBU message.

3) Root-MR Handover in RODBU

The procedure of root-MR handover is shown in Fig. 8. In this type of handover, the HLN becomes the root-MR in the new network. Therefore, the root-MR has to create the new CoA using the new MNP in the RA message sent by the new access router AR and put the new CoA in the field of the CoA of the root-MR along with its MNP into the RA message to its HA, and an HBU message to the old AR or the old root-MR.

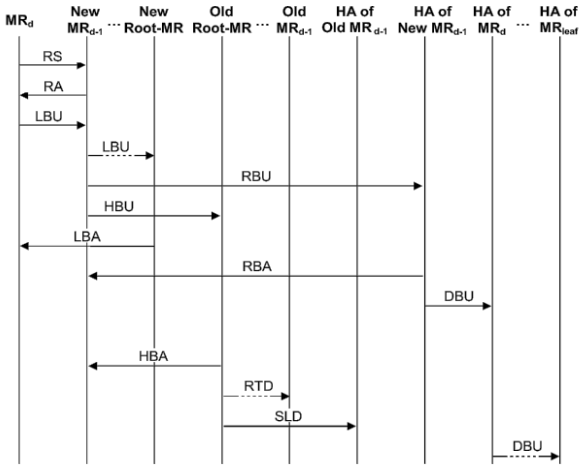

Fig. 7. Message flows for the inter-domain handover

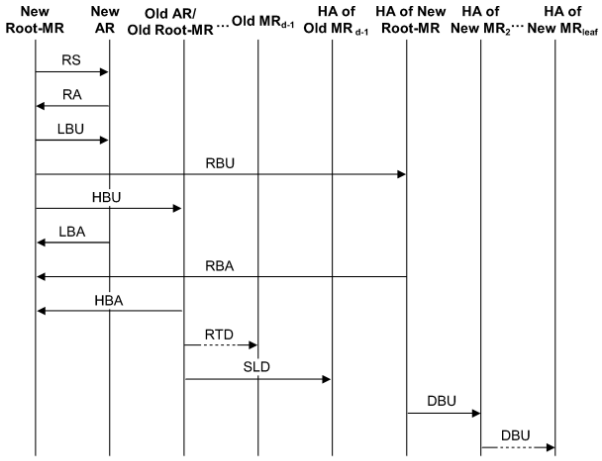

Fig. 8. Message flows for the root-MR handover

The difference between inter-domain handover and root-MR handover resides in the node to send an RBU message and an HBU message. For the inter-domain handover, this performs by the parent-MR of the HLN, while it performs by HLN itself in the root-MR handover. After receiving the HBU message and the SLD message, like in the intra-domain handover procedure, the HA of the root-MR needs to send a DBU message to all HAs of its subtree MRs recursively after it accepts the request of the RBU message [2].

VI. RRP AND NEMO SECURITY

In NEMO, security mechanisms are needed to ensure secure packet transmission between the CN and MNN. The BU provides authenticity and integrity to the packets. Incorrect BU can leads to malicious. To avoid these attacks, we have to employ RRP. In this scenario, CN can works as a proxy to the network. RRP is proposed to provide a way of sharing a common key between CN and MN for authenticity and BU as shown in Fig. 9, and to verify if the MN is still a live at its CoA claimed. MIPv6 assumes exist security association between MN and its HA. It means all messages are tunneled by IPSec in communication between MNN and HA, the procedure is depicted in Fig. 9.

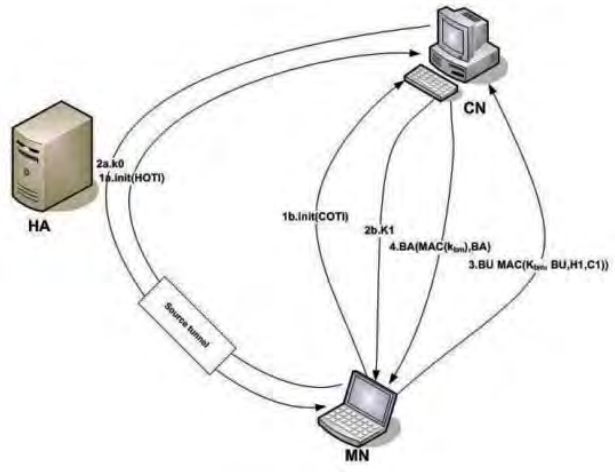

Fig. 9. Route routability procedure (RRP)

MN sends a Home Test Init (HoTI) message including a home init cookie (N0) (nonce0) to CN via HA. At the same time, MNN sends a Core of Test Init (CoTI) message including a care of test init cookie (N1) (another nonce), to CN the source address of HoTI and CoTI are HoA and CoA of MN respectively. Upon receiving HoTI and CoTI CN replies with home test HoT and care of test CoT messages respectively. To prepare HoTI message the CN prepare a nonce (nonceH1) indexed by H1 for use in generating the home Keygen token K0. K0 is calculated as:

$$K0 = FIRST\ (64, HMAC\_SHA1\ (KCN, (HoA|nonceH1|0))) \quad (1)$$

where '|' denotes string concentration, KCN is a secret value only kept in CN. HMAC_SHA1 denotes a key hashing MAC using hash function SHA1. And first (n,M) denote to first n bits of message M. similarly for CoT, CN select a nonceC1 indexed by C1, for use in generating the core of Keygen token K1. K1 is calculated as:

$$K1 = FIRST(64, HMAC\_SHA1(KCN, (HoA|nonceC1|1))) \quad (2)$$

Then the CN sends out the HoT message including three parameters N0, K0 and H1 destined to HoA. And send out CoT message including three parameters N1, K1 and C1 destined to CoA. The nonce indices carried in HoT remind CN of which nonce value is used in generating the K0 and K1. Beside 0 and 1 are used to distinguish home and care of cookies. The two tokens exchanges are useful to make sure the liveners of MNN on both HoA and CoA. The MNN obtains home key token K1 from HoT and CoT.

The exchanged tokens test whether packet destined to claim addresses are routed to MNN. It is assumed that if MNN can get these two massages correctly, then MNN is actually at the claimed IP address. When K0 and K1 are both received by MNN, MN creates binding key denotes by K_{bm} generated from SHA1(K0|K1). K_{bm} become the shared secret key between the MN and the CN. The binding update message contains H1,C1 and MAC

$$MAC = FIRST(96, HMAC\_SHA1(Kbm, (CoA|CN's\ address|BU))) \quad (3)$$

where binding update indicates the binding update message itself. While CN receives the binding update with message authentication code using K_{bm} as MAC key, it can rebuild K_{bm} dynamically and verify the validity with the help of home and care of nonce index H1 and C1. If it is legal, the CN sends back an acknowledgment with MAC [9].

VII. SIMULATION SETTINGS

In this section, we presents the settings the RODBU with security addition, we choose RRP because it is the best mechanism to secure the connectivity between the MN and its CN, here the procedure will be as that, after handover occur in RODBU and the DBU is done between HAs, RRP starts to authenticate the connectivity, and this generates addition messages in the network. Here, we need to calculate the number of messages sent in the handover and the authentication process via hope by hope manner, which is the sum of total massages generated in the wireless link with certain value of Packet Error Rate (PER) and the total massages generated over the wired link. The average number of messages generated one hope over the wireless link ω expressed as follows [2]:

$$\omega = 1 + \frac{q}{(1-q^N)(1-q)}[q^{N-1}\big((N-1)(q-1)-1\big)+1] \quad (4)$$

where q is retransmission probability and calculated as follow:

$$q = 1 - (1-p)^{(n_1+n_2)} \quad (5)$$

where p is the probability of packet being erroneous, n_1 number of packets in solicitation frame, n_2 number of packets in RA frame, and N is the maximum number of transmission.

In intra-domain handover RS, RA and SLD requires one hope transmission; LBU, LBA, RBA, RBA and all RRP messages required $(d-2)$ hopes; and RTD messages requires $(d_{old}-1)$ hops transmission over the wireless link. Over wired link RBU and SLD require γ hop and RBA and RRP messages requires 2γ hops for transmissions so that the total messages generated in intra domain handover can be calculated as follows:

$$M_{intra}^{RO} = (12d + d_{old} - 13)\omega + 16y \quad (6)$$

The signaling overhead in inter domain handover will be expressed as:

$$M_{inter}^{RO} = (12d + d_{old} - 9)\omega + \left(\sum_{i=0}^{d_{leaf}-d} k^i + 19\right)\gamma \quad (7)$$

where k^i is the number of MRs in each nesting level and $\sum_{i=0}^{d_{leaf}-d} k^i$ denotes the number of DBU messages sent in this type of handover. Noting that two more hops are required for the HBU message and two more are required for the HBA message as compared to the intra-domain handover in the first part of equation, in second part which belong to wired network HBU passes throw one hop transmission γ, 2γ for HBA and RRP messages and $\sum_{i=0}^{d_{leaf}-d} k^i\,\gamma$ for DBU messages.

For root-MR handover, the number of messages sent will be obtained as follows:

$$M_{root}^{RO} = (d_{old} + 15)\omega + (\sum_{i-1}^{d_{leaf}-1} k^i + 18)\gamma \quad (8)$$

Here the number of messages sent over the wireless link requires one hope transmission for RS, RA, LBU, LBA, RBU, RBA, RTD and RRP messages, and two hops of transmission of HBU and HBA and $d_{old}-2$ hops of transmission the SLD message. While the message sends over the ired link requires γ hops of transmission for the RBU, RBA, HBU and SLD messages and 2γ hops of transmission for HBA and RRP messages, and $\sum_{i-1}^{d_{leaf}-1} k^i\gamma$, for DBU message.

VIII. Simulation and Results

By using Matlab software for simulation under 0 – 10% PER and nesting level of two, we got the following results:

Intra-domain handover as shown in Fig. 10. The handover increases to 69% in the number of messages overhead when the RRP applied to the RODBU routing mechanism. While in inter-domain handover, there is a 48% increment in the number of messages overhead as shown in Fig. 11.

In root-MR handover, with one nesting level, the number of messages overhead increases with 43% as shown in Fig. 12.

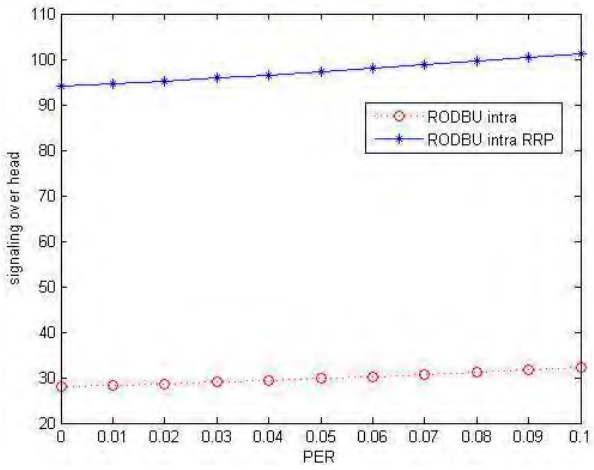

Fig. 10. Number of messages overhead in intra-domain RODBU handover

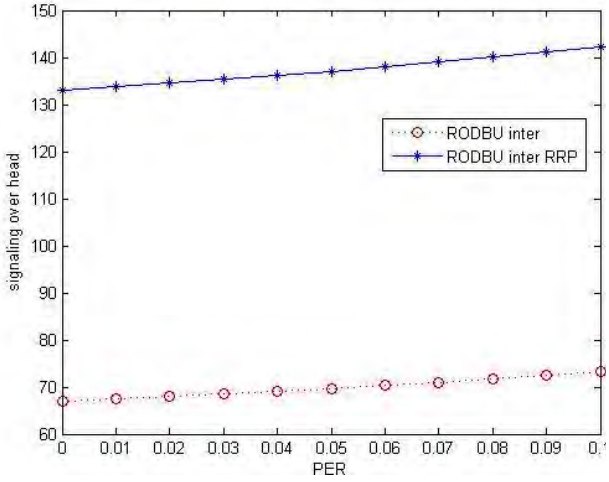

Fig. 11. Number of messages overhead in inter-domain RODBU handover

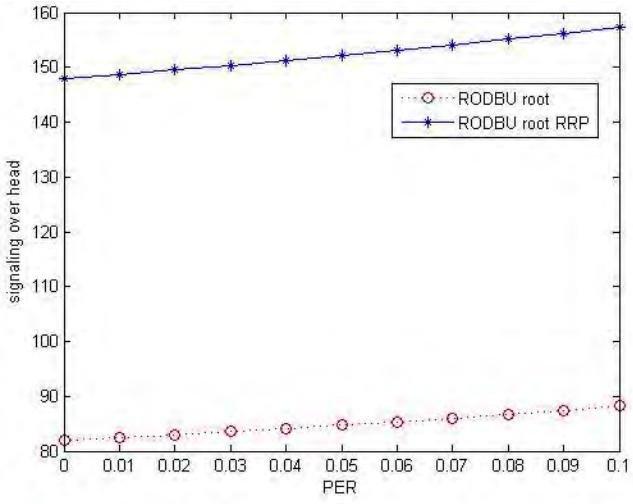

Fig. 12. number of messages overhead in root-MR in handover in RODBU

IX. Conclusion

In this paper, we study the effect of the security aspects to RODBU mechanism and see how the performance will effect by adding RRP to the RODBU routing mechanism.

When the RRP applied to the handover procedure, we observed that the number of message overhead increases, so this considers a signal of congestion in the network.

When applying the RRP to RODBU routing mechanism, we observed the following results, Intra-domain handover, the overhead increases to 69%. While in inter-domain handover, there is a 48% increment in the messages overhead. In root-MR handover, with one nesting level, the number of messages overhead increases with 43%.

We found that it is important to measure the effect during the planning phase of implementing NEMO network and to avoid this temporary congestion and also to protect the network from malicious attacks.

ACKNOWLEDGMENT

The authors gratefully acknowledge the support of this work by the Centre for Research and Instrumentation Management (CRIM), University Kebangsaan Malaysia (UKM), Malaysia. Grant numbers: UKM-GGPM-ICT-035-2011 and UKM-GUP-2012-089.

REFERENCES

[1] A. A. Mosa, A. H. Abdalla, and R. A. Saeed, "Evaluation of MANEMO route optimization schemes," *Journal of Network and Computer Applications*, vol. 35, pp. 1454–1472, 2012.
[2] G. Tsirtsis, H. Soliman, N. Montavont, G. Giaretta, and K. Kuladinithi, "Flow bindings in mobile IPv6 and network mobility (NEMO) basic support," *IETF RFC6089, January*, 2011.
[3] M. Dinakaran and P. Balasubramanie, "Avoiding Pin Ball Routing Problem in Network Mobility Hand-Off Management," *World Academy of Science, Engineering and Technology*, vol. 57, pp. 267-271, 2011.
[4] N. Bahaman, A. S. Prabuwono, R. Alsaqour, and M. Z. Masud, "Network Performance Evaluation of Tunneling Mechanism," *Journal of Applied Sciences*, vol. 12, pp. 459-465, 2012.
[5] M. Dinakaran and P. Balasubramanie, "A Routing Technique for Visiting Mobile Nodes in NEMO," *International Journal of Computer Applications*, vol. 27, pp. 9-13, 2011.
[6] M. Abdelhaq, S. Serhan, R. Alsaqour, and A. Satria, "Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol," *Australian Journal of Basic and Applied Sciences*, vol. 5, pp. 1137-1145, 2011.
[7] M. Abdelhaq, R. Hassan, and R. Alsaqour, "Using Dendritic Cell Algorithm to detect the Resource Consumption Attack over MANET," *Software Engineering and Computer Systems*, pp. 429-442, 2011.
[8] M. Uddin, R. Alsaqour, and M. Abdelhaq, "Intrusion Detection System to Detect DDoS Attack in Gnutella Hybrid P2P Network," *Indian Journal of Science and Technology*, vol. 6, pp. 71-83, 2013.
[9] R. Koodli and F. Zhao, "Mobile IPv6 Location Privacy Solutions," 2010.
[10] A. A. Mosa, A. H. Abdalla, and R. A. Saeed, "Evaluation of MANEMO route optimization schemes," *Journal of Network and Computer Applications*, vol. 35, pp. 1454-1472, 2012.
[11] M. Dinakaran and P. Balasubramanie, "Network Mobility (NEMO) Security: Threats And Solutions," *Journal of Theoretical and Applied Information Technology*, vol. 35, pp. 77-82, 2012.
[12] T. Aura and J. Arkko, "MIPv6 BU attacks and Defenses, draft-aura-mipv6-bu-attacks-01. txt," *IETF, February*, 2002.
[13] M. Roe, T. Aura, and G. O'Shea, "J. Arkko," Authentication of Mobile IPv6 Binding Updates and Acknowledgments," *IETF Draft*, 2002.
[14] O. Elkeelany, M. M. Matalgah, K. P. Sheikh, M. Thaker, G. Chaudhry, D. Medhi, and J. Qaddour, "Performance analysis of IPSec protocol: encryption and authentication," in *Communications, 2002. ICC 2002. IEEE International Conference on*, 2002, vol. 2, pp. 1164-1168.
[15] Y.-C. Chen and F.-C. Yang, "An efficient MIPv6 return routability scheme based on geometric computing," in *Proceedings of world academy of science, engineering and technology*, 2009, pp. 238-243.
[16] H.-W. Ferng and T. Laksmono, "Route optimization using the distributed binding update for nested mobile networks," *Wireless Communications and Mobile Computing*, pp. n/a-n/a, 2012.
[17] T. Laksmono, "Route optimization using the distributed binding update for nested mobile networks," Master's thesis, National Taiwan University of Science and Technology, 2009.