Scientific Research and Essays Vol. 7(21), pp. 1986-1996, 7 June, 2012
Available online at http://www.academicjournals.org/SRE
DOI: 10.5897/SRE10.1211
ISSN 1992-2248 © 2012 Academic Journals

Full Length Research Paper

Security verification of the return routability protocol by Murphi

Wafaa A. H. Ali Alsalihy* and Mohammed I. Younis

[1]Network Research Group, School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia.
[2]Department of Computer Engineering, College of Engineering, University of Baghdad, Baghdad, Iraq.

Accepted May 21, 2012

The return routability protocol (RRP) is commonly used in route optimization to secure and authenticate mobile IPv6 signals between the mobile node and its correspondent node. In this paper, the correctness and the security of RRP were verified using a Murphi model checker. The results show that RRP has no failure and is correct. However, it is not secure, because an intruder may impersonate a mobile node. Therefore, the design of RRP needs to be revised to overcome these obstacles.

Key words: Return routability protocol, Murphi model checker, binding update message, route optimization.

INTRODUCTION

Internet Protocol version 6 (IPv6) is the next-generation internet protocol used to overcome the limitations of Internet Protocol version 4 (IPv4) (Blanchet, 2002). The IPv6 protocol, sometimes called IPNG, solves the problem of the limited number of available IP addresses, which has become a significant impediment to the rapid growth of the internet. However, this new protocol must be developed further to correct a number of weaknesses inherent in the current internet protocol, such as a failure to provide safety and support for mobile devices that need automatic configuration of network devices and improved quality of service.

Mobility-oriented research currently focuses on mobile networks. These networks are called mobile IPs. They were categorized by the Internet Engineering Task Force (IETF) in terms of both homogenous and heterogeneous networks (Aura and Roe, 2006). Mobile IPv6 (MIPV6) is the mobile IP support protocol for IPv6. Its specifications were standardized by the IETF to include several security mechanisms, such as mobility protocols (Radhakrishnan et al., 2008). The MIPv6 protocol is a network layer of IPv6 that allows one node to communicate directly with another node. The mobile network allows its user to remain connected while it changes its location to a foreign network (Aura and Roe, 2006).

The basic idea in MIPv6 is to allow a home agent (HA) to work as a stationary proxy for a mobile node (MN) (Aura and Roe, 2006; Blanchet, 2002). Whenever the MN is away from its home network, the HA intercepts packets destined to the node and forwards the packets by tunneling them to the node's current address, the care-of address (CoA). The transport layer (for example, TCP and UDP) uses the home address (HoA) as a stationary identifier for the MN. The basic solution requires tunneling through the HA, thereby leading to longer paths and degraded performance. This tunneling is sometimes called triangular routing (Aura and Roe, 2006).

If the node supports mobile IPv6, any IPv6 node can access the host by defining its HoA, regardless of the host's location. The mobile IPv6 protocol allows an MN to move seamlessly from one network to another. If the CoA is changed when the MN moves, the HoA remains the same (Chen and Yang, 2009).

To alleviate performance penalty, MIPv6 includes a mode of operation that allows the MN and its peer, a correspondent node (CN), to exchange packets directly,

*Corresponding author. E-mail: wafaa@cs.usm.my.

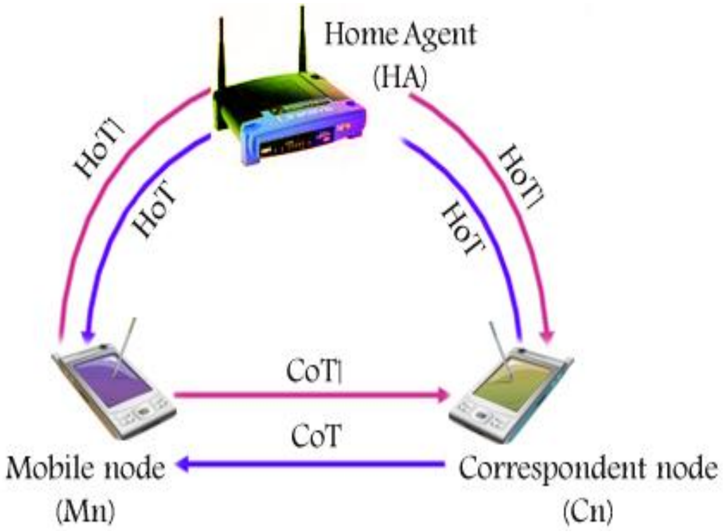


Figure 1. The RRP mechanism.

bypassing the HA completely after the initial setup phase. This mode of operation is called route optimization (RO) (Harini and Ramanaiah, 2008; Jeong and Shin, 2008). When route optimization is used, the MN sends its current CoA to the CN using binding update (BU) messages (Ahmed et al., 2007). The CN stores the binding between the HoA and CoA into its binding cache. In MIPv6, BUs to CNs are supposed to be protected using a binding management key (K_{bm}). K_{bm} is established using data exchanged during the return routability protocol (RRP) (Kavitha et al., 2009). This study aims to verify whether possible attacks exist on the RRP in the current MIPv6 specification and whether RRP has achieved its design purpose or not.

The paper is organized as follows: a background on the RRP; methodology for simulating the RRP and the possibility of impersonation by the intruder; the security evaluation of the RRP; and finally, conclusion and suggestions for future research.

THE RRP

RRP is a mechanism for securing the BU message (Ahmed et al., 2007; Aura and Roe, 2006; Blanchet, 2002; Chen and Yang, 2009; Harini and Ramanaiah, 2008; Jeong and Shin, 2008; Kavitha et al., 2009; Radhakrishnan et al., 2008). This mechanism requires two cookies: home test initiation (HoTI) message and care-of test initiation (CoTI) message. The RRP consists of four messages: HoTI, CoTI, home test (HoT) message, and care-of test (CoT) message. One of the main goal of the normal RRP is to verify the BU message between MN and CN, as illustrated in Figure 1.

RRP enables the CN to obtain some reasonable assurance that the MN is in fact addressable at its claimed CoA as well as at its HoA. With this assurance, the CN can accept BUs from the MN, which would then instruct the CN to direct MN's data traffic to its claimed CoA. This procedure is done by testing whether the packets addressed to the two claimed addresses are routed to the MN. The MN can pass the test only if it can prove that it received certain data (keygen tokens), which the CN sends to those addresses, as shown in Relation 1.

Care-of keygen token = First (64, HMAC_SHA1 (Kcn, (care-of address | nonce | 1))) (1)

HoTI and CoTI messages are sent simultaneously, whereas HoT and CoT messages are returned simultaneously. When the MN has received both HoT and CoT messages, RRP is complete. The MN will then have the data it needs to send a BU to the CN (Figure 2). The MN hashes the tokens together to form a 20 binding key Kbm, as shown in Relation 2.

K_{bm} = SHA1 (home keygen token | care-of keygen token) (2)

This key is used to protect the first and the subsequent BUs as long as it remains valid.

The Murphi model checker is adopted to verify the security of RRP, which will be explored subsequently.

METHODOLOGY

The Murphi model checker has been used to analyze and verify security protocols as well as the correctness of certain software in

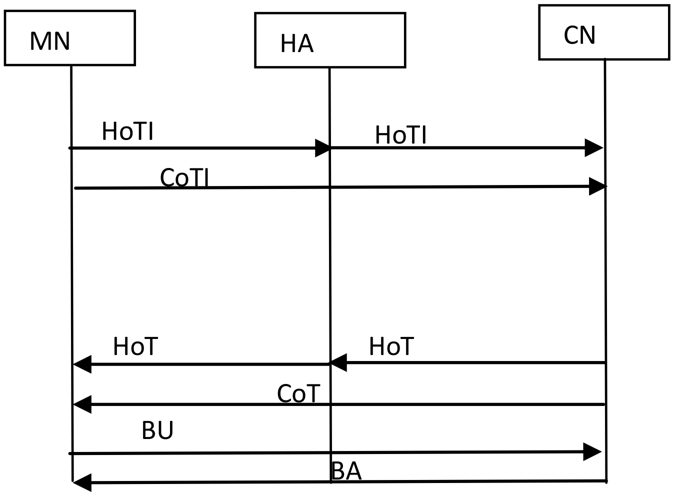


Figure 2. Message exchange in the RRP.

the early development cycle and in each subsequent development phase (Murphi, 2012; Shmatikov and Mitchell, 2002). The Murphi model checker has the following advantages:

1) It provides a better view of the protocol by analyzing its weaknesses and strengths.
2) It is systematic and provides an exhaustive solution to verifying the intended protocol.
3) It is used during both the development and implementation cycles of the protocol.
4) It provides a thorough insight into the specifications and the properties that the protocol is trying to satisfy.

Here, explains the methodology of the implementation of RRP using Murphi. The RRP is analyzed using the following four steps.

Step 1 (Formulation of RRP): This procedure generally involves simplifying the protocol by identifying the key steps and primitives. However, the Murphi formulation of a protocol is more detailed than the high-level descriptions often found in the literature, because one has to decide exactly which messages will each participant accept in the protocol. Given that Murphi communication is based on shared variables, an explicit message format must be defined as a Murphi type.

Step 2 (Verification of the correctness of RRP after formulating and modeling the protocol in Murphi): The protocol has to be run and verified to check for any error or failure.

Step 3 (Addition of an intruder model after verifying the correctness of the protocol): The intruder model is added as follows:

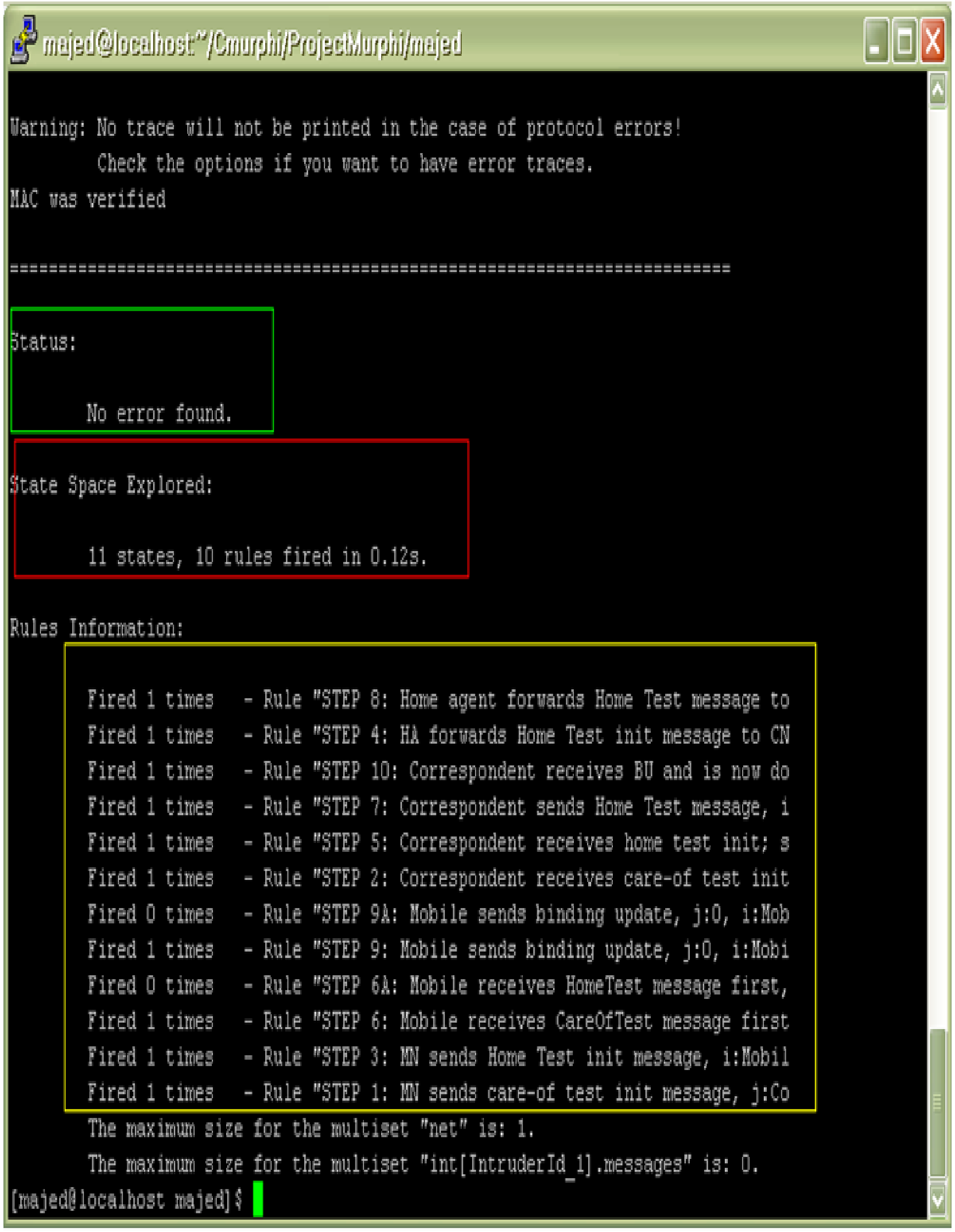
1) The intruder can masquerade as an honest participant in the system, capable of initiating communication with a truly honest participant. This capability will allow the intruder to masquerade as any valid MN or HA.
2) Intercept every message, remember all or parts of each message, and decrypt cipher-text when it has the key. This ability will allow the intruder to mount all types of man-in-the-middle (MITM) attack.
3) Intercept every message and send it again. This ability will allow the intruder to mount the replay attack.
4) Generate new messages using any combination of initial knowledge about the system and parts of overheard messages. This ability will allow the intruder to mount a spoof address attack (the MN's HoA and CoA) and subsequently send new messages to the same addresses.

Step 4 (State the security verification conditions (invariant) to identify the conditions and properties of the protocol verification environment): The conditions are mainly intruder-specific. A typical criterion includes the fact that no secret information can be learned by the intruder that allows it to construct the key K_{bm}.

Briefly, RRP could be simulated as follows:

i. First, all three nodes (that is, MN, HA, and CN) must be defined.
ii. Second, the protocol must be simulated in 10 steps.
a. Step 1, MN sends HoTI message to HA.
b. Step 2, HA receives HoTI message from MN.
c. Step 3, MN sends CoTI message directly to CN.
d. Step 4, HA forwards HoTI message to CN.
e. Step 5, CN receives HoTI message from HA.
f. Step 6, CN receives CoTI message from MN and then CN sends CoT to MN.
g. Step 6A, MN receives HoT message before CoT message.
h. Step 7, CN sends HoT message to HA.
i. Step 8, HA forwards HoT message to MN.
j. Step 9, MN sends BU message when it receives HoT before CoT message.
k. Step 9A, MN sends BU message when it receives CoT before HoT message.
l. Step 10, CN receives BU message from MN, then sends the binding acknowledgement (BA) immediately to MN. After this step, the protocol is complete.
iii. The protocol should be run to check that every step works without the addition of an intruder.
iv. An intruder must be added between MN and CN (that is, the MITM) to test the protocol.

The Murphi model of the protocol consists of four finite state machines corresponding to MNs, HAs, CN, and intruders. The number of MNs, HAs, CNs, and intruders is scalable and defined by



```
Warning: No trace will not be printed in the case of protocol errors!
         Check the options if you want to have error traces.
MAC was verified

==========================================================================

Status:

        No error found.

State Space Explored:

        11 states, 10 rules fired in 0.12s.

Rules Information:

        Fired 1 times   - Rule "STEP 8: Home agent forwards Home Test message to
        Fired 1 times   - Rule "STEP 4: HA forwards Home Test init message to CN
        Fired 1 times   - Rule "STEP 10: Correspondent receives BU and is now do
        Fired 1 times   - Rule "STEP 7: Correspondent sends Home Test message, i
        Fired 1 times   - Rule "STEP 5: Correspondent receives home test init; s
        Fired 1 times   - Rule "STEP 2: Correspondent receives care-of test init
        Fired 0 times   - Rule "STEP 9A: Mobile sends binding update, j:0, i:Mob
        Fired 1 times   - Rule "STEP 9: Mobile sends binding update, j:0, i:Mobi
        Fired 0 times   - Rule "STEP 6A: Mobile receives HomeTest message first,
        Fired 1 times   - Rule "STEP 6: Mobile receives CareOfTest message first
        Fired 1 times   - Rule "STEP 3: MN sends Home Test init message, i:Mobil
        Fired 1 times   - Rule "STEP 1: MN sends care-of test init message, j:Co
        The maximum size for the multiset "net" is: 1.
        The maximum size for the multiset "int[IntruderId_1].messages" is: 0.
[majed@localhost majed]$
```

Figure 3. RRP testing without intruder.

constants. Each MN can participate in a number of parallel sessions. This number can also be configured by changing the value of the constant.

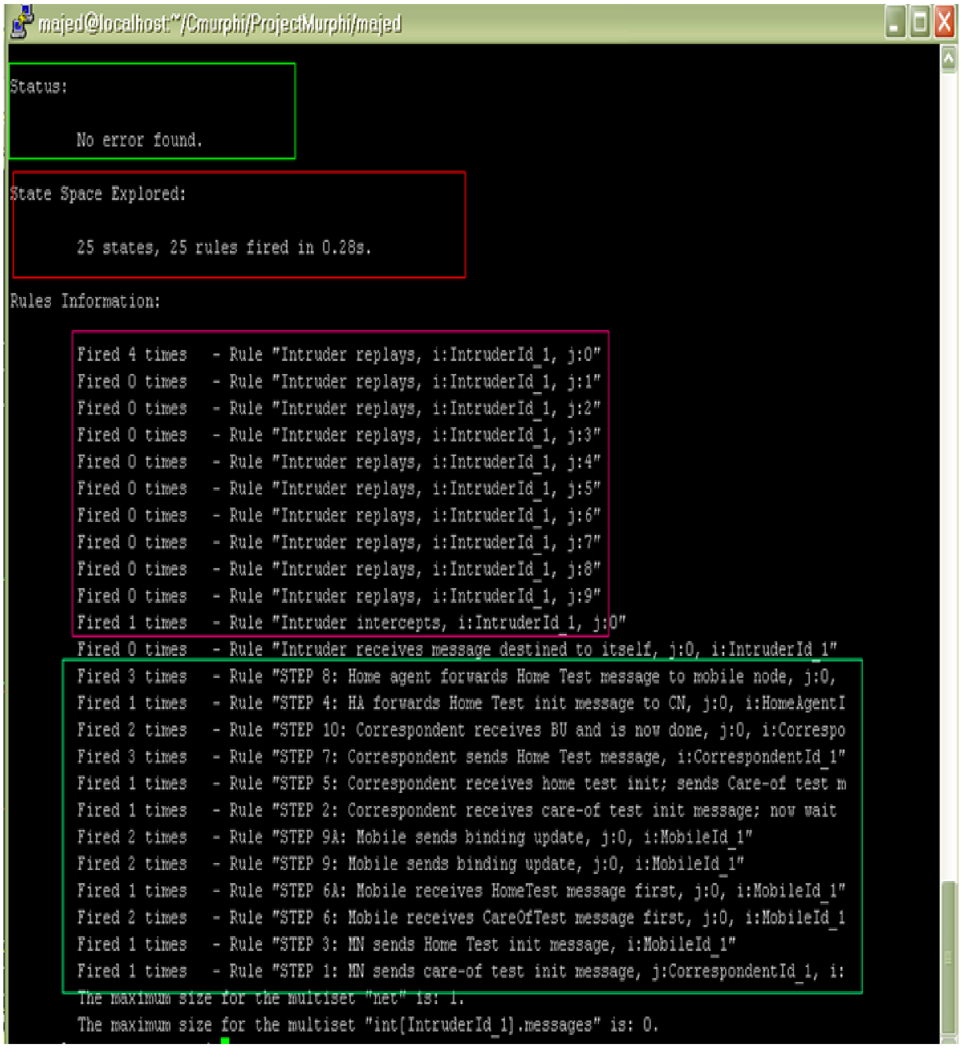
The following security verification conditions were modeled in the Murphi implementation: the cookies exchanged between the MN and its correspondent are not in the intruder's database; the session of the protocol is complete after the MN constructs the key K_{bm}; and the intruder does not construct the key K_{bm}.

The evaluation of the RRP consists of the following four parts: Part 1 (The protocol was designed and tested without an intruder); Part 2 (The intruder was placed between the MN and the CN in different paths); Part 3 (The intruder intercepted and modified the packet successfully); and Part 4 (The protocol was tested using the MN as an intruder).

RESULTS

RRP without intruder

Figure 3 depicts the simulation results obtained when using the RRP without an intruder. In this test, the packets are securely transferred through the network between the



```
Status:

        No error found.

State Space Explored:

        25 states, 25 rules fired in 0.28s.

Rules Information:

        Fired 4 times   - Rule "Intruder replays, i:IntruderId_1, j:0"
        Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:1"
        Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:2"
        Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:3"
        Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:4"
        Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:5"
        Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:6"
        Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:7"
        Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:8"
        Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:9"
        Fired 1 times   - Rule "Intruder intercepts, i:IntruderId_1, j:0"
        Fired 0 times   - Rule "Intruder receives message destined to itself, j:0, i:IntruderId_1"
        Fired 3 times   - Rule "STEP 8: Home agent forwards Home Test message to mobile node, j:0,
        Fired 1 times   - Rule "STEP 4: HA forwards Home Test init message to CN, j:0, i:HomeAgentI
        Fired 2 times   - Rule "STEP 10: Correspondent receives BU and is now done, j:0, i:Correspo
        Fired 3 times   - Rule "STEP 7: Correspondent sends Home Test message, i:CorrespondentId_1"
        Fired 1 times   - Rule "STEP 5: Correspondent receives home test init; sends Care-of test m
        Fired 1 times   - Rule "STEP 2: Correspondent receives care-of test init message; now wait
        Fired 2 times   - Rule "STEP 9A: Mobile sends binding update, j:0, i:MobileId_1"
        Fired 2 times   - Rule "STEP 9: Mobile sends binding update, j:0, i:MobileId_1"
        Fired 1 times   - Rule "STEP 6A: Mobile receives HomeTest message first, j:0, i:MobileId_1"
        Fired 2 times   - Rule "STEP 6: Mobile receives CareOfTest message first, j:0, i:MobileId_1
        Fired 1 times   - Rule "STEP 3: MN sends Home Test init message, i:MobileId_1"
        Fired 1 times   - Rule "STEP 1: MN sends care-of test init message, j:CorrespondentId_1, i:
        The maximum size for the multiset "net" is: 1.
        The maximum size for the multiset "int[IntruderId_1].messages" is: 0.
```

Figure 4. RRP testing with a passive intruder.

MN and CN, because of the absence of an intruder. This test is used with three components: MN, HA, and CN. No authentication problems were encountered between the MN and CN.

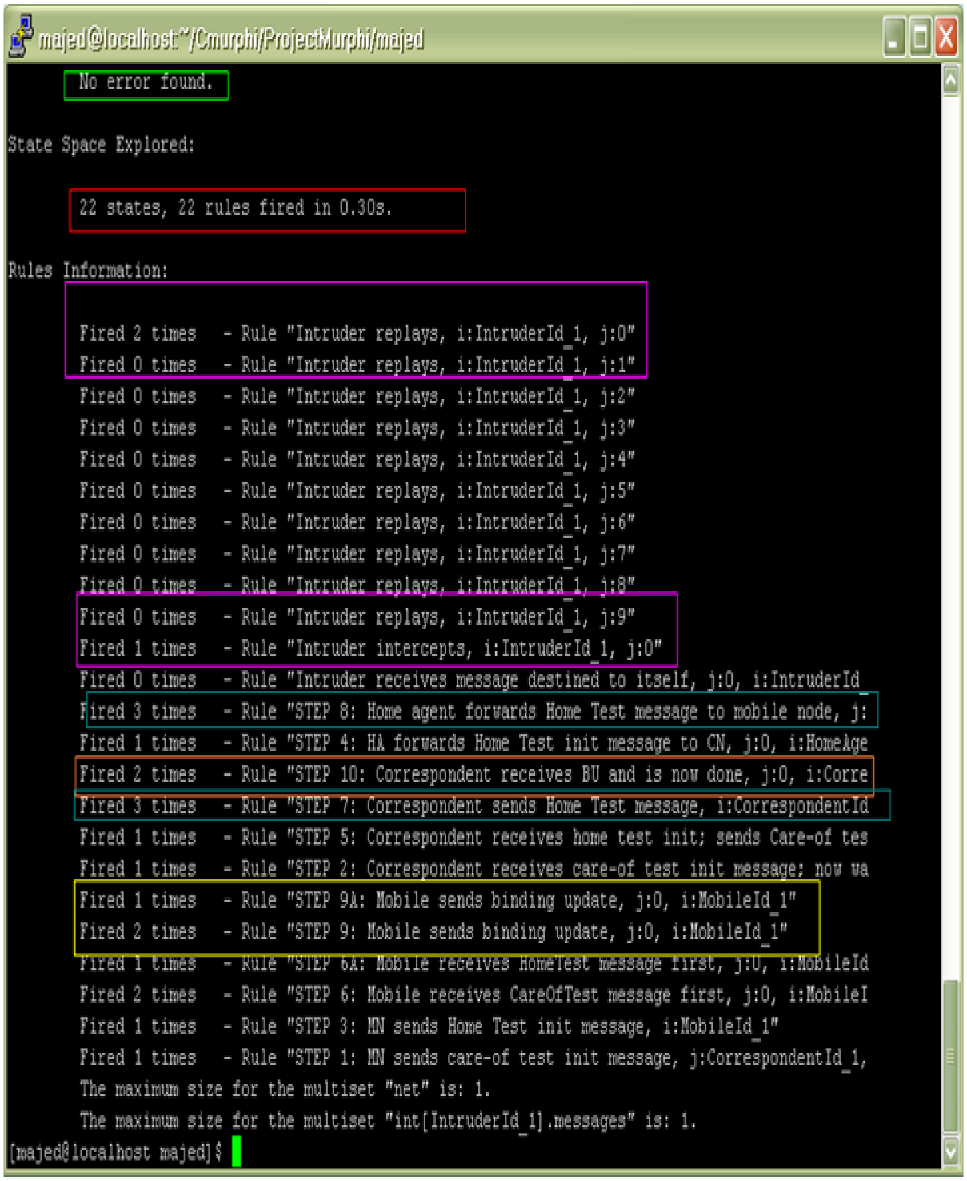
RRP with a passive intruder

This segment is similar to the previous one, except that it includes a passive intruder. In this case, the intruder intercepted and replayed the packet without making any modifications; it only listened.

Figure 4 depicts the simulation results obtained when the RRP is used with a passive intruder. In this case, the intruder intercepted messages that are sent from the MN to the CN and then replayed them without making any modifications. In the scenario, the CN received and compared the HoTI and CoTI messages. Subsequently, it generated two secret keys (Kcn), wherein one was sent with the HoT message and the other with the CoT message. Thereafter, the CN sent the HoT and CoT messages to the MN via different paths. In this result, the MN received all the sent messages without any changes from the intruder. The security and authentication strength between the MN and CN were fair because the intruder did not modify any messages and was simply aware of them. However, the intruder can intercept packets in the RRP. In addition, the sender did not know whether the packets were modified or not.

RRP with an active intruder

Figure 5 depicts the simulation results for the RRP with an



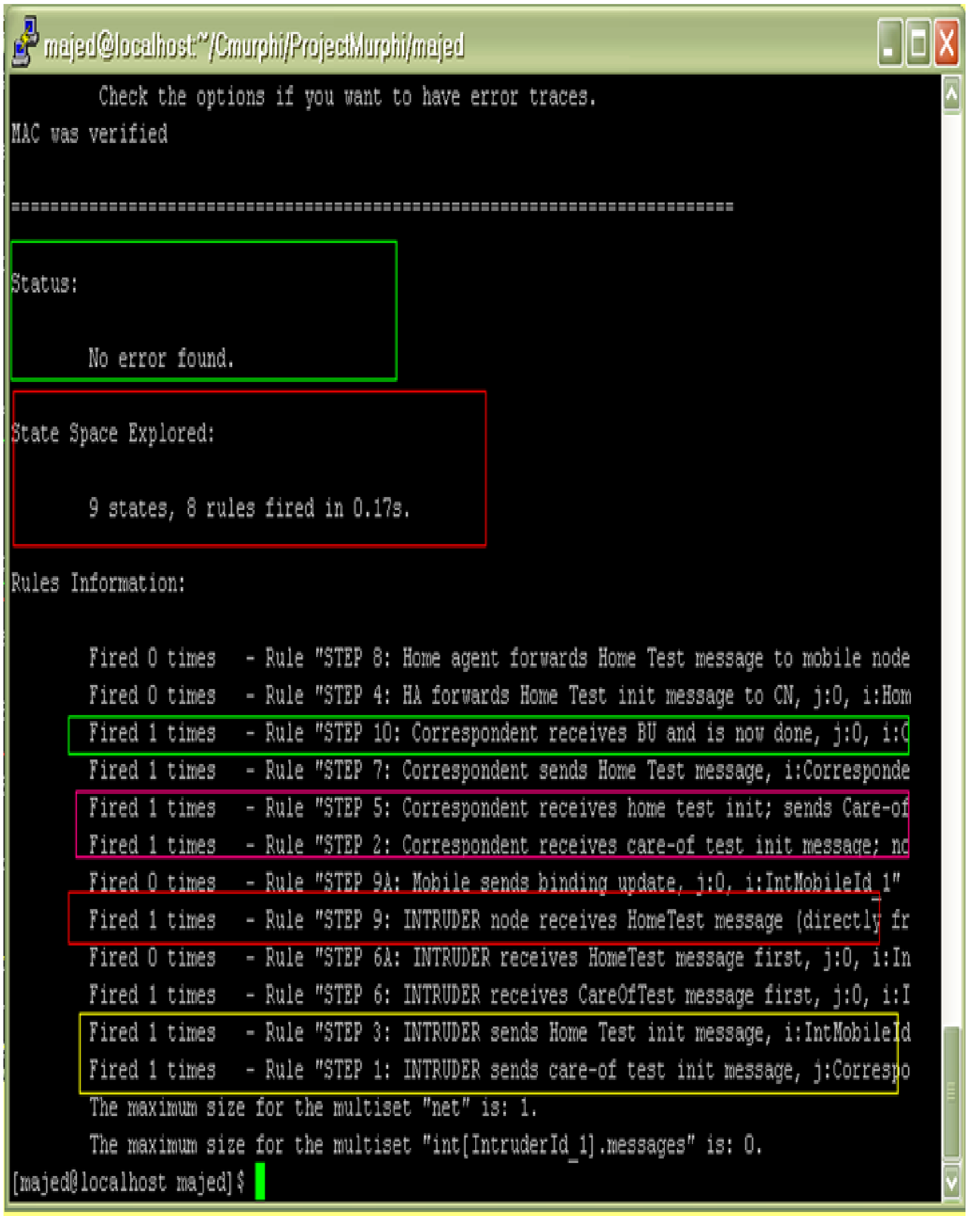
```
      No error found.

State Space Explored:

      22 states, 22 rules fired in 0.30s.

Rules Information:


      Fired 2 times   - Rule "Intruder replays, i:IntruderId_1, j:0"
      Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:1"
      Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:2"
      Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:3"
      Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:4"
      Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:5"
      Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:6"
      Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:7"
      Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:8"
      Fired 0 times   - Rule "Intruder replays, i:IntruderId_1, j:9"
      Fired 1 times   - Rule "Intruder intercepts, i:IntruderId_1, j:0"
      Fired 0 times   - Rule "Intruder receives message destined to itself, j:0, i:IntruderId_
      Fired 3 times   - Rule "STEP 8: Home agent forwards Home Test message to mobile node, j:
      Fired 1 times   - Rule "STEP 4: HA forwards Home Test init message to CN, j:0, i:HomeAge
      Fired 2 times   - Rule "STEP 10: Correspondent receives BU and is now done, j:0, i:Corre
      Fired 3 times   - Rule "STEP 7: Correspondent sends Home Test message, i:CorrespondentId
      Fired 1 times   - Rule "STEP 5: Correspondent receives home test init; sends Care-of tes
      Fired 1 times   - Rule "STEP 2: Correspondent receives care-of test init message; now wa
      Fired 1 times   - Rule "STEP 9A: Mobile sends binding update, j:0, i:MobileId_1"
      Fired 2 times   - Rule "STEP 9: Mobile sends binding update, j:0, i:MobileId_1"
      Fired 1 times   - Rule "STEP 6A: Mobile receives HomeTest message first, j:0, i:MobileId
      Fired 2 times   - Rule "STEP 6: Mobile receives CareOfTest message first, j:0, i:MobileI
      Fired 1 times   - Rule "STEP 3: MN sends Home Test init message, i:MobileId_1"
      Fired 1 times   - Rule "STEP 1: MN sends care-of test init message, j:CorrespondentId_1,
      The maximum size for the multiset "net" is: 1.
      The maximum size for the multiset "int[IntruderId_1].messages" is: 1.
[majed@localhost majed]$ 
```

Figure 5. RRP testing with an active intruder.

active intruder. These results are different from those depicted in Figure 3, because the intruder intercepted the message, made modifications, and then sent it to the CN. In this result, the intruder intercepted the CoT message and made modifications, which were subsequently sent from the CN to the MN. In addition, the CN received two BU messages, one from the correct MN and the other from the intruder. The security and authentication strength in this case were weak, because the intruder sent a false BU message to the CN. In addition, the intruder intercepted the CoT message as well as modified and created false CoA and HoA messages to establish the BU message. This message was subsequently sent to the CN, which simply received it.

RRP with an intruder acting as an MN

Here, the intruder acted as the MN to generate both HoTI and CoTI messages and send them to the CN. Figure 6 depicts the simulation results for cases when the intruder generated false HoTI and CoTI messages, which were sent to the CN. In the normal RR protocol, the trust between the MN and CN is weak. Therefore, the CN did not know whether the two messages came from the correct MN or the intruder. In any case, the CN received



```
        Check the options if you want to have error traces.
MAC was verified

==========================================================================

Status:

        No error found.

State Space Explored:

        9 states, 8 rules fired in 0.17s.

Rules Information:

        Fired 0 times   - Rule "STEP 8: Home agent forwards Home Test message to mobile node
        Fired 0 times   - Rule "STEP 4: HA forwards Home Test init message to CN, j:0, i:Hom
        Fired 1 times   - Rule "STEP 10: Correspondent receives BU and is now done, j:0, i:C
        Fired 1 times   - Rule "STEP 7: Correspondent sends Home Test message, i:Corresponde
        Fired 1 times   - Rule "STEP 5: Correspondent receives home test init; sends Care-of
        Fired 1 times   - Rule "STEP 2: Correspondent receives care-of test init message; nc
        Fired 0 times   - Rule "STEP 9A: Mobile sends binding update, j:0, i:IntMobileId_1"
        Fired 1 times   - Rule "STEP 9: INTRUDER node receives HomeTest message (directly fr
        Fired 0 times   - Rule "STEP 6A: INTRUDER receives HomeTest message first, j:0, i:In
        Fired 1 times   - Rule "STEP 6: INTRUDER receives CareOfTest message first, j:0, i:I
        Fired 1 times   - Rule "STEP 3: INTRUDER sends Home Test init message, i:IntMobileId
        Fired 1 times   - Rule "STEP 1: INTRUDER sends care-of test init message, j:Correspo
        The maximum size for the multiset "net" is: 1.
        The maximum size for the multiset "int[IntruderId_1].messages" is: 0.
[majed@localhost majed]$
```

Figure 6. RRP testing with the MN acting as an intruder.

the two messages and created a secret key for them. This key was sent to the intruder in steps 6 and 9A. The security and authentication strength were weak, because the intruder easily sent a false BU message for the CN to receive on the basis that it was from the MN.

DISCUSSION

RRP has some security threats, such as the MITM. The intruder can compromise the RRP from the following five positions:

1. In the RRP design, the intruder is in the first position between the HA and CN, because of the absence of security protection at this location (Figure 7). The intruder can intercept the HoTI message sent from the HA to the CN, and it can change the message traffic or modify the data, because the HoTI message is not encrypted. This situation will succeed only if the intruder generates a false CoTI message and sends it to the CN, because the intruder is unable to create a secret key before receiving two messages from the MNs. If this case is achieved, then the intruder can easily create a false k_{bm} that will be used to create the BU message after it is sent to the CN.

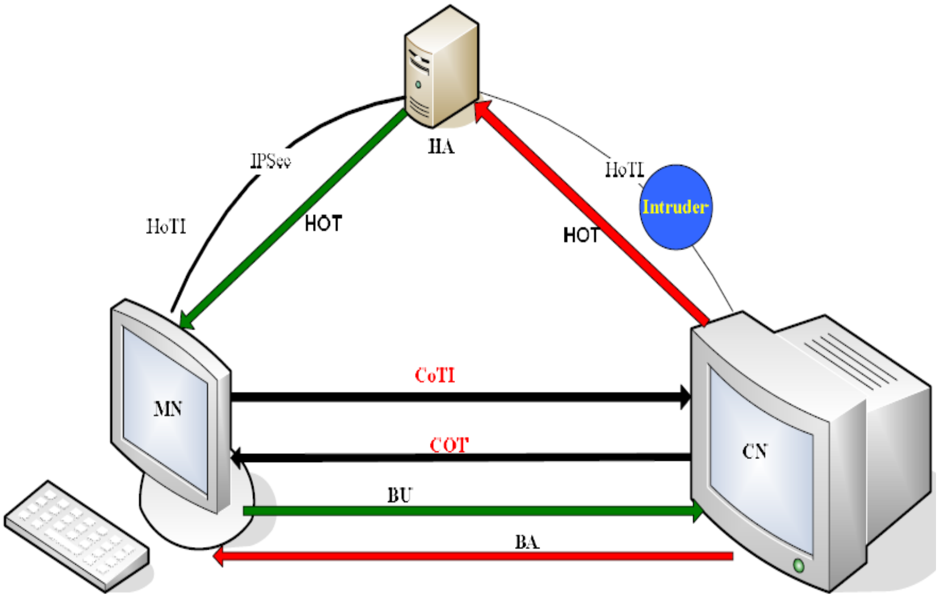


Figure 7. Intruder between the HA and CN in the RRP.

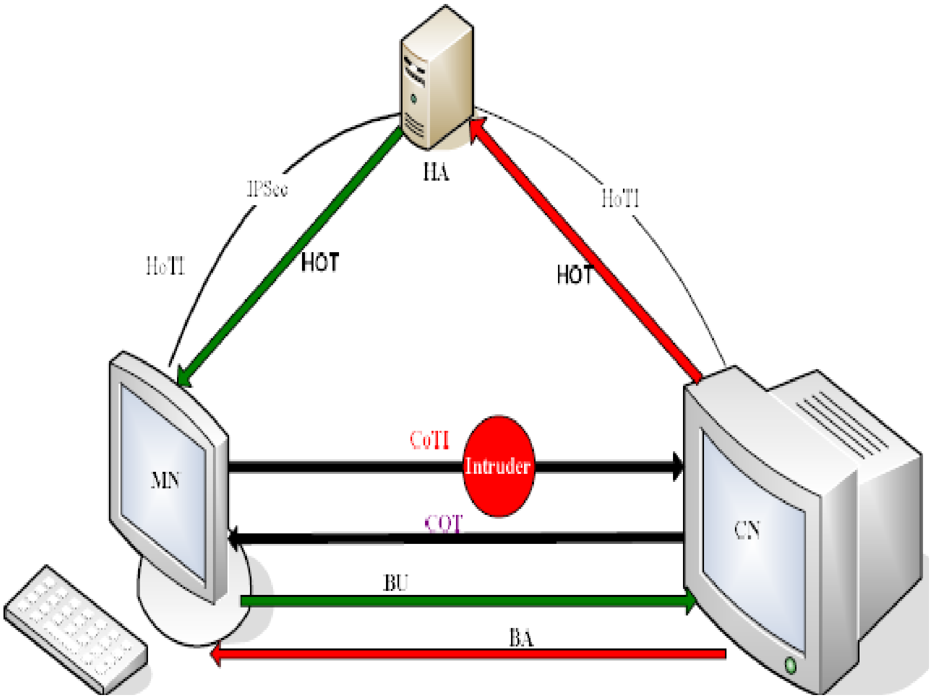


Figure 8. Intruder intercepting the CoTI.

2. The second MITM attack is between the MN and the CN. The message between the MN and CN is not encrypted, allowing the intruder to modify and send the message to the CN easily. The intruder managed to access the CN when it generated a false HoTI message to obtain the secret key (K_{cn}). Subsequently, the intruder generates the secret key for the BU to enable the false BU to communicate with the CN (Figure 8).

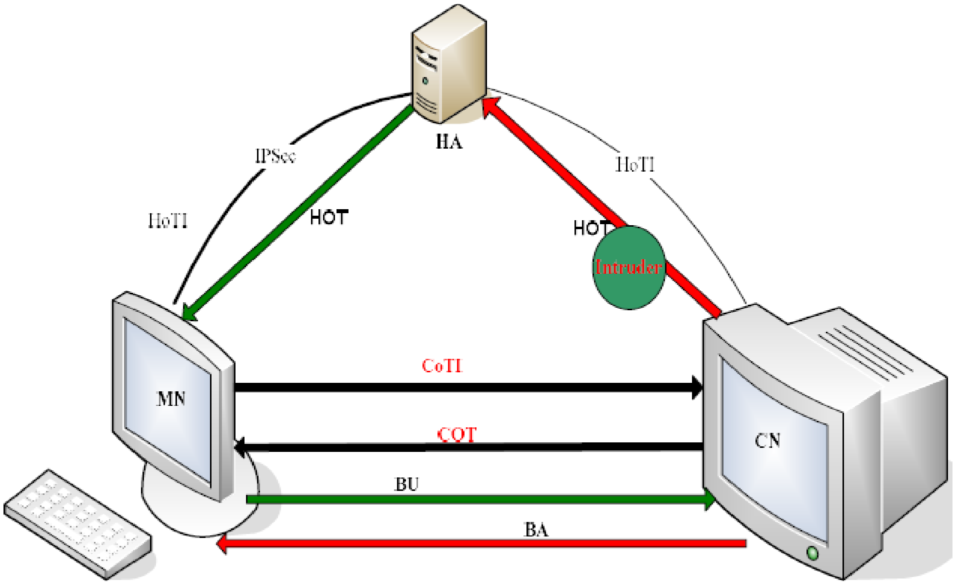


Figure 9. Intruder intercepts the HoT message.

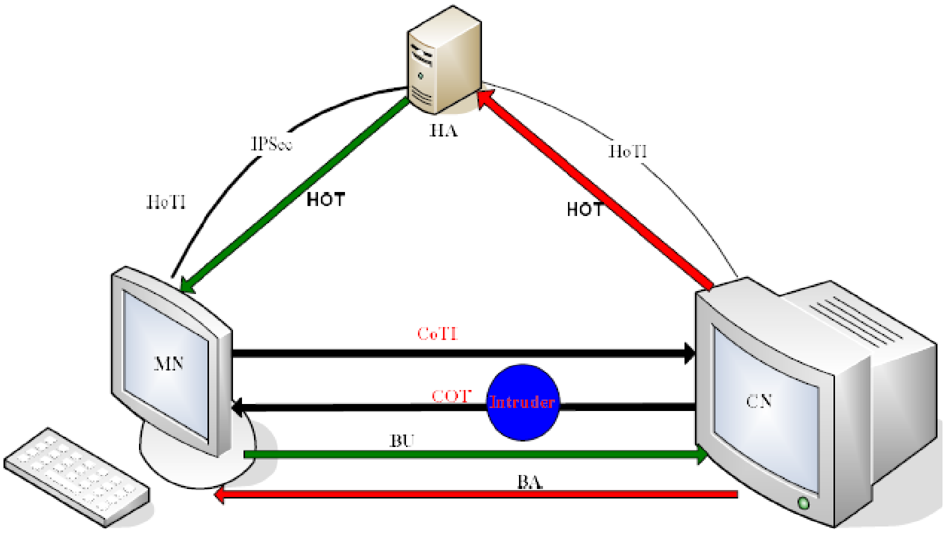


Figure 10. Intruder intercepts the CoT message.

3. The third MITM attack is between the CN and the HA. The intruder intercepts the HoT message and changes the value. Subsequently, the message is re-sent to the HA and forwarded to the MN via the IPSec tunnel. The intruder cannot benefit from this case (that is, obtain the BU message), because the MN sends the BU directly to the CN without using the HA. However, the intruder can create an amplification attack, as shown in Figure 9.

4. The fourth MITM attack is between the CN and the MN. In this case, the intruder can intercept the CoT message and then create a false K_{bm} to generate a false BU message. Subsequently, the intruder sends the CoT message to the MN before obtaining the BU message from the MN. When the MN receives the HoT and CoT, it compares the messages and creates a secret key to generate the BU. The MN sends the BU message to the source that sent the CoT message, which in turn modifies the message sent to the CN. The CN accepts this message because it is waiting for the BU message from the MN due to the weak trust between the MN-CN and CN-MN communication links (Figure 10).

5. The fifth position for the intruder in the RRP is between

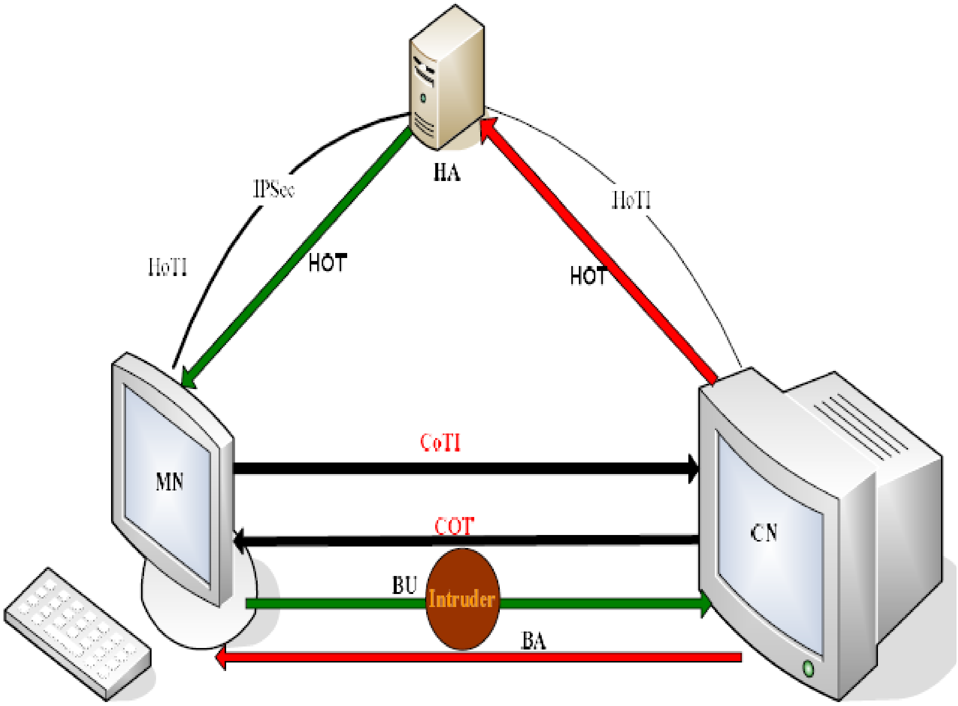


Figure 11. Intruder sends the BU message.

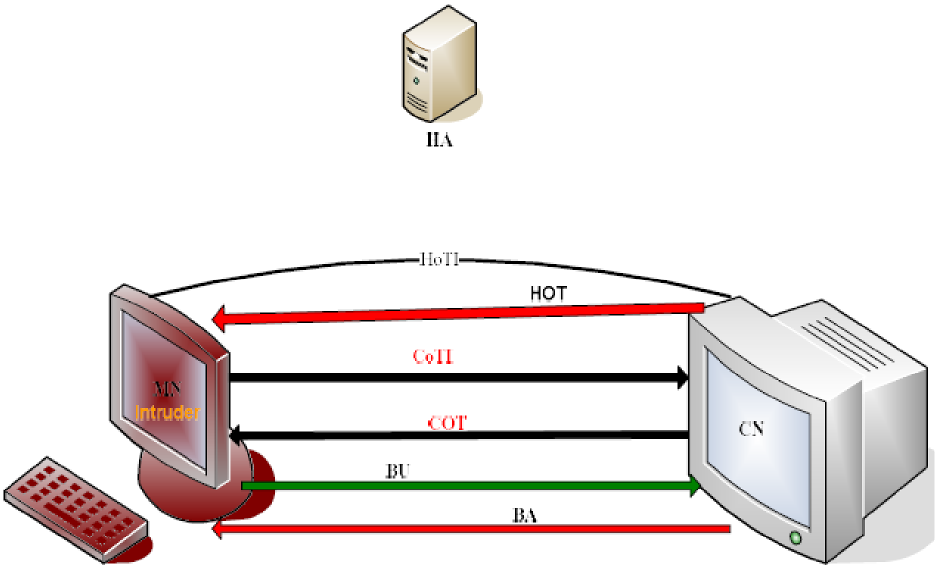


Figure 12. The intruder acts on the MN in the normal RRP.

the MN and the CN, because the intruder can send a false BU message with false HoA and CoA addresses to the CN. The CN accepts every BU message, whether or not it is from a valid MN or an intruder. The BA message is sent from the CN to the intruder to confirm that it has received the BU message (Figure 11).

As shown in Figure 12, the intruder acts like an MN because it generates false HoTI and CoTI messages that are sent to the CN. The CN receives both messages and creates a secret key for the HoTI and CoTI by sending

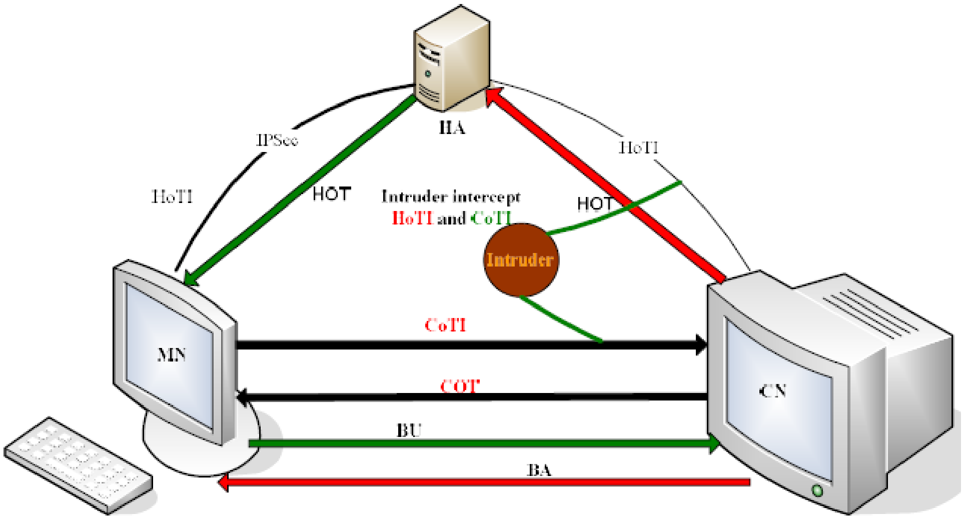


Figure 13. The intruder intercepts both the HoTI and CoTI messages.

HoT and CoT items to the intruder. Subsequently, the intruder generates the BU from the keygens and then forwards it to the CN. After the CN receives the BU, it immediately sends a BA message to the intruder. This works as though the intruder has intercepted the HoTI and CoTI messages and then replayed them to the CN (Figure 13).

Conclusion

This paper described the RRP and attempted to discuss in detail the possible attacks to the RRP in the current MIPv6 specification. The protocol was then implemented and verified using the Murphi model checker. The Murphi model checker verified the security of RRP and presented the associated attacks. The goal was to ensure that the security of RRP was equal to that of the non mobile IPv4. However, the result is less secure than IPv4.

REFERENCES

Ahmed I, Tariq U, Mukhtar S, Lhee S, Yoo SW, Yanji P, Hong M (2007). Binding update authentication scheme for mobile IPv6. Proceed. 3rd Int. Sympos. Inform. Assur. Secur., pp. 109-114.

Aura T, Roe M (2006). Designing the mobile IPv6 security protocol. Network Inform. Syst. Secur., 61: 1-27.

Blanchet M (2002). Migrating to IPv6: a practical guide for mobile and fixed networks, John Wiley & Sons, Inc.

Chen YC, Yang FC (2009). An efficient MIPv6 return routability scheme based on geometric computing, Proceed. World Acad. Sci. Eng. Technol., pp. 238-243.

Harini P, Ramanaiah OP (2008). Optimal routing in mobile IP with mobile IPv6. J. Mobile Commun., 2: 59-63.

Jeong S, Shin MK (2008). Route optimization scheme for proxy mobile IPv6. Proceed. 10th Int. Conf. Adv. Commun. Technol., pp. 1097-1100.

Kavitha D, Murthy EK, Hug SZ (2009). A secure route optimization protocol in mobile IPv6. Int. J. Comput. Network Secur. 9: 27-33.

Murphi web site (2012). Protocol analysis using murphi. Available at http://theory.stanford.edu/~aderek/murphi/links.html.

Radhakrishnan R, Jamil M, Mehfuz SM (2008). A robust return routability procedure for mobile IPv6. Int. J. Comput. Sci. Network Secur., 8: 234-240.

Shmatikov V, Mitchell JC (2002). Finite state analysis of two contract signing protocols. Theor. Comput. Sci., 283: 271-304.