A Secure and Decentralized Registration Scheme for IPv6 Network-Based Mobility

Senthil Kumar Mathi [1], M.L.Valarmathi [2]

[1] Department of Computer Science and Engineering, Amrita School of Engineering,
Amrita Vishwa Vidyapeetham University, Coimbatore, India.
[1] msenthil_cse@yahoo.co.in
[2] Department of Computer Science and Engineering,
Government College of Technology, Coimbatore, India.
[2] ml_valarmathi@rediffmail.com

***Abstract* — For frequent movement of a mobile device, there is a need for a secure registration procedure of the mobile device by announcing its current location to the home network, especially, if it is not in the home domain. While devising the registration procedure for mobile IPv6 (MIPv6) based network, it is essential to consider the security issues for cryptographic approaches and an infrastructure requirement on the network. If a public key based cryptography is used for improving the security, then the key exchange mechanisms of the communicants must be handled appropriately. The infrastructure based approach increases the complexity of the mobile device and the mobility agents and also requires an additional message exchanges. Hence, this paper deals with an infrastructure-less registration scheme with symmetric key approach that acts upon MIPv6 environment consisting of the mobile node, home agent, and correspondent node. The proposed scheme is simulated and evaluated for security using Murphi checker. The correctness of the signaling/message sequences of the proposed scheme are verified by the finite state machine. Finally, the simulation results reveals that better security and mutual authentication between MIPv6 nodes have been achieved, and further, mitigation for the various attack scenarios have also been addressed.**

Keyword- MIPv6, Transitions, Home registration, Correspondent registration, Hash function, Return routability

I. Introduction

Internet protocol (IP) mobility [1] allows mobile devices to get the services from the home network where it is initially registered and from the correspondents through the internet in spite of their position [2]. This is achieved for IPv4 based network with various registration schemes [3] proposed so far with an intermediate entity, called a foreign agent through which a mobile node (MN) can communicate with a home agent (HA) and a correspondent node (CN). But with IPv6 mobility (MIPv6), the MN can communicate with HA and CN directly without the need of the foreign agent, since the MN obtains its new IPv6 address called co-located care-of address (CoA) by stateless auto-configuration [4]. The mobility agent and CNs in MIPv6 store the MN's home address (HoA) with its CoA and then they send the packets destined for the MN directly at this CoA. The route optimization of the registration procedure is an integral part of MIPv6 and it's just an extension in IPv4 mobility and hence it requires the following design requirements for MIPv6: (i) movement detection - MN must detect that it has moved; (ii) address configuration - MN must discover or configure its CoA; (iii) binding update (BU) - MN must inform the HA about its new CoA; (iv) binding acknowledgement (BA) - HA must reply the MN for new binding updation; and (v) tunneling - HA must forward packets through a secure channel from the home network to MN's CoA.The MIPv6 registration is carried out in two-phases: home registration (HR) and correspondent registration (CR) and these phases are depicted in Fig. 1. The steps involved in the registration process are as follows.

1. MN performs address auto-configuration to get its CoA after the movement from the home link.
2. MN sends the BU message to HA and registers its CoA with the home link.
3. HA updates its binding list (BL) and sends the BA message back.
4. MN sends the BU message with the destination option to CN directly.
5. After the binding updation, ultimately, the CN can post the BA message to the MN's CoA directly.
6. If CN desires to send packets to MN, it sends them to the MN's new CoA directly.

A large number of related works [5]-[6] have been investigated on security issues of IPv6 mobility between the communicants. Almost, all of the works have described the schemes with the intention to improve the security and/or reduce the computational complexity of the MIPv6 registration. The crams have recommended that the reinstating of the scheme with new schemes to improve security. Therefore, the present paper focuses on infrastructure-less based registration scheme for the enhancement of security by incorporating the symmetric key approach. The organization of this paper is as follows: Section II explains briefly the related works on the existing registration schemes. In section III, a new infrastructure-less based scheme is proposed with the descriptions. Section IV discusses the security verification with Murphi model checker and finite state machine. Section V analyses the security consideration of the various registration schemes with the proposed one. Finally, section VI provides the conclusion.

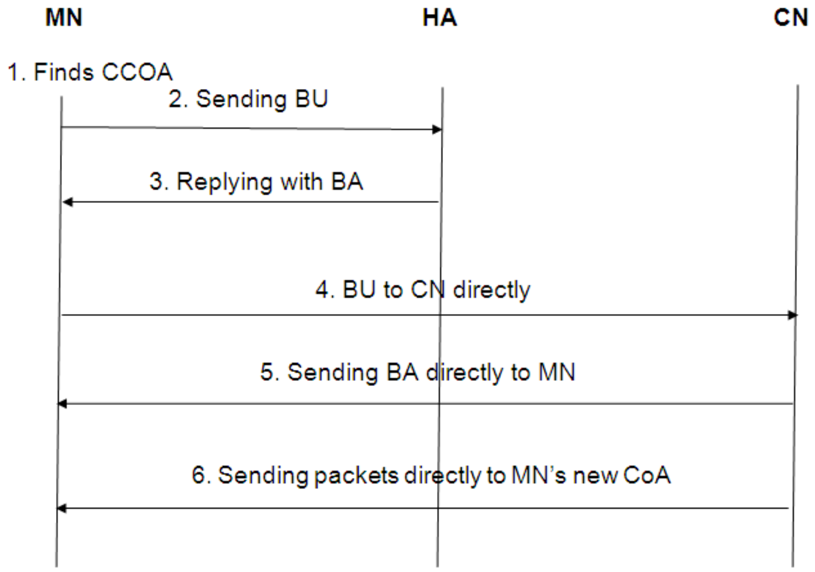

MN
HA
CN
1. Finds CCOA
2. Sending BU
3. Replying with BA
4. BU to CN directly
5. Sending BA directly to MN
6. Sending packets directly to MN's new CoA

Fig. 1. Registration in MIPv6 = HR Steps - 1, 2 and 3 + CR Steps - 4, 5, and 6

II. RELATED WORKS

In this section, we discuss some of the related works on the registration schemes of MIPv6. Basically, the registration schemes for MIPv6 are categorized into two major groups. The first group depends on an additional support for protecting registrations due to the key handling concerns and they can be categorized into two subgroups. The first subgroup is known as the symmetric-key based approach since they protect the registration process by the symmetric key shared between the communicants. The second subgroup is known as asymmetric based approach since they depend on a public/private key pair. The second group is known as an infrastructure-less registration schemes. They are suited to the scenarios where nodes do not have the dependency on infrastructure support for key handling issues during the registration process.

A. Infrastructure-based Registration Schemes

1) Symmetric-key based approach

Static shared key version 1 (SSKv1) scheme [7] relies on an initial setup for a secret key shared between MN and CN. However, the SSKv1 scheme is vulnerable to malicious MNs flooding attacks due to the intercept of the message by an intruder between the MN and CN. Dupont et al. enhanced the SSKv1 scheme by incorporating a CoA reachability test to derive at a new scheme SSKv2 [8]. But, the SSKv2 scheme has the same features, pros, and cons as the SSKv1 scheme. Password-based authenticated key exchange BU (PAKBU) scheme [9] entails a password sharing between the MN and CN. This approach provides the authentication between them by establishing a one-time binding management key for protecting the successive CR. Nevertheless, it needs the difficulty on key handling issues. Koo et al. (2006) proposed a new authentication scheme for BU which is based on ticket-based BU (TBU) scheme [10]. For protecting the connection securely between MN's home link and CN, the scheme uses IPSec tunnel. But, the TBU scheme imposes the overhead of synchronizing the clocks of the MN, HA, and CN as it uses timestamps to detect the rerun attacks. Additionally, it increases the complexity at HAs for supporting CRs.

2) Asymmetric-key based approach

Certificate-based BU (CBU) scheme [11] creates a long-term shared secret key between the MN and CN by using a digital signature and unilateral authenticated Diffe-Hellman key exchange scheme. However, this approach is suffered from the same shortcomings as the TBU scheme. Ren et al. (2006) proposed a hierarchical certificate-based BU (HCBU) scheme [12] with the enhancement on the CBU scheme with assurance of MN's ownership for a claimed CoA. Nevertheless, the MN might continuously necessitate to replicate the pre-handover phase, thereby, increasing the signaling overhead of the registration message sequence. The HCBU scheme also requires the use of trusted third parties to verify the CoAs used by the MNs and the infrastructure that supports the authentication service on the third parties.

Koo et al. (2007) proposed an extended ticket-based BU (ETBU) scheme [13] for extending the TBU scheme with the assumptions on CN's mobility. The scheme uses digital signature scheme and the CGA based technique to provide communal authentication among the MN and CN. On the other hand, it raises the vulnerabilities for denial of service (DoS) attacks; and involves the CN to perform the verification of digital signature in the initial CR.

Wafaa et al. proposed an ID-based encryption for enhancing the MIPv6 registration (INF-Based) signaling security [14] with the centralized network infrastrucure approach. The approach requires the third party called, public key generator for maintaining the private keys for the CN which can be used for decryption. In a basic HR (BHR) [15], MN instigates a HR process after moving from its home station for registering through secure tunneling [16]-[17]. Then HA updates its BL and sends BA message back. However, the HA possibly will not authenticate the CoA sent by the MN, since the MN might recline about its current position and entice HA to transmit traffic to a third party causing a DoS attack.

B. *Infrastructure-less Registration Schemes*

Child-proof authentication (CPA) scheme [18] aims to authenticate the primary entities of CRs in MIPv6. The CPA scheme requires one message and one-way hash function between the MN and the CN, causing minimal signaling overhead thereby reducing registration delay. On the other hand, the scheme is vulnerable to malicious MNs flooding attacks since it cannot endorse the claimed CoA. In addition, as the scheme uses timestamps to detect replayed BUs, it requires the synchronization in the clocks of the MN and the CN. Unauthenticated BU (UBU) scheme [19] is proposed to obtain a shared session key between the MN and the CN by using Diffe-Hellman key exchange scheme. The MN and the CN use the shared secret in authenticating initial and successive CRs. However, it is susceptible to false BU attack as it engrosses an unauthenticated key exchange based on Diffe-Hellman between the MN and the CN. Optimizing MIPv6 (OMIPv6) scheme [20] combines the return routability procedure (RRP) and Diffe-Hellman key exchange scheme. It consists of an initial registration phase and a subsequent registration phase with a correspondent node. The scheme uses a shared session key between an MN and a CN. Nevertheless, the MN and the CN first execute the RRP to set up a shared secret with the similar susceptibilities in the initial registration.

Early BU (EBU) scheme [21] is intended to lessen the high registration latency caused by the RRP. Since the scheme improves the RRP by moving HoA and CoA tests to a handover stage. However, there is a cost for this lessening in delay due to the usage of additional messages, and the periodic test on HoA by the MN. CGA-OMIPv6 scheme [22] combines the use of the RRP and the concept of cryptographically Generated Address (CGA) based technique [23]. But, this scheme engrosses the following requirements on MN: generation of public/private key pair; involvement of CGAs procedure to configure its HoA; CoA reachability proof by sending the test messages with a CN; and providing initial HoA ownership and reachability proofs at initial CR with the CN. However, it necessitates the MN and the CN to carry out additional public key operations during the initial CR for CGA based technique. Enhanced route optimization for mobile IPv6 (ERO-MIPv6) scheme [24] is a combination of EBU and the CGA-OMIPv6 schemes. It decreases the registration time between the MN and the CN during any CRs by sending one-way message. But, it increases the complexity at the CN for implementing the credit-based authorization technique [25] to restrict the amount of data that the CN can send to new CoA while simultaneously executing the CoA test.

Most of the investigations on the registration methods have accentuated that, on and average, the proposals are addressed with the requirement on network infrastructure based model for key management issues and cryptographic approaches and only few research attempts have been addressed with the decentralized registration procedure. Therefore, this paper proposes an infrastructure-less based mobile IPv6 registration scheme with the motivation to improve security on the signaling messages. The main contribution of this paper includes secure communication and mutual authentication between the mobile IPv6 principals by using shared key concepts. The correctness of the proposed scheme is verified by using finite state machine modeling. The proposed scheme is also evaluated using Murphi checker for the security functions and analyzed the attack prevention measures with the different scenarios. The next section discusses the proposed scheme.

III. Proposed Scheme

A. *Notations used*

The notations used in the proposed scheme with the descriptions are listed in Table I.

B. *Scheme description*

The proposed scheme is based on the suppositions that the nonces and the secret key values are pre-shared between the communicants without a third-party involvement. In the proposed scheme with decentralized network infrastrucure as depicted in Fig. 2, the steps HR1 to HR4 and CR1 to CR4 are used to describe the home and correspondent registrations respectively. The intricacies of the scheme are explained as follows.

(HR1): MN → HA: BUM, TID_{MN}, N_{HA}, $E_{K\text{-}MN\text{-}HA}$ [M_1], H [BUM || N_{MN} || $E_{K\text{-}MN\text{-}HA}$ [M_1]] where M_1 = ID_{HA}, CoA_{MN}, TID_{MN}, N_{HA}, and N_{MN}.

TABLE I
Notations used in the proposed scheme

Notations	Descriptions
$F_1 \| F_2$	Concatenation of fields F_1 and F_2
H [message]	Hash value of the message
ID_{HA} and ID_{CN}	Identity of HA and CN
N_{HA}, N_{MN}, and N_{CN}	Nonce of HA, MN and CN
TID_{MN}	Temporary identity of MN
CoA_{MN}	Care-of-address of MN
$E_K[M]$	Encryption of message M with key k
K-MN-HA	Shared secret key between MN and HA
SSK-CN-MN	Secure session key between MN and CN
K-MN-CN	Shared secret key between MN and CN
BUM and BAM	Bit patterns for indicating BU and BA message

(HR2) : HA: (upon receiving HR1)

- Search for an entry in HA's dynamic parameter database whose values (N_{HA}, N_{MN}) matches with (TID_{MN}, N_{HA}) in received HR1, then HA computes a new hash value $H^{'}$ with the received fields along with MN's nonce and validate it with the received hash value and finds the corresponding the shared secret key K-MN-HA to decrypt $E_{K\text{-}MN\text{-}HA}$ [M_1].
- Produce a new nonces $N^{'}_{HA}$, $N^{'}_{MN}$ and MN's new temporary identity $TID^{'}_{MN}$.
- Compute a new secret key $K^{'}$-MN-HA via one-way function:

$$K^{'}\text{-MN-HA} = \text{HMAC-SHA-1}\ (\text{K-MN-HA} \,\|\, N^{'}_{HA} \,\|\, TID^{'}_{MN} \,\|\, ID_{HA})$$

- Now, update the entry (TID_{MN}, N_{HA}, N_{MN}, K-MN-HA, Old_CoA_{MN}) in HA's dynamic parameter database with the new BU ($TID^{'}_{MN}$, $N^{'}_{HA}$, $N^{'}_{MN}$, $K^{'}$-MN-HA, CoA_{MN}).

(HR3): HA → MN: BAM, ID_{HA}, N_{HA}, $E_{K\text{-}MN\text{-}HA}$[$M_2$], H [BAM || ID_{HA} || N_{MN} || $E_{K\text{-}MN\text{-}HA}$[$M_2$]] where M_2 = $TID^{'}_{MN}$, $N^{'}_{HA}$, $K^{'}$-MN-HA, and $N^{'}_{MN}$.

(HR4) : MN: (upon receiving HR3)

- Compute $H^{'}$and validate it with the received hash value.
- Decrypt M_2 using K-MN-HA and store the new values $TID^{'}_{MN}$, $N^{'}_{HA}$, $K^{'}$-MN-HA, and $N^{'}_{MN}$.

Finally, the MN stops the message exchanges and ends with the successful completion of the HR registration.

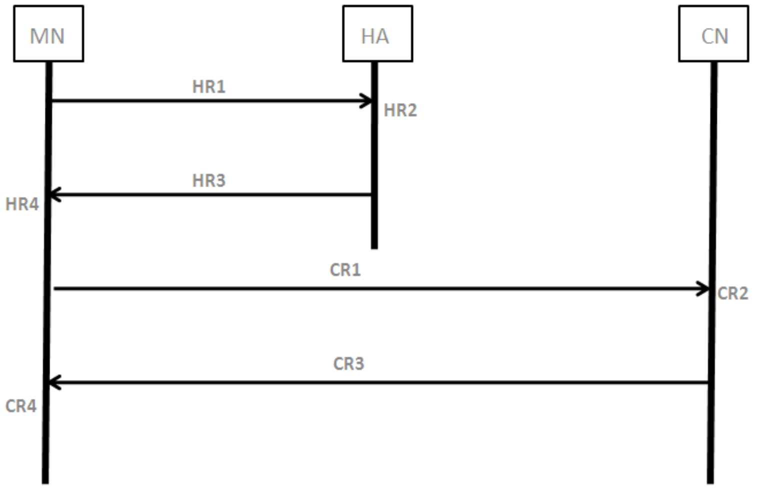


Fig. 2. Proposed registration scheme

(CR1): MN → CN: BUM, TID_{MN}, N_{CN}, $E_{K\text{-}MN\text{-}CN}$ [M_3], H [TID_{MN} || N_{MN} || $E_{K\text{-}MN\text{-}CN}$ [M_3]] where M_3 = TID_{MN}, CoA_{MN}, N_{CN}, and N_{MN}.

(CR2): CN: (upon receiving CR1)

- Compute new hash value with the received fields along with MN's nonce and compare it with the received hash value.
- CN decrypts $E_{K\text{-}MN\text{-}CN}$ [M_3] using K-MN-CN.
- Store the new CoA of MN.
- Generate new nonce N'CN and secure session key via one-way function.

$$SSK^{'}\text{-CN-MN} = \text{HMAC-SHA-1 (K-MN-CN} \parallel N^{'}_{CN} \parallel ID_{CN})$$

(CR3): CN → MN: BAM, TID_{MN}, N_{MN}, $E_{K\text{-}MN\text{-}CN}$ [M_4], H [TID_{MN} || N_{MN} || $E_{K\text{-}MN\text{-}CN}$ [M_4]] where M_4 = $SSK^{'}$-CN-MN, and $N^{'}_{CN}$.

(CR4) : MN: (upon receiving CR3)

After receiving the CR3 message, MN verifies the hash values to authenticate the CN and decrypts the encrypted part of the message using K-MN-CN to get a new nonce $N^{'}_{CN}$ and secure session key $SSK^{'}$-CN-MN for subsequent communication. Finally, the MN ends with the successful completion of CR.

IV. EVALUATION

A. *Finite State Machine and Murphi model*

The proposed scheme is simulated and evaluated using the Murphi model checker and finite state machine (FSM). Murphi verification system [26] consists of a Murphi compiler and Murphi description language. The Murphi compiler creates a special purpose verifier from the Murphi description. The modeling of the proposed scheme is designed with the FSM [27]-[28], whose descriptions are coded with the transition functions. The scenario for evaluation comprises of the input messages HR1, Upon_HR1, HR2, HR3, Upon_HR3, HR4, CR1, Upon_CR1, CR2, CR3, Upon_CR3 and CR4. The states of the FSM corresponding to the three entities are created with the internal states and they are 1) MN: {m_sleep, m_wakeup, m_validate, m_wait, m_commit}; 2) CN: {c_sleep, c_wakeup, c_wait, c_validate, c_commit}; and 3) HA: {h_sleep, h_wakeup, h_wait, h_validate, h_commit}. A transition function *Δ* of an individual message is defined and denoted by, *Δ (current_internal states, input_message) = {set of next_internal states}.*

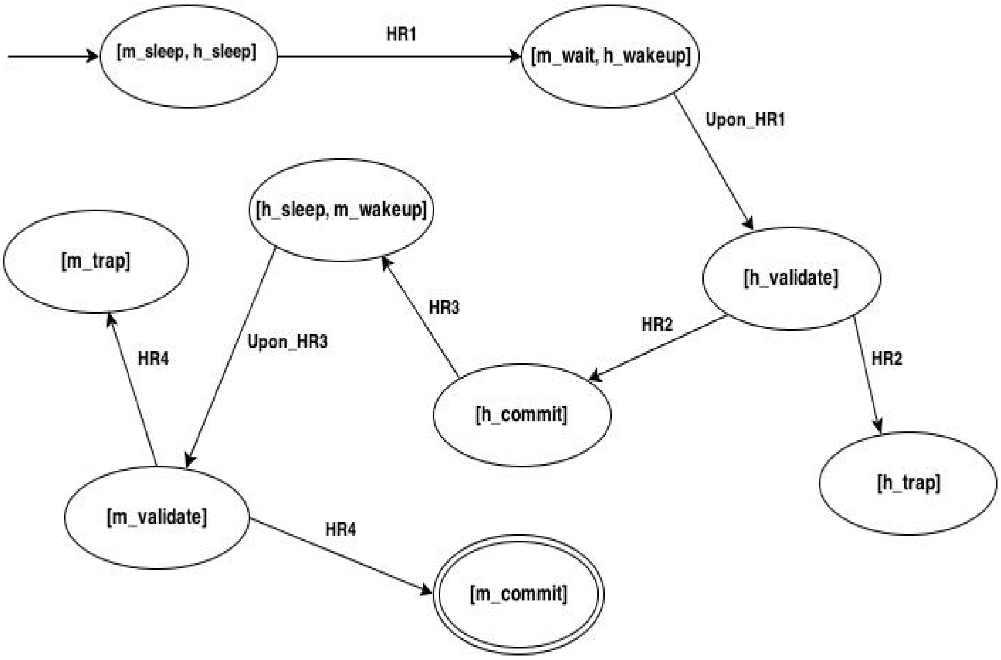


Fig. 3(a). FSM model - home registration

The finite state modeling of the HR procedure is depicted in Fig. 3(a). The FSM for HR starts with an initial state [m_sleep, h_sleep] and generates the transitioning to [m_wait, h_wakeup] on receiving the input of HR1 message for BU. Upon receiving HR1, the machine goes to the validation state on HA, [h_validate] and then switches the state to either an acceptance [h_commit] or a trap state [h_trap] based on the verification and validation of the HR1 message. If the machine in [h_trap], then the registration of the MN is rejected, otherwise it moves up with the next transition from [h_commit] to the state [h_sleep, m_wakeup] for the input of HR3 message and from this transitioned state, MN goes to validate state [m_validate]. After checking the HR3 message, MN switches to either the acceptance state [m_commit] on successful completion of the registration or to the trap state [m_trap] for rejection of the registration reply from HA. In HR, the BA message for MN is assured when it is entered into m_commit with the successful completion of the messages HR3.

In the similar way, the FSM for CR as depicted in Fig. 3(b) starts with an initial state [m_sleep, c_sleep] and generates the set of transition functions for ends up with either the final state [m_commit] or the trap state [m_trap] for BA on the registration.

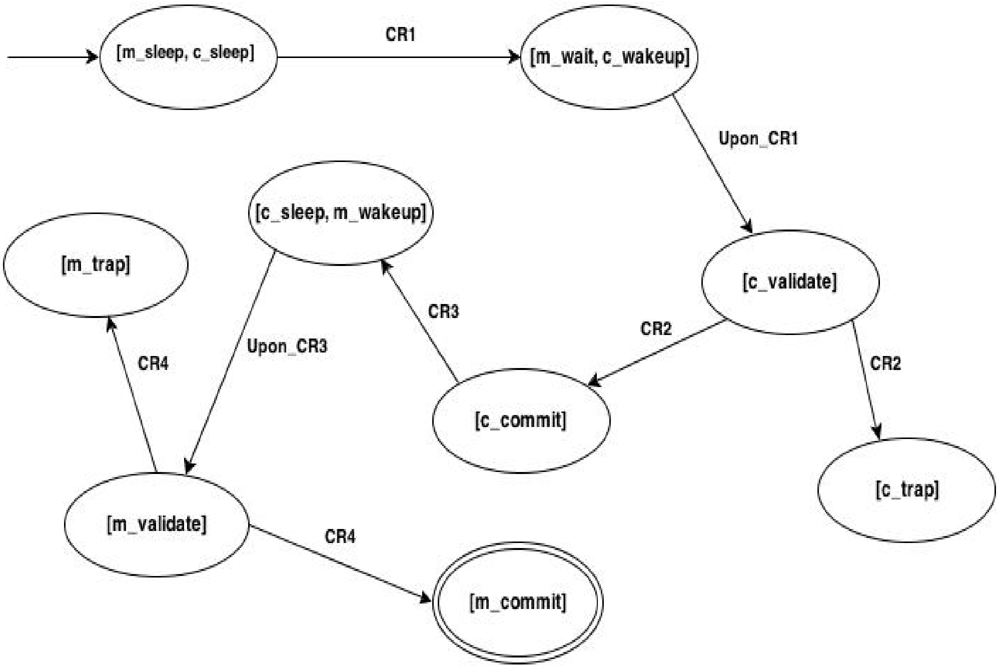


Fig. 3(b). FSM model - correspondent registration

B. *Security Verification*

In this current section, we analyzed our scheme for the prevention of the security threats by verifying the scheme sequence written in Murphi specifications and illustrated the proposed scheme with FSM transitions for the attacking scenarios which cause the failure to the intruder. For the security verification, we introduced the intruder for rerun attack, man-in-the-middle (MITM) attack and false binding attack. The model of the intruder allows the record of the messages. The intruder can be triggered with the following three different cases; 1) intruder intercepts the packet in the network 2) intruder performs rerun attack and 3) intruder modifies the packet. The proposed scheme is implemented in both cases (with and without the intruder). When the intruder model is triggered, the intruder can assail our scheme similar to the way it attacks the existing schemes. But, the attempt will be made to failure for the intruder in all the three cases. The sample scenarios are examined for the failure cases:

- The intruder captures HR1 message in the Murphi sequence as shown in Fig. 4 and changes the contents for TID_{MN}, and N_{HA}. Then the intruder sends a bogus message I_HR1 to the HA to deceive it. Nevertheless, HA computes the hash value H for M_1 in the bogus message and validate it with the received hash value. If they are not matching then, the HA rejects the I_HR1 message and fails to authenticate MN. Hence, the HA can easily detect the intruder and stop HR2 step from being proceeded to the MN without entering into the state h_commit. The following FSM transitions are accounted when the intruder captures HR1 message and sends the bogus message I_HR1 instead of the original message,

  Δ ([m_sleep, h_sleep], I_HR1) = [m_wait, h_wakeup]

  Δ ([m_wait, h_wakeup], Upon_I_HR1) = [h_validate]

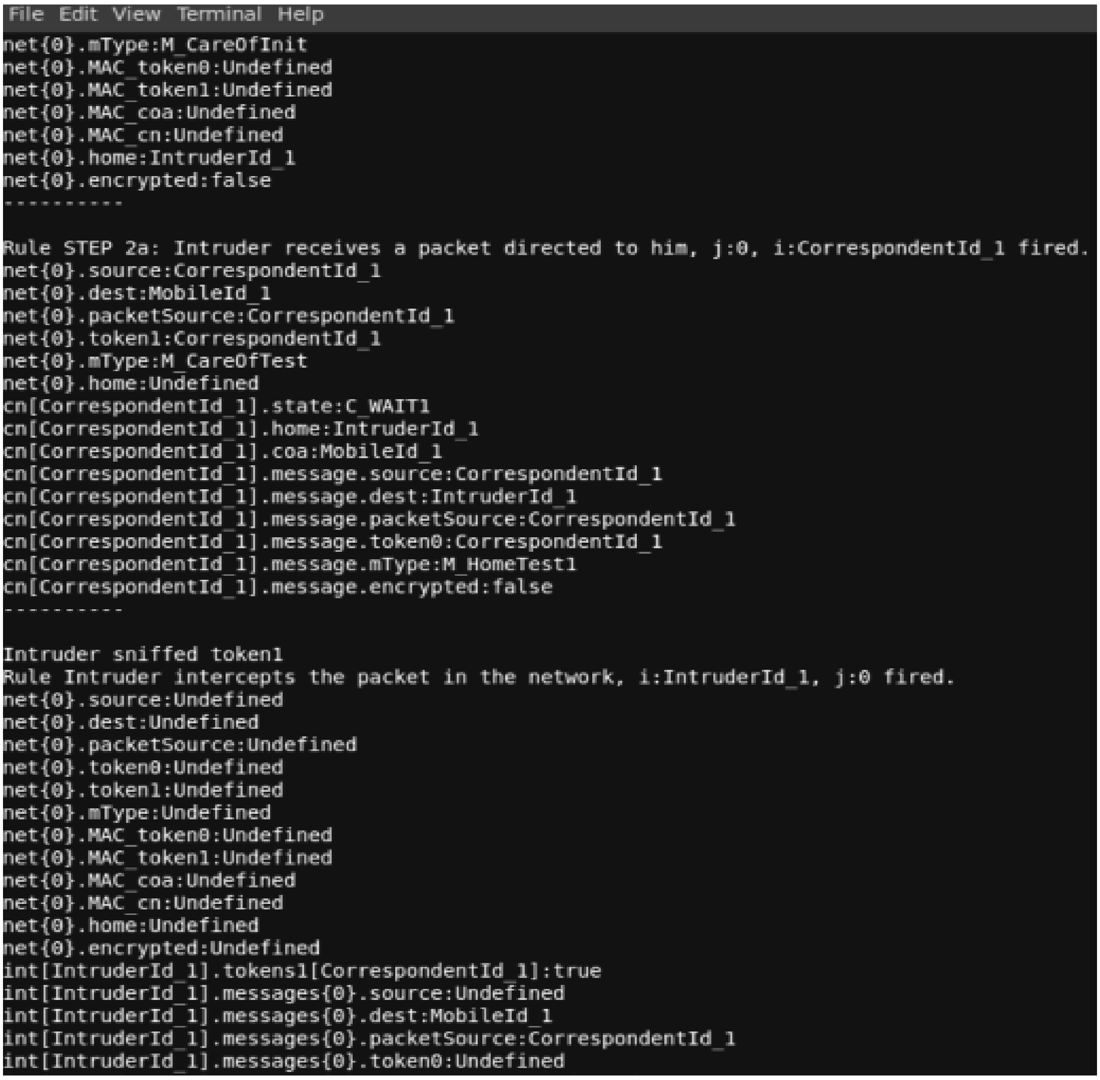
  Δ ([h_validate], I_HR2) = [h_trap]

- The intruder intercepts and reruns the CR3 message as I_CR3 to the MN as shown in Fig. 5. In this case, the intruder fails to determine the values of TID'_{MN}, N'_{HA}, N'_{MN} and SSK-CN-MN and goes to trap state. The corresponding transitions are recorded as follows,

  Δ ([c_commit], I_CR3) = [c_sleep, m_wakeup]

$$\Delta\ ([c\_sleep,\ m\_wakeup],\ Upon\_\ I\_CR3) = [m\_validate]$$
$$\Delta\ ([m\_validate],\ I\_CR4) = [m\_trap]$$

The intruder alters the temporary identity of the MN (TID_{MN}), which is easy for the CN to identify because the CR3 message has the original address for the correct sender (MN) with the encrypted value $E_{K\text{-}MN\text{-}CN}$ [M_4], such that when the MN decrypts the M_4 with K-MN-CN, it finds that their contents do not match henceforth, the MN does not make the transition to c_commit state.



```
net{0}.mType:M_CareOfInit
net{0}.MAC_token0:Undefined
net{0}.MAC_token1:Undefined
net{0}.MAC_coa:Undefined
net{0}.MAC_cn:Undefined
net{0}.home:IntruderId_1
net{0}.encrypted:false
----------

Rule STEP 2a: Intruder receives a packet directed to him, j:0, i:CorrespondentId_1 fired.
net{0}.source:CorrespondentId_1
net{0}.dest:MobileId_1
net{0}.packetSource:CorrespondentId_1
net{0}.token1:CorrespondentId_1
net{0}.mType:M_CareOfTest
net{0}.home:Undefined
cn[CorrespondentId_1].state:C_WAIT1
cn[CorrespondentId_1].home:IntruderId_1
cn[CorrespondentId_1].coa:MobileId_1
cn[CorrespondentId_1].message.source:CorrespondentId_1
cn[CorrespondentId_1].message.dest:IntruderId_1
cn[CorrespondentId_1].message.packetSource:CorrespondentId_1
cn[CorrespondentId_1].message.token0:CorrespondentId_1
cn[CorrespondentId_1].message.mType:M_HomeTest1
cn[CorrespondentId_1].message.encrypted:false
----------

Intruder sniffed token1
Rule Intruder intercepts the packet in the network, i:IntruderId_1, j:0 fired.
net{0}.source:Undefined
net{0}.dest:Undefined
net{0}.packetSource:Undefined
net{0}.token0:Undefined
net{0}.token1:Undefined
net{0}.mType:Undefined
net{0}.MAC_token0:Undefined
net{0}.MAC_token1:Undefined
net{0}.MAC_coa:Undefined
net{0}.MAC_cn:Undefined
net{0}.home:Undefined
net{0}.encrypted:Undefined
int[IntruderId_1].tokens1[CorrespondentId_1]:true
int[IntruderId_1].messages{0}.source:Undefined
int[IntruderId_1].messages{0}.dest:MobileId_1
int[IntruderId_1].messages{0}.packetSource:CorrespondentId_1
int[IntruderId_1].messages{0}.token0:Undefined
```

Fig. 4. Intruder model - Recording the HR messages for intercepting

V. Security Analysis

In this section, the security considerations are discussed with the analysis on existing and proposed schemes.

A. *Confidentiality*

In the proposed scheme, the secrecy of CoA_{MN} is preserved in both HR and CR between the communicants. In the HR, the BU message of MN with the HA is encrypted with the secret key K-MN-HA and the BA message of the HA with the MN is encrypted with the shared secret key K-MN-HA. Since the enciphered message of MN will not be deciphered at the attacker side. In the CR, the BU and BA messages with MN are encrypted with the secret key (K-MN-CN) and session key (SSK-CN-MN).

B. *Data integrity*

In the proposed scheme, the MN sends two messages (HR1 and CR1) to the HA and CN respectively. The intruder can intercept the messages, but he cannot correctly decipher or tamper the content because the two messages are enciphered using the shared secret keys. Hence, any alteration to the exchanged information would be not possible.

C. *Authentication*

The proposed scheme enables the communicants to satisfy the requirement on mutually authenticated procedure by the use of hash functions. As described in HR2, after receiving the message, HA finds an entry (TID_{MN}, N_{HA}) in their dynamic parameter database and gets the corresponding K-MN-HA of MN, Then, HA decrypts the encrypted message using K-MN-HA. This is the authentication of MN to HA. As described in HR4, MN decrypts M_2 using K-MN-HA and uses the values TID'_{MN}, N'_{HA}, K'-MN-HA, and N'_{MN} to compute the new hash value and compare it with H [M_2 || N_{MN}] in HR3. This is the authentication of HA to MN if the computed and received hash values are equal. In CR, after receiving the CR1 message, the CN computes a new hash value with the fields TID_{MN}, N_{CN} and $E_{K\text{-}MN\text{-}CN}$ [M_3] and compare it with the received hash value from CR3. If they are found equivalent then this is the authentication of MN to CN. Similarly MN verifies the hash values to authenticate the CN after receiving the CR3 message. Table II summarizes the authentication and confidentiality analysis of the various registration schemes with the proposed scheme.

D. *Rerun attack protection*

The nonce is used to thwart the rerun attack between the communicating parties of the MIPv6 registration. As mentioned in the proposed scheme, all the communicants MN, CN and HA in HR and CR messages are used with nonces for identifying the unique transaction in the registration environment for preventing the rerun attack.

E. *MITM attack prevention*

Any impostor attempts to make a false message cannot be accomplished in the proposed scheme since, it does not allow him to send a bogus BU message to the HA or CN due to the verification of the legitimacy of the principals with the hash functions of messages (HR2, HR4, CR2, and CR4) in both HR and CR steps and the unavailability of the shared and secure session keys in the channel as conferred in detail in the previous section.

TABLE II
Authentication and confidentiality analysis

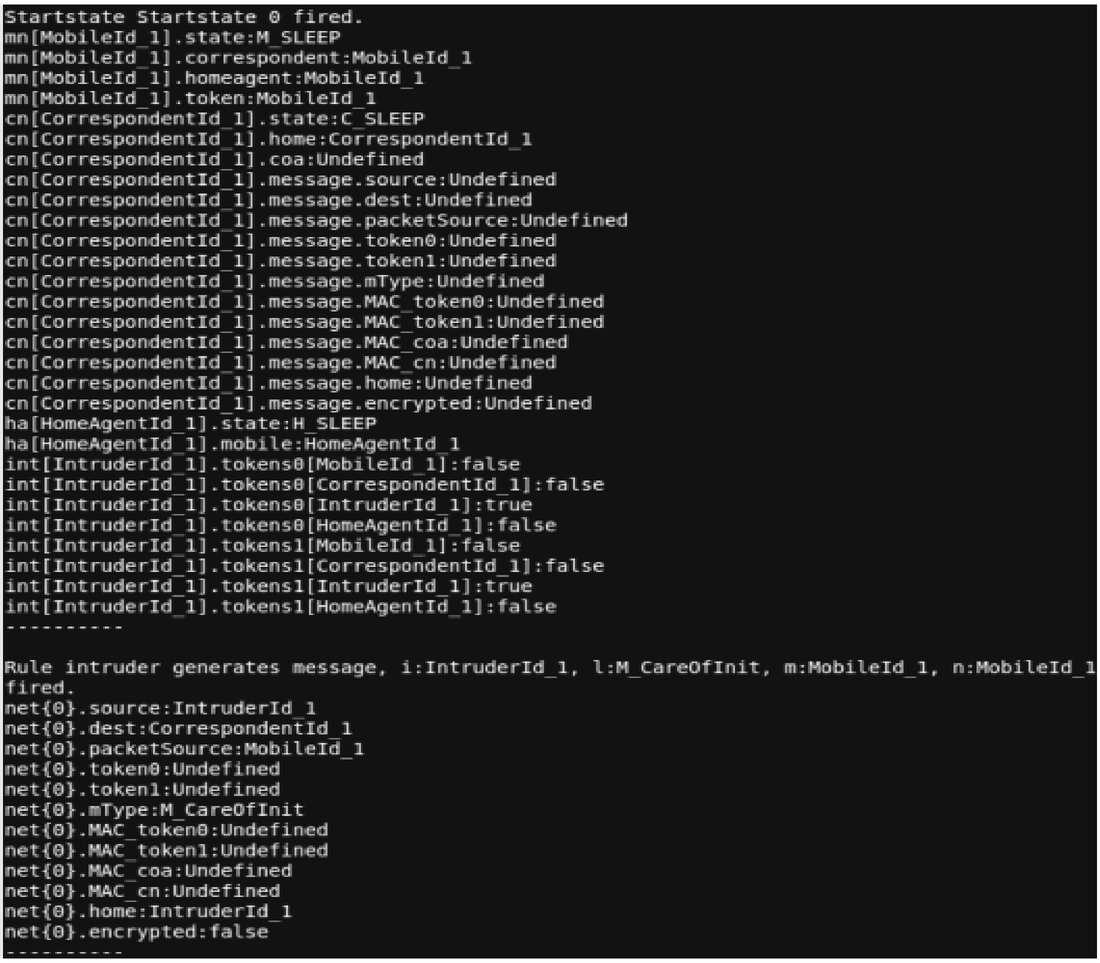
Scheme	Authentication of MN	Authentication of CN	Confidentiality of BU and BA
CPA	Yes	No	No
UBU	No	No	Yes
OMIPv6	No	No	No
EBU	No	No	Yes
CGA-OMIPv6	Yes	No	Yes
ERO-MIPv6	Yes	No	Yes
INF-Based	Yes	Yes	Yes
BHR	No	No	Yes
Proposed	Yes	Yes	Yes

F. *False BU attack prevention*

If an invader is on the channel between MIPv6 nodes and CN, he can send the false BU messages to HA and CN. The invader can detain these messages and alters them. Then, he delivers them to the CN or HA. If no authentication of these BU messages is to be completed, then HA and CN, deem that the message is delivered from the MN, will update their BL. But in the steps HR2 and CR2 of the proposed scheme, the invader fails at HA and CN during the validation of authentication since N_{MN} is not included in the message exchange rather it is stored at the recipient's side. The attack prevention analysis is tabulated in Table III.

TABLE III
Attack prevention analysis

Scheme	Rerun attack prevention	MITM prevention	False BU attack prevention
CPA	No	No	No
UBU and EBU	Yes	No	Yes
OMIPv6	Yes	No	No
CGA-OMIPv6	No	Yes	Yes
ERO-MIPv6	Yes	No	Yes
INF-Based	Yes	Yes	Yes
BHR	Yes	No	No
Proposed	Yes	Yes	Yes



```
Startstate Startstate 0 fired.
mn[MobileId_1].state:M_SLEEP
mn[MobileId_1].correspondent:MobileId_1
mn[MobileId_1].homeagent:MobileId_1
mn[MobileId_1].token:MobileId_1
cn[CorrespondentId_1].state:C_SLEEP
cn[CorrespondentId_1].home:CorrespondentId_1
cn[CorrespondentId_1].coa:Undefined
cn[CorrespondentId_1].message.source:Undefined
cn[CorrespondentId_1].message.dest:Undefined
cn[CorrespondentId_1].message.packetSource:Undefined
cn[CorrespondentId_1].message.token0:Undefined
cn[CorrespondentId_1].message.token1:Undefined
cn[CorrespondentId_1].message.mType:Undefined
cn[CorrespondentId_1].message.MAC_token0:Undefined
cn[CorrespondentId_1].message.MAC_token1:Undefined
cn[CorrespondentId_1].message.MAC_coa:Undefined
cn[CorrespondentId_1].message.MAC_cn:Undefined
cn[CorrespondentId_1].message.home:Undefined
cn[CorrespondentId_1].message.encrypted:Undefined
ha[HomeAgentId_1].state:H_SLEEP
ha[HomeAgentId_1].mobile:HomeAgentId_1
int[IntruderId_1].tokens0[MobileId_1]:false
int[IntruderId_1].tokens0[CorrespondentId_1]:false
int[IntruderId_1].tokens0[IntruderId_1]:true
int[IntruderId_1].tokens0[HomeAgentId_1]:false
int[IntruderId_1].tokens1[MobileId_1]:false
int[IntruderId_1].tokens1[CorrespondentId_1]:false
int[IntruderId_1].tokens1[IntruderId_1]:true
int[IntruderId_1].tokens1[HomeAgentId_1]:false
----------

Rule intruder generates message, i:IntruderId_1, l:M_CareOfInit, m:MobileId_1, n:MobileId_1
fired.
net{0}.source:IntruderId_1
net{0}.dest:CorrespondentId_1
net{0}.packetSource:MobileId_1
net{0}.token0:Undefined
net{0}.token1:Undefined
net{0}.mType:M_CareOfInit
net{0}.MAC_token0:Undefined
net{0}.MAC_token1:Undefined
net{0}.MAC_coa:Undefined
net{0}.MAC_cn:Undefined
net{0}.home:IntruderId_1
net{0}.encrypted:false
----------
```

Fig. 5. Intruder model: Generating I_CR3 message

VI. Conclusion

In the current research, the registration scheme for MIPv6 with the infrastructure-less based method has been proposed for securing the signaling messages of MN with HA and CN. The proposed scheme investigates the security issues in the registration of IPv6 mobility. This research has highlighted the several security parameters such as authentication, integrity and confidentiality with the symmetric key shared between principals and discusses the prevention measures against the security attacks such as rerun attack, MITM attack and false BU attack. The registration steps of the scheme are simulated and verified by the Murphi model checker. The correctness of the scheme sequences are verified by finite state machine. The scheme can be modeled for further concepts such as UMTS, distributed MIPv6, proxy MIPv6, WLAN, and beyond 3G based mobile networks.

References

[1] C. E. Perkins, “Mobile IP”, IEEE Communication Magazine, pp. 84-99, May 1997.

[2] C. E. Perkins, “IP encapsulation within IP”, RFC 2003, pp. 1-18, Oct. 1996.

[3] Senthil Kumar Mathi, and M.L.Valarmathi, “Mobile IP registration schemes: A survey”, International Journal of Computer Applications, vol. 51(17), pp.24-34, August 2012.

[4] S. Thomson, and T. Narten, “IPv6 Stateless Address Autoconfiguration”, RFC 2462, December 1998.

[5] Hero Modares, Amirhossein Moravejosharieh, Jaime Lloret, and Rosli Salleh, “A survey of secure schemes in MobileIPv6”, Journal of Network and Computer Applications, 2013, [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2013.07.013.

[6] Arun Kumar Tripathi, Anchal Srivastava, Harish Pal, Somendra Tiwari and Pandey, “Security Issues in Mobile IPv6”, IJCA Proceedings on Development of Reliable Information Systems, Techniques and Related Issues, pp. 12-15, April 2012.

[7] C. Perkins, “Securing Mobile IPv6 Route Optimization Using a Static Shared Key”, RFC 4449, June 2006.

[8] F. Dupont, and J.M. Combes, “Care-of Address Test for MIPv6 using a State Cookie”, Internet-Draft: draft-dupont-mipv6-rrcookie-06.txt, June 2008.

[9] H.S. Yoon, R.H. Kim, S.B. Hong, and H.Y. Youm, “PAK-based Binding Update Method for Mobile IPv6 route optimization”, In Proceedings of the International Conference on Hybrid Information Technology, (Washington, DC, USA), pp. 617-623, IEEE Computer Society, 2006.

[10] J. D. Koo, J. Koo, and D. C. Lee, “A New Authentication Scheme of Binding Update Scheme on and over in Mobile IPv6 Networks”, Emerging Directions in Embedded and Ubiquitous Computing, vol.4097, pp. 972-978, Springer Berlin, 2006.

[11] F. Bao, R. Deng, Y. QIU, and J. Zhou, “Certificate-based Binding Update Scheme ”, Internet-Draft: draft-qiu-mip6-certificatedbinding-update-03.txt, March 2005.

[12] K. Ren, W. Lou, K. Zeng, F. Bao, J. Zhou, and R. H. Deng, "Routing optimization security in mobile IPv6", Computer Networks, vol. 50 (13), pp. 2401-2419, 2006.
[13] J.D. Koo, and D.C. Lee, "Extended Ticket-Based Binding Update Scheme for Mobile IPv6 Networks," IEICE transactions on communications, vol. 90-B (4), pp. 777-787, 2007.
[14] Wafaa A. H. Ali Alsalihy, and Majed Salam S. Alsayfi, "Integrating Identity-Based Encryption in the Return Routability Scheme to Enhance Signal Security in Mobile IPv6", Wireless Personal Communication, Vol.68, no 3, pp. 655-669, February 2013.
[15] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
[16] S. Kent, "IP Encapsulating Security Payload", RFC 4303, 2005.
[17] J. Arkko, V. Devarapalli, and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.
[18] G. O' Shea, and M. Roe, "Child-proof Authentication for MIPv6," ACM SIGCOMM Computer Communication Review, vol. 31(2), pp. 4-8, 2001.
[19] S. M. Faccin, and F. Le, "Dynamic Diffie Hellman based Key Distribution for Mobile IPv6", Draft-le-mobileip-dh-01.txt, December 2001.
[20] W. Haddad, F. Dupont, L. Madour, S. Krishnan, and S. Park, "Optimizing MIPv6", Internet-Draft: draft-haddad-mipv6-omipv6-01.txt, February 2004.
[21] C. Vogt, R. Bless, M. Doll, and T. Kuefner, "Early Binding Updates for Mobile IPv6", in IEEE Wireless Communications and Networking Conference-2005, vol. 3, pp. 1440-1445, March 2005.
[22] W. Haddad, L. Madour, J. Arkko, and F. Dupont, "Applying Cryptographically Generated Addresses to Optimize MIPv6", Internet-Draft: draft-haddad-ip6-cga-omipv6-04.txt, May 2005.
[23] T. Aura, "Cryptographically Generated Addresses", RFC 3972, 2005
[24] J. Arkko, C. Vogt, and W. Haddad, "Enhanced Route Optimization for Mobile IPv6", RFC 4866, May 2007.
[25] C. Vogt, "Credit-Based Authorization for Concurrent IP-Address Tests", Tech. Rep.TM-2005-3, Institute of Telematics, University of Karlsruhe, Germany, June 2005.
[26] "Murphi description language and verifier", http://sprout.stanford.edu/dill/murphi.
[27] Nabil Elkadhi, and Hazem El-Gendy. "Advanced method for cryptographic scheme verification", Journal of Computational Methods in Sciences and Engineering, vol. 6(5), pp. 109-119, 2006.
[28] Ferdinand Wagner, Ruedi Schmuki, Thomas Wagner, and Peter Wolstenholme, Modeling software with Finite State Machines, Auerbach publications, 2006.