Journal of Engineering Science and Technology
Vol. 13, No. 3 (2018) 573 - 588

AN ENHANCED BINDING UPDATE SCHEME FOR NEXT GENERATION INTERNET PROTOCOL MOBILITY

SENTHILKUMAR MATHI[1,*], M. L. VALARMATHI[2]

[1]Department of Computer Science and Engineering
Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India
[2]Department of Electrical and Electronics Engineering,
Alagappa Chettiar College of Engineering and Technology, Karaikudi, India
*Corresponding Author: m_senthil@cb.amrita.edu

Abstract

In recent years, the usage of mobile devices has become essential for people, both for business and for their daily activities. The mobile devices can get services directly from their home network and from other correspondent devices regardless of their position without using any intermediate agent. It is achieved by using mobility based Internet Protocol version 6, called as next generation internet protocol mobility. Since network mobility uses open air interface as a communication medium, it is possible for many security threats and attacks that might attempt to get unauthorized access from the participating entities. Consequently, the protection of network mobility from threats is one of the most demanding tasks as it must be considered without increasing the complexity while enhancing security. Hence, the paper proposes an enhanced location update scheme by incorporating the optimal asymmetric encryption method based on the random oracle model for providing security and efficiency. It emphasizes the security goals such as authentication, integrity, and confidentiality from the security analysis. In addition, it addresses the attack prevention analysis for the attacks such as rerun, man-in-the-middle and false location update. The proposed scheme is simulated and verified for security properties using a security validation tool - Automated Validation of Internet Security Protocols and Applications. Finally, the simulation studies show that the latency of the proposed scheme is reduced significantly when compared the other location update schemes.

Keywords: Binding update, Optimal asymmetric encryption, Authentication, Cryptographically generated address, Location update.

Nomenclatures

CN-Private, CN-Public	Private and public keys of CN
$E_K\{M\}$	Encryption of message M using key k diameter
H[fields]	Generation of hash value with the given fields
HA-Private, HA-Public	Private and public keys of HA
MN-Private, MN-Public	Private and public keys of MN
N'_{CN}	New nonce of CN generated at CN for MN
N_{HA}, N_{MN}, N_{CN}	Nonce of HA, MN and CN respectively
N'_{HA}, N'_{MN}	New nonces of HA and MN generated at HA
OAEP(m, r)	Generation of OAEP for the inputs m and r
R_1, R_2, R_3, R_4	Random integers based on OAEP model
$R_{HA\text{-}MN}$, $R_{CN\text{-}MN}$	Random integers among HA, CN and MN
TID_{MN}	Temporary identity of MN

Greek Symbols

μ_{HMN}, μ_{MHA}	MN's and HA's signatures
μ_{CMN}, μ_{CNM}	MN's and CN's signatures
$\oplus$	Exclusive-OR operation

Abbreviations

AVISPA	Automated Validation of Internet Security Protocols and Applications
BA	Binding Acknowledgement
BU	Binding Update
CGA	Cryptographically Generated Address
CL-AtSe	Constraint-Logic-based Attack Searcher
CN	Correspondent Node
CNA	Address of CN
CoA	Care-of Address
ECC	Elliptic Curve Cryptography
HA	Home Agent
HAA	Address of HA
HLPSL	Higher-Level Protocol Specification Language
HMAC	Hash-based Message Authentication Code
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
K-CGA	Keyed-Cryptographically Generated Address
MIP	Mobile Internet Protocol
MITM	Man-in-the-Middle
MN	Mobile Node
OAE	Optimal Asymmetric Encryption
OAEP	Optimal Asymmetric Encryption Padding
OFMC	On-the-fly Model-Checker
SHA-1	Secure Hash Algorithm 1
TTP	Trusted Third Party

1. Introduction

Due to the rapid increase in the number of mobile devices, mobile computing is now becoming a very hot topic. The mobile user's requirement involves continuous internet connectivity regardless of the physical location. This leads to the development of the various mobility based internet protocols [1].

Accordingly, the latest trends follow a line of investigation on the internet using MIP or IP mobility. It is intended to allow MN to be reachable forever with a single address, namely a home address, regardless of its tangible location. It is also possible for the MN to maintain existing connections with a peer node, also known as CN. The MN also obtains a temporary CoA when it roams to another visitor link as in IPv4 mobility. However, it does not route the packets destined to HA through a foreign agent. Since the MN obtains a new IPv6 address from the foreign link using stateless or stateful address auto-configuration, the MN can communicate with HA and CN directly without the need of the foreign agent in IPv6 mobility [2].

The MN may possibly have several CoAs at the same time with different subnet prefixes in the case of overlapping coverage of wireless networks. The MN registers one of its up-to-date CoAs with the HA by executing a home registration procedure. The MN starts the home registration by sending a BU message to the HA, which contains the MNs home address and CoA. The HA then stores the association/binding between the home address and the CoA in its database. Using this binding, the HA maintains the location updates of the MNs that are away from home CoAs. The HA then terminates the home registration process by returning a BA message to the MN.

While MN is outside the home network, it can communicate with CN either indirectly or directly. In an indirect path [3], all the packets transferred to the MN are routed through its home network as discussed previously. However, in the case of the direct path, also called as route optimization, the MN must register its current location with the CN by establishing a registration wherein the MN and the CN exchange BU and BA messages. Consequently, the CN creates a database entry and stores the association between the MN's home address and CoA. The IP mobility uses various location update or binding update approaches. These approaches must be secured against attacks that might try to obtain unauthorized benefits from any participating principals. Hence, the research in location update for IPv6 mobility has focused more towards next generation mobility based networks for improving the security. Depending on the way the security elucidations are necessitated, there exist many strategies for improving security and as a result of many location update methods, also known as binding update schemes, were developed. Nevertheless, an efficacy in terms of the considerable reduction in the computational load and binding update time plays an important role with the same significance as the security improvement of the location update process.

The contribution of the paper includes a new location update scheme with the decentralized design for IPv6 based network mobility. It constitutes the BU scheme with the adoption of optimal asymmetric encryption method which does not require a separate entity called as a private-key generator. It is based on the assumption that the entity pairs MN-HA and MN-CN will establish a pre-shared security association consists of public-private key pairs, parameters required for random oracle model, secret keys, and nonces through the secure tunnel. Also, the proposed scheme is validated using a security tool AVISPA. The simulation

studies are conducted for the latency estimation of the proposed scheme and the delay is reduced significantly when compared the other BU schemes.

The rest of the paper is organized as follows. Section 2 discusses the related works. In section 3, the preliminaries for the proposed scheme are reviewed. The detailed description of the proposed location update scheme is described in section 4. Section 5 presents the security analysis. The formal validation of the proposed scheme using AVISPA is given in section 6. Section 7 discusses the performance evaluation. Finally, section 8 concludes the paper.

2. Related Works

This section discusses a state of art survey of binding update schemes in IPv6 mobility. Basically, the BU schemes are classified into two, infrastructure independent and infrastructure dependent. The former classification requires an additional support for key management and they can be sub-divided into two approaches: a symmetric key based approach and an asymmetric key based approach and it is shown in Fig. 1. The latter specifies the major BU schemes based on infrastructure independent are shown in Fig. 2.

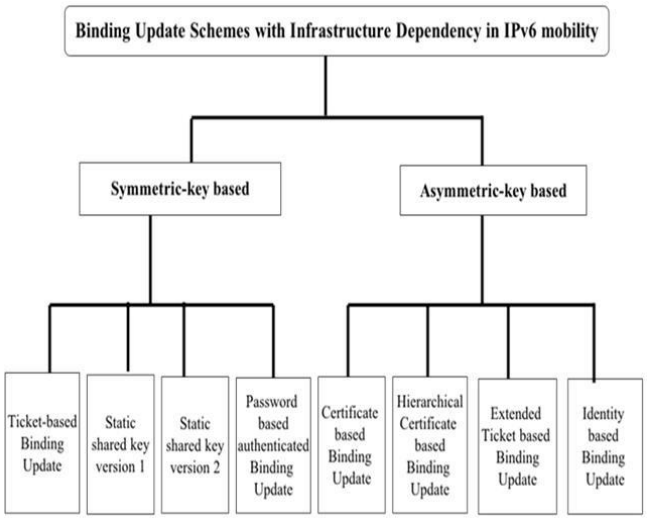

Fig. 1. Existing BU Schemes with Infrastructure dependency.

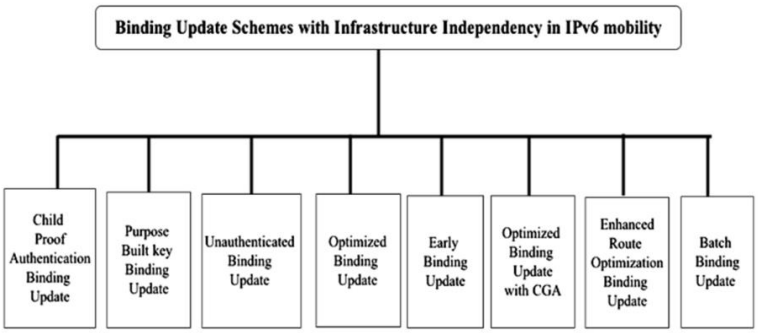

Fig. 2. Existing BU Schemes with Infrastructure independency.

2.1. Symmetric key based BU schemes

Koo et al. recommended an authentication scheme for BU based on ticket-based method [4]. This scheme uses a tokenized timestamp for validating the binding update packets. However, it imposes the overhead of synchronizing the clocks of MN, HA, and CN. Subsequently, two versions of static shared key [5, 6] were proposed for the binding update. They require a pre-shared setup for distributing the secret keys between the communicants, but both the schemes were exposed to malicious MNs flooding attacks.

The password-based authenticated BU was then suggested by Yoon et al. [7]. It aims to provide authentication between MN and CN by sharing a password. This approach establishes a one-time binding password for protecting the successive registration with an overhead on each password handling issues.

2.2. Asymmetric key based BU schemes

The digitally signed secret key is shared between the communicating principals in certificate-based BU scheme [8]. However, this scheme imposes the operating cost for signature operations on shared secret key at MN. An enhancement version of the above scheme was proposed by Ren et al. [9], namely, a hierarchical certificate based BU scheme with TTP. Nevertheless, the CN might continuously necessitate communicating with TTPs, thus, increasing the signaling overhead of the BU message sequence. It also requires the use of TTPs to verify the CoAs used by the MNs and the use of an additional infrastructure that supports the authentication of TTPs.

In extended ticket based BU scheme [10], the MN uses digital signature and CGA technique to generate CoA. The CGA technique is used to provide mutual authentication among the MN and CN. Conversely, it involves the CN to make the verification of digital signature in the initial registration. Subsequently, an identity-based encryption is incorporated in the binding update scheme [11] for enhancing the signal security. However, it requires a third party called as the private key generator for maintaining the private keys which can be used for decryption at CN.

2.3. Infrastructure independent BU schemes

Child-proof authentication scheme [12] requires time-stamped messages between the communicants of IPv6 mobility. As this scheme uses the timestamp to detect replayed signaling messages, it also demands synchronization of the clocks. In addition, it is vulnerable to malicious MNs flooding attacks since it cannot endorse a claimed CoA. The purpose-built key BU approach [13] intends to authenticate the originator of a communication with additional two messages. However, it cannot reduce the registration time since it requires a total of four messages in any correspondent registration between MN and CN. Next, a shared session key between the MN and the CN was introduced in unauthenticated BU scheme [14]. Nevertheless, it was prone to initiate false BU messages between MN and CN.

Optimized BU scheme [15] aims to integrate the return routability procedure and Diffie-Hellman key exchange scheme to share a session key. However, it introduces the high registration latency. To overcome this drawback, early BU

scheme [16] was suggested with additional messages and periodic test on home address of MN. An enhanced version of optimized BU is suggested with CGA scheme [17] that combines the use of the return routability and the concept of CGA based technique. However, it necessitates MN and CN to carry out additional public key operations. Enhanced route optimization for BU [18] uses a credit-based authorization technique for authenticating the entities. This scheme reduces the registration delay by sending one one-way message. However, it increases the complexity caused by credit-based authorization. Subsequently, the research [19] proposed by Yeh et al. explores BU scheme using ECC based Diffie-Hellman key exchange protocol. Other proposals on location update scheme for IPv6 mobility [20-25] were suggested for improving signaling security of BU messages. However, the present paper proposes a new location update scheme with the decentralized design for IPv6 based network mobility. The proposed scheme constitutes the BU scheme with the adoption of optimal asymmetric encryption method which does not require a separate entity called as the private-key generator.

3. Optimal Asymmetric Encryption

The current section briefly discusses the OAE method. OAEP is a randomized and cryptographic hash-based method to provide mutual authentication between the communicating hosts. The OAEP method uses two cryptographic hash functions G and H, called as random oracles prior to the optimal asymmetric encryption. The random oracles are arbitrary mapping function from a possible input domain to a random response from its output domain [26]. The output of OAEP is the concatenated values of P and Q. This output of the OAEP is then encrypted using public key cryptosystem. The receiving entity decrypts the message using the private key to retrieve the message and random value r for further verification. OAEP method makes use of less cryptographic operations than the other methods relying on discrete logarithm problem with heavy computations. Thus, it is easy and can be computed with a low communication cost which is suitable for low power mobile devices.

4. Proposed Binding Update Scheme

The proposed binding update scheme with OAEP is based on the assumption that the entity pairs MN-HA and MN-CN will establish a pre-shared security association through the secure tunnel. The security association consists of public-private key pairs, parameters required for random oracle model, secret keys, and nonces. This section discusses the generation of CoA, proposed binding update scheme with home agent and proposed binding update scheme with the correspondent node.

4.1. Generation of CoA

The mobile node generates a new CoA (128-bit IPv6 address) after moving from its home network in IPv6 mobility environment [17]. Basically, an IPv6 address consists of a 64-bit subnet prefix and a 64-bit interface identifier. In the proposed scheme, the 64-bit interface identifier is computed using hash-based message authentication code algorithm, HMAC-SHA1 with the secret key shared between the communicating entities along with the other parameters such as public-key, nonces, and the random oracle values.

The process of generating CoA using hash-based message authentication code algorithm with the shared secret key is called a K-CGA procedure. When MN moves to a new network, the nearest router sends a broadcast message containing the network prefix to it. It then adopts the K-CGA procedure to generate a CoA. In K-CGA procedure as shown in Fig. 3, the input parameters defined for the CoA generation includes a randomized 128-bit modifier value, a 64-bit subnet prefix, a public key of an entity, nonces, random oracle parameters and a security parameter sec with three bits – a predefined security flag with the binary values between 000 to 111. There are two HMAC-SHA1 passes used in K-CGA procedure in which the first pass uses the 128-bit modifier, 9 octets of zero i.e. 18 hexadecimal 0's, public key, and other fields. From the output of the first pass, the leftmost 112 bits are assigned to hash1. The leftmost 16-bit of hash1 is then multiplied with security flag value and checked if the value is zero or not. If so, the modifier value is incremented by one bit. The loop proceeds until the first leftmost *16*sec* values are zero.

The second pass of HMAC-SHA1 is then continued with the arguments such as the modifier, subnet prefix, and other fields. Subsequently, the first 64 bits of this hash2 from the second pass is assigned as the interface identifier. If the newly generated IPv6 address is duplicated, the procedure is then continued until no duplication is found. Finally, the subnet prefix is concatenated with the newly obtained interface identifier.

Input = Subnet prefix (64 bit), modifier (128 random bit), public-key of HA / CN, *sec* (security flag), MN-HA secret key / MN-CN secret key, nonce of MN, nonce of HA / CN, and the random oracle parameter $R_{HA\text{-}MN}$ / $R_{CN\text{-}MN}$.

Output = A new *care-of address*.

Begin:

1. Apply HMAC-SHA1 algorithm using MN-HA secret key / MN-CN secret key on the concatenated values of modifier, nine octets of zero, public-key of HA / CN, nonce of MN, nonce of HA / CN, and $R_{HA\text{-}MN}$ / $R_{CN\text{-}MN}$.
2. Set leftmost 112 bits of HMAC-SHA1 output as *hash1*.
3. If leftmost bits of (16**sec*) of *hash1* is equal to zero

   Set collision count to zero.

   else

   Increment the modifier.
4. Apply *HMAC-SHA1* algorithm using MN-HA-secretkey / MN-CN-secretkey on the concatenated values of subnet prefix, modifier, collision count (current count), HA's / CN's public key, nonce of MN, nonce of HA / CN and $R_{HA\text{-}MN}$ / $R_{CN\text{-}MN}$.
5. Set leftmost 64 bits of *HMAC-SHA1* output of the above as *hash2*.
6. Form the interface identifier from hash2 by considering selected 3 bits of sec as leftmost bits and set 70^{th} and 71^{st} bits as zero.
7. Concatenate the subnet prefix and interface identifier.
8. If the calculated *care-of address* is a duplicate of existing address

   Increment collision count and go to *step 4*.

   else

   Stop the procedure.

Fig. 3. K-CGA procedure for CoA generation.

4.2. Proposed binding update scheme with HA

After computing CoA, the MN carries out the BU scheme to register its current location with HA. The message flow diagram of the proposed BU with HA is shown in Fig. 4. The proposed BU with HA consists of the following steps.

1. MN → HA: TID_{MN}, HAA, N_{MN}, $H[R_{HA\text{-}MN} \oplus R_1]$, M_1, μ_{HMN}
   where
   $M_1 = E_{HA\text{-}Public}\{OAEP(TID_{MN}, HAA, newCoA, oldCoA, R_1, N_{MN}, R_{HA\text{-}MN})\}$,
   $R_{HA\text{-}MN} \in \{0, 1\}^L$, L is the number of bits in the modulus operation of the encryption
   $R_1 \in \{0, 1\}^U$, U is a fixed integer
   $\mu_{HMN} = Sign_{MN\text{-}Private}(newCoA \| N_{MN} \| N_{HA})$
2. Upon receiving the message, HA first decrypts M_1 using its private key (HA-Private) and extracts the fields of OAEP. It then validates the nonce N_{MN} and verifies the signature μ_{HMN} using the public key of HA. If the outcome of signature verification succeeds, the HA validates the address owner of the CoA. Next, the HA computes the hash value using the random values $R_{HA\text{-}MN}$ and R_1. If the computed hash value does not match with the received hash value, the HA then rejects the packet.
3. HA → MN: HAA, TID_{MN}, N_{HA}, $H[R_{HA\text{-}MN} \oplus R_2]$, M_2, μ_{MHA}
   where
   $M_2 = E_{MN\text{-}Public}\{OAEP(HAA, TID_{MN}, new\_TID_{MN}, R_2, N'_{HA}, N'_{MN}, R_{HA\text{-}MN})\}$
   $R_2 \in \{0, 1\}^U$, U is a fixed integer
   $\mu_{MHA} = Sign_{HA\text{-}Private}(newCoA \| N'_{MN} \| N'_{HA})$
4. Upon receiving the message, MN decrypts M_2 using its private key (MN-Private) and obtains OAEP fields. Next, it performs the verification on the appended signature μ_{MHA} and authenticates HA by computing the hash value using the extracted values of $R_{HA\text{-}MN}$ and R_2. If it does not match with the received hash value, the MN rejects the packet. Otherwise, it stores the new_ TID_{MN}, N'_{HA}, and N'_{MN}.

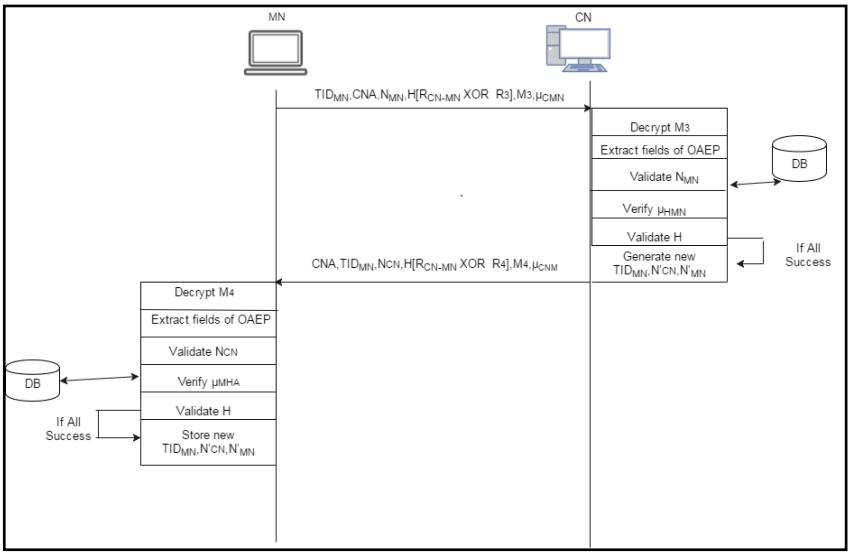

Fig. 4. Message flow diagram of the proposed BU with HA.

4.3. Proposed binding update scheme with CN

After generating CoA, the MN carries out the BU scheme to register its location with CN. The message flow diagram of the proposed BU with CN is shown in Fig. 5. The proposed BU with CN consists of the following steps.

1. MN → CN: TID_{MN}, CNA, N_{MN}, $H[R_{CN\text{-}MN} \oplus R_3]$, M_3, μ_{CMN}
   where
   $M_3 = E_{CN\text{-}Public}\{OAEP(TID_{MN}, CNA, newCoA, oldCoA, R_3, N_{MN}, R_{CN\text{-}MN})\}$
   $R_{CN\text{-}MN} \in \{0, 1\}^L$, L is the number of bits in the modulus operation of the encryption
   $R_3 \in \{0, 1\}^U$, U is a fixed integer
   $\mu_{CMN} = Sign_{MN\text{-}Private}(newCoA \| N_{MN} \| N_{CN})$
2. Upon receiving the message, CN deciphers M_3 using its private key (CN-Private) and extracts the fields of OAEP. It then validates the nonce N_{MN} and verifies the signature μ_{CMN} using the public key of CN. If the outcome of signature verification succeeds, the CN validates the address owner of the CoA. Next, the CN computes the hash value using the random values $R_{CN\text{-}MM}$ and R_3. If the computed hash value does not match with the received hash value, the CN then rejects the packet.
3. CN → MN: CNA, TID_{MN}, N_{CN}, $H[R_{CN\text{-}MN} \oplus R_4]$, M_4, μ_{CNM}
   where
   $M_4 = E_{MN\text{-}Public}\{OAEP(CNA, TID_{MN}, R_4, N'_{CN}, R_{CN\text{-}MN})\}$
   $R_4 \in \{0, 1\}^U$, U is a fixed integer
   $\mu_{CNM} = Sign_{CN\text{-}Private}(newCoA \| N_{MN} \| N_{CN})$
4. Upon receiving the message the MN decrypts M_4 using its private key (MN-Private) and obtains OAEP fields. Next, it carries out the validation on N_{CN}, and verifies the signature μ_{CNM}. It then authenticates CN by computing the hash value using $R_{CN\text{-}MN}$ and R_4. If it does not match with the received hash value, the MN rejects the packet.

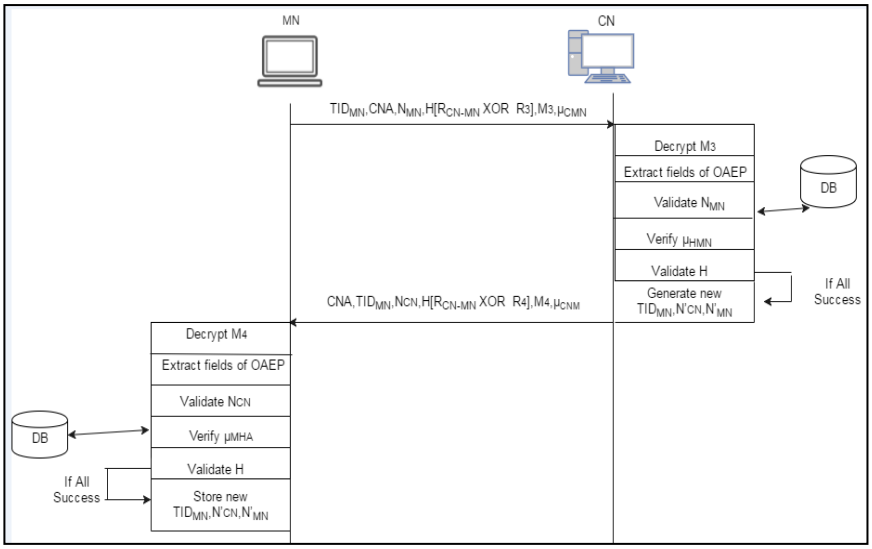

Fig. 5. Message flow diagram of the proposed BU with CN.

5. Security Analysis

In this section, the security analysis of the proposed binding update with the existing schemes is discussed. In addition, it addresses the prevention measures for attacks such as false BU attack, replay attack, and MITM attack. The proposed BU is an infrastructure-less scheme and involves fewer security computations than the other BU schemes. The comparison of the methods used in the proposed and other schemes is tabulated in Table 1.

Table 1. Comparisons of methods used.

Binding update scheme	Dependency on Infrastructure	Method
O'shea & Roe [12]	Dependent	Hash function
Veigner & Rong [20]	Dependent	Hash function
Radhakrishnan et al. [21]	Independent	Hash function
Kavitha et al. [22]	Dependent	Hash function
Chen & Yang [23]	Partially dependent	Hash function
Rajkumar et al. [24]	Dependent	Hash function
Alsalihy & Alsayfi [11]	Dependent	ID based encryption
Yeh et al. [19]	Dependent	ECC based encryption
Proposed	Independent	OAE

5.1. Confidentiality and integrity

For achieving the secrecy of BU and BA messages, the proposed scheme uses the optimal asymmetric encryption. Thus, the BU messages containing CoA is combined with the random integers and sent to HA and CN in an encrypted form. As it requires a private key for decryption, it is impossible to take out any value from the message exchanges between the communicants of the proposed scheme.

In the proposed scheme, the data integrity of the packets is provided in both binding update and acknowledgement messages. After receiving the messages at the receiver, the integrity of the messages can be verified in the proposed scheme using hash values $H[R_{HA\text{-}MN} \oplus R_1]$, and $H[R_{HA\text{-}MN} \oplus R_2]$ in home registration. Also, the alteration of the original BU message is not possible since it can be opened only by HA's private key which is unknown to the other users. Similarly, the hash codes $H[R_{CN\text{-}MN} \oplus R_3]$, and $H[R_{CN\text{-}MN} \oplus R_4]$ are verified for the integrity of the messages at the respective recipient sides.

5.2. Authentication

In the proposed binding update scheme, the HA authenticates MN by comparing the hash value of $(R_{HA\text{-}MN} \oplus R_1)$ using HMAC-SHA1 with the shared secret key between MN and HA. If they are equal, the MN's authentication is then verified. In addition, HA verifies the obtained CoA using K-CGA verification procedure to authenticate the ownership of MN. Similarly, after receiving the binding update message from MN, CN decrypts M_3 using its private key to get $R_{CN\text{-}MN}$. The CN then computes the hash value using $R_{CN\text{-}MN}$ and R_3. If the computed hash value matches with the received hash value, CN then authenticates the packet by MN. Besides, CN authenticates the CoA's ownership by using K-CGA verification procedure. Table 2 summarizes the security analysis of the existing BU schemes with the proposed BU scheme.

Table 2. Comparison of security attributes of CoA.

BU scheme	Authentication	Data integrity	Confidentiality
O'shea & Roe [12]	No	No	No
Veigner & Rong [20]	No	No	No
Radhakrishnan et al. [21]	No	No	No
Kavitha et al. [22]	No	Partially	No
Chen & Yang [23]	Partially	No	No
Rajkumar et al. [24]	No	Partially	No
Alsalihy & Alsayfi [11]	No	No	Yes
Yeh et al. [19]	Yes	No	No
Proposed	Yes	Yes	Yes

5.3. Protection against replay and MITM attack prevention

The flow of communication can be disrupted if an attacker replays an existing BU message in IPv6 mobility. Based on the usage of nonces (N'_{HA}, N'_{MN}, N'_{CN}) in each BU and BA messages of the proposed scheme, the replay attack is prevented. In the proposed scheme, it is unfeasible for an adversary to impersonate as a legitimate user for obtaining the CoA through MITM attack since the MN's CoA has been encrypted with OAEP method. On the other hand, it cannot be decrypted without knowing the private key of the recipient.

5.4. False BU attack prevention

An opponent can intentionally send a false BU message to either HA or CN. This type of attack allows the opponent to imitate and reject the service of MN for redirecting all the packets. It is not possible in the proposed scheme since it uses the pre-shared random values $R_{HA\text{-}MN}$ and R_1 between MN and HA. Similarly, the random values $R_{CN\text{-}MN}$ and R_3 are used between MN and CN. Table 3 summarizes the attack prevention analysis.

Table 3. Attack prevention analysis

BU scheme	False BU	MITM	Replay
O'shea & Roe [12]	No	No	No
Veigner & Rong [20]	No	No	No
Radhakrishnan et al. [21]	No	Yes	No
Kavitha et al. [22]	No	Yes	No
Chen & Yang [23]	No	No	No
Rajkumar et al. [24]	No	Yes	No
Alsalihy & Alsayfi [11]	Yes	Yes	No
Yeh et al. [19]	No	Yes	Yes
Proposed	Yes	Yes	Yes

6. Formal Evaluation Using AVISPA

The proposed scheme is simulated and evaluated using AVISPA – a widely accepted security analysis tool [27]. The simulation of the proposed scheme using AVISPA consists of four role definitions written in HLPSL for MN, HA, CN and session wherein, the other three roles are triggered. The MN's role in the

proposed scheme is written in HLPSL. The HLPSL specifications are then translated into equivalent specifications. Subsequently, these specifications are given to the back-ends such as OFMC and CL-AtSe that performs the automatic analysis. The back-end results of the HLPSL for the proposed scheme is shown in Fig. 6. The translation time for the operation has been noted as 0.17 seconds and computation time as 0.91 seconds respectively. Thus, from the analysis of OFMC and CL-AtSe results, it is observed that no attacks are found, and the security goals are achieved in the proposed scheme. From the OFMC analysis of the proposed scheme, it is seen that the scheme is safe and runs with a bounded number of sessions with the number of visited nodes at 123 and the search time is 0.84 seconds with a depth search of 9 plies. From the CL-AtSe results, it is observed that the proposed scheme executes a bounded number of sessions with 93 analysed states and 27 reachable states.

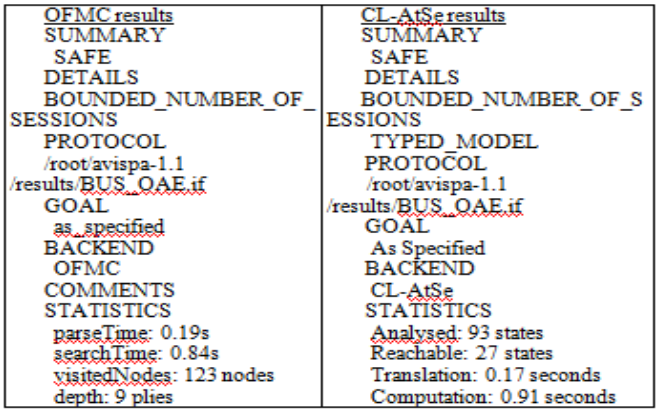

Fig. 6. OFMC and CL-AtSe results of the proposed BU scheme.

7. Performance Evaluation

In this section, the performance results of the proposed BU schemes with the other related works are discussed. The message sizes from the simulation of the proposed binding update with HA and CN and system parameters [28] shown in Table 4 are used for estimating the binding update latency.

Table 4. System parameters

Processing time in HA, CN, and MN	0.5 ms
Propagation time in wireless links	2×10^{-3} s
Bit rate in wireless links	2×10^{6} bps
Propagation time in wired links	0.5 ms
Bit rate in wired links	100×10^{6} bps
Hash operation	0.019111 ms

The total binding update latency can be calculated as, total BU latency = time required at source for BU and BA messages + time required at intermediate nodes + time required at destination for processing BU and BA messages.

Here, time required at source = time required for processing BU and BA messages at source + time required for transmitting BU and BA messages over wireless links + time required for propagation over wireless links (propagation time).

Time required at intermediate nodes = time required for transmitting BU and BA messages + propagation time in wired links at intermediate nodes.

Time required at destination = Processing time required for BU message + processing time required for BA message

Accordingly, total BU delay for the proposed scheme between MN and HA is estimated as follows,

Time required at source = 2(0.5+0.19+1.01234) + 0.461 + 0.789 + 4 = 6.9523 ms

Time required at intermediate nodes = 0.04312 + 0.03413 + 0.5 + 0.5 = 1.073 ms

Time required at destination = 2(0.5 + 3.02 + 0.172331) = 7.38466 ms

Total BU delay = 6.95234 + 1.07725 + 7.38466 = 15.41425 ms

Similarly, total BU delay for the proposed scheme between MN and CN is computed as follows,

Time required at source = 2(0.5 + 0.19 + 0.87132)+ 0.257+0.279+4 = 7.65864 ms

Time required at intermediate nodes = 0.00031+ 0.0071 + 0.5 + 0.5 = 1.00741 ms

Time required at destination = 2(0.5 + 3.02 + 0.152134) = 7.344268 ms

Total BU delay = 7.65864 + 1.00741 + 7.344268 = 16.010318 ms

Figures 7 and 8 illustrate the comparison of binding update latency between the communicants of the proposed scheme. Here, the proposal O'shea and Roe [12] and Jo and Inamura [25] show less binding update time but offers low-level security. Ren et al. [9] give a little high binding update latency with the considerable amount of security than the previous proposals. Subsequently, the scheme suggested by Chen and Yang [23] provide some degree of security and a reduction in latency of about 16.89 ms and 15.527 ms for the pairs MN-HA and MN-CN respectively.

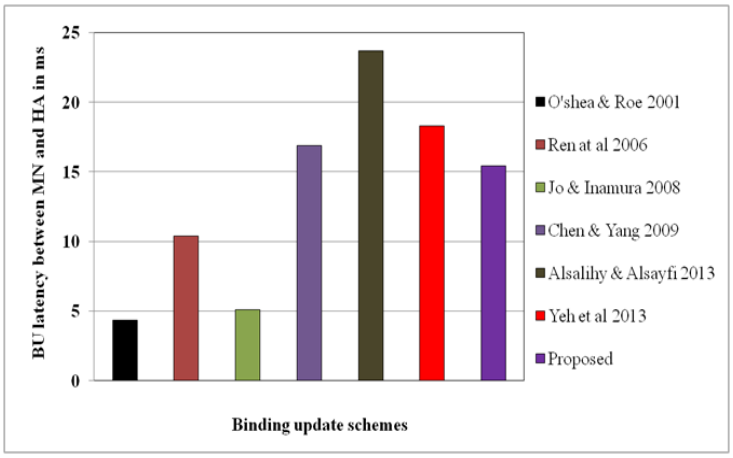

Fig. 7. BU latency between MN and HA.

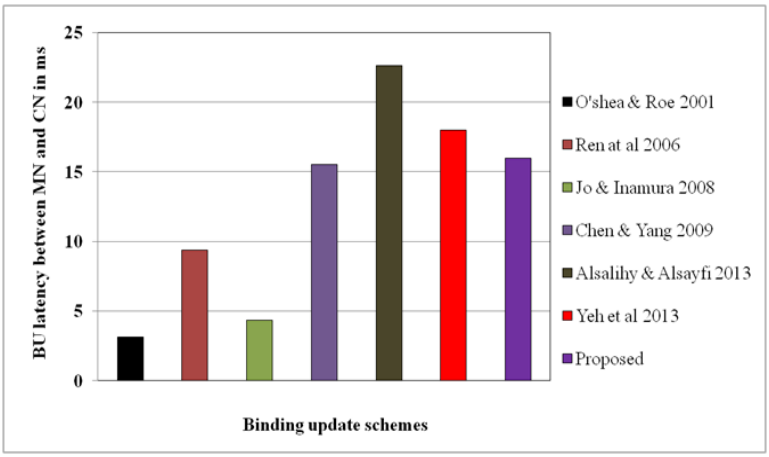

Fig. 8. BU latency between MN and CN.

When compared to all the other BU schemes, the scheme proposed by Alsalihy and Alsayfi [11] afford the highest latency due to the usage of infrastructure based private-key generator and the redundant repetition of message exchanges between the communicants. Yeh et al. [19] provide a significant reduction in the latency while improving security. However, compared to all the proposals, the proposed scheme shows less binding update latency while providing better security.

8. Conclusion

In this paper, the BU scheme for IPv6 mobility with decentralized design has been proposed for securing location update messages of MN with HA and CN. The proposal using OAE employs the K-CGA procedure to generate CoA. It is an infrastructure-less scheme since it does not involve the private-key generator. Here, the OAE is used to provide mutual authentication between all the correspondent pairs. The proposed BU scheme has achieved the necessary goals of security such as authentication, integrity, and confidentiality. It has also highlighted the prevention measures against the security attacks such as rerun attack, MITM attack, and false BU attack. The BU steps of the proposed scheme are simulated and verified using AVISPA model checker. No successful attacks were found from the results of the AVISPA for the proposed binding update with HA and CN by MN. Finally, the numerical results demonstrate that the proposed location update scheme provides the significant reduction in the binding update latency than all the other schemes of IPv6 mobility. The design of a binding update scheme for distributed IP mobility (compatible architecture) with all correspondent nodes including those that do not support route optimization is a point of further research.

References

1. Saha, D.; Mukherjee, A.; Misra, I.S.; and Chakraborty, M. (2004). Mobility support in IP: a survey of related protocols. *IEEE network*, 18(6), 34-40.
2. Mathi, S.K.; and Valarmathi, M.L. (2015). A secure and efficient binding update scheme with decentralized design for next generation IP mobility. In

Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, Springer India, 423-431.

3. Modares, H.; Moravejosharieh, A.; Lloret, J.; and Salleh, R. (2014). A survey of secure protocols in mobile IPv6. *Journal of Network and Computer Applications*, 39, 351-368.
4. Koo, J. D.; Koo, J.; and Lee, D.C. (2006). A new authentication scheme of binding update protocol on handover in mobile IPv6 networks. *Proceedings of the International Conference on Embedded and Ubiquitous Computing*, Springer Berlin Heidelberg, 972-978
5. Perkins, C.E. (2006). Securing Mobile IPv6 route optimization using a static shared key, RFC 4449.
6. Vogt, C.; and Arkko, J. (2007). A taxonomy and analysis of enhancements to mobile IPv6 route optimization (No. RFC 4651).
7. Yoon, H.S.; Kim, R.H.; Hong, S.B.; and Youm, H. Y. (2006). PAK-based binding update method for mobile IPv6 route optimization. In *2006 International Conference on Hybrid Information Technology*, 2, 617-623.
8. Bao, F.; Deng, R.; Qiu, Y.; and Zhou, J. (2005). Certificate-based binding update protocol (CBU). *IETF Draft*.
9. Ren, K.; Lou, W.; Zeng, K.; Bao, F.; Zhou, J.; and Deng, R.H. (2006). Routing optimization security in mobile IPv6. *Computer Networks*, 50(13), 2401-2419.
10. Jung-Doo, K.O.O.; and Dong-Chun, L.E.E. (2007). Extended ticket-based binding update (ETBU) protocol for mobile IPv6 (MIPv6) networks. *IEICE transactions on communications*, 90(4), 777-787.
11. Alsalihy, W.A.A.; and Alsayfi, M.S.S. (2013). Integrating identity-based encryption in the return routability protocol to enhance signal security in mobile IPv6. *Wireless personal communications*, 68(3), 655-669.
12. O'shea, G.; and Roe, M. (2001). Child-proof authentication for MIPv6 (CAM). *ACM SIGCOMM Computer Communication Review*, 31(2), 4-8.
13. Bradner, S.; Mankin, A.; and Schiller, J. (2003). A framework for purpose-built keys (PBK).
14. Le, F.; and Faccin, S.M. (2001). Dynamic Diffie Hellman based key distribution for mobile IPv6. *Internet Engineering Task Force*.
15. Dupont, F.; and Haddad, W. (2006). Optimizing Mobile IPv6 (OMIPv6). *draft- dupont-mipshopomipv6-00. txt*.
16. Vogt, C.; Bless, R.; Doll, M.; and Kuefner, T. (2005). Early binding updates for mobile IPv6. In *IEEE Wireless Communications and Networking Conference*, 3, 1440-1445.
17. Anbarasi, P.N.; and Mathi, S. (2016). A tokenized binding update scheme for next generation proxy IP mobility. In *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, Springer India, 193-207.
18. Arkko, J.; Vogt, C.; and Haddad, W. (2007). *Enhanced route optimization for mobile IPv6*, (No. RFC 4866).
19. Yeh, L.Y.; Yang, C.C.; Chang, J.G.; and Tsai, Y.L. (2013). A secure and efficient batch binding update scheme for route optimization of nested

NEtwork MObility (NEMO) in VANETs. *Journal of network and computer applications*, 36(1), 284-292.

20. Veigner, C.; and Rong, C. (2004). A new route optimization protocol for Mobile IPv6 (ROM). *Proceedings of the International Computer Symposium*.
21. Radhakrishnan, R.; Jamil, M.; and Mehfuz, S. (2008). Moinuddin, A robust return routability procedure for mobile IPv6. *International Journal of Computer Science and Network Security (IJCSNS)*, 8, 243-240.
22. Kavitha, D.; Murthy, E.K.; and Hug, S.Z. (2009). A secure route optimization protocol in mobile IPv6. *International Journal of Computer and Network Security (IJCSNS)*, 9(3), 27-34.
23. Chen, Y.C.; and Yang, F.C. (2009). An efficient MIPv6 return routability scheme based on geometric computing. *Proceedings of world academy of science, engineering and technology*, 39, 238-243.
24. Rajkumar, S.; Prabhu, M.R.; and Sivabalan, A. (2012). Securing binding updates in routing optimization of mobile IPv6. *Research Journal of Applied Sciences, Engineering and Technology*, 4(12), 1633-1636.
25. Jo, M.; and Inamura, H. (2008). Secure route optimization for mobile network node using secure address proxying, *Proceedings of the network operations and management symposium*, IEEE, 137-143.
26. Liu, J.; and Li, J. (2008). A novel key exchange protocol based on RSA-OAEP. *Proceedings of the Tenth International Conference on Advanced Communication Technology*, 3, 1641-1643.
27. AVISPA Team. (2006). AVISPA v1.1 user manual. 2013, 1, 20. Retrieved February 15, 2016, from http://www.avispa-project.org.
28. Argyroudis, P.G.; Verma, R.; Tewari, H.; and O'Mahony, D. (2004). Performance analysis of cryptographic protocols on handheld devices. *IEEE International Symposium on Network Computing and Applications*, 169-174.