Investigation of binding update schemes in next generation internet protocol mobility

Lingam Srikanth and Mathi Senthilkumar*

Department of Computer Science and Engineering,
Amrita School of Engineering, Coimbatore,
Amrita Vishwa Vidyapeetham, India
Email: cb.en.p2cse17014@cb.students.amrita.edu
Email: m_senthil@cb.amrita.edu
*Corresponding author

Abstract: IPv6 development and deployment have opened up several concerns in reference to its transition from IPv4 to IPv6 and its practical challenges. Mobility support is one of the significant features in IPv6 that has improved in every efficient manner than IPv4. Mobile IPv6 allows mobile devices to be connected to the correspondent node even when it moves to the other network. The current location of the mobile node is informed to the home agent and correspondent node through binding update schemes. With the aim of experiencing this improvised network and to perform IPv6 related research, the binding update schemes of mobile IPv6 are explored in this paper. The paper emphasises the number of messages exchanged between the communicants during the location update of mobile devices in the various binding update schemes in mobile IPv6. In addition, it discusses the attacks that are involved in the binding update messages of the existing methods. Finally, the paper focuses on the comparative analysis of the various binding update schemes based on the number of messages communicated between nodes.

Keywords: mobile IPv6; home agent; binding update; route optimisation; correspondent node.

Reference to this paper should be made as follows: Srikanth, L. and Senthilkumar, M. (2023) 'Investigation of binding update schemes in next generation internet protocol mobility', *Int. J. Advanced Intelligence Paradigms*, Vol. 24, Nos. 1/2, pp.190–205.

Biographical notes: Lingam Srikanth is pursuing his MTech in Computer Science and Engineering from Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India.

Mathi Senthilkumar received his PhD and ME in Computer Science and Engineering from Anna University, Chennai, India. He received his BE in Computer Science and Engineering from Bharathiar University, Coimbatore, India. Currently, he is working as an Assistant Professor (Selection Grade), under Computer Science and Engineering Department, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India. He is a member of IETE. He has published more than 30 technical papers in national, international conferences and international journals. His research interest includes: information security, mobile IP, and formal languages and automata.

1 Introduction

The invention of the internet is revolutionary in the world of computers and communications. Since then it has been widely used as a broadcasting mechanism, source of information dissemination, collaboration medium, and computer communications irrespective of the location. Then, it has been under the research and development phases in order to gain efficiency and become better than earlier. The National Science Foundation started an idea to build a contemporary backbone network, an interconnected network, running transmission control protocol or otherwise called as internet protocol (TCP/IP) to connect supercomputer hubs and provincial network (Botta et al., 2016). Now, the terms such as *http://www.example.com* are being used by almost every human of the world (Saha et al., 2004).

The constant rise in the growth of internet population (Ziegler and Ladid, 2016) imposes many issues to the innovators and engineers to be addressed. A node/computer system must be named based on some standards to become visible among the internet population. The IP is an international standard set for the communication among the nodes present on the internet and makes the nodes to be reachable from every other node present in the network. In a connected system of nodes, if any node sends data (e.g., an e-mail message) then the message gets split into little pieces of data called packets and reaches the gateway of the network. These little chunks might contain both the sender's and receiver's address. The gateway upon receiving the message reads the destination address in the packet and forwards it to the adjacent gateway which in turns reads the destination address and so forth goes across the internet till one realises the packet (Vinnarasi and Chandrasekar, 2019). This is done using TCP which when used in the internet applications is called IP (Zhang et al., 2016).

When the first IP was proposed, the addresses assigned to the nodes were called IPv4 addresses. This address is 32-bits long which could cover around 4.3 billion addresses (2^{32} addresses). The address allocation in IPv4 is based on the network class it belongs to. Since addresses got depleted gradually, classless interdomain routing came into existence for the network communications (Carlos et al., 2009).

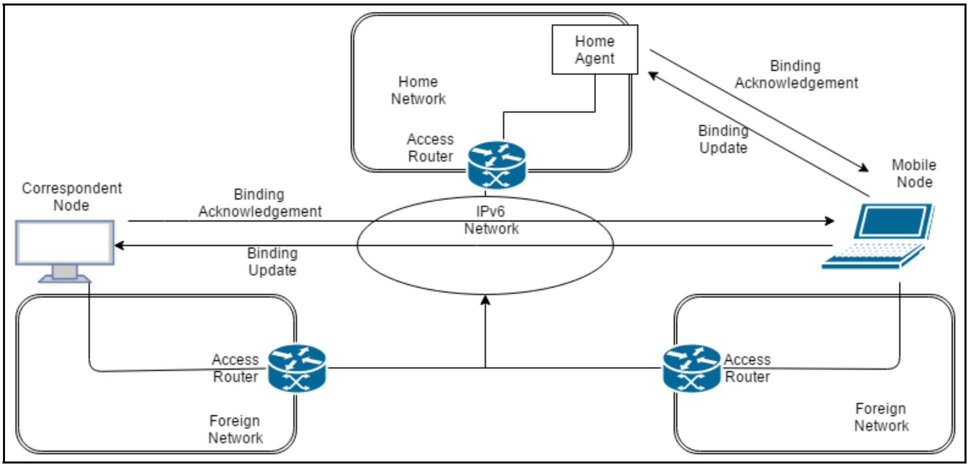
The PCs, smartphones, gaming systems and everything else connecting to the internet have been assigned addresses from almost all the available addresses of IPv4 address pool (Cui et al., 2015). Consequently, the IETF had to develop a newer version of IP, IPv6 to rescue from the situation of IPv4 address exhaustion. IPv6 follows 128-bit addressing and have the capacity of assigning 2^{128} addresses (Soininen and Korhonen, 2015) until it becomes exhausted. This amount is 340 times 10 to the power of 36 possible IP addresses.

Expanding the pool of IP addresses might yield other advantages as well. Due to the scarcity of IPv4 addresses, much of the present day internet relies on network address translation (Francis, 2015). But, with IPv6 addressing (Liu et al., 2015; Waddington and Chang, 2002) almost every device can connect to the internet. In addition, the security features of the IPv6 itself are much efficient and accurate than IPv4 (Akilandeswari et al., 2017). Encryption techniques are used to ensure the integrity and authenticity of each IPv6 packet and the procedures targeted at thwarting packet spoofing are also improving. The IPv6 is much better than IPv4 in checking if the internet traffic is forwarded to the right direction and the packets are delivered to the accurate destination without getting intercepted (Henry et al., 2016; Zhu et al., 2008; Iapichino and Bonnet, 2009). It uses a

128-bit addressing scheme, out of which, 64 bits are assigned to the network identifier and the rest 64 bits are assigned to the host identifier (Sahadevaiah et al., 2015; Grgić et al., 2016).

The written form of an IPv6 address is *aaaa:aaaa: aaaa:aaaa:aaaa:aaaa:aaaa:aaaa*, where '*a*' is a hexadecimal representation of a number, expressed in 4 bits. The leading zeros of each section can be omitted (Amutha et al., 2016). The lifetime of the IPv6 address is categorised into two; valid and preferred. The valid lifetime is more than the preferred lifetime. Once the preferred address is expired, it cannot be considered as a valid source IP. And, if valid lifetime gets expired; the address is not acknowledged as legal destination IP for any incoming packets or used as a source IP address. IPv4 uses subnet mask for identifying the network id from the host id. The IPv6 does not use any mask for identification. For this, IPv6 subnet prefix (Weniger and Zitterbart, 2002; Troan and Droms, 2003) is introduced to indicate the number of bits comprising network subnet prefix (Cooper and Yen, 2005).

Figure 1 Mobile IPv6 networking environment (see online version for colours)



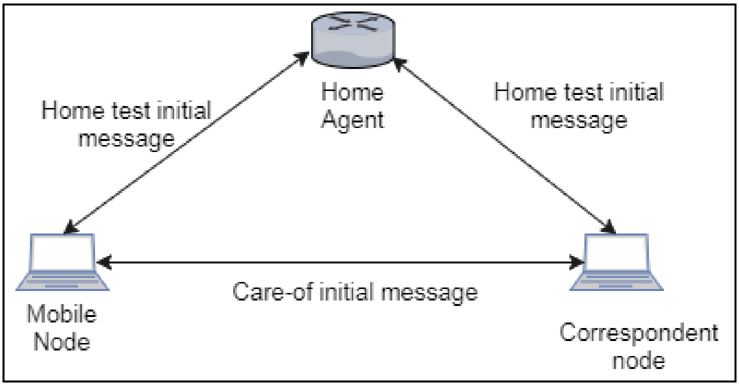
Home agent (HA) allocates its home network router as an authority of itself when a mobile node (MN) travels from home network to an external link (Gohar et al., 2015). The HA provides services to all the nearby MNs that are connected to it and sends address information to all the MNs (Muraleedharan and Mathi, 2017). Hence, it needs to know the location of all the MNs wherever they move and updates its binding cache about the location of the MNs. It includes two types of messages, one is router broadcast (sending periodically on the link by the IPv6 router to MNs) and the second message is router request (sending request packet directly to the router from MN) (Loo et al., 2016). The MN sends the information about its care-of address regardless of how far it is so that the HA can get in touch with the MN (Khatri and Senthilkumar, 2017). When the first packet arrives at the MN through the tunnel on the internet (Shahriar et al., 2010; Al-asadi et al., 2017), and the MN recognises that the packet is forwarded by the HA, it sends binding information to the communicant. The HA generates a record in its binding memory, including the care-of address and the previous address of MN when it receives the binding update (Parenti et al., 2002; Stewart et al., 2004; Lee and Kim, 2017; Atzori et al., 2010).

The paper is organised as follows. In Section 2, the works related to binding update schemes in an IPv6 mobility environment are discussed. In Section 3, a comparative study of the binding update schemes based on the number of messages exchanged between the nodes for communication is investigated to analyse the efficiency among them. Section 4 concludes the paper.

2 Material and method

Return routability (RR) protocol uses an infrastructure-less solution to achieve route optimisation and that enables to avoid triangle routing problem (Ren et al., 2006; Fernandez et al., 2016). Here, the MN requests a correspondent node (CN) to examine the ownership of its care-of-address (CoA) and home-of-address (HoA) as shown in Figure 2. In order to achieve it, two independent messages: the Home address Test initial and CoA Test Init are sent at the same time. It forms the return routability procedure and requires little processing at the CN. Simultaneously, HoT and CoT can be returned rapidly. However, this procedure lacks security and requires additional message computations (Modares et al., 2014; Kim et al., 2017).

Figure 2 Return routability message exchange



The crypto-based identifiers method (CBID) is a 128-bit non-routable identifier derived from hashing a public key and a 64-bit imprint (Koo and Lee, 2007). Using a modified version of the CBID technology, mutual authentication between the nodes can be provided by the cryptographically generated address (Modares et al., 2012; Qadir et al., 2015). It is not necessary for the MN to create a signature whenever it is gaining a fresh CoA. The CBID uses one message for digital signature and two messages for exponential calculation during the calculation of MN and CN. It has the following rounds of messages: pre-binding update (PBU) from the MN to the CN and pre-binding acknowledgement (PBA) from the CN to the MN, both are through the HA; pre-binding test (PBT) is directly from the CN to the MN (Montenegro and Castelluccia, 2004).

The MN sends a PBU message to the CN via its HA when it moves to a foreign network for the first time. CN computes two keygen tokens after receiving the PBU message and sends them to the MN in PBA and PBT messages. The MN combines the received tokens such that the result of it can be used to authenticate the BU messages.

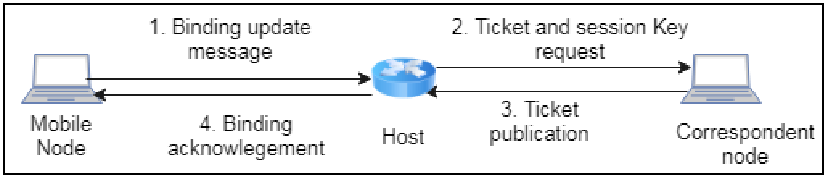
When the CN receives the BU message, the validity of the CBID is verified. Although messaging count by the HA can be taken as negligible in nature; the number of messages by the MN is more in number.

Child-proof authentication for MIPv6 (CAM) makes use of only one message; therefore mutual authentication cannot be attained because it requires at least two messages (Fathi et al., 2008). Moreover, MN faces more computational load because MN is required by each and every BU message to generate a signature. Subsequently, the CN carries out the signature verification. In elliptic curve based binding update (ECBU), the shared master secret is established by the MN and CN by using the elliptic curve which is based on the Diffie-Hellman key agreement protocol. It is followed by the derivation of the binding management key from the shared master secret. The key conformity protocol data is conceded out in the RR and BU messages. Simultaneously, HoT and CoT messages are sent. In order to acquire the CN's public key, the MN sends a home address test initial to the CN (via the HA). It uses one message for the signature calculation at the CN and MN.

Elliptic curve crypto-based identifiers (ECBID) method is based on the elliptical curve cryptography (ECC) which is a public key encryption technique. ECC uses the properties of the elliptic curve equation to generate faster, smaller, and more efficient cryptographic keys (Biehl et al., 2000). This scheme comprises of six rounds of messages and the cost of using IPSec is not enclosed within the protocol. ECBID uses one message for digital signature and two messages for exponential calculation by the CN. Further, it takes one message for digital signature, two messages for exponential calculation and one message for MAC by the HA (Yu et al., 2016).

The communication and computation cost is less in ticket-based binding update (TBU) protocol (Lee and Kim, 2017). Hence, in comparison to the above discussed BU protocols, TBU is more effective. There are four rounds of messages that are used in this method as given in Figure 3. One message is used for MAC alone during the calculation of CN and MN. It performs better in terms of the number of messages exchanged between the MN and CN. However, each message transfer takes a little amount of time which sums up to a delay in receiving a message.

Figure 3 Ticket binding update mechanism (see online version for colours)


1. Binding update message
2. Ticket and session Key request
Mobile Node
4. Binding acknowlegement
Host
3. Ticket publication
Correspondent node

The proactive handover technique is discussed in Dutta et al. (2007). The current location of MN is determined in addition to the information received from the neighbouring nodes. The packet loss and delay is less in the location assisted handover method (Koo et al., 2006). A mobile assisted authorisation, authentication and handover mechanisms provide smooth and secure mobility to the MNs. The process of pre-configuration and pre-authentication offers timely and seamless handover. The resource utilisation can be improved by implementing the pre-authentication over the intersecting area of the various networks. Although it provides optimised handover, it suffers from the additional signalling and tunnelling overhead.

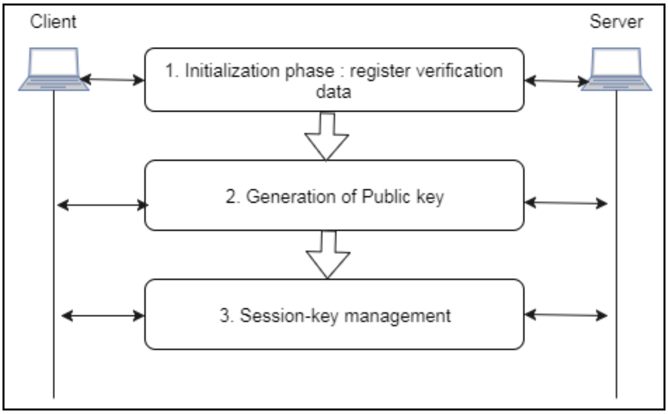
The context-aware ticket-based binding update authentication (caTBUA) protocol relies on the context information to validate CoA. It balances the trade-off between efficiency and security (You et al., 2010). Existing BU authentication protocols either bypasses the validation process of CoA or CN performs its own validation (Bouaziz and Rachedi, 2016; Goswami and Das, 2016; Kumar and Krishna, 2018).

The modified leakage resilient-authenticated key establishment protocol is discussed in Fathi et al. (2008) to address the authentication authorisation and accounting problems of the mobility networks. Figure 4 presents the working of this protocol that follows the client-server model based on RSA public-key cryptography. The verification data is registered to the server by the client. Further, the server's key generation is verified by the challenge-response protocol. After the client and server are authenticated each other, the shared session key is generated. The transmission and encryption delays are high in this method. However, higher performance can be attained with a compromise on the complexity overhead.

The batch binding update mechanism incorporates elliptic curve cryptography that benefits from the reduction of the computational overhead. The address ownership of the MN is taken care by the multi-key cryptographically generated address. The various BU messages can be verified by the CN whose authenticity can be identified as well (Yeh et al., 2013).

The detailed analysis of the IPsec protocol for real-time communication is discussed in Perlman and Kaufman (2001). Internet key exchange consists of two sections. The exchange in the first section is dependent on the identities and secret shared keys of the MNs, HA and CN. The second section is reliant on the establishment of the session key of the first section. Moreover, the first section can be followed by multiple second sections. Its performance gets affected due to the expensive nature of the first section key establishment.

Figure 4 Resilient-authenticated key establishment protocol

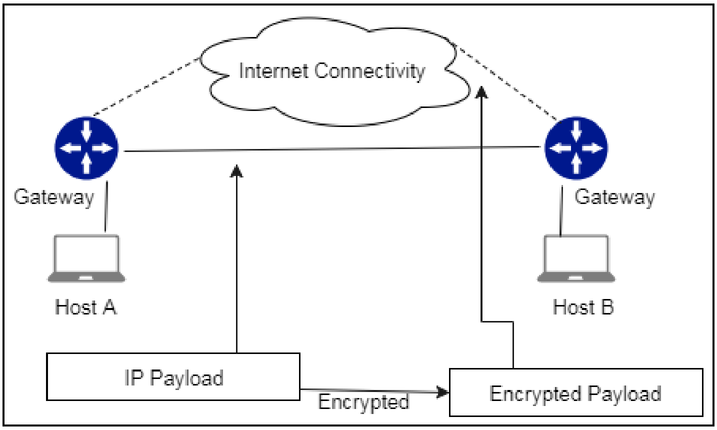

Client
Server
1. Initialization phase : register verification data
2. Generation of Public key
3. Session-key management

The major concerns related to security in wireless sensor networks are presented in Kavitha and Sridharan (2010). The attacks are classified as per the various characteristics such as active and passive attacks, internal and external attacks, host domain and protocol-based attacks. The jamming attack comes under the category of denial of service and can be deceptive, reactive and random in nature. The solution discussed for the flooding attack is solving the puzzle by the client to address its commitment towards the session. The authentication of the packets is required to prevent the de-synchronisation; hence add to the delay overhead. The private key encryption techniques add to the overall computation cost. Although, symmetric key crypto-system is faster but is not scalable. Furthermore, it summarises the deployment works in security susceptible perspective and provides details on the insider attacks (Amin and Biswas, 2016).

Encapsulated security payload and authentication header provide the necessary security measures in IP security as shown in Figure 5. It can work in transport as well as tunnelling mode. The confidentiality of the data messages and the authentication of the source are ensured by the encapsulated security payload. The intrusion detection system collects the network related information followed by the analysis of the gathered details and finally takes preventive actions if any security threat is encountered (Žagar et al., 2007). The body area network based on mobile health is discussed in Varga et al. (2014). The mobile health monitoring requires secure BU and BA to work efficiently in real-time situations.

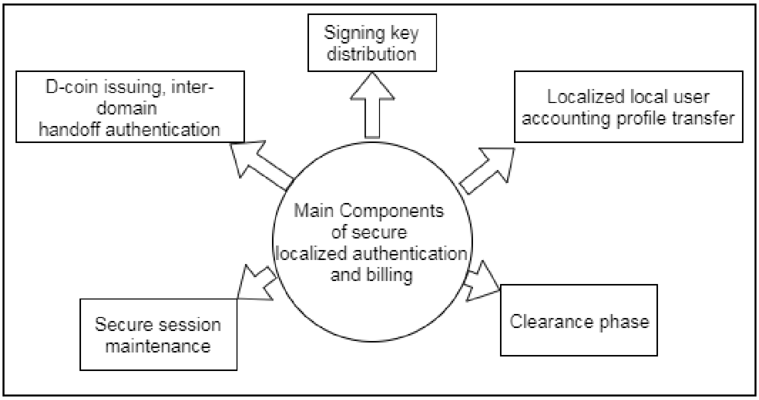
Moreover, the stealthy denial-of-service attack impacts the resource utilisation in addition to the denial-of-service (Manohar and Baburaj, 2016). A new attack scheme named slowly increasing and decreasing under constraint denial of service attack is proposed to control the various network vulnerabilities. There are many factors that govern over the selection of the encryption algorithm and session key management. The maintenance of the key secrecy is vital to determine the strength of the end-to-end secured communication among the entities over the mobile network. The detail description of the security aspects related to the authorisation and session key management is discussed in Amin and Biswas (2016).

Figure 5 IP security flow (see online version for colours)



The mobile users send the authentication request via mesh access points or gateway to a centralised entity for the authentication. The signalling path is longer and can face propagation delay; hence cannot perform efficiently in the real-time applications. There are many fast authentication mechanisms such as pre-key-distributions, enhanced inter-access point protocol and predictive authentication. The requirement of the bilateral service level agreement makes most of the exiting fast authentications ineffectual for the inter-domain handoff. It experiences scalability problems.

Figure 6 Components of localised authentication and billing


Signing key distribution
D-coin issuing, inter-domain handoff authentication
Localized local user accounting profile transfer
Main Components of secure localized authentication and billing
Secure session maintenance
Clearance phase

The short digital signature method is used in secure localised authentication and billing technique (Zhu et al., 2008). The digital signature overhead is reduced in this and discussed as an efficient approach in the crypto-systems. It has a length of 160 bits and is small in comparison to the RSA encryption which has 1,024-bit length. This security technique is distributed in nature and comprises five components as given in Figure 6. It is based on the traditional public key infrastructure.

The accounting profile of local users is generated and maintained at the mesh access point to track the spending time of the mobile users. Any updation on the information requires a secure protocol for the accounting. Consequently, it adds to the signalling and maintenance overhead. The clearance phase is event-driven in which each and every D-coin is considered to be an event. The submission of the D-coins to the roaming broker is done once the minimum time frame or the size is satisfied. Subsequently, the procedure of the summative signature after verification of the collected D-coins reduces the verification and transmission cost.

In the nested mobile network, a mobile router performs the role of a gateway. In case of the movement in the network, mobile router acquires a CoA with respect to the visited link and registers the same to the foreign network. Consequently, a tunnel that is bidirectional in nature is constructed to enable the flow of packets between the CN and the MNs. The further rise in the network nesting level leads to more tunnelling. Therefore, it results in more hand-off delay and service disruption (Bhattacharya et al., 2017). The route optimisation is focussed on the access router option scheme. The information related to the BUs is gathered by the HAs from the upper-level mobile routers in the network. But, it faces communication cost penalty in case of the more nested network. The hand-off mechanism in this scheme is not permanent in nature; as a result, it faces disruption in the communication. Therefore, it can be concluded that the scheme is not efficient in highly dynamic situations.

The quality of experience and service agreement level in case of the handovers is discussed in Piri et al. (2015). The reliable metric measurement in real time environment is difficult in nature. The quality-based mobility scheme facilitates the MN to identify the appropriate base station with respect to its service requirements (Vidhya and Mathi, 2018). The quality metric results are stored in the database of the information service that permits the end system to find the suitable near-by networks. An adequate range of information can be obtained by using any single query to decide the handover and binding targets in the heterogeneous networks. This scheme requires a satisfactory amount of resources in order to improve the overall performance of the network.

In order to overcome the complexity of the traditional public key cryptography, the identity-based approach is used. It follows a new modified scheme for the generation of the private key (He and Zeadally, 2015). The three main components are the controller, server and mobile users. The private key of the controller is derived by performing the hash function on the identity of the controller and its private key at the server end.

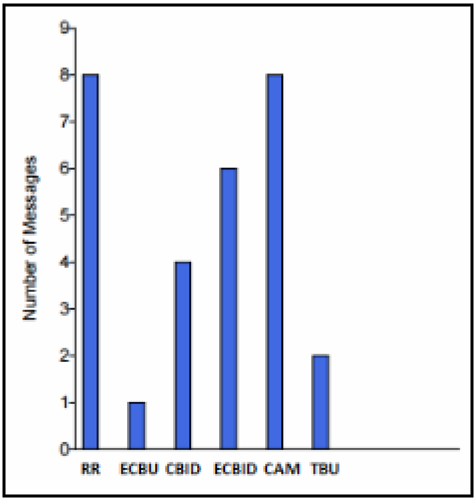
To achieve smooth BUs of the MNs in addition to the minimal packet loss, predictive handover is discussed in Yousaf et al. (2016). There is a bidirectional tunnel between the MN’s new IP subnet and the previous one. When the handover occurs, all the packets pass via the tunnel to the new CoA of the MN. This scheme experiences high tunnelling overhead in case of the rise of the MNs and the network traffic. Additionally, the packet size also increases and over-consumption of the resources. It also faces processing load and congestion issues. Moreover, the performance depends on the mobility speed of the MNs and the time constraints of the handover.

The method discussed in Qiu et al. (2004) states that MNs are provided proxy security by the HAs and authentication is the function of the HA’s certificate (Douligeris and Mitrokotsa, 2004). Session key management is also deployed at the HA end in order to provide the balance between the security measures and the communication speed. Machine learning approach for the decision making of efficient energy consumption for IoT sensors is presented in Sharad et al. (2015) and Kumar and Krishna (2018). XXTEA is the encryption module used for the security purpose because it utilises less resource. The reliability and correctness of data can be attained by the use of the security primitives in the distributed environment.

3 Results and discussion

Based on the number of messages exchanged between the nodes for communication, the efficiency of the scheme is measured. The BU schemes considered for the comparison are RR, ECBU, CAM, CBID, ECBID and TBU. Here, the CAM scheme uses merely single message; therefore communal endorsement is not possible because at least two messages are required to achieve mutual authentication. Figure 7 shows the comparison between the message count and the different BU schemes based on the total messages communicated in all the schemes. The RR and CAM have the highest messaging count whereas ECBU has the least number of messages exchanged between the nodes. The CBID scheme has less number of message count than ECBID but more than the TBU scheme.

Figure 7 Total number of message exchanges (see online version for colours)



Out of the number of messages used for communication, few are used for calculating parameters such as digital signature, exponential calculation, symmetric key and MAC by the MN, CN, and HA. The comparison between the message count and the different BU methods based on the number of messages transmitted by the MNs is presented in Figure 8. RR and CAM have a similar number of messages for the MAC. CBID and TBU schemes have less number of messages exchanged in comparison to CAM and RR. In the case of a digital signature, the similar count of messages is transmitted by the MN in ECBU and CBID schemes. Furthermore, CBID presents the highest number of messages for the exponential calculation.

Figure 8 Number of message exchanges by MN (see online version for colours)

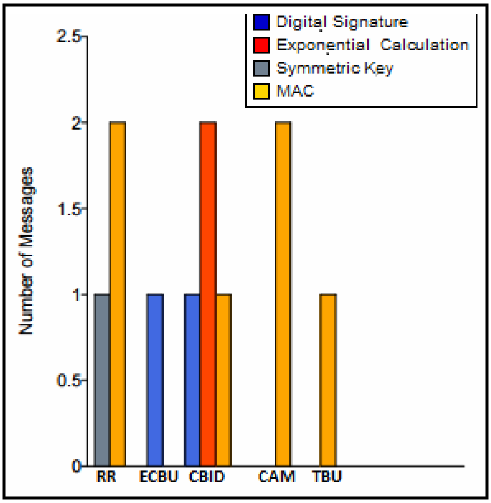


Figure 9 shows the comparison between the message count and the different BU schemes based on the number of messages transmitted by the CNs. CAM has the most number of messages exchanged followed by the RR for the MAC whereas the other schemes have an almost similar number of messages count. In case of digital signature as well, CAM has the highest number of messages exchanged whereas ECBU, CBID and ECBID have reduced and comparable messaging count. However, when the exponential calculation is considered, the number of messages transmitted by the CN is almost similar in CBID, ECBID and CAM schemes.

Figure 9 Number of message exchanges by CN (see online version for colours)

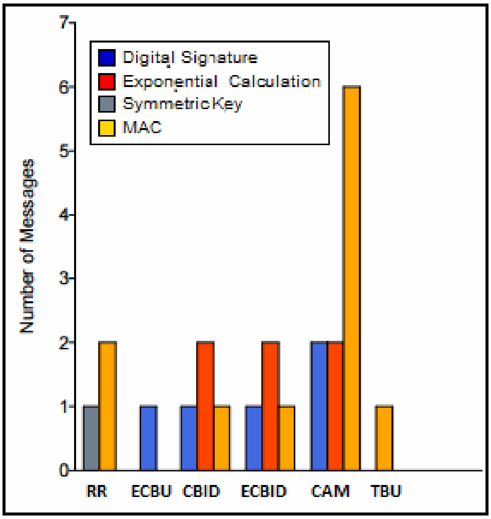


Figure 10 shows the relationship among the message count and the various BU schemes based on the number of messages transmitted by the home agents in the various schemes. TBU exchanges the most number of messages in the case of MAC in comparison to the other schemes. The number of messages exchanged for exponential calculation is almost similar for ECBID and CAM. For the digital signature, CAM has the number of messages transmitted by the HAs as compared to ECBID. The RR and CAM consume more signalling overhead as shown in Figure 11. The ECBID has less overhead in comparison to the CAM but more than the CBID. TBU and ECBU schemes present less signalling overhead and are more efficient than the other discussed schemes.

From the comparative report on the exchange of the messages of the various BU schemes, the current location of the MN is notified to the HA and CN via BU messages. The number of messages exchanged during the BU impacts the delay and the efficiency of the binding schemes. Hence, the exchange of messages needs to be processed in such a manner that it results in faster networking. The TBU scheme has low messaging overhead but CAM and RR schemes have high signalling overhead.

Figure 10 Number of message exchanges by HA in BU schemes (see online version for colours)

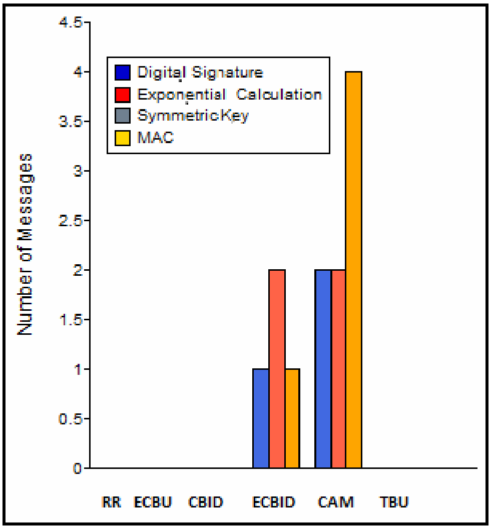
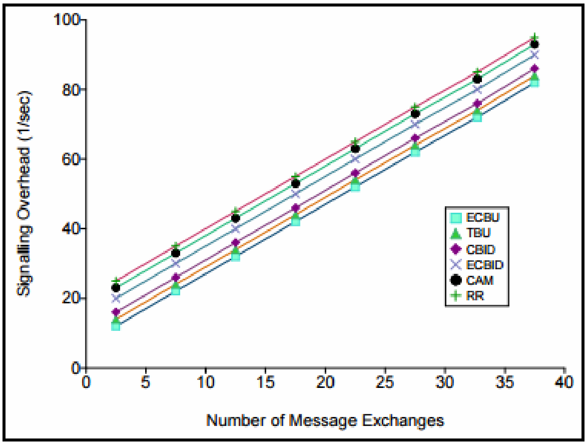


Figure 11 Signalling overhead vs. number of message exchanges (see online version for colours)



4 Conclusions

The main motive of the present paper is to do a comparative investigation of various mobile IPv6 binding update schemes and understand their efficiency with respect to the number of messages exchanged between MN and HA. There are many binding update schemes used between the MN and the HA. To understand the working and the way of exchanges, a comparative analysis is done in the paper among the binding update schemes. The paper discusses the number of messaging count during the binding of MNs in MIPv6. The BU is used to notify HA and CN regarding the current location of the MN for exchanging messages. The delay and the number of messages exchanged play a vital role in the efficiency of the binding schemes being used. The messages are meant to be processed rapidly in order to achieve a faster and responsive network. The comparative study of various BU schemes is presented in this paper. It is identified that RR and CAM schemes have the most number of messages exchanged whereas TBU scheme has less messaging overhead.

References

Akilandeswari, D., Rabara, S.A. and Bai, T.D. (2017) 'Enhanced security architecture for IPv6 transition', *Proc. WCCCT*, pp.61–64.

Al-asadi, T.A., Obaid, A.J., Hidayat, R. and Ramli, A.A. (2017) 'A survey on web mining techniques and applications', *International Journal on Advanced Science, Engineering and Information Technology*, Vol. 7, No. 4, pp.1178–1184.

Amin, R. and Biswas, G.P. (2016) 'A secure lightweight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks', *Ad Hoc Networks*, Vol. 36, pp.58–80.

Amutha, J., Rabara, S.A. and Sundaram, R.M. (2016) 'An integrated secure architecture for IPv4/IPv6 address translation between IPv4 and IPv6 networks', *Proc. Second International Conference on Computer and Communication Technologies*, pp.669–679.

Atzori, L., Iera, A. and Morabito, G. (2010) 'The internet of things: a survey', *Computer Networks*, Vol. 54, No. 15, pp.2787–2805.

Bhattacharya, A., Das, S., Gayen, A. and Chakraborty, N. (2017) 'HAP: hierarchical attachment process for mobile nodes in nested network mobility', *Proc. IEEE TENSYMP'17*, pp.1–4.

Biehl, I., Meyer, B. and Müller, V. (2000) 'Differential fault attacks on elliptic curve cryptosystems', *Proc. Advances in Cryptology – CRYPTO 2000*, pp.131–146, Springer Berlin/Heidelberg.

Botta, A., De Donato, W., Persico, V. and Pescape, A. (2016) 'Integration of cloud computing and internet of things: a survey', *Future Generation Computer Systems*, Vol. 56, pp.684–700.

Bouaziz, M. and Rachedi, A. (2016) 'A survey on mobility management protocols in wireless sensor networks based on 6LoWPAN technology', *Computer Communications*, Vol. 74, pp.3–15.

Carlos, C.E.E., Joshi, J.B. and Tuladhar, S.R. (2009) 'IPv6 security challenges', *Computer*, Vol. 42, No. 2, pp.36–42.

Cooper, M. and Yen, D.C. (2005) 'IPv6: business applications and implementation concerns', *Computer Standards & Interfaces*, Vol. 28, No. 1, pp.27–41.

Cui, Y., Chen, Y., Liu, J., Lee, Y.L., Wu, J. and Wang, X. (2015) 'State management in IPv4 to IPv6 transition', *IEEE Network*, November, Vol. 29, No. 6, pp.48–53.

Douligeris, C. and Mitrokotsa, A. (2004) 'DDoS attacks and defense mechanisms: classification and state-of-the-art', *Computer Networks*, Vol. 44, No. 5, pp.643–666.

Dutta, A., Chakravarty, S., Taniuchi, K., Fajardo, V., Ohba, Y., Famolari, D. and Schulzrinne, H. (2007) 'An experimental study of location assisted proactive handover', *Proc. GLOBECOM'07*, pp.2037–2042.

Fathi, H., Shin, S., Kobara, K., Chakraborty, S.S., Imai, H. and Prasad, R. (2008) 'LR-AKE-based AAA for network mobility (NEMO) over wireless links', *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 9, pp.1545–1557.

Fernandez, P.J., Santa, J., Bernal, F. and Skarmeta, A.F. (2016) 'Securing vehicular IPv6 communications', *IEEE Transactions on Dependable and Secure Computing*, Vol. 13, No. 1, pp.46–58.

Francis, P. (2015) 'Network address translation (NAT)', *ACM SIGCOMM Computer Communication Review*, Vol. 45, No. 2, p.50.

Gohar, M., Choi, S.I. and Koh, S.J. (2015) 'Mobility support for proxy mobile IPv6 in TRILL-based mobile networks', *Proc. ICUFN*, pp.677–681.

Goswami, S. and Das, C.B. (2016) 'A survey on various route optimization techniques in network mobility', *Journal of Uncertain Systems*, Vol. 10, No. 2, pp.91–107.

Grgić, K., Čik, V.K. and Radivojević, V.M. (2016) 'Security aspects of IPv6-based wireless sensor networks', *International Journal of Electrical and Computer Engineering Systems*, Vol. 7, No. 1, pp.9–37.

He, D. and Zeadally, S. (2015) 'Authentication protocol for an ambient assisted living system', *IEEE Comms. Magazine*, Vol. 53, No. 1, pp.71–77.

Henry, S.S., Kumar, B.V., Kumar, V.S. and Singh, G. (2016) 'Protocol verification of translation in mobile internet protocol version 4 and 6', *Journal of Computers*, Vol. 11, No. 2, pp.149–158.

Iapichino, G. and Bonnet, C. (2009) 'Host identity protocol and proxy mobile IPv6: a secure global and localized mobility management scheme for multihomed mobile nodes', *Proc. GLOBECOM'09*, pp.1–6.

Kavitha, T. and Sridharan, D. (2010) 'Security vulnerabilities in wireless sensor networks: a survey', *Journal of Information Assurance and Security*, Vol. 5, No. 1, pp.31–44.

Khatri, A. and Senthilkumar, M. (2017) 'Investigation of home agent load balancing, failure detection and recovery in IPv6 network-based mobility', *International Journal on Advanced Science, Engineering and Information Technology*, Vol. 7, No. 2, pp.632–641.

Kim, H.S., Kim, H., Paek, J. and Bahk, S. (2017) 'Load balancing under heavy traffic in RPL routing protocol for low power and lossy networks', *IEEE Trans. on Mobile Computing*, Vol. 16, No. 4, pp.964–979.

Koo, J.D. and Lee, D.C. (2007) 'Extended ticket-based binding update (ETBU) protocol for mobile IPv6 (MIPv6) networks', *IEICE Transactions on Communications*, Vol. 90, No. 4, pp.777–787.

Koo, J.D., Koo, J. and Lee, D.C. (2006) 'A new authentication scheme of binding update protocol on handover in mobile IPv6 networks', *Proc. EUC Workshops'06*, pp.972–978.

Kumar, T.S.P. and Krishna, P.V. (2018) 'Power modelling of sensors for IoT using reinforcement learning', *International Journal of Advanced Intelligence Paradigms*, Vol. 10, Nos. 1–2, pp.3–22.

Lee, D.C. and Kim, K.J. (2017) 'Improved authentication of binding update protocol in mobile IPv6 networks', *Wireless Personal Communications*, Vol. 94, No. 3, pp.351–367.

Liu, Y., Ren, G., Wu, J., Zhang, S., He, L. and Jia, Y. (2015) 'Building an IPv6 address generation and traceback system with NIDTGA in Address Driven Network', *Science China Infn. Sciences*, Vol. 58, No. 12, pp.1–4.

Loo, J., Mauri, J.L. and Ortiz, J.H. (Eds.) (2016) *Mobile Ad Hoc Networks: Current Status and Future Trends*, CRC Press, ISBN 9781439856505.

Manohar, R.P. and Baburaj, E. (2016) 'Detection of stealthy denial of service (S-DoS) attacks in wireless sensor networks', *International Journal of Computer Science and Information Security*, Vol. 14, No. 3, p.343.

Modares, H., Moravejosharieh, A., Keshavarz, H. and Salleh, R. (2012) 'Protection of binding update message in Mobile IPv6', *Proc. Computer Modeling and Simulation (EMS) – UKSim/AMSS European Symposium*, pp.444–447.

Modares, H., Moravejosharieh, A., Lloret, J. and Salleh, R. (2014) 'A survey of secure protocols in mobile IPv6', *Journal of Network and Computer Applications*, Vol. 39, pp.351–368.

Montenegro, G. and Castelluccia, C. (2004) 'Crypto-based identifiers (CBIDs): concepts and applications', *ACM Transactions on Information and System Security*, Vol. 7, No. 1, pp.97–127.

Muraleedharan, P. and Mathi, S. (2017) 'An investigational testbed design for next generation internet protocol mobility', *2017 International Conference on Computer Communication and Informatics (ICCCI)*, IEEE.

Parenti, E., Knipp, E., Chen, N., Saylor, B. and Browne, S. (2002) *Configuring IPv6 with Cisco IOS*, Syngress Publishing, ISBN:1928994849.

Perlman, R. and Kaufman, C. (2001) 'Analysis of the IPsec key exchange standard', *Proc. WET ICE'01*, pp.150–156.

Piri, E., Varela, M. and Prokkola, J. (2015) 'A network information service for quality-driven mobility', *Proc. CCNC'15*, pp.412–417.

Qadir, S., Siddiqi, M.U. and Al-Khateeb, W.F. (2015) 'An investigation of the Merkle signature scheme for cryptographically generated address signatures in mobile IPv6', *International Journal of Network Security*, Vol. 17, No. 3, pp.311–321.

Qiu, Y., Zhou, J. and Bao, F. (2004) 'Protecting all traffic channels in mobile IPv6 network', *Proc. IEEE WCNC'04*, Vol. 1, pp.160–165.

Ren, K., Lou, W., Zeng, K., Bao, F., Zhou, J. and Deng, R.H. (2006) 'Routing optimization security in mobile IPv6', *Computer Networks*, Vol. 50, No. 13, pp.2401–2419.

Saha, D., Mukherjee, A., Misra, I.S. and Chakraborty, M. (2004) 'Mobility support in IP: a survey of related protocols', *IEEE Network*, Vol. 18, No. 3, pp.4–40.

Sahadevaiah, K., Ramakrishnaiah, N. and Reddy, P.P. (2015) 'IPv6 address auto-configuration protocol for mobile ad hoc networks', *Procedia Computer Science*, Vol. 57, pp.907–914.

Shahriar, A.Z., Atiquzzaman, M. and Ivancic, W. (2010) 'Route optimization in network mobility: solutions, classification, comparison, and future research directions', *IEEE Communications Surveys & Tutorials*, Vol. 12, No. 1, pp.24–38.

Sharad, S., Sivakumar, P.B. and Narayanan, V.A. (2015) 'A novel IoT-based energy management system for large scale data centers', *Proc. ACM Sixth International Conference on Future Energy Systems*, pp.313–318.

Soininen, J. and Korhonen, J. (2015) 'Survey of IPv6 Support in 3GPP specifications and implementations', *IEEE Communications Surveys & Tutorials*, Vol. 17, No. 3, pp.1634–1648.

Stewart, L., Banh, M. and Armitage, G. (2004) *Implementing an IPv6 and Mobile IPv6 testbed using FreeBSD 4.9 and KAME*, CAIA tech. rep., March.

Troan, O. and Droms, R.A. (2003) *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*, RFC 3633.

Varga, N., Bokor, L. and Takács, A. (2014) 'Context-aware IPv6 flow mobility for multi-sensor based mobile patient monitoring and tele-consultation', *Procedia Computer Science*, Vol. 40, pp.222–229.

Vidhya, S.S. and Mathi, S. (2018) 'Investigation of next generation internet protocol mobility-assisted solutions for low power and lossy networks', *Procedia Computer Science*, Vol. 143, pp.349–359.

Vinnarasi, F.S.F. and Chandrasekar, A. (2019) 'VANET routing protocol with traffic aware approach', *International Journal of Advanced Intelligence Paradigms*, Vol. 12, Nos. 1–2, pp.3–13.

Waddington, D.G. and Chang, F. (2002) 'Realizing the transition to IPv6', *IEEE Communications Magazine*, Vol. 40, No. 6, pp.138–148.

Weniger, K. and Zitterbart, M. (2002) 'IPv6 autoconfiguration in large scale mobile ad-hoc networks', *Proc. European Wireless*, Vol. 1, pp.142–148.

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*, Vol. 36, No. 1, pp.284–292.

You, I., Lee, J.H. and Kim, B. (2010) 'caTBUA: context-aware ticket-based binding update authentication protocol for trust-enabled mobile networks', *International Journal of Communication Systems*, Vol. 23, No. 11, pp.1382–1404.

Yousaf, F.Z., Wietfeld, C. and Mahmud, S.A. (2016) 'Optimizing tunnel management in predictive handover protocols', *Computer Networks*, Vol. 104, pp.198–212.

Yu, F., Zhang, H., Zhao, B., Wang, J., Zhang, L., Yan, F. and Chen, Z. (2016) 'A formal analysis of Trusted Platform Module 2.0 hash-based message authentication code authorization under digital rights management scenario', *Security and Communication Networks*, Vol. 9, No. 15, pp.2802–2815.

Žagar, D., Grgić, K. and Rimac-Drlje, S. (2007) 'Security aspects in IPv6 networks-implementation and testing', *Computers & Electrical Engineering*, Vol. 33, No. 5, pp.425–437.

Zhang, Y., Afanasyev, A., Burke, J. and Zhang, L. (2016) 'A survey of mobility support in named data networking', *Proc. INFOCOM WKSHPS'16*, pp.83–88.

Zhu, H., Lin, X., Lu, R. and Ho, P.H. (2008) 'SLAB: a secure localized authentication and billing scheme for wireless mesh networks', *IEEE Trans. on Wireless Communications*, Vol. 7, No. 10, pp.3858–3868.

Ziegler, S. and Ladid, L. (2016) 'Towards a global IPv6 addressing model for the internet of things', *Proc. WAINA'16*, pp.622–627.