Enhanced Authentication Scheme for Proxy Mobile IPv6

Kanwal Imran, Saeed Mahfooz, Azhar Rauf, Shah Khusro

Department of Computer Science, University of Peshawar, Peshawar 25000, Pakistan.
kanwalim@upesh.edu.pk

Abstract: Mobility management protocols play a vital role during mobile node transmission. That's why IETF NETLMM working group has recently presented a new approach, i-e, Proxy Mobile IPv6 (PMIPv6) which is a network-based mobility management protocol. But, PMIPv6 still suffers from the long authentication latency during the handover process. In order to improve the performance of Proxy Mobile IPv6, HyunGon Kim and Jong-Hyouk Lee, propose a Diffie-Hellman key based authentication scheme that exchange Diffie-Hellman variables with mobile node's profile for secure ongoing sessions. The above scheme improved handover latency by reusing session keys. But, this proposed protocol is required more computation time for generation of these session keys which affect the handover latency. To overcome this deficiency, we proposed another authentication scheme which use elliptic curve diffie-hellman key based algorithm for generation of shared secret session keys in Proxy Mobile IPv6. The propose authentication scheme needs Shorter Key Length, having Lesser Computational Complexity, required Low Power Requirement , More Secure and achieve minimum handover latency. The simulation results show remarkable improvements over PMIPv6, Predictive FPMIPv6, and DH-FPMIPv6 in terms of handover latency.
[Kanwal Imran, Saeed Mahfooz, Azhar Rauf, Shah Khusro. **Enhanced Authentication Scheme for Proxy Mobile IPv6.** *Life Sci J* 2014;11(3s):12-18]. (ISSN:1097-8135). http://www.lifesciencesite.com. 3

Keywords: Proxy Mobile IPv6, Handover Latency, Authentication, Security

1. Introduction

In wireless system, various networks are accumulate which coordinate with each other for better communication and can be accessed easily. But during handover process performance degradation occurs, because different networks are integrated. So that to improve the performance during mobility IETF standardized a protocol, Mobile IPv6 [1]. During the transmission of on-line multimedia applications, handover latency becomes increased. Then various new extensions of MIPV6 are proposed to reduce handover latency. These various new enhancements also reduce signaling load and packet loss. These new enhanced schemes are host based protocols. i-e fast handovers for mobile IPv6 scheme (FMIPV6) [2], and Hierarchical Mobile IPv6 scheme (HMIPV6) [3] which improve the performance MIPv6. These schemes need to modify the protocol stack of Mobile Node (MN).Due to which complexity becomes and it introduce battery problem. To overcome the above problems, a new network based mobility management protocol against host based schemes is developed called Proxy Mobile IPv6 (PMIPV6). PMIPV6 is easily deployed and need low installation cost because MN does not participate in any mobility-related signaling [4]. In this protocol the entities MAG (Mobile Access Gateway) and LMA (Local Mobility Anchor) are used. IETF, are being actively developed many extensions for PMIPv6. That is Fast Proxy Mobile IPv6 (FPMIPv6) [5]. FPMIPv6 reduce handover latency and packet loss during handover process, but it does not consider security issues. In other words, the MN must undergo its authentication procedure to have network access authorization when it attaches to a new network [10]. FPMIPv6 does not supply to reduce authentication latency occurred when the MN changes its access network. We therefore need an efficient and secure handover scheme to deploy PMIPv6 mobility service. To enhance the efficiency for authentication mechanism various schemes are proposed [10, 11]. This research study analyze and compare different authentication schemes and also introduced new authentication scheme i.e. Elliptic Curve Diffie Hellman key based authentication scheme which generates shared secret keys and reuse these session keys for efficient authentication.

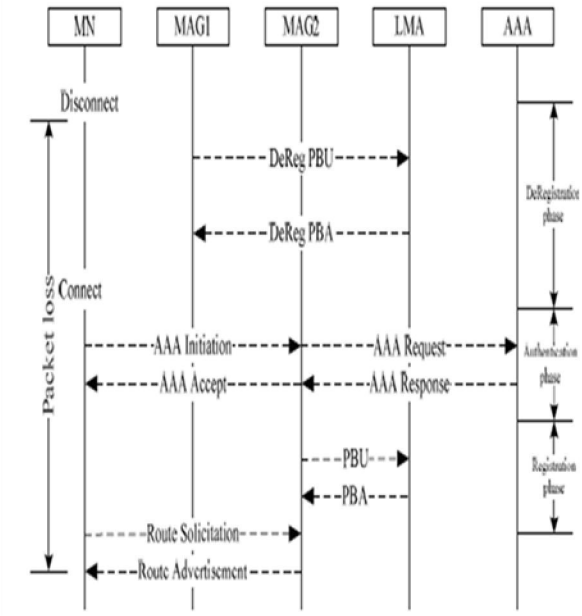
The remainder of this paper is organized as follows: Section 2 describes the specification of PMIPv6, FPMIPv6 within the AAA architecture and Diffie Hellman key based authentication scheme with the operation scenario. Then, in Section 3, the proposed ECDH key based authentication scheme is presented with the timing diagrams. In Section 4, shows the results of performance evaluation which analyze and compare the different authentication schemes. The conclusions of this paper are presented in Section 5.

2. Related Work

2.1 Proxy Mobile IPv6

Recently a network based mobility management protocol called Proxy Mobile IPv6 (PMIPV6) is proposed and standardized by IETF NETLMM

working group. PMIPV6 can be easily deployed and installed in low cost because MN does not participate in any mobility-related signaling [1]. PMIPV6 uses two entities MAG (Mobile Access Gateway) and LMA (Local Mobility Anchor). MN communicates with MAG by sending and receiving signals. LMA provides the three services i.e. mobility management, binding updates and data tunneling. MN sends a Router Solicitation message on entering in a domain. Proxy Binding Update Message (PBU) is sent by MAG to detect the attachment of LMA. Then LMA assigns its home network address to MN after processing PBU. With Proxy Binding Acknowledgement (PBAck), LMA sends binding cache entry with home prefixes. A bidirectional tunnel is established between MAG and LMA for forwarding the traffic. Then Router Advertisement message (RA) is sent by MAG after receiving PBAck to MN. This message configures the IP addresses. AAA (Authentication, Authorization, and Accounting) is an authenticated server that authenticates the MN with MAG to provide the services of mobility and network access. There are two phases of authentication, MN enters in the network in the initial phase of authentication and in second phase MN attached to the other MAG. The handoff occurs, when MN, MAG and AAA interact with each other every time. This frequent handoff makes communication inefficient [4].

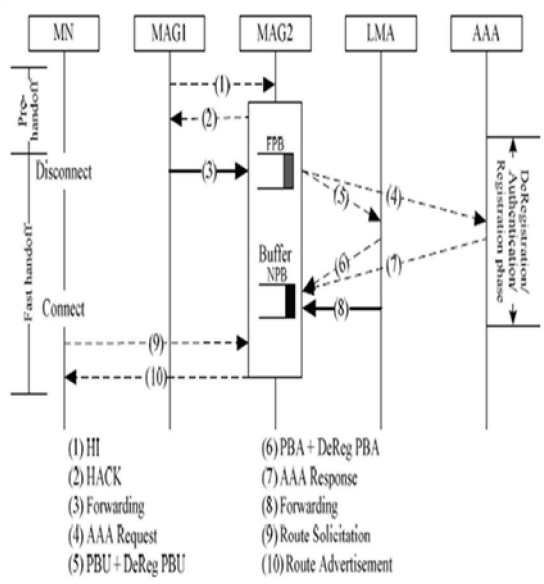


The Handover Procedure of PMIPV6

2.2 Fast Proxy Mobile IPV6

For achieving an efficient handover and reducing packet loss a new scheme has proposed i-e Fast Handover for Proxy Mobile IPv6 (F-PMIPv6)[5]. In (F-PMIPv6) the context is transfer by establishing bidirectional tunnel between previous MAG (PMAG) and New MAG (NMAG) without involving the MN. In this protocol each MAG and an AP (Access Point) works combine as an entity. FPMIPv6 has two modes of operation one is the predictive mode and other is the reactive mode. The difference between the two modes is establishing a bidirectional tunnel between NMAG and PMAG. The tunnel is established prior to handover process in predictive mode and in reactive mode it will established after handover process [9]. In the case, if the MN detached from both PMAG and NMAG, then the both links can buffer the packets, which help to forward the packets in future.

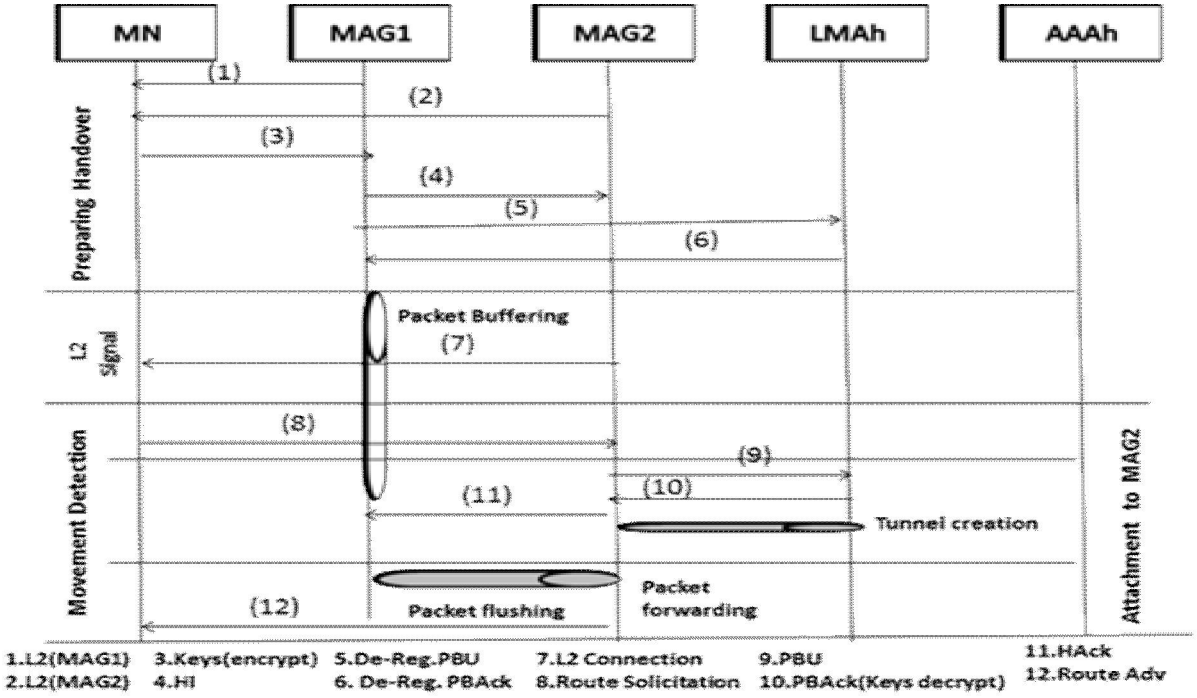
As FPMIPv6 improves handover performance of PMIPv6, but it cannot address the handover authentication latency occurred during the MN undergo its authentication process. For instance, the required times for several message exchanging between the MN and the AAAh, and executing cryptography operation yield long latency. To reduce such long handover authentication latency needs to utilize authentication schemes for achieving secure and efficient handover.



The Handover Procedure of Predictive FPMIPV6

2.3 Diffie-hellman key based authentication

HyunGon Kim and Jong-Hyouk Lee proposed an efficient secure handover scheme which use **Diffie**-hellman algorithm for key generation in proxy mobile ipv6.In this scheme they reused the session keys S_{MN-MAG} and $S_{MAG-LMA}$ which make process efficient [11]. DH key based authentication scheme avoids the contact with the AAAh for authentication of the MN every time. The encryption and decryption of these session keys is done by using a secret key $K_{MAG1-MAG2}$. To provide mobility service for the newly attached MN, M_ρ and K_χ are also transmitted from the MAG1 to the MAG2. The MAGs also compute n, g ,g^x and g^y for generating shared secret keys. This authentication scheme use mathematical operations (exponent) that need much time to compute, and also hard to reverse. That's why it can encrypt a message, but reversing the encryption is difficult. So this scheme needs Exponential running time which affects the handover latency. Due to computational complexity of this protocol infeasible to calculate key $K_{MAG1-MAG2}=g^{xy}$ mod n, when the values (g^x mod n) and (g^y mod n) are given. Especially in case sufficiently large of prime(n) is needed. This scheme needs Maximum computation power consumption by using Longer Key Length for session keys. The Diffie-Hellman key exchange algorithm is not secure as it is vulnerable to a man-in-the-middle attack (MITM). Therefore we propose new authentication scheme which is based on elliptic curve diffie hellman algorithm for key generation. It needs Shorter Key Length for key generation, having Lesser Computational Complexity as it just doing addition and multiplication instead of exponent computation, required Low Power Requirement, More Secure and achieve minimum handover authentication latency by reusing the session keys.

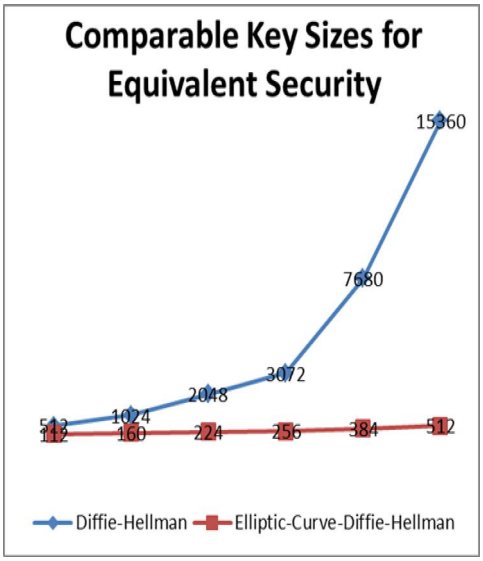


The handover process of DH key based authentication scheme

3. Enhanced Authentication Scheme for Proxy Mobile IPv6

Elliptic-Curve-Diffie-Hellman (ECDH) is a relatively new key agreement algorithm based on Diffie-Hellman but using the elliptic-curve cryptography. It establishes a shared secret key over an insecure channel between two parties using an elliptic curve public-private key pair. The main feature of Elliptic key is that it needs smaller key size to operate. Such as , ECC(elliptic-curve cryptography) uses a 160-bit key in as secured as a 1024 bit key in Diffie-Hellman[13].

As seen in following graph that compare the key sizes of diffie-hellman and elliptic curve diffie-hellman approach foe equivalent security.



In ECDH except the public keys anything is secret. This scheme is secure because intruder cannot derive the private keys of other party [14].

3.1 How the key exchange takes place in ECDH:

1. A and B have to agree on an elliptic curve domain parameters i-e elliptic curve (E), finite field(F) and a point(P) on the curve.
2. A and B have to choose random integers, denoted by n and m
3. A computes nP on E and sends it to B. B computes mP on E and sends it to A by using elliptic curve point-addition.
4. Now A and B can compute nmP, A multiplies the value of mP by its secret number n and B vice-versa.
5. For A and B the secret value is the x-coordinate of computed point.

Elliptic-Curve-Cryptography is an algorithm which may replace Diffie-Hellman protocol because it give equivalent security with respect to DH approach at a smaller key size.ECC compute keys in less time and can secure information on mobiles, wireless devices and smart cards [15].

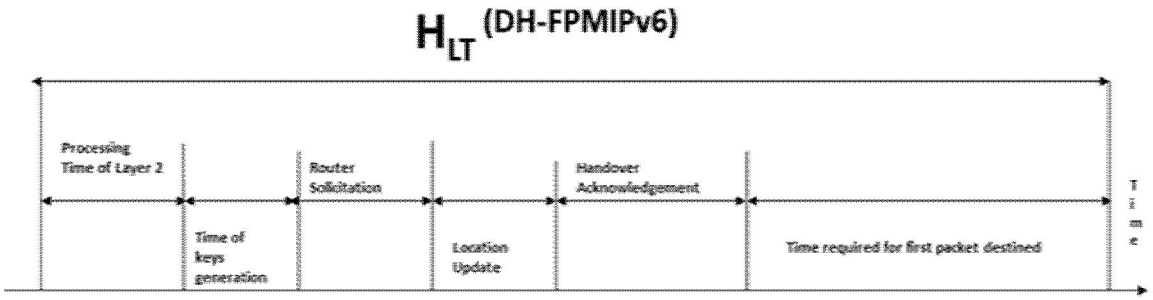


Fig.1 The timing diagram for DH key based scheme's handover

Fig 1 represents the timing diagram for the Diffie-hellman key based authentication scheme.DH key exchange operation takes enough time for key generation which affects handover latency as shown in timing diagram. This deficiency can be improved in proposed scheme by using elliptic curve diffie hellman scheme for keys generation. The improvement is visible in fig 2.Timming diagram of ECDH.

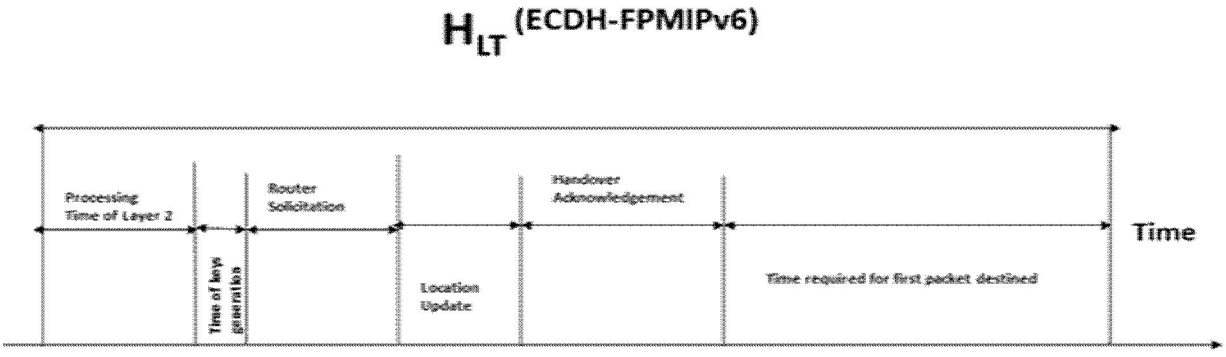


Fig. 2 The timing diagram for the proposed scheme's handover.

The Diffie-Hellman key exchange is vulnerable to a man-in-the-middle attack (MITM). In MITM attack, an intruder C translate A's public value and substitutes its own public value to B. When B sends his public value, C interchange it with its own value and sends to A.C and A now communicate with each other by using a shared key same as C and B communicate with each other by using their shared key. Now the intruder C can decrypt messages easily, sending through A and B.C can also read and modify the messages with the shared key and transmit to other party. The reason of this vulnerability of DH key exchange is that this protocol does not authenticate the participants [16].

The followings are the design principles and assumptions of the ECDH key based authentication scheme.

- Minimizing the computation power consumption by using Shorter Key Length.
- Providing Higher security per key-bit.
- Lesser Computational Complexity as ECDH needs scalar multiplications as compared to DH needs exponential computation for key genration.
- Lesser computational expense or complexity due to lesser number of key bits.
- Shorter key-length ensures lesser power requirement for computation of session keys.
- Protecting session keys against various attacks.
- More Secure than DH because of the Diffie–Hellman problem (DHP).

Diffie–Hellman problem (DHP) is a mathematical problem which describes that, some security systems uses mathematical operations which takes less computational time to solve but difficult is to reverse the operation. It means that encryption of a message is easy but decryption is very tough.

4. Performance analysis

This section presents analysis of comparison among different authentication schemes for PMIPv6. For the analysis of handover latency of different schemes, H_{LT} defines for, the handover latency The definition of handover latency is the time interval in which any packet cannot be sent or received by MN during handover process between two networks. This paper is focus on the authentication process of PMIPv6 which is done by Authentication, Authorization and Accounting server(AAA).The time of delay between AAA server and MAG for message exchanging is T_{AAA}. This delay can be saved by using our proposed scheme because of reusing session keys and do not need to interact with AAA server. The handover latency between MAG and LMA is termed as $T_{MAG\text{-}LMA}$, the time between a MAG and MN as $T_{MAG.MN}$ and between two nearest MAGs is termed as $T_{MAG\text{-}MAG}$. So the equation for handover latencies is given as:

$$H_{LT}^{(PMIPv6)} = T_{L2} + T_{AAA} + 2T_{MAG\text{-}MN} + 3T_{MAG\text{-}LMA} \quad (1)$$

$$H_{LT}^{(FPMIPv6)} = T_{L2} + T_{AAA} + 2T_{MAG\text{-}MN} \quad (2)$$

$$H_{LT}^{(DH\text{-}FPMIPv6)} = T_{L2} + 2T_{Gkeys} + 2T_{MAG\text{-}LMA} + 2T_{MAG\text{-}MN} + 2T_{MAG\text{-}MAG} \quad (3)$$

$$H_{LT}^{(ECDHFPMIPv6)} = T_{L2} + T_{Gkeys} + 2T_{MAG\text{-}LMA} + 2T_{MAG\text{-}MN} + 2T_{MAG\text{-}MAG} \quad (4)$$

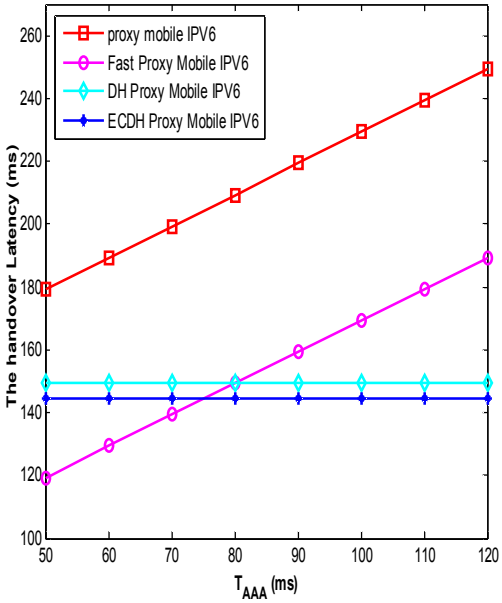


Fig. 3 The variation of the handover latency

Numerical Results

For the numerical analysis, we assume that T_{L2} = 45.35 ms, $T_{MAG–MN}$ = 12 ms, $T_{MAG–MAG}$ = 15 ms, $T_{MAG–LMA}$ = 20ms, and T_{Gkeys}=5ms[4],[5].

For the measuring of variation of the handover latency, T_{AAA} and the number of handovers n are used. Figure 1 presents the variation of the handover latency with respect to T_{AAA}. From results in Fig1, we can find that the DH key based authentication scheme and ECDH key based authentication scheme is not affected by T_{AAA}, but other schemes are affected. This is because that these authentication schemes reuse the previously assigned session keys for an MN. The session keys used in the previous network are securely transferred to the new network. In other

words, these authentication schemes do not require to contact with the AAAh in order to authenticate the MN. DH-FPMIPv6 and ECDH-FPMIPv6 has shown least latency values as compared with other authentication schemes. These two schemes are affected by T_{GKeys}. We can see in Fig. 3,that when T_{AAA} is enough small value, Predictive FPMIPv6 outperforms other schemes, but as T_{AAA} increases, the proposed authentication scheme shows the best performance compared to others.

Then in Fig.4 we increases n from 0 to 10 and fix T_{AAA} as 80 ms. the increase in the handover latency with respect to n (number of handovers). The handover latency cumulatively increases with increase of number of handovers. So it shown clearly that the proposed scheme requires lower handover latency due to its reduced handover authentication time.

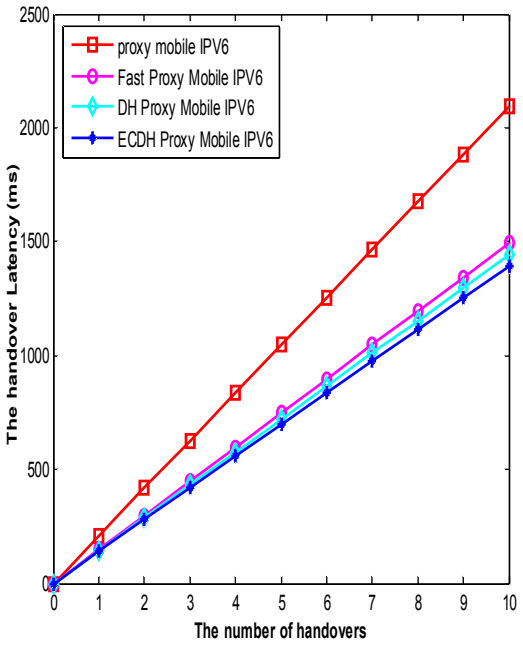


Fig. 4 The variation of handover latency

Conclusions

In this paper, the handover processes of Proxy Mobile IPv6 have been discussed. The other enhanced authentication protocols are also discussed for improving handover latency of PMIPv6.These schemes are, Fast Proxy Mobile IPv6, Diffie-Hellman key based authentication scheme for PMIPv6, and Elliptic-Curve-diffie-Hellman based authentication scheme for keys generation (F-PMIPv6, DH-FMIPv6 and ECDH-FPMIPv6). This paper also provides their analysis for handover latency. The proposed scheme use Elliptic Curve Diffie Hellman (ECDH) key based algorithm for the generation of session keys in PMIPv6 to authenticate MN during handover process. The authentication latency for session keys generation is minimized and more secure in proposed scheme as compared to other authentication schemes. The numerical results demonstrate that the proposed scheme (ECDH) reduces the handover authentication latency and it outperforms PMIPv6, Predictive FPMIPv6, and DH-FPMIPv6 with respect to handover latency.

References

1. D. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6,” RFC 3775, June 2004.
2. Ed. R. Koodli, “Mobile IPv6 Fast Handovers,” RFC 5268, June 2008.
3. Soliman, H., et al., “Hierarchical MIPv6 mobility management”. IETF draft, draft-ietf-mobileip-hmipv6-05. txt, 2001.
4. S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil,“Proxy Mobile IPv6,” RFC 5213, August 2008.
5. Yokota, H., Chowdhur, K., Koodli, R., Patil, B., Xia, F.," Fast Handovers for Proxy Mobile IPv6", RFC 5949, Sept 2010.
6. Momtaz, A., M.E. Khedr, and M.M. Tantawy. “Comparative performance analysis of different Proxy Mobile IPv6 fast handover schemes”. 2010: “IEEE. International Conference on Information, Networking and Automation (ICINA)”, pp. 978-1-4244-8106-4
7. K. Kong; W. Lee; Y Han; M Shin, "Handover Latency Analysis of a Network-Based Localized Mobility Management Protocol,"IEEE International Conference on Communications, 2008, pp.5838-5843.
8. Kong, K.S., et al., “Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6”.IEEE, Wireless Communications, 2008. 15(2): p. 36-45.
9. Ming-Chin Chuang and Jeng –Farn Lee,”FH-PMIPV6: A Fast Handoff scheme in Proxy Mobile IPv6”IEEE International Conference on Consumer Electronics, Communication and Networks (CENet), pp. 1297-1300, April 2011.
10. Ming-Chin Chuang and Jeng –Farn Lee, “A Secure Fast Handover Mechanism for Proxy Mobile IPv6 Networks” The Journal of Systems and Software (2010), doi:10.1016/j.jss.2012.09.015
11. HyunGon-Kim and Jong-Hyouk Lee, “Diffie-Hellman key based authentication in proxy mobile IPv6”, Mobile Information Systems 6 (2010), DOI:10.3233/MIS-2010-0095, page:107-121.

12. Hamid Pirooz ,"Diffie-Hellman Public Key Distribution Scheme: A Complete Overview" December 4, 2000, © SANS Institute 2000 – 2002
13. Chandrasekar, V.R. Rajasekar & V. Vasudevan, "Improved Authentication and Key Agreement Protocol Using Elliptic Curve Cryptography", International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (4) (2009)
14. Yong Wang, Byrav Ramamurthy, Xukai Zou," The Performance of Elliptic Curve Based Group Diffie-Hellman Protocols for Secure Group Communication over Ad Hoc Networks" ICC '06. IEEE International Conference on Communications, Volume: 5 DOI: 10.1109/ICC. 2006.255104, Publication Year: 2006, Page(s): 2243 – 2248
15. K. Igoe, M. Salter,"Fundamental Elliptic Curve Cryptography Algorithms" RFC: 6090, February 2011.
16. Herzog, R. Khazan," Use of Static-Static Elliptic Curve Diffie-Hellman Key Agreement in Cryptographic Message Syntax", RFC: 6278, June 2011.

1/26/2014