Jurnal Teknologi

Full paper

Anonymity and Untraceability Assessment of Authentication Protocols in Proxy Mobile IPv6

Mojtaba Alizadeh[a*], Sabariah Baharun[a], Mazdak Zamani[b], Touraj Khodadadi[a], Mahdi Darvishi[c], Somayyeh Gholizadeh[d], Hossein Ahmadi[c]

[a]*Malaysia-Japan International Institute of Technology, Universiti Teknologi Malaysia, 54100 Kuala Lumpur, Malaysia*
[b]*Advanced Informatics School, Universiti Teknologi Malaysia, Federal Territory, 54100 Kuala Lumpur, Malaysia*
[c]*Faculty of Computing, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia*
[d]*Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 Serdang, Malaysia*

*Corresponding author: amojtaba2@live.utm.my

Article history

Received : 15 August 2014
Received in revised form :
15 October 2014
Accepted :15 November 2014

Abstract

The Proxy Mobile IPv6 or the PMIPv6 is a protocol for mobile management as established by the Internet Engineering Task Force or IETF to assist in the intense usage of mobile devices and to lower the overhead of signaling. As the inclusion of the mobile node in the signaling related to mobility is not necessary, this type of solutions based on networks optimize the performance of the handover based on signaling overhead and handover latency. Nevertheless, the PMIPv6 has several disadvantages such as issues of privacy and security. The process of authentication of users is usually needed at the time of connecting to a wireless network. The mobile users might wander away from their home networks and be approached by other network services. These network services would usually require the users' credentials to authorize the usage of the service. In order to retain a level of anonymity, various degrees of information are required to be safe guarded including the Local Mobility Anchor ID, Media Access Gateway, and Mobile Node. Nevertheless, a few methods of authentication have been suggested to enhance the PMIPv6's performance since 2008 when this protocol was first established [1]; however, the issues of privacy are often ignored. This study attempts to evaluate the authentication methods of the PMIPv6 according to the anonymity of several network mechanisms. The findings of this study reveal that it is important to suggest an appropriate method of enhancing the protection and privacy of network mechanisms.

Keywords: Authentication; privacy evaluation; proxy Mobile IPv6; PMIPv6

1.0 INTRODUCTION

The next generation wireless networks are integrated and as such, the resources of the available networks that are heterogeneous are combined to support connection. It is inevitable that there is mobility in joining these networks. Hence, in order to assist in a seamless migration and connection across these networks, a seamless handover is a requirement that is needed. One such requirement to ensure a seamless handover is the decrease in the delay that happens in the process of a handover. Several protocols for the management of mobility have been suggested and standardized to assist in the mobility over various networks that are heterogeneous; however, these are unable to offer a seamless handover in the present method. Nevertheless, the Proxy Mobile IPv6, which consists of a mobility management that is networked-based, assist tremendously in lowering the delay time during handovers [2]. Therefore, to retain an active connection, the handover function must ensure that it is capable of identifying mobile nodes that have more than one interface when moving across networks that are heterogeneous. A strong and secure device is necessary for this to occur. This function must assist in ensuring that the handover across networks that are heterogeneous are seamless as well as secure without causing extra delay in handover and in the overhead of signaling. Mobile users will face security complications if the handover function is unable to carry out this function.

Privacy issues when utilizing an IP for communication purposes are quite essential. The IP privacy concerns in general deal with protecting communication of the users from accidentally exposing information that might be jeopardized and used for maleficent purposes. This includes instances of collecting data at particular vantage points, gathering information that is linked to particular traffic, and the observation of particular groups of users for activities at particular times daily [3].

Wireless users connect and disconnect voluntarily to a system quite frequently. The process of authentication of the user is usually needed when connecting to a wireless network. The mobile users might wander away from their home networks and be approached by other network services. These network services

would usually require the users' credentials to authorize the usage of the service [4].

In the IP communication for mobile devices, anonymity and privacy of location are not isolated security features as the privacy of location services can be offered in addition to the services of anonymity. The disclosure of the location of the MN is not an infringement of the privacy of the MN, as long as the identification of the MN is kept private since no one knows the identity of the person who is at the location. Thus, here the location privacy is maintained while anonymity is also offered [5]. Section 2.0 will explain the privacy concerns of Proxy Mobile IPv6 further. Moreover, Section 3.0 will further evaluate the present authentication methods according to the privacy matters.

2.0 ANONYMITY in PMIPv6

Chaum in his prominent study entitled, "Untraceable electronic mail, return address, and digital pseudonyms" published in 1981, initiated the study of preserving of the privacy communications [6]. After this time, extensive research was conducted in many areas related to anonymous communication. The present systems in anonymous communication are mainly categorized into four classifications: routing-based schemes, cryptosystem-based schemes, peer-to-peer communication systems, and broadcasting-based systems.

There is a suitable set of subjects with the same potential features to ensure the subject's anonymity. A subject's anonymity is described as the position of not identifying among the set of subjects or the anonymity set [7].

This set includes all the potential sets of subjects, also known as the ambiguity set [8]. In reference to the entities at play, which includes the senders, the anonymity set involves the subjects who would initiate an action. In reference to the acting entities, which include the recipients, the anonymity set involves the subjects who would be acted on. Using this manner, both senders and recipients are as anonymous as their particular anonymity sets. The sets of anonymity for the senders and recipients could be disjointed, similar, or overlap and it may differ over a period of time. The anonymity's security requirement for calculating the probability of a verifier who successfully establishes the real source is precisely 1/n, where n represents the number of members in the set of anonymity.

There are two beneficial effects of anonymity [9]. Firstly, establishing the successful anonymity of network users lowers breaches in security over different attacks. Many of these attacks are made through the form of impersonations. Keeping network users' identities anonymous stops the successful anonymity of network users from linking the identities to the texts sent to or from the users, or taking part in the users' network sessions, which the unscrupulous parties are not meant to be a part of. This prevents the unscrupulous parties from attempting to impersonate the network users. Secondly, establishing the successful anonymity of network users stops the unscrupulous people from misusing the privacy of the users [4].

Anonymity is used effectively as a tool to secure users' privacy and to comply with the rule of the least information given out. Quite a few studies have been conducted to provide channels with anonymous communication mainly to deter attack using these channels [10]. For example, the practical service of anonymity namely Tor [11] has been used to protect the privacy and prevent censorship of users widely. The emergence of wireless networks has caused many extra complications in achieving anonymity as recorded in Reference [12].

The identity of a mobile user has to remain hidden from some networks, especially the visiting networks to maintain anonymity and to disable the tracking function that would lead to the user. It is apparent that the users' privacy protection and authentication processes are two functions that conflict in their requirements. In addition, mobile users normally do not possess sufficient network bandwidth and computational power. Therefore, the protocols for wireless authentication should not be too complicated as when this happens, the demand for bandwidth and computational power will cause the protocols to become unattainable.

3.0 RELATED WORKS

The PMIPv6 lowers the MIPv6's handoff latency substantially as its handoff process takes over the detection of movement (MD) and duplicates the process of address detection (DAD) from the handoff process of layer 3 for the MIPv6. An analytical framework is utilized in [13-15], to evaluate and compare the latency of the handoff of PMIPv6 [1], HMIPv6 [16], MIPv6 [17], and FMIPv6 [18]. The findings reveal that the latency of the handoff of PMIPv6 is lesser than the other three hosting-based protocols of mobility management. In a study by Guan *et al.* [19], they established a testbed to analyze the PMIPv6's performance and compared it to the MIPv6, HMIPv6, and FMIPv6. Similarly, the findings showed that the handoff latency of the PMIPv6 was much lesser than the other used schemes. Another study by Kong *et al*. [13; 14] utilized the AAA infrastructure for authentication of the MN in the PMIPv6 network; however, their schemes revealed the problems of packet loss and ineffective authentication from the PMIPv6. The research by F. Xia and B. Sarikaya [20] opted to enhance the PMIPv6 by improving the performance of the handoff and transferring the context by adopting several ideas from the protocol of the FMIPv6. Nevertheless, [20] did not consider how the authentication process would be carried out. A proposal by Ryu *et al*. [21] used the packet lossless PMIPv6 (PL-PMIPv6) as a buffer mechanism to avoid the packet loss that occurred at handoff, however, the ineffective authentication process of PL-PMIPv6 caused a long latency during the handoff. Furthermore, the PL-PMIPv6 still experienced packet loss complications prior to the bi-direction tunnel being built between the new MAG and the LMA.

Based on this review, many of the past studies concentrated on the improvement of performance using the PMIPv6. According to these studies [22-29], the performance measurements were packet loss, signaling cost, and delay. Nevertheless, the researchers involved in these studies managed to reduce a lot of the handoff latency; but the PMIPv6 still experienced packet loss and ineffective authentication process complications during the handoff [22; 24]. Furthermore, in reference to [30], PMIPv6 faces a lot of security threats. The various current methods that are available should be analyzed in terms of performance measurements and security to establish an appropriate authentication algorithm that would be more secure compared to the current methods. The researchers in [31] quantitatively evaluated the effect of authentication on QoS and security. Firstly, a systematic framework according to the challenges/responses of the authentication mechanisms was introduced, that was widely utilized in different mobile settings. After that, the idea of security levels was suggested to define the communication protection in terms of the nature of the security, such as data integrity, resource availability, and information secrecy. Thirdly, the patterns of mobility and traffic were considered in conducting the quantitative analysis of QoS. The Proxy Mobile IPv6 lowers the delay in handover in comparison to other schemes including the MIPv6 [17], the HMIPv6 [16], and the FMIPv6 [18], Nevertheless, the authentication method is not defined. Zhou

Zhang and Qin [29] for the first time, suggested an authentication method for PMIPv6 to end this problem. Nevertheless, Jiang *et al.* [32] revealed that their method failed to gain the mutual authentication between the network and the Mobile Node (MN). In addition, it only performs authentication unilaterally from the MN to the network, while the MN does not have information about the network's authenticity, hence, it would be at risk to malicious MAG attack and scrupulous network spoofing attacks. After this, they suggested an improvement to overcome these security defects.

[30] discusses the threats to security in the PMIPv6 on the architecture's two interfaces, namely the interface between the MAG and the LMA, and the interface of the MN and its present MAG. Lee *et al*. [33] suggested an authentication mechanism that was based on tickets to optimize the handover authentication process during the handover process to overcome the inefficiency of the normal authentication methods including the Kerberos and the Extensible Authentication Protocol (EAP) when utilized for the PMIPv6. They used the BAN logic to prove the security of the mechanism. A variant of the Diffie-Hellman key agreement was utilized in [34] to remove time needed for re-authentication purposes by the AAA server when the handover occurred to lessen the delay during handover. [35] suggested a pre-shared key based authentication method to exchange mobility signaling. The reference from [36] used a certificate-based public key authentication method for PMIPv6, that is based on the EAP-TLS. This authentication method includes both the initial authentication and the handover authentication, and it is evaluated using the BAN logic. The study by Lee and Chung [37] proposed three authentication mechanisms that are relayed in terms of the security levels namely based on plaintext, based on hash function, and based on shared secret key. The authentication mechanisms are compared based on the security levels and signaling costs.

Ming-Chin Chuang et.al [22; 24] in 2013, suggested two authentication methods and quick handover mechanisms such as the SPAM [22] and the SF-PMIPv6 [24] for networks using PMIPv6 as a means to overcome the problems of long latency during authentication and high packet losses of the PMIPv6 networks during the handover process. The SF-PMIPv6 [24] offers a lower latency during handover, supports local processes during authentication, solves the problem of packet loss, and deals with packets that are out of sequence. The SPAM [22] carries out a bi-casting scheme to avoid the problem of packet loss, utilizes the piggyback method to lower the signaling overhead, and offers a secured mechanism for password authentication (SPAM) for securing authentic users from threats in the PMIPv6 network. Even though the key objectives of both approaches are to offer a secure method of authentication, these approaches still experience security problems including phishing attacks and privacy matters. Table 1 reveals the comparison of the present methods of authentication in the PMIPv6.

Based on Table 1, previous researches did not completely protect the privacy of network entities. The findings of this research reveal that it is important to suggest an appropriate and more secured method of authentication for the Proxy Mobile IPv6 to enhance the protection and privacy of network mechanisms.

Table 1 Privacy evaluation of existing authentication methods for PMIPv6

	Authentication			Anonymity			
	A1	A2	A3	MN	MAG	LMA	AAA
PMIPv6 [1]	AAA	–	–	–	–	–	–
Ticket-Based Authentication [33]	AAA	No	No	No	No	No	No
Secure and low latency handoff scheme for proxy mobile IPv6 [34]	AAA	No	No	No	No	No	No
Mutual Authentication Scheme [35]	AAA	Yes	No	Yes	No	No	No
Certificate-based public key authentication mechanism [36]	LMA	Yes	No	No	No	No	No
Symmetric encryption based challenge-response mechanism [29]	AAA	Yes	No	No	No	No	No
C-PMIPv6 [38]	LMA	Yes	No	No	No	No	No
Enhanced symmetric encryption based challenge-response mechanism [32]	AAA	Yes	No	No	No	No	No
SF-PMIPv6 [24]	MAG	Yes	Yes	Yes	No	No	Yes
SPAM [22]	MAG	Yes	Yes	Yes	No	No	Yes

A1: Authentication Component; A2: MN-MAG Mutual Authentication; A3: MAG-LMA Mutual Authentication

4.0 CONCLUSION

The Proxy Mobile IPv6 was suggested to be utilized to enable a network-based mobility support, as it does not need a mobile host to be included in the mobility signaling. In the specification of the Proxy Mobile IPv6, a procedure for authentication is needed during the initial registration process to access the network. This study discussed the critical issue of authentication methods suggested for the Proxy Mobile IPv6 network namely user anonymity. The findings of this study revealed that many of the past studies have ignored the area of anonymity, which is an important criterion for privacy. In conclusion, suitable protocols for authentication with common limitations of the wireless networks, such as having low network bandwidth, low computational power at the mobile terminals, and high channel error rates, have to be developed to preserve anonymity and making them untraceable.

Acknowledgement

This research is in affiliation with Ministry of Higher Education, Universiti Teknologi Malaysia, Malaysia-Japan International Institute of Technology (MJIIT) and Communication System and Network (CSN) research group.

References

[1] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., Patil, B., andLeung, K. 2008. *Proxy Mobile IPv6*. 1–92.

[2] Magagula, L. A., Falowo, O. E., andChan, H. A. 2009. *PMIPv6 and MIH-enhanced PMIPv6 for Mobility Management in Heterogeneous Wireless Networks*. Paper presented at the AFRICON, 2009. AFRICON '09. 23–25 Sept. 2009.

[3] Koodli, R. 2007. IP Address Location Privacy and Mobile IPv6: Problem Statement.

[4] Chen, H., Xiao, Y., Hong, X., Hu, F., andXie, J. 2009. A Survey of Anonymity in Wireless Communication Systems. *Security and Communication Networks*. 2(5,): 427–444.

[5] Choi, S., Kim, K., andKim, B. 2004. Practical Solution for Location Privacy in Mobile IPv6. In K.-J. Chae & M. Yung (Eds.). *Information Security Applications* Springer Berlin Heidelberg. 2908: 69–83.

[6] Chaum, D. L. 1981. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Commun. ACM*. 24(2): 84–90.

[7] Ren, J., andWu, J. 2010. Survey on Anonymous Communications in Computer Networks. *Computer Communications*. 33(4): 420–431.

[8] Rivest, R., Shamir, A., andTauman, Y. 2001. How to Leak a Secret. In C. Boyd (Ed.). *Advances in Cryptology—ASIACRYPT 2001* Springer Berlin Heidelberg. 2248: 552–565.

[9] Asokan, N. 1994. *Anonymity in a Mobile Computing Environment*. Paper presented at the Mobile Computing Systems and Applications, 1994. Proceedings. Workshop on. 8–9 Dec 1994.

[10] Danezis, G., andDiaz, C. 2008. A Survey of Anonymous Communication Channels: Technical Report MSR-TR-2008-35, Microsoft Research.

[11] McCoy, D., Bauer, K., Grunwald, D., Kohno, T., andSicker, D. 2008. Shining Light in Dark Places: Understanding the Tor Network. In N. Borisov & I. Goldberg (Eds.). *Privacy Enhancing Technologies*. Springer Berlin Heidelberg. 5134: 63–76.

[12] Xinwen, F., Ye, Z., Graham, B., Bettati, R., andWei, Z. 2005. *On Flow Marking Attacks in Wireless Anonymous Communication Networks*. Paper presented at the Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on. 10–10 June 2005.

[13] Ki-Sik, K., Wonjun, L., Youn-Hee, H., Myung-Ki, S., andHeungRyeol, Y. 2008. Mobility Management for all-IP Mobile Networks: Mobile IPv6 vs. Proxy Mobile IPv6. *Wireless Communications, IEEE*. 15(2): 36–45.

[14] Ki-Sik, K., Wonjun, L., Youn-Hee, H., andMyung-Ki, S. 2008. *Handover Latency Analysis of a Network-Based Localized Mobility Management Protocol*. Paper presented at the Communications, 2008. ICC '08. IEEE International Conference on. 19–23 May 2008.

[15] Jun, L., andXiaoming, F. 2008. *Evaluating the Benefits of Introducing PMIPv6 for Localized Mobility Management*. Paper presented at the Wireless Communications and Mobile Computing Conference, 2008. IWCMC '08. International. 6–8 Aug. 2008.

[16] Soliman, H., Bellier, L., Elmalki, K., andCastelluccia, C. 2008. Hierarchical Mobile IPv6 (HMIPv6) Mobility Management.

[17] Johnson, D., Perkins, C., andArkko, J. 2004. RFC 3775: Mobility Support in IPv6. *IETF*.

[18] Koodli, R. 2009. Mobile IPv6 Fast Handovers.

[19] Guan, J., Zhou, H., Xiao, W., Yan, Z., Qin, Y., andZhang, H. 2008. *Implementation and Analysis of Network-based Mobility Management Protocol in WLAN Environments*. Paper presented at the Proceedings of the International Conference on Mobile Technology, Applications, and Systems, Yilan, Taiwan.

[20] Xia, F., andSarikaya, B. 2007. Mobile Node Agnostic Fast Handovers for Proxy Mobile IPv6. *IETF ID draft-xianetlmm-fmip-mnagno-02*.

[21] Seonggeun, R., Gye-Young, K., Byunggi, K., and Youngsong, M. 2008. *A Scheme to Reduce Packet Loss during PMIPv6 Handover considering Authentication*. Paper presented at the Computational Sciences and Its Applications, 2008. ICCSA '08. International Conference on. June 30 2008–July 3 2008.

[22] Ming-Chin, C., Jeng- Farn, L., and Meng-Chang, C. 2013. SPAM: A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks. *Systems Journal, IEEE*. 7(1): 102–113.

[23] Lee, J.-H., andBonnin, J.-M. 2013. HOTA: Handover Optimized Ticket-Based Authentication In Network-Based Mobility Management. *Information Sciences*. 230(0): 64–77.

[24] Chuang, M.-C., andLee, J.-F. 2013. SF-PMIPv6: A Secure Fast Handover Mechanism for Proxy Mobile IPv6 Networks. *Journal of Systems and Software*. 86(2): 437–448.

[25] Illkyun, I., andJongpil, J. 2012. *Security-effective fast authentication scheme for PMIPv6-based NEMO with global mobility support*. Paper presented at the Digital Information Processing and Communications (ICDIPC), 2012 Second International Conference on. 10–12 July 2012.

[26] Melia, T., Giust, F., Manfrin, R., De La Oliva, A., Bernardos, C. J., andWetterwald, M. 2011. *IEEE 802.21 and Proxy Mobile IPv6: A Network Controlled Mobility Solution*. Paper presented at the Future Network & Mobile Summit (FutureNetw), 2011.

[27] Soto, I., Bernardos, C. J., Calderón, M., andMelia, T. 2010. PMIPv6: A network-based Localized Mobility Management Solution. *The Internet Protocol Journal*. 13(3): 2–15.

[28] Muslam, M., Chan, H. A., Ventura, N., andMagagula, L. A. 2010. *Hybrid HIP and PMIPv6 (HIPPMIP) Mobility Management for Handover Performance Optimization*. Paper presented at the Wireless and Mobile Communications (ICWMC), 2010 6th International Conference on. 20–25 Sept. 2010.

[29] Zhou, H., Zhang, H., and Qin, Y. 2009. An Authentication Method for Proxy Mobile Ipv6 and Performance Analysis. *Security and Communication Networks*. 2(5): 445–454.

[30] Kempf, J., andVogt, C. 2007. Security Threats to Network-Based Localized Mobility Management (NETLMM).

[31] Liang, W., andWang, W. 2005. On Performance Analysis of Challenge/Response Based Authentication in Wireless Networks. *Computer Networks*. 48(2): 267–288.

[32] Jiang, Q., Ma, J., Li, G., andYe, A. 2012. *Security Enhancement on an Authentication Method for Proxy Mobile IPv6*. Paper presented at the Proceedings of the 2011 International Conference on Informatics, Cybernetics, and Computer Engineering (ICCE2011) November 19-20, 2011, Melbourne, Australia.

[33] Joong-Hee, L., Jong-Hyouk, L., andTai-Myoung, C. 2008. *Ticket-Based Authentication Mechanism for Proxy Mobile IPv6 Environment*. Paper presented at the Systems and Networks Communications, 2008. ICSNC '08. 3rd International Conference on. 26–31 Oct. 2008.

[34] Kim, H., and Oh, B. 2008. *Secure and Low Latency Handoff Scheme for Proxy Mobile IPv6*. Paper presented at the Proceedings of the International Conference on Mobile Technology, Applications, and Systems, Yilan, Taiwan.

[35] Youngsong, M., Miyoung, K., and Gye-Young, K. 2008.. *Mutual Authentication Scheme in Proxy Mobile IP*. Paper presented at the Computational Sciences and Its Applications, 2008. ICCSA '08. International Conference on. June 30 2008–July 3 2008.

[36] Park, S.-S., Lee, J.-H., andChung, T.-M. 2009. Authentication Analysis Based on Certificate for Proxy Mobile IPv6 Environment. In O. Gervasi, D. Taniar, B. Murgante, A. Laganà, Y. Mun & M. Gavrilova (Eds.), *Computational Science and Its Applications–ICCSA 2009*: Springer Berlin Heidelberg. 5592: 885–896.

[37] Jong-Hyouk, L., andTai-Myoung, C. 2008. *A Traffic Analysis of Authentication Methods for Proxy Mobile IPv6*. Paper presented at the Information Security and Assurance, 2008. ISA 2008. International Conference on. 24–26 April 2008.

[38] Ling, T., andDi, H. 2009. *A Certificated-based Binding Update Mechanism for Proxy Mobile Ipv6 Protocol*. Paper presented at the Microelectronics & Electronics, 2009. PrimeAsia 2009. Asia Pacific Conference on Postgraduate Research in. 19–21 Jan. 2009.