Vol.2009-MBL-50 No.10
2009/9/11

Security Architecture Establishment and Mobility Management for Information Networks

Ruidong Li[†1] and Jie Li[†2]

We investigate the security architecture establishment and mobility management for information networks. In this paper, we do not intend to provide an overall security architecture for information networks. In particular, we focus on the following issues: key management and trust management for MANETs, and hierarchical access control for group communications. Also, we study one aspect of mobility management, handover for mobile IPv6. For each of them, a more efficient and effective scheme is proposed in our dissertation. That is, we propose a localized public-key management for MANETs, a robust and reliable objective trust management for MANETs, a distributed key management scheme for secure group communications, and an enhanced fast handover for mobile IPv6. We perform performance evaluation for each of them, and the results show that the proposed schemes can achieve better performance.

1. Introduction

Information networks are the interconnected systems of terminals, such as Internet, mobile ad hoc networks, mobile IP networks. Currently, most studies on information networks are performed from the viewpoint of either only security or only performance. However, they cannot provide practical mechanisms, since these two aspects are not completely separate issues. Therefore, in this paper, we consider both of them comprehensively to make a balance between security and performance. Based on this idea, we focus on security architecture establishment and mobility management for information networks.

Security architecture is to provide following security services: confidentiality, authentication, integrity, non-repudiation, access control, availability. This paper is not an overall security architecture for information networks and instead focused on the fundamental issues to security architecture establishment: key management and trust management for MANETs (Mobile Ad Hoc Networks), and hierarchical access control for group communications on Internet. For these issues, we firstly focus on security aspect and secondly on performance aspect.

Besides these issues, we also investigate one of the most challenging issues for mobility management, fast handover for Mobile IPv6 network. For this issue, we mainly focus on performance aspect and secondly on security aspect. The four topics we investigated will be described below, respectively.

1.1 Key management for MANETs

Mobile ad hoc networks (MANETs) are multi-hop wireless networks dynamically constructed by mobile nodes without aid of any established infrastructure. Recently much attention has been placed on the public key management for MANET, which plays a crucial role to establish security architecture. Currently, the key management schemes for MANETs can be classified into two categories. One centers on the notion of distributed trust[21] and another adopts web of trust approach[4]. We are interested in web of trust approach, where individual nodes sign each other's public keys by their private keys and progressively form a web of individual public keys interconnected by links formed by these signatures[4].

In order to reduce the overhead caused by the scheme proposed in 4), we propose an localized public-key management scheme (LPM)[8),13)], by which the public key authentication can be achieved by the verification of a certificate chain. By the proposed LPM scheme, each node can save a large storage which originally used as non-updated repository in the self-organized scheme[4].

1.2 Trust Management for MANETs

To force nodes in MANETs to obey the protocol and cooperate with each other, *trust management framework* was firstly introduced as a sperate security service in 2). As another important aspect to the foundation of security architecture in MANETs besides key management, it has attracted much research attention.

To solve the problems in these existing trust management frameworks, we propose an objective trust management framework (OTMF)[12] to establish trust environment for MANETs. The proposed OTMF can obtain more reliable trust than the reputation-based framework and it can inhibit the selective misbehavior attack more effectively than the trust establishment framework.

†1 National Institute of Information and Communications Technology (NICT), Tokyo, Japan
†2 Graduate School of Systems and Information Engineering, University of Tsukuba, Japan

© 2009 Information Processing Society of Japan

1.3 Hierarchical Access control for Multicast

Multicast is an internetwork service that provides efficient delivery of data from a source to multiple recipients. Access control for multicast is to assure that only the registered members of a multicast group can send packets to the group or receive packets sent to the group. A novel access control mechanism supporting multi-level access privilege is referred to as hierarchical access control, which can be achieved by multi-group key management scheme (MKMS)[17]. But MKMS bring much communication overhead.

To reduce the communication overhead, we propose a distributed key management scheme (DKMS)[9),10),14)] to solve the hierarchical access control problem. By the proposed DKMS, the communication overhead will be reduced greatly. In addition, the trust and the storage burden over the centralized server has been distributed to many service group servers.

1.4 Fast Handover for Mobile IPv6

Handover is the process by which an mobile node (MN) keeps its connection active when it moves from one access medium to another[1)]. In Mobile IPv6[5)], handover is achieved primarily through using CoA (Care of Address) to indicate the location of the MN. Fast handover scheme is the scheme to reduce the handover latency by anticipating handover and performing some operations prior to a break of the radio link. It intends to solve two problems[6)]: how to allow an MN to send packets as soon as it detects a new subnet link, and how to deliver packets to a mobile node as soon as its attachment is detected by the new access medium. To solve these problems, a fast handover scheme for Mobile IPv6[6)] has been proposed by others.

However, after investigation, we found that the nCoA (new CoA) generation and DAD procedure can be performed before handover starts. Thus, we propose an enhanced fast handover scheme for Mobile IPv6[11),15)]. Compared with the existing fast handover scheme[6)], the handover latency and packet delay can be reduced by the proposed enhanced scheme.

2. Localized Public-key Management for MANETs

2.1 Background

Key management encompasses techniques and procedures supporting the generation, distribution, and installation of keying material, the controlling the use of keying material, the update, revocation, and destruction of keying material. In this paper, we focus on web of trust approach to design key management schemes for MANETs. By such approach, it is important to solve the credential chain discovery problem[7)]. An interesting scheme circumventing this approach, the self-organized public-key management scheme[4)], has been provided. In this scheme, each node in the network maintains two kinds of repositories, non-updated certificate repository and updated certificate repository. The approximate global certificate graph is stored in the non-updated certificate repository and the certificates required to be updated periodically are stored in the updated repository. The main problem with this scheme is large overhead for the certificate repository of a mobile node to store an approximate global certificate graph.

2.2 Proposed Localized Public-key Management Scheme

To solve these problems, we propose a localized public-key management scheme (LPM) by which the public key authentication can be achieved by the verification of a certificate chain[8),13)]. The main idea in LPM scheme is to provide a method to combine the certificate chain and the communication path. To discover the combination of them, all the nodes in the neighborhood should issue certificates to each other. In the mean time, each node in the network should maintain a certificate repository, where all the certificates issued from her and to her should be stored. Therefore, as long as a route can be discovered from the source node to the destination node, a certificate chain can be obtained hop by hop. Then the authentication procedure can be achieved subsequently. Also, by the LPM scheme, certificate update and certificate revocation mechanism will be carried out locally and efficiently.

The LPM scheme is implemented by three parts: the certificate management part, the public key authentication part and the communication part. In the certificate management part, each node issues certificates in the neighboring hood, stores the certificates issued from her and to her to its certificate repository and performs certificate revocation. The public key authentication part is a procedure to achieve the public key authenticities of the two opposite end nodes of a communication line by the verification of certificate chain. The communication part is the objective of the above two parts. It realizes the communication

© 2009 Information Processing Society of Japan

between any two nodes who have achieved the authenticities of each public key.

2.3 Simulations and results

We have simulated the proposed LPM to compare the average overhead of certificate repository between the proposed LPM scheme and the self-organized scheme in 4).

We set certificate expiration time to range from 20s to 240s. The confidence level in our simulation is 95%, and the confidence interval is set as 10%. We get the results as Figs. 1. Fig. 1 shows the comparison of the average overhead of certificate repository between our scheme and the self-organized scheme.

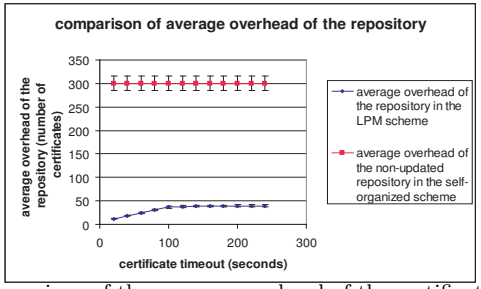

Fig. 1 Comparison of the average overhead of the certificate repository

From Fig. 1, we can see that the average overhead of non-updated repository in the self-organized scheme is around 300, however, the one of our scheme is under 45. Thus even without updated repository, the total overhead of repository will be reduced to be less than 15% of that of the self-organized scheme without updated repository. Thus we can know that the overhead of repository of our scheme is much smaller than the one of the self-organized scheme.

Thus we can see that the proposed LPM scheme can achieve better performance than the self-organized scheme.

2.4 Summary

Here we provide the design and analysis of an proposed on-demand, fully localized and hop-by-hop public key management called LPM for MANETs[8),13)]. There is no non-updated repository to store the approximate global graph, which will consume much storage, in LPM. Our simulation results show that the average overhead of repository in the LPM scheme will be reduced to be less than 15% of that of the self-organized scheme. On the other hand, the proposed LPM scheme is accustomed well to the self-organized nature of MANETs.

3. A Robust and Reliable Objective Trust Management Framework for MANETs

3.1 Background

Trust management and key management are the foundation to provide security service for MANETs. In this section, we investigate trust management framework for MANETs. *Trust* is defined as the *belief level* that one node can put on another node for a specific action based on previous direct or indirect observations. The nodes in a network evaluate the trusts for other participating nodes, and then form the trust relations between them. *Trust management framework* is the framework to establish and manage this kind of trust relations.

In MANETs, currently two categories of trust management frameworks for MANETs have been proposed. One is *reputation-based framework*[3)]. The other is *trust establishment framework*[18),19),22)].

By the reputation-based frameworks[3)], the trusts for other nodes are evaluated objectively by direct observations and second-hand information distributed among a network. Reputation-based frameworks suffer from some attacks including bad mouthing attack, on-off attack, conflicting behavior attack, sybil attack and newcomer attack[18)]. In addition, for the reputation-based framework, *confidence value*, which is another important parameter characterizing the statistical reliability of the computed trust[22)], has not been considered.

For the trust establishment framework[18),22)], trusts for neighbors are evaluated by direct observations and trust relations between two nodes without previous direct interaction are established through combination of the opinions from intermediate nodes. This category of frameworks also suffer from the attacks as mentioned for reputation-based frameworks. Additionally, trust establishment framework is identified to be vulnerable under a novel attack, *selective misbehavior attack*.

In the following, we elaborate selective misbehavior attack and propose an objective trust management framework for MANET to solve these problems.

© 2009 Information Processing Society of Japan

3.2 Selective Misbehavior Attack

Here we identify that trust establishment framework is vulnerable under a novel attack called selective misbehavior attack. By this attack, the attacker performs normal behavior to some nodes that play crucial role to provide network service to it and misbehavior to some other nodes whom it wants to attack.

There is an example given in Fig. 2. In this figure, node n_6 is an attacker. To make node n_2 be excluded from the network and at the same time keep the trust from other nodes to it at a high level, n_6 will forward the packets from node n_2 with drop ratio 90%, but the packets from other neighbors with drop ratio 10%. By the trust establishment framework, the behaviors from n_6 to n_2 only can be reflected in the opinion from n_2 to n_6. However, they cannot influence the opinion from nodes n_1, n_3, n_4, n_5 to n_6. Thus, n_6 performs misbehavior to node n_2, but other nodes still think it is a good guy.

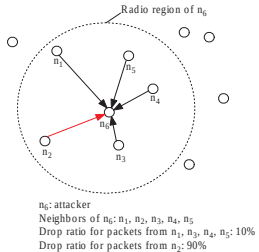

Fig. 2 Selective misbehavior attack performed by n_6

3.3 Proposed Objective Trust Management Framework (OTMF)

To solve the vulnerabilities with existing trust management frameworks including the selective misbehavior attack for trust establishment framework and the absence of considering another parameter, *confidence value*, for reputation-based framework, we propose an objective trust management framework (OTMF) to establish trust relations for a MANET[12]. To make the proposed OTMF more robust and reliable, it is designed based on the modified Bayesian approach by which different weights are put on different information related to the observations on the behaviors according to their occurrence time and providers. That is, the influence exponential decrease method is used to expire old observations, and the trust in recommendation framework is used as the weight for the second-hand information when performing trust evaluation.

In the proposed OTMF, two parameters, *trust value* and *confidence value*, are considered and combined into the metric *trustworthiness*, which is dramatically different from the reputation-based framework. Also the detailed second-hand information distribution and process method is given, where bad mouthing attacks including false accusation and false praise are excluded by deviation test and other checks. On the other hand, in contrast with the trust establishment framework, the opinion of other nodes is formed objectively not only based on the direct observations but the second-hand information by the proposed OTMF.

3.4 Performance Evaluation

3.4.1 Comparison with Reputation-based Framework

To show the necessity of introducing *confidence value*, we compare the evaluated trusts by the proposed OTMF and the reputation-based framework. There are three cases we consider: case 1: α=1; case 2: α=25; case 3: α=50. In all the cases, β varies from 1 to 50. Here, α means the number of normal behavior, and β means the number of misbehavior. We can obtain the results as Fig. 3. From Fig. 3, we can see that for all cases when the number of observations is low, the evaluated *trustworthiness* by OTMF is lower than the reputation obtained by reputation-based framework. This is because that the low *confidence value* influences on the evaluated trust. On the other hand, when the number of observations becomes larger, the *confidence value* will become higher which reflects in the higher trust for the OTMF than that for reputation-based framework. Therefore, we can see that by OTMF, the more reasonable trust can be obtained.

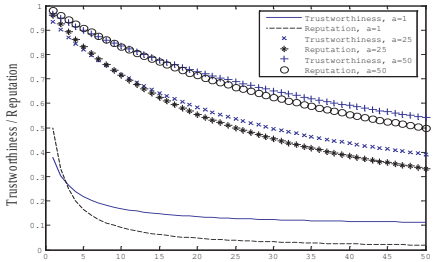

Fig. 3 Trustworthiness obtained by OTMF Vs Reputation obtained by reputation-based framework under the following cases: case 1: α=1; case 2: α=25; case 3: α=50; In all cases, β varies from 1 to 50.

© 2009 Information Processing Society of Japan

3.4.2 Comparison with Trust Establishment Framework

In order to demonstrate that the proposed OTMF can inhibit the selective misbehavior attack, which can be performed in the trust establishment framework, we investigate the metric as the *trustworthiness* value to the attack node.

we consider the scenario depicted in Fig. 2. Under this situation, we can obtain the result as in Fig. 4. In Fig. 4, we can see that by the trust establishment framework, the *trustworthiness* from n_2 to n_6 is much lower. However, the *trustworthiness* from other neighbors to n_6 is much higher. Obviously, the behavior from n_6 to n_2 has not influenced the *trustworthiness* from other neighbors to n_6. In contrast, by the proposed OTMF and the reputation-based framework, the *trustworthiness* and the corresponding reputation will be the same for each neighbor. Therefore, we can see that the OTMF and the reputation-based framework can inhibit the selective misbehavior.

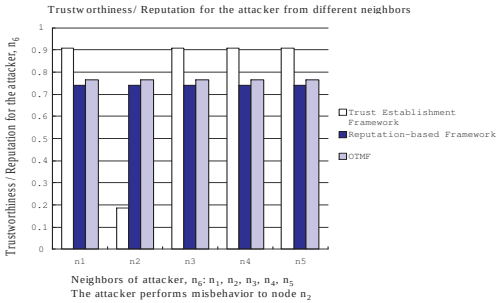

Fig. 4 Trustworthiness to the attacker from different nodes in the neighborhood

3.5 Summary

To prevent nodes from performing misbehaviors or selfish behaviors in MANETs, we propose a robust and reliable objective trust management framework (OTMF) for MANETs[12]. The main contributions are summarized as follows. 1. An objective trust definition is given. 2. The selective misbehavior attack for the trust establishment framework is provided. 3. We propose an objective trust management framework (OTMF), which include the *confidence value* parameter into the trust evaluation. 4. To make the proposed OTMF robust and reliable, it is designed based upon modified Bayesian approach. 5. We perform performance evaluation for the proposed OTMF. From the results, we can see that the proposed objective framework is more robust.

4. Distributed Hierarchical Access Control for Multicast

4.1 Background

Here, we mainly focus on the most important topic for security architecture establishment in multicast communications, access control. Access control is a mechanism to enable each user to determine/obtain the same session key (SK) without permitting unauthorized users to do likewise and securely update keys to prevent the leaving/joining user from accessing the future/prior communications, which is referred to as forward and backward secrecy[16].

We focus on hierarchical access control, which provides access control to assure that group members can subscribe different data streams or possibly multiple of them. Here a Data Group (DG) is defined as a set of users who receive the same single data stream. Here the DGs are denoted by $D_1, D_2, \ldots, D_M$, where M is the total number of the DGs. A Service Group (SG) is defined as a set of users who have the same access privilege. SGs are denoted by $S_1, S_2, \ldots, S_I$, where I is the total number of SGs.

Currently, multi-group key management scheme (MKMS)[17] is the promising method for hierarchical access control. By MKMS, one integrated key graph is employed to manage keys for all users. This key graph is constructed by three steps. Firstly, some subtree referring to as the SG-subtree (Service Group subtree) is constructed for each SG S_i with the root associated with a key K_i^S and the leaves being the users in this SG. Secondly, for each DG, construct some subtree called DG-subtree whose root is the DG key K_m^D and whose leaves are $\{K_i^S, \forall i : t_m^i = 1\}$. Thirdly, combine the SG-subtrees and DG-subtrees by connecting the leaves of the DG-subtrees and roots of SG-subtrees. MKMS is a good mechanism to achieve hierarchical access control. However, the merging key tree step seems complex. Another problem for MKMS is that each rekey message will be broadcast to all the users in the group even who cannot decrypt it and do not need it.

4.2 Proposed Distributed Key Management Scheme (DKMS)

To solve the problems in MKMS, we propose a distributed key management scheme (DKMS) to solve the hierarchical access control problem[9),10),14]. We

© 2009 Information Processing Society of Japan

recommend that each service group, which is a set of users who share the same access privilege and receive the exactly same set of data streams, maintains one service group server. The server is used to manage keys in this service group.

The structure proposed in DKMS includes two kinds of parts: DG part which is used to manage SG servers, and SG part which is used to manage users who subscribe to this SG. The DG part is composed of all the SG servers. The SG part includes an SG server and all users who subscribe to that SG.

The structure construction for DKMS includes 3 steps as follows.

Step 1: In the DG part construction, an SG server group (SGSG) constituting all SG Servers is constructed. One multicast address and one multicast key are assigned to all these servers. At the same time, one SG key K_i^S is allotted to each SG server. Also the related SKs should be given to related SG servers during DG part construction.

Step 2: In the SG part construction, for each SG S_i, a SG-subtree having the root being associated with an SG key, K_i^S, and the leaves being the users in S_i is constructed. Also one multicast address is assigned to each SG.

Step 3: Simply combine these two kinds of groups by connecting the SG keys to the roots of SG-subtrees.

4.3 Performance Analysis

We will consider the performance metrics for MKMS and DKMS provided as follows : storage overhead at servers (R_{SER}), storage overhead of users ($R_{u\in S_i}$), rekey overhead (C_{ij}), communication overhead of the network (TC_{ij}).

The key tree constructed is assumed to be fully loaded and maintained as balanced as possible. We use analytical model to perform performance analysis. We summary the results as in Table 1. From Table 1, we can see that the storage overhead of each user can be reduced. At the same time, the similar performance on the storage overhead of the servers and rekey overhead can be achieved. However, the proposed scheme, DKMS, can achieve better performance than MKMS on the communication overhead since the rekey message is restricted to the users in the related SGs when broadcast is performed.

4.4 Summary

Here, we propose a distributed key management scheme to achieve hierarchical access control[9),10),14)]. Compared with MKMS[17)], the main advantages of our scheme are summarized as follows. 1. There is no complex merging key tree algorithm in our scheme. 2. The communication overhead can be greatly reduced. 3. The storage overhead of each user is reduced. 4. The system will be more robust. 5. Also the better scalability can be achieved by our scheme.

Table 1 Results Summarization

Metrics	MKMS	DKMS
R_{SER}	$O(\frac{M\cdot d\cdot n_0}{d-1})$	$O(\frac{M\cdot d\cdot n_0}{d-1})$
$R_{u\in S_i}$	$O(\log_d(n_0))$	$O(\log_d(n_0))$
C_{ij}	$O(d\cdot\log_d(n_0))$	$O(d\cdot\log_d(n_0))$
TC_{ij}	$O(M\cdot d\cdot n_0\cdot\log_d(n_0))$	$O(d\cdot n_0\cdot\log_d(n_0))$
NOTE	$R_{u\in S_i}^{MKMS} \geq R_{u\in S_i}^{DKMS}$	

5. An Enhanced Fast Handover with Low Latency for Mobile IPv6

5.1 Background

Handover is the process by which an MN keeps its connection active when it moves from one access medium to another[1)]. Handover includes layer 2 handover and layer 3 handover. In this paper, we focus on layer 3 handover for mobile IPv6. The layer 3 handover process is composed of the following components: movement detection, new Care-of-Address (CoA) configuration and binding update. During movement detection, mobile node detects whether it moves from one domain to another domain. By new CoA configuration, a new CoA is generated and assigned to the mobile node. Binding update is used to notify the home agent and correspondent node the update of new CoA.

Fast handover scheme is the scheme to reduce the handover latency by anticipating handover and performing some operations prior to a break of the radio link. A fast handover scheme for Mobile IPv6 has been proposed in 6). In this scheme, the movement detection latency is reduced by providing the MN with the information about the new access point and the associated subnet prefix information when the MN is still connected to its current subnet. The new CoA configuration latency is reduced by neglecting DAD (Duplicated Address Detection)[20)] and by generating and configuring new CoA by MN itself. To reduce the binding update latency, a bidirectional tunnel between previous access router (PAR) and the new access router (NAR) is established. However, the handover

© 2009 Information Processing Society of Japan

latency is still long, which can be reduced.

5.2 Proposed Enhanced Fast Handover Scheme for Mobile IPv6

Consider the network architecture depicted in Fig. 5. There are three entities in the network architecture: HA (Home Agent), AR (Access Router), AP (Access Point). Besides these, there are two kinds of nodes, CN (Correspondent Node) and MN (Mobile Node). The MN connects to the Internet via AP and AR.

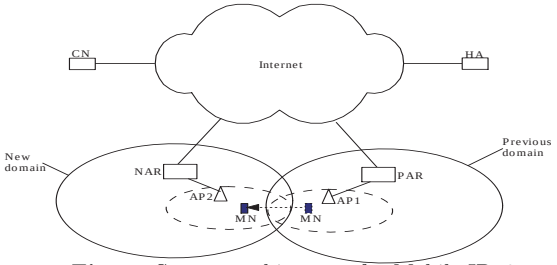

Fig. 5 System architecture for Mobile IPv6

We propose an enhanced fast handover scheme for Mobile IPv6[11),15)]. We let the new AR construct a new CoA, perform DAD for the MN and store this new CoA to the nCoA (new CoA) table when anticipating that a handover for an MN is about to happen. Then when the MN requests the nCoA through the previous AR, this new CoA will be distributed to the MN from the NAR via PAR. At the same time, to reduce the registration latency in the binding update, the binding update to the HA/CN will be performed after the PAR knows the nCoA. Also the localized authentication procedure cooperated with the proposed scheme is provided.

The proposed scheme includes two parts. One is the new CoA generation maintenance method. By this method, the new CoA is generated by NAR beforehand and NAR maintains a CoA table for communications. The other is the proposed enhanced fast handover scheme. In this scheme, the binding updates to HA/CN are brought beforehand. Here, we merge the movement detection procedure and tunnel establishment procedure, and let PAR send BU_HA/CN (Binding Update to HA and CN) directly after PAR knows the new CoA. Also the DAD will not be performed during the period when the tunnel is established as in the predictive fast handover scheme, because DAD has already been performed beforehand.

5.3 Performance Evaluation

Here we conduct performance evaluation on the metric of latency of handover to compare the enhanced fast handover scheme with the existing scheme[6)]. We consider two cases.

- Case 1: $T_{BU} <= T_{pre2} + T_{L2} + T_{FNA}$
  we can obtain the latency comparison as Fig. 6. From Fig. 6, we can see that the proposed enhanced fast handover scheme can reduce the handover latency compared with the existing fast handover scheme in case 1.

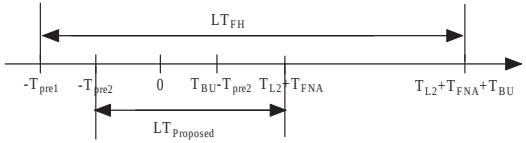

Fig. 6 Handover latency comparison in Case 1

- Case 2: $T_{BU} > T_{pre2} + T_{L2} + T_{FNA}$
  We can get the latency comparison as Fig. 7. From Fig. 7, we can see that the latency for handover can be improved by the proposed enhanced fast handover scheme in case 2.

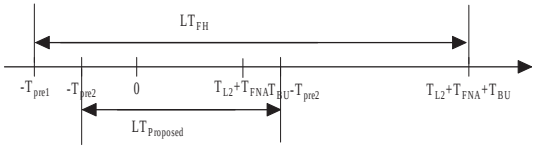

Fig. 7 Handover latency comparison in Case 2

5.4 Summary

In this paper, we propose an enhanced fast handover scheme for Mobile IPv6[11),15)]. In our scheme, each AR maintains a CoA table, and generates a new CoA for the MN that is anticipated to move to its domain. At the same time, we propose that binding updates to HA/CN are performed by PAR from the time point when the nCoA is known by PAR. Finally, we analyze the handover delay and the packet delay. The analysis shows that with the proposed

© 2009 Information Processing Society of Japan

enhanced scheme, the handover latency can be reduced compared to the existing fast handover scheme.

6. Conclusions

To balance security and performance, we focus on the following issues: key management and trust management for MANETs, and hierarchical access control for group communications, and handover for mobile IPv6. For each of them, we proposed a more efficient and effective scheme in this paper. That is, we propose a localized public-key management for MANETs[8),13)], a robust and reliable objective trust management for MANETs[12)], a distributed key management scheme for secure group communications[9),10),14)], and an enhanced fast handover for mobile IPv6[11),15)]. Performance evaluations have been performed, which show that the proposed schemes can achieve better performance besides security.

References

1) I. F. Akyildiz, J. Xie, and S. Mohanty, "A Survey of Mobility Management in Next-Generation All-IP-Based Wireless Systems," IEEE Wireless Communications, Aug. 2004.
2) M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," *Proceedings of the 1996 IEEE symposium on Security and Privacy*, pp. 164 - 173, 1996.
3) S. Buchegger, and J.-Y. Le Boudec, "A Robust Reputation System for P2P and Mobile Ad-Hoc Networks," *Proceedings of P2PEcon 2004*, Harvard University, Cambridge MA, USA, June 2004.
4) S. Capkun, L. Buttyan, and J. P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks", *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, pp. 52-64, Jan.-Mar. 2003.
5) D. Johnson, E. C. Perkins and J. Arkko, "Mobility Support in IPv6," RFC 3775, June 2004.
6) R. Koodli, "Fast Handovers for Mobile IPv6," RFC 4068, July 2005.
7) N. Li, W. Winsborough, and J. Mitchell, "Distributed Credential Chain Discovery in Trust Management (Extended Abstract)", *Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS-8)*, ACM Press, pp. 156-165, Philadephia, Pennsylvanis, Nov. 2001.
8) R. Li, J. Li, H. Kameda and P. Liu, "Localized Public-Key Management for Mobile Ad Hoc Networks", *Proceedings of the IEEE 2004 Global Communications Conference (IEEE GlobeCom 2004)*, Nov. 29 - Dec. 3, 2004, Dallas, Texas, USA.
9) R. Li, J. Li and H. Kameda, "Distributed Hierarchical Access Control for Secure Group Communications", in *2005 International Conference on Computer Networks and Mobile Computing (ICCNMC'05), LNCS 3169*, pp. 539-548, Zhangjiajie, China, 2005.
10) R. Li, J. Li, and H.-H. Chen, "Analysis and Design of Distributed Hierarchical Access Control for Multimedia Networks", *Proceedings of the IEEE 2005 Global Communications Conference (IEEE GlobeCom 2005)*, Nov. 28 - Dec. 2, 2005, St. Louis, MO, USA.
11) R. Li and J. Li, "An Enhanced Fast Handover Scheme for Mobile IPv6", *International Wireless Communications and Mobile Computing Conference (IWCMC 2006)*, July 3 - 6, 2006, Vancouver, Canada.
12) R. Li, J. Li, P. Liu and H.-H. Chen, "An Objective Trust Management Framework for Mobile Ad Hoc Networks", *2007 IEEE 65th Vehicular Technology Conference VTC 2007 Spring (IEEE VTC 2007 Spring)*, 23 C 25 April 2007, Dublin, Ireland.
13) R. Li, J. Li, P. Liu and H.-H. Chen, "On Demand Public-Key Management for Mobile Ad Hoc Networks", *Wiley's Journal of Wireless Communications and Mobile Computing*, Vol. 6, no. 3, pp. 295-306, May, 2006.
14) R. Li, J. Li, and H.-H. Chen, "DKMS: Distributed Hierarchical Access Control for Multimedia Networks", *International Journal of Security and Networks*, Vol. 2, no. 1/2, 2007.
15) R. Li, J. Li, K. Wu, Y. Xiao, and L.-J. Xie, "An Enhanced Fast Handover Scheme with Low Latency for Mobile IPv6", *IEEE Transactions on Wireless Communications*. (Accepted)
16) S. Rafaeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication", *ACM Computing Surveys*, vol. 35, no. 3, pp 309-329, Sept. 2003.
17) Y. Sun and K. J. Ray Liu, "Scalable Hierrarchical Access Control in Secure Group Communications", *Proc. IEEE INFOCOM'04*,Hong Kong,Mar. 2004.
18) Y. Sun, Z. Han, W. Yu and K. J. Ray Liu, "A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks," *Proceedings of the IEEE Infocom 2006*, Apr. 2006, Barcelona, Spain.
19) G. Theodorakopoulos, and S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," *IEEE Journal on Selected areas in Communications*, Special Issue on Security in Wireless Ad-Hoc Networks, Feb. 2006.
20) S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration," RFC 2462, Dec. 1998.
21) L. Zhou and Z. J. Hass, "Securing Ad Hoc Networks", *IEEE Network*, vol. 13, no. 6, pp. 24-30, Nov.-Dec. 1999.
22) C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs," *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2005)*, Alexandria, VA, USA, November 7, 2005.

© 2009 Information Processing Society of Japan