Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 189389, 7 pages
http://dx.doi.org/10.1155/2015/189389

Research Article

Pseudonyms in IPv6 ITS Communications: Use of Pseudonyms, Performance Degradation, and Optimal Pseudonym Change

Jong-Hyouk Lee,[1] Giwon Lee,[2] and Sangheon Pack[2]

[1]*Department of Computer Science and Engineering, Sangmyung University, Cheonan 330-720, Republic of Korea*
[2]*School of Electrical Engineering, Korea University, Seoul 136-729, Republic of Korea*

Correspondence should be addressed to Sangheon Pack; shpack@korea.ac.kr

Received 25 September 2014; Accepted 24 January 2015

Academic Editor: Kun Hua

IPv6 developed as a next generation Internet protocol will provide us with safer and more efficient driving environments as well as convenient and infotainment features in cooperative intelligent transportation systems (ITS). In this paper, we introduce the use of pseudonyms in IPv6 ITS communications for preserving location privacy. We conduct qualitative study on the performance degradation due to the use of pseudonyms and quantitative analysis on the optimal pseudonym change interval. Numerical results demonstrate that an appropriate pseudonym change interval should be changed depending on the packet arrival rate, mobility rate, and security level.

1. Introduction

Cooperative intelligent transportation systems (ITS) aim at providing new advanced solutions to today's transport problems. Communications among ITS stations (e.g., cars and roadside infrastructures) are essential parts of the cooperative ITS for improving road safety, efficiency, and comfort during driving. As the communications between ITS stations are the heart of the cooperative ITS, it is important to correctly understand how the deployment of cooperative ITS will affect an individual's privacy during his/her driving.

Privacy is one of the fundamental rights of human being. In particular, location privacy is a specific type of privacy that can be defined as follows [1]: "the ability to prevent other parties from learning one's current or past location." Imagine your car as a vehicle ITS station constantly communicating with other nearby ITS stations, for example, cars and roadside infrastructures. Your car emits its location (e.g., GPS position information), speed, heading direction, and even identity 10 times per second. Thus, anyone that has a wireless radio receiver system (e.g., wireless access point) within the wireless radio transmission range (probably in 500 meters or 1,000 meters) is able to capture all messages sent out from your car. Now imagine the ability to set up a set of wide-range wireless radio receiver systems in a city. It means that the activity of every single car in the city can be surveilled including yours. In other words, without sophisticated skills, communications among ITS stations, for example, vehicle, roadside, and personal ITS stations, are exposed to an observer in a wireless radio transmission range because of the nature of wireless communications. As the observer extracts identifiers from a message such as addresses in each protocol layer in transmissions, he/she could link messages and track a vehicle ITS station emitting the messages having the same identifiers.

To address location privacy in cooperative ITS, the use of pseudonyms has been chosen as a baseline approach for preserving location privacy. A pseudonym, which is an arbitrary bit string to generate a temporary identifier in each protocol layer, is used with an appropriate changing scheme [2]. For instance, a vehicle ITS station uses a pseudonym P_i in a short period t_{P_i} and changes P_i to a new pseudonym P_{i+1} for the next short period $t_{P_{i+1}}$. By using a pseudonym only in a short period, observers are only able to link messages sent in the

Table 1: Cooperative ITS applications and IPv6 applicability.

ITS application	Type	Required latency	Message priority	IPv6 applicability
Collision avoidance	Road safety	Very low (in microseconds)	High	Probably not
Road sign notifications	Road safety	Low (in milliseconds)	High	Possible
Incident management	Road safety	Low (in milliseconds)	High	Possible
Traffic management	Traffic efficiency	Low-medium (in milliseconds)	Medium	Yes
Road monitoring	Traffic efficiency	Low (in milliseconds)	Medium	Yes
Entertainment	Infotainment	Average (in seconds)	Average	Yes
Contextual information	Infotainment	Medium (in milliseconds)	Medium	Yes

short period. It thus may help to prevent the observers from identifying the vehicle ITS station emitting the messages with different pseudonyms [2–5]. However, while high frequency of pseudonym changes improves location privacy, it badly influences communication overhead as a pseudonym change causes the communication identifier change, especially IPv6 address change in IPv6 communications. Note that research results from [5] suggested that a simple pseudonym change does not effectively preserve location privacy but it does not mean that the pseudonym change is ineffective.

In this paper, which is an extension of the paper published in [6], we focus on the use of pseudonyms in IPv6 ITS communications for preserving location privacy. In particular, we present an IPv6 address configuration with pseudonyms and then study a performance degradation issue due to frequent pseudonym changes at the IPv6 layer. We also investigate the optimal pseudonym change algorithm that makes a balance between communication overhead and location privacy at the IPv6 layer.

2. IPv6 Communications in Cooperative ITS

2.1. IPv6 Communications and Applications. The ISO/ETSI ITS station reference architecture specified in [7, 8] introduces various communication protocols designed to meet specific requirements for cooperative ITS. However, among communication protocols in the network layer, IPv6 is a major communication protocol as it provides Internet connectivity and communication capacity for various applications. The use of IPv6 especially satisfies the addressing needs of a growing number of vehicles and personal devices [9] and provides session continuity between heterogeneous networks, thanks to a mobility support extension, that is, NEtwork MObility (NEMO) [10].

Various ITS applications have been investigated and studied with respect to their functionalities: safety, efficiency, and infotainment applications [11]. At the beginning of ITS research, most of studies focused on the road safety applications that are basic and essential applications as those applications aim at minimizing the risk of accidents. However, cooperative ITS does not only provide such limited functionalities. It also provides advanced applications such as traffic efficiency and infotainment applications. In particular, as shown in Table 1, IPv6 communications can be applied into the traffic efficiency and infotainment ITS applications that do not require strict message transmission and very low latency. Then, among the road safety applications, some applications like road sign notifications and incident management are possibly supported by IPv6 communications. For instance, messages of road sign notifications and incident management may be delivered to specific vehicles via roadside infrastructures that use IPv6 communications.

2.2. IPv6 Related Standardization Efforts. As IPv6 has been originally developed for the Internet, its adaptation into cooperative ITS requires a set of standardizations that do not intend to define new protocols or message modification at the IPv6 layer but define how standard IPv6 protocols developed by the IETF are combined for cooperative ITS. The following are standardization efforts at the ISO and ETSI levels.

(i) ISO 21217 [7] and ETSI EN 302 665 [8]: the ISO/ETSI ITS station reference architecture containing IPv6 communications at the network layer is specified.

(ii) ISO 21210 [9]: IPv6 networking between two or more ITS stations has been specified.

(iii) ETSI TS 102 636-6-1 [12]: IPv6 networking over GeoNetworking capabilities has been specified.

(iv) ETSI TR 101 555 [13]: as of writing this paper, IPv6 networking analysis is being documented.

(v) ISO 16788 [14]: as of writing this paper, IPv6 network security is being documented.

(vi) ISO 16789 [15]: as of writing this paper, IPv6 network optimization is being documented.

2.3. IPv6 Related European Projects. IPv6 communications have been widely tested and validated through successful ITS related projects. In the Cooperative Vehicle Infrastructure Systems (CVIS) European FP6 project (2006–2010), an implementation of the ISO CALM architecture has demonstrated capabilities offered by IPv6, for instance, session continuity support during handovers between M5 (IEEE 802.11p variant) and 3G access technologies. The GeoNet European FP7 project (2006–2010) was also launched to investigate a combination of IPv6 and GeoNetworking, that is, IPv6 networking over GeoNetworking capabilities. The recently launched European FP7 project, ITSSv6 (IPv6 ITS Station Stack for Cooperative ITS Field Operational Tests, 2011–2014), aims at developing an IPv6 ITS station communication stack complying related ISO, ETSI, and IETF standards. In particular, the IPv6 ITS station communication stack, which

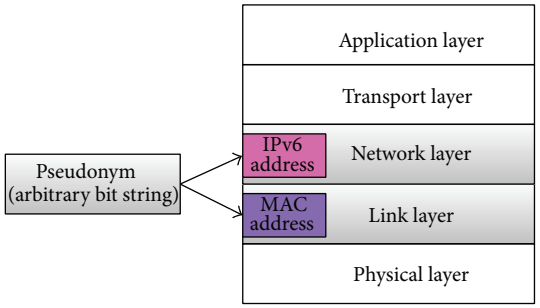


Figure 1: Example of a pseudonym use in the link and network layers.

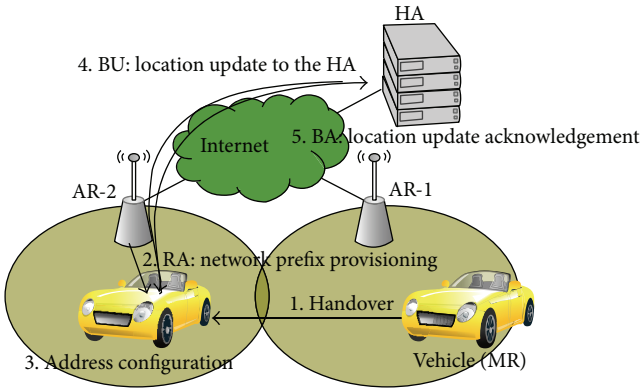


Figure 2: Movement of a vehicle.

is being developed based on the existing open source software with additional software components, will be released as an open source software.

3. Use of Pseudonyms in IPv6 ITS Communications

3.1. IPv6 Address and Pseudonym. At the IPv6 layer, the IPv6 address is an identity that is globally unique when the address is a unicast address. In order to provide location privacy at the IPv6 layer, a pseudonym, an arbitrary bit string, is used to generate an arbitrary IPv6 address.

Figure 1 shows an example of a pseudonym use in the link and network layers for preserving location privacy. Note that pseudonyms can be used in all communication stacks against observers examining not only one communication layer. In this example, the pseudonym is assumed to be 48 bits long and it thus replaces the 48 bits of MAC address, while a new IPv6 address, which is 128 bits long, is generated based on the supplied pseudonym. More specifically, the rightmost 64 bits of IPv6 address, that is, interface identifier, are generated based on the pseudonym while the leftmost 64 bits of IPv6 address, that is, network prefix, are supplied from a router advertisement (RA) sent from an access router.

As mentioned earlier, the pseudonym is synchronously changed across the entire communication stack in order to make sure that identity information at each layer is changed. For instance, as shown in Figure 1, when a current pseudonym P_i is changed to a new one P_{i+1}, the whole MAC address is replaced by P_{i+1}, while the IPv6 address is changed accordingly [3]. Hereinafter, we focus on the use of pseudonym at the IPv6 layer.

3.2. Pseudonym Change. An example of pseudonym changes at the IPv6 layer is introduced in detail. In particular, we illustrate two specific pseudonym changes similar to [3]: (1) pseudonym change due to a handover and (2) pseudonym change due to a pseudonym expiration.

Figure 2 shows a considered network topology wherein a vehicle ITS station implementing IPv6 mobility, that is, NEMO, changes its attachment point from an access router, AR-1, to a new access router, AR-2. The vehicle ITS station is thus assumed to be equipped with a mobile router (MR)

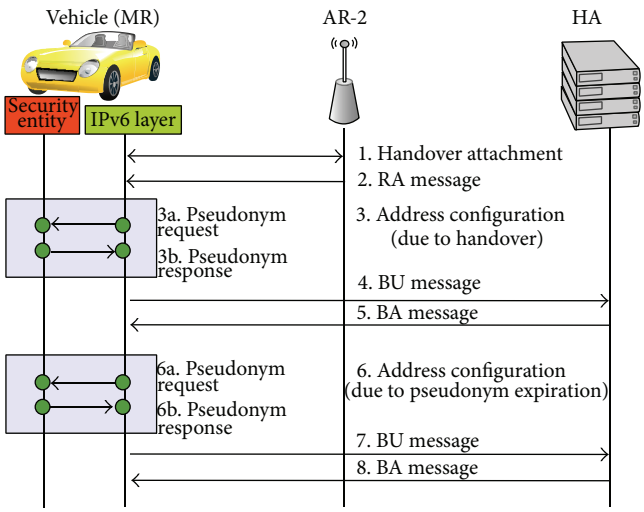


Figure 3: Example of pseudonym changes for handover and pseudonym expiration.

functionality defined in [10]. Each access router provides the Internet connectivity to the vehicle in its access network. The home agent (HA) is located at the Internet.

Figure 3 shows pseudonym change procedures. The details of each step are as follows.

(1) First, a pseudonym change due to handover is considered. Suppose that the vehicle ITS station V attaches to a new access network of AR-2.

(2) V receives an RA message from AR-2. The RA message includes the network prefix NP_2 for the new access network of AR-2.

(3) V is required to configure a new address called care-of address (CoA) with NP_2 at the new access network. However, in this step, a new pseudonym P_2 instead of its previous pseudonym P_1 or its MAC address is used to generate the CoA CoA_2 with NP_2. If P_1 would be still used at the new access network, an observer who can access both access networks could recognize the vehicle's movement by checking the use of P_1 in address generation. The IPv6 layer thus requests P_2 to

the security entity. As P_2 is provided to the IPv6 layer, it is used to generate CoA_2 with NP_2:

$$\mathrm{CoA}_2 = F_{U-L}\left(\mathrm{NP}_2 \parallel \mathrm{EUI64}\left(P_2\right)\right), \quad (1)$$

where $\parallel$ is a concatenation operation, EUI64$(\cdot)$ is an EUI-64 function that generates the interface identifier based on P_2, and $F_{U-L}(\cdot)$ is a function for the modified EUI-64 that inverts universal/local bit. For instance, suppose NP_2 and P_2 are `2002:db8:1:2::/64` and `00:1D:BA:06:36:62`, respectively. Let IID_{P_2} denote the interface identifier generated based on P_2. Then, by EUI64(P_2), IID_{P_2} is obtained as `00:1D:BA:FF:FE:06:36:62`. Then, an unlinkable address, that is, CoA_2, with its previous address, is generated as `2002:db8:1:2:021d:baff:fe06:3662`.

(4) Before the use of CoA_2 in unicast communications, the uniqueness is checked via the duplicate address detection (DAD) procedure. Then, if CoA_2 is unique, V uses CoA_2 to inform its new location by sending a BU message to its HA. The new location of V is registered to the binding cache of HA.

(5) The HA replies with the BA message to V.

(6) A pseudonym change due to pseudonym expiration is now considered. Suppose that the current pseudonym's lifetime t_{P_2} has expired. Then, V has to reconfigure its current CoA, CoA_2, even if it has not moved to another access network. For this, the IPv6 layer requests a new pseudonym to the security entity as in step (3). After a successful provision of the new pseudonym P_3, similar to the previous address generation, a new CoA, CoA_3, is generated as

$$\mathrm{CoA}_3 = F_{U-L}\left(\mathrm{NP}_2 \parallel \mathrm{EUI64}\left(P_3\right)\right), \quad (2)$$

where P_3 is used for generating its new interface identifier, IID_{P_3}. In order to check the uniqueness of CoA_3, the DAD procedure is performed again.

(7) V sends a new BU message containing CoA_3 as a source address.

(8) Upon receiving the BU message, the HA updates its binding cache for V and replies with the BA message.

4. Qualitative Analysis

In this section, we examine performance degradation with the use of pseudonym at the IPv6 layer.

A pseudonym at the IPv6 layer is changed mostly due to the following:

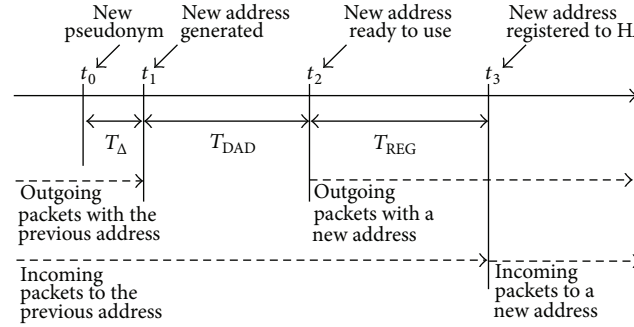
(i) the pseudonym change interval, that is, pseudonym expiration,

(ii) the change of point-of-attachment, that is, network-level handover.

Figure 4 is the timing diagram showing which procedures are performed when the IPv6 address is changed due to the pseudonym change. At t_0, P_i is expired and P_{i+1} is provided to generate a new IPv6 address at an interface. Then, at t_1, the new IPv6 address is generated. In order to use the newly generated IPv6 address for IPv6 ITS communications, it is required to check the IPv6 address uniqueness via the duplicate address detection (DAD) procedure, which is another time-consuming procedure. If the IPv6 address successfully passes the DAD procedure, it is ready to use at t_2. Then, the IPv6 address is used to send a registration message to its HA [9, 10].

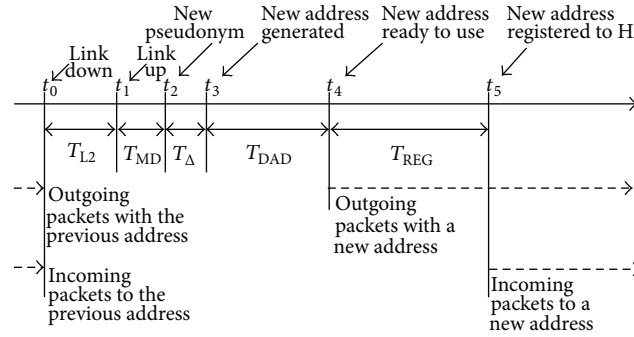
As shown in Figure 4, during the time for the DAD procedure T_{DAD}, outgoing packets are delayed until the DAD procedure is successfully completed. If the outgoing packets are for a session based communication, for example, TCP communication, the session can be disconnected due to the address change.

Figure 5 shows the time diagram on the procedures that occurred when the IPv6 address changed due to the network-level handover [9, 10]. At t_0, the link switch occurs and



- T_Δ: time required to generate a new address at an interface
- T_{DAD}: time required to perform a duplicated address detection (DAD)
- T_{REG}: time required to register the new address to the home agent (HA)

Figure 4: Pseudonym change due to the pseudonym expiration.



- T_{L2}: time required to perform the link-layer handover, link switching time
- T_{MD}: time required to detect the handover at the network level
- T_Δ: time required to generate a new address at an interface
- T_{DAD}: time required to perform a duplicated address detection (DAD)
- T_{REG}: time required to register the new address to the home agent (HA)

Figure 5: Pseudonym change due to the network-level handover.

ends at t_1. As the link is changed, the movement detection time is required at the IPv6 layer. Then, as its movement is detected, P_{i+1} is supplied to generate the new IPv6 address at an interface at t_2. The remaining procedures are the same as for the case described in Figure 4.

5. Quantitative Analysis

A pseudonym change badly influences communication performance as it yields the IPv6 address change during IPv6 communications. If a pseudonym change interval is long, the privacy exposure time increases. On the other hand, if the pseudonym change interval is short, the overhead due to frequent pseudonym changes increases. Accordingly, an algorithm that finds an optimal pseudonym change interval for making a balance between communication overhead and location privacy is needed.

Figure 6 shows a timing diagram for modeling the privacy exposure time, which is defined as the time until a new pseudonym is set. The following are the used notations with explanations:

(i) t_0: subnet enter (come-in) time,

(ii) t_3: subnet leave (come-out) time,

(iii) $t_s = t_3 - t_0$: subnet residence time,

(iv) t_1: current observation time,

(v) t_2: new pseudonym update time,

(vi) T_r: pseudonym change interval.

With the timing diagram, we model the privacy exposure time and develop the optimal pseudonym change algorithm. After the observation starts at t_1, a pseudonym is changed (updated) either at t_2 by a periodical pseudonym change or at t_3 by a handover. Therefore, the privacy exposure time z is given by

$$z = \min\{z_1, z_2\}, \tag{3}$$

where $z_1 = t_2 - t_1$ $(0 < z_1 < T_r)$ and $z_2 = t_3 - t_1$ $(0 < z_2 < \infty)$. Then, the probability density function (PDF) of z is given:

$$f(z) = f_1(z) \int_z^{\infty} f_2(t)\, dt + f_2(z) \int_z^{T_r} f_1(t)\, dt, \tag{4}$$

where $f_1(z)$ and $f_2(z)$ are PDFs of z_1 and z_2, respectively.

Now, we need to find proper distributions for z_1 and z_2. The pseudonym change interval T_r is a constant and t_1 is a random observer time epoch. Therefore, z_1 follows a uniform distribution in $[0, T_r]$ and thus $f_1(z)$ is obtained as

$$f_1(z) = \frac{1}{T_r}. \tag{5}$$

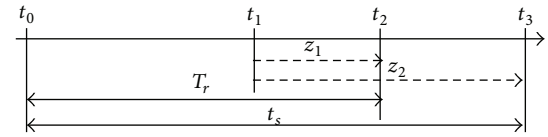


Figure 6: Diagram for the optimal pseudonym change interval.

On the other hand, if the subnet residence time t_s follows an exponential distribution with mean of $1/\mu_s$, $f_2(z)$ is calculated as

$$f_2(z) = \mu_s e^{-\mu_s z}. \tag{6}$$

Then, the PDF of z, $f(z)$, can be expressed as

$$\begin{aligned} f(z) &= f_1(z) \int_z^{\infty} f_2(t)\, dt + f_2(z) \int_z^{T_r} f_1(t)\, dt \\ &= \frac{1}{T_r} e^{-\mu_s z} + \mu_s e^{-\mu_s z} \frac{1}{T_r} (T_r - z). \end{aligned} \tag{7}$$

From (7), the Laplace transform of $f(z)$, $f^*(s)$, can be obtained and the expected privacy exposure time, $E[z]$, can be obtained from $E[z] = (d/ds) f^*(s)|_{s=0}$.

Suppose a vehicle generates packets with rate λ_p (packets/sec). Let N denote the expected number of packets influenced by the privacy exposure. Then, N is calculated as

$$N(T_r) = \lambda_p \times E[z]. \tag{8}$$

Intuitively, $N(T_r)$ increases with the increase of T_r. Therefore, the optimal value of T_r can be obtained from the following problem:

$$\begin{aligned} &\text{maximize} \quad T_r \\ &\text{subject to} \quad N(T_r) \le \Theta. \end{aligned} \tag{9}$$

That is, the optimal value of T_r is the maximum value of T_r while $N(T_r)$ does not exceed a predefined threshold value Θ. Note that Θ should be determined depending on the application type, security level, and vehicle's mobility.

Figure 7 shows $N(T_r)$ as T_r increases. With the increase of T_r, the pseudonym is infrequently updated and more packets can be affected by the privacy exposure. In addition, it can be found that low μ_s leads to the increase of $N(T_r)$. This is because low μ_s or low mobility reduces the number of pseudonym changes due to subnet movements. Figure 7 can be used to determine the optimal T_r. For example, when μ_s and T_r are set to 1.0 and 9, respectively, $N(T_r)$ is 8.89. On the other hand, when T_r becomes 10, $N(T_r)$ exceeds 9.00. Therefore, if the threshold (or upper limit) on $N(T_r)$, that is, Θ, is given by 9.0, the optimal T_r should be less than 10. From Figure 7, it can be shown that a larger T_r can be set when μ_s is high under the same threshold Θ. This can be explained as follows. If μ_s or mobility is high, the pseudonym can be frequently updated by subnet changes. Hence, a longer T_R is allowed to save the pseudonym update cost in such a situation.

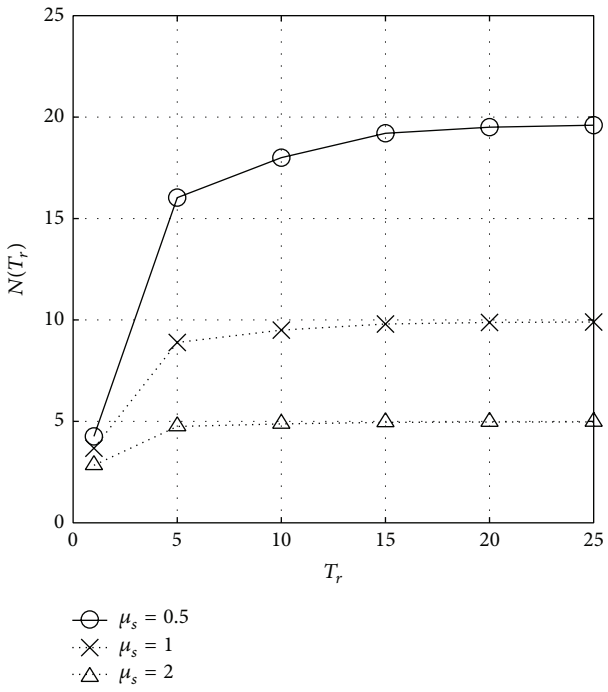


Figure 7: Effect of μ_s and T_r ($\lambda_p = 10$).

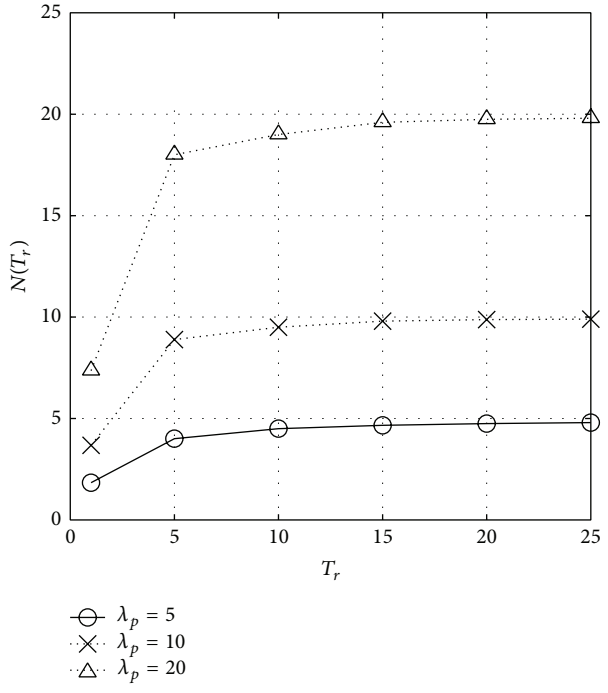


Figure 8: Effect of λ_p ($\mu_s = 1$).

Figure 8 shows the effect of λ_p. Intuitively, when λ_p is large, more packets can be affected by the privacy exposure. Due to this reason, a smaller T_R should be set when λ_p is large as shown in Figure 8.

6. Conclusions

As IPv6 is considered as a main communication protocol for accessing the Internet during driving, location privacy at the IPv6 layer is becoming an important issue in cooperative ITS. In this paper, we have presented an IPv6 address configuration with pseudonyms and then studied a performance degradation issue due to the pseudonym change at the IPv6 layer. We moreover proposed the optimal pseudonym change algorithm that adaptively finds an optimal pseudonym change interval with given parameters.

Disclosure

A preliminary version of this paper was presented at IEEE Intelligent Vehicles Symposium Workshops 2012 [6].

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2014R1A1A1006770 and NRF-2014K1A3A1A21001357).

References

[1] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55, 2003.

[2] J.-H. Lee and T. Ernst, "IPv6 security issues in cooperative intelligent transportation systems," *The Computer Journal*, vol. 56, no. 10, pp. 1189–1197, 2013.

[3] J.-H. Lee, T. Ernst, and J.-M. Bonnin, "Cross-layered architecture for securing IPv6 ITS communication: example of pseudonym change," in *Proceedings of the 3rd International Workshop on Cross Layer Design (IWCLD '11)*, November 2011.

[4] E. Fonseca, A. Festag, R. Baldessari, and R. L. Aguiar, "Support of anonymity in VANETs—putting pseudonymity into practice," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '07)*, pp. 3402–3407, Hong Kong, March 2007.

[5] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: why simple pseudonym change is not enough," in *Proceedings of the IEEE/IFIP International Conference on Wireless On-Demand Network Systems and Services (WONS '10)*, pp. 176–183, February 2010.

[6] J.-H. Lee, J.-M. Bonnin, F. Garcia, and A. F. Skarmeta, "Use of pseudonyms in IPv6 ITS communication: performance degradation and exposure new identity with security protocols," in *Proceedings of the IEEE Intelligent Vehicles Symposium Workshops*, June 2012.

[7] ISO, "Intelligent transport systems—communications access for land mobiles (CALM)—architecture," ISO 21217, International Organization for Standardization, London, UK, 2010.

[8] European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Communications Architecture," ETSI EN 302 665 V1.1.1, September 2010.

[9] ISO 21210, *Intelligent Transport Systems—Communications access for Land Mobiles—IPv6 Networking*, 2011.

[10] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network mobility (NEMO) basic support protocol," RFC 3963, IETF, 2005.

[11] K. Dar, M. Bakhouya, J. Gaber, M. Wack, and P. Lorenz, "Wireless communication technologies for ITS applications," *IEEE Communications Magazine*, vol. 48, no. 5, pp. 156–162, 2010.

[12] ETSI TS 102 636-6-1 v1.1.1, *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols*, 2012.

[13] European Telecommunications Standards Institute, "Analysis of IPv6 for networking," ETSI TR 101 555, European Telecommunications Standards Institute, 2012.

[14] ISO 16788, "Intelligent transport systems—communications access for land mobiles—IPv6 networking security," 2012.

[15] ISO 16789, *Intelligent transport systems—Communications access for land mobiles—IPv6 Networking Optimisation*, 2012.