ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/4140284

Enhancing wireless location privacy using silent period

Conference Paper · April 2005

DOI: 10.1109/WCNC.2005.1424677 · Source: IEEE Xplore

CITATIONS
276

READS
823

4 authors, including:

Leping Huang
asdfad
20 PUBLICATIONS **1,050** CITATIONS

SEE PROFILE

Kaoru Sezaki
The University of Tokyo
317 PUBLICATIONS **4,581** CITATIONS

SEE PROFILE

All content following this page was uploaded by Kaoru Sezaki on 25 February 2015.

The user has requested enhancement of the downloaded file.

Apple EX1042
Apple Inc. v. Secure Comm. Techs., LLC
IPR2026-00445

Enhancing Wireless Location Privacy Using Silent Period

Leping Huang*†, Kanta Matsuura†, Hiroshi Yamane†, and Kaoru Sezaki†
*Nokia Research Center Japan, Arco Tower 17F, 1-8-1, Shimomeguro, Meguro-ku, Tokyo, 153-0064, Japan, +81-3-5437-3613
†Institute of Industrial Science, University of Tokyo, 4-6-1 Komaba, Meguro-ku, Tokyo, Japan, +81-3-5452-6266

***Abstract*— The advance of ISM-band radio-based tracking systems (for example, wireless LAN-based tracking system) extends the application of location-based services (LBS), but it also threatens to allow the movement of users to be tracked whenever they are transmitting frames. Several protection methods based on periodical address updates have already been proposed. However, new correlation attacks, which utilize the correlation between the old and new addresses of the same node, can defeat current protection methods. To combat such attacks, we propose the concept of a silent period. A silent period is defined as a transition period between the use of new and old pseudonyms, when a node is not allowed to disclose either the old or the new address. Through analysis, we find that a silent period should contain a constant period and a variable period. The effect of the constant period is to mix the spatial relation between the node's disappearing points and emerging points. The variable period mixes the temporal relation between the node's disappearing times and emerging times. In addition, we evaluate the performance of silent period through simulation. Simulation results show that silent period proposal significantly reduces the duration of time a node can be tracked continuously. Finally, we denote that there are still many open research problems before random address can be implemented to protect wireless location privacy. Silent period protocol is the first step for us to realize random address in wireless location privacy protection.**

I. Introduction

Recent technological advances in wireless location-tracking present unprecedented opportunities for monitoring the movements of individuals. While such technology can support many useful location-based services (LBSs), which tailor their functionality to a user's current location, privacy concerns might seriously hamper user acceptance. Within those technologies, the positioning technologies using short-range radio such as Bluetooth and Wireless LAN receives great attention recently. Due to the short range characteristics of those radios and the advance of tracking technology, tracking system based on them [1], [2], [3] achieves very high accuracy up to one meter. However, some of short-range radio based tracking systems track users' movement by eavesdropping their communication, and do not need any cooperation or approval from users. We believe that such eavesdropping-based tracking system may cause serious location privacy problem.

Our motivation of this research is to provide better protection on user's location privacy to those eavesdropping-based location tracking attack. Our major contributions in this paper are (1) we identified a new wireless location privacy attack–correlation attack–in the context of wireless LAN system, and (2) we provided a solution–silent period–to defeat this attack. The remainder of the paper is organized as follows. Section II provides background and prior arts in the field of location tracking and privacy protection. In Sec.III, we first define a wireless LAN communication and tracking framework to be used throughout this paper, and then evaluate the location privacy risks in it. In Sec. IV, we propose our privacy protection algorithm silent period and its effect to alleviate address's temporal and spatial relations. The simulation results are presented in Sec. V. Section VI discusses some open issues in wireless location privacy. Finally, we conclude the paper in Sec.VII with a discussion of proposed future work.

II. Background and Prior Arts

There are various approaches for estimating the location of a mobile nodes. Those methods can be classified by signal metric as AOA(angle of Arrival), RSS(Received Signal Strength), TOA(Time of Arrival), or by metric processing as triangulation and pattern matching. TOA and triangulation-based system developed by Hitachi Ltd. achieves accuracy of about 1 meter, while RSS and pattern match based method developed by Guvenc[4] achieves an accuracy of about 3 meters. Such high precision tracking system may harm user's location privacy in the future. To protect user from potential threat, there are several research results in Bluetooth and Wireless LAN respectively.

In Bluetooth, there is a need to prevent location tracking using Bluetooth MAC address, channel access code (CAC), device access code (DAC), or a hopping sequence. Since all these parameters are determined by the device address, they can be used to perform different types of location tracking. Bluetooth SIG proposed *anonymity mode* to combat such attack in its latest draft[5]. A Bluetooth unit in anonymity mode combats location tracking by regularly updating its active device address. The active device address is used in all communications. After the standard authentication procedure, a node can show its own permanent (private) address to its authenticated pair.

Similar approach are also proposed in Wireless LAN. Recently, Gruteser and Grunwald have worked extensively on protecting location privacy in wireless LANs. They presented a middleware architecture and algorithm to adjust the resolution of location information along spatial and temporal dimensions [6], and enhanced location privacy by frequently disposing of

a client's interface identifier [7], [8]. They propose updating the node's interface identifier whenever a station associates to a new access point. From their experiment, a node associates with a new access point once every approximately 30 minutes. They assume that an attacker may comprise some of the access points, and may track a user's movements based on the information with which the access point user is associated. Location-tracking methods that measure the RSSI and/or the TOA of frames are not considered attacking methods in their paper. However, RSSI/TOA-based tracking methods have much higher tracking accuracy than those that only analyze association logs in the access point (AP), and are stronger threats to location privacy. We should not ignore such an attack when providing location privacy protection.

In the other hands, the provision of anonymity and pseudonymity has been studied extensively in the context of anonymous communication. In the 1980s, Chaum [9] worked extensively to develop techniques for secure, untraceable electronic transactions over fixed networks. They introduced the novel mix network, which is a set of servers that serially decrypt or encrypt lists of incoming messages. These are sent out in a random order, in such a way that an attacker cannot correlate output message with input messages without the aid of mixer nodes (when several messages are passed simultaneously). Other important proposals to establish such anonymous communication channel include Onion Routing[10], Crowds[11], and Anonymizer [12]. Most of these try to provide either sender/receiver anonymity, or unlinkability between sender and receiver.

To protect location privacy, Beresford and Stajano have proposed the concept of the mix zone [13] based on Chaum's mix network. They assumed LBS application providers are hostile adversaries, and suggested that application users hide their own identifier from providers. A mix zone for a group of users is defined as the largest connected spatial region in which none of the users in the area have registered an application callback. Because application providers do not receive any location information when users are in a mix zone, their identities are "mixed". Beresford and Stajano also point out a problem with the frequent pseudonym update method when the spatial and temporal resolution of the location-tracking system is high. They claim that it will be possible to find a strong correlation between a trail left by an old address and that left by a new address, as a device can now be positioned accurately. The old and new address can therefore be linked to defeat the frequent pseudonym update approach. They propose using the mix zone when a pseudonym is updated. Assuming users change their identity to a new and unused pseudonym whenever they enter a mix zone, applications that see a user emerging from the mix zone cannot distinguish that user from another who was in the mix zone at the same time. Therefore, the application provider cannot link people going into the mix zone with those coming out of it. The mix zone works well to protect a user's location from an application provider, but it is doubtful whether this technique is also effective when the attacker is a malicious eavesdropper of the communication channel. Unlike an application provider, an eavesdropper tracks user's movement by locating where a user transmits a frame, instead of reading the location information contained inside the frame. From an eavesdropper's point of view, location information is disclosed continuously whenever the user is transmitting frames. If the eavesdropper is instead considered the adversary in the mix zone, the mix zone now only includes areas where no node sends any frames. In wireless communication, this requirement means it is necessary to deploy anechoic chambers to restrict users' communication with external nodes. It is infeasible to deploy as many chambers as required to provide location privacy protection.

III. Framework and Privacy Analysis

A. System Model

The system described in this paper is composed of four types of node: authentication server (AS), access point (AP), station (STA), and eavesdropper (E). Access point, station and eavesdropper nodes are incorporated with wireless LAN radio interfaces operating at identical frequencies. In commercial hotspot wireless LAN services, users of STA nodes always contract with one service provider. This service provider controls at least one AS. The area around users may be covered by other APs not controlled by the station's contracted service provider. The eavesdropper is capable of working in sniff mode, where it can capture all frames transmitted in the channel within its proximity. In addition, it is assumed that the wireless LAN interface in the eavesdropper is capable of providing a radio signal strength indication (RSSI) or time of arrival (TOA) for the eavesdropper's upper layer to estimate the STA's current position. We also assume that all regions that the STA may visit are covered by at least three eavesdroppers.

We illustrate the system architecture in Fig. 1. Before data communication, STA1 first authenticates with AP1 by utilizing the authentication information stored in AS. After authentication, the STA communicates with the external network via AP1. When STA1 moves to the area covered by AP2, it should reauthenticate with AP2 using AS. STA1 is then within the proximity of three eavesdroppers (E1, E2, and E3). Eavesdroppers monitor the movement of the STA continuously by measuring the RSSI and/or the TOA information of each frame sent by STA1.

B. Privacy Risks for Wireless LANs

Generally, a location privacy threat occurs when an untrusted party can locate a transmitting device and identify the subject using the device. A wireless LAN network poses very serious location privacy threats for the following reasons.

Shared Channel Radio: The MAC layer of 802.11 is based on CSMCA/CD, which requires all stations in its proximity to share the same communication channel. Any node can overhear all frames sent by others within its proximity.

Unsecured Frame Header: The format of the 802.11 MAC frame is shown in Table I. The encryption algorithms of 802.11 (AES and WEP) provide data confidentiality only for the frame body field of the frame; header and tail fields are sent in plain

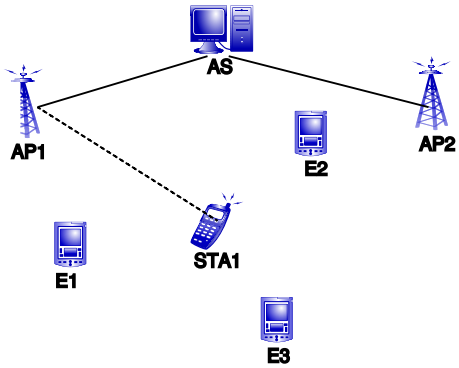

Fig. 1. System Architecture

TABLE I
802.11 MAC FRAME FORMAT

2	2	2	6	6	2	6	0-2312	4
Frame Control	Dur. /ID	A1	A2	A3	Seq. Control	A4	Frame Body	FCS

text. Considering the shared channel characteristics of 802.11 radios, it is obvious that the station understands the sender address (field A1) and receiver address (field A2) of all frames sent by nodes within its proximity. This opens the possibility for an adversary to monitor the movement of a station without its cooperation.

Frequent broadcast of MAC address: An eavesdropper can capture the MAC address of all frames sent in its proximity. If the sender transmits frames continuously, an eavesdropper can obtain the identity of the sender regularly. Continuous reception of the frame identity improves the accuracy of the tracking system. Maximum MAC address broadcast frequency can be derived by calculating the time to transmit one IP frame (containing only an IP header) from one station to the AP. The operation rate of 802.11 used here is 11Mbps DSSS/CCK in short-preamble mode. The procedure of frame transmission is as follows. STA first sends an IP frame with T_{data} μs, and the AP sends back an acknowledgment with T_{ack} μs, after waiting for the SIFS (short inter-frame space) to avoid frame collision. The station then waits for the SIFS again before being ready for the next transmission. SIFS is 10 μs in 802.11b. The round trip time(RTT) of transmitting one frame is shown in Eq. 1. Therefore, the eavesdropper will receive the identity of sender at a frequency up to 5KHz. In general, more frequent identity broadcasting improves the location-tracking accuracy.

$$\begin{aligned} RTT &= T_{data} + SIFS + T_{ack} + SIFS \\ &= (96\mu s + 54 \times 8/11\mu s) + 10\mu s \\ &\quad +(96\mu s + 14 \times 8/11\mu s) + 10\mu s \\ &\cong 262\mu s \end{aligned} \tag{1}$$

High tracking accuracy: The radio signal properties of a WLAN system allow relatively precise determination of a client's position. When an access point receives a signal from a client, it is highly probable that the client's position will be within a typical range of the AP (say, 100 meters). As discussed in Sec.II, tracking accuracy can be further improved to the order of 1 meter by triangulation or pattern matching methods.

Low-cost wireless LAN radio: It is relatively inexpensive to deploy enough wireless LAN nodes to cover large areas for location tracking, compared with covering the same area with a cell-based tracking system. This non-technical reason also greatly increases the risk to location privacy in wireless LANs.

TABLE II
NOTATIONS AND TERMINOLOGY

Terminology	Explanation
DT_n	Latest time when the tracking system monitored node n with its old pseudonym
DP_n	Last location where the tracking system monitored node n with its old pseudonym
ET_n	Earliest time when the tracking system monitored node n with its new pseudonym
EP_n	First location where the tracking system monitored node n with its new pseudonym

C. Correlation Attack

We assume that the clocks of eavesdroppers are synchronized. Eavesdroppers measure the RSSI/TOA of frames received from a specified STA to estimate its position. Frequent broadcasts of the MAC address provide adequate temporal and spatial tracking accuracy. STA uses the same periodical pseudonym update approach as that specified in the Bluetooth anonymity mode. With enough temporal and spatial precision, it may be possible for an adversary to correlate two pseudonyms that are sent separately from the same device moving through space. Temporal correlation may be used because the period with which stations change their pseudonym may be small. Spatial correlation may be used if it is assumed that a station will generally continue in the same direction, with the same speed as it traveled in the past. Such correlation attacks become easier as the distance between devices increases, as the speed of a device decreases, and as the accuracy with which a device may be located increases.

An example is shown in Fig.2. The definitions of disappearing time (DT), disappearing place (DP), emerging time (ET), and emerging place (EP) can be found in Table II. Assuming that the system provides enough temporal and spatial precision, a node coming from the right with identity A updates its identity to A' at some time within $[DT_1, ET_1]$. The last trail monitored by the system for A is recorded at time DT_1 and position DP_1; the first trail monitored by the system for A' is recorded at time ET_1 and EP_1. The objective of an adversary is to link A with A' with high probability by using knowledge such as the tracking history for A, a user movement model, or a building layout. From the similarity between both the times and locations of the two records, the tracking system can infer that node A changed its address to A' sometime between $[DT_1, ET_1]$ and near the position $[DP_1, EP_1]$.

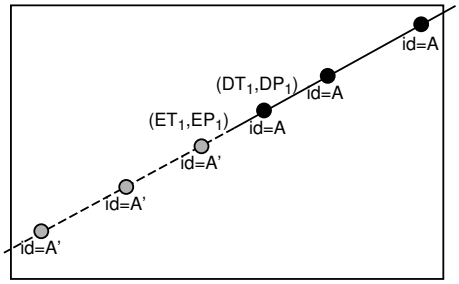

Fig. 2. The correlation attack on periodical pseudonym updates

IV. Silent Period

To combat the correlation attack discussed in the previous section, we propose the new concept of a silent period. The silent period is defined as a transition period between using new and old pseudonyms in which a station is not allowed to disclose either the old or the new pseudonym. As a result, the silent period introduces ambiguity into the determinations of the time and/or place at which a change of anonymous address occurred. This makes it more difficult to associate two separately received pseudonyms with the same station, because the silent period disrupts the temporal and/or spatial correlation between two separately received pseudonyms and obscures the time and place where a pseudonym changed.

When multiple stations within the same region follow the rule of the silent period by ceasing transmission after updating their MAC address (pseudonym), the effect is the same as if those nodes had entered a mix zone in which no user's movement could be monitored by the system. Therefore, the silent period can be seen as an extension or implementation of the mix zone concept. It creates virtual mix zones by controlling the transmission of frames.

An example using the silent period is shown in Fig. 3. In the figure, node 1 moves along a path from the upper right corner to the lower left corner. Meanwhile, node 2 moves along a path from the lower right corner to the upper left corner. Both nodes update their addresses and then enter the silent period. The effects of the proposal are illustrated near the intersection of the path of both nodes. The silent period is illustrated as a rectangle in the center of this graph. Node 1 arrives at the border of the silent period at time DT_1 and position DP_1, and node 2 arrives at time DT_2 and position DP_2. Here we assume that two nodes arrive at the border simultaneously ($DT_1 = DT_2$). Both node 1 and node 2 disable frame transmission for a silent period. After the silent period, nodes 1 and 2 restart frame transmission. The tracking system monitors a new trail with address A' emerging at position EP_1 and time ET_1, and another new trail with address B' emerging at time ET_2 and position EP_2. The tracking system knows that node 1 changed its address within the silent period. However, as it detects that two new address A' and B' emerge after the silent period, the tracking system cannot determine whether node 1 changed its address to A' or B', because both position EP1 and EP2 are reachable by node 1 from position DP_1, due to the

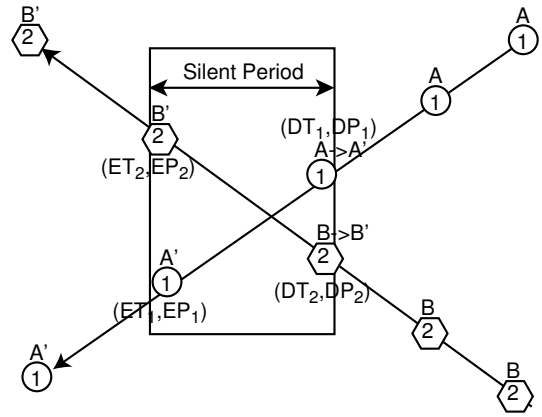

Fig. 3. Illustration of the movement of two stations, node 1 and node 2, which both use a silent period

silent period introduced during the moving time. This method obscures the temporal and spatial correlation between new and old pseudonyms by "mixing" the pseudonyms of nodes.

The discussion above assumes that nodes 1 and 2 switch their addresses at the same time for the sake of simplicity. The length of the silent period is assumed implicitly constant and identical for all nodes. However, when the address update time is not synchronized between nodes, the constant length of the silent period may not effectively mix the pseudonyms of nodes. This is because when the length of the silent period is constant, the tracking system can link the old and new pseudonyms to the same node. It does this by comparing the order of the emerging times of the two nodes (with their new pseudonyms) with the disappearing time of those with the old pseudonyms. As shown in Fig. 3, if the tracking system knows that node 1 with identity A enters the silent period at a time DT_1 (earlier than node 2), it can infer that the emerging time of node 1 is earlier than that of node 2. When the system detects that a node with identity A' emerges earlier than another node with identity B', the system can easily infer that node 1 updates its address to A'.

To solve this problem, we propose the use of a variable length silent period. If the range of the emerging time of a node overlaps with that of another node, the tracking system cannot link the detected pseudonym to the correct node. We illustrate the idea of a variable-length silent period in Fig. 4. The silent period is determined by a random variable varying within the range $[T2_{min}, T2_{max}]$. When the ranges of the emerging times of two nodes overlap, the temporal relation between the emerging time and the disappearing time of the two nodes is obscured. The tracking system cannot correctly link the new pseudonym of a node to its old pseudonym. This approach is motivated by the CSMA/CD medium-access control algorithm used in collision-avoidance schemes.

In summary, the silent period should contain constant and variable periods. The effect of the constant period is to mix the spatial relation between a node's disappearing points and its emerging points, while the effect of the variable period is to mix the temporal relation between the node's disappearing times and its emerging times.

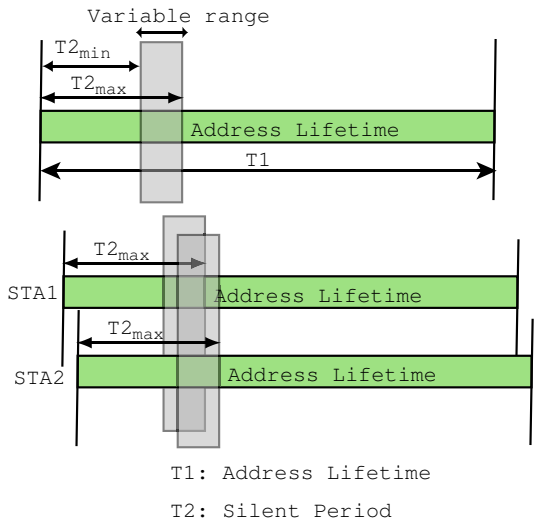

Fig. 4. Synchronization issues in silent networks. Anonymity is guaranteed when the variable periods of Silent Period overlap

V. Simulation Result Analysis

We have conducted preliminary simulations to evaluate the performance of our proposal. In the simulation, some nodes are put in a $20m \times 20m$ 2-dimensional area. All nodes moves within simulation area by following random walk mobility model. Adversaries track users with a simple tracking method as described below.

Assuming that tracking system knows the length of nodes' silent period $T_{speriod}$, and the maximum velocity of nodes v_{max}. We classify that all nodes involved in the location-information protection system into two types, target and mixer. Target is defined as a node whose privacy system is measuring. All other nodes that involved in this system are defined as mixers. Mixers contribute to the privacy of target by restricting frame transmission for silent period of time to obscure the temporal and spatial relation between their and target's pseudonyms. Here, we use the terminology $P(N_i, t_j)$ to represent a trail of node N_i at position P taken at time t_j. From target's the last trail with old identifier T tracked at time t_1 $P(T, t_1)$, tracking system derive an area–which is called *reachable area* in this paper– that target may appear after the silent period. The reachable area is a circle centered at $P_T(t_1)$, and with radius $v_{max} \times T_{speriod}$. Adversaries associates one unobserved identifier in that area to the target randomly. Consequently. if there are n nodes in the reachable area, the probability that target's old and new identifier can be associated correctly is $1/n$.

In the simulation, we measure how long a node can be tracked continuously. When all nodes update their address in a synchronized way, nodes' privacy level is independent to the length of address lifetime. In the other hand, address lifetime is linearly proportional to node's maximum tracking time(MTT). As a result, we use a new terminology Maximum Tracking Round(MTR) as measure to evaluate the performance of silent period. MTR is defined as the number of rounds that a node is tracked continuously after its *first* address update. Because

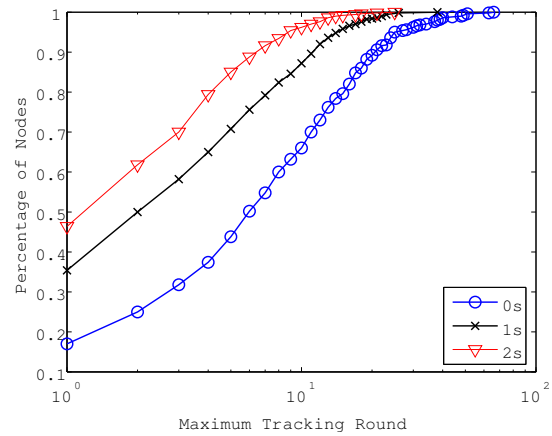

Fig. 5. Cumulative Distribution Function of Tracking Time

the node may start communication at any time before first address update, The maximum time that a node may be tracked continuously can be derived by the equation below.

$$MTT = (MTR + 1) \times Lifetime \tag{2}$$

Figure 5 shows how long an adversary can track nodes. MTR is plotted as a normalized cumulative distribution function with a logarithmic x-axis; that curve indicates the fraction of the sample population (y-axis) that can be observed for no more than a specified duration (x-axis). The '0s' curve describes an unprotected system, where no silent period occur after each address update. In this case, the adversary can track about half of all nodes for more than 6 rounds. In other words, if nodes update their address every 10 minutes, it means that half of nodes is tracked continuously for more than one 70 minutes. Only 7% of nodes are traced less than one round. In the other hand, silent period proposal significantly reduces the maximum tracking round. The '2s' curve describes a system, where nodes have two seconds silent period after each address update. In this system, less than half the nodes are tracked for more than 3 rounds, and about 28% of nodes are stalked less than one round.

VI. Discussion about Open Issues

It is a relatively new research approach to protect wireless location privacy by using randomized address. In this paper, we proposed silent period to control the interval between the use of new and old pseudonyms. This proposal alleviates the threat from correlation attack. We noticed that there are still some other unsolved issues before random address can be integrated into wireless communication protocols such as 802.11. Silent period protocol is the first step for us to realize wireless location privacy protection by random address.

A. Duplicate Address Detection

The first problem of random MAC is that node may select an address that is used by other nodes in the same radio coverage. Current wireless and wired LAN use 48-bit extended unique identifier(EUI-48) defined by IEEE to avoid such address duplication[14]. EUI-48 is a concatenation

of a 24-bit Organizationally Unique Identifier (OUI) value administered by the IEEE Registration Authority, and a 24-bit extension identifier assigned by individual organizations. Current 802.11 wireless LAN, Bluetooth, and Ethernet uses this EUC-48 address hierarchy to avoid same address be used by multiple nodes. When a random address is used, it is difficult to avoid the possibility of such address duplication. As a result, duplicate address detection (DAD) is a very important issue. Regarding to the wireless LAN, DAD algorithm should avoid duplicated address of nodes associated with same AP, and those associated with different AP but within same radio coverage. Several preliminary approaches may be used here. First, a station records the history of addresses used by others recently, and then avoids those addresses when updating its address. Secondly, an AP refuse address update request from STA, when it detects that this address is used by this BSS or neighboring BSS. We believe such simple algorithms cannot fully avoid address duplication perfectly, but may somewhat reduce collision probability. Some new address architectures, such as the spatial-temporal addressing architecture are discussed within our research group[15]. Similar approaches may be integrated into location privacy protection system to avoid address duplication.

B. Verifiable Address

The second problem of random MAC is that randomly selected address may open new security problem in MAC. For example, a malicious node can 'steal' the address that is currently used by a normal node in another management domain. As a result, this blocks the possibility of that normal node to handover into the management domain used by malicious node. A similar problem in IP layer has been discussed for a long time. Narten proposed the use of randomized IPv6 address in [16], while Dupont pointed out security problem of RFC 3041 in [17]. This is concluded as the address ownership problem. Several solutions like SUCV[18] and HIP[19] are proposed. We believe it will cause serious security problem if we don't consider the MAC address ownership problem when implementing randomized MAC address. However, some simpler and lighter protocols are preferred than current IP layer proposals because of the link local characteristics of MAC address, comparing with the necessity of globally unique IP address.

VII. Conclusion and Future Work

In this paper, we first evaluated the new risks imposed by high-accuracy location-tracking systems. A correlation attack is identified as a threat that cannot be defeated using existing periodical pseudonym update solutions. We proposed the new concept of a silent period to combat correlation attacks. Through analysis, we determined that the silent period should contain constant and variable periods. The effect of the constant period is to mix the spatial relation between a node's disappearing points and emerging points, while the variable period is used to mix the temporal relation between a node's disappearing times and emerging times. Simulations demonstrated the effectiveness of our proposal. Finally, we also discussed some open issues in location privacy research area. In the future, we plan to study the effect of many factors such as node density, address lifetime, tracking system accuracy on user's location privacy. We will also focus on the open issues raised in this paper.

Acknowledgment

Thank Dr. Tracy Camp and Toilers Group at Colorado School of Mines [20] for providing the source code of their mobility model.

References

[1] U. Bandara, M. Hasegawa, M. Inoue, H. Morikawa, and T. Aoyama, "Design and implementation of a bluetooth signal strength based location sensing system," in *Proc. of IEEE Radio and Wireless Conference (RAWCON 2004)*, Atlanta, U.S.A, 2004.

[2] Hitachi's air location. [Online]. Available: http://www.hitachi.co.jp/airlocation/

[3] P. Bahl and V. Padmanabhan, "Radar: an in-building rf-based user location and tracking system," in *Proc. of IEEE INFOCOM 2000*, vol. 2, Tel-Aviv,Israel, 2000, pp. 775–784.

[4] I. Guvenc, C. Abdallah, R. Jordan, and O. Dedeoglu, "Enhancements to rss based indoor tracking systems using kalman filter," in *Proc. of Intl. Signal Processing Conf.(ISPC)*, Dallas, TX, U.S., 2003.

[5] *Bluetooth 1.2 Draft 4*, Bluetooth SIG Std., 2003.

[6] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. of ACM MobiSys 2003*. San Francisco, CA, USA: USENIX, 2003, pp. 31–42.

[7] ——, "Enhancing location privacy in wireless lan through disposable interface identifiers: a quantitative analysis," in *Proc. of 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots(WMASH 2003)*, San Diego, CA, USA, 2003.

[8] ——, "A methodological assessment of location privacy risks in wireless hotspot networks," in *Proc. of 1st Intl. Conf. on Security in Pervasive Computing(SPC 2003)*, ser. LNCS, vol. 2802. Boppard, Germany: Springer, 2003.

[9] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.

[10] P. Syverson, G. Tsudik, M. Reed, and C. Landwehr, "Towards an analysis of onion routing security," in *Proc. of Workshop on Design Issues in Anonymity and Unobservability*, Berkeley, CA, USA, 2000.

[11] M. Reiter and A. Rubin, "Crowds: Anonymity for web transactions," *ACM Transactions on Information and System Security*, vol. 1, no. 1, pp. 66–92, 1998.

[12] Anonymizer. [Online]. Available: http://www.anonymizer.com/

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

[14] *48-bit Extended Unique Identifier*, IEEE Standard Association Std. [Online]. Available: http://standards.ieee.org/regauth/oui/tutorials/EUI48.html

[15] K. Yamazaki and K. Sezaki, "Spatio-temporal addressing scheme for mobile ad hoc networks," in *Proc. of IEEE TENCON 2004*, Chiang Mai, Thailand, 2004.

[16] T. Narten and R. Draves, "Privacy extensions for stateless address autoconfiguration in ipv6," RFC 3041, IETF, 2001.

[17] F. Dupont and P. Savola, "RFC 3041 considered harmful," draft-dupont-ipv6-rfc3041harmful-05.txt, IETF, 2004.

[18] G. Montenegro and C. Castelluccia, "Statistically unique and cryptographically verifiable (sucv) identifiers and addresses," in *Proc. of Network and Distributed System Security Symposium 2002 (NDSS2002)*, San Diego, CA, U.S., 2002.

[19] IETF host identity protocol wg. [Online]. Available: http://www.ietf.org/html.charters/hip-charter.html

[20] Toilers group. [Online]. Available: http://toilers.mines.edu/