Enhancing Location Privacy in Wireless Local Area Networks

Po-Jen Chuang, Jer-Sheng Deng, and Chih-Shin Lin
Department of Electrical Engineering
Tamkang University
Tamsui, Taipei County
Taiwan 25137, R. O. C.
E-mail: pjchuang@ee.tku.edu.tw

Abstract- *A desirable location privacy protection scheme is important for secure node communication in a wireless local area network (WLAN). By pausing transmission or updating nodes independently, a location privacy protection scheme can avoid deliberate adversary attack to prevent nodes from being tracked and transmitting information from being snapped. This paper first introduces an ID Tracking approach to show that nodes which swap IDs with other nodes in some existing location privacy protection schemes are actually easy to track. To improve the situation, i.e., to achieve better location privacy, we then propose a new (user-centric) location privacy protection scheme based mainly on local synchronization and independent ID update. With its special design of node ID switching, the new scheme is shown through experimental evaluation to give more enhanced location privacy than schemes which swap node IDs.*

Keywords: Wireless local area networks, location privacy protection, tracking approaches, user-centric, local synchronization, independent ID update, experimental performance evaluation.

1. Introduction

The advances of technology in recent years are shaping a ubiquitous world in which people can communicate with anyone on anything anywhere and anytime (4A). In such a technology-supported world, we can virtually obtain all needed information to facilitate our daily life through certain decisive technical infrastructures, including the wireless networks, mobile devices, sensors and radio frequency identification (RFID). The desired information is first collected by sensors and RFID, and then distributed through networks to people in any place at any time. In such an information-pervasive environment, maintaining the privacy of individual information becomes a particularly important issue.

The privacy problem associated with a wireless network, which plays a key role in shaping the above ubiquitous world, is the location privacy [1]. In a wireless network, the ID and location information of a node are linked together, thus some choose to protect the location privacy of a node by using pseudonyms to anonymize the node (and to generate useless location information), by processing the location information for the receiving end to get inaccurate values, or by unlinking a node's ID and location information. In the application layer, using pseudonyms may turn out unable to receive services due to authentication problems [2]. A more popular way to attain location privacy is to set policies acceptable to both sides [3]. In the network layer, the location information and user information can be separated by routing, e.g., [4] and [5] proposes a new protocol to separate the routing function and the identifying function of an IP address. In the data link layer, some attempt to provide anonymity through frequent switch of pseudonyms [6,7,8,9].

In this paper, we set our focus on achieving location privacy in the data link layer of a wireless local area network (WLAN). In a WLAN, when a node passes data down to the data link layer, the data are encrypted and transmitted in packets with headers, but headers are not encrypted [10]. After the physical address (or the MAC address -- simplified as ID in this paper) inside a header is sent out, the location of a node can be traced via triangulation, the received signal strength or the position of the signal source [6,8,9,11], and long term tracking of a node may lead to acquirement of users' information. Such is the location privacy problem in a WLAN. The global passive adversary (GPA) attack model, which has an adversary eavesdrop all communication packets, is assumed for a WLAN because its detecting devices can be small and everywhere. The main goal of this research is to enhance location privacy by reducing the influence of node tracking.

2. Background Study

2.1. The Mix Zone [7]

The authors in [7] attempt to solve the location privacy problem in wireless networks by using the Mix Zone [12] approach, which is based on the MIX concept in [13]. A Mix Zone is a predetermined area in which nodes will update their IDs but not access application services. Thus, when multiple nodes update their IDs and leave the Mix Zone, an adversary can not tell which node with the new ID is the original target node (i.e., the node under tracking). Involving multiple nodes to achieve the mixing and confusing effect is indeed the basic idea for most

location privacy protection schemes.

2.2. The Silent Period [6]

The Silent Period (SP) approach [6] makes use of the Mix Concept in [7] which confuses an adversary from tracking, and modifies it into a mechanism suitable for WLAN. In the SP mechanism, nodes will temporarily stop communication and update IDs during the timeframe. When multiple nodes update their IDs simultaneously, an adversary will get confused and unable to determine the target node. The location privacy of the target node is thus protected. The major problem for this approach lies in that the movement of a node during a short silent period usually forms a straight line which is likely to be tracked by an adversary through prediction and therefore incurs a high probability of location leaking.

2.3. Swing and Swap [8]

Two new ideas, Swing and Swap, are introduced in [8] to improve the SP mechanism. As mentioned, a node's trajectory during a short timeframe usually forms a straight line, and SP can not stop an adversary from tracking a silent target by route predicting based on such a "simple" movement. For improvement, [8] introduces two approaches, Swing and Swap. Swing maintains that SP should be executed only when velocity change happens and to increase the Mix effect, a local synchronization signal should be broadcast before the silent period to loosely synchronize the silent periods of neighboring nodes. Swap has nodes negotiate and decide what IDs are to be updated, and through exchange of IDs increases the number of mixed nodes to maximize location privacy.

3. The Proposed Location Privacy Protection Scheme

As stated in [8], a location privacy protection scheme should be user-centric, i.e., distributed. Location privacy gained by a distributed approach is nevertheless lower than that gained by a centralized approach which allows all nodes to update simultaneously. [8] thus adopts a local synchronization technique and an ID exchange approach (Swap) to increase location privacy for nodes. When Swap works with Simple Tracking (which tracks a target using the anonymity set constructed by the target's reachable area), the anonymity set will consist of all node IDs in the reachable area of the target and involved in the exchange process.

In this paper, we first use an ID Tracking approach to construct a set of exchangeable IDs, which along with the set of possible target IDs obtained by "the reachable area" of Simple Tracking constructs a more accurate anonymity set to facilitate the tracking of nodes using Swap, i.e., to challenge the location privacy of nodes using Swap. To improve Swap, our new location privacy protection scheme will put all involving nodes in an ID exchange process to generate a more intrigue anonymity set which even the proposed ID Tracking can hardly decode -- location privacy is thus enhanced.

3.1. The Proposed ID Tracking Approach

In Swap, an initiating node will exchange ID with only one of the cooperating nodes, i.e., only two nodes actually exchange IDs. This allows an adversary to acquire additional information and to construct the target's anonymity set accordingly, thus challenging the target's location privacy. In this section, we present an ID tracking approach able to track a cooperating node and also an initiating node in the Swap operation.

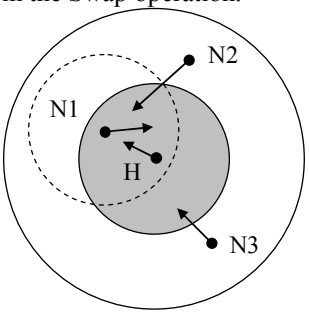

Figure 1. The Reachable Area of Initiating Node H and Cooperating Node N1.

3.1.1. Reducing the Location Privacy of a Cooperating Node. As mentioned in [8], an initiating node is indistinguishable from all cooperating nodes, but a cooperating node is indistinguishable only from the initiating node. A cooperating node will have only two possible IDs, the exchanged ID (of the initiating node) or its original ID. Thus when the target is a cooperating node, an adversary may easily locate it by looking into these two IDs. Figure 1 gives an example case. Assume the shaded inner circle is the reachable area of initiating node H, the outer circle (in which are cooperating nodes N1, N2 and N3) is the range of the local synchronization broadcast transmitted by H, and the dotted circle is the reachable area of N1. When N1 turns out the target, there will be three situations.

N1 and H are in the target's reachable area: If H exchanges its ID with N1 or N2, the IDs of N1, N2 and H are within target N1's reachable area. As cooperating nodes N1 and N2 can not exchange IDs with each other, the node with ID N2 obviously will not be the target. That makes the remaining two nodes (with IDs N1 and H) possible target candidates, each having 1/2 probability to be correctly tracked.

ID N1 stays in the target's reachable area, while ID H is elsewhere: Assume that H exchanges its ID with N3 and therefore IDs N1, N2 and N3 are in the target's reachable area. If the target exchanges IDs with initiating node H, ID H will appear within the reachable area of the target, indicating the target does not exchange IDs.

ID H is in target's reachable area, but ID N1 is elsewhere: Assuming initiating node H travels against the direction of the arrow, it will not appear in the reachable area of the target. If H exchanges IDs with the target, ID H will fall in the target's reachable area while the node with ID N1 will stay outside the area. One can thus conclude that the target exchanges IDs with H.

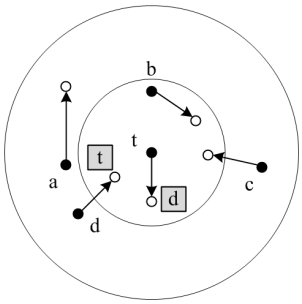

Figure 2. An Example of Exchanging Node IDs.

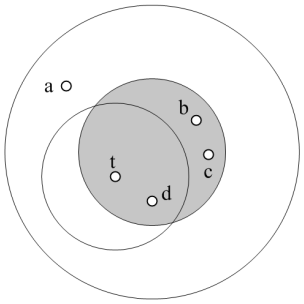

Figure 3. Node Locations after ID Update.

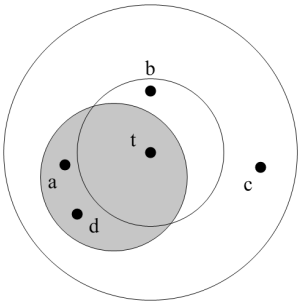

Figure 4. The Reverse Reachable Area.

As the above example indicates, if a cooperating node becomes the target, it will gain location privacy only when both its ID and the initiating node's ID are within its reachable area. To maximize the location privacy of a cooperating node, all cooperating nodes should be able to exchange IDs with one another.

3.1.2. Lowering the Location Privacy of an Initiating Node. Despite an initiating node is indistinguishable from all cooperating nodes, an adversary can still detect its location by tracing the relationship between exchanged IDs. As the initiating node and the cooperating node will start using each other's ID after ID exchange, an adversary may locate the initiating node's ID and trace back to find possible cooperating nodes (i.e., possible target nodes) which have previously exchanged IDs with the initiating node. The adversary, however, has to wait until the nodes finish their silent period and resume communication to pinpoint the node carrying the target's ID. The location and time of finding the node (carrying the target's ID) can be used to attain the set of possible exchanged IDs. As Figure 2 illustrates, the target is initiating node t and there are 4 cooperating nodes *a*, *b*, *c* and *d*. The black dots indicate nodes before ID update while the white dots are nodes resuming communication after ID update. Now suppose *t* exchanges ID with *d* and the exchanged IDs are in the shaded frame.

We first construct a set of possible target IDs using the reachable area of t (set A): When nodes resume communication, all node IDs within the reachable area of t become possible target IDs, which makes set A = {b, c, d, t} as Figure 3 shows.

After discovering the node with the target's ID, the location of the node can be used to determine a reverse reachable area, which will be a circular area centered by this node with a radius which is the exchange processing time multiplied by the maximum speed of this node (in Figure 3, the circular area centered by the node with ID t is the reverse reachable area). Using the location information of nodes during the exchange process, an adversary will conclude that nodes in this reverse reachable area may have exchanged IDs with the initiating node (i.e., the target) and get a set of possible IDs $B = \{a, d, t\}$ as shown in Figure 4.

Since the elements in both *A* and *B* are possible IDs of the target after the ID exchange process, it is easy to derive the anonymity set *C* by taking the intersection of *A* $\{b, c, d, t\}$and $B\{a, d, t\}$, and get $C = \{d, t\}$. The result is obtained based on the fact that an element not in *B* ($B' = \{b, c\}$) will not exchange IDs with the initiating node and therefore should be excluded from set *A* which is constructed from the reachable area of the initiating node. This example reveals that when the target is an initiating node, Simple Tracking holds a probability of 1/4 to pick up the correct target (by choosing 1 possible candidate out of 4 from set *A*); while our ID Tracking outperforms Simple Tracking by having the probability of 1/2 to make the right decision (i.e., choosing 1 out of 2 from set *C*).

3.2. The New Location Privacy Protection Scheme

In Section 3.1, we put ourselves in the view of an adversary and present an ID Tracking mechanism to track nodes using Swap in a more effective way. (Swap attempts to attain the mixing effect by exchanging IDs between two nodes whose relationship is yet easy to trace, thus failing to achieve maximum location privacy for a target.) In this section, we move forward to neutralize the performance of ID Tracking on Swap by having all involved nodes, not just two nodes, switch their IDs.

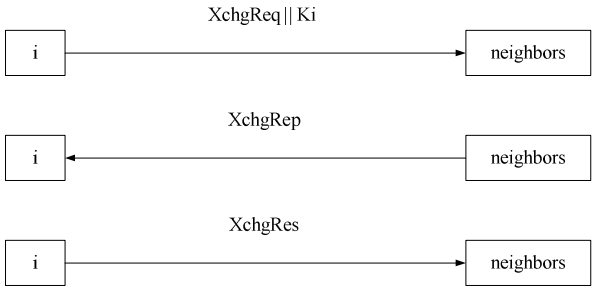

Figure 5. The Three-way Handshake in Our New Scheme.

3.2.1. The Switching Protocol of the New Scheme. Our new protocol uses a three-way handshake, like Swap, to decide each node's ID before it enters the silent state. When a node, say *i*, discovers its location privacy level is below its need and its velocity is changing, it will check the communication record to see if there is any neighbor node around. If there is, *i* will become an initiating node and start the ID switching process specified in Figure 5, which includes the exchange request phase, the exchange reply phase and the exchange result acknowledge.

The Exchange Request Phase (XchgReq): Initiating node *i* sets its transmission power to meet the need of a

local synchronization broadcast and sends out an exchange request (Xchg_Req)=$sign_i\{ID_i, tstamp_i\}$ and its public key (K_i).

The Exchange Reply Phase (XchgRep): A neighbor receiving the request responds by sending (Xchg_Rep)= $E_{Ki}(sign_n\{ID_i, rep_n, nounce_n, tstamp_n\} \parallel K_n)$ back to the initiating node. The message includes the ID of initiating node i (ID_i), the neighbor's reply (rep_n), a nonce and the neighbor's public key K_n. The ID of initiating node i is sent for i to validate XchgRep. The content of the reply depends on the neighbor's location privacy level: If it is lower than the desired level, "accept" the request; otherwise, "reject" it. The one time value nonce is created for initiating node i to notify the exchange result. The content of the reply message is timestamped and encrypted by the neighbor's private key for the purpose of validation and authentication, and the encrypted content along with the neighbor's public key is encrypted by the initiating node's public key for confidentiality purpose. This message is then returned to initiating node i.

The Exchange Result Acknowledgement Phase (XchgRes): Initiating node i will wait for a certain period of time to receive exchange replies from its neighbors, and then decrypt a neighbor's reply with its private key to get $sign_n\{ID_i, rep_n, nonce_n, tstamp_n\} \parallel K_n$. In the reply, the contents of ID_i, rep_n and $nonce_n$ can be decrypted by the neighbor's public key K_n. Combined with the neighbor's ID_n (known when the neighbor replies), the obtained information will help decide the exchange outcome.

Initiating node i also generates its $nonce_i$, thus having the ID-nonce pair for each neighbor node which has sent a reply. ID exchange is then conducted by assigning a new ID-nonce pair for each node. The initiating node will randomly assign a nonce to an ID. If the reply of a neighbor x is "reject", its ID_x and $nonce_x$ are to be paired together. Initiating node i then uses its private key to timestamp and encrypt the result and sends the formed exchange result message Xchg_Res = $sign_i\{ID_1, nonce_1,\ldots, ID_x, nonce_x, tstamp_i\}$ to the neighbors. After receiving the exchange result, a neighbor can use the initiating node's public key (attained in the exchange request phase) to decrypt the message and to find its nonce and the switched new ID.

3.2.2. The Algorithm of the New Scheme. The algorithm of a node using the new scheme is illustrated in Figure 6. A node will listen for any Xchg_Req and respond to it according to its location privacy level. With enough location privacy, it will respond by "reject" and return to its initial state. Without enough location privacy, it will check its own velocity change over the next SP_{MAX} time: If there is no velocity change, respond by "reject" and return to its initial state; if there is velocity change, respond by "accept" or "reject" in the Xchg_Rep and cooperate in the ID switching process.

Without receiving any Xchg_Req, a node may move to check its location privacy level, velocity change and neighborhood. If all requirements are met (i.e., if the location privacy level is less than desired, there is velocity change and neighbor nodes are present), the node itself becomes an initiating node to broadcast the Xchg_Req message. If the requirements are not all met, the node then goes back to its initial state.

Under the operation of the three-way handshake protocol, a node (whether an initiating node or a cooperating node) will get a new ID from the exchange result, go into the silent state immediately, and update its ID into the exchanged new ID. Each node will decide the length of its silent period which must be long enough to cover the time when it changes velocity. After the silent period, the node resumes communication and returns to the initial state listening for Xchg_Req.

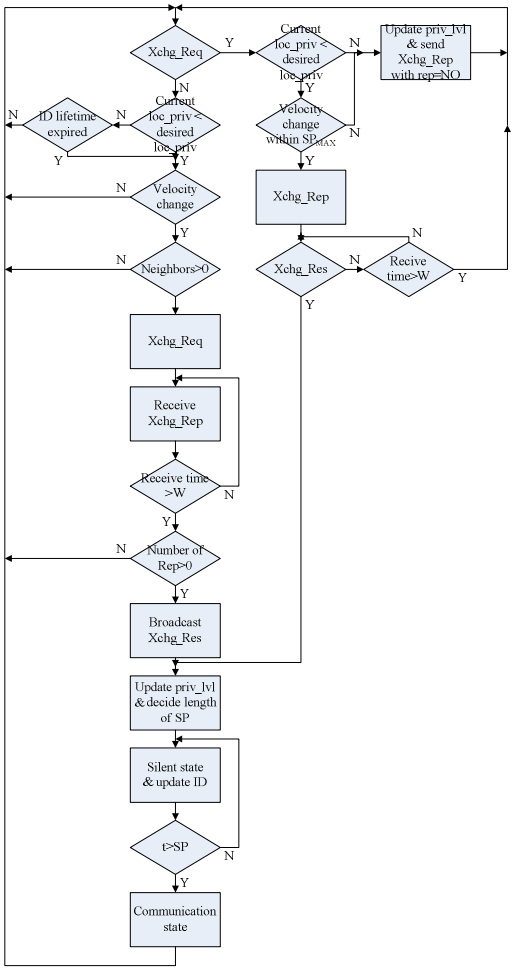

Figure 6. The Flowchart of a Node Using the New Scheme.

3.3. Evaluation on the New Scheme

In our scheme, the initiating node and cooperating nodes all get a chance to switch IDs, i.e., all nodes that are involved in the switching process will mix together. The relationship between these nodes gets so interwoven that even our ID Tracking approach can hardly untangle or track it. Take the nodes in Figure 1 as an example. Under our new location privacy protection scheme, as all nodes in the reachable area of cooperating target N1 will get a chance to switch IDs, it will be hard for an adversary to rule any nodes with switched new IDs out of the anonymity set. On the other hand, if the target is an initiating node, it may not carry the ID of the cooperating

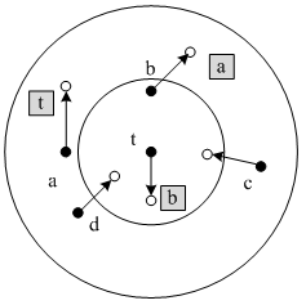

Figure 7. An Illustration of Nodes Switching IDs

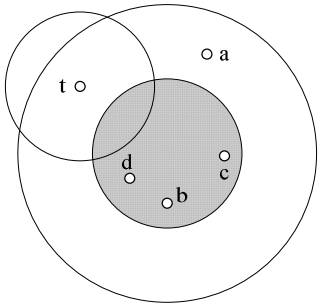

Figure 8. An Illustration of the Node after ID Update.

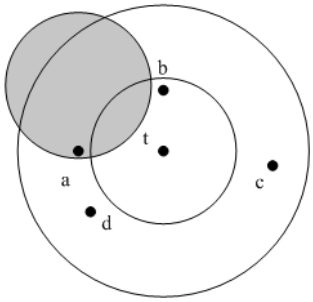

Figure 9. An Illustration of the Reverse Reachable Area.

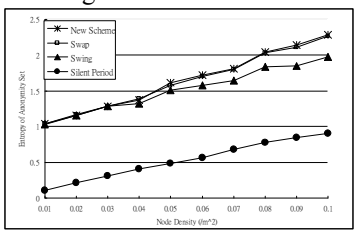

Figure 10. Performance of Various Schemes Under Simple Tracking.

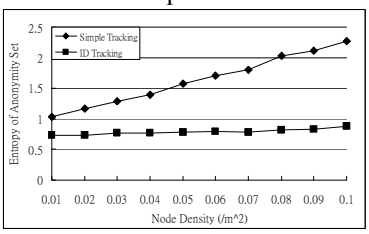

Figure 11. Entropy for Swap under Simple Tracking and ID Tracking.

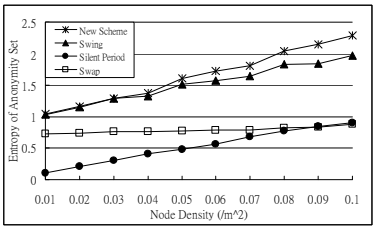

Figure 12. Entropy for Various Schemes Obtained under Different Node Density.

node which exchanges IDs with it. An adversary thus can not construct a set of possible exchanged IDs to exclude any nodes in the target's reachable area. The location privacy of the initiating node is hence maximized.

In Figure 7, assume the target is initiating node t and the switching result is as follows: Node t uses ID b, node b uses ID a and node a uses ID t. Figure 8 presents the set of possible target IDs using the reachable area of the target, A = {b, c, d}. The node with ID t is located to form the reverse reachable area which helps generate the set of possible exchanged IDs, B = {a} in Figure 9. As we can see, the intersection of the two possible target ID sets A and B is a null set. The above two examples exhibit that employing ID Tracking on nodes using our new location privacy protection scheme is impractical and may produce such an unreasonable result as "no ID is possible of being the target".

4. Experimental Evaluation

Table 1. The Simulation Parameters

Parameter	Value
Node mobility model	Random walk with reflection
Node velocity	Speed: 1~3 m/s; Direction: $[0,2\pi)$
Movement step time	3~5 sec
Node communication model	Continuous transmission; no collision
Simulation area	100*100 m^2
Node density (/m^2)	0.01~0.1
Silent period	0~5 sec
ID lifetime	60~600 sec

4.1. The Simulation Model

Extended simulation runs are conducted to evaluate and compare the performance of our new scheme and previous schemes, such as SP, Swing and Swap. Our simulation employs Visual C++ and the following parameters (listed in Table 1) which are set mainly based on References [6] and [8].

Privacy: The location privacy level is one condition in Swing, Swap and the new scheme that allows nodes to enter the silent state and update IDs. In this simulation, location privacy increases during an update and decreases as time passes.

The transmission range of a local synchronization broadcast is two times the radius of the reachable area, which is two times the maximum speed times the maximum silent period, e.g., 2 * 3 (m/sec) * 5 (sec)＝30 (m).

The number of neighbors is approximately the density (D) times the broadcasting area, which is around $(30)^2\pi D \fallingdotseq 2800D$. As the reachable area of a cooperating node does not center at the initiating node, the cooperating node can mix with only a small part of the neighbors, which is assumed to be one third of the total neighbors (about $1000D$) in the simulation. Thus the privacy of a cooperating node will increase by $1000D$ during an update. Meanwhile, to prevent an initiating node from initiating again, we increase the privacy of an initiating node by twice the number of neighbor nodes during an update, which is around $5600D$. When Swap is used, an initiating node gets to know the number of cooperating nodes by the received amount of the reply messages, and thus sets its privacy twice the amount of the reply messages. Privacy is set to decrease every 30 seconds.

4.2. Simulation Results

4.2.1. Location Privacy Under Simple Tracking. Figure

10 gives the performance of different location privacy protection schemes under Simple Tracking. The entropy [14] is calculated by the obtained anonymity set [15]. As exhibited, SP performs not as well as the other schemes – because it does not adopt local synchronization. Swing, not updating the IDs of any nodes with desirable privacy levels and thus excluding these IDs from the anonymity set, performs only better than SP. Swap and our new scheme, which have nodes reply even if they reach the desired privacy levels to enlarge the anonymity set, achieve the maximum location privacy and the slight advantage is to our scheme.

4.2.2. Location Privacy of Swap Under Simple Tracking and ID Tracking. The location privacy of Swap obtained under the operation of Simple Tracking and ID Tracking is depicted in Figure 11. As observed, Swap produces significantly lower privacy under the function of ID Tracking, regardless of node density. That is, ID Tracking can track more target nodes by generating smaller anonymity sets (than that of Simple Tracking) to reduce entropy and as a result to increase the success rates of tracking. Node density has little to do with the performance of ID Tracking but clearly affects that of Simple Tracking.

4.2.3. Comprehensive Results. In our simulation, the entropy of anonymity sets is taken to evaluate the performance of the above location privacy protection schemes, and the result is given in Figure 12. The result for SP, Swing and our new scheme is obtained by the anonymity sets which are constructed using the reachable areas of target nodes. As to Swap (whose special design allows an adversary to pursue the target by the ID Tracking mechanism), the initiating target's anonymity set will be constructed using both the reachable area and the possible ID exchange approaches. Its cooperating target's anonymity set will consider only the IDs of the target node and the corresponding initiating node. Adopting anonymity sets based on ID Tracking makes Swap performs inferior to Swing and the new scheme.

5. Conclusion

A desirable location privacy protection scheme is important for secure node communication in a WLAN. By pausing transmission or updating nodes, a location privacy protection scheme can prevent nodes from being tracked and transmitting information from being snapped. However, the ID exchange protocol in the Swap mechanism allows an adversary to learn about the fact that only two nodes exchange IDs during the exchange process and one of them carries the ID of the initiating node. Such a fact endangers the location privacy of the involved nodes and may help an adversary locate a target node easily. This paper first introduces an ID Tracking approach to trace nodes which swap their IDs to increase location privacy during transmission, and the result shows our ID Tracking can easily track a cooperating node and also an initiating node in the Swap operation, revealing the vulnerability of Swap.

To achieve better location privacy for nodes in WLANs, we propose a new user-centric location privacy protection scheme based on local synchronization and independent ID update. In our new scheme, the initiating node and cooperating nodes all have the chance to switch IDs, i.e., all nodes involved in the switching process will mix together. The relationship between the initiating node and cooperating nodes gets so interwoven that even the proposed ID Tracking can hardly untangle or track it. Location privacy is thus maximized. Simulation results show that nodes using Swap and our new scheme hold good location privacy under Simple Tracking. But when under ID Tracking, the location privacy of nodes using Swap apparently decreases.

References

[1] R. P. Minch, "Privacy Issues in Location-Aware Mobile Devices," *Proc. 37th Hawaii Int'l Conf. on System Sciences*, Jan. 2004.

[2] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking," *Proc. 1st ACM/USENIX Int'l Conf. on Mobile Systems, Applications, and Services*, May 2003, pp. 31-42.

[3] J. Al-Muhtadi, R. Campbell, A. Kapadia, D. Mickunas, S. Yi, "Routing Through the Mist: Privacy Preserving Communication in Ubiquitous Computing Environments," *Proc. 2002 Int'l Conf. on Distributed Computing Systems*, July 2002, pp.74-83.

[4] R. Moskowitz, "Host Identity Protocol," *draft-ietf-hip-base-08.txt*, IETF, June 2006.

[5] R. Moskowitz, "Host Identity Protocol (HIP)Architecture," *RFC 4423*, IETF, May 2006.

[6] L. Huang, K. Matsuura, H. Yamane and K. Sezaki, "Towards Modeling Wireless Location Privacy," *Proc. 2005 Privacy Enhancing Technologies*, May 2005, pp. 59-77.

[7] A. Beresford and F. Stajano, "Location Privacy in Pervasive Computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46-55, 2003.

[8] M. Li, K. Sampigethaya, L. Huang and R. Poovendran, "Swing & Swap: User-Centric Approaches Towards Maximizing Location Privacy," *Proc. 5th ACM Workshop on Privacy in Electronic Society*, Oct. 2006, pp. 19-28.

[9] M. Gruteser and D. Grunwald, "Enhancing Location Privacy in Wireless LAN through Disposable Interface Identifiers: a Quantitative Analysis," *Proc. 1st ACM Int'l Workshop on Wireless Mobile Applications and Services on WLAN Hotspots*, Sep. 2003, pp. 46-55.

[10]IEEE 802.11 WG. http://grouper.ieee.org/groups/ 802/11/.

[11]L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Silent Cascade: Enhancing Location Privacy without Communication QoS Degradation," *Proc. 2006 Security in Pervasive Computing*, Apr. 2006, pp. 165-180.

[12]A. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-Aware Services," 2004 *IEEE Int'l Workshop on Pervasive Computing and Communication Security*, Mar. 2004, pp. 127-131.

[13]D. Chaum, "Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms," *Comm. ACM*, vol. 24, no. 2, pp. 84-88, 1981.

[14]C.E. Shannon, "A Mathematical Theory of Communication," *Bell System Tech. J.*, vol. 27, pp. 379-423, July 1948, and pp.623-656, Oct. 1948.

[15]A. Serjantov and G. Danezis, "Towards an Information Theoretic Metric for Anonymity," *Proc. 2002 Workshop on Privacy Enhancing Technologies*, Apr. 2002, pp. 41-53.