Global Journal of researches in engineering
Electrical and electronics engineering
Volume 12 Issue 1 Version 1.0 January 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Location Privacy in Mobile Ad Hoc Network Measuring V2X Location Based Communication Systems with Accumulated Information

By Yatin Chauhan, Prof Jaikaran Singh, Prof Mukesh Tiwari, Dr Anubhuti Khare

Department of Electronics and Communication University

Abstract - Wireless Mobile Ad Hoc Networks are particularly vulnerable due to their fundamental characteristics such as an open medium, dynamic topology, distributed cooperation, Vehicle - to - vehicle / vehicle - to - infrastructure (V2X) communication systems are envisioned to greatly improve road safety, traffic efficiency, and driver convenience. However, many V2X applications rely on continuous and detailed location information, which raises location privacy concerns. A multitude of privacy protection mechanisms have been proposed in recent years. However, few efforts have been made to develop privacy metrics, which can provide a rigorous way to assess the privacy risk, evaluate the effectiveness of a given mechanism, and exploit the full possibilities of protection methods in V2X systems. Therefore, in this paper we present a trip-based location privacy metric for measuring user location privacy in V2X systems. The most distinguishable aspect of the metric is to take into account the accumulated information, which is the privacy-related information acquired by an adversary for an extended period of time, e.g., days or weeks.

Keywords : Vehicle-to-vehicle/vehicle-to infrastructure (V2X) communication Ad Hoc Networks systems.

GJRE-F Classification: FOR Code: 090604

LOCATION PRIVACY IN MOBILE AD HOC NETWORK MEASURING V2X LOCATION BASED COMMUNICATION SYSTEMS WITH ACCUMULATED INFORMATION

Strictly as per the compliance and regulations of:

Open Association of Research Society, USA
Research | Diversity | Ethics

Location Privacy in Mobile Ad Hoc Network Measuring V2X Location Based Communication Systems with Accumulated Information

Yatin Chauhan [α], Prof Jaikaran Singh [σ], Prof Mukesh Tiwari [ρ], Dr Anubhuti Khare [Ѡ]

Abstract - Wireless Mobile Ad Hoc Networks are particularly vulnerable due to their fundamental characteristics such as an open medium, dynamic topology, distributed cooperation, Vehicle - to - vehicle / vehicle - to - infrastructure (V2X) communication systems are envisioned to greatly improve road safety, traffic efficiency, and driver convenience. However, many V2X applications rely on continuous and detailed location information, which raises location privacy concerns. A multitude of privacy protection mechanisms have been proposed in recent years. However, few efforts have been made to develop privacy metrics, which can provide a rigorous way to assess the privacy risk, evaluate the effectiveness of a given mechanism, and exploit the full possibilities of protection methods in V2X systems. Therefore, in this paper we present a trip-based location privacy metric for measuring user location privacy in V2X systems. The most distinguishable aspect of the metric is to take into account the accumulated information, which is the privacy-related information acquired by an adversary for an extended period of time, e.g., days or weeks. We develop methods to model and process the accumulated information, and reflect the impact on the privacy level in the metric. We further prove the viability and correctness of the metric by various case studies. Our simulations find out that under certain conditions, accumulated information can significantly decrease the level of user location privacy. The metric and our findings in this paper give some valuable insights into location privacy, which can contribute to the development of effective privacy-protection mechanisms for the users of V2X systems. and constrained capability. Location information of nodes can be critical in wireless ad hoc networks, especially in those deployed for military purposes. In this paper, we present study of various method of receiver location privacy in mobile adhoc network.

Keywords : Vehicle-to-vehicle/vehicle-to infrastructure (V2X) communication Ad Hoc Networks systems.

I. Introduction

The emerging vehicle-to-vehicle/vehicle-to infrastructure (V2X) communication systems enable a new way of cooperation among vehicles, traffic operators, and service providers. Based on Dedicated Short Range Communications (DSRC) technology, vehicles can communicate among each others and with the entities in the back-end system via Roadside Units (RSU). It is envisioned that V2X communication systems can significantly improve road safety, traffic efficiency, and driver convenience. Example V2X applications include collision warning, floating car data, and location-based services. If deployed, such systems will be one of the biggest realizations of Mobile Ad Hoc Networks (MANET).However, many V2X applications rely on continuous Recent wireless research indicates that wireless Mobile Ad Hoc Networks (MANET) present a larger security problem than conventional wired and wireless networks [1,2]. In the traditional Internet, routers within the central parts of the network are owned by a few well-known operators and are therefore assumed to be somewhat trustworthy. This and detailed location information of the vehicles. Vehicles are personal devices. Locations of a vehicle reveals the movements and activities of its driver and passengers. Sending and disseminating location information of the users of V2X systems has the potential to infringe the users' location privacy. The location privacy issue inV2X communication systems has been identified and amultitude of privacy-protection mechanisms have been proposed in recent years, e.g., in [1]-[4].To evaluate the effectiveness of these mechanisms, a metric for measuring the level of user location privacy is crucial and indispensable. For example, we need a metric which can tell us that the user privacy level has been increased by 20% after applying one of the protection mechanisms. However, so far the main focus on the topic is to devise privacy-protection mechanisms, very few metrics exist for measuring user location privacy in V2X systems in a rigorous way. Hence, the usefulness of privacy-protection mechanisms cannot be strictly evaluated and compared and the trustworthiness of V2X systems cannot be assessed. Furthermore, the range of possible protection methods cannot be fully exploited. In our previous work [5], we introduced a trip-based location privacy metric to measure the level of location privacy of individual users in V2X systems. Based on the observation that the uncertainty of a potential adversary and the user privacy level are indeed two sides of the same coin, the metric measures the level of location privacy as the link ability of location information to the individuals who generate it. The uncertainty in the information is quantified into entropy. Our previous work assumes that the information available to the adversary

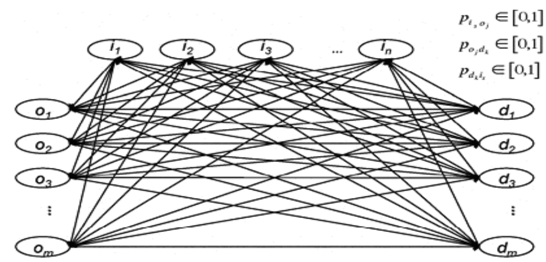
Author [α σ ρ] : Department of Electronics and Communication, Sri Satya Sai Institute of Science and Technology,Sehore M.P. India.
E-mails : yatin.dd@gmail.com, jksingh81@yahoo.co.in
Author [Ѡ] : Department of Electronics and Communication University Institute of Technology,RGPV Bhopal M.P. India.

is limited to a short period of time. To stay realistic, it is reasonable to assume that an adversary will do its best to decrease the uncertainty of the obtained information. Therefore, the adversary is likely to take the maximum available information into account. In particular, the adversary will try to utilize the accumulated information, which is privacy-related information acquired by capturing communications from running V2X systems for an extended period of time, e.g., days or weeks. Hence, the assumption of a limited time period is over-simplified from the real world.

To reflect the true underlying privacy value in V2X communication systems, the metric must take into account the impact of accumulated information on privacy level. Intuitively, the more information an adversary has, the more it can draw conclusions with fewer uncertainties. However, the impact of accumulated information on location privacy has not been investigated up to now. In this paper, we address this issue by extending the current location privacy metric to take into account accumulated information. As a result, the metric can more accurately reflect users' privacy value in V2X communication systems. Specifically, in this paper we develop a method to model the accumulated information, design approaches to process, propagate, and utilize the accumulated information, and reflect the effect in the metric, prove the viability and correctness of the metric by means of various case studies. In the following, Section II gives the background information on the basics of the trip-based location privacy metric. Section III describes the method to model the accumulated information. Section IV introduces two approaches to process the accumulated information and reflects it in the metric. Section V evaluates the metric by case studies. Section VI discusses the related work, followed by the conclusion in Section VII

II. Metric Fundamentals

This section gives the necessary background information on the tripbased location privacy metric introduced in [5].In V2X communication systems, each time a vehicle sends a message, it gives out its location information to the system. Although there are different levels of granularities, the location information in V2X systems can be categorized into three types, i.e., single locations, tracks, and trips. Location information only becomes privacy relevant if it can be linked to identifiable individuals. Since for privacy concerns vehicles are very likely to use pseudonyms in communications [6], [7], information on single locations and tracks are less privacy-sensitive than the information on trips, which can be used to infer an individual's identity and activities. The first step to measure privacy is to capture the information on trips and individuals in an arbitrary defined area and time period. Hence the metric virtually takes a "snapshot" of the dynamic V2X systems. he information captured in the snapshot is then modelled in a weighted tripartite graph, shown in Fig.1. The graph contains three distinct sets of vertices,i.e., I , 0 , and D, which represent Individuals, Origins and Destinations of the trips. An adversary's knowledge on the link ability of an individual to a set of trips is expressed in probability distributions. The probabilities are used as the weights on the directed edges. For example, Pjk is a weight on an edge (Vj ,Vk) between the vertices Vj and Vk .



information modelled in weighted tripartite graph

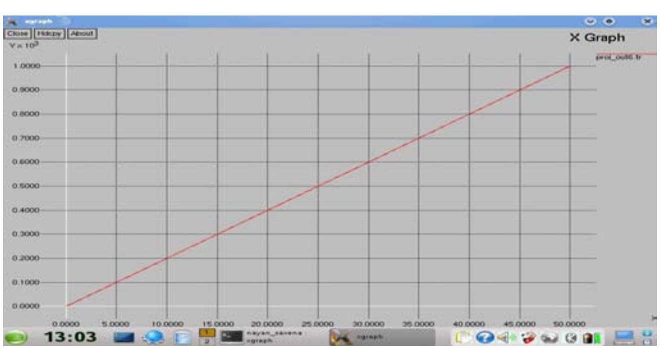
For an individual to make a trip (e.g., 01 -----. d1) , he or she must start from one of the origins, e.g., i 1 from 01 . If the trip from 01 ends at one of the destinations, it must be possible to link i 1 to d1 as well. Due to the uncertainty in the information, there can be many of such possible linkings among the vertices. A closed walk or a cycle starting from a vertex *is* and passing vertices *{oj ,dd* in the graph has the semantics of is 's probability *Pjk* to make a trip with origin *OJ* and destination *dk.* By collecting all cycles connected to a particular individual in the graph, we can extract the probability distribution of the link ability of that individual to a set of trips. The probability distribution can be graphically expressed as a hub-and-spoke structure, shown in Fig. 2. The last spoke with probability *pC* in the clock-wise order denotes the probability of an individual not making any trips, i.e.,"staying at home". assumption no longer holds in an Ad Hoc network, since all nodes entering the network are expected to take part in routing. Also, because the links are usually wireless, any security that was gained because of the difficulty of tapping into the network is lost.

Furthermore, because the topology in such a network can be highly dynamic, traditional routing protocols can no longer be used. Thus, Ad Hoc network has much harder security requirements than the traditional network and the routing in Ad Hoc networks is an especially hard task to accomplish securely, robustly, and efficiently.

In general, the wireless MANET is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, absence of central authorities, distributed cooperation, and constrained capability. The existing security solutions for wired networks cannot be applied directly in wireless MANETs.

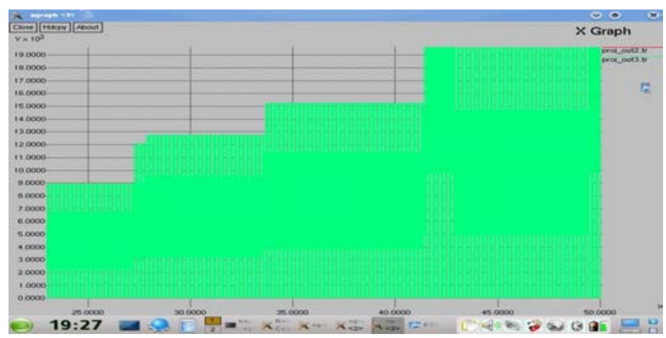
Applications that make use of ad hoc routing have heterogeneous security requirements. *Authentication*, *message integrity*, and *nonrepudiation* to an ad hoc environment are part of a minimal security policy. Apart from these, there are several other security issues [1, 3] such as *black hole attacks, denial of service*, and *information disclosure*. A location disclosure attack can reveal something about the locations of nodes or the structure of the network. The information gained might reveal as to which other nodes are adjacent to the target, or the physical location of a node. In the end, the attacker knows which nodes are situated on the route to the target node. If the locations of some of the intermediary nodes are known, one can gain information about the location of the target as well. In many cases, the location information might be very crucial. In MANETs installed for tactical/military missions in a hostile and/or unknown territory, these types of attacks have to be prevented. In many cases, the communicating nodes need to be anonymous—no other node in the network should know who is communicating with whom. Initially, we present a solution that achieves complete anonymity and discuss trade-offs between complete anonymity and difficulty in identifying misbehaving nodes.

We then present enhancements to our protocol to prevent these attacks albeit at the cost of complete anonymity The problem we are going to address in this paper is receiver location privacy even while the routing protocol is already supporting identity anonymity. In such a scenario the eavesdropping adversary tries to track the route discovery messages to infer some information about the destination's venue or the route established between source and destination. To realize the importance of location privacy imagine a MANET in a battlefield where the nodes are living soldiers. If the adversary breaks the location privacy of the nodes in such a scenario the existence of the soldiers would be revealed and also their lives Might be in danger The rest of this paper is organized as follows. In section II some related works are reviewed. Section III gives an overview of the ANODR protocol. Section IV describes the adversary model. Section V concludes this paper



III. Related Work

Chaum's mixnet [8] and DC-net [9] were the origin of many future ideas to address private communication. Mixnet removes the correlation between sources and destinations. A mix node is a network member that performs encryption and padding on its received messages and sends them out in a random order so that it is impossible for outsiders to distinguish which output message belongs to which input message. DC-net [9] is based on binary superposed sending. In DC-net the anonymity set is composed of all potential senders. Each sender shares a secret key at least with one other user. If sender A is wishing to send a message, it should superpose the message with its exchanged secrets. Other users superpose in the same manner (if no message to send they superpose zero with shared keys). All messages are transmitted to the receiver. The sum of these messages is the message of A, because every secret is added twice and canceled. Therefore, the message is delivered without revealing the originator. Another solution proposed for wired networks is Crowds [10]. Crowds consists of a number of network users. Before a data request is sent to the server it is chained randomly through a number of crowds members, so that the server knows that it came from one of the members, but he has no idea about the original sender. The protocols proposed to provide anonymity



in wired networks assume having a fixed topology and usually having trusted third parties. Such solutions are not suitable for MANETs as well as any other mobile scenario in which the network topology might change all the time. Most of the routing-based anonymous protocols for MANETs try to address the identity anonymity issue, e.g. are static and data is always sent to a powerful sink. One of the first simple ideas to address the destination location privacy in ad hoc routing protocols was not to stop the route request packet flow at the destination node and continue with that for several extra hops to hide the receiver's venue. Also for route location privacy the authors of ARM [7] proposed not to forward the RREP message only on the discovered route which is the case in every other MANET routing protocols, but to form a cloud of routes around the real one. This is done by adding a TTL field to the packets which is used to forward them for a number of hops around the discovered path. The neighbors of the nodes en route who receive the RREP message should broadcast it after replacing some fields by random numbers and their neighbors would do so till the TTL reaches zero. Therefore the discovered route is covered by some fake flows. Also the data packets will be broadcasted in a limited number of hops around the discovered route for the same purpose. This solution provides *route location privacy* to some level, i.e. makes the adversary uncertain about the real route's location inside the cloud, but can not hide the destination's location which might be of higher importance. We refer to this idea of ARM as *route cloud idea*. Some location privacy solutions for MANETS are proposed for geo-routing scenarios, e.g. [14] addresses destination location privacy for the category of MANETs in which geographic information of the nodes is available.

This protocol uses the location information of the destination node to generate an area including the destination to deliver the data packets to all of the nodes in that. The number of nodes inside the anonymity zone determines the privacy level provided by the protocol. On the other hand, measuring the network anonymity in general is another issue in private communication research area. [15] and [16] have proposed information theory based metrics to quantify privacy. The basic idea is that the privacy degree is maximized when all anonymity set members have the same probability to be the real object of interest.

IV. Overview of the Underlying Routing Protocol

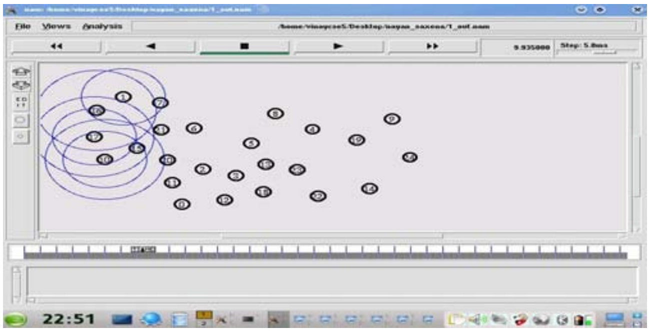
We use the identity free routing protocol, ANODR [5], to evaluate the location privacy ideas of RDIS. We apply our ideas to ANODR as an underlying routing protocol to Provide it with destination location privacy. In fact, it could be possible to apply RDIS techniques to other identity anonymous MANET routing protocols in appropriate ways. ANODR is an ID-free anonymous routing protocol in which each hop on the route is associated with a random route pseudonym. The sender initiates a RREQ packet containing a sequence number, a global trapdoor and an onion. The sender initiates the onion by generating some random nonce as the onion core and encrypting it with its own secret key. The global trapdoor is some well known tag encrypted by the destination node's public key, so it can be opened only by the intended destination. If a node receives a RREQ, it will try to open the trapdoor with its private key. If it succeeds and sees the well known tag it will consider itself as the destination and initiates the RREP message. Otherwise, it adds a self aware layer to the one is a highly motivated passive avesdropper who has the ability to monitor the traffic all over the network, for example by employing several overhearing nodes in different points of the network to cover the whole area. Our goal against this adversary is to prevent it from finding the destination's venue and also the path between communicating pairs. The second attacker considered is an internal adversary, which is a compromised node in the network. The adversary can take control of the compromised node. The private routing protocol should make it impossible for him to break the location privacy of the destination even if it is located on the route. Internal Adversaries should be prevented from finding out if their neighbor nodes are source or destination even if they are on the same route. We suppose that the compromising capability of the adversary is not unlimited onion and encrypts the new onion with its secret key and also attaches a one time public key to the message and rebroadcasts it. The next nodes would do the same and would record the one time public key sent by the previous node which will be used in RREP phase. Eventually if the destination receives the RREQ message it will initiate the RREP message. The nodes on the route from the destination to the sender will directly forward this message to the sender. The RREP message includes the proof of trapdoor opening, *Proofdes*, generated by the destination, which the sender will use to verify if the RREP is initiated by the intended destination. Every node on the route generates a random route pseudonym, *Kseed*, encrypts it by the one time public key of the previous node and replaces that in the appropriate field of the received RREP message. The route seudonym will be used as the shared secret key between every two consecutive nodes en route in data forwarding phase. The onion and the proof of trapdoor opening are encrypted by the route pseudonym to hide them from outsiders. Every intermediate node opens the random route pseudonym with its one time public key and then uses it to extract the onion. Then it strips its own layer from the onion expecting to see what it has encrypted a while ago and modifies that with its route pseudonym and stored one time public key and forwards that to the previous node on the route. Eventually when the sender receives the RREP packet it will open the onion and check for the appropriate proof of successful trapdoor decryption. If the onion data matches the previously generated onion core and the proof of trapdoor decryption is shown, the route discovery is done.

The RREQ
and RREP packet formats are as follows:

$$RREQ : < RREQ, seq\#, global\ trap, onion, PK - 1time >$$

$$RREP : < RREP, \{Kseed\}PK{-}1time, fKseed\ (Proofdes, onion) >$$

Each intermediate node records the correspondence between its own route pseudonym and its upstream node's route pseudonym in its routing table. When a data packet is received, the intermediate node looks up its routing table for the received route seudonym. If it is found, the node would replace the route pseudonym with the next hop's corresponding one and forward the packet. Otherwise, the packet will be discarded. A symmetric key would be piggybacked in the first global trapdoor from the destination to the sender as the end to end encryption key for next contacts. To avoid public cryptosystem's expenses, this symmetric key will be used for the next RREQ messages from the same sender to the same destination

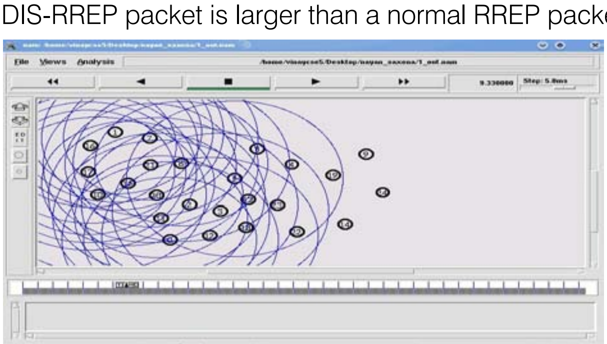


e.g. in case that the route is broken due to node mobility and a new route shall be reestablished [17].

V. Attacker Model

a) Message Type Unification Idea

In ad hoc routing protocols when the intermediate nodes receive the route reply packet, they typically use their keys/secrets stored in RREQ forwarding phase to realize that they are located on the route and they must forward the received reply message. A global eavesdropper can track the RREP message flow to find the discovered route between the source and the destination. Also he is able to discover the physical location of the communicating pair by observing the origins of RREQ/RREP messages. The main contribution of this work is to hide the destinations' location by making it impossible for the adversary to determine the origin of route reply packets. We use the same message type, *RDIS*, for RREQ and RREP packets. The nodes on the route use the keys to check if this is a RREP message intended to them. So when a RDIS-RREP message is forwarded, the nodes out of the route would behave exactly as they do about a RDISRREQ message till the TTL field reaches zero. As we will describe, after a random number of hops the RDIS-RREP packet is changed to a RREP packet as Figure 1 shows. This is because forwarding the reply packet in RDIS-RREP format toward the source causes a high overhead due to two reasons. First, the RDIS-RREP packet will be broadcasted by every node receiving that till $TTL = 0$, and second the size of a RDIS-RREP packet is larger than a normal RREP packet.



b) Applying RDIS to ANODR

In this section we are going to describe how the ideas of RDIS can be applied to ANODR to provide destination location privacy as well as route privacy. To apply RDIS to ANODR we need to change the appearance of the route request and the route reply messages to the unified one so that the RDIS-RREP flow seems to be part of the RDIS-RREQ flow to any outsider without losing the routing functionalities. For this purpose several properties should be considered. One is the size of RDIS-RREP and RDIS-RREQ packets which should be the same to prevent the outsider to distinguish them. Another one is that the appearance difference from the RDISRREQ packet the destination node receives and the RDISRREP packet it initiates should be similar to the difference between a received RDISRREQ packet received at any other node and the RDIS-RREQ packet broadcasted consequently by it. Therefore the initiation of the RDISRREP message would look like a part of the RDIS-RREQ flow. Also every field of one of these two message types should change with the same pattern as the other one. For example, the sequence number which is a fixed field in RDIS-RREQ should be preserved the same in the corresponding RDIS-RREP flow. As a matter of course we change the content of the message type field in both of them to the same packet type, *RDIS*. When a node receives a *RDIS* packet with a new *seq#*, it will generate a random number between 0 and 1. If the number is less than a fixed parameter *Pf* the node will proceed with the packet, otherwise it will do nothing and therefore discard the packet.If the node decides to proceed with the received packet it will record the *seq#* in its routing table and will proceed with the message to follow the ordinary ANODR behavior (described in section III). When the destination node receives the RDISRREQ message it generates the corresponding RDIS-RREP packet. It decreases the received TTL by one. The RDIS-RREP packet includes a sequence number field filled with the same *seq#* of the corresponding RDISRREQ (in regular ANODR there is no sequence number or TTL in reply packets). The global trapdoor is preserved in RDIS-RREP. We change *Kseed}PK−1time* to *{REPLY,Kseed}PK−1time* in the RDISRREP packet. In order to match the size of the RDIS-RREP packets we need to add an additional field in the RDIS-RREQ packets filled with random data. So all in all a RDIS-RREQ packet will look like < *RDIS, TTL, seq#, global trap, onion, PK− 1time, random field* > and a RDIS-RREP packet will look like < *RDIS,TTL, seq#, global trap, REPLY,Kseed}PK−1time, fKseed* (*Proofdes, onion*) > The adversary may distinguish between the RDIS-RREQ and RDIS-RREP messages because he knows that the onion length in RREQ messages increases as the message nears the destination and the onion length in RREP messages decreases as the message gets further from the destination. Therefore the onion length should be fixed. In an improved version of ANODR the length of

Global Journal of Researches in Engineering (F) Volume XII Issue I Version I January 2012

the onion is fixed at 128 bit [18].Every node applies its symmetric key encryption on the 128 bit long onion. In RDIS, we use this mechanism to prevent the adversary from using the varying length of the onion to analyze the message type or the distance from the destination. When a node receives a *RDIS* message while it has forwarded another *RDIS* message with the same *seq#* before, it will try to open $\{REPLY,Kseed\}PK-1time$ using its one time public key generated during the RREQ phase. If after such a decryption the node can see the REPLY tag it realizes that this packet is a RDIS-RREP intended to it. Then it will generate a random number between 0 and 1. If this number is greater than a fixed parameter *Pr* it will decrease TTL by one and replace the *Kseed* and the onion with its own (see section III). Otherwise, it will change the RDIS-RREP message to a normal RREP message as shown below, but the TTL field will be preserved to be used for the route cloud idea. So one of the nodes en route randomly will change the RDIS-RREP packet to a normal RREP as follows, which except having the TTL field is the ordinary reply packet format in ANODR: < *RREP, TTL, {Kseed}PK−1time, fKseed* (*Proofdes, onion*) > Let us assume *Trep* is the maximum time that a source node waits to receive the corresponding RREP after initiating the RREQ. We consider the recorded one time public keys at the nodes as fresh keys during *Trep* seconds after being generated. When a node receives a packet like the above RREP packet and it has a fresh one time public key it will use it to find out if the packet is intended to it (by opening the onion as in ordinary ANODR). If so, the node will modify the reply packet as described in III and will also decrease TTL by a random number among 1,2,3 and 4. Therefore this packet will be forwarded on the discovered route normally till it reaches the destination. When a node that is not located on the discovered route receives such a packet and it realizes that the packet is not intended to it, it will generate a random number among 1,2,3 and 4 and will decrease the TTL by that. It will also replace the next two fields with random bits without changing the packet size and broadcasts the packet. Therefore a cloud of routes will be formed around the route and the discovered route will be hidden among them. This will provide the protocol with route location privacy.

c) Ring route idea in RDIS

As mentioned before, in RDIS instead of a route between the source and destination we form a ring route such that the two communication end nodes are located on that. For this purpose the destination node should respond not only to the first received RREQ message but to the first two of them. Therefore two routes will be formed between the source and the destination. As mentioned above, in RDIS every received RREQ packets are proceeded by every node by some probability. One consequence of this property is that the first discovered route is not necessarily the shortest one and also the first two discovered routes might be quite far from each other (because the intermediate nodes are chosen quite randomly and the two paths are not necessarily the shortest ones). When the source node realizes that two routes are discovered it starts sending data packets to the receiver through the first one. We use the established routes bidirectionally. It is possible because every two neighboring nodes on a route are sharing a link pseudonym pair which are used to forward the data packets over the route. When the destination receives any data packet it forwards it to the first node on the other route and the data packet will be forwarded (in the reverse direction) through that route to reach the source node. Then the source node will discard it. Therefore it is impossible for any eavesdropping adversary to distinguish the destination among the nodes on the ring by tracing the data packets.

VI. Conclusion and Future Work

In this paper we present a trip-based location privacy metric for measuring location privacy of the users of V2X communication systems. To reflect the true underlying privacy values, the metric includes accumulated information and reflects the impact in the privacy measurement. We model the accumulated information and develop approaches to process, propagate, and utilize the accumulated information in the metric. We evaluate the viability and correctness of the metric by various case studies and extensive simulations. Our simulations show that under certain conditions, accumulated information can significantly decrease users' location privacy. is a valuable tool to evaluate and develop privacy- V2X systems. In future work, we will further evaluate our metric with more scenarios and realistic V2X applications. The evaluation will also include existing privacy-protection mechanisms proposed to V2X systems. The current metric only measures privacy of individual users. The possible interrelations among individuals and their impacts on the level of location privacy will be investigated to determine location privacy in a global view. The metric is extensible, which means when it is necessary, we can add other identified attacks on location privacyto the metric in the future.

References Références Referencias

1. G. Resta, P. Santi, and J. Simon, “Analysis of multi-hop emergency message propagation in vehicular ad hoc networks,” in *MobiHoc ’07*. New York, NY, USA: ACM, 2007, pp. 140–149.
2. H. W. Y.C. Hu, “A framework for location privacy in wireless networks,in *ACM SIGCOMM Asia Workshop 2005*.
3. Q. He, D. Wu, and P. Khosla, “Quest for personal control over mobile location privacy,” *IEEE Communications Magazine*, vol. 42, 2004.
4. P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk,

"Enhancing sourcelocation privacy in sensor network routing," in *ICDCS '05*, 2005.
5. J. Kong and X. Hong, "Anodr: anonymous on demand routing with untraceable routes for mobile ad-hoc networks," in *MobiHoc '03:Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, New York, NY, USA, 2003, pp. 291–302.
6. J. Kong, X. Hong, and M. Gerla, "An identity-free and ondemand routing scheme against anonymity threats in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 8, 2007.
7. S. Seys and B. Preneel, "Arm: Anonymous routing protocol for mobile ad hoc networks," pp. 133–137, 2006.
8. *L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Commun. ACM, vol. 24, no. 2, pp. 84–90, 1981.*
9. *Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," Journal of Cryptology, vol. 1, 1988.*
10. M. K. Reiter and A. D. Rubin, "Crowds: anonymity for Web transactions,"*ACM Transactions on Information and System Security*, vol. 1, no. 1, pp. 66–92, 1998.
11. Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in *INFOCOM 2005*, pp. 1940–1951 vol. 3.
12. Hong, J. Kong, and M. Gerla, "Mobility changes anonymity: new passive threats in mobile ad hoc networks: Research articles," *Wirel. Commun. Mob. Comput.*, vol. 6, no. 3, pp. 281–293, 2006.
13. K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global avesdropper." in *ICNP*. IEEE, 2007, pp. 314–323.
14. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous geoforwarding in manets through location cloaking," *IEEE Trans. Parallel Distrib. Syst.*, vol. 19, no. 10, pp. 1297–1309, 2008.
15. C. D´ıaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," in *Privacy Enhancing Technologies*, 2002, pp. 54–68.
16. A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity." Springer- Verlag, 2002, pp. 41–53.
17. S. K. Makki, P. Reiher, K. Makki, N. Pissinou, and S. Makki, *Mobile and Wireless Network Security and Privacy*. Springer, 2007.
18. J. Kong, "Anonymous and untraceable communications in mobile wireless networks," Ph.D. dissertation, 2004, chair-Gerla, Mario.
19. S. network Technologies (SNT) Qualnet, *http://www.qualnet.com*.