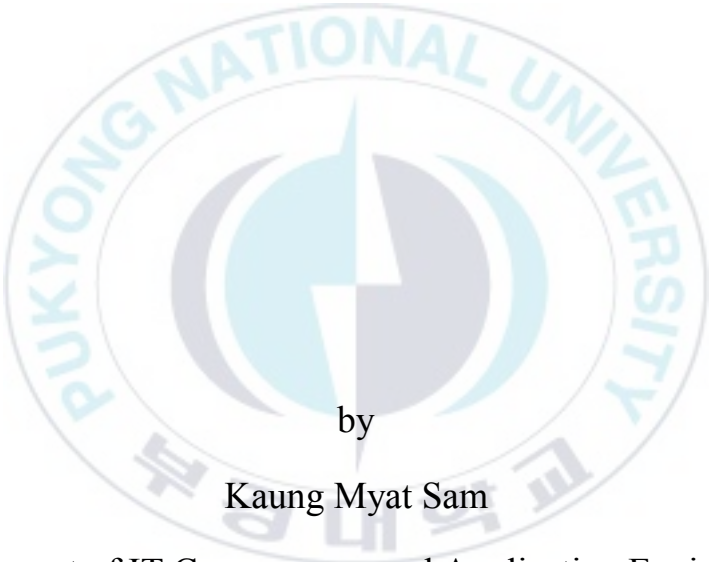
Thesis for the Degree of Master of Engineering

Practical Approach on Pseudonym Changing Strategy for Urban Environment in VANETs



by

Kaung Myat Sam

Department of IT Convergence and Application Engineering

The Graduate School

Pukyong National University

February 2016

Practical Approach on Pseudonym Changing Strategy for Urban Environment in VANETs

Advisor: Prof. Kyung-Hyune Rhee

by

Kaung Myat Sam

A thesis submitted in partial fulfilment of the requirements for the degree of

Master of Engineering

in Department of IT Convergence and Application Engineering,

The Graduate School,

Pukyong National University

February, 2016

Practical Approach on Pseudonym Changing Strategy for Urban Environment in VANETs

A dissertation

by

Kaung Myat Sam

Approved by:

_____

Professor Kim-Chang Soo,
(Chairman)

_____

Professor Kyung-Hyune Rhee,
(Member)

_____

Professor Man-Gon Park,
(Member)

February, 2016

Table of Contents

List of Figures

List of Tables

Acknowledgement

First and foremost, I would like to present my utmost gratitude to my supervisor, Professor, Kyung-Hyune Rhee not only for his guidance but also for providing me with the opportunity to pursue the Master's degree in the Laboratory of Information Security and Internet Applicaion (LISIA), at Pukyong National University, Busan, South Korea. His thorough supervision and appreciable support have enabled me to gain valuable knowledge about security area and support successful completion of Master's degree in Korea.

I would like to express my sincere thanks extend to all members in the Office of International Relations and other department offices in Pukyong National University for the facilities and supports given me for the stay in Korea.

I would like to thank and appreciate my colleagues in the LISIA laboratory and the other friends I met in Korea for their support given me in one way or another throughout my precious life in Korea.

I would like to thank and appreciate a chief monk PYIDAWOO SAYADAW Ashin Pandicca, an instructor of Buddha's taught, inspire me to overcome difficulties, stress and depression during my whole study period and to achieve such a great success.

Needlessly to say, my sincere love and a huge thanks to my mother, father, sister and brother for their words of encouragement and love which brought me faith and happy life while staying far away from home which is situated in Myanmar.

Kaung Myat Sam

Department of IT Convergence and Application Engineering.

Pukyong National University, Busan, South Korea.

Practical Approach on Pseudonym Changing Strategy for Urban Environment in VANETs

Kaung Myat Sam

Interdisciplinary Program of Information Systems,

The Graduate School, Pukyong National University

Abstract

Vehicle privacy and untraceability are important requirements in VANET. Although vehicular public key infrastructure seems to protect the vehicle privacy for certain degree, there are other privacy concerns regarding on safety messages so called heartbeat (in America) messages or beacons (in Europe). These messages used by many safety applications provide a constant stream of location data, and without any proper protection measures, they make tracking of vehicles easy even for a passive eavesdropper. One publicly accepted solution is to transmit heartbeat messages using the changed pseudonyms according to the desired period. However, if the pseudonyms are changed in an improper time or location, such solution may become the threat for vehicle privacy. In order to enhance these challenges, we present more practical method of changing pseudonym under the urban environment. Precisely, this thesis studies on the capabilities of adversary attack on pseudonym and develop the pseudonym changing analytic model by performing a simulative study of the strategy using the open source simulator VANETsim.

Chapter 1. Introduction

1.1. Motivation

Vehicular ad-hoc networks (VANETs) are designed for convenience and improving driving safety in transportation systems. Nowadays, the modern vehicles are already equipped with on-board unit (OBU) to become the part of vehicular ad-hoc network (VANETs) communicating with both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) using vehicular road side units (RSUs). In safety-related application, each vehicle requires to broadcast safety message periodically including sensitive information such as identity, position, time stamp, speed and acceleration in order to function properly [2]. Indeed these messages can benefit to prevent accidents, they may also be used by the adversary to get the clue about the vehicles. Unless these action are not properly measures, the strong relationship between safety message of vehicle and drive will compromise his or her privacy, since an adversary can easily eavesdrop on all the broadcast messages and decide the location visited by the vehicles over a period of time. Furthermore, an adversary can transmit false warnings to nearby vehicles to mislead yield the lane or slow down them and in extreme case, can even cause a fatal accident. These lacking of privacy and safety may diminish the wide recognition of VANET technology. The first measure for protecting such case is to use of pseudonym which are the multiple identifier instead of real identifiers. Vehicles can then change their pseudonym and acceptable privacy is acquired since pseudonyms cannot be linked to each other. However, the amount of location information overhears by adversary at designated traffic area to reconstruct the traces of certain vehicles within that same area. Hence, pseudonym alone cannot grantee the privacy of vehicles and how to change the pseudonym give rise the scope of our thesis.

1.2. Related Works

The first method to change pseudonym is the SLOW(Silence at low speeds) [1] which is based on the accomplishing unlinkability between the pseudonyms of a vehicle and its locations is to change it during silent periods. Meanwhile there is no message to be transmitted during such periods, becoming harder for the attacker to make the linkage between pseudonyms. For instance, the vehicles should not transmit safety messages when they are within predefined speed threshold (below 30km per hour) and they should change pseudonym during each period. But, in silent period of SLOW method, not only vehicles or pedestrian can still encounter accident but also these period may be broken when vehicle sense the risk of collisions or accidents. In addition, this method make unpractical to some safety application such as collision avoidance prevention and blind spot warning need regular stream of safety messages from nearby vehicles.

The second pseudonym changing method is the Pseudonym Changing at Social spot (PCS) [2]. In urban area, there are many social spot can be determine the place where several vehicle may gather including intersection, shopping mall vehicle parking and landmark area. At road junction or intersection with traffic light, many vehicle may stop and waiting when the light is red and they delay the change of pseudonym. Then they start to change the pseudonym as soon as the traffic light turn green. In other social spot such as shopping mall car parking or landmark places, the vehicle change their pseudonym after they leave social spots.

The other work done by Gerlach and al [3] introduce a concept called mix zone context which is defined as any situation that provides sufficient anonymity with respect to an attacker to change a pseudonym. In the considered mix context, they assume that each vehicle assesses permanently

its neighbourhood and changes pseudonym only if they detects *k* vehicles with same direction in a mixing region. Instead of storing a large number of pseudonyms, they suggest that every vehicle maintains a time-slotted pseudonyms pool [4]. In each time slot, there is exactly one assigned pseudonym. When a time slot is passed, each vehicle will change their pseudonym.

1.3. Purpose and Scope of Thesis

This research aims to develop a privacy preserving pseudonym changing strategy on urban environment which is simulated using real small model of Namgu (Busan, South Korea) open street map by open source vehicle simulator (VANETsim). This research included all procedure of pseudonym management, sharing and changing. But we are narrow the scope and more emphasize on pseudonym changing strategy and, based on these changing, we constructed the sample model of Namgu to simulate the real world scenario.

1.4. Thesis Outline

The thesis has been divided into five chapters which are:

Chapter I, Introduction: introduction consists of thesis background, related work, thesis objective, scope and thesis outlines.

Chapter II, Preliminary: preliminary explains the theoretical supports and methods. It is includes an explanation about VANET, Safety messages, the open source simulator VANETsim.

Chapter III, How location privacy is breaching: this chapter contains recent know attack on location privacy, demerit of public key infrastructure and tracking techniques are considered.

Chapter IV, System Implementation and Analysis: We discuss about configuration of our proposed strategy in the system, we briefly explain about pseudonym life cycle which is used in our model and more emphasize on pseudonym changing strategy by using real world map and simulator.

Chapter V, Conclusion: this chapter contains conclusions and additional features that is required but not yet developed in this thesis.

Chapter 2. Preliminary

2.1. Applications in VANETs

There are many applications are created for various purposes from vehicle manufactures [5]. Different manufactures have different idea about developing software to implement in vehicle to fulfill the different ranges and requirement of customer's needs [6], we have divided the application into two major categories:

1) Safety-related applications, such as collision avoidance and cooperative driving (e.g., for lane merging) consist of monitoring the surrounding road, approaching vehicles, surface of the road and road curves. For instance, the real time traffic data can be download from the RSU to the vehicles whenever and wherever needed in order to solve the problem such as traffic jams, accidents and avoid congestions. In addition, vehicle alerting about road condition such as road curve, road material spilling and sudden downhill. And also vehicle involved in accident would broadcast to trailing vehicles so that it can take decision with prior time to prevent multiple post-accident crush. The main feature of this category is to ensure the safety of the service user and application should be low or zero tolerance and guaranteed even in the presence of the adversary.

2) Other applications or commercial application, will provide the driver with the entertainment and services as internet access, streaming video, traffic optimization, payment services (e.g., toll collection), location-based services (e.g., finding the closest fuel station), infotainment (e.g., Web access). Apparently, security is also required in this some part of this application category, particularly in the case of payment services. However, we focus on the security and privacy aspects of safety-related applications

because they are the most direct and specific to the vehicular environment and therefore they raise the most challenging and life threating problems.

2.2. Safety Messages

There are three main classes of safety messages, based on their properties related to privacy and real-time constraints [7], as shown in Table 1. Traffic information messages are require to broadcast the surrounding traffic condition ahead of vehicle or in a given region and therefore do not require real time broadcast thus affecting public safety only indirectly (by preventing potential accidents due to congestion); hence they are not time-critical. General safety-related messages are used by public safety applications such as cooperative driving and collision avoidance and hence should satisfy stringent constraints such as an upper bound on the delivery delay so they need to broadcast in real time. Liability-related messages are distinguished from the previous class because they are exchanged in liability-related situations such as traffic offence or accidents. Therefore, the liability of the message originator should be determined by revealing his identity to the law enforcement authorities. This classification of messages will be useful later in describing the attacks on VANETs [8].

Table 1. Message classes and properties

Class/Property	Legitimacy	Privacy Protection		Real Time constraints
		Against other	Against police	
Traffic Information	yes	yes	yes	no
General safety messages	yes	yes	yes	yes
Liability-related messages	yes	yes	no	yes

In these message classes consist of common property of broadcasting with geo-cast and mainly standalone [9] (i.e, there is no dependency of content between two or more broadcasted messages like in media streams). The typical safety message includes position, speed, direction, time stamp, and acceleration of the vehicle, in addition to the specific traffic events data such as road congestion notification or accident warning. In the case of a sender faces an abnormal situation such as accident, these data help the receiver of trailing vehicles to compute their positions with respect to the sender and determine if they are in danger. The message may not necessarily contain explicit information [10]. The main feature of ad-hoc networks is broadcasting with multi-hop. However according to the DSRC specifications and because of their broadcast nature, safety messages are transmitted over a single-hop with a sufficient power to warn vehicles in a range of less than 15 seconds travel time, thus eliminating the need for multi-hop. Nonetheless, some form of multi-hop still exists in case like vehicles that receive warning messages estimate whether the reported problems can also affect their trailing vehicles. In this sense, they forward the message to them.

2.3. VANETsim

VANETsim is the open source simulator for privacy and security concepts in VANETs [11]. It can be used as an intuitive tool that allows the researcher to evaluate their proposals and compare them with related work efficiently to get better result. The main features of this simulator regarding on our work is given below-

- ❖ It is especially designed to analyze the attacks on privacy and security and privacy as well as countermeasures on the application layer especially. We can easily integrated new

scenario of new attacks and countermeasures since API provides high-level access to all relevant data structures.

- The default scenario creator allows us to design, simulate, and save the complex and repeatable experiments with varying parameters and can run batch experiments with desire script to achieve nearest target.
- It already contains a close approximation of the real world in order to obtain realistic results. The simulated cars within this simulator have driving decisions individually make them realistic micro-traffic model. In addition, It allows to import real world map and road network form *OpenStreetMap*, ready to use map API of the whole world.
- The simulator offers a high level customization between map, road networks and vehicle mobility model based upon the researcher goal to achieve realistic simulations and artificial scenarios (eg, with simple graphs as road networks for simulation) can be created to verify analytic results.
- It allows to create large-scale experiments in real time with more than 20,000 vehicles and large road networks to city level since their code is highly optimized and supports multi-core systems
- In addition to a lightweight terminal interface we have also designed a powerful GUI that visualizes the simulation, and thus allows for the explorative experimentation with intuitive debugging facilities.

Chapter 3. How Location Privacy is Breaching

In this chapter, we investigate the location privacy threats and why vehicular public key infrastructure (PKI) is not enough to protect location privacy [12].

3.1. Location Privacy Threats in VANET

The privacy breaching can happen when the vehicle former position and current location is access by an attacker. The attacker recorded the vehicle visited places location or destination using eavesdropping broadcasted safety message [13]. The first way is to use tradition method of collecting history for long period, and second way is to tag the vehicle to its visited places of interest thereby getting to know the personal interest of the vehicle owner. For instance, the shopping advice application or traffic jams and road condition alerting application will automatically tag to vehicular navigation system and therefore becoming the clue for attacker. In addition, many safety related application heavily depend on position and time information which is requires to function properly. This will lead all vehicle using this application will force to broadcast frequently their time and position information [14]. As the nature of vehicular transmissions cannot be shut down entirely and can be eavesdropped by anyone within its vicinity becoming the clear threat. By developing a malicious RSUs or other means of network of any public, private, commercial and criminal attacker can collect these information containing detailed location profiles attached with their drivers. Such possession could easily breach safety and privacy of drivers. By establishing a network of RSUs, any public, private, commercial, or criminal attacker can collect these packets and create detailed location profiles of vehicles and consequently their drivers. Possession of such location profiles could easily breach the privacy of drivers.

3.2. Limitation of Vehicular Public Key Infrastructure (PKI)

Vehicular Public Key Infrastructure seem to guarantee identity privacy although lack of supporting location privacy [15]. Even a vehicle changes its pseudonym or certificate along the way to its destination, the possible way of attacking is to observe the two observation points controlled by an attacker while moving with same velocity, speed, acceleration on the same road will make it easier for the attacker to correlate the pseudonyms used by that vehicle and track the vehicle. In addition, the set of anonymity can only be done by the set of vehicles changing their pseudonym between two designated points. When the anonymity set size of vehicle become one, it said to be tracked by the attacker. Accordingly, a mechanism for ensuring location privacy is needed to overcome this PKI limitation.

3.3. The Adversary Model

Global vs. Local: This is mainly based on the range and coverage of an adversary. The local adversary can only eavesdrop the smaller radius and number of receiver to develop the malicious network. On the other hand global attacker has larger coverage and in extreme case they can use RSU to deploy their network. Both of them are focusing on the breaching of location privacy of vehicle to identify it user. Therefore they try to link multiple pseudonym gradually to track vehicle and then identify the user

Active vs. Passive: A passive attacker try to collect as many as pseudonym at every intersection where their receivers are deployed and cannot alter or modify message content. A passive adversary cannot inject or modify messages, but can collect pseudonyms at every intersection where he/she has an eavesdropping station. The role of active one is to alter or

implement within pseudonym infrastructure. Their aim is to block pseudonym change, disturb the management or force pseudonym change the designated set of vehicles in order to revote the group key or forcing to change pseudonym very fast to deplete pseudonym.

Internal vs. External: The internal adversary is considered to be within the authentic set of vehicle and can communicate with other vehicle. The external one is defined by the outer intruder and therefore cannot communicate with internal set and limited in internal attacks.

3.4. Tracking Techniques

The primary goal for an adversary is to identify and track the location of different vehicles throughout a designed area [18]. The attacker can still observe all messages even though whether they can break encryption or not. The global passive adversary (GPA, an outsider) can observe all communication in a specific area but cannot interact with VANET participants and infrastructure. To prevent the GPA from linking pseudonyms, radio silence or encrypted communication can be used.

Insiders can participate in the VANET and act like a normal VANET vehicle. In this case, protection is almost impossible: During radio silence the attacker just drives as close as possible and visually keeps contact to the victim. Insiders can also operate attacker road side units (ARSU) whether as deployed hardware by the attacker, or malware infected RSUs or other wifi enabled devices. In this paper we assume that an attacker is able to create fake or misuse genuine VANET identities (e.g. pseudonyms, key pairs) for his attack. Note that this, depending on the chosen VANET setting (e.g. tamper-proof-hardware, trusted third parties), could be challenging and expensive for the attacker. In order to link two visited

locations of the target an adversary needs to (i) identify an anonymity set of the target defined as the set of vehicles that are indistinguishable from the target, with the set including the target itself and, (ii) choose a potential candidate for target.

1) Identifying an Anonymity Set: the common way of identifying the vehicle from the anonymity set can be performed by the attacker as follow. First the attacker mark a point where he receive the observed message location at given time based on all possible movements. Then he try to calculate all reachable area is determined. The calculated area is called a region in which the possible target vehicle will likely to appear and rebroadcast the message again. The calculation can be done using known values of time, speed range and the silent period range. All the vehicle have to update their pseudonym of messages within one point of the reachable area and based on this point, attacker can filter possible vehicle in its vicinity.

2) Choosing a Potential Candidate from Anonymity Set: Upon identifying the target's anonymity set, for tracking a target the adversary must choose a potential candidate from the anonymity set to be the target. Based on how the potential candidate is chosen, the following two types of tracking methods are considered –

(i) Simple Tracking: In this method, the adversary assumes that each element of the anonymity set is equally likely to be the potential candidate for the target, and hence, randomly chooses an element as the target. the simple tracking of a vehicle where, given a set of three vehicles A, B, C that update pseudonym in the reachable area, the adversary randomly chooses one of the three vehicles to be the target.

(ii) Correlation Tracking: In this method the attacker calculate the estimated location of the target vehicle within reachable radius and then choose a candidate based on the anonymity set updates pseudonym and seem to be the closet to the calculated region. After considering the targets last observe location, direction, speed at given time of former time stamp and estimated future time stamp in order to get most likely possible candidate from the anonymity set. Therefore, using correlation tracking the adversary can assign a non-uniform probability distribution to the target anonymity set. An element $\boldsymbol{i}$ that is chosen as a candidate at $\boldsymbol{m}$ of $\boldsymbol{n}$ estimated target positions in $\boldsymbol{A_r}$ is assigned a probability of $\mathbf{pi = m{=}n}$. The element in the anonymity set that has the highest probability will most likely be chosen to be the target. Given that there is at least one vehicle, the target, in the reachable area $\boldsymbol{A_r}$, the probability that the target can be uniquely identified at each transmission, denoted by $\mathbf{p_{track}}$, is:

$$\boldsymbol{p_{track}} = \mathbf{Pr}\{\boldsymbol{v}(\boldsymbol{A_r}) = \mathbf{1} | \boldsymbol{v}(\boldsymbol{A_r} \geq \mathbf{1}|\}$$

The expected maximum tracking time is;

$$\boldsymbol{E_{track}} = \frac{\boldsymbol{\rho A_r}}{\mathbf{1} - \boldsymbol{e^{-\rho A_r}}}$$

Each element of E_{track} is equally likely to be the target. The expected entropy of the anonymity set of the target is

$$\boldsymbol{E}\{\boldsymbol{H}(\boldsymbol{p})\} = \boldsymbol{log_2 E_{track}}$$

These kinds of tracking can be used to determine the probability of the vehicle position and trajectory then compromise its privacy.

Chapter 4. System Implementation and Analysis

In chapter 4. We discuss about configuration of our proposed strategy in the system, we briefly explain about pseudonym life cycle which is used in our model and more emphasize on pseudonym changing strategy by using real world map and simulator [19][20][21].

4.1. Pseudonym model in VANETs

In order to make new strategy in pseudonym changing model, we should firstly consider the architecture of pseudonym cycles in VANETs.

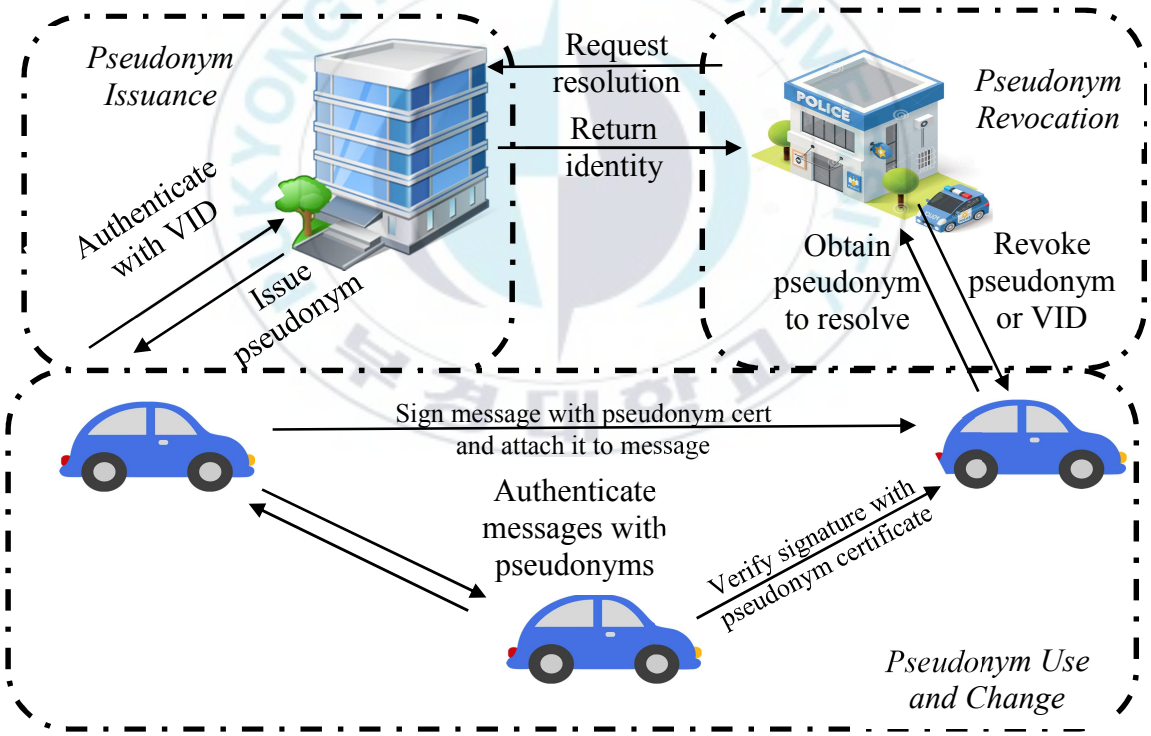


Fig. 1. Pseudonym managing architecture

4.1.1. Pseudonym Issuance

When the vehicle want to use pseudonym service within vehicular communication, it must have the unique digital identifier called vehicle id (VID) [19][24]. This VID can be used as a primary signed certificate that allows to authenticate a vehicle which is similar to the physical vehicle identification number (VIN) located on the mechanical chassis created by the car manufacture. This kind of VID can be used as long term identifier required to pre-install in the vehicle onboard unit. When the vehicle makes registration at the traffic authority license plate and VID will be issued. A pseudonym issuing authority authenticates the vehicle with its VID, verifies whether the vehicle is eligible to obtain the pseudonyms or not. If the VID is valid and never been revoked then the authorities will issue some pseudonyms. In this pseudonym issuance stage, the unique VID is the primary factor to be valid and authentic in order to ensure vehicle's OBU is real member of vehicular communications.

This stage depend on third- party issuance, where pseudonyms are created by a pseudonym issuing authority. To share the right between these third party entities, this may consists of multiple sub-entities, which consists of certificate authority (CA), pseudonym provider (PP), or only trusted authority (TA). The right to manage the pseudonym is disturbed among upper level (CA), lower level (CA), PP, RSUs, or split between both.. In either case, a pseudonym issuing authority authenticates the vehicle with its VID, verifies the vehicle's eligibility to obtain pseudonyms (i.e., the vehicle's VID is valid and has not been revoked), and then issues some pseudonym credentials. Pseudonyms are typically assigned an expiry date or validity period.

4.1.2. Pseudonym Revocation and Resolution

Pseudonym revocation can be done when misbehaving or faulty nodes or vehicles are found within the vehicular network to ensure proper performance and operation of the network. Firstly the misbehavior node should be taken by the law enforcement authority to revoke from the authentic user list. In order to revoke them, the authority need to send the resolution request to the pseudonym issuing authority or pseudonym provider to obtain the misbehavior pseudonym node holder's VID. In addition, another way to revoke the malicious node is the deny requests for further pseudonym refill as the pseudonyms are issued with short lifespan. And then, the malicious node will no longer join authentic network and finally, revoked the long-term identifier VID.

4.1.3.Pseudonym Use and Change

Pseudonym can be used for engaging in vehicular communication with other vehicles or infrastructure. Pseudonym use entails two steps: authentication (i.e., signing) of outgoing messages and verification of received messages. Pseudonym Change performed under one pseudonym can be linked to each other, due to the mentioned characteristics of pseudonyms. Thus, to prevent the link ability of actions, the actions must be performed under different pseudonyms, i.e., a vehicle must change pseudonyms over time. An adversary could then only link a limited number of messages. Changing the pseudonym when alone is not sufficient for confusing an observer, if that observer is able to monitor locations before and after the area in which the pseudonym change occurred. The frequency of pseudonym changes depends on the desired level of privacy, i.e., what

change rate is considered sufficient to prevent adversaries from deriving driving and movement patterns of individuals.

4.2. Pseudonym Change Strategies

The most important aspect of pseudonym changes is the change rate and its impacts largely on the communication, computation, storage overhead, and the level of privacy. We define our model based on following criteria-

1) Fixed Time Change (Periodic): In this strategy, a vehicle changes its pseudonym according to a fixed, periodic schedule. Instead of storing a very large amount of pseudonyms, every vehicle maintains a set of pseudonyms (called pseudonym pool) which are used at specific time slots. The time slot length determines how often a vehicle changes its pseudonym. A benefit of this strategy is that a vehicle always has a valid pseudonym even if the PP is not reachable. It also introduces an upper bound for pseudonym storage. However, as soon as the attacker knows the period of pseudonym change, which is easy to assess then tracking becomes trivial.

2) Random Change: To solve the issue of fixed periods, vehicles can change their pseudonym randomly. As a result, an adversary cannot predict the next pseudonym change. However, tracking is still possible if only one or few vehicles change pseudonyms at a specific time, because all other neighbors would keep the same identity. Thus, linking of new and old pseudonym of the vehicle that performed the change is still trivial.

3) Silent Period between changes: a vehicle remains silent after changing its pseudonym. The silent period makes tracking attacks more complex. Indeed, if a vehicle changes at an intersection and then waits for a short silent period the computation of movement prediction is difficult. The

silent period strategy is a good example for a tradeoff between privacy and safety.

4) Vehicle-Centric or Social Spot: In a distributed, vehicle-centric approach, vehicles independently determine where and when to change their pseudonyms. A silent period is also used in the SLOW protocol, but the vehicle only stops beaconing if its speed drops below 30 km/h and changes its pseudonym during such silent periods.

5) Density-Based: In this strategy, the vehicle changes its pseudonym based on a function of the current neighbor density. Therefore, it avoids ineffective pseudonym changes when the vehicle is alone.

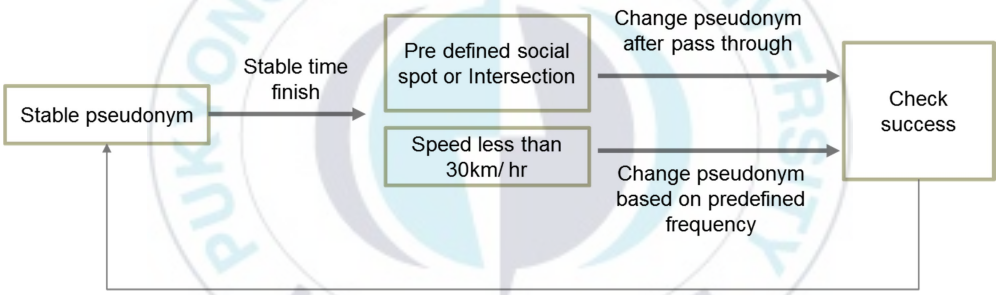


Fig. 2. Pseudonym changing strategy

Fig. 2 depicts a general state diagram of a pseudonym changing strategy. Before entering the predefined social spot or intersection, we assume that single vehicle or set of vehicles already passed pseudonym issuance state. In addition, the minimal stable should be considered for the desire application requirement of a stable communication session. After the stable time finishes, each vehicles' pseudonym waits for the trigger to change its pseudonym, whether pre-defined social spot or intersection or speed less than 30 km/hr. If requirements are met, they change pseudonym after pass through the intersection and change pseudonym based on

predefined frequency. For more in depth description of this strategy, we will try to explain using real world map implantation in VANETsim, an open source traffic modeling simulator.

4.3. Implementation in VANETsim.

We can download default VANETsim version 1.3 form www.vanet-simulator.org which contain ready to use scenario, privacy module and infrastructure [22]. In order to meet our requirements and new idea of defining strategy, we need to modify that source code. Therefore, we get that source code from www.codeforge.com/vanetsim.java_html.

4.3.1.Overview of VANETsim.

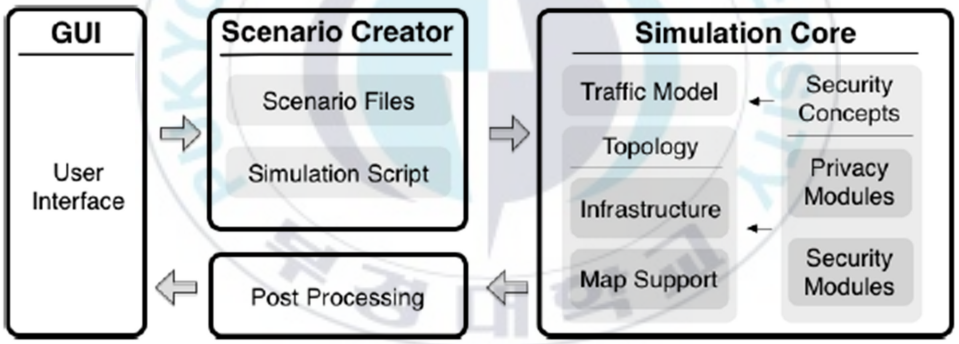


Fig. 3. VANETsim architecture.

The GUI provides a graphical map editor that allows the researcher to create and manipulate road maps. Maps can either be created from scratch or imported from *OpenStreetMap*. Further, the GUI visualizes the simulation process in an interactive, zoomable map that displays both roads and vehicles. As an alternative to the GUI mode the simulation can be executed

on the command line to run multiple experiments in a batch (faster than real time).In this case, we do not need to modify in this section.

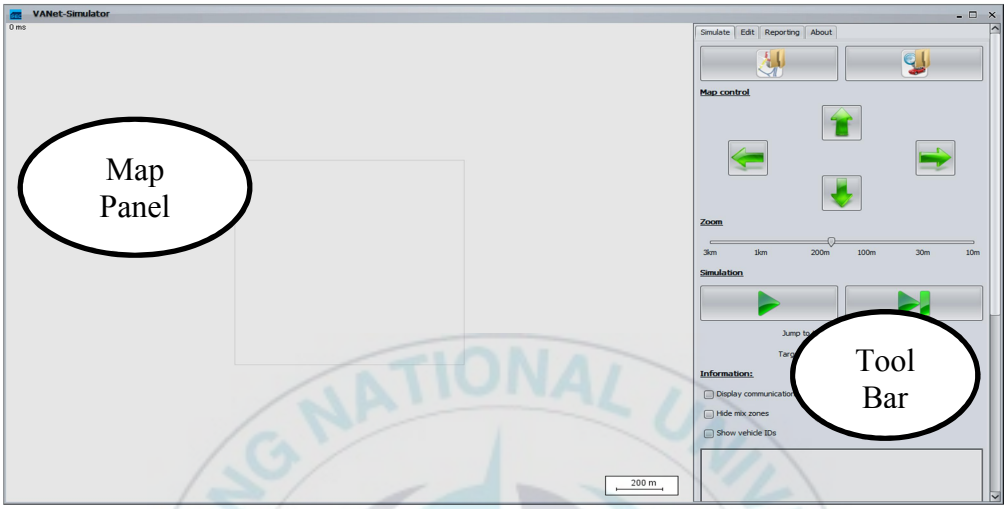


Fig. 4. VANETsim GUI.

The Scenario Creator offers the ability to rapidly prepare a series of experiments in which individual parameters are varied automatically. In this section, we import the real world map of Namgu, Busan from the *OpenStreetMap*. The scenario creation is more related to the simulation core so that we need to modify the core first to get our desire result [23]. For instance, if the attacker know the timing and location of the entering and exiting vehicles at intersection or social spot, the attacker can derive a probability distribution over the possible mappings. A possible way of collecting profile about vehicle can be done by marking messages sent over multiple points and link them to get exact vehicle which travelled at those points. In this case, we should taking account this fact to create better scenario in simulation.

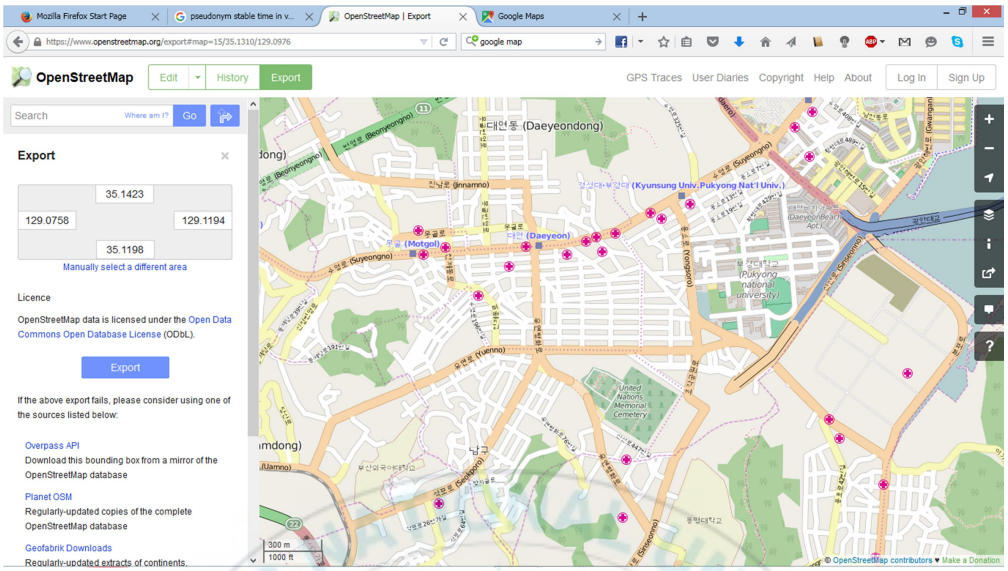


Fig. 5. Export from *OpenStreetMap.org*

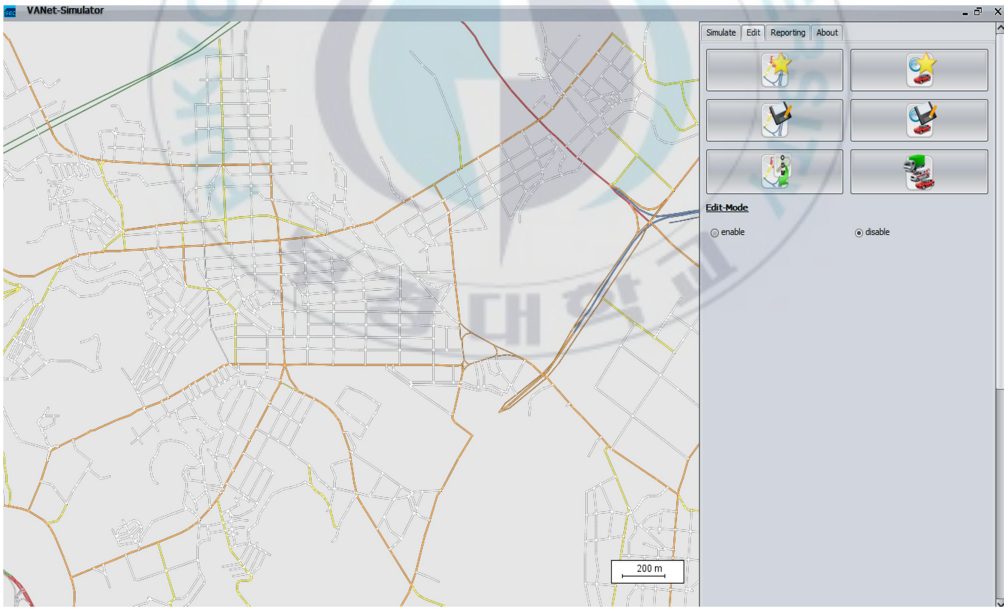


Fig. 6. Import to VANETsim.

4.3.2. The Simulation Core Implementation

The Simulation Core carries out the actual simulation. It has access to the map, including all infrastructure, vehicles and security/privacy concepts relevant for the simulation. Vehicles operate with a Traffic Model. It consist of five sub-components, which will be described in the following sections.

Maps contain various elements, e. g., streets and vehicles, which have to be accessed during the simulation with low latency. The road network is modeled with a graph-like data structure consisting of nodes (e. g., for intersections) and streets (used by OpenStreetMap). After imported from OpenStreetMap, the plain road network as well as meta information is extracted, including street names, speed limits, the number of lanes and their directions. In this case, we consider waypoints or POIs (Points of interest) around the map to make it more realistic rather than default setting.

```
16  public final class Junction{
17
18      /** For passing a node, the needed distance is calculated by multiplying
19       * the max. speed of the street with this factor. Measured in seconds. */
20      private static final double JUNCTION_PASS_TIME_FREE = 2.5;
21
22      /** The interval for cleaning up the junction queues. */
23      private static final int JUNCTION_QUEUES_CLEANUP_INTERVAL = 1000;
24
25      /** The maximum time in milliseconds to wait for a vehicle to pass the junction. If a vehicle
26       * doesn't signal that it has passed the junction within this time, another vehicle gets the permission! */
27      private static final int MAXIMUM_TIME_ON_JUNCTION = 2500;
28
29      /** A static reference to the renderer. */
30      private static final Renderer renderer_ = Renderer.getInstance();
31
32      /** The node this junction belongs to. */
33      private final Node node_;
34
35      /** An array with all priority street */
36      private final Street[] priorityStreets_;
37
38      /** The source nodes for the junction rules. */
39      private Node[] rulesSourceNodes_ = null;
40
41      /** The target nodes for the junction rules. */
42      private Node[] rulesTargetNodes_ = null;
43
44      /** The priorities for the junction rules. */
45      private int[] rulesPriorities_ = null;
46
47      /** A queue for the junction if more than one vehicle arrives. This is used for priority 3 streets (left tu
48      private JunctionQueue junctionQueuePriority3_ = new JunctionQueue();
49
50      /** A queue for the junction if more than one vehicle arrives This is used for priority 4 streets (normal t
51      private JunctionQueue junctionQueuePriority4_ = new JunctionQueue();
52
```

Fig. 7. Intersection behavior.

Infrastructure – there are two types of road-side Units (RSUs) in our model authentic road side unit and attacker road-side units (ARSUs). RSUs take the role of making mix-zone in intersection and even if there is a big gap between vehicles, they might enable communication between them.

RSUs can be distributed on the map and their transmission range can be configured individually.

```
public final class RSU {

    /** A reference to the reporting control panel so that we don't need to call this over and over again. */
    private static final ReportingControlPanel REPORT_PANEL = Vehicle.getREPORT_PANEL();

    /** A common counter to generate unique IDs */
    private static int counter_ = 1;

    /** How long a Road-Side-Unit waits to communicate again (in milliseconds). Also used for cleaning up outdated known messages. */
    private static int communicationInterval_ = Vehicle.getCommunicationInterval();

    /** How long a Road-Side-Unit waits to send its beacons again. */
    private static int beaconInterval_ = Vehicle.getBeaconInterval();

    /** If communication is enabled */
    private static boolean communicationEnabled_ = Vehicle.getCommunicationEnabled();

    /** If beacons are enabled */
    private static boolean beaconsEnabled_ = Vehicle.getBeaconsEnabled();

    /** A reference to the map so that we don't need to call this over and over again. */
    private static final Map MAP = Map.getInstance();

    /** An array holding all regions of the map. */
    private static Region[][] regions_;

    /** When known vehicles are rechecked for outdated entries. Measured in milliseconds. */
    private static final int KNOWN_VEHICLES_TIMEOUT_CHECKINTERVAL = 1000;

    /** A unique ID for this Road-Side-Unit */
    private final long rsuID_;

    /** The x coordinate. */
    private final int x_;

    /** The y coordinate. */
    private final int y_;
```

Fig. 8. Road-side unit behavior

```
public final class AttackRSU {

    /** A common counter to generate unique IDs */
    private static int counter_ = 1;

    /** The x coordinate. */
    private final int x_;

    /** The y coordinate. */
    private final int y_;

    /** The wifi radius */
    private final int wifiRadius_;

    /** A unique ID for this Attack-Road-Side-Unit */
    private final long arsuID_;

    /**
     * Instantiates a new Attack-RSU.
     *
     * @param x the x coordinate
     * @param y the y coordinate
     * @param radius the signal radius
     */
    public AttackRSU(int x, int y, int radius) {
        x_ = x;
        y_ = y;
        wifiRadius_ = radius;

        arsuID_ = counter_;
        ++counter_;

        //add this Attack-RSU to the list with all ARSUS (an array is used for a better performance)
        int arrayLength = Vehicle.getArsuList().length;
        AttackRSU[] tempArray = new AttackRSU[arrayLength+1];
        for(int i=0;i<arrayLength;i++){
            tempArray[i]=Vehicle.getArsuList()[i];
        }
```

Fig. 9. Attacker road-side unit behavior

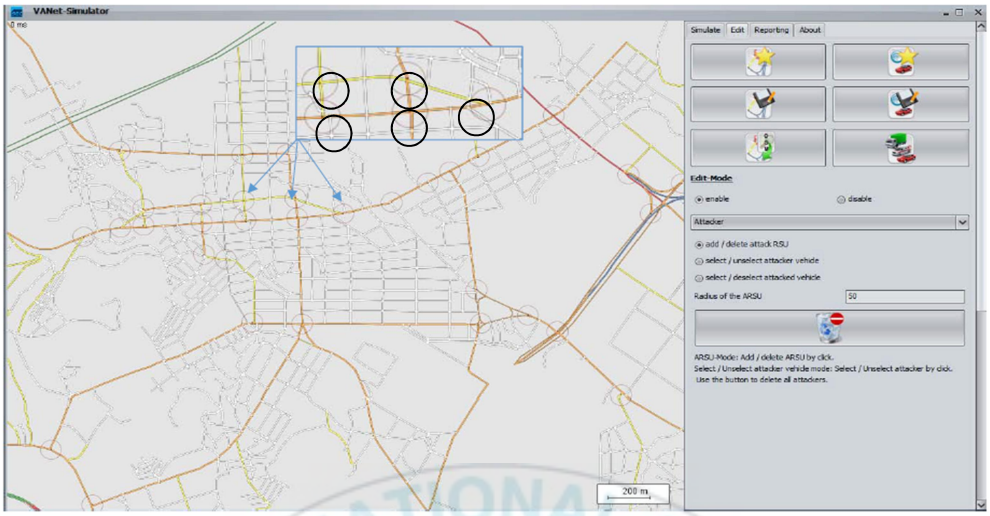


Fig. 10. Attacker road-side unit placement

Vehicular Traffic Model – VANETsim simulates vehicular traffic on two levels, the first one determines movement and behavior of vehicles on a microscopic level in a given situation, while the second one is responsible for macroscopic decisions (navigation and routing). Although individual vehicles have its own decisions on traffic flow, we still need to consider its waypoints and POI on our map.

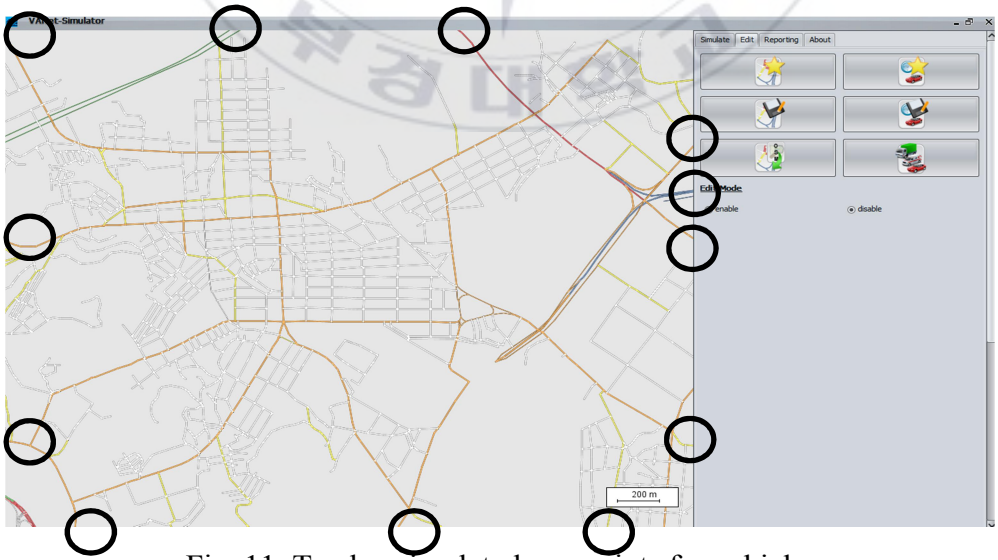
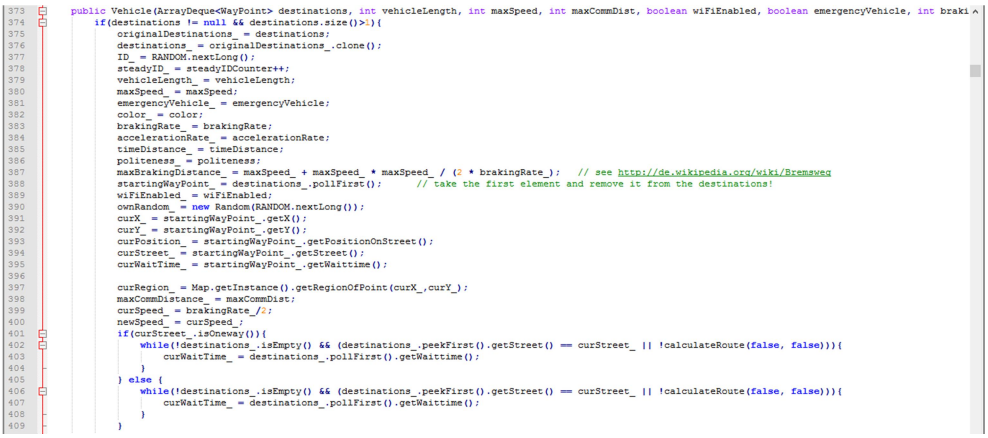


Fig. 11. Twelve simulated waypoints for vehicles



```
public Vehicle(ArrayDeque<WayPoint> destinations, int vehicleLength, int maxSpeed, int maxCommDist, boolean wiFiEnabled, boolean emergencyVehicle, int braki
    if(destinations != null && destinations.size()>1){
        originalDestinations_ = destinations;
        destinations_ = originalDestinations_.clone();
        ID_ = RANDOM.nextLong();
        steadyID_ = steadyIDCounter++;
        vehicleLength_ = vehicleLength;
        maxSpeed_ = maxSpeed;
        emergencyVehicle_ = emergencyVehicle;
        color_ = color;
        brakingRate_ = brakingRate;
        accelerationRate_ = accelerationRate;
        timeDistance_ = timeDistance;
        politeness_ = politeness;
        maxBrakingDistance_ = maxSpeed_ + maxSpeed_ * maxSpeed_ / (2 * brakingRate_);   // see http://de.wikipedia.org/wiki/Bremsweg
        startingWayPoint_ = destinations_.pollFirst();      // take the first element and remove it from the destinations!
        wiFiEnabled_ = wiFiEnabled;
        ownRandom_ = new Random(RANDOM.nextLong());
        curX_ = startingWayPoint_.getX();
        curY_ = startingWayPoint_.getY();
        curPosition_ = startingWayPoint_.getPositionOnStreet();
        curStreet_ = startingWayPoint_.getStreet();
        curWaitTime_ = startingWayPoint_.getWaittime();

        curRegion_ = Map.getInstance().getRegionOfPoint(curX_,curY_);
        maxCommDistance_ = maxCommDist;
        curSpeed_ = brakingRate_/2;
        newSpeed_ = curSpeed_;
        if(curStreet_.isOneway()){
            while(!destinations_.isEmpty() && (destinations_.peekFirst().getStreet() == curStreet_ || !calculateRoute(false, false))){
                curWaitTime_ = destinations_.pollFirst().getWaittime();
            }
        } else {
            while(!destinations_.isEmpty() && (destinations_.peekFirst().getStreet() == curStreet_ || !calculateRoute(false, false))){
                curWaitTime_ = destinations_.pollFirst().getWaittime();
            }
        }
```

Fig. 12. Vehicles behavior

Vehicular communication – VANETsim focuses on the application layer, the lower protocol layers are omitted. So that we are simulating on application layer we do not need to modify in this section. We assume all the messages are encrypted and that adversaries cannot know the inside contents.

5) Security and Privacy Modules - Security and Privacy Modules are either executed by vehicles on their own or they are part of the infrastructure on the map. The default privacy modules of VANETsim contain ready-to-use implementation of vehicle-enabled privacy concepts such as SLOW, Mix Zones and Social Spot. In order to cope with our strategy we modify in this modules.

if ((*vehicle enter intersection or pass social spot*) OR (*changing velocity<30km/hr)*)

change pseudonym after pass through

change pseudonym based on predefined frequency
endif
or else
loop

Fig. 13. Pseudonym changing protocol

We consider the place of changing pseudonym can be effective at the intersection and social spot where many vehicles are gathered. The system initiate the waiting time when the stable time finish. The system is then ready to change its pseudonym and listen to the nearby intersection or social spot. If these are eventually found, a new pseudonym is retrieved and used after passing through the intersection. After this stable time finishes, each vehicle's pseudonym waits for the trigger to change its pseudonym, whether pre-defined social spot or intersection or speed less than 30 km/hr. Moreover, we added the weights to these criteria occurrences approximately 0.6 to 0.4 and 0.7 to 0.3. If these requirements are met, they change pseudonym after pass through the intersection and change based on predefined frequency with above weight.

```
public void addIntersectionRule(Node startNode, Node targetNode, int priority){
    Node[] newArray;
    int[] newArray2;
    if(rulesSourceNodes_ == intersection){
        newArray = new Node[1];
        newArray[0] = startNode;
    } else {
        newArray = new Node[rulesSourceNodes_.length + 1];
        System.arraycopy(rulesSourceNodes_,0,newArray,0,rulesSourceNodes_.length);
        newArray[rulesSourceNodes_.length] = startNode;
    }
    rulesSourceNodes_ = newArray;

    if(rulesTargetNodes_ == social spot){
        newArray = new Node[1];
        newArray[0] = targetNode;
    } else {
        newArray = new Node[rulesTargetNodes_.length + 1];
        System.arraycopy(rulesTargetNodes_,0,newArray,0,rulesTargetNodes_.length);
        newArray[rulesTargetNodes_.length] = targetNode;
    }
    rulesTargetNodes_ = newArray;

    if(rulesPriorities_ == less than 30 km ){
        newArray2 = new int[1];
        newArray2[0] = priority;
    } else {
        newArray2 = new int[rulesPriorities_.length + 1];
        System.arraycopy(rulesPriorities_,0,newArray2,0,rulesPriorities_.length);
        newArray2[rulesPriorities_.length] = priority;
    }
```

.Fig. 14. Pseudonym changing strategy modification

4.3.3.The Simulation Result

We simulate and build our model on this following machine and environment.

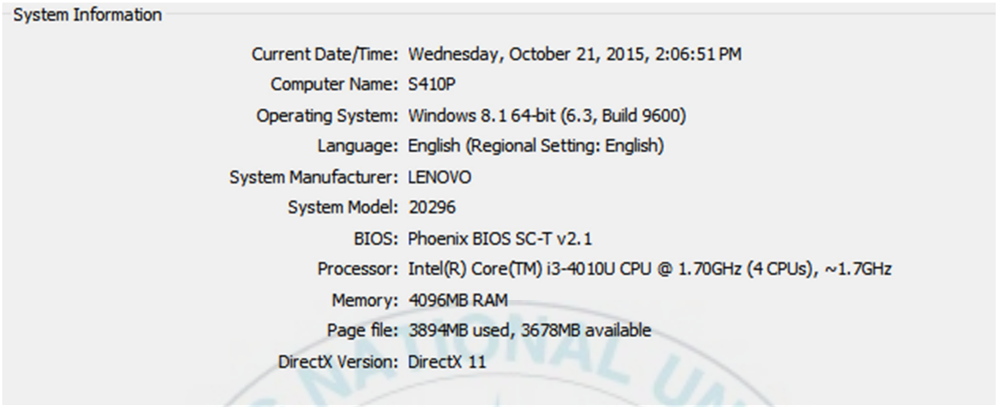


Fig. 15. Workstation system information

Simulation Parameter- The following parameters were changed in the simulation runs below:

Map - We use the real world map of the Namgu 5km x 3km area. The simulation uses a map of a real urban area. It contains different street types with different predefined speed limits. And also consists of 16 major intersections and many other small intersection with assigned pseudonym change frequency. We exclude small streets which is difficult to model all at once.

Traffic density - The traffic density defines how many vehicles could be found on one kilometer street length at specific point in time.

< 16 vehicles per one km = low traffic density

16 – 23 vehicles per one km = medium traffic density

24 – 31 vehicles per one km = high traffic density

32 -45 vehicles per one km = overload or congested

Attacker model – we consider attacker mode based on SLOW and pseudonym changing at social spot. Simple tracking expects the vehicle to send message in a fixed area around where the previous message was sent. It fails if there are several vehicles in that region. Multi target tracking can link the pseudonym if it detects that only one vehicle in a set of suspects within the expected area has changed the pseudonym. We assume that attackers are using attacker road-side unit. We start the simulation with 6000 vehicles from 12 waypoints and distributed around the map and run for 1 hour.

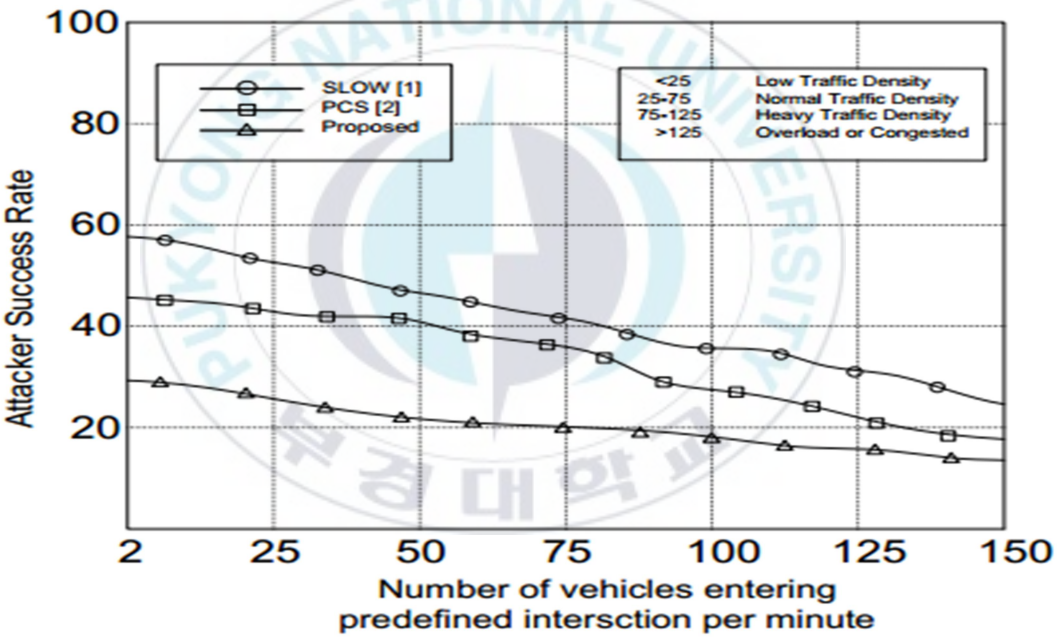


Fig. 16. Average attacker success rate at predefined intersection

Fig.16 depict the average attacker success rate on individual intersection which vehicles are gathered. We try to find the predefined intersection among major intersection and normal intersection to get highest and lowest density of vehicles. Our work has lower success rate even for two vehicles for 40% although the previous work is over 50%. Both strategies

reduce attacker success rate dramatically when the vehicle density becomes higher.

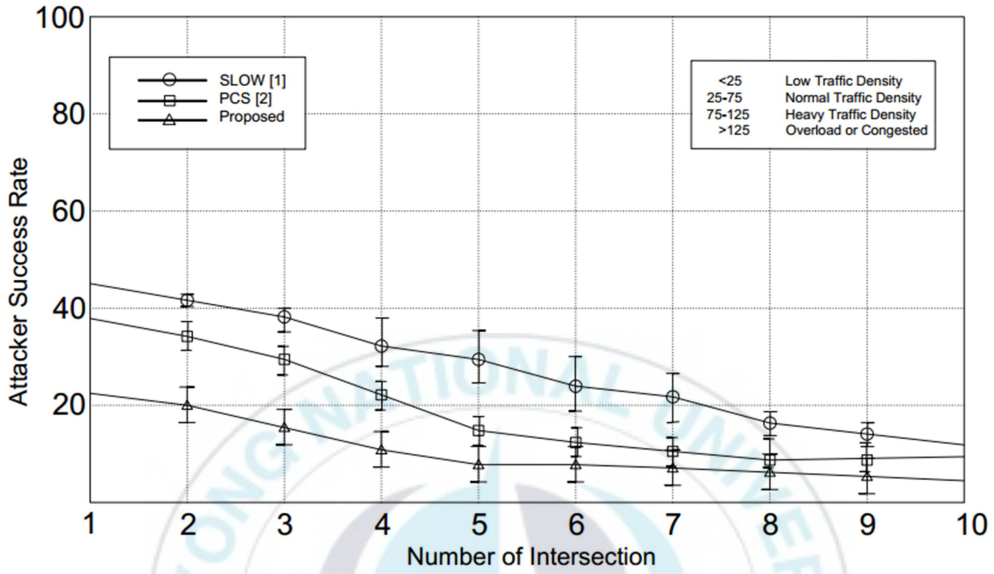


Fig. 17. Attacker success rate versus number of intersection

We capture the possible success rate of individual vehicle or set of vehicles using ARSUs at each intersection. This result is based on the very first 10 intersections encounter by the vehicles and intersections' ARSUs. The following result is interesting as the vehicle or set of vehicles pass through the first intersection both strategies are not acceptable since the attacker success rate are slightly more than 30% to 40% respectively. However, when vehicles pass through the third intersection our strategy can reduced to less than 20%, though default strategy cannot make notable reduction. After passing fifth intersection, our model has reached to the optimum state which less than 5% attacker success rate while they can only is reached our first stage 30%. Based on these outcomes, one can understand

that if someone need to protect his or her privacy to its optimum state, they only need to pass the five intersections.

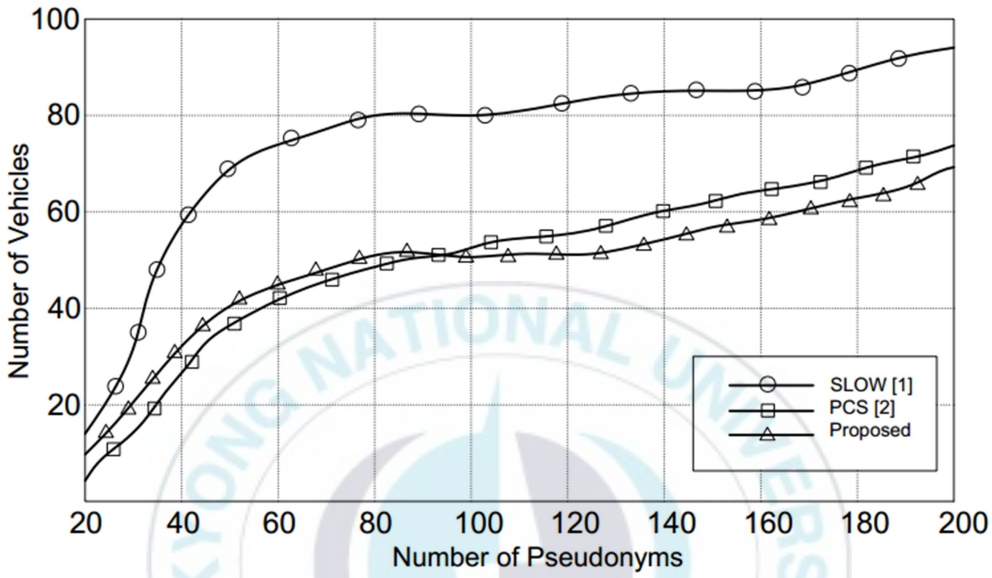


Fig. 18. Number of vehicle versus number of pseudonym

This result showed the trade-off between number of pseudonym and privacy protection. The previous work of SLOW method has lowest pseudonym usage while our work and PCS method needed slightly more pseudonym. At situation of the vehicle number rose to 50 and number of pseudonyms was almost 100, our work needed marginally more pseudonym than PCS method while maintaining better privacy and security level. All in all, each methods has its own strength and weakness therefore, how to use in different situation was directly based on the trade-off between privacy protection and number of pseudonym to satisfy customer requirements.

Chapter 5. Conclusions

To protect unlinkability and privacy of VANETs is still the open problem for many researchers. Hence, there are many requirements to get the perfect privacy and many problems to be solved. In our thesis, we try to focus on location privacy and pseudonym changing strategy of safety messages use in many safety related applications in vehicles. First, we find the recent ways of breaching privacy and tracking techniques and introduce public key infrastructure alone cannot guarantee location privacy. Then, we try to build the real world practical model of Namgu, Busan, South Korea for studying real nature of vehicles and pseudonym changing strategy. For in depth, we get the real world map from *opensourcemap* about 5km length and 3km depth to get vehicular road network. Then, based upon this map, we created the scenario for moving vehicle from twelve simulated destination around the map. From these points, vehicle find the path to these destination on their own decision and find shortest path. Although, we made exception on the smaller lane and street which is negligible impact on simulation. After that, we developed the attacker road side unit to meet with our requirement and placed at major and minor intersection around the map. Next, we applied the strategy of our work within vehicular behavior of changing pseudonym whenever they enter social spot or intersection. In this strategy, we added weighted method to trigger the probability of the occurrence of change pseudonym upon two criteria; after passing through the social spot or intersection and speed threshold is less than 30km per hour. In that case, we use the open source vehicular modeling and simulation engine “VANETsim” to get better result. Moreover, we make changes at the source code level of VANETsim to meet with our requirements. Finally, we get the result based on vehicle passing intersection and attacker road-side unit (ARSU). We

compare with our strategy and previous researcher works based on attacker success rate at the intersections and found that our work is better that others. While the number of pseudonym overhead is slightly increase when number of vehicles increase. Needlessly to say, even first intersection tracking from adversary is still difficult for them and our work reach optimum privacy level faster than other. In addition, previous work relies on total communication cut off when vehicle pass through the intersection although ours are not. Based on above result, we can conclude that the probability of the success rate of the attacker is largely depend on the number of vehicle, road, intersection, number of pseudonym usage and the attacker road-side unit placement. In order to get the acceptable privacy of vehicle, one should be handle the the trade-off among above mention factors to achieve desire goal.

On the other hand, this thesis has some unrealistic feature in simulation and need to be considered for future work. Firstly, our map model is about 5km into 3km area which is considered to be relatively small comparing to whole city map. Secondly, we cannot add all type of vehicles as the real world because there are many difficulty to get such data. For the long run, we will try to model whole city map with different type of vehicles to find the strength and weakness within VANETs infrastructure.

References

[1] L. Butty´an, T. Holczer, A. Weimerskirch, and W. Whyte, “SLOW: A practical pseudonym changing scheme for location privacy in VANETs,” in Proceedings of the IEEE Vehicular Networking Conference (VNC), Tokyo, Japan, 2009. IEEE, October 2009.

[2] R. Lu, X. Lin, T. Luan, X. Liang, and X. Shen, “Pseudonym changing at social spots: An effective strategy for location privacy in vanets,” IEEE T. Vehicular Technology, pp. 86–96, 2012.

[3] M. Gerlach and F. Güttler, “Privacy in vanets using changing pseudonyms - ideal and real,” in VTC Spring. IEEE, pp. 2521–2525, 2007.

[4] K.Sampigethaya, M. Li, L. Huang, and R. Poovendran, “Amoeba: Robust location privacy scheme for vanet,” IEEE Journal on Selected Areas in Communications,pp. 1589, 2007.

[5] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, “Swing &swap: user-centric approaches towards maximizing location privacy,” in Proceedings of the 2006 ACM Workshop on Privacy in the Electronic Society, WPES 2006, Alexandria, VA, USA, October 30, 2006. ACM, 2006, pp. 19–28.

[6] M. M. Haklay and P. Weber, “OpenStreetMap: User-Generated Street Maps,” IEEE Pervasive Computing, vol. 7, no. 4, pp. 12–18, 2008.

[7] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, “Privacy in inter-vehicular networks: Why simple pseudonym change is not enough,” in Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on. IEEE, 2010, pp. 176–183.

[8] F. Dötzer, “Privacy issues in vehicular ad hoc networks,” in Proc. PETS, Jun. 2006, pp. 197–209.

[9] Y. Pan, J. Li, L. Feng, and B. Xu, “An analytical model for random changing pseudonyms scheme in VANETs,” in Proc. Int. Conf. NCIS, May 2011, pp.

141–145.

[10] R. Lu, X. Lin, T. Luan, X. Liang, and X. Shen, “Anonymity analysis on social spot based pseudonym changing for location privacy in VANETs,” in Proc. IEEE ICC, Jun. 2011, pp. 1–5.

[11] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, “Quantifying location privacy,” in Proc. IEEE Symp. Security Privacy, May 2011, pp. 247–262.

[12] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, “Protecting location privacy: Optimal strategy against localization attacks,” in Proc. ACM Conf. CCS, Oct. 2012, pp. 617–627.

[13] F. Schaub, Z. Ma, and F. Kargl, “Privacy requirements in vehicular communication systems,” in Proc. IEEE Int. Conf. PASSAT, Aug. 2009, pp. 139–145.

[14] Intelligent Transport Systems (ITS); Communications Architecture, European Norm EN 302 665, Sep. 2010, ETSI—European Telecommunications Standards Institute.

[15] E. Schoch and F. Kargl, “On the efficiency of secure beaconing in VANETs,” in Proc. 3rd ACM Conf. WiSec, Mar. 2010, pp. 111–116.

[16] E. Fonseca, A. Festag, R. Baldessari, and R. Aguiar, “Support of anonymity in VANETs—Putting pseudonymity into practice,” in Proc. IEEE WCNC, Mar. 2007, pp. 3400–3405.

[17] N. Bißmeyer, J. Petit, and K. M. Bayarou, “CoPRA: Conditional pseudonym resolution algorithm in VANETs,” in Proc. 10th IFIP/IEEE Annu. Conf. WONS, Mar. 2013, pp. 9–16.

[18] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, “Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping,” in Proc. 2nd IEEE VNC, Dec. 2010, pp. 174–181.

[19] J Petit, F Schaub, M Feiri, and F Kargl " Pseudonym Schemes in Vehicular Networks: A Survey" IEEE communication surveys & tutorials, vol. 17, no. 1, first quarter pp.228-255, 2015.

[20] B. Chaurasia, S. Verma, G. Tomar, and A. Abraham, “Optimizing pseudonym updation in vehicular ad hoc networks,” in Trans. Comput. Sci. IV, 2009, pp. 136–148.

[21] J. Liao and J. Li, “Effectively changing pseudonyms for privacy protection in VANETs,” in Proc. 10th ISPAN, Dec. 2009, pp. 648–652.

[22] A. Tomandl, D Herrmann et al., “ VANETsim; An open source simulator for security and privacy concepts in VANETs”, International Confernce on High Performance Computing and Simulation, 2014, pp.16-19

[23] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, “Mix-zones for location privacy in vehicular networks,” in Proc. ACM Workshop WiN-ITS, Aug. 2007, pp. 1–7.

[24] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, “An identity-based security system for user privacy in vehicular ad hoc networks,” IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 9, pp. 1227–1239, Sep. 2010.