ECHAHID HAMMA LAKHDAR UNIVERSITY - EL-OUED
Under the Supervision of the DGRSDT and in collaboration with the CRTI
International Pluridisciplinary PhD Meeting (IPPM'20)
23-26, 2020 1st Edition, February
Theme: Modern Technology and Fineness Life

Security-Aware Monitoring Approach for Location Abusing and Suspicious Behavior in Internet of Vehicles

Messaoud Babaghayou[a,*], Nabila Labraoui[a], Ado Adamou Abba Ari[b,c], Nasreddine Lagraa[d], Mohamed Amine Ferrag[e]

[a]*STIC Lab, Abou Bekr Belkaid University, P.O. Box 230, chetouane, Tlemcen 13000, Algeria*

[b]*LI-PaRAD Lab, Saint-Quentin-en-Yvelines University, 45 Avenue Etats-Unis 78035 Versailles cedex, France ´*

[c]*LaRI Lab, Maroua University, P.O. Box 814 Maroua, Cameroon*

[d]*LIM Lab, Amar Telidji University, P.O. Box G37, Route de Ghardaia (M'kam), Laghouat 03000, Algeria*

[e]*Department of Computer Science, Guelma University, B.P. 401, 24000, Algeria*

Email addresses: babaghayoumessaoud@hotmail.com (Messaoud Babaghayou), nabila.labraoui@mail.univ-tlemcen.dz (Nabila Labraoui), adoadamou.abbaari@gmail.com (Ado Adamou Abba Ari), n.lagraa@lagh-univ.dz (Nasreddine Lagraa), ferrag.mohamedamine@univ-guelma.dz (Mohamed Amine Ferrag)

Abstract

The fast and huge revolution on the wireless communication technologies and embedded systems had opened the gate towards promising implementations and applications; Vehicular-Ad-hoc Networks (VANETs) and the safety enhancing applications provided by the Internet of Vehicles (IoV) paradigm are one of them. By periodically broadcasting safety-beacons, vehicles can ensure a better safety driving experience as these beacons contain fine-grained location spread next to the neighborhood. Nevertheless, some attacks that modify, remove and encrypt location-related data included in beacons are threatening the road-safety considerably. In this paper, we provide a Security-Aware Monitoring Approach (SAMA) that protects against such a location abusing by allowing the Law-Side Authorities (LSAs) to monitor the potential malicious vehicles. SAMA is Implemented using the well-known triangulation concept via Received Signal Strength Indicator (RSSI) in conjunction with c++ map and multimap data-structures. The performances of SAMA are evaluated in terms of location-estimation precision and beacons collection per type (mono, duo and triangulation).

Keywords: location monitoring, position detection, triangulation, location privacy, malicious attacks, IoV, VANETs

1. Introduction

Vehicular Ad-hoc Network (VANET), the wireless network of cars had boosted the driving experience of road users enormously via communication types like Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) [1], in addition to providing a bases for the Vehicle to Everything (V2X) that serves as a core for the Internet of Vehicles (IoV) paradigm [2]. Parallelly, location detection techniques such as GPS, RSU-aided and Location Based Service (LBS) [3] are getting much attention due to their high utility [4]. To avoid accidents and traffic jams, vehicles must broadcast safety-beacon messages that contain the vehicle's status [5] including its location which, as a consequence, forms an environment instantiation. This beaconing is done in a range of 300m and up to 10 beacons per second [6].

1.1. Problematic and Research Motivation

This beaconing had opened location-privacy issues which were an incentive for the research community to find mitigation to these limitations; using pseudonyms and changing them over time was accepted as a fair solution [7] and much schemes had emerged [6]. In spite of being these schemes benign to the IoV users' location-privacy, they also open an attack vector to malicious vehicles as they can escape monitoring when modifying and/or encrypting such spatio-related beacons from the Law Enforcement Authority (LEA) without a defending mechanism, in addition for giving the option to launch Sybil attacks [8]. Localization techniques are becoming a must in such a case.

1.2. Contributions and Paper Organization

The contributions of the paper are stated as follows:

- Introducing our system model that leverages the power and financial abilities of the Law-Side Authority to monitor and protect against the resulting vector attacks.
- Recalling and formulating the used triangulation technique to detect a node (vehicle) by its Received Signal Strength Indicator (RSSI) and the nearby monitoring stations.
- Providing our proposed Security-Aware Monitoring Approach (SAMA) that estimates the location of potential malicious vehicles and explaining the used c++ map and multimap data-structures in addition to giving the pseudo-code of SAMA protocols and its results.

The remaining paper parts are presented as follows: Section 2, sheds light on legitimate privacy-schemes that encrypt beacon fields and discuss the localization-related state of the art. Next, the system model and coverage modes are described in section 3. Then, the proposed SAMA approach is explained in details in section 4. After

that, section 5 shows the location precision and collection per type results. Section 6 is consecrated for discussing the obtained results and potential future enhancements to the technique. Finally, section 7 concludes this research.

2. Related Work

This section is two folds; (a) the used techniques to encrypt location data included in beacons and (b) the location detection techniques deployed for wireless networks:

(a) altering the safety-messages format (for good) was highly debated in the previous years. Freudiger et al. had proposed the Cryptographic MIX-zones (CMIX) scheme [9] that aims at encrypting beacon messages in some areas (mixzones) to defend against unauthorized overhearing of these beacons, thus, having an opportunity to confuse the attacker when leaving the CMIX zones. Similarly, Wasef and Shen had presented the random encryption periods (REP) scheme [10] . REP lets vehicles encrypt their beacon messages in a group manner using a group key kg. This is done after one of the group members (called coordinator) launches the random encryption process that is followed by a certificate updating to confuse the tracker. Ying et al. [11] had provided another mix-zone based scheme that uses the encryption but the mix-zones here are created on the fly (dynamically) according to the vehicle's predicted location and other parameters.

Despite being these schemes an addition to the privacy level, they also entail the use of such techniques for subversion purposes, thus, finding mechanisms to deter such abusing is a must. (b) Location detection techniques are considered to be a plausible direction against such threats. In the context of location detection inside buildings, Bahl and Paramvir had suggested the use of a radio-frequency (RF) based system made for locating and tracking users inside buildings and was called RADAR [12]. RADAR gets benefit from the recorded and processed signal strength information received by multiple base stations situated at the area of interest. Their real world experiment showed that despite the signal's nature and the environment obstacles, they could achieve a precision ranging from 2 to 3 meters which in fact can correctly pinpoint a room inside a building. In the same context, Youssef et al. [13] had investigated a WLAN location determination technique called (the Joint Clustering technique). They base on the signal strength probability distributions and the clustering of locations in their scheme. The scheme's best advantage is the complexity reducing as it uses cluster based techniques and can be applied indoor and outdoor environments. The scheme can be applied as a helping tool to other context-aware applications. In [14], Svecko et al. had evaluated a particle filter algorithm used for the distance estimation via multiple antennas that are attached to the receiver. They had conducted the study on a real world environment and their proposed particle filter achieved better results than other propagation models (e.g., the ground reflection propagation model) which permits it to be a reliable distance estimator.

Besides being the transmitted signal a mean to reduce the IoV users' location privacy, they also can defend against location abusing and data encryption used by attackers.

3. System Model

3.1. Network Model

It consists of (a) the vehicles set S that is defined as $S = \{v_1, v_2, \ldots v_n\}$ where n represents the vehicles number and they communicate using the 802.11p standard via their On Board-Units (OBUs). and (b) the infrastructure that allows the use of different provided services via Road-Side-Units (RSUs), cellular towers and across the Internet to explore the V2X feature. This is illustrated in Fig. 1.

3.2. Threat Model

It refers to the malicious entity in the network. The main actor is (a) the attacker that possesses and controls (b) a set of vehicles Sa where Sa belongs to S. The attacker is responsible for spreading malicious and suspicious messages that, for example, use unknown encryption algorithms and encrypting indispensable message fields. The trigger for spreading this kind of messages is supposed to be done via Unmanned Aircraft-Vehicles (UAVs) by giving missions to deliver malicious orders. This is also illustrated in Fig. 1.

3.3. Security Model and Coverage Modes

It is the law-side entity that aims at ensuring road-safety and data-security by only allowing legitimate vehicles to be present in the network. Thus, keeping an eye on the potential malicious and suspicious vehicles is its main task. For this purpose, the use of many security monitoring stations ms(s) becomes a must. These ms(s) are meant to collect the suspicious messages and reporting them to a security tracking module (also defined as central module cm) and this later is responsible for performing the triangulation to pinpoint the monitored vehicle (mvi)'s whereabouts. A Law-Enforcement Authority (LEA) is connected to the system to make decisions (e.g., excluding an entity if proven to be guilty). The supposed available coverage modes are illustrated in Fig. 2. The densities are supposed to be applicable, we justify this by being the LEW a part of the government, hence, having both (a) the financial and (b) the reachability to deploy such a massive ms(s) implanting.

4. Proposed Approach

For the implementation, we use two c++ data-structures namely: map and multimap [15] and the detailed working will be explained in the next point. Fig. 3 shows the modus operandi of SAMA.

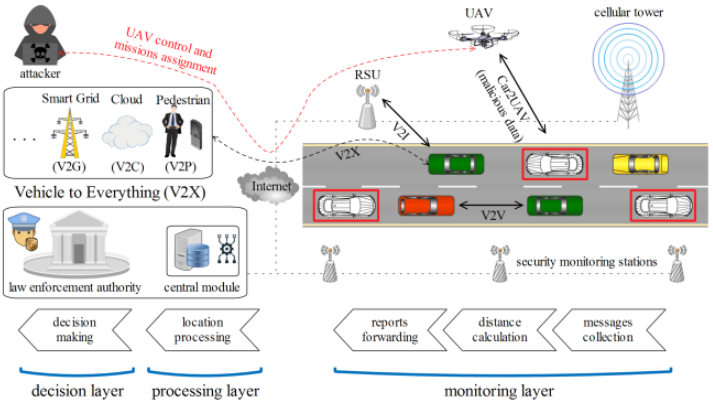

Figure 1: System model, principle actors and security layers

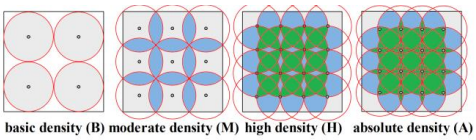

Figure 2: The assumed and used coverage modes

The adversary is able to use UAVs to give orders for data encryption; hiding his vehicle(s)' location becomes so foreseeable. In light of this, finding a counter-mechanism is a fair motivation. Benefiting from the location detection techniques serves to protect, expose and thwart such malicious acts substantially.

One of the most simplified and used distance estimation formulas is given in equation 1. Where Pt is the transmission power in (dBm) and d is the distance between the sender and the receiver in meter (m) [16]:

$$RSSI = Pt - 10n * log_{10}(d) \qquad (1)$$

This allows to find and calculate the distance d as follows (equation 2):

$$\boxed{d = 10^{\frac{Pt-RSSI}{10n}}} \qquad (2)$$

The distance d is at hand, what is remaining is just applying the geometric method to determine a location from three points knowing that each point Pi is represented by the triple location (xi, yi, zi) where i 2 f1;2;3g and their three distances a, b and c from the target point respectively. It is done via the equations set 3, 4 and 5:

$$\begin{cases} (x-x_1)^2 + (y-y_1)^2 = a^2 & (3) \\ (x-x_2)^2 + (y-y_2)^2 = b^2 & (4) \\ (x-x_3)^2 + (y-y_3)^2 = c^2 & (5) \end{cases}$$

By expanding and combining the equations (3 and 4) then (3 and 5), we get the equations set :

$$\begin{cases} 2(x_1-x_2)x + 2(y_1-y_2)y = -a^2 + b^2 + {x_1}^2 + {y_1}^2 - {x_2}^2 - {y_2}^2 & (6) \\ 2(x_1-x_3)x + 2(y_1-y_3)y = -a^2 + b^2 + {x_1}^2 + {y_1}^2 - {x_3}^2 - {y_3}^2 & (7) \end{cases}$$

We assume and define the following (the set 8):

$$\begin{cases} \alpha_1 = 2x_1 - 2x_2 \\ \alpha_2 = 2x_1 - 2x_3 \\ \beta_1 = 2y_1 - 2y_2 \\ \beta_2 = 2y_1 - 2y_3 \\ \gamma_1 = -a^2 + b^2 + {x_1}^2 + y_1 - {x_2}^2 - y_2 \\ \gamma_2 = -a^2 + c^2 + {x_1}^2 + y_1 - {x_3}^2 - y_3 \end{cases} \qquad (8)$$

This results in a one more step to the final solution:

$$\begin{cases} \alpha_1 x + \beta_1 y = \gamma_1 & (9) \\ \alpha_2 x + \beta_2 y = \gamma_2 & (10) \end{cases}$$

Finally, the obtained location, in terms of x and y (assuming z is identical) coordinates, is gotten as follows:

$$\begin{cases} x = \dfrac{\alpha 2\gamma 1 - \alpha 1\gamma 2}{\alpha 2\beta 1 - \alpha 1\beta 2} & (11) \\ y = \dfrac{\beta 2\gamma 1 - \beta 1\gamma 2}{\beta 2\alpha 1 - \beta 1\alpha 2} & (12) \end{cases}$$

SAMA Implemented Protocols

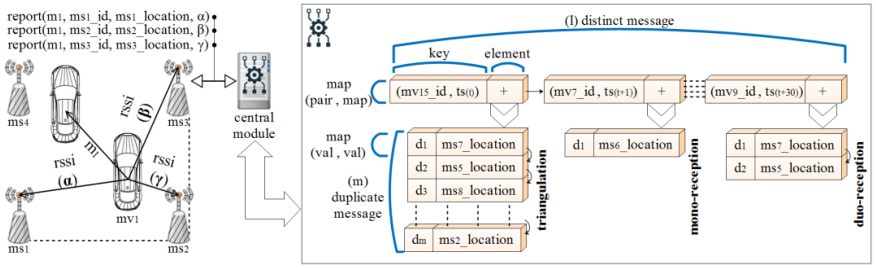

Figure 3: SAMA implementation and functioning illustration

1. on message reception by a monitoring station

each ms_i is devoted to collect the nearby messages and supposed to be integrating a lightweight calculation module dedicated to find a distance d from a gotten RSSI value of the received message. A report is sent next to the central module. This is shown in kind of a pseudo-algorithm; Algorithm. 1.

2. on message reception by the central module

upon receiving a report from msi, cm proceeds to treating the obtained information like the distance between msi and the target vehicle in addition to the coordinates of msi which will be stored in the database of cm to be used next to calculate the vehicle's estimated location. The pseudo-code is given in Algorithm. 2.

Algorithm 1 message reception by a monitoring station ms_i

```
1: procedure Receiving_Packet(Message* msg)
2:     if (Is_Suspicious(msg)) then
3:         RSSI ← getReceivedPower(msg);
4:         d ← calculateDistance(RSSI);
5:         send2Central(msg, ms_i.ID, ms_i.Location, d);
6:     end if
7: end procedure
```

Algorithm 2 message reception by central module from ms_i

```
1: procedure Receiving_Report(Message* msg, int ms_i.ID, Coord ms_i.Location, double d)
2:     if I had not received this msg before then create a new entry in the Distinct_msg_Map with the (ms_i.ID, ms_i.timeStamp) pair as a key and attach a multimap duplicate_msg_Map in the value field of Distinct_msg_Map and add (d) as a key and (ms_i.Location) as a value.
3:     else, just add the received message to the multimap duplicate_msg_Map belonging to the entry of the received message msg by adding the distance (d) as a key and the location (ms_i.Location) as a value.
4:     end if
5: end procedure
```

5. Simulation Runs and Results

5.1. Simulation Setup

or the evaluation, the following tools are used: SUMO as the mobility simulator, Omnet++ as the network simulator and Veins [17] as the vehicular extension that acts as a bridge between SUMO and Omnet++. The used environment is an urban map consists of Munich city central taken by the OpenStreet-Map tool. The exact model is found in [18]. As for the vehicles generation, we use the inter-arrival rate of 2.61 seconds per vehicle in a total simulation time of 300 seconds which leads to a generation of 115 vehicles. A variation of monitoring scenarios is also exploited and shown in table 1. Additionally, we modified the PREXT [18] extension; that is a privacy extension, to integrate the central module and to add the triangulation technique to locate a specific node. For a holistic evaluation, we monitor every vehicle to measure the performances of SAMA under the toughest possible case with a frequency of one message per second.

5.2. Obstacles and Obstacles-Free Scenarios

In these two scenarios, we are interested on evaluating the effects of the Simple Obstacle Shadowing mode; that is an Analogue Model used to model the physical characteristics of the wireless medium. Thus, we consider the Obstacles scenario model when we are taking the obstacles' effect during the communication into account and when we are not, we consider that as an Obstacles-Free Scenario.

5.3. Simulation Results

Table 1: Density details and achieved precision for Obstacle and Obstacles-Free scenarios

Density characteristics			Achieved precision during triangulation (m)					
			With obstacles			Without obstacles		
Density mode	Overlapping (m)	Number of MSs	Average	Best	Worst	Average	Best	Worst
Absolute (A)	166	110	24.75	$5.9*10^{-5}$	87.55	$2.3*10^{-2}$	$3.7*10^{-7}$	52.26
High (H)	150	90	22.15	$1.1*10^{-5}$	83.59	$5.1*10^{-5}$	$5.5*10^{-7}$	$9.8*10^{-5}$
Moderate (M)	88	42	-	-	-	$7.1*10^{-6}$	$3.3*10^{-7}$	$1.5*10^{-5}$
Basic (B)	0	25	-	-	-	-	-	-

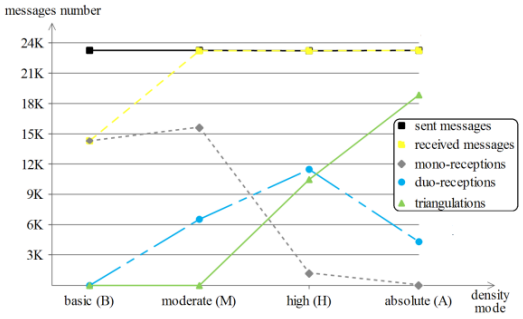

Figure 4: The sent messages number and the different reception types in the Obstacles scenario

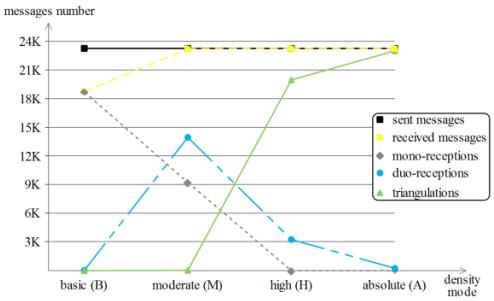

Figure 5: The sent messages number and the different reception types in the Obstacles-Free scenario

Fig. 4 shows that the monitoring stations could only collect about half of the sent message in the network when applying the basic density and they were just mono-receptions. However, the collection was increased to 100% in the other densities and the triangulations achieved their pick (more than 18k message) when in the absolute density.

as shown in Fig. 5, the almost same results happened, but, with a remarkable powerful messages collection than that of the previous scenario. The better collection of sent messages in the basic density is an example for that in addition to the approximate 100% of successful triangulations in the absolute density.

Now is the difference between the real and the estimated location. Three parameters are taken per each scenario: the average, the best and the worst precision. From Table 1, the Simple Obstacle Shadowing mode had affected the triangulation method enormously letting it be only feasible for the high and the absolute densities in the Obstacles scenario. Additionally, the obtained average is ranging in the order of 20 to 25 meters which is not so precise, however, still gives a hint about the zone of the monitored vehicle mvi. For the Obstacles-Free, the triangulation method was successful in all density modes but the basic density. This is due to the absence of the Simple Obstacle Shadowing mode that used to affect the communications, not just for that, but it also enhanced the average precision that is, in all three densities, less than the order of $3*10^{-2}$. This, gives the security bodies a very accurate location of the mv_i.

6. Discussion and Future Work

A set of observation can be drawn: (a) the different density modes influence the amount of collected messages, the collection per type and the achieved precision. Also, (b) when considering the Simple Obstacle Shadowing mode, a lot of messages do not reach the monitoring stations appropriately leading to few receptions and less triangulations, hence, thwarting the location estimation. Additionally, (c) in the absolute density model, the dense overlapping stations, despite them giving higher number of triangulations, they unfortunately also degrade the achieved precisions. Finally, (d) when moving from the lowest (base) to the highest (absolute) density, the dominant type of collection will be that of the triangulations which is so natural as, theoretically, the intense implementation of monitoring stations leads to higher triangulation chances.

Even though being the Simple Obstacle Shadowing mode a real world effect that influences the precision of the monitoring stations considerably, it still gives some degree of precision which can be given as an entry to other location detection techniques. Moreover, the road map restriction can be used to infer the exact location of a monitored vehicle by excluding the non-common locations by the help of the different time instants and the moving context. This emphasizes a possible promising work direction with just mono-receptions for the location detection task.

7. Conclusion

The location data hampering via encrypting and sealing the location fields in messages can be seen as a serious secrity breach. In this work we recalled the possibility of blurring the location by legitimate privacy schemes which highlights the negative effect if used maliciously. Fortunately, a set of location detection techniques does also exist; the set that uses the transmission signal as an indicator to the location. Among the applications, there is the triangulation method, explained and used on our proposed Security-Aware Monitoring Approach (SAMA). A malicious attacker that gives order to his controlled vehicles via UAV-assisted missions in where, and for an extreme evaluation, we suppose that the orders are given to all present vehicles in the map which exposes the performances of SAMA under the worst possible situation. Two scenarios are considered: Obstacles and Obstacles-Free in addition to four density modes: basic, moderate, high and absolute. The obtained results are discussed in Section 6 where it showed the precision and the feasibility of SAMA especially in the Obstacles-Free scenario.

References

1. G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," IEEE communications surveys & tutorials, vol. 13, no. 4, pp. 584–616, 2011.

2. S.-h. Sun, J.-l. Hu, Y. Peng, X.-m. Pan, L. Zhao, and J.-y. Fang, "Support for vehicle-to-everything services based on lte," IEEE Wireless Communications, vol. 23, no. 3, pp. 4–8, 2016.

3. M. Babaghayou, N. Labraoui, and A. A. A. Ari, "Epp: Extreme points privacy for trips and home identification in vehicular social networks." in JERI, 2019.

4. N. Saeed, W. Ahmad, and D. M. S. Bhatti, "Localization of vehicular ad-hoc networks with rss based distance estimation," in 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET). IEEE, 2018, pp. 1–6.

5. S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," Journal of network and computer applications, vol. 37, pp. 380–392, 2014.

6. M. Babaghayou and N. Labraoui, "Transmission range adjustment influence on location privacy-preserving schemes in vanets," in 2019 International Conference on Networking and Advanced Systems (ICNAS). IEEE, 2019, pp. 1–6.

7. M. Babaghayou, N. Labraoui, and A. A. A. Ari, "Location-privacy evaluation within the extreme points privacy (epp) scheme for vanet users," International Journal of Strategic Information Technology and Applications (IJSITA), vol. 10, no. 2, pp. 44–58, 2019.

8. Y. Yao, B. Xiao, G. Yang, Y. Hu, L. Wang, and X. Zhou, "Power control identification: A novel sybil attack detection scheme in vanets using rssi," IEEE Journal on Selected Areas in Communications, vol. 37, no. 11, pp. 2588–2602, 2019.

9. J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," in ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS), no. LCA-CONF-2007-016, 2007.

10. A. Wasef and X. S. Shen, "Rep: Location privacy for vanets using random encryption periods," Mobile Networks and Applications, vol. 15, no. 1, pp. 172–185, 2010.

11. B. Ying, D. Makrakis, and H. T. Mouftah, "Dynamic mix-zone for location privacy in vehicular networks," IEEE Communications Letters, vol. 17, no. 8, pp. 1524–1527, 2013.

12. P. Bahl, V. N. Padmanabhan, V. Bahl, and V. Padmanabhan, "Radar: An in-building rf-based user location and tracking system," 2000.

13. M. A. Youssef, A. Agrawala, and A. U. Shankar, "Wlan location determination via clustering and probability distributions," in Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003.(PerCom 2003). IEEE, 2003, pp. 143–150.

14. J. Svecko, M. Malajner, and D. Gleich, "Distance esti- ˇ mation using rssi and particle filter," ISA transactions, vol. 55, pp. 275–285, 2015.

15. "<map>," http://www.cplusplus.com/reference/map, accessed: 2019-12-01.

16. J. Du, J.-F. Diouris, and Y. Wang, "A rssi-based parameter tracking strategy for constrained position localization," EURASIP Journal on Advances in Signal Processing, vol. 2017, no. 1, p. 77, 2017.

17. C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved ivc analysis," IEEE Transactions on mobile computing, vol. 10, no. 1, pp. 3–15, 2011.

18. K. Emara, "Poster: Prext: privacy extension for veins vanet simulator," in 2016 IEEE Vehicular Networking Conference (VNC). IEEE, 2016, pp. 1–2.