









SAMA: Security-Aware Monitoring Approach for Location Abusing and UAV GPS-Spoofing Attacks on Internet of Vehicles

Messaoud Babaghayou¹ , Nabila Labraoui¹ , Ado Adamou Abba Ari^{2,3} ,
Nasreddine Lagraa⁴ , Mohamed Amine Ferrag⁵ ,
and Leandros Maglaras^{1,2,3,4,5,6} 

¹ STIC Lab, Abou Bakr Belkaid University of Tlemcen,
P.O. Box 230, 13000 Chetouane, Tlemcen, Algeria
nabila.labraoui@univ-tlemcen.dz

² LaRI Lab, University of Maroua, P.O. Box 814, Maroua, Cameroon

³ LI-PaRAD Lab, Saint-Quentin-en-Yvelines University, 45 Avenue Etats-Unis,
78035 Versailles cedex, France
n.lagraa@lagh-univ.dz

⁴ LIM Laboratory, UATL University,
P.O. Box G37, Route de Ghardaia (M'kam), 03000 Laghouat, Algeria
ferrag.mohamedamine@univ-guelma.dz

⁵ School of C, University of Guelma,
B.P. 401, 24000 Guelma, Algeria
leandros.maglaras@dmu.ac.uk

⁶ School of Computer Science and Informatics, De Montfort University,
Leicester LE1 9BH, UK

Abstract. The quick revolution on the wireless communication technologies had opened the gate towards promising implementations; 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 since beacons contain fine-grained location that is sent to the neighborhood. Nevertheless, some attacks basing on falsify or encrypt location-related data are threatening the road-safety considerably. In this paper, and by assuming a GPS-spoofing attack originated from Unmanned-Aircraft-Vehicles (UAV) system, we provide a Security-Aware Monitoring Approach (SAMA) that protects vehicles against such location abusing by allowing the Law-Side Authority (LSA) to monitor the potential malicious or tricked vehicles. SAMA is Implemented using the 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.

Keywords: Location monitoring · Position detection · RSSI · Triangulation · Location privacy · Malicious attacks · UAV attacks · GPS-spoofing · Data falsification · IoV · VANETs

1 Introduction

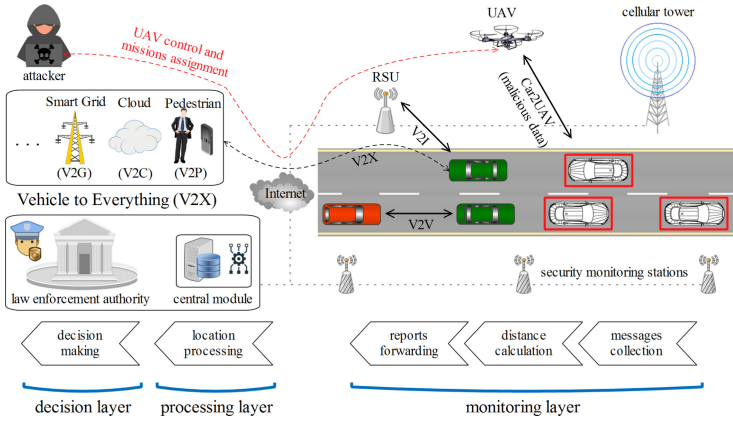


Fig. 1. System model, principle actors and security layers

Vehicle Ad-hoc Network (VANET) [1], 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) [2], in addition to providing a bases for the Vehicle to Everything (V2X) [3] that serves as a core for the Internet of Vehicles (IoV) paradigm [4]. Moreover, location detection techniques such as Global Positioning System (GPS) [5], Road-side Unite (RSU)-aided and Location Based Service (LBS) [6] are getting much attention due to their high utility [7]. To avoid accidents and traffic jams, vehicles must broadcast safety-beacon messages [8] that contain the vehicle’s status [9] 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 [10].

1.1 Problematic and Research Motivation

Since the world is diving more and more into the technology, many serious cyber attacks and exploits are emerging each time [11]. This beaconing had opened location-privacy issues which were an incentive for the research community to find mitigation to these limitations [12]; using pseudonyms and changing them over time was accepted as a fair solution [6] and much schemes had emerged [13]. 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) [14] without a defending mechanism, in addition for giving the option to launch Sybil attacks [15]. Localization techniques are becoming a must in such a case. Generally speaking, much cryptography and

trust-based mechanisms [16, 17] were proposed and used to cope with the emerging security threats but they do not treat all kinds of security gaps. Another reason for the necessity of location techniques may be noticed when considering the critical vulnerability of the GPS technique [18]; we are talking about the GPS-spoofing attack [19]. The GPS-spoofing attack is defined as forging a falsified spatio-temporal data to the receiving devices using GPS-mimicker devices that aim at emitting a GPS signal but this later is falsified and coming from a malicious source and is hard to get verified [20, 21]. With this said, we give a high importance to checking the transmitted location by vehicles to their vicinity where our assumed spoofer is considered to be a set of Unmanned-Aircraft-Vehicles (UAVs) [22] controlled by an attacker who aims at wreaking havoc on the system functioning. The exact scenario and used mechanisms are explained later on. Moreover, the used abbreviations in this paper are provided in Table 1.

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.
- Giving and shedding-light to a GPS-spoofing mechanism that exploits the possession of a UAV system to let vehicles send falsified locations.
- 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: Sect. 2, sheds light on legitimate privacy-schemes that encrypt beacon fields in conjunction with the GPS-spoofing attacks that let vehicles send falsified locations and discuss the localization-related state of the art. Next, the system model and coverage modes are described in Sect. 3. Then, the proposed SAMA approach is explained in details in Sect. 4. After that, Sect. 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, Sect. 7 concludes this research.

2 Related Work

This section is three folds; (a) the used techniques to encrypt location data included in beacons, (b) the GPS spoofing problem that leads to sending a

Table 1. List of abbreviations

SAMA	Security-Aware Monitoring Approach
LSA	Law-Side Authority
RSSI	Received Signal Strength Indicator
RSU	Road-side Unite
LBS	Location Based Service
LEA	Law Enforcement Authority
CMIX	Cryptographic MIX-zones
REP	Random Encryption Periods
RADAR	An In-Building RF-based User Location and Tracking System
OBU	On-Board-Unit
ms_i	Monitoring station number i
CM	Central Module
mv_i	Monitored vehicle number i
PREXT	Privacy Extension for Veins

wrong geo-location data by vehicles and (c) 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 [23] that aims at encrypting beacon messages in some areas (mix-zones) 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 [24]. REP lets vehicles encrypt their beacon messages in a group manner using a group key k_g . 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. [25] 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 the location-privacy preserving schemes an addition to the privacy level, they also entail the use of such techniques for subversion purposes; i.e., encrypting the location for the bad. (b) Similarly, and indirectly, a vehicle may send wrong geo-location data due to a wrong GPS signal reception; we point out to the GPS-spoofing attack [26] that is by definition: leading the receiver GPS device to believe receiving a legit GPS signal while in fact it is falsified and forged

from another malicious source. The powerfulness and usability of GPS-spoofing is shown to be a fact as stated in [27] where J. Noh et al. demonstrated the exploit of the Unmanned-Aircraft-Vehicles UAV safe-hijacking using the GPS spoofing technique for the good (defending against terrorist UAVs). Another work by Y. Guo et al. that investigated a covert spoofing algorithm [28] in the UAV context had shown the applicability of such spoofing techniques. This just proves the possibility of exploiting the GPS spoofing attacks on other fields; spoofing the location of vehicles. As a result, vehicles are expected to send falsified location data upon receiving forged GPS signals and from here the necessity of detecting such an odd behavior becomes a must.

With all of this said, finding mechanisms to deter such abusing becomes a must. (c) 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 An In-Building RF-based User Location and Tracking System (RADAR) [29]. 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 m which in fact can correctly pinpoint a room inside a building. In the same context, Youssef et al. [30] 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 [31], Svečko 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

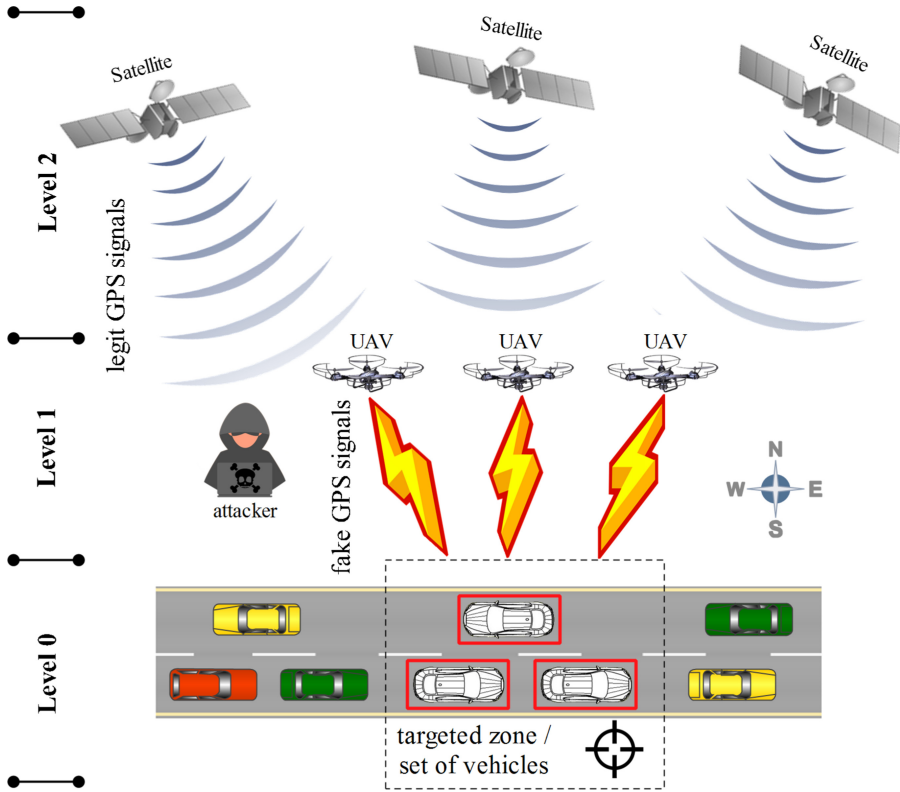


Fig. 2. GPS spoofing illustration using UAV technology

In this section, we give our network and threat models. Then, we demonstrate our adversary’s GPS spoofing technique that bases on UAVs. Additionally, we describing the security model and the used coverage modes.

3.1 Network Model

It consists of (a) the vehicles set S that is defined as $S = \{v_1, v_2, \dots, v_n\}$ where n represents the vehicles number and they communicate using the 802.11p standard (explained in [32]) via their On-Board-Units (OBUs) [33]. and (b) the infrastructure that allows the use of different provided services via Road-Side-Units (RSUs) [34], 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 S_a where $S_a \in S$. The attacker [35] 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 UAVs by giving UAV-missions [36] to deliver malicious orders. This is also illustrated in Fig. 1.

3.3 UAV GPS-Spoofing Attack

This kind of attacks is foreseeable with the advent of UAVs, their cheapness and their availability. Our scenario, which is illustrated in Fig. 2, consists of three levels:

- *Level 2* : that is the origin of the legit GPS signal. Normally, vehicles take their locations by receiving the emitted GPS signal from the satellites to help determining their whereabouts.
- *Level 1*: that is the exploited point by the adversary who aims at emitting a stronger and faked GPS signal to mislead the vehicles on their location/whereabouts. The taken scenario considers two kind of attacks (a) zone targeting and (b) vehicles set targeting and in both of them, a set of UAVs are used to emit the falsified GPS signal.
- *Level 0*: that is the lower level where vehicles operate. When those vehicles are targeted, their sensing of the location are likely to be tricked especially that detecting a legit GPS signal from a fake one is still a big challenge to the research community; the GPS-spoofing attack [37].

By being the attacker able to forge falsified location and execute the GPS-spoofing attack, the targeted vehicles are expected to begin sending wrong geo-location data. Sending a wrong geo-location data may also be intentional in the case of attacker vehicles but considering the scenario of the GPS-spoofing attack, we do not want to instantly judge the behavior of the vehicle. Either way, comparing what is sent to where the vehicles is really at becomes mandatory to deal with such a possible attack scenario.

3.4 Types of Signal Receptions

When communicating, the sending vehicle emits a signal. Now when trying to receive that signal by a reception device, four main scenarios may occur: (a) an unsuccessful eavesdropping or reception with no collection at all, (b) single or mono-reception, (c) due-reception and a successful reception by getting the sent signal with at least three devices; that is the triangulation technique. Figure 3 shows the aforementioned scenarios.

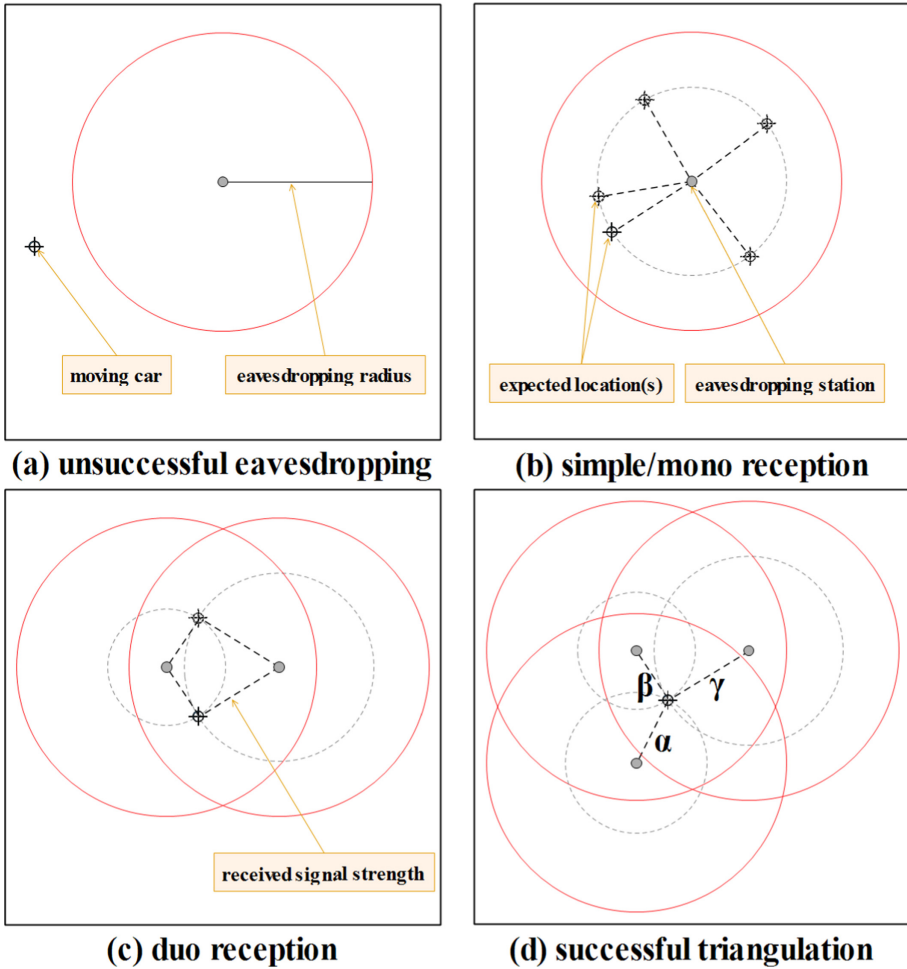


Fig. 3. The different reception scenarios of an emitted signal by a moving car

3.5 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 (also mislead vehicles; the GPS-spoofing attack victims) 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 (mv_i)'s whereabouts. A 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. 4. The

densities are supposed to be applicable, we justify this by being the LEA a part of the government, hence, having both (a) the financial and (b) the reachability to deploy such a massive $ms(s)$ implanting would not be a problem (unlike for individual persons [38]).

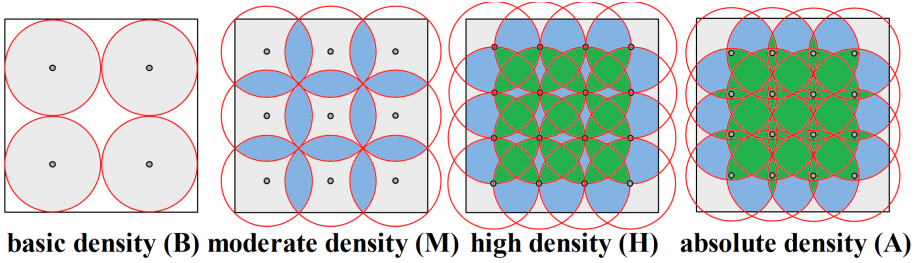


Fig. 4. The assumed and used coverage modes

4 The Proposed Approach: SAMA

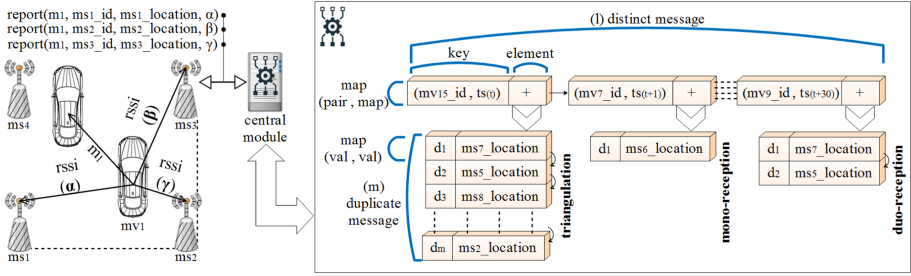


Fig. 5. SAMA implementation and functioning illustration

SAMA bases on the different received signal strengths from the proximal vehicles to the $ms(s)$. For the implementation, we use two c++ data-structures namely: map and multimap [39] and the detailed working is explained in the next point. Figure 5 shows the modus-operandi of SAMA.

4.1 Description and Motivation

The adversary is able to use UAVs either to give orders for data encryption; hiding his vehicle(s)' location or using his UAVs in order to execute the GPS-spoofing attack; misleading the targeted vehicles. Thus, location protection.

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.

4.2 The Techniques' Principles

SAMA bases on two depending steps: (a) a prior distance estimation then (b) location estimation using the calculate distances afterward. The two steps are explained as follows:

Distance Estimation. One of the most simplified and used distance estimation formulas is given in Eq. 1. Where Pt is the transmission power in (dBm) and d is the distance between the sender and the receiver in meter (m) [40]:

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

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

$$d = 10^{\frac{Pt - RSSI}{10n}} \tag{2}$$

Location Estimation via the Triangulation Technique. 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 P_i is represented by the triple location (x_i, y_i, z_i) where $i \in \{1, 2, 3\}$ 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):

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

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

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

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

$$\begin{cases} x = \frac{\alpha_2 \gamma_1 - \alpha_1 \gamma_2}{\alpha_2 \beta_1 - \alpha_1 \beta_2} \\ y = \frac{\beta_2 \gamma_1 - \beta_1 \gamma_2}{\beta_2 \alpha_1 - \beta_1 \alpha_2} \end{cases} \quad (11)$$

$$\quad (12)$$

4.3 SAMA Implemented Protocols

In this part, the *on message reception by a monitoring station* and *on message reception by the central module* protocols are explained in details with additional pseudo-algorithms as follows:

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.

Algorithm 1. Message reception by a monitoring station ms_i

```

1: procedure RECEIVING_PACKET(MESSAGE* MSG)
2:   if ( $Is\_Suspicious(msg)$ ) then
3:      $RSSI \leftarrow getReceivedPower(msg)$ ;
4:      $d \leftarrow calculateDistance(RSSI)$ ;
5:     send2Central(msg,  $ms_i.ID$ ,  $ms_i.Location$ ,  $d$ );

```

On message reception by the central module upon receiving a report from ms_i , CM proceeds to treating the obtained information like the distance between ms_i and the target vehicle in addition to the coordinates of ms_i 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 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 Simulation Runs and Results

Table 2. 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	-	-	-	-	-	-

5.1 Simulation Setup

For the evaluation, the following tools are used: SUMO as the mobility simulator, Omnet++ as the network simulator and Veins [41] 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 Open-Street-Map tool. The exact model is found in [42]. As for the vehicles generation, we use the inter-arrival rate of 2.61 seconds per vehicle in a total simulation time of 300 s which leads to a generation of 115 vehicles. A variation of monitoring scenarios is also exploited and shown in Table 2. Additionally, we modified the PREXT [42] 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. Thus, the case of only a set of targeted vehicles that are receiving the GPS-spoofing attack alone are not considered, but, all vehicles are considered.

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

For the Obstacles Scenario Figure 6 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.

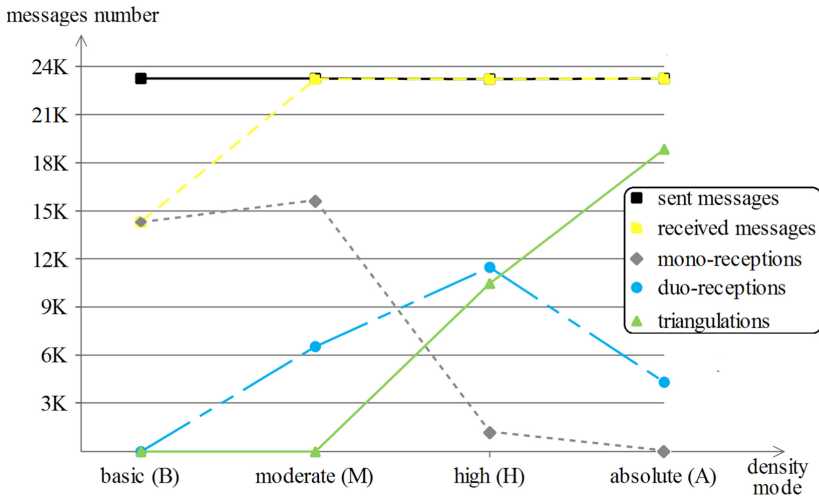


Fig. 6. The sent messages number and the different reception types in the Obstacles scenario

For the Obstacles-Free scenario as shown in Fig. 7, 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.

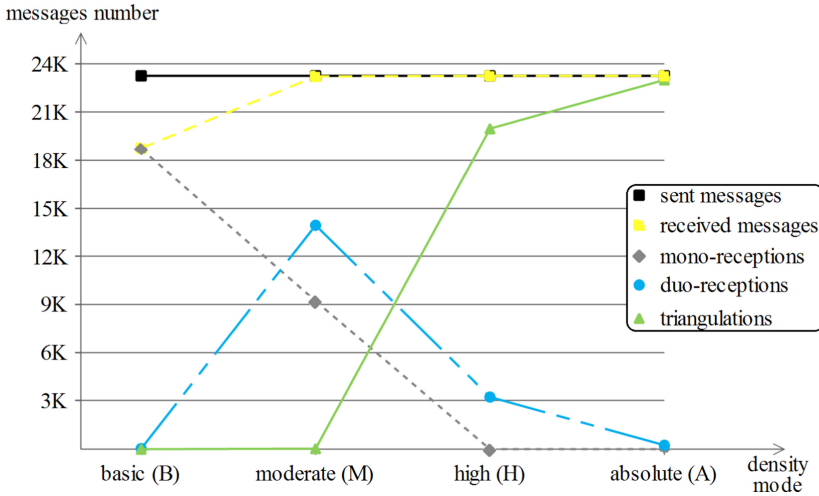


Fig. 7. The sent messages number and the different reception types in the Obstacles-Free scenario

The achieved location precision which 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 2, 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 m which is not so precise, however, still gives a hint about the zone of the monitored vehicle mv_i . 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 with the help of the different time instants and the moving context as shown in Fig. 8. This emphasizes a possible promising work direction with just mono-receptions instead of the reliance on triangulation for the location detection task.

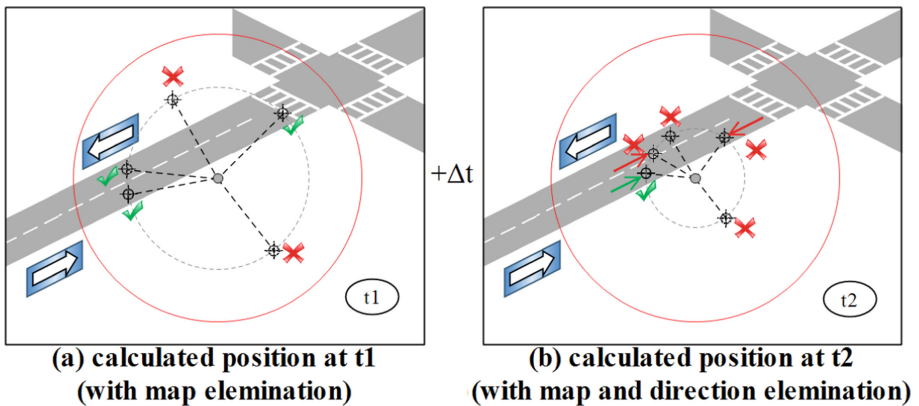


Fig. 8. Exploiting the road restriction and time instances to eliminate false samples in just a mono-reception scenario

7 Conclusion

The location data hampering via encrypting and sealing the location fields in messages or launching GPS-spoofing attacks on a set of targeted vehicles can be seen as a serious security breach. In this work, we recalled the possibility of blurring the location by legitimate privacy schemes which highlight the negative effect if used maliciously in addition to the location misleading possibility resulted from the GPS-spoofing attacks. 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 an order to his controlled vehicles and/or uses GPS-spoofing attacks 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 Sect. 6 where it showed the precision and the feasibility of SAMA, especially in the *Obstacles-Free* scenario.

References

1. Shilin, P., Kirichek, R., Paramonov, A., Koucheryavy, A.: Connectivity of VANET segments using UAVs. In: *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, pp. 492–500. Springer, Cham (2016), <https://doi.org/10.1007/978-3-319-23126-6>
2. Karagiannis, G., et al.: Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Commun. Surv. Tutor.* **13**(4), 584–616 (2011)
3. Chen, S., et al.: Vehicle-to-everything (v2x) services supported by LTE-based systems and 5g. *IEEE Commun. Stand. Mag.* **1**(2), 70–76 (2017)
4. Sun, S.-H., Hu, J.-L., Peng, Y., Pan, X.-M., Zhao, L., Fang, J.-Y.: Support for vehicle-to-everything services based on LTE. *IEEE Wirel. Commun.* **23**(3), 4–8 (2016)
5. Parkinson, B.W., Enge, P., Axelrad, P., Spilker, Jr., J.J.: *Global Positioning System: Theory and Applications*, Vol. II. American Institute of Aeronautics and Astronautics, Reston (1996)
6. Babaghayou, M., Labraoui, N., Ari, A.A.A.: Location-privacy evaluation within the extreme points privacy (EPP) scheme for VANET users. *Int. J. Strat. Inf. Technol. Appl.* **10**(2), 44–58 (2019)
7. Saeed, N., Ahmad, W., Bhatti, D.M.S.: Localization of vehicular ad-hoc networks with RSS based distance estimation. In: *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, pp. 1–6. IEEE (2018)
8. Kerrache, C.A., Calafate, C.T., Cano, J.-C., Lagraa, N., Manzoni, P.: Trust management for vehicular networks: an adversary-oriented overview. *IEEE Access* **4**, 9293–9307 (2016)
9. Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H., Zedan, H.: A comprehensive survey on vehicular ad hoc network. *J. Netw. Comput. Appl.* **37**, 380–392 (2014)
10. Babaghayou, M., Labraoui, N., Ari, A.A.A., Gueroui, A.M.: Transmission range changing effects on location privacy-preserving schemes in the internet of vehicles. *Int. J. Strat. Inf. Technol. Appl.* **10**(4), 33–54 (2019)
11. Ferrag, M.A., Babaghayou, M., Yazici, M.A.: Cyber security for fog-based smart grid SCADA systems: solutions and challenges. *J. Inf. Secur. Appl.* **52**, (2020)
12. Babaghayou, M., Labraoui, N., Ferrag, M.A., Maglaras, L.: Between location protection and overthrowing: a contrariness framework study for smart vehicles. In: *39th IEEE International Conference on Consumer Electronics (ICCE)*. IEEE (2020)
13. Babaghayou, M., Labraoui, N., Ari, A.A.A., Lagraa, N., Ferrag, M.A.: Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: a survey. *J. Inf. Secur. Appl.* **55** (2020)
14. Hasrouny, H., Samhat, A.E., Bassil, C., Laouiti, A.: VANET security challenges and solutions: a survey. *Veh. Commun.* **7**, 7–20 (2017)
15. Yao, Y., Xiao, B., Yang, G., Hu, Y., Wang, L., Zhou, X.: Power control identification: a novel Sybil attack detection scheme in VANETs using RSSI. *IEEE J. Select. Areas Commun.* **37**(11), 2588–2602 (2019)

16. Tchakounté, F., Calvin, K.A., Ari, A.A.A., Mbogne, D.J.F.: A smart contract logic to reduce hoax propagation across social media. *J. King Saud. Univ. Comput. Inf. Sci.* (2020)
17. Ferrag, M.A., Maglaras, L., Ahmim, A., Derdour, M., Janicke, H.: RDTIDS: rules and decision tree-based intrusion detection system for internet-of-things networks. *Fut. Internet* **12**(3), 44 (2020)
18. Risbud, P., Gatsis, N., Taha, A.: Vulnerability analysis of smart grids to GPS spoofing. *IEEE Trans. Smart Grid* **10**(4), 3535–3548 (2018)
19. Shepard, D.P., Humphreys, T.E., Fansler, A.A.: Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *Int. J. Crit. Infrastruct. Prot.* **5**(3–4), 146–153 (2012)
20. Warner, J.S., Johnston, R.G.: GPS spoofing countermeasures. *Homel. Secur. J.* **25**(2), 19–27 (2003)
21. Kosmanos, D., et al.: A novel intrusion detection system against spoofing attacks in connected electric vehicles. *Array* **5**, 100013 (2020)
22. Shakhathreh, H., et al.: Unmanned aerial vehicles (UAVs): a survey on civil applications and key research challenges. *IEEE Access* **7**, 48 572–48 634 (2019)
23. Freudiger, J., Raya, M., Félegyházi, M., Papadimitratos, P., Hubaux, J.-P.: 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)
24. Wasef, A., Shen, X.S.: Rep: location privacy for VANETs using random encryption periods. *Mobile Netw. Appl.* **15**(1), 172–185 (2010)
25. Ying, B., Makrakis, D., Mouftah, H.T.: Dynamic mix-zone for location privacy in vehicular networks. *IEEE Commu. Lett.* **17**(8), 1524–1527 (2013)
26. Ahmad, M., Farid, M.A., Ahmed, S., Saeed, K., Asharf, M., Akhtar, U.: Impact and detection of GPS spoofing and countermeasures against spoofing. In: *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, pp. 1–8. IEEE (2019)
27. Noh, J., et al.: Tractor beam: safe-hijacking of consumer drones with adaptive GPS spoofing. *ACM Trans. Privacy Secur.* **22**(2), 1–26 (2019)
28. Guo, Y., Wu, M., Tang, K., Tie, J., Li, X.: Covert spoofing algorithm of UAV based on GPS/INS-integrated navigation. *IEEE Trans. Veh. Technol.* **68**(7), 6557–6564 (2019)
29. Bahl, p., Padmanabhan, V.N.: Radar: an in-building RF-based user location and tracking system. In: *Proceedings IEEE INFOCOM 2000 Conference on Computer Communications, Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No. 00CH37064)*, vol. 2. pp. 775–784. IEEE (2000)
30. Youssef, M.A., Agrawala, A., Shankar, A.U.: WLAN location determination via clustering and probability distributions. In: *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003 (PerCom 2003)*, pp. 143–150. IEEE (2003)
31. Svečko, J., Malajner, M., Gleich, D.: Distance estimation using RSSI and particle filter. *ISA Trans.* **55**, 275–285 (2015)
32. Jiang, D., Delgrossi, L.: IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments. In: *VTC Spring 2008-IEEE Vehicular Technology Conference*, pp. 2036–2040. IEEE (2008)
33. Tengler, S., Auflick, J.: Vehicle on-board unit. US Patent 7,554,435, 30 June 2009
34. Park, S., Aslam, B., Turgut, D., Zou, C.C.: Defense against sybil attack in vehicular ad hoc network based on roadside unit support. In: *MILCOM 2009–2009 IEEE Military Communications Conference*, pp. 1–7. IEEE (2009)

35. Sumra, I.A., Ahmad, I., Hasbullah, H., et al.: Behavior of attacker and some new possible attacks in vehicular ad hoc network (VANET). In: Sumrain, I.A., et al. (eds.) 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pp. 1–8. IEEE (2011)
36. Wegener, S., et al.: UAV autonomous operations for airborne science missions. In: AIAA 3rd “Unmanned Unlimited” Technical Conference, Workshop and Exhibit, 2004, p. 6416 (2004)
37. Haq, S., Bashir, A., Sholla, S.: Cloud of things: architecture, research challenges, security threats, mechanisms and open challenges. *Jordan. J. Comput. Inf. Technol.* **06**(04), 415–433 (2020)
38. Babaghayou, A., Labraoui, N., Ari, A.A.A., Ferrag, M.A., Maglaras, L.: The impact of the adversary’s eavesdropping stations on the location privacy level in internet of vehicles. In: 2020 5th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), 2020, pp. 1–6 (2020)
39. <map>. <http://www.cplusplus.com/reference/map>. Accessed 01 Dec 2021
40. Du, J., Diouris, J.-F., Wang, Y.: A RSSI-based parameter tracking strategy for constrained position localization. *EURASIP J. Adv. Signal Process.* **2017**(1), 77 (2017)
41. Sommer, C., German, R., Dressler, F.: Bidirectionally coupled network and road traffic simulation for improved IVC analysis. *IEEE Trans. Mobile Comput.* **10**(1), 3–15 (2011)
42. Emara, K.: Poster: PREXT: privacy extension for veins VANET simulator. In: IEEE Vehicular Networking Conference (VNC). 2016, pp. 1–2. IEEE (2016)