VANET privacy by "Defending and Attacking"

Andreas Tomandl, Hannes Federrath
University of Hamburg

Florian Scheuer
University of Regensburg

***Abstract*—A major concern regarding Vehicular Ad Hoc Networks (VANETs) is the protection of the participants' privacy. Through the frequent transmission of beacons containing pseudonyms and telematic data like speed, acceleration and location of the vehicles, attackers are able to track VANET users. To address this problem, several privacy concepts have been proposed in the past to protect the participants. These concepts often work with a single centralized provider, require radio silence or are restricted to defense only. This can lead to weak protection or to major restrictions of VANET functionality. In this paper we propose the concept of "Defending and Attacking" to overcome these issues.**

I. Introduction

Vehicular Ad Hoc Networks (VANETs) enable vehicles to communicate by using wireless ad hoc networks and exchange traffic information to significantly improve road safety. As described in [1] the data sent can be classified into warnings, emergency messages, value-added services and beacons. While warnings are multi-hop messages sent out to inform other vehicles about current traffic situations like traffic jams or crashes, emergency messages are used by authorities (e. g. police, firefighters) to stop VANET users or clear the way to, e. g., a scene of an accident. With value-added services like internet on the road or location based services the comfort for the user can be increased. The beacons contain an ID and active telematic data like the position or the speed of the vehicle and are used by advanced driver assistance systems (ADAS) to increase the users safety on the road.

In this paper we will attend the tracking problem caused by sending a vehicle's current location constantly. Depending on the VANET setting, an attacker just needs a wifi receiver to monitor streets and track users. Standard solutions against tracking, such as the usage and change of pseudonyms, will not work because of the short intervals of beacons (e. g. 100 to 300 ms). The attacker is still able to link the different pseudonyms [2], [3]. Therefore privacy concepts that combine pseudonym change with radio silence (called mix-zones and/or silent-periods) have been proposed [5], [6], [12].

This paper is structured as follows. In Sect. II the related work, the existing solutions and their limitations are discussed. Sect. III explains the attacker model used in our paper and Sect. IV discusses our privacy concept, structured in four subsections including the general setting, the multi provider key exchange, the intrusion detection system and possible system limitations. Finally we conclude the results in Sect. V and summarize our contributions.

II. Related Work – Existing solutions and limitations

In this section, a variety of location-based, time-based and user-centric privacy concepts will be discussed and open issues identified. For a more detailed discussion the dissertation of Florian Scheuer [4] can be consulted.

In **location-based mix zones** [2], [5], [6] a specific location, called mix zone, with high traffic is chosen. Within this zone, the vehicles keep radio silence and change their pseudonyms. Because of the spacial gap between the last beacon sent with the old pseudonym and the first beacon sent after the mix-zone with a new pseudonym, the two datasets – depending on the mix-zone parameters – cannot be linked [7]. While this concept can produce feasible results in protecting the users privacy a major problem is the radio silence, because driver assistance systems (ADAS) will not work properly due to missing beacons.

Based on location privacy, various concepts, such as CMIX [8], density-zone [9], social spot [10] and the PMZ system [11] have been proposed. In *CMIX* [8] the participants start to encrypt their beacons with symmetric cryptography in a specific zone and change their pseudonyms before leaving. The concept seems to provide the same privacy protection as a mix zone, but does not use radio silence. However, a closer look at privacy protection through encryption exposes an issue: While VANET outsiders cannot monitor the encrypted zone, an insider is still able to eavesdrop on the communication. First, the attacker can manipulate a Road Side Unit (RSU) dispensing the symmetric keys, and second, he can place an own "attacker RSU" (ARSU) next to genuine RSUs and act as a normal VANET vehicle which causes the RSU to provide it with the zone's key. For this attack, the attacker needs a valid VANET identity (see next section). In the *density zone* [9] concept, VANET users measure the amount of vehicles next to them. Above a threshold value, the vehicles change their pseudonyms. Even though this concept ensures a defined vehicle density before changing the pseudonyms, there are still major issues. First, every vehicle is used for calculating the threshold value, even vehicles driving into the opposite direction. Second, there is no radio silence or encrypted communication mentioned in the paper. Therefore, the attacker can link the last pseudonym directly with the new pseudonym by using beacon data (e. g. direction, acceleration and speed). *Social spots* [10] consist of small social spots (like a group waiting in front of a traffic light) and/or large social spots (like parking places in which vehicles change their pseudonym). Due to the fact that the authors do not use encryption or radio silence, the vehicles should be linked quite easily. In *PMZ* [11] vehicles register with a RSU before entering a specific mixing area. Within this area, asymmetric cryptography is used to send beacons to the RSU. RSUs forward the beacons to other participants which

are located close to the sender. Outsiders cannot intercept the communication inside the PMZ and insiders need to drive very close in order to receive the beacons. Although this concept is an improvement, the dependency on one RSU is a problem. Moreover, the vulnerability to sybil attacks, i. e., faking a vehicle by sending beacons containing false location information (as described in Sect. III) is still an issue.

In the second major concept – **time-based silent-periods** [12] – vehicles keep radio silence for a specific duration at a particular time and, similar to mix zones, change their pseudonyms before continuing communication. Examples for concepts based on silent-periods are "silent cascade" [13] and CARAVAN/AMOEBA [14], [15]. The problem of lost VANET functionality while keeping radio silence, as described for mix-zones, is also an issue for silent-periods. *Silent cascades* [13] provide an extension to the silent-periods and analyze the trade off between the protection of privacy and the loss of VANET functionality. *CARAVAN/AMOEBA* [14], [15] addresses the problem of radio silence and the resulting limitation in the VANET functionality, too. In their threat model, they define that the attacker cannot listen to all radio signals in an area, but has ARSUs with a specific distance between them. If the vehicles change their pseudonyms between the reception of two ARSUs the attacker could have problems to link vehicles. Although these papers show interesting results, their threat model (Sect.III), in contrast to the one used in this paper, is weaker because a global attacker listening to the whole area is not considered.

The third major type includes **user-centric approaches** such as swing & swap [16], slow [17] and REP [18]. In *swing & swap* [16] users decide whether they want to change their pseudonyms depending on a time threshold and an appropriate situation with a lot of participants in the swing-phase. After sending an update message, other vehicles can decide if they want to join the radio silence period and also change their pseudonyms. As a second option, the vehicles can swap their pseudonyms to maximize the privacy provided by the concept. In the *slow model* [17] vehicles enter radio silence after driving below a specific speed limit (e. g., 30 $\frac{km}{h}$) and change their pseudonym before leaving it. This could happen at an intersection or in an area with low speed limit. The idea behind *slow* is that fewer and less harmful accidents will happen if vehicles drive slower and therefore, radio silence and missing ADASs are acceptable. In *REP* [18] vehicles trigger a random encryption period (REP) in which the vehicles use a symmetric key to encrypt their communication. As CMIX, this can protect against outsiders. Insiders are still able to track because an attacker just needs a vehicle to get the key and listen to the communication.

As shown above, there are still unsolved privacy issues in VANETs.

1) The use of radio silence leads to loss of VANET functionality. If the driver assistance stops working every few minutes a mayor benefit of VANETs is lost.
2) The use of RSUs with only one service provider leads to a single point of failure (regarding privacy). Advanced privacy concepts make use of distributed trust.
3) The concepts are not able to avoid future attacks. An effective instrument to prevent an adversary from attacking is to expose him, revoke his VANET identity and therefore, make an attack "expensive" for him.

TABLE I. ISSUES IN PRIVACY CONCEPTS

	Radio silence	One provider	Defense only
Mix-zone	Yes	No	Yes
Cmix	No	Yes	Yes
Density-Zone	No	Yes	Yes
Social spot	No	No	Yes
PMZ	No	Yes	Yes
Silent-Period	Yes	No	Yes
CARAVAN/AMOEBA	Yes	No	Yes
Swing & Swap	Yes	No	Yes
Slow	Yes	No	Yes
REP	No	No	Yes

Tab. I shows the introduced privacy concepts and the evaluation on the discussed issues.

III. THREAT MODEL

In our model, the main goal of an adversary is to track the location of different VANET users throughout a specific area. The attacker cannot break encryption but is able to observe all messages.

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. However, armed with a set of identities and ARSUs the attacker can participate as a VANET insider and also simulate vehicles by using sybil-nodes [19].

Furthermore, infrastructure providers could be compromised and support the attacker. This is especially dangerous for privacy concepts using RSUs. The possible challenges can be summarized as follows:

1) Observation of the area by the GPA,
2) participation in the VANET with infrastructure of the attacker,
3) simulation of vehicles (sybil attack) and
4) collaboration with RSUs.

IV. THE D&A ZONE

In this section, our new privacy concept, called Defense&Attack zone (D&A zone), will be presented. The structure of the encrypted zone will be explained in Sect. IV-A,

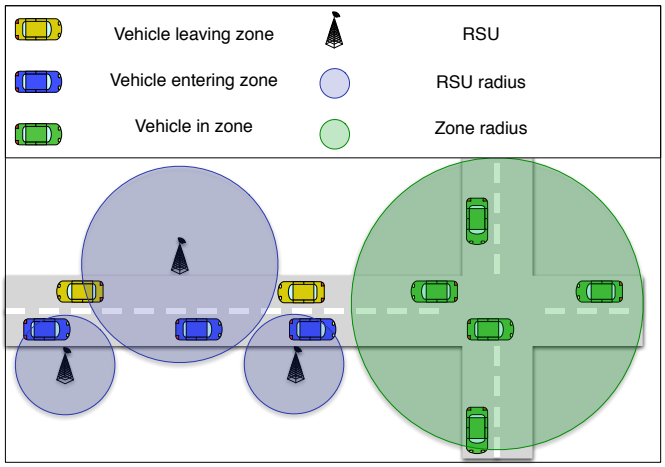

Fig. 1. D&A-zone in general

followed by a description of the key exchange in Sect. IV-B and the used intrusion detection system in Sect. IV-C. In Sect. IV-D possible system limitations will be discussed.

A. General setting

Our privacy scheme consists of a specific area where all communication is encrypted (see Fig. 1) to avoid the linking of two pseudonyms. Like CMIX [8] inside the D&A-zone, the beacons are encrypted with a symmetric key (K):

$$E_K(\text{position, speed, acceleration, direction, pseudonym})$$

Before leaving the area, all vehicles change their pseudonyms and start sending without encryption. This zone achieves the same privacy level as a standard mix zone [7] for outside attackers, because the attacker is not able to break encryption. In contrast, inside adversaries can participate in the VANET and therefore legally obtain the key. This problem will be addressed in Sect. IV-C.

B. Multi provider key exchange

This section addresses the issue of the dependency on one RSU operator. Concepts like CMIX or PMZ use just one provider and therefore are dependent on the RSU not being compromised. Our concept makes use of (at least) three RSUs with different providers at the entrance point of a zone. Each RSU will send one third of the symmetric key to the VANET users and will sign the messages to prevent an attacker from injecting fake key parts into the system. A RSU working together with the attacker will still only have one third of the key. RSUs communicate with each other for IDS (Sect. IV-C) and time synchronisation purposes. At first, the possibility to calculate the symmetric key K as XOR of three key parts will be discussed.

If one provider is having technical difficulties or is denying his service, the other two seem to be sufficient to dispense the keys, i. e., K is calculated from two parts. A closer look shows that an attacker, having compromised one RSU, could use this fact to his advantage. If he wants to monitor the D&A zone for a specific time, he can stop one RSU from sending the data. The other two RSUs will send their two keys and, therefore, the key, now only being created of two shares, changes. For a short period of time two different keys are used in the encrypted zone and the vehicles cannot communicate. Depending on the used protocol the users would either accept the loss of communication or switch to non encrypted beacons. In the second case, the attacker could monitor the area. Because of the other RSUs not being able to distinguish if the one RSU has real technical issues or is being compromised, the attacker can run this attack once a while without being reported by the other RSUs.

To avoid this attack a threshold secret sharing scheme can be used. While the technique above would be a (t, t) scheme, because all the t shares are needed to create the key, there are also (t, n) schemes, with t being the number of participants and n being the number of shares needed to create the key. Shamir's secret sharing [20], which is based on polynomial interpolation can be used to share the key. This method can be configured in the way that only two of the three shares dispensed to the RSUs will be required to generate K. If one RSU experiences a malfunction, all services can be delivered without interruption. A third party is needed to generate and dispense the keys to the provider. While this is a single point to attack, it will be more difficult to attack this third party as it is to attack RSUs placed on a street.

For the symmetric cryptography any encryption system such as AES/256 can be used. The key will change periodically, e. g. every 3 to 15 minutes. If a vehicle enters the zone and less then 5 minutes are left, it will get two keys, the current and the next K. To keep an adversary from establishing a fleet of attacker vehicles driving to each zone in a specific timetable, random periods of time can be scheduled. Thus, the attacker not knowing at which time the key is changed, needs to have a vehicle near the zone every 3 minutes (with 3 minutes being the shortest time interval) to make sure that his keys are up to date. Consequently the adversary needs as much vehicles as zones, which leads to high personnel and vehicle costs.

The key exchange can be done by a simple request/response/acknowledge protocol, using asymmetric encryption, as shown in Tab. II [8]. Like CMIX, each VANET user v_i and RSU needs a public and a private key signed by a certificate authority (CA). In the request phase, a user sends a message with a *REQUEST* command, a timestamp T_s, his certificate $Cert_i$ and signs the message ($Sign_i$). The RSU responds with a timestamp, the symmetric key SK, signs the data with its key, encrypts the data with the users public key K_i and adds its certificate $Cert_{RSU}$. After decrypting the message the user answers with an acknowledgement Ack, a timestamp, signs the message and adds his certificate. Instead of sending the whole key with one RSU, like the CMIX system, in our concept, we use three RSUs next to each other. Furthermore, the RSUs will choose the transmission power on such a low level that it is barely reaching the vehicles. Therefore, ARSUs used by the attacker have to be near by. Besides the gain of having three carriers, this setting helps defending the users privacy against adversaries. While a normal VANET user passes all the RSUs on his way to the zone, the attacker uses fixed infrastructure. The GPA can be excluded from the key exchange because of the missing ability to actively communicate with the RSUs. This is the

TABLE II. KEY ESTABLISHMENT (CMIX) [8]

Sender	Receiver	Message
v_i	RSU	$\textit{Request}, T_s, Sign_i(\textit{Request}, T_s), Cert_i$
RSU	v_i	$E_{k_i}(v_i, SK, T_s, Sign_{RSU}(v_i, SK, T_s)), Cert_{RSU}$
v_i	RSU	$Ack, T_s, Sign_i(Ack, T_s), Cert_i$

major difference between normal users and the attacker.

The attacker has three options to get the symmetric key. First, he could send a vehicle to get the key, but of course if he has a vehicle near the tracked car he could also follow it manually (see Sect. III). As a second attack, he could use three ARSUs with the same pseudonym next to the three RSUs. The same pseudonym is important because the RSUs could exchange hashed pseudonyms of the vehicles already passed and a vehicle not passing the first, but passing the second RSU could be noticed. A third attack would be the sybil node attack. In this attack, the adversary is sending beacons with wrong location information and simulating a real car. For the last two attacks, an IDS as described in the following section can be used.

C. Intrusion detection system

1) IDS proposal: The idea behind the use of an IDS is to detect whether a message has originated from a vehicle or from an ARSU. With the placement of three RSUs, we exploit the fact that a vehicle is moving and a ARSU is standing still. Of course an attacker could still fake the location of his beacons and thereby simulate a vehicle. This is often done in sybil attacks [19] in Mobil Ad Hoc Networks (MANETs), VANETs or large-scale peer-to-peer systems. Especially in reputation- or trust-based-systems, an adversary can use sybil attacks to increase his reputation or trust level. Another possible sybil attack would be the reinforcement of the attackers fake message by sybil nodes or the disruption of routing protocols. In this field, a lot of research has been done [21]–[25]. On the other hand, to the best of our knowledge, there has not been any attempt to include intrusion detection systems in privacy concepts, although privacy concepts are areas in which it is very important to detect (and expose) attackers.

To detect a sybil node attack, we could save pseudonyms as hashes and set a threshold value on how often a pseudonym is allowed to pass within a specific time period, because a normal user does not need to get every new key, but an attacker saving all data has to. The problem with this approach is that there can be vehicles that circle a specific area for a long time, e. g., taxi drivers. So this technique can only be used as an indicator for a sybil attack but not as a reliable technique. As a second way to discover sybil attacks, radio resource testing could be considered. This method works fine if the attacker has only one radio device and if a vehicle is faking another node. The tester is assigning a different channel to each tested vehicle and broadcasts a message. The attacker needs to listen to both channels at the same time, which is not possible with only one radio device. This detection technique does not work in our approach because the ARSU just has to fake exactly one (and only one) vehicle. Other ways would be wifi fingerprinting to detect the continuos presence of an entity or position verification with techniques like the Enhanced Observed Time Difference (E-OTD). Fingerprinting and the use of implicit identifiers can be very effective tools to identify users as shown in [26], but as long as the VANET protocols are not defined completely, an analysis and forecast on the effectiveness will be very hard. The last method mentioned here is position verification. This method has often been used to detect sybil attacks in VANETS or other areas like mobil communication for location services (Timing Advance, Uplink Time Difference of Arrival, Enhanced Observed Time Difference). While in the area of mobile phones a time-based technique is often used for wifi-devices, the signal strength can be analyzed. Two key facts in favor of signal strength are often stated in the literature. First, time of arrival can be manipulated if the location of the RSUs is known by using own infrastructure to supply delayed signals. Because of the route being chosen by the attacker he can prepare a database with vehicle positions and the corresponding time differences for his ARSUs. Second, when using challenge response to prevent the first scenario, the RSUs measure the time from sending the challenge to receiving the response. The attacker needs to send the challenge to his infrastructure before answering, which leads to a time difference depending on the placement of the infrastructure (e. g., 300m, ˜1 microsecond). Without having standardized VANET components, it is almost impossible to state if this time discrepancy is enough to expose the attacker because of possible deviations of the vehicles' message processing and therefore, the implementation of Time-Of-Arrival will be postponed. In the following part, the possibility to locate senders through their signal strength will be discussed.

TABLE III. EXAMPLE OF POSSIBLE RSSI VALUES WITH TWO WIFI DEVICES APPROACHING

m	1	2	3	4	5	6	7	8	9
RSSI(dB)	-68	-67	-65	-62	-60	-59	57	-55	-55

2) The system: In this section, three different scenarios covering the possible types of attacks are examined.

a) Scenario 1: For our first scenario, we take a look at one vehicle approaching our key exchange zone (Fig. 2). The first RSU will receive beacons and can measure the received signal strength indication (RSSI). By comparing the location information of beacons with the RSSI, the RSU can evaluate if the vehicle is really moving, because RSSI will increase (Tab. III) while the vehicle is approaching and the distance d between vehicle and RSU is decreasing. By using the Friis Attenuation Model the authors in [25] show that it is possible to discover a sybil node with only one measuring node, if nodes and attackers have a fixed signal strength. For normal vehicles this is a valid assumption because it is likely that a standard will be established before launching VANETs. The authors in [25] furthermore explain that an attacker has to send with constant and standardized signal strength because otherwise nodes outside the wifi coverage will still receive signals and can expose the attacker. While this assumption is valid for mobil nodes and attackers, we work here with fixed infrastructure. In our example, the attacker will adapt his signal strength to simulate a vehicle approaching the RSU. Therefore, he can use a similar formula (e. g., Friis Attenuation Model) like the RSU uses it to verify moving vehicles. This can be done because we only looked at one RSU in this scenario.

b) Scenario 2: As a second example in Fig. 3, the sybil node is approaching the first RSU. At a specific point it would

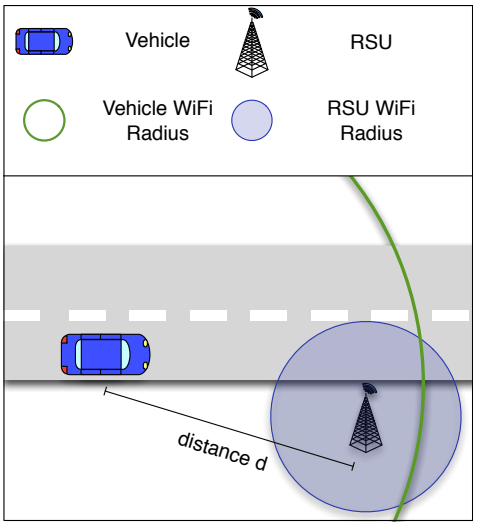

Fig. 2. Scenario 1

be the normal case that the second RSU can make contact with the vehicle. Therefore, the attacker has to increase the signal strength or use a second ARSU. Both ways will lead to major issues because the RSUs are placed so close that the signals will reach each other at a specific point in time or if one ARSU is used the RSSI will indicate an attack. In Fig. 3 the distance between the sybil vehicle to the RSUs and the ARSU to the RSUs is different and therefore $\frac{d(v,RSU1)}{d(v,RSU2)} \neq \frac{d(ARSU,RSU1)}{d(ARSU,RSU2)}$ with $d(v, RSU1)$ being the distance between vehicle v and $RSU1$ can be calculated. Of course, depending on the ARSU placement, the ratio will be correct for some cases, but there are two important facts to keep in mind. First, it is hard to place the ARSU on the street and a placement next to the street will lead to small deviations in the ratio. Second, the sybil node should be moving and therefore pass the RSUs. No single ARSU can simulate this different ratios. Because an adversary only needs two out of the three shares to generate the key, the second RSU has to wait until enough RSSI values for vehicle positioning are collected, before it sends its share. We can conclude that it is not important to measure the exact distance between vehicle, ARSU and RSUs, however the ratio should be correct. The ratio between signal strength and distance can be calculated as described in [27]. If a RSU receives a signal from a vehicle v the signal strength R (RSSI) can be calculated like

$$R_{RSU1} = \frac{P_v \cdot K}{d(v, RSU1)^\alpha} \tag{1}$$

with P_v being the transmission power, $d(v, RSU1)$ representing the Euclidean distance, K being constant and α as a distance-power gradient. Factor α depends on the used hardware and the environment. With hardware being standardized for VANET vehicles and the environment being permanent, it should be quite easy to determine α. Furthermore, environmental influence should be minimal because of the RSU's height. If another RSU receives the signal, we can calculate the ratio:

$$\frac{R_{RSU1}}{R_{RSU2}} = \frac{\frac{P_v \cdot K}{d(v,RSU1)^\alpha}}{\frac{P_v \cdot K}{d(v,RSU2)^\alpha}} = \left(\frac{d(v, RSU2)}{d(v, RSU1)}\right)^\alpha \tag{2}$$

With the distance between the sybil vehicle and the RSUs being established, the expected ratio of the RSSI values can be determined and sybil vehicle attacks eventually identified.

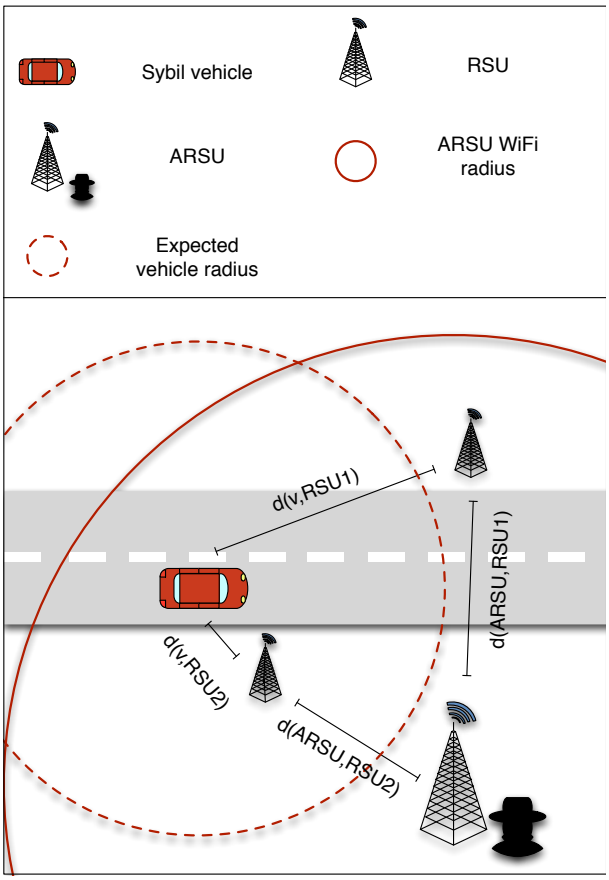

Fig. 3. Scenario 2

c) Scenario 3: To fool the system with two or three RSUs, the adversary has to adapt his strategy as shown in Fig. 4. Instead of using isotropic radio antennas, which diversify in each direction, the attacker can use directional antennas and supply each RSU with a specific signal. Because of the other two RSUs not receiving this signal they will not notice that the vehicle is fake. Each RSU will receive the correct signal strength. This can be done with any number of RSUs and with any infrastructure no solution seems to be possible because the attacker can prepare for the RSUs. When taking a look at the privacy zone setup, we could consider a traffic intersection with a lot of traffic which ensures that it is hard to link new and old pseudonyms of vehicles. On the one hand, we can conclude that there will be other vehicles near the sybil node and, on the other hand, an adversary is limited to a small amount of sybil nodes, because of the attackers limited ability to fake identities and free space on the street. To help the RSUs identifying sybil nodes, all vehicles have to send lists of their neighbors and received signal strength as shown in Tab. IV. While RSUs could be fooled by using directional antennas, it is unlikely that the majority of the moving vehicles can be fooled, too. In Fig. 4, all vehicles should receive a signal from the sybil vehicle and by doing so, the attacker needs to use normal antennas which again will be noticed by the RSUs. If the majority of the vehicles did not receive any data from a vehicle in reach, the RSUs can conclude that they are under a

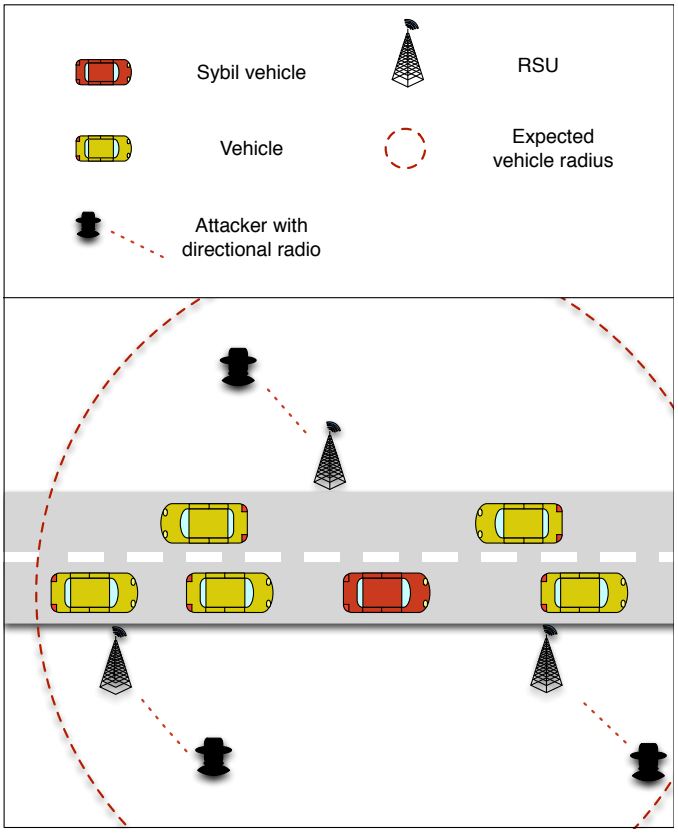

Fig. 4. Scenario 3

TABLE IV. EXAMPLE DATA OF A VEHICLE SENT TO A RSU

timestamp	pseudonym	RSSI
1347544528	8c090f8ee01c666a	-27
1347544539	97eaae377a7a0d8f	-51
1347544541	387c8592ae9181a8	-50
...	...	...

sybil attack and getting their signal from directional antennas.

As a result of identifying a sybil attack, the RSUs will report the vehicle, which will lead to blacklisting or revoking the VANET-identity. Of course, the attacker is still able to use another identity but as discussed in Sect. III, acquiring a new identity is quite expensive.

D. Possible system limitations

Even though our privacy concept solves some open problems of other concepts, there are still issues left. As mentioned in Sect. III, single attacker vehicles can follow a car through the D&A zone, because they also get the symmetric key. Of course, this is not really an issue, because the attacker can visually follow a single car anyway. The only advantage is that the vehicle could send the key to an ARSU and monitor the whole area. Of course, in this case the attacker needs as many vehicles as D&A zones are existing.

In contrast, many vehicles collaborating and exchanging key information via an "attack platform" could be a major issue. However, with the key changing every 3 to 15 minutes (see Sect. IV-B) lots of users have to join the "attack platform", and a normal user will hopefully not be interested in joining such a network. A more practical attack would be to pay users for joining. Depending on the size of such a network, it is a valid assumption that it gets noticed by the authorities and the transfer of keys to an attacker and payment to collaborators (normal users) could be punished. In summary, it is unlikely that an adversary would be able to build a community big enough to make this a serious threat.

V. CONCLUSION

In this paper we introduced a new privacy concept called D&A-zone. We discussed related work and identified three mayor issues with existing privacy concepts. A lot of concepts use radio silence to keep the adversary from linking pseudonyms. While this works well from the privacy point of view, it also reduces VANET functionality. Another issue is that concepts that work with RSUs only use one provider and therefore are dependent on the provider not being corrupted by the attacker nor being the attacker itself. A last mayor issue is that the privacy concepts only defend against the adversary but do not deal economic damage to the attacker (e. g. report the used identity).

To fix these issues, we introduced our new privacy concept. It uses three different service providers and therefore can bear one provider being corrupted. Furthermore, encryption instead of radio silence is used, which maintains all VANET functionalities, and at the same time makes it hard for the attacker to link pseudonyms. The last and most important component of our concept is the IDS which protects VANET users from attackers and simultaneously causes economic damage to the adversary by blacklisting and revoking identities. It protects against attackers having multiple ARSUs equipped with isotropic or directional antennas and stolen VANET identities.

As future work, further analysis of the used IDS based on simulations and real wifi data traffic is planned. Furthermore, the possibility of transferring our IDS to different concepts (e. g. PMZ) and other VANET areas will be examined.

REFERENCES

[1] K. Plößl and H. Federrath, "A privacy aware and efficient security infrastructure for vehicular ad hoc networks," in *Security in Information Systems: Proceedings of the 5th International Workshop on Security in Information Systems – WOSIS 2007*, 2007.

[2] F. Scheuer, K. Plößl, and H. Federrath, "Preventing profile generation in vehicular networks," in *WIMOB '08: Proceedings of the 2008 IEEE International Conference on Wireless & Mobile Computing, Networking & Communication*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 520–525.

[3] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in vanets," in *Proceedings of the Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2007)*, Juli 2007.

[4] F. Scheuer, "Schutz der privatsphäre in ad-hoc-fahrzeugnetzen," Ph.D. dissertation, Universität Hamburg, Von-Melle-Park 3, 20146 Hamburg, 2012. [Online]. Available: http://ediss.sub.uni-hamburg.de/volltexte/2013/6016

[5] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, 2003.

[6] ——, "Mix zones: User privacy in location-aware services," in *2nd IEEE Conference on Pervasive Computing and Communications Workshops (PerCom 2004 Workshops), 14-17 March 2004, Orlando, FL, USA*. IEEE Computer Society, 2004, pp. 127–131.

[7] A. Tomandl, F. Scheuer, and H. Federrath, in *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'2012)*, 2012.

[8] 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)*, Vancouver, 2007.

[9] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, "Wireless location privacy protection in vehicular ad-hoc networks," *Mobile Networks and Applications*, vol. 15, no. 1, pp. 160–171, February 2010.

[10] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Anonymity Analysis on Social Spot Based Pseudonym Changing for Location Privacy in VANETs," in *Proceedings of IEEE International Conference on Communications, ICC 2011*. Kyoto, Japan: IEEE, Juni 2011, pp. 1–5.

[11] F. Scheuer, K.-P. Fuchs, and H. Federrath, "A Safety-Preserving Mix Zone for VANETs," in *Proceedings of Trust, Privacy and Security in Digital Business - 8th International Conference, TrustBus 2011, Toulouse, France*, ser. Lecture Notes in Computer Science, S. Furnell, C. Lambrinoudakis, and G. Pernul, Eds. Springer Berlin / Heidelberg, 2011, vol. 6863, pp. 37–48.

[12] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Proceedings of the 2005 IEEE Wireless Communications and Networking Conference (WCNC)*, New Orleans, LA, USA, March 2005, pp. 1187–1192.

[13] L. Huang, H. Yamane, K. Matsuura, and K. Sezaki, "Silent cascade: Enhancing location privacy without communication qos degradation," in *Security in Pervasive Computing, Third International Conference, SPC 2006, York, UK, April 18-21, 2006, Proceedings*, ser. Lecture Notes in Computer Science, J. A. Clark, R. F. Paige, F. Polack, and P. J. Brooke, Eds., vol. 3934. Springer, 2006, pp. 165–180.

[14] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," in *Embedded Security in Cars (ESCAR)*, 2005.

[15] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "Amoeba: Robust location privacy scheme for vanet," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1569–1589, 2007.

[16] 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*, A. Juels and M. Winslett, Eds. ACM, 2006, pp. 19–28.

[17] L. Buttyán, 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.

[18] 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, Februar 2010.

[19] J. R. Douceur, "The sybil attack," in *Peer-to-Peer Systems*. Springer Berlin / Heidelberg, 2002.

[20] A. Shamir, "How to share a secret," *Commun. ACM*, 1979.

[21] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, ser. VANET '04, 2004, pp. 29–37.

[22] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in vanets," in *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, 2006.

[23] G. Guette and B. Ducourthial, "On the sybil attack detection in vanet," *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, 2007.

[24] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against sybil attack in vehicular ad hoc network based on roadside unit support," in *Proceeding MILCOM'09 Proceedings of the 28th IEEE conference on Military communications*, 2009.

[25] M. S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil nodes detection based on received signal strength variations within vanet," *International Journal of Network Security*, vol. 9, no. 1, pp. 22–33, 2009.

[26] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall, "802.11 user fingerprinting," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, ser. MobiCom '07. New York, NY, USA: ACM, 2007, pp. 99–110.

[27] M. Demirbas and Y. Song, "An rssi-based scheme for sybil attack detection in wireless sensor networks," in *Proceeding WOWMOM '06 Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, 2006.