Simulation-based evaluation of techniques for privacy protection in VANETs

Andreas Tomandl
University of Regensburg

Florian Scheuer
University of Regensburg

Hannes Federrath
University of Hamburg

***Abstract*—In vehicular ad hoc networks (VANETs) tracking of participants is an issue that is examined by many research groups. These groups came up with several different concepts of counter measures against tracking attacks. All of these presented techniques seem to offer a pretty good protection. We pick out two very promising concepts – the Mix Zones and the Silent Periods – to examine them in a simulation environment to actually identify their strengths and weaknesses. Our simulation results show rather high success rates for attackers with relatively unsophisticated attack heuristics. Furthermore we confirm the correlation between several influencing factors and the success rates of attacks and study the connection to the common metrics k-anonymity and entropy.**

I. Introduction and related work

Vehicular ad hoc networks (VANETs) have the potential to dramatically increase the safety on the road network by interconnecting vehicles via wifi and therefore empower them to share information about the current traffic situation. This may include telematic data like position, speed and direction of vehicles (so-called *beacons*), warnings about dangerous situations (e. g. crashes, traffic jams, aquaplaning, ...) or messages from emergency vehicles. In addition, value-added services may be used for increased convenience. Plößl presented an overview over different message types in VANETS in [1].

However, the frequent sending of beacons containing telematic data (one every *200 ms*) may enable attackers to track vehicles along their trips and therefore threaten their privacy (see [2], [3] for details). The concept of this attack is based on the fact that transmitting the exact position at frequent intervals leaves very little uncertainty of the movement and so tracking is very easy. Even a pseudonym change will not distract attackers since linking of beacons works based on the telematic data and not on matching identifiers.

Lots of different techniques for a secure pseudonym change and distracting attackers have been proposed, for instance *Mix Zones* [2], [4], [5], [7] and their variations like the *CMIX Zone* [6], *Density Zones* [8] or *Social Spots* [9], coordinated location-independent radio silences like the concepts of the *Random Silent Periods* [10] or *Silent Cascades* [11], or other concepts like *Swing & Swap* [12], *SLOW* [13] and *Random Encryption Periods* [14].

All of the concepts promise an effective solution to securely changing pseudonyms and the respective authors prove this by analytical reflection or empiric data provided by simulations. However, hardly any of these considerations are comparable.

This gap should be filled by our studies. We used the VANET Simulator[1] that has been in development since 2008 to evaluate two concepts that promise a high level of privacy protection – variants of the *Mix Zone* and of the *Silent Period*.

After a more detailed description of the privacy threats in VANETs in section II we shortly outline the main features of the simulator in section III. In section IV, the main part of our work, we describe the performed attacks, the calculations of the examined metrics and the variation of the simulation parameters. The results of our simulations are outlined in section V before we conclude this paper in section VI.

II. Privacy threats and analyzed countermeasures

Vehicles in VANETs regularly broadcast messages (referred to as *beacons*) to others containing telematic data like e. g. their position, speed and acceleration and usually some kind of identifier. This identifier might be a public key-related certificate or some other kind of pseudonym to ensure prosecution of misbehaving nodes. So these messages may be linked by trivially matching their contained identifiers and therefore tracking is very easy. To prevent observers from tracing vehicles during their complete journeys, the used pseudonym must be changed regularly.

However, a simple change of the pseudonym is not sufficient since an attacker might be able to link two beacons of the same sender simply by the contained telematic data. Due to the frequent transmission of beacons (about five per second), the expected position of a vehicle when sending the next beacon based on the data of its predecessor may deviate only by a fraction of a meter (independent of the speed): even if a vehicle initiates a strong breaking application immediately after sending a beacon, its distance to its expected position differs by approx. 0.1 to 0.2 meters (cf. [2]). This is – taken the size of a vehicle into account – an exact match. So it is necessary to provide an environment where an unobservable pseudonym change is possible.

The first concept to provide such an environment we examined is the Mix Zone of which many variations are published. We wanted to achieve maximum privacy therefore absolutely no communication (encrypted or unencrypted) is allowed inside the zone. The Mix Zone is of round shape with a certain radius and the position and spatial dimension

[1] http://www-sec.uni-regensburg.de/vanet/

of the zone is known to all vehicles. Any vehicle entering the Mix Zone immediately ceases any communication and changes its pseudonym. Right after leaving the Mix Zone a vehicle resumes sending beacons with the new pseudonym. In the case of a Mix Zone an attack is considered successful if the attacker correctly links two pseudonyms – one before and one after the zone.

The concept of the Silent Periods (like the Random Silent Period or Silent Cascades) was adapted to a Coordinated Silent Period by us to further increase privacy protection even though the (real-world) coordination overhead rises dramatically. That is a period of time in which every single vehicle – wherever it is – completely ceases any communication and changes its pseudonym. Since all vehicles in our simulation possess exactly synchronized clocks, no random part of the silent period is required as described by Huang et al. in [10]. After the Coordinated Silent Period (further simply referred to as Silent Period) ends, each vehicle returns to sending beacons with its new pseudonym. Similar to the Mix Zone scenario, an attack is considered successful if the attacker correcty links the two pseudonyms of the same vehicle.

III. VANET Simulator

For our studies we use the VANET Simulator that provides a simulation environment for traffic simulation on realistic street networks and the simulation of inter-vehicle communication and supports privacy preserving techniques like Mix Zones and Silent Periods. Each vehicle is simulated individually to provide realistic behavior by the use of microscopic traffic simulation (our model is based on the works of Krauss [15] and Treiber et al. [16]) and we use road networks from the OpenStreetMap Project[2]. In principle, each vehicle has a certain radio range but for our analysis all broadcasted messages are written to a log file to create the view of a global passive adversary and analyzed in a succeeding step which is the simulation of the attacks. Additional information is stored about the real identities of the user of a certain pseudonym to provide a correct solution to measure the success of an attack. Of course this data is not available for the implemented adversary.

IV. Simulation

A. Attacker Model

We designed two different attackers (*simple* and *advanced*) for both the Mix Zones and Silent Periods to analyze the effectiveness of the provided privacy protection. All of these attackers are of the type of a global passive adversary (GPA) that receives every single message that is sent (*global*) and does not actively participate in the communication (*passive*).

1) Simple attack on Mix Zones: The goal of an attacker on vehicles crossing a Mix Zone is to correctly link incoming and outgoing vehicles by determining the correct exit point and the right exit time of an entering vehicle. The main difference of a Mix Zone compared to Silent Periods is its fixed location. On the one hand, locations with rather good conditions for mixing vehicles may be chosen, but on the other hand, an attacker might analyze the traffic flow and use this knowledge to improve his attacks.

The attacker can act on the assumption that the vehicle has to travel a distance that equals approximately twice the radius r of the Mix Zone. As an average speed the attacker uses the speed limit v_s of the current street. Consequently, the time the vehicle spends in the zone is estimated by $t = \frac{2r}{v_s}$. The attacker observes the exits of the Mix Zone and picks the vehicle that leaves the zone closest to the expected point in time.

To increase the accuracy of his estimation the attacker may include a factor called *readjustExpectedTime* f_t to take into account that the rather optimistic estimation for the time needed to cross the Mix Zone might be too short since traffic lights or other vehicles' right of way might interfere and slow vehicles down. This modification is highly dependent on the location of the Mix Zone and has to be determined by empiric analysis. Therefore the estimation of the time to cross the zone is calculated with equation 1.

$$t = \frac{2r}{v_s} f_t \tag{1}$$

When comparing the exiting vehicles to deduce the correct one, further information may be used to render the estimation more precisely. Observations show that vehicles tend to go on bigger streets (i. e. streets with higher speed limit). So the probability that a vehicle changes from a bigger to a smaller one is lower than the other way round and therefore vehicles leaving the Mix Zone on a smaller street than the observed vehicle entered obtain a penalty in further calculations which is represented by the *streetSizeWeight* w_s.

Another observation indicates that vehicles tend to pass intersections straight ahead instead of taking a turn. We introduced another modifier, the *streetTurnWeight* w_t, to take this behaviour into account. Depending on the location of the Mix Zone this modifier will be low if a vehicle turns and high if it crosses the intersection straight ahead.

Taking these modifiers into account, a score for each possible vehicle will be calculated as displayed in equation 2.

$$score = (1 - w_t)\,(1 - w_s)\,|t_{out} - t_{in} - t| \tag{2}$$

The vehicle with the lowest calculated score is assumed to be the seeked one. All used information is either common knowledge (like the size and position of the Mix Zone) or transmitted in beacons (like speed and position of the vehicles).

2) Advanced attack on Mix Zones: An attacker might gather empiric data on the traffic flow of a Mix Zone (and the underlying intersection) to predict the movement of a certain vehicle more precisely and carry out a more sophisticated attack. Once again a vehicle entering the Mix Zone at entrance i is compared to each vehicle leaving the zone at exit j. An attacker knows the average travel time t_{ij} from entrance i to exit j and the probability p_{ij} that a vehicle travels this route. The score for this attack is calculated with equation 3.

[2]http://openstreetmap.org

$$score = \left(1 - \frac{p_{ij}}{2}\right) |t_{out} - t_{in} - t_{ij}| \quad (3)$$

As previously at the simple attack, the actual time between an entry event at i and a possible exit event at j is compared to the estimated time t_{ij}. The impact of the probability of the combination of entry and exit is lowered by dividing it by 2. Our studies showed that otherwise too many false negatives would occure. The vehicle with the lowest calculated score will be selected by the attacker.

This advanced attack requires knowledge about the traffic flow and is therefore more expensive.

3) Simple attack on Silent Periods: Silent Periods take place at a fixed point in time and the position of vehicles is not taken into consideration. As a consequence, an attacker cannot focus on a defined location where he might analyze the average traffic flow but many vehicles will enter a Silent Period at locations like straight streets where they do not have the option to change directions.

The approach of the simple attack is to estimate the distance an attacked vehicle might travel during the Silent Period. The expected distance d is calculated as the product of the Silent Period's duration t_{sp} and the street's speed limit v_s as $d = t_{sp}v_s$. As before, a modifier called *readjustExpectedDistance* f_d is used to take into account that vehicles might advance slower than expected due to dense traffic. The travelled distance of a vehicle is therefore calculated by equation 4.

$$d = t_{sp}v_s f_d \quad (4)$$

Again, a score for each possible vehicle is calculated by comparing the expected distance d to the actual travelled distance Δx assuming the current examined vehicle would be the seeked one (cf. equation 5).

$$score = |d - \Delta x| \quad (5)$$

For all vehicles the score is determined and the vehicle with the smallest score will be chosen. The information used in this attack is contained in the transmitted beacons.

4) Advanced attack on Silent Periods: Vehicles do not change their direction very often and the probability for doing so during a Silent Period is even lower. To exploit this insight the advanced attack was designed to estimate an exact position x of a vehicle after the Silent Period by using a vector with the travelling direction of the vehicle and its expected distance during the period as magnitude. The score for this attack is calculated as the distance Δx of the estimated position x and the actual position l of the examined vehicle as shown in equation 6.

$$score = |\Delta x| = |x - l| \quad (6)$$

To exclude vehicles that are near the expected point, but drive in the wrong direction, a maximal deviation of the direction vector of the vehicles can be set in the form of an angle.

B. Metrics

To quantify our examinations, we decided to use two popular metrics of this field (cf. [17] for an overview), the k-anonymity [18] and the entropy [19]. Furthermore, we want to have a look at the metrics themselves and to what extent they actually describe our findings.

1) K-anonymity: The k-anonymity is based on the number of similar entities that are indistinguishable for an observer in a certain resultion. Gruteser and Grunwald describe in [20] the attributes of an anonymity set (and therefore of each of its elements) as a tuple $[x_1, x_2], [y_1, y_2], [t_1, t_2]$ that outlines a rectangular region where the elements are located at a time interval. As a result the extension of the anonymity set varies with the size of the observed region and the observed time.

We calculate the k-anonymity of a Mix Zone for a certain vehicle with the time between the entry t_{in} and the exit t_{out} of the zone and, instead of a rectangular shape, the round area that is covered by the zone with the center of the circle $[x_1, x_2]$ and the radius r.

The k-anonymity of a Silent Period is a little more complex. Theoretically the whole simulation map would be the area for the anonymity set, however, this would presume infinite speed for the vehicles. Since we limit the maximum speed to $250\frac{km}{h}$, the covered region is again of round shape with the center as the position of the vehicle when entering the Silent Period and a radius of the maximum distance d_{max} a vehicle can travel during the period with a duration of t_{sp}.

We define the k-anonymity of a concept for privacy preservation as the average of the k-anonymity values of all vehicles that participate in a radio silence.

2) Entropy: A problem using k-anonymity is that all vehicles have the same probability to be the seeked one, but an attacker could use additional information to assign different probabilities [21], [22]. This drawback is addressed by the entropy that is calculated by $H(X) = \sum_{i=1}^{N} p_i log_2(p_i)$. N represents the amount of analyzed objects, whereas p_i represents the probability that a certain object (vehicle) i is the seeked one.

An interesting way to calculate the entropy in Mix Zones is proposed by Beresford and Stajano [4], [5]. In this concept the zone is monitored for a specific time and all vehicles following the different connections $[i, j]$ with entrance i and exit j are counted. Then the probabilities can be determined by $p_{i,j} = \frac{N}{\sum_{i,j} N_{ij}}$.

To determine the probabilities for the silent-periods the maximal driving distance d_{max} is reused as previously described . With Δx_i, as the distance between the silent-period starting point of the vehicle and the currently tested vehicle, and d_i, as the expected travel distance during the Silent Period (for the time t_{sp}) with the maximum driving speed on the current street, a_i can be calculated as $a_i = (d_{max} - d_i) - |d_i - \Delta x_i|$. Finally, the probabilities can be determined as $p_i = \frac{a_i}{\sum_j^n a_j}$.

C. Simulation Parameters

For our simulations we considered several aspects of the simulation parameters to obtain meaningful results. First of all we decided to simulate only urban areas and postpone the study of rural areas. Furthermore we distinguished two types of cities, planned ones with roads forming (roughly) a grid and historically grown ones with a rather obscure street layout, and a hybrid form of both. The maps were imported from the OpenStreetMap project and therefore should match the real road networks. We selected the following areas:

- Manhattan, New York City, NY, USA (planned city, *546.62 km* of streets simulated)
- Berlin, Germany (historically grown city, *853.91 km* of streets simulated)
- Puebla, Mexico (hybrid, *496.38 km* of streets simulated)

The total length of the streets of Berlin are a little higher than the other cities' because there are so many densly packed small streets and many of them are one-way streets, so we need a larger map to obtain a comparable traffic density.

The dimensions *traffic density*, *traffic flow* and *size of Mix Zones* or *duration of Silent Periods* should have a high impact on the effectiveness on the concepts for secure pseudonym changes. Whereas the *traffic flow* is established by the selected map, the other dimensions were varied in the simulations as following:

- Number of vehicles (*1250*, *2500*, *5000*, *10000*, *20000*)
- Mix Zone radius (*25 m*, *50 m*, *100 m*, *200 m*, *400 m*)
- Silent Period duration (*1250 ms*, *2500 ms*, *5000 ms*, *10000 ms*, *20000 ms*)

Each combination of street network, number of vehicles and one configuration of a privacy-preserving technique has been simulated five times over 15 minutes with new randomly generated starting positions and destinations for the vehicles. The results of the 150 simulations are summarized in the following section.

V. Results

We present selected results in figures 1 and 2 and an overview in table I.

Figure 1 compares the two types of attacks and the previously described metrics, k-anonymity and entropy. In the diagrams we display the multiplicative inverse of k-anonymity, $\frac{1}{k-anonymity}$, because our ordinate represents the chance of a successful attack. For the same reason, we display $\frac{1}{2^{entropy}}$ instead of the entropy itself. By combining together the actual success rates of our attacks and the theoretically determined metrics we want to verify the validity of the latter. The closer the metrics reflect the actual success rates the better they are in respect to predict the effectiveness of techniques for a secure pseudonym change.

Figures 1a to 1d exemplarily show the comparison of the attacks and metrics in Berlin and New York City respectively. First of all, the intuitive assumptions about the influence of simulation parameters are confirmed: a denser traffic results in better privacy (represented by lower success rates of the attacker) as well as larger Mix Zones and longer Silent Periods. However, increasing the time or area where no communication takes place, the safety features of the VANET might decrease and endanger traffic participants.

Both metrics reveal a different curve progression as the success rate of the attacks. Whereas k-anonymity has a somewhat similar progression, the entropy shows an extreme deviation. Especially in the Silent Period scenarios (shown in figure 1c and 1d) the metrics show a rather constant prediction for the level of privacy that is definitely not true regarding the success rates of the attacks.

Figure 2 shows the success rates of tracking vehicles through several Mix Zones or Silent Periods respectively. In theory, when crossing multiple Mix Zones or Silent Period each providing a success rate for the attacker of p_i, the total success rate would be $p = \prod p_i$. As expected, figures 2a to 2d show a logarithmic curve progression (please note the logarithmic scale in figures 2c and 2d). Curves end abruptly when either no further tracking was successful or no vehicle actually went through that many Mix Zones or Silent Periods. Once again, the correlation between the simulation parameters like the size of the Mix Zones, the duration of the Silent Periods and the number of vehicles and the success rates of attacks correspond with the intuitive assumptions.

All the success rates are summarized in table I. Even with simulation parameters like *20000* vehicles, Mix Zone radii of *400 m* or Silent Period durations of *20000*, which should supply a very high level of privacy, the attacker could still achieve pretty good success rates between *8.51 %* and *33.77 %* carrying out the advanced attacks. Note that these high parameters settings, especially the Mix Zone radius and the Silent Period duration, are impractical because of their long radio silences. With minimal parameters settings like 1250 vehicles, Mix Zone radii of *25 m* and Silent Period durations of *1250 ms* the success rates rise to between *50.32 %* and *78.44 %*. When one parameter is varied, the other one was set to a constant value of *5000* for the number of vehicles, *100 m* for the size of the Mix Zones and *5000* for the duration of Silent Periods.

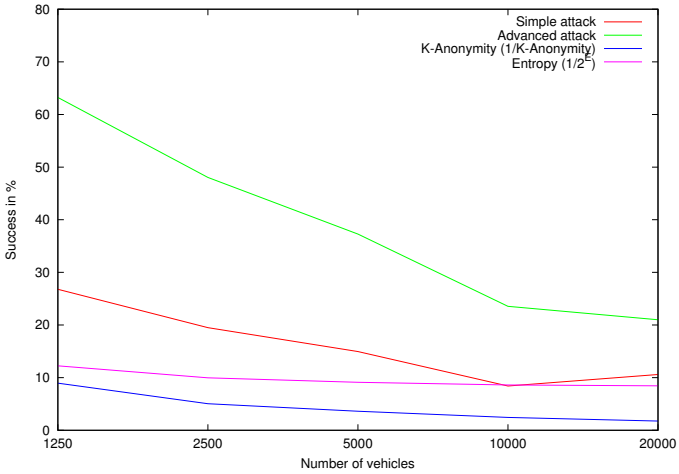
VI. Conclusion and future work

We examined the effectiveness of the Mix Zones and Silent Periods in a simulation environment. The implemented variants of these two techniques for secure pseudonym changes probably provide the best protection possible with these concepts. All simulations were carried out on realistic maps provided by the OpenStreetMap Project and with the use of microscopic traffic simulation.

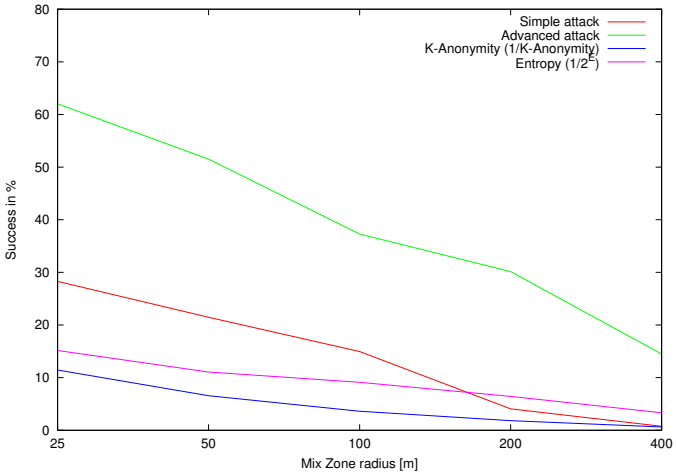
Our results confirm the assumptions that a higher number of vehicles – resulting in a more dense traffic – provides a higher level of privacy protection as well as larger Mix Zones or longer Silent Periods – both resulting in longer radio silence and therefore more unpredictability for an attacker. However, Silent Periods seem to work much better in a more regular street network like the one of New York City than in

City / length of all streets	concept	varied parameter	simple attack (success in %)		advanced attack (success in %)	
			minimum	maximum	minimum	maximum
Berlin 853.91 km	Mix Zone	vehicles (1250 - 20000)	8,41	26,79	21,03	63,24
		mix zone radius (25 - 400 m)	0,77	28,29	14,48	62,03
	Silent Period	vehicles (1250 - 20000)	23,97	57,87	33,77	75,82
		silent period duration (1250 - 20000 ms)	12,56	39,60	22,49	78,44
New York City 546.62 km	Mix Zone	vehicles (1250 - 20000)	12,08	28,58	21,60	50,40
		mix zone radius (25 - 400 m)	2,11	39,58	10,88	61,14
	Silent Period	vehicles (1250 - 20000)	5,18	32,11	8,51	50,32
		silent period duration (1250 - 20000 ms)	4,58	27,65	9,96	53,62
Puebla 496.38 km	Mix Zone	vehicles (1250 - 20000)	7,15	28,65	13,46	57,27
		mix zone radius (25 - 400 m)	1,29	37,13	8,66	58,60
	Silent Period	vehicles (1250 - 20000)	10,86	44,28	16,23	60,99
		silent period duration (1250 - 20000 ms)	8,62	25,95	18,62	62,27

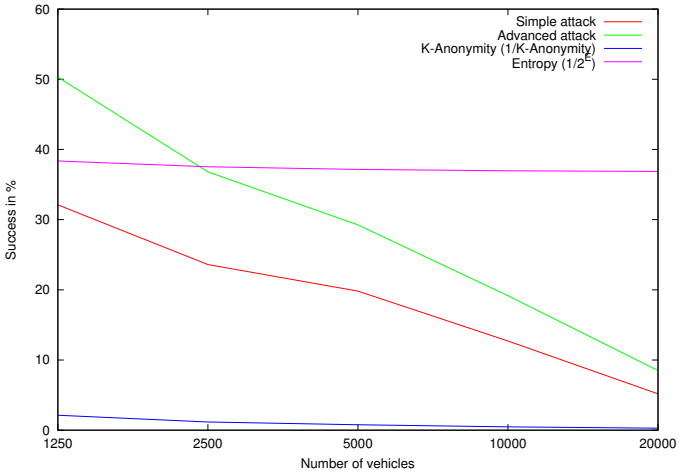
TABLE I
SIMULATION RESULTS SUMMARIZED



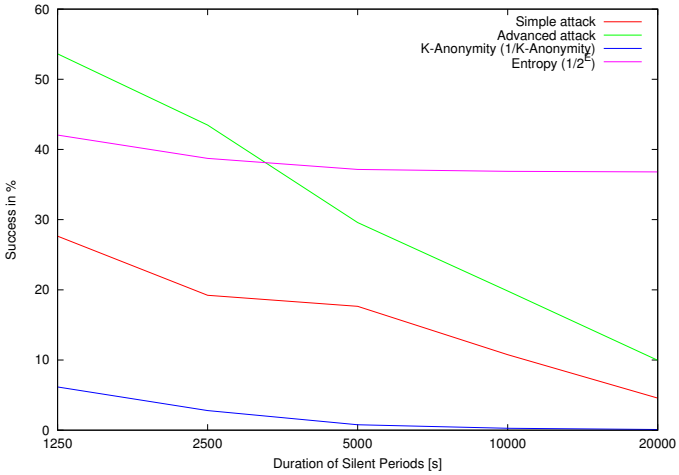
(a) Berlin – Mix Zones (1)



(b) Berlin – Mix Zones (2)



(c) New York City – Silent Periods (1)



(d) New York City – Silent Periods (2)

Fig. 1. Simulation results (1)

Berlin's. We are currently working on an explanation for this observation.

The metrics do not provide a very reliable prediction for the attacks we implemented in our simulations. Since they also tend to present an average case ignoring the situation a certain vehicle might be in, we should look for a better way to calculate them.

Regarding the alarmingly high success rates an attacker could achieve with the not very sophisticated attacks we implemented, the presented techniques for privacy protection in VANETs seem very insufficient. It is even more alerting considering the fact that the very long radio silences we carried out in several simulations are hardly possible because during these periods of time no communication is possible and this could lead to a serious threat to the safety of traffic participants who might rely on their VANET-enabled drivers assistant systems.

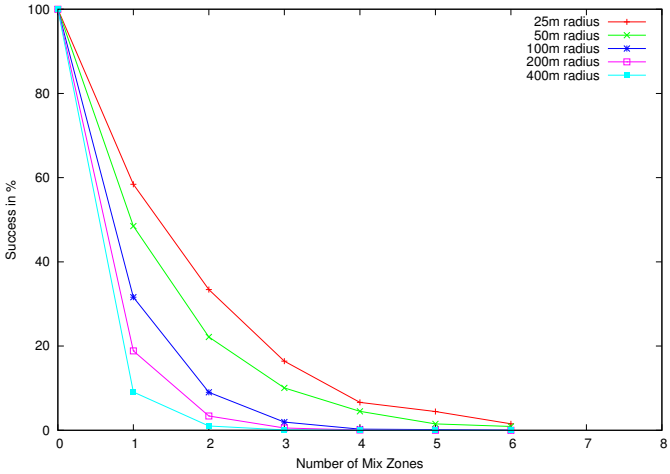
As a next step we will study the impact of the positioning of Mix Zones on their effectiveness to join the discussion about an optimal placement (cf. [7] for details). Furthermore we will take a deeper look into the effects that the parameters have on the success rates of adversaries to determine optimal setups while trying to interfere with the safety messages as little as possible. In addition, we will examine further promising techniques like the *SLOW* concept of Buttyan et al. [13] and expand our studies to rural areas and the characteristics of these road networks with high speeds and few intersections.

References

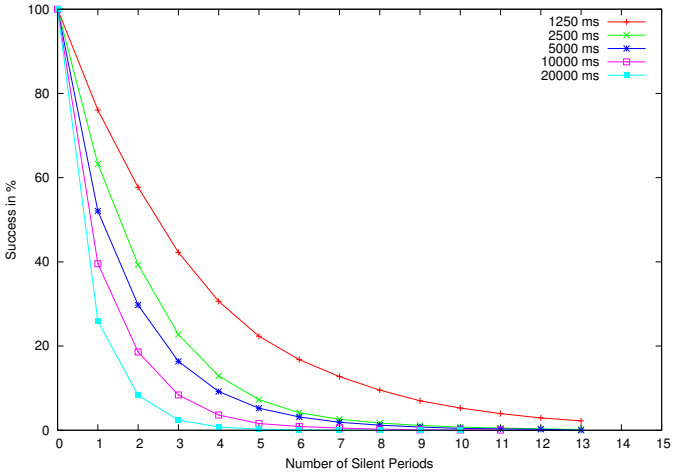
[1] K. Plößl and H. Federrath, "A privacy aware and efficient security infrastructure for vehicular ad hoc networks," in *Security in Information Systems: Proceedings of the 5th International Workshop on Security in Information Systems – WOSIS 2007*, 2007.

[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.

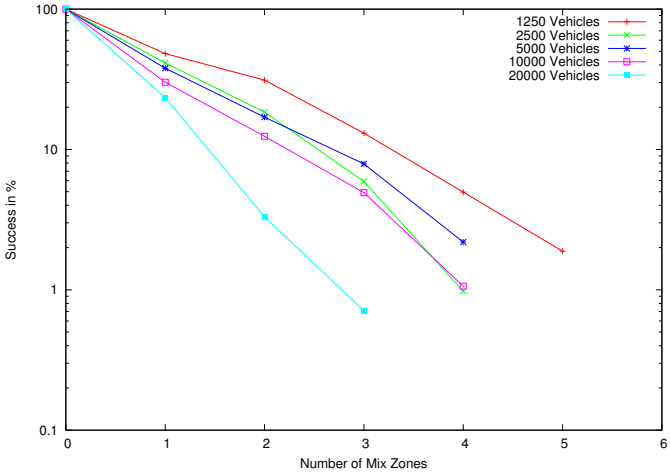
[3] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in vanets," in *Proceedings of*



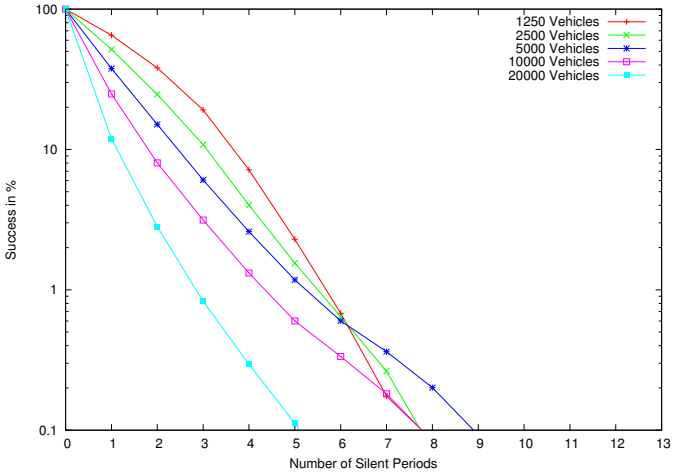
(a) Puebla – Longterm tracking (Mix Zones)



(b) Puebla – Longterm tracking (Silent Periods)



(c) New York City – Longterm vehicle tracking (Mix Zones)



(d) New York City – Longterm vehicle tracking (Silent Periods)

Fig. 2. Simulation results (2)

the Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2007), Juli 2007.

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

[5] ——, "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.

[6] 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.

[7] J. Freudiger, R. Shokri, and J.-P. Hubaux, "On the Optimal Placement of Mix Zones," in *Privacy Enhancing Technologies Symposium (PETS)*, Seattle, 2009, pp. 216–234.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] S. Krauß, "Microscopic Modeling of Traffic Flow: Investigation of Collision Free Vehicle Dynamics," Dissertation, Universität Köln, Köln, April 1998.

[16] M. Treiber, A. Hennecke, and D. Helbing, "Congested traffic states in empirical observations and microscopic simulations," *Physical Review*

E, vol. 62, pp. 1805–1824, August 2000.

[17] Z. Ma, "Location privacy in vehicular communication systems: a measurement approach," Ph.D. dissertation, University of Ulm, 2011.

[18] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[19] C. E. Shannon, "A mathematical theory of communication," *The bell system technical journal*, vol. 27, pp. 379–423, July 1948.

[20] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proceedings of the 1st international conference on Mobile systems, applications and services*, 2003.

[21] C. Diaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," in *Proceedings of the 2nd international conference on Privacy enhancing technologies, PET'02*, 2003.

[22] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Proceedings of the 2nd international conference on Privacy enhancing technologies*, 2003.