Proceedings of the
2007 IEEE Intelligent Vehicles Symposium
Istanbul, Turkey, June 13-15, 2007

Strategies for Pseudonym Changes in Vehicular Ad Hoc Networks depending on Node Mobility

Stephan Eichler

Abstract— **Security and especially privacy is an important requirement for the success of vehicular ad hoc networks (VANETs) in the future. To introduce and realize privacy a common method is to use pseudonyms to improve the unlinkability of nodes, events, and locations. Each node will own a multitude of pseudonyms and has to change them once in a while. The mobility of nodes has an important impact on the use and the change mechanism of pseudonyms in VANETs. This influence is analyzed by means of simulation and mathematical analysis. To have a simple yet solid mobility model the Manhatten Grid Mobility model was designed to model vehicle mobility. Using this model the two important parameters *node re-interaction*, how often and in what time intervals do nodes re-interact, and *node quiet-time*, how long should a node stay quiet before changing its pseudonym, are examined using simulation. In addition, an analytical method for determining the upper bound of the node quiet-time is presented. These results can mainly help to set parameters for pseudonym change protocols and estimate the impact of using these concepts in VANETs.**

Index Terms— **Vehicular ad hoc networks, mobility models, privacy, pseudonyms, security**

I. Introduction

The use of ad hoc network technology to connect vehicles will be a key technology to realize new services in the vehicles of the future. The goal of the networked vehicle is to increase the safety as well as the comfort of the passengers. Hence, besides services like collision warning, intersection assistance, and hazard warning also infotainment services and multimedia in the vehicle will play an important role. The wireless technology mainly studied in this context is the so-called Dedicated Short-Range Communication (DSRC) which is similar to the IEEE 802.11 wireless LAN. The DSRC for vehicular ad hoc networks (VANETs) is standardized as IEEE 802.11p by the IEEE 1609 working group [1].

A very crucial aspect of future VANETs and their services is security and especially privacy. The introduction of wireless technology into vehicles increases the identifiability of the vehicle itself but, depending on the implementation of the services, maybe even of the driver of the vehicle. Being able to identify vehicles fast and automatically without human interaction could be used to trace vehicles and record their trajectories. However, this strong infringement of peoples privacy is not desired and has to be prevented by means of security and privacy included in the VANET technology. The terminology concerning privacy we use in the following is based on the definitions proposed in [2].

S. Eichler (*s.eichler@tum.de*) is with the Institute of Communication Networks, Technische Universität München, D-80290 München, Germany

Privacy in the context of VANETs has been investigated in several previous publications already. A common and very feasible idea to realize privacy is the use of several identities, so-called pseudonyms. These pseudonyms can not be linked to each other, therefore, they provide a certain degree of privacy as long as they are changed once in a while. The change of a pseudonym can lead to problems, especially if an ongoing communication relies on the identity information. Hence, these type of protocols have to take a possible identity change into account. A very basic question concerning the change of a pseudonym is still unanswered: independent of any protocol used, what is a good point in time to change a pseudonym? In this paper we'll discuss this general issue of pseudonym changes in VANETs and will additionally focus on the influence of the node mobility on the pseudonym changes. We show that node mobility has an influence on privacy and pseudonym changes and will give an insight to what extend this is the case. The generated simulation results can be used to define strategies for the change of pseudonyms in VANETs.

The rest of the paper is structured as follows. In Sec. II the related work for the topic will be presented. A brief introduction to privacy and pseudonym aspects in VANETs is laying the starting point in Sec. III. A motivation for the analysis of node mobility in the context of privacy is given in Sec. III-A. In addition a new mobility model for the vehicle scenario is presented in Sec. III-B, which is used in the following simulations presented in Sec. IV and the analysis in Sec. V. The paper closes with a conclusion in Sec. VI.

II. Related work

One of the first publications concerning security and privacy issues in VANETs was published by Zarki et al. [3], presenting a secure networking infrastructure for vehicles. In the same year Duri et al. presented in [4] a framework for security in vehicle telematics. They see the success of vehicle telematics directly connected with the use of security and privacy mechanisms. In their architecture they use policies to protect the users privacy. In [5] the *mix zone* concept is introduced, which helps to provide location privacy. Further the authors introduce a method to assess user privacy using information theory. In [6] security and privacy needs for sensor networks are presented. In their discussion on privacy aspects the authors point out a very crucial aspect also true for VANETs: Due to the wireless communication the privacy breaches are aggravated. Information becomes more easily available to observers which can remain anonymous. In addition, physical presence is no longer necessary since

1-4244-1068-1/07/$25.00 ©2007 IEEE.

a small device can perform the eavesdropping task. In [7] Hubaux et al. point out the specific security and privacy challenges raised by introducing intelligent vehicles and VANETs. They point out that the electronic identifiability of vehicles creates an urgent need for security and especially privacy mechanisms to protect drivers from being tracked easily and automatically. The authors also propose the use of pseudonyms which change over time to ensure privacy. Further, they propose an entropy-based measurement for the degree of anonymity. The authors of [8] present a scheme to provide location privacy called CARAVAN. The authors discuss the general constraints posed on privacy by the very specific mobility patterns of vehicles. However, the analysis of the influence on privacy caused by the mobility of the nodes alone is yet missing. Raya et al. presented an overview on security requirements for VANETs in [9]. The authors propose the use of anonymous keys to ensure privacy in the network. These keys are only valid for a short period of time and may only be used once. Further, they present a key changing mechanism depending i.a. on the vehicles speed to ensure the anonymity. In [10] an approach to realize privacy in VANETs is proposed. The approach also uses pseudonyms in addition to a trusted-third party approach to realize anonymity. In a very recent publication the impact of pseudonym changes on geographic ad hoc routing has been examined [11]. The authors analyzed the impact of different pseudonym change intervals on the quality of the route discovery process.

Pseudonyms are used in most of the known approaches to protect privacy. Their use and influence on the scenario as well as on protocols has been looked at in many publications. However, to the best of our knowledge no strategies for the change of pseudonyms, regarding the influence of node mobility, exist so far.

III. Privacy and pseudonym changes in VANETs

The most important privacy mechanisms in VANETs are *anonymity* and *unlinkability* (refer to [2] for terminology). The use of pseudonyms is one possibility to achieve these mechanisms while sustaining other security mechanisms like authentication. The nodes have to hold several pseudonyms to be able to substitute to a previously unused pseudonym. Several parameters have to be considered when analyzing and developing mechanisms for pseudonym use in VANETs. Some examples are the number of pseudonyms, the validity period of a pseudonym, and the influence of pseudonym use on network protocols. A very crucial parameter is the change rate for pseudonyms, how often does a node have to change a pseudonym to achieve a sufficient degree of privacy. This change rate is influenced by several aspects, e.g. the communication activity or the node mobility.

The main impact of mobility concerning privacy is that nodes can interact more than once. Depending on speed, region size, and node lifetime the *node re-interaction* frequency can vary. Any re-interaction should happen preferably using a different pseudonym than before, concealing the re-interaction. However, as the number of re-interactions increases with time and the number of pseudonyms may be limited, a linkable node re-interaction becomes more likely. In case each node has an unlimited number of pseudonyms available the simplest and most effective strategy is to change pseudonyms after each encounter. But if the number of pseudonyms is limited, their use has to be optimized to achieve the highest degree of privacy possible.

Besides the mobility parameters, the rate of communication activities has to be considered for pseudonym changes. Concerning communication especially the unencrypted messages have to be taken into account, since they most likely leak context information. This is a crucial aspect, since context information helps an eavesdropper to create linkability between events, hence, aggravating the node's privacy. This observation leads to an important requirement: during any open, most likely context leaking communication cycle no pseudonym change shall occur. In fact, to increase the probability for unlinkability between pseudonyms of the same node a *quiet-time* shall be introduced. After a communication process has been finished the node waits for the *quiet-time* t_q until the next communication process is started, then using a different pseudonym. During the quiet-time the communication neighborhood changes due to the node mobility, hence, eavesdropping nodes have a lower probability of linking different pseudonyms to the same node. The maximum reasonable quiet-time is defined by the duration of a full neighborhood change. In this case non of the new nodes has the chance of linking the old and the new pseudonym of the sending node, since the old pseudonym is not know to any of the new neighboring nodes. This case has been simulated and analyzed in our work (see Sec. IV).

A. Motivation for node mobility analysis

Especially the node mobility is an important parameter for the configuration of pseudonym changes. In a mere static scenario a node has a group of N_n neighbors. Any sent message can be mapped to a specific node with the likelyhood of $\frac{1}{N_n}$. The same is true for the linkability of pseudonyms to a certain node, as long as all nodes in the neighborhood change their pseudonyms simultaneously. However, as soon as mobility has to be considered, traceability becomes much harder. In this case a newly detected pseudonym could derive from either a pseudonym change of an already known node or a new node entering the neighborhood. This simple example gives a good impression on the influence of mobility on the privacy of nodes. In the static scenario privacy comes down to simple math, which is definitely not the case for the mobile scenario. Thus, mobility will have an influence on privacy and pseudonym changes in VANETs.

B. Manhatten grid mobility model

Node mobility can have various characteristics, thus, many different mobility models exist in the research community [12], [13]. Most models have very few restrictions on the node movement, which does not correspond well to the movement of vehicles. Hence, we designed a simple road-like mobility model, which is presented in the following.

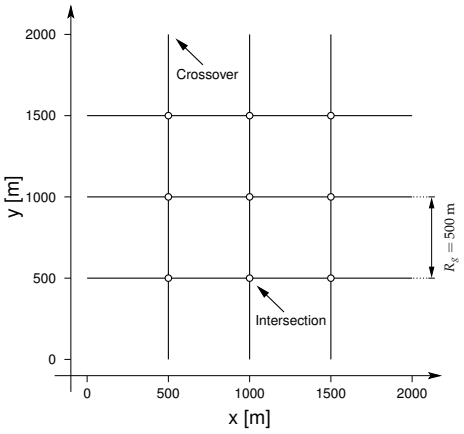

Fig. 1. The Manhatten Grid mobility model

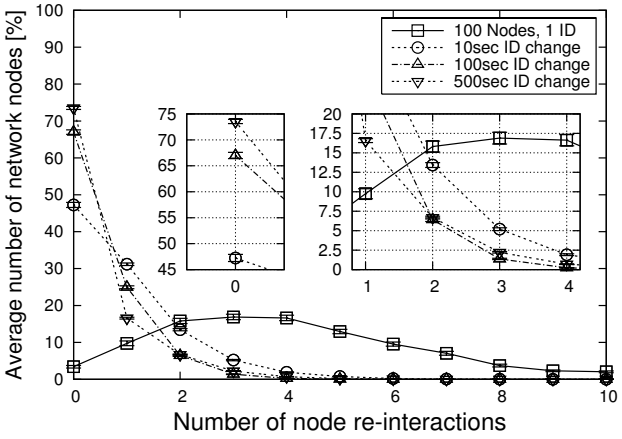

Fig. 2. Average number of nodes seen more than once (part 1)

A more specific mobility model than the mere random models, e.g. Random Waypoint, Random Direction, is the so-called Manhatten Grid Mobility model, which has been used for the simulations presented in Sec. IV. As the name suggests the mobility of the nodes is taking place on a grid, somewhat close to real road movement of vehicles in a city like New York. In Fig. 1 the road setup of the scenario is depicted.

Nodes are placed randomly on the road grid at the beginning of the simulation. The model uses three steps to place a node. First, a road segment is chosen, while all of the 24 segments have an equal probability to be picked. In the second step the node is placed on the segment. Again, all positions on the segment are equally probable. In the final step the movement direction is chosen.

During the simulation of node mobility two different events can occur which influence the movement pattern of the node. The node can reach an intersection or it can come to a crossover point. At an intersection the node position is corrected to the exact intersection coordinates. This is necessary since the movement intervals do not necessarily add up to the correct coordinates exactly. In a second step a new movement direction is chosen. All four directions are possible, hence, the node could even return to the previous segment. At a crossover the model selects one of the twelve crossover points as new entry point for the node.

The Manhatten Grid Mobility model provides a good while simple approximation of vehicle movement in large cities. Due to its low complexity compared to very realistic models using digital maps and driver models [14] it is possible to simulate large scenarios (several hundred nodes) in a very short time (up to three times faster than realtime). Hence, the model was used for our simulations.

IV. Mobility influence on node re-interaction and quiet-time

In Sec. III the terms *node re-interaction* and *quiet-time* have been introduced briefly and their relevance to the pseudonym challenge has been shown. In this section we'll present simulation results for the node re-interaction and the required quiet-time. First, the simulation settings will be presented.

A. Simulation environment and settings

To simulate the different scenarios the simulation system OMNeT++ [15] (`http://www.omnetpp.org/`, Version 3.2) in combination with the INET-Framework (Version 20060912a) has been used. The Manhatten Grid Mobility model with a grid size $R_g = 500$ m and an overall simulation size of 2000 m $\times$ 2000 m was the basis for all simulations. The position update interval of the mobility model was set to 0.1 s. Since only the potential neighbor nodes were examined, no propagation model was used, however, a radio-range R_r of 100 m has been assumed. Both the node speed (6 m/s up to 24 m/s) and the node density ($\approx$ 1 up to $\approx$ 10 neighbors) has been varied in the different simulation runs. All results in the plots show the 95% confidence intervals to document the dependability of the results.

B. Node re-interaction against pseudonym change interval

The first results of the simulations are on node re-interaction. Concerning these results one weakness of the simulative approach has to be kept in mind. In reality node movement would not be limited to a defined and very limited area. However, since we're primarily interested in the local and short term effects of mobility the influence of the fixed dimensions is acceptable. One advantage of the limited simulation area is that the results can be interpreted as a worst case scenario, therefore, in reality the number of re-interactions would be similar but most likely much smaller.

For the results on re-interaction a simulation duration of 1 h has been used. The 100 nodes had a speed of 12 m/s and where equipped with 10 pseudonyms if not stated otherwise. The simulation model checked the communication neighborhood of each node after every position update of the mobility model. Every newly detected node was logged with the respective pseudonym used at that moment. Using this logdata the number of node re-interactions has been analyzed

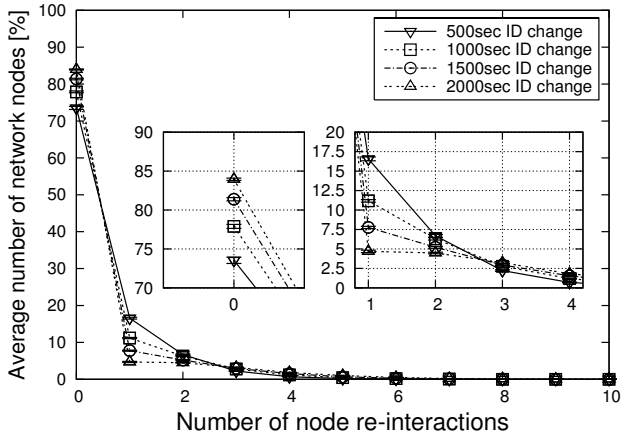

Fig. 3. Average number of nodes seen more than once (part 2)

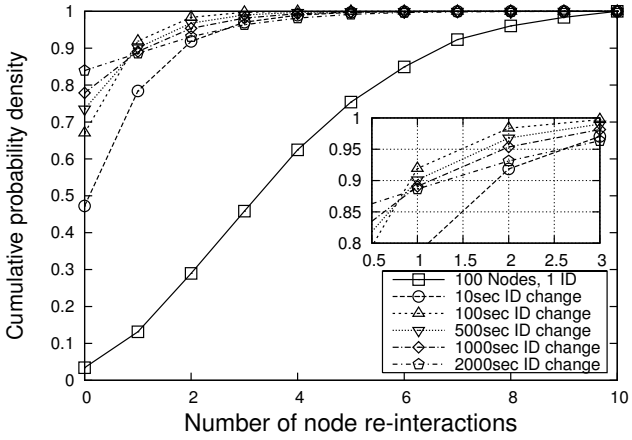

Fig. 4. Redrawing Fig. 2 and Fig. 3 using a cumulative PDF

at the end of each simulation run. The reference runs used a scenario where each node had only *one identity*, thus, no pseudonyms where used. In all the other runs 10 pseudonyms where used and randomly changed in a certain interval.

In Fig. 2 the results for the reference model as well as for the pseudonym change intervals (t_{pc}) of 10 s, 100 s, and 500 s are presented. The result for the reference scenario is the flat curve with its maximum at around three, representing the worst case for the given settings. In this scenario many node re-interactions occur, since every interaction after the first encounter can be linked due to the missing pseudonyms. The other plots (simulations using pseudonyms) have their maximum at 0, representing no or one interaction, but no re-interaction. Depending on t_{pc} the case of one-time re-encounters occurs between 15% and just above 30% of all cases. Node re-interactions of four and above have a very low percentage.

First of all these results prove, introducing pseudonyms reduces the number of detectable re-encounters quite significantly as could be expected. But which change interval t_{pc} is the best? To answer this question, several values for t_{pc} have been simulated (Fig. 2 and Fig. 3). The results show an interesting and for future implementation helpful result. Not the fast pseudonym change is the best, the 10 s change interval actually performs rather poorly. The reason for this is the *average node interaction time* (t_i). The length of t_i is depending on the mobility model and the node speed, in our setting it amounts to $t_i = 13$ s. The change interval should be bigger than t_i, hence, the 10 s can not be the best parameter value. A second scenario specific parameter which is helpful to identify the best value for t_{pc} is the average time duration elapsing between a re-interaction (t_w). For the given scenario t_w amounts on average to 583 s with a 95% confidence of 10 s. Therefore, t_{pc} should be just smaller than t_w to achieve an optimal result for the pseudonym change. Looking at the results plotted in Fig. 2 this claim seems to hold, the plot for $t_{pc} = 500$ s is decreasing faster. However, including larger values for t_{pc} into the analysis seems to counter the claim. In Fig. 3 the plots for values of t_{pc} larger than t_w are presented. They decline even faster.

But the decline of the plots is somewhat misleading. Larger values for t_{pc} definitely lead to higher probabilities for the low re-interaction values. However, they also cause a higher probability for the re-interaction values of three and above. This can not be seen in Fig. 3 since the difference is very small. Re-plotting the same results to a cumulative probability density function (PDF) results to Fig. 4, where the effect is more visible. The larger t_{pc} gets, the higher is the starting value of the plot. But the inclination of the plot decreases at the same time. In Fig. 4 can be seen that $t_{pc} = 100$ s has the biggest incline, even slightly better than $t_{pc} = 500$ s which would be closer to t_w. We assume that the selected scenario was yet too small to show the desired effect better. Even though $t_w = 583$ s, still many samples of t_w are smaller than this average, since the uncertainty of the random processes in a small scenario is rather big. That's why $t_{pc} = 100$ s leads to a slightly better performance.

C. Required node quiet-time before a pseudonym change

In the second group of simulations we looked at the quiet-time (t_q). In these simulations t_q is defined as follows: The nodes of the simulation make a snapshot of their neighborhood at a random point in time. Then the simulator measures the time t_q until *all* neighboring nodes of the snapshot have left the radio-range of the respective node.

The simulation results shown in Fig. 5 have been measured using a static node (N_s) analyzing its neighborhood. The node N_s was located at an intersection in the simulation scenario while the other nodes where moving at one of the plotted node speeds. It can be seen that depending on node speed and density the quiet-time changes. In this rather simple scenario with N_s measuring t_q, an upper bound can be calculated. Since $R_r < R_g$, the maximum length any node has to move in the range of N_s is $2R_r$. Therefore, regarding the node speed (s_n), the upper bound for t_q can be calculated: $t_{q,upper} = 2\frac{R_r}{s_n}$. In Fig. 5 the upper bound for the given scenario is presented with the round, solid points.

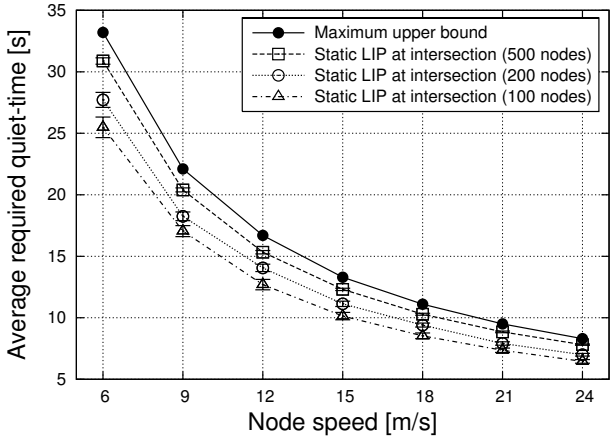

Fig. 5. Average required quiet-time t_q for a static node

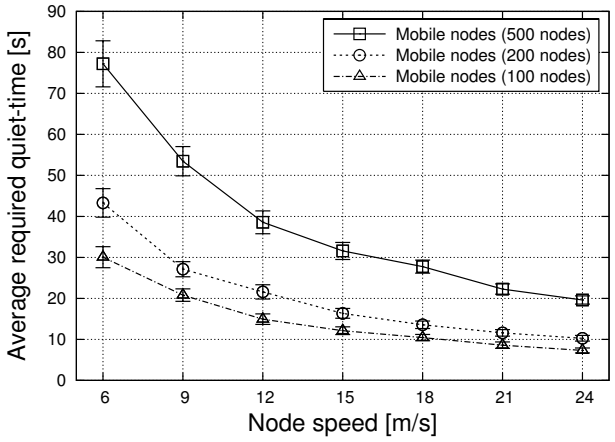

Fig. 6. Average quiet-time t_q in a mobile scenario

In Fig. 6 the results for an all mobile scenario are given. In this case no upper bound can be calculated, since two nodes could move along the same path throughout the whole simulation time. It can be seen that in an all mobile scenario t_q is much longer, especially for simulation scenarios with many nodes moving at a rather low speed. But for common vehicle speeds in urban areas t_q is much shorter than one minute and can be as low as 10 s.

Overall, the results given in Fig. 5 and Fig. 6 can be used to identify parameters for a pseudonym change algorithm used in VANETs. To increase the effects of pseudonyms, a minimum value of t_q should be set.

V. Analysis of Parameters and Characteristics

In this section we'll present a method to calculate t_q for the static node scenario analytically. First, the parameters and the setup for the analysis will be described. In the second step the equations of the analysis will be given.

The setup for the calculation is shown in Fig. 7. The calculation is mainly based on the node density, the radio-range (R_r), and the node speed (s_n). The node density

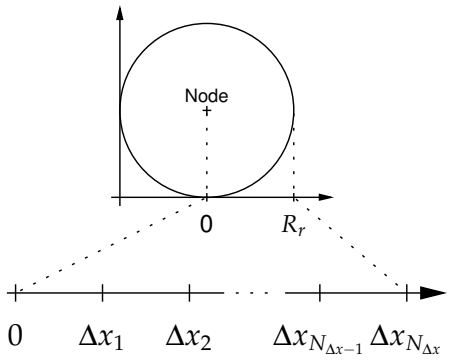

Fig. 7. Radio range and distance increments Δx_i

can be transferred to an average number of neighbors (N_n) that are within radio-range. The length of the radio-range is segmented into equally long distance increments Δx_i (see Fig. 7). The index parameter i equals the number of increments taken into account at the respective calculation step. The main principle of the calculation is the use of the binomial coefficient (Eqn. 1) and its variants.

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{(n-k)!k!} \tag{1}$$

The analytical way of determining t_q uses the statistical characteristics of the mobility model, to determine an upper bound for a given number of neighbors. Due to the symmetry of the mobility model, the intersection with four directions can be reduced to one direction only. Since the nodes are distributed equally over the simulation area all increments Δx_i have the same probability containing a node at any random point in time. The upper bound of t_q is only influenced by the node having the longest remaining distance within the radio-range. For example having only one node within radio-range being located within increment Δx_i allows for two possibilities: Either the node has to travel the i increments towards the intersection plus the distance R_r to leave the radio-range or it only has to travel the remaining distance $R_r - i \cdot \Delta x$ to the edge of the radio-range. Only the first case is relevant for the calculation, since it is setting the longer time. The number of possible combinations to place N_n nodes within the i distance increments closest to the intersection is defined by Eqn. 2. The maximum number of possible combinations including all distance increments is an important parameter to be able to determine the combination probabilities. They can be calculated using Eqn. 2 and setting $i = N_{\Delta x}$.

$$C_i\left(N_n, i\right) = \left(\begin{array}{c} N_n + i - 1 \\ N_n \end{array} \right) \tag{2}$$

The probability to have at least one node placed within the i-th distance increment and all other nodes in an increment closer to the intersection is defined by Eqn. 3. The sum of all probabilities p_i has to fulfill Eqn. 4. Finally, the upper

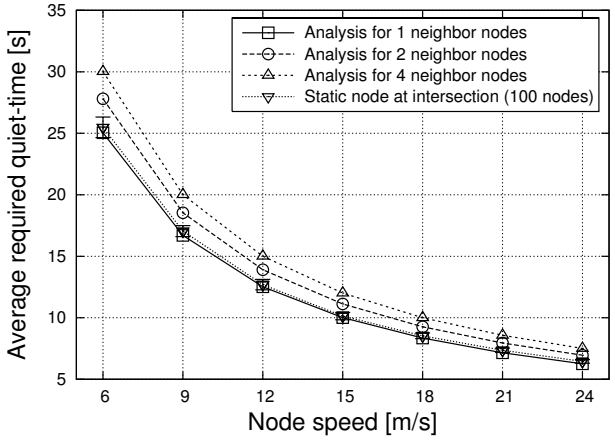

Fig. 8. Average required quiet-time $t_{q,max}$ using statistical analysis

bound of the quiet-time for a static node is given by Eqn. 5.

$$p_i = \frac{C_i - C_{i-1}}{C_{max}} \tag{3}$$

$$1 = \sum_{i=1}^{N_{\Delta x}} p_i \tag{4}$$

$$t_{q,max}\left(N_n,\, N_{\Delta x}\right) = \frac{R_r}{s_n} + \sum_{i=1}^{N_{\Delta x}} p_i \cdot \frac{i \cdot \Delta x}{s_n} \tag{5}$$

Using Eqn. 5 to calculate the upper bound of the quiet-time t_q for a given number of neighbors generates the results shown in Fig. 8. To be able to compare simulation and analysis the simulation result for the scenario with 100 nodes is plotted again. A node density of 100 nodes is just above the neighbor density of one average neighbor. Therefore, the analysis using Eqn. 5 gives a good upper bound for the quiet-time t_q.

VI. Conclusion

In a final step the simulation results shall be used to define strategies for the change of pseudonyms in VANETs. The two parameters *node re-interaction* and *quiet-time*, which are mainly influenced by the characteristics of the node mobility, have to be considered to optimize the privacy effects achieved by pseudonyms. The better the pseudonym change interval is adapted to the node re-interaction interval, defined by the mobility, the higher is the degree of unlinkability between different pseudonyms of a node. To optimize the results presented in Fig. 2 and Fig. 3 other scenarios (e.g. different size or including a driver behavior model) have to be considered. Especially a bigger difference between t_i and t_w would lead to better results proving the claim that $t_{pc} \leq t_w$. However, our results already define the limiting factors mainly influencing the value of t_{pc}.

The second important parameter, the quiet-time, can be set using the results presented in Fig. 5 and Fig. 6 or using the analytical way presented in Eqn. 5. The results could either be used to define a fixed value for t_q, resulting in a compromise for all possible scenarios. However, this would lead to a quiet-time that is not satisfying the scenario in most cases. Either the time is too short or too long. Moreover the results can be used within an algorithm used to change the pseudonyms of a node. In this case the algorithm can determine or estimate the parameters *speed* and *node density* and set t_q accordingly. This would achieve the highest level of unlinkability in any scenario.

The influence of mobility on node privacy, especially when using pseudonyms can not be neglected and has to be considered in respective algorithms. Two crucial parameters, *node re-interaction* and *quiet-time*, have been identified and quantified in the course of several simulations. Our results are a solid basis to incorporate node mobility effects in pseudonym change strategies. In a next step our findings will be included into a pseudonym management strategy to test the degree of influence in different VANET-scenarios.

References

[1] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 GHz DSRC-based vehicular safety communication," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 36–43, Oct. 2006.

[2] A. Pfitzmann and M. Hansen, *Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*, 0.28 ed., TU Dresden and ULD Kiel, May 2006. [Online]. Available: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[3] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," in *Proceedings of European Wireless, Next Generation Wireless Networks*, vol. 1, Feb. 2002, pp. 270–274.

[4] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh, and J.-M. Tang, "Framework for security and privacy in automotive telematics," in *Proceedings of the 2nd International Workshop on Mobile Commerce*. ACM Press, 2002, pp. 25–32.

[5] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55, Jan. 2003.

[6] H. Chan and A. Perrig, "Security and privacy in sensor networks," *IEEE Computer Magazine*, vol. 36, no. 10, pp. 103–105, Oct. 2003.

[7] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, vol. 4, no. 3, pp. 49–55, May 2004.

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

[9] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*. ACM Press, 2005, pp. 11–21.

[10] F. Dötzer, "Privacy issues in vehicular ad hoc networks," in *Proceedings of the Workshop on Privacy Enhancing Technologies*, May 2005.

[11] E. Schoch, F. Kargl, T. Leinmüller, S. Schlott, and P. Papadimitratos, "Impact of pseudonym changes on geographic routing in VANETs," in *Proceedings of the 3rd European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS)*, Sept. 2006.

[12] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless Communication & Mobile Computing (WCMC)*, vol. 2, no. 5, pp. 483–502, Sept. 2002.

[13] J.-Y. L. Boudec and M. Vojnovic, "Perfect simulation and stationarity of a class of mobility models," in *Proceedings of the IEEE Infocom*, Mar. 2005.

[14] S. Eichler, B. Ostermaier, C. Schroth, and T. Kosch, "Simulation of car-to-car messaging: Analyzing the impact on road traffic," in *Proceedings of the 13th Annual Meeting of the IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, Sept. 2005.

[15] A. Varga, "The OMNeT++ discrete event simulation system," in *Proceedings of the European Simulation Multiconference (ESM)*, June 2001.