Optimizing Pseudonym Updation in Vehicular Ad-Hoc Networks

Brijesh Kumar Chaurasia[1,*], Shekhar Verma[2], G. S. Tomar[3], and Ajith Abraham[4]

[1,2] Indian Institute of Information Technology-Allahabad,
Deoghat, Jhalwa, Allahabad – 211012, India
[3] Vikrant Institute of Technology and Management, Indore, India
Center of Excellence for Quantifiable Quality of Service
[4] Norwegian University of Science and Technology, Trondheim, Norway
bkchaurasia@iiita.ac.in, sverma@iiita.ac.in, gstomar@ieee.org,
ajith.abraham@ieee.org

Abstract. A vehicle can be tracked by monitoring the messages broadcast from it. The broadcast by a source contains its current identity and also allows estimation of its location by receivers. This mapping between the physical entity and the estimated location through the communication broadcast is a threat to privacy. A vehicle can preserve its anonymity by being indistinguishable in the neighborhood crowd through continual change of identity and by hiding among its neighbors. This paper addresses the challenges in providing anonymity to a moving vehicle that uses a temporary identity for transmission and continually changes this pseudonym. As a vehicle moves on a road, its neighbors change in accordance to its relative speed with neighboring vehicles. The nature and size of the neighborhood changes the effective crowd provided by the vehicles constituting this neighborhood. Since, all neighboring vehicles do not contribute to the anonymity; the degree of anonymity is reduced. The work focuses on updation of pseudonym by a vehicle in order to sustain or enhance its anonymity by decorrelating the relation between its physical location and identity. A heuristic that allows a vehicle to switch its pseudonym at a time and place where the anonymity can be enhanced is proposed. Results indicate that updating pseudonyms in accordance to the heuristic enhances the anonymity of a vehicle.

Keywords: Anonymity, vehicular networks, pseudonyms, anonymity set (key words).

1 Introduction

Transmission in the shared wireless medium reaches all the nodes in the communication range. An adversary can determine the identity and position of the source vehicle from the contents of the communication packets [1, 2]. Its position can further be confirmed by gauging the position of the vehicle from the signal strength [3]. Using

[*] Corresponding author.

M.L. Gavrilova et al. (Eds.): Trans. on Comput. Sci. IV, LNCS 5430, pp. 136–148, 2009.
© Springer-Verlag Berlin Heidelberg 2009

this information, the physical vehicle and its communication identity can be traced and related [1, 4]. Thus, location tracking through eavesdropping of source transmission and physical observation can breach the location privacy of the user. This can be used to disclose personal data of a user and would potentially dissuade a user from joining and reaping benefits from such networks [2].

To obtain and sustain anonymity, a temporal identity, pseudonym, is used for communication. Pseudonyms allow a vehicle to interact with other vehicles anonymously. Pseudonyms are ephemeral and distinct pseudonyms hide their relation from each other and to the user's identity [5]. To preserve privacy, a pseudonym system must prevent credential forgeability and disallow usage of false pseudonym by a user. Moreover, the transaction of obtaining and the process of switching pseudonyms should not reveal the identity of the user or link pseudonyms to each other. Continually changing pseudonyms conceal the real identity of a vehicle by de-linking the source of signals to its original identity [6]. But, the relation between a communicating vehicle and its estimated location can reveal the identity of a vehicle. This vehicle can, then, be physically traced and switching pseudonyms would be meaningless [7]. A vehicle can be under sustained observation and transmissions at different intervals of time with the same pseudonym can reveal the relation between physical vehicle and its current pseudonym if the vehicle is relatively isolated in a crowd. This relation can be established even when pseudonyms are updated when the time interval between transmission prior to and after the updation is short [8]. There is, moreover, one more challenge that needs to be addressed. When a vehicle under observation moves from one cluster and enters another cluster and changes its pseudonym, it can be spotted with high probability as soon as it transmits. This can happen if the number of vehicles from the previous cluster to the current cluster is small and the pseudonyms of vehicles belonging to current cluster are known a priori. The anonymity of the vehicle under observation is limited by the number of vehicles that join the current cluster from the previous cluster [9, 10].

Existing solutions address the problem of randomizing the location based relation between pseudonyms and physical identity through pseudonyms update at a specific time [11] or at pre-determined locations known as MIX-Zones [12]. Continuous transmission before and after an identity switch can be used by an adversary or observer to link pseudonyms through the message contents and signal properties. A random silent period technique [13] in which a node does not transmit for a random period during update of identifiers excludes the possibility of forging this relation. However, the location privacy provided by these solutions is limited by tracking methods that leverage the predictability of the movement of vehicles to correlate their locations before and after the switch [14]. The increase in the size of the MIX-Zone and silence time period mitigate the possibility of any relation formation [12, 15]. The formation of any such relationships based on the predictability of node movement and signal transmission can be diminished further by increasing the frequency of pseudonym switch. However, the switching time and the frequency of switching can be limited by routing [16] and other network needs [17]. To strike a balance, a vehicle should switch as soon as possible after such change is warranted by anonymity requirements. In this work, we focus on the problem of diminishing the possibility of forging a relationship between vehicle identity and its transmissions by determining the conditions that maximize anonymity during an identity switch.

The rest of the paper is organized as follows. Section 2 describes the problem along with a measure of anonymity for a moving vehicle, section 3 gives the proposed heuristic with analytical analysis of anonymity in section 4. The simulation and results are given in section 5; section 6 concludes the work.

2 Problem Formulation and Analysis

2.1 Measuring Anonymity

We assume that a vehicle is under sustained physical observation and all communication emanating from a source (with the same pseudonym) in a region can be listened to by the adversary. The adversaries can also share their observations to obtain a rough estimation of the zone of the presence of communicating vehicle. This zone Z is the anonymity zone. Then, level of anonymity of a vehicle is the inability of the adversary to pinpoint a vehicle as the source of the communication in the set of vehicles V (anonymity set) in the region estimated from the communication. This anonymity set $V \subseteq V_{total}$ with V_{total} being the total number of vehicles in Z. The cardinality of the anonymity set is the measure of the anonymity of a vehicle in the set.

If a vehicle V_i is the source of transmission, then the probability p_i that the vehicle V_i under observation is the target,

$$p_i = P_r(V_i = V), \ \forall i \in Z \text{ and } \sum p_i = 1$$

The entropy is defined as [18]

$$H(p) = -\sum_{i=1}^{V} p_i \log_2 p_i$$

The anonymity of a given vehicle is maximized when all the vehicles are equally likely to be the potential target (source of communication). Under this uniform distribution, the probability p_i that the vehicle V_i under observation is the target becomes

$$p_i = \frac{1}{V} \text{ for all the vehicles}$$

Following the definition of level of anonymity given in [19], we have,

$$A_l = 1 - 1/\,|V|$$

The population of a zone is dynamic with vehicles joining and leaving a cluster. Let there be a cluster of vehicles (set of initial vehicles $V_{initial}$) at time instant t_i. Some vehicles are communicating while others are silent. At time, $t_i + \Delta\, t$, a few other vehicles join this cluster. Some of these vehicles had been transmitting just prior to joining the cluster. Some are silent. Let the target vehicle V_i be one of the vehicles in the set of late entrants, V_{late} , in the cluster.

The level of anonymity of a target vehicle is dependent on the size of the crowd indistinguishable from the target vehicle and not the total number of vehicles in the zone Z. The vehicles that stay with the target vehicle when it joins or leaves a cluster determine the level of anonymity enjoyed by a target vehicle.

Following conditions may arise.

Condition 1: Some vehicles in the set V_{late} had communicated immediately prior to joining the cluster. Once these vehicles join the cluster (time $t \geq t_i + \Delta t$), one of the vehicles of the set V_{late} again communicates without a change in its pseudonym. In this case, the anonymity set $V_{c(late)}$ is equal to the number of vehicles who entered cluster and had communicated just prior to entering the cluster.

$$A_l = 1 - {}^{1}\!/_{|V_{c(late)}|}, \qquad V_{c(late)} \subseteq V_{late}$$

When a vehicle moves from one cluster to another without changing its pseudonym, its anonymity set is the number of vehicles that are common (move with the vehicle) through different clusters. For example, if some vehicles from cluster C_1 join cluster C_2 and a few vehicles from C_2 join C_3, then, the anonymity set for a target vehicle that moved from $C_1 \rightarrow C_2 \rightarrow C_3 \rightarrow \cdots \rightarrow C_n$ would be $C_1 \cap C_2 \cap C_3 \cap \ldots \cap C_n$ and $A_l = 1 - {}^{1}\!/_{|C_1 \cap C_2 \cap C_3 \cap \ldots \cap C_n|}$. Thus, the anonymity set may be very small even though a large number of vehicles are present in *Z*.

Condition 2: All the vehicles in the set V_{late} are silent for a random period before joining the cluster. Communication is received from a source with a pseudonym not used before in the ongoing communication emanating from the cluster. In this case, the anonymity set is the set of all vehicles silent just prior to this communication. If the number of different communication (with different pseudonyms) emanating from the cluster at time *t* was $V_{c(silent)}$, then the anonymity level is

$$A_l = 1 - {}^{1}\!/_{|V_{c(late)} \cup V_{silent}|}, V_{c(silent)} \subseteq V_{initial}$$

If all the vehicles in the set $V_{initial}$ were communicating, then the anonymity set reduces to the vehicles that have just joined (assuming in this case that pseudonym switch is preceded by a silence period). The anonymity level is

$$A_l = 1 - {}^{1}\!/_{|V_{c(late)}|}$$

Consequently, for a target vehicle under observation by an adversary or group of adversaries, the anonymity is maximized when the cardinality of the set is more than k (known as k-anonymity) and all the vehicles in the zone of anonymity have equal probability of being the target. The anonymity level becomes $(A_l = 1 \; \forall |V| \geq k)$.

The target is hidden in a crowd of k vehicles in the zone of uncertainty around the target, this enables anonymity even when the time of communication, extended position and pseudonym of a source are known.

3 Heuristic for Pseudonym Updation

The level of anonymity is a function of the cardinality of the anonymity set. Achieving k anonymity is tantamount to increasing the number of vehicles in the intersection set close to k. The proposed heuristic aims to achieve this objective by changing its pseudonym such that the size of the anonymity set becomes sufficiently large to hide the vehicle in the crowd of its neighboring vehicles. Moreover, this change process itself should not expose the vehicle. The heuristic identifies two cases.

Case1: To maximize its anonymity, a moving vehicle V_i continually observes the number of vehicles in its vicinity Z that are communicating.

After an updation, a vehicle does not change its pseudonym for a short period (order of mill seconds) which is fixed. After this period, pseudonym is updated to enhance its effective crowd cover. If sufficient time has elapsed since V_i had from the previous to the current pseudonym or the number of vehicles in the neighborhood from the last transmission becomes less than k; updation in pseudonym is imperative. The change is effected as soon as the number of vehicles that are transmitting becomes more than the critical mass, k. Till such time, the vehicle remains silent. If the vehicle has to transact with an RSU (Road Side Unit) [1] to obtain a pseudonym, it may obtain it a priori and update its identity when the aforesaid condition is satisfied. It can be further observed that the silence period can be before or after the identity change. Hence, if the pseudonym change is immediately warranted; the change must be followed by a time lag before next transmission is done.

Case 2: The above condition of critical mass of the anonymity zone can be relaxed if vehicles are able to observe all the vehicles in their vicinity (using radar). In this case, a pseudonym switch can be performed when the total number of vehicles (silent and communicating) is at least equal to k. All the other conditions remain identical to Case 1.

In general, if the vehicle continues to transmit without change in pseudonym, the cardinality progressively becomes smaller and ultimately, the adversary would be able to map the vehicle to its pseudonym. Thus, if a vehicle is able to monitor the traffic in its neighborhood, it can update its pseudonyms to remain hidden in a crowd of effective size. However, if none of vehicles in the neighborhood are communicating, the vehicle may not be able to decide upon updation. The actual effective size cannot be gauged by the vehicle itself as it knows only of the existence of the vehicles that are communicating. When a vehicle can sense the communication and observe the vehicles in is proximity physically, then, it can measure the effective size of the neighborhood and take decision of pseudonym updation to maximize its anonymity with minimum number of updations.

4 Anonymity Analysis

4.1 System Model

VANETs (**V**ehicular **A**d-hoc **Net**works) are characterized by a highly dynamic topology with vehicles moving at high speed in restricted geographical strait jackets (highways). When vehicles move on a road, they lateral motion is very restricted and the motion is unidirectional except at the junctions. A vehicle moving on the road in a particular direction can move at different speeds and also pause. Since, the speed of a vehicle can be variable; vehicles may overtake one another without any restriction. Since the transmission range of any vehicle is more than the total width of the road, this sideways motion for vehicle overtaking etc. has no effect on communication and can therefore be neglected. At the junctions or crossroads, the vehicle has a choice of taking one of options. At any junction, new vehicles may enter and continue on the road. Thus, if we consider a single unidirectional road or highway, then vehicles may enter the road at different junction points. A junction is also an exit point where vehicles from may depart from the road or continue their onward journey on the road. In the present model, a departed vehicle does not reenter or participate. Each vehicle on the road is either continually transmitting periodically, aperiodically or is silent. The aim is to find the distribution of the vehicle population on the road when the vehicles move from one end of the highway to the other end to estimate the size of the anonymity set of a target vehicle. To determine the anonymity set, the system model of the road with vehicle mobility is taken from [20].

4.2 Road Model and Input Traffic

A road with multiple unidirectional lanes is considered. The vehicles move in a single direction with different speeds and multiplicity of the lanes allows vehicles to overtake each other without any restriction in the number of lanes. The road has *S* segments of *D* meters each. The road length is *S.D* meters. Vehicles can enter and exit at the end points of a segment and there is no waiting period or queue required to enter the road. There are two end points of the road and there is no exit point at the start of the initial segment or entry at the end of the last segment. Vehicles arrive at the beginning of a segment follow a Poisson distribution $p_y(y)$ and travel towards the end point independently of other existing vehicles on the road. The arrival rate at the $(kl)^{th}$segment at $(k)^{th}$ point is λ_k with the departure rate at the $(l)^{th}$ point being δ_l $(\lambda_k\ = 0\, for\, k = 0\, and\, \delta_k\, for\, l = S)$. Once it enters the road at an entry point, it cannot exit from the same point i.e. every vehicle must traverse at least one segment as soon as it enters the road. Hence, this system can be modeled as an $M/G/\ \infty$ queue [21]. This means that the vehicles can be seen as arriving on the road in accordance with a Poisson process. An arriving vehicle is admitted in the road and starts traversing on the road without any waiting period (on the side of the road). It is assumed that no vehicle has to wait at the side of the road to enter the road. Once on the road, a vehicle cannot exit from the same junction and must traverse at least one segment before it can depart at one of the junctions. The time which a vehicle spends on the road is assumed to be independent general random variable with a distribution function *G* [21].

The vehicles travel in one direction with variable velocity. The velocity of a vehicle is assumed to be piecewise constant i.e. a vehicle moves with a constant speed for a time period and then changes its speed [20]. The velocity of a vehicle v_i in during time periods follows a normal distribution with mean speed μ and variance σ^2: $N(\mu, \sigma^2)$. The time durations t_i form i.i.d. random variables with exponential distribution with distribution parameter ${}^{1}/_{\alpha}$. The distance covered in a time duration $t_i$is $d_i = v_i t_i$ and the total distance covered in *i* time periods is $TD_i = \sum d_i = v_i t_i$.

The vehicles transmit as they move along the road. Depending on the conditions on the road and other needs, they may transmit. In this simulation, it assumed that the vehicles transmit with Poisson distribution with mean transmission rate as ρ_i.

The uncertainty zone *Z* of a vehicle is the number of vehicles within its broadcast range. If the target vehicle can be any of the vehicles in the zone *Z*, then number of vehicles in *Z* would constitute the anonymity set. However, since a global adversary can observe vehicles during an extended period of time over a large length of the road, hence, as discussed in section 2, the actual size of the anonymity set would depend on the number of vehicles communicating before they join the zone and after they leave *Z*.

4.3 Change in Cardinality of the Anonymity Set

The effective size of anonymity set Z changes in accordance with communication emanating from different locations and location of the vehicle under observation at that instant of time. There is a group G_1 of vehicles at time instant t_i with some vehicles in the group actively transmitting. After a time duration $t_i \ +\Delta\ t$, n_1 vehicles of this group join another group G_2 with $n_2$vehicles to form a group G_{2c}. If there is a transmission from the group with a pseudonym used by a source at time instant t_i in G_1, then, the cardinality of anonymity set reduces to n_1 i.e. $|G_1 \cap G_{2c}|$ from $(n_1 + n_2)$ where the total number of vehicles and the vehicles starting from the initial segment can be obtained. The transmissions from the vehicles are ignored by assuming that all the vehicles under consideration are transmitting.

If $n_1 \geq k$, then the target vehicle may not change its pseudonym, however, if $n_1 < k$, then, it is imperative for a vehicle $V_i \in G_1 \cap G_{2c}$ to change its pseudonym to increase its anonymity set to $|G_{2c}|$ before any further signal transmission. This process continues as a vehicle moves along the road.

5 Simulation and Results

A road of S segments is considered. The vehicles arrive at the start of each segment with a Poisson rate λ and their speeds are normally distributed. The vehicles travel along the road as per the mobility model and transmit in accordance to a Poisson distribution. The simulation is run independently multiple times and various statistics like the density of vehicles at different times and distances from the respective start segment is collected.

The total length of the road is taken as 18 km with segments of 3 km each. It is assumed that six segments would sufficient to observe the change in the nature of neighborhood of a vehicle [20]. The input traffic can enter from the junctions *A,..., F* and exit from *B…G*. The vehicle mean arrival rates are taken as λ = 0.7 with departure rates as δ = 0.1. The time period for constant velocity is exponentially distributed with mean 1, 2 and 3 seconds and the velocities are normal variates with mean μ (15 and 30 ms^{-1}) and σ (2 ms^{-1}). The mean transmission rate of a vehicle is taken as $\rho_i = 0.5$ [20].

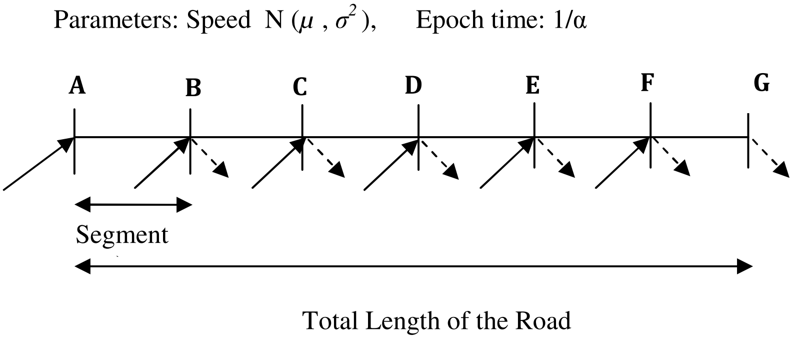


Fig. 1. Road Model

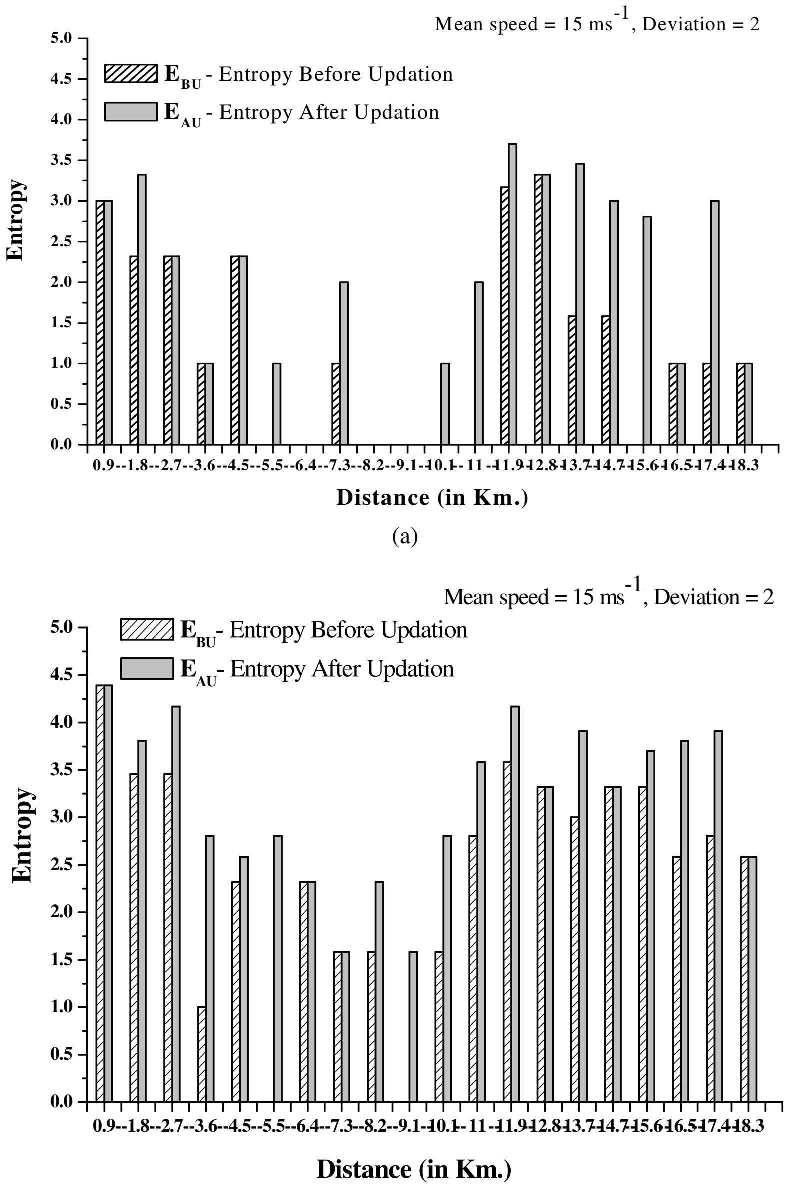
Fig.1 depicts the number of vehicles with distances. Since vehicles enter at different junctions, the number of vehicles increases with distance. The total number of vehicles at different distance becomes sparse at higher speeds (μ = 30 *ms*$^{-1}$) but interestingly, higher deviation (σ = 2 *ms*$^{-1}$) at these speeds results in more stable population of vehicles on the road. This might result in a stable cluster size but to determine whether is neighborhood itself is stable; the number of vehicles that stay with the vehicle under observation needs to be traced. To determine the number of vehicles around a vehicle of interest, a vehicle from the initial segment is considered. As this vehicle travels towards the destination, some vehicles form a part of the cluster around this vehicle. The size of the cluster and the neighborhood is a function of the transmission range and the speed of different vehicles. In the present study, we consider that the vehicles have a fixed transmission ranges of 100 and 500 *meter* radius and observe the cluster size around the vehicle for low and very high speeds (μ = 15 and 30 *ms*$^{-1}$) and variations in speed (σ =2 *ms*$^{-1}$). To study the effective size of the anonymity set or entropy, the number of vehicles in the neighborhood cluster that contribute to effective entropy is determined. The scenarios that arise are as follows.

Initially, when the vehicle of interest is silent, all the vehicles around it contribute to its entropy which is effectively infinity. When this vehicle starts transmitting, its entropy becomes finite and becomes equal to the number of vehicles in its transmission radius. The third case is arises when this vehicle is intermittently transmitting and its neighbors change due to speed variations, departure of vehicles from the road and new vehicles are come within its range of transmission. Depending on number of vehicles from the old neighborhood, their transmission pattern with or without pseudonym updation; number of fresh vehicles in the neighborhood and their transmission with or without pseudonym change; the entropy is determined. For example, in a changed neighborhood with $n_1$old neighbors and n_2 new neighbors, the vehicle of interest and its old neighbors transmit without pseudonym updation, then for the attacker, anonymity set has only n_1 vehicles reducing the effective entropy. If n_1 is small, a pseudonym updation would useful but for a large n_1 pseudonym updation would be futile and unnecessarily deplete the pseudonym pool.

The effect of speed, frequency of transmission and transmission range on entropy priori ($\mathrm{E_{BU}}$) and posterior ($\mathrm{E_{AU}}$) to pseudonym updation are depicted in Fig 2 and 3.

Fig 2a illustrates the effect of pseudonym updation on entropy that for a low speed vehicle (μ = 15 *ms*$^{-1}$) with variation (σ =2 *ms*$^{-1}$) and transmission range of 100 meters at an interval of 2 minutes. Initially, the vehicle of interest was the only transmitting vehicle and pseudonym updation did not have any effect on entropy. In the 2nd minute, however, E_{AU}became significantly larger than E_{BU}. In some portions of the road, 5th to 7th minute, the vehicle had the same set of neighbors remitting without change in pseudonym. This practically reduced the entropy to zero. In the 8th to 10th minute, the vehicle was without neighbors, hence no crowd to hide in. As the vehicle sped towards its final destination, most of vehicles departed and the entropy was low and did not change with pseudonym updation. For the same conditions, when the transmission range increased to 200 meters, the entropy increased significantly as the neighborhood increased. However, the nature of change in entropy before ($\mathrm{E_{BU}}$)and after ($\mathrm{E_{AU}}$) pseudonym updation did not vary.

As the speed of the vehicle of interest increased, the neighborhood became sparse and the effective entropy dropped (Fig. 3a and 3b). Interestingly, in most of cases,

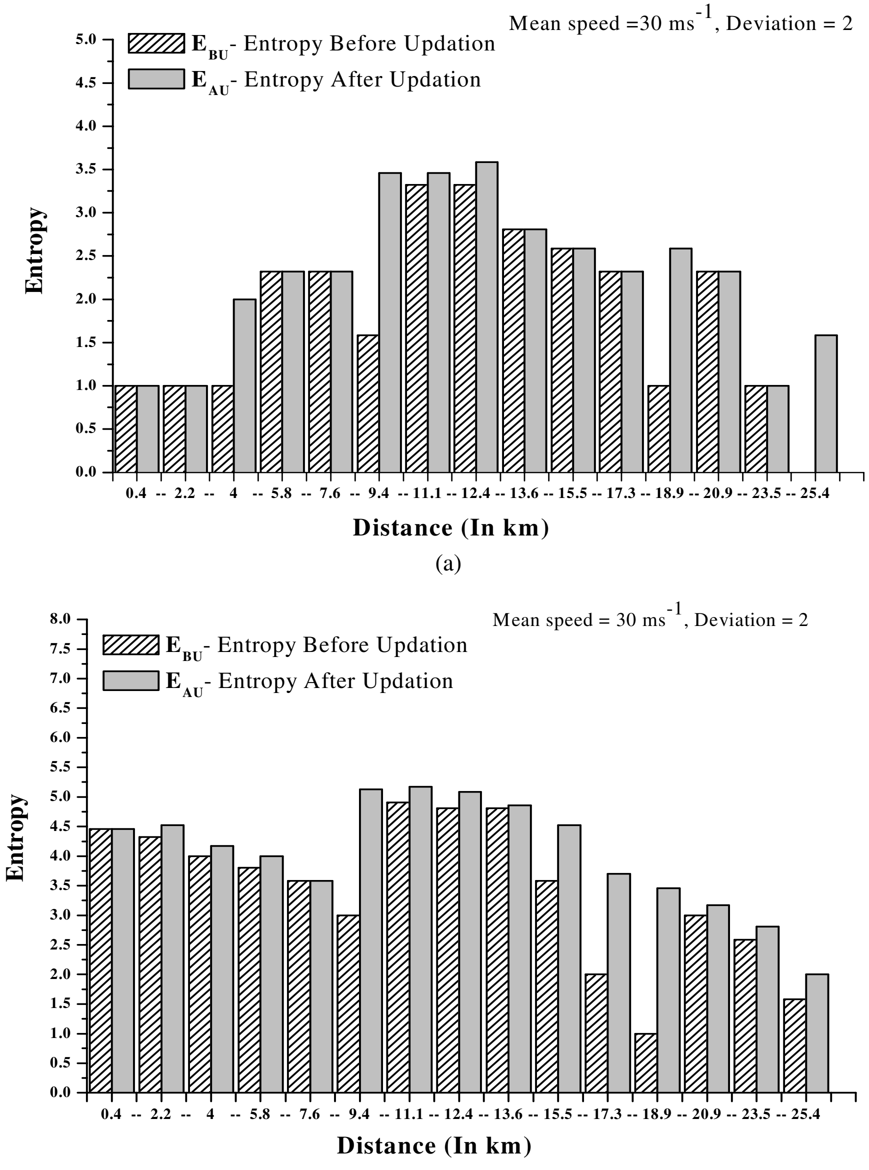


(a)

(b)

Fig. 2. (a) Entropy of the Vehicle of Interest (Transmission range =100 m). (b) Entropy of the Vehicle of Interest (Transmission range =200 m).

E_{BU} was equal to E_{AU} as the probability of transmission was not changed. It was also observed that the vehicles with similar high speeds formed a neighborhood that remained unchanged except in the initial and final phase of the vehicle's journey from initial to final segment.



(a)

(b)

Fig. 3. (a) Entropy of the Vehicle of Interest (Transmission range =100 m). (b) Entropy of the Vehicle of Interest (Transmission range =500 m).

To increase the effective entropy, the transmission range of the vehicle was increased to 500 meters. The effective entropy increased significantly. Moreover, with the increase in transmission range, the neighborhood not only increased but also became varied. Thus, updation had increased effect on entropy especially when the neighborhood became sparse. In most of such cases, (E_{AU}) became much larger than

(E_{BU}). However, in most of the cases, the entropy was large and a change in pseudonym was not warranted.

6 Conclusion

The paper dwelt on the issue of maximization of anonymity of a vehicle through enhancement of the effective crowd size around the vehicle. The transmissions of the vehicle prior to becoming a part of a zone and the other communications emanating from the zone make the probability distribution non uniform. This entails that all the vehicles present in the zone of anonymity do not contribute to the effective entropy. In accordance with the number of vehicles observed along with a vehicle and the need for transmission, a vehicle, may change its pseudonym. This updation dissociates the relation of the vehicle with its a previous neighborhood and makes its indistinguishable in the larger crowd by increasing its entropy. This confirms the efficacy of the proposed heuristics for updating the pseudonym at specified time and place when a minimum critical mass of neighbor vehicles is present for maximization of anonymity with minimum updation frequency. This would reduce the communication required for acquiring pseudonyms and the related possibility of tracking during this process of acquisition. Further, adhoc dynamic zones for pseudonym updation also reduces the possibility of tracking and the cost involved in setting up of such zones.

References

1. Raya, M., Hubaux, J.-P.: The Security of Vehicular Ad Hoc Networks. In: Proceedings of SASN 2005, pp. 11–21 (2005)
2. Raya, M., Hubaux, J.-P.: Securing vehicular ad hoc networks. Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks 15(1), 39–68 (2007)
3. Dotzer, F.: Privacy issues in vehicular ad hoc networks. In: Danezis, G., Martin, D. (eds.) PET 2005. LNCS, vol. 3856, pp. 197–209. Springer, Heidelberg (2006)
4. Papadimitratos, P., Buttyan, L., Hubaux, J.-P., Kargl, F., Kung, A., Raya, M.: Architecture for Secure and Private Vehicular Communications. In: International Conference on ITS Telecommunications (ITST 2007), Sophia Antipolis, France (2007)
5. Andreas, P., Marit, H.: Anonymity, unobservability, and pseudonymity: A proposal for terminology, Draft, v0.21, HBCC 2004 (2004)
6. Gerlach, M., Guttler, F.: Privacy in VANETs using Changing Pseudonyms - Ideal and Real. In: Proceedings of 65th Vehicular Technology Conference VTC 2007-Spring, pp. 2521–2525 (2007)
7. Kewei, S., Yong, X., Weisong, S., Loren, S., Tao, Z.: Adaptive Privacy-Preserving Authentication in Vehicular Networks. In: Proceedings of IEEE International Workshop on Vehicle Communication and Applications (2006)
8. Sampigethaya, K., Li, M., Huang, L., Poovendran, R.: AMOEBA: Robust Location Privacy Scheme for VANET. IEEE JSAC 25(8), 1569–1589 (2007)
9. Jinyuan, S., Chi, Z., Yuguang, F.: An id-based framework achieving privacy and non-repudiation in Vehicular ad hoc networks. In: Military Communications Conference, MILCOM 2007. IEEE, Los Alamitos (2007)
10. Emanuel, F., Festag, A., Baldessari, R., Aguiar, R.: Support of Anonymity in VANETs - Putting Pseudonymity into Practice. In: IEEE Wireless Communications and Networking Conference (WCNC) (2007)

11. Li, M., Sampigethaya, K., Huang, L., Poovendran, R.: Swing & swap: user-centric approaches towards maximizing location privacy. In: WPES 2006, Proceedings of the 5th ACM workshop on Privacy in electronic society, pp. 19–27 (2006)
12. Freudiger, J., Raya, M., Felegyhazi, M., Papadimitratos, P., Hubaux, J.-P.: Mix-Zones for Location Privacy in Vehicular Networks. In: ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS 2007), Vancouver (2007)
13. Bettstetter, C., Resta, G., Santi, P.: The node distribution of the random waypoint mobility model for wireless ad hoc networks. IEEE Trans. on Mobile Computing 2(3), 257–269 (2003)
14. Huang, L., Matsuura, K., Yamane, H., Sezaki, K.: Silent cascade: Enhancing location privacy without communication qoS degradation. In: Clark, J.A., Paige, R.F., Polack, F.A.C., Brooke, P.J. (eds.) SPC 2006. LNCS, vol. 3934, pp. 165–180. Springer, Heidelberg (2006)
15. Berthold, O., Federrath, H., Köpsell, S.: Web mIXes: A system for anonymous and unobservable internet access. In: Federrath, H. (ed.) Designing Privacy Enhancing Technologies. LNCS, vol. 2009, pp. 115–129. Springer, Heidelberg (2001)
16. Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Sezaki, K.: CARAVAN: Providing location privacy for VANET. WPES 2006. In: Proc. of Embedded Security in Cars (ESCAR) (2005)
17. Gruteser, M., Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking. In: Proc. of ACM MobiSys., pp. 31–42 (2003)
18. Samarati, P., Sweeney, L.: Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression, Tech. Report SRI-CSL-98-04, CS Lab, SRI International (1998)
19. Wu, X., Elisa, B.: An Analysis Study on Zone-Based Anonymous Communication in Mobile Ad Hoc Networks. IEEE Trans. On Dependable and Secure Computing 4(4), 252–264 (2007)
20. Khabazian, M., Ali, M.K.: Generalized Performance Modeling of Vehicular Ad Hoc Networks (VANETs). In: ISCC 2007, pp. 51–56 (2007)
21. Trivedi, K.S.: Probability and Statistics with Reliability, Queuing, and Computer Science Applications, 2nd edn. John Wiley & Sons, Chichester (2002)

Biographies

Brijesh Kumar Chaurasia is persuing his Ph.D. from Indian Institute of Information Technology, Allahabad, India in Privacy in Ad hoc Networks. He is received his M. Tech. degree from D.A.V.V., Indore, India. His research interest area is Security in infrastructureless Networks.

Shekhar Verma received his Ph.D. from IT, BHU, Varanasi, India in Computer Networks. He is Associate Professor at Indian Institute of Technology, Allahabad, India. His research interest area is Computer Networks, Data Aggregation in Wireless Sensor Networks, Networks Security.

Geetam Singh Tomar received his Ph. D. degree in electronics Engineering from R.G.P.V. Bhopal. He is presently Director, Vikrant Institute of Technology & Management, Indore, India. His research work is air interface for cellular and mobile ad-hoc networks, Antenna design and fabrication, sensors and sensor networks and underwater communication.

Ajith Abraham received his Ph.D. degree in Computer Science from Monash University, Australia. Currently works in Norwegian University of Science and Technology and also holds an Adjunct Professor appointment in Jinan University, China and Dalian Maritime University, China. He works in a multidisciplinary environment involving computational intelligence, network security, sensor networks, e-commerce, Web intelligence, Web services, computational grids, data mining and applied to various real world problems.