Contemporary Engineering Sciences, Vol. 8, 2015, no. 3, 109 – 114
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2015.412268

Anonymization Based Location Privacy Preservation in Vehicular Ad Hoc Networks

Y. Bevish Jinila

Department of Information Technology
Sathyabama University
Chennai – 600119, India

Abstract

The Vehicular Adhoc Networks (VANETs) are used for many safety related applications like accident avoidance, controlling traffic and emergency warning. All these applications require vehicles to broadcast their position, velocity, direction and identity during fixed intervals. It becomes necessary to preserve the location privacy of the vehicle since global attackers can collect obtain these values and misuse them. In this paper, a more robust and scalable approach for privacy preservation based on t-closeness model is proposed. By experimental analysis, it is inferred that even when the number of vehicles in a lane increases, the information gained by the observer is less in t-closeness model when compared to the previous k-anonymity model.

Keywords: K-anonymity, Privacy, Security, T- closeness, VANET

1 Introduction

Traffic safety has become an important concern for the safety of human lives. The statistics shows that the number of road accidents that occur in India has crossed 1,35,000 mark [5]. The safety measures like air bags don't provide an exact solution. This safety can be obtained if all the vehicles that travel on the road can communicate with each other and with certain fixed units on the road side which forms the Vehicular Ad hoc Network.

Each vehicle in this network holds an On Board Unit (OBU) which consists of Global Positioning System (GPS), transceiver, antenna and sensors. This enables inter vehicle communication and the communication between the vehicle

and the fixed Road Side Units (RSU's). The RSU can also communicate with the other RSU's and forms a backbone network. There is a trusted centralized entity called Certificate Authority (CA) which is responsible for the registration and renewal of the vehicles in the network.

Even though this network offers more safety and comfort to the public, there may be a situation where a malicious user may overhear the broadcast messages send between vehicles and misuse them by causing severe mishaps [12]. So security and privacy becomes a more important concern. Especially when the location of a vehicle is tracked by a malicious user, by continuous tracking he can correlate the location with the identity of the vehicle and therefore misuse even its identity. Hence location privacy becomes a more important concern [10].

Earlier works carried out on privacy preservation is based on pseudonymization, aggregation, association and cryptographic methods [9]. In this paper, anonymization approaches are considered for location privacy. Section 2 describes the related works. Section 3 describes the system model. Section 4 describes the performance evaluation. Section 5 briefs the conclusion of the work and the future direction.

2 Related Work

Generation of pseudonyms is one of the most common solutions proposed for preserving the privacy. An Electronic License Plate (ELP) [3] that has anonymous key pair is introduced, which can be changed frequently according to the driving speed and can be loaded in a tamper proof device.

Certain solutions suggested were based on cryptographic methods like group signatures and blind signatures [1]. But such methods increase overheads in RSU and also the signature size. Raya et.al. [2] has suggested a security protocol based on anonymous key pairs. Large numbers of short lived pseudonyms are installed in the vehicle and randomly one of them is selected to sign the message. When a malicious activity is detected, the CA identifies the source of the message. The limitation with this approach is that, the CA has to do an exhaustive search in its database when a malicious activity is detected.

Yipin et.al. [4] have suggested a strong privacy preservation based on pseudonyms. The limitation with this approach is maintaining a large set of pseudonyms causes high overhead on a vehicle. The authors in [6] have suggested an user centric scheme accompanied with k-anonymity technique [7] and modeled with mixed zones to preserve the privacy of the user. Though this provides traffic safety, it is susceptible to Sybil attacks. In [10] [11], various methods are proposed to detect the intruders in the network. Though these methods detect false attacks, they are susceptible to Sybil attacks.

3 System Model

A. System Architecture

Figure 1 shows the system architecture of the vehicular adhoc network. It includes the certificate authority (CA), certain Road Side Units (RSU's) and vehicles on the road.

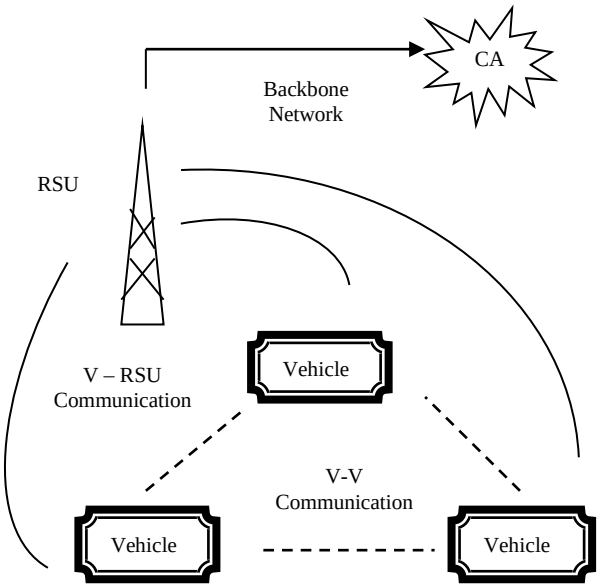

Fig 1. System Architecture of VANET

Initially, a vehicle has to register its real identity with the certificate authority which is a trusted entity responsible for the registration and renewal of the vehicles.

B. Model Used

The proposed scheme uses t-closeness model to preserve the location privacy. The EMD (Earth Mover's Distance) metric is based on the minimal amount of work which has to be done to transform one distribution to another by moving distribution mass between each other. This distance measure reflects semantic distance among values which is not available in the metrics mentioned above. T-closeness [8] can be used with any distance measure to measure the distance between the two distributions P and Q. limiting the difference between P and Q is the key to privacy.

$$\text{WORK (P, Q, F)} = \sum_{i=1}^{m} \sum_{j=1}^{m} \mathbf{d}_{ij} f_{ij} \quad (1)$$

Where, dij is the ground distance between i in P and j in Q and fij is the flow of mass to transform i in P into j in Q using the minimal amount of work.

$$\text{WORK (P, Q, F)=D(P,Q)} \quad (2)$$

Since the location attribute is categorical, hierarchical distance is used. The hierarchical distance for two values v1 and v2 is defined to be level (v1,v2) / H, where level (v1,v2) is the lowest common ancestor node of v1 and v2.

4 Performance Evaluation

Mobisim is used to generate the vehicular traffic. Freeway model is used for this vehicular traffic. Nodes are varied from 5 to 50. The NS2 simulator is used to analyze the performance in the network. Privacy can be measured based on the factor information gain. The information gain is the difference between the prior belief and the posterior belief.

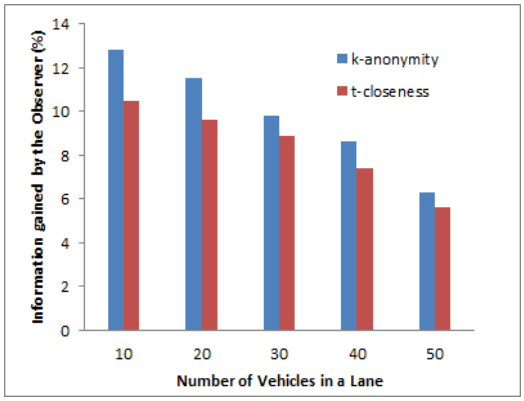

Fig 3 Information Gained by the Observer

From figure 3, it is evident that the information gained by the observer using k-anonymity approach is quiet higher when compared to the information gained by the observer when using the t-closeness model.

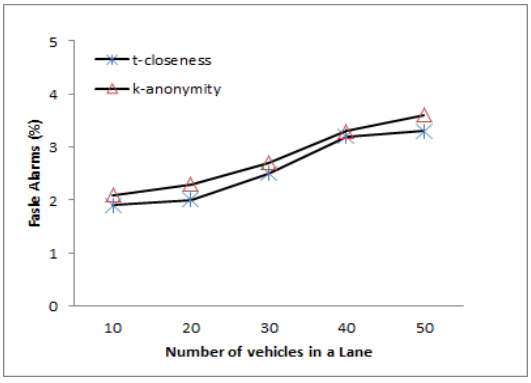

Fig 4. Percentage of false alarms

It is also more important to measure the percentage of false alarms in order to prove the effectiveness of the scheme used. It is also proved that, the number of false alarms generated while using k-anonymity approach is higher when compared

to the number of false alarms generated while using t-closeness. It is evident from the graph that even when there is an increase in the number of vehicles in a lane, the percentage of false alarms remains constant in the case of t-closeness model when compared to the k-anonymity model. Also, the percentage of false alarms is less in the case of t-closeness when compared to the k-anonymity model.

5 Conclusion

It is evident from the analysis that even when there is an increase in the number of vehicles in a lane, the information gained by the observer using t-closeness model is less when compared to the information gained by the observer using k-anonymity model. Also, t-closeness model incurs less percentage of false alarms when compared to the k-anonymity model. As a future direction, this scheme can be tested for traffic in urban areas.

References

[1] Chenxi Zhang, Pin Han, Anyi Chen, A location privacy preserving authentication scheme in vehicular networks", IEEE 2008.
http://dx.doi.org/10.1109/wcnc.2008.447

[2] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," J. Computer Security, Special Issue on Security, Ad Hoc and Sensor Networks, vol. 15, no. 1, 2007, pp. 39–68.

[3] Yipin Sun, Rongxing Lu, Jinshu," An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications", IEEE transactions on Vehiculat Technology, Vol. 59,No. 7, Sept 2010.
http://dx.doi.org/10.1109/tvt.2010.2051468

[4] Yi Ming Chen, Yue Chin Wei, "A Safe Location Privacy Scheme for Vehicular Networks", Telecommunication Systems, Springer 2010.
http://dx.doi.org/10.1007/s11235-010-9408-x

[5] Shabnam Khomejani, Ali Movaghar, "Privacy Consideration for Trustworthy Vehicular Adhoc Networks", International Conference on Electronics and Information Engineering, ICEIE 2010.
http://dx.doi.org/10.1109/iceie.2010.5559670

[6] Charu C. Aggarwal, Philip S. Yu, "Privacy Preserving data mining: Models and Algorithms".

[7] V. Ciriani, De Capitani, S. Foresti, P. Samarati, "K- anonymity", Advances in Information Security, Springer US, 2007.

http://dx.doi.org/10.1007/978-0-387-27696-0_10

[8] Ninghui Li, Tiancheng Li, Suresh, “t-closeness: Privacy beyond k-anonymity and l-diversity”.

[9] Rajalakshmi, V., GS Anandha Mala. "Anonymization by Data Relocation Using Sub-clustering for Privacy Preserving Data Mining." Indian Journal of Science and Technology 7.7 (2014): 975-980.

[10] L. Mary Gladence, T. Ravi, ” Mining the Change of Customer behavior with the aid of Similarity Computation Index (SCI) and Genetic Algorithm (GA)” in the International Review on Computers and Software(IRECOS) in November 2013 issue, Vol. 8N. 11, pp. 2552-2561.

[11] Arokia Renjit .J, Shunmuganathan .K. L, “Distributed anomaly intrusion detection system based on multi-agents”, International Journal on Information sciences and computing”, Vol.5, No.1, Jan 2011, pp. 7-12.

[12] Jatinder Singh, Rajiv, “Performance evaluation of mobile ad hoc networks using routing with selfish nodes”, International Journal on Intelligent Electronic Systems”, Vol.2, No.1, July 2008, pp. 86-91.

Received: January 10, 2015; Published: February 5, 2015