ISSN (online) : 2277-5390
ISSN (Print) : 2277-5382

A Survey on Pseudonym Management Scheme in Vehicular Ad-Hoc Networks

T. Sivakumar[1], Nidhin A.S[2]

[1]*Assistant Professor,* [2]*Research Scholar, Department of Computer Science, SNGC, Chavadi, Coimbatore-641105, Tamilnadu, India*
tsktiruppur@gmail.com[1], nidhiarackal@gmail.com[2]

Abstract

Objectives: To evaluate various pseudonym management schemes in vehicular Ad-hoc Network (VANET) for enhancing confidentiality or ambiguity.
Methods: Vehicular Ad-hoc Network (VANET) is one of the categories in mobile ad-hoc networks (MANET), which is created for the intelligent transport system (ITS).VANET is utilizes to permit vehicles in terms of self-organized network system not including the requirement of the enduring transportation. The pseudonym management is the technique amongst the road side units (RSU) and vehicles for providing the requirements of the vehicles. The major issue in VANET is anonymity which is achieved through pseudonym management technique. There are different approaches developed to support the anonymity in VANET.
Findings: This paper investigates detailed information of different approaches and finally compared their effectiveness.
Application/Improvements: The finding of this work shows that Pseudonym shuffling process based scheme is better than other techniques.

***Keywords*:** Pseudonym management system, Vehicular Ad-hoc Network (VANET), Mobile Ad-hoc Network (MANET), Anonymity.

1. Introduction

Vehicular Ad-hoc Networks (VANET) are created according to the standards of mobile ad-hoc networks (MANET) [1]. It is defined as the impetuous establishment of wireless network to exchange the information to the vehicle areas. VANETs are the major component of Intelligent Transportation Systems (ITS). In modern years, VANET develops with inter-vehicle communication (IVC). The main objective of VANET is improving security and transportation effectiveness in different applications such as emergency purposes, adaptive speed control, and traffic lane keeping, and assisted braking.

The IEEE standard 802.11p offers less significant PHY and MAC layer conditions for cooperating vehicles wireless access [2].In addition, IEEE 1609 standards are also called as Wireless Access for Vehicular Networks (WAVE) protocol which is developed for affording conditions for higher layers to provide vehicles multi-channel abilities for enabling them to access infotainment services. Particularly, vehicles are capable for accessing six service channels (SCH) as well as the control channel (CCH). The security information's are transmitted on the CCH and vehicles may transmit non-security information on SCH. Vehicles synchronously adjust to CCH for 50ms for receiving the entire cyclic and event-driven information's then switch to any SCH for other 50ms.

The main opinion of vehicular security applications is the requirement for vehicles for transmitting the information's about their location, speed and path direction. However, malicious information's are allowed for following an individual easily and probably blackmail them [3].Hence, the utilization of pseudonyms is developed for hiding vehicles and improving the privacy. Vehicles can utilize these pseudonyms as source address for their signals and communications with other vehicles. Therefore, information cannot connect to the vehicle and the privacy of users will keep back protected. There were several approaches developed in pseudonyms for vehicular networks. This paper will provide short description about those approaches and compared them to know about the effectiveness.

In [4] considered the consequences of pseudonym changes on the act of geographic directing which is utilized in VANET systems. The call-back technique was introduced for notifying the routing about unsuccessful communications. The effect of privacy-enhancement techniques on location based routing protocols were analyzed and improved.

In [5] developed pseudonymity for supporting anonymity in VANET. The challenges in pseudonymity and its incorporation in VANET system were explained. The different characteristics such as cross-layer addressing process, absolute position service, pseudonymity-improved packet transmitting approaches, and link-layer call-backs were discussed to obtain the solutions for pseudonymity.

In [6]discussed about the efficiency of the pseudonyms in VANET for confidentiality by varying pseudonyms. The various attacks on pseudonym change were described. The context combination method was established for illustrating the pseudonym change algorithms. The optimization technique was also explained for enhancing the confidentiality of VANET.

In [7] considered the efficiency of varying pseudonym in VANET for location confidentiality. The combine zone concept based representation was developed for differentiating the routing approach of challenger. The metric which is utilized for evaluating the level of confidentiality in vehicles was introduced. The issue in change of pseudonyms was solved by this model.

In [8] proposed an analytical framework for random changing pseudonym in VANET. The random changing pseudonym was described for evaluating the level of location confidentiality. This random changing pseudonym was compared with the uniform discrete distribution and age-based distribution to know about the effectiveness. The location privacy was provided by random changing pseudonym was improved.

In [9] described about the changing pseudonyms in VANET for confidentiality protection. The synchronous pseudonym change model was introduced for improving privacy protection. This model was developed based on the vehicular status information and simultaneously changing pseudonym. The attacks on changing pseudonym were also described. This model was analyzed according to the comparison with position and similar status models.

In [10] studied on the time of pseudonyms in Mobile Ad-hoc Network. The era of pseudonyms study was portrayed. The quantitative representation was produced for selecting the parts of pseudonym based confidentiality scheme in distributed wireless networks. The versatility of nodes and privacy level over period were captured by using this model.

In [11] investigated threshold anonymous announcement in VANET. The threshold anonymous announcement scheme based on direct anonymous verification was described. One-time anonymous verification was explained for simultaneously obtaining the reliability, privacy and audit ability. The performance of threshold anonymous announcement method was also analysed.

In [12] investigated an efficient approach in VANET for location confidentiality. An efficient pseudonym varying mechanism at social spots was proposed for establishing provable location privacy. Different anonymity models were introduced for investigating about the location privacy established by pseudonym changing strategy. The game-theoretic methods were provided for verifying the feasibility of pseudonym changing.

In [13] developed pseudonym management system in VANET for providing anonymity. According to the pseudonym generation, distribution and replenishing, the anonymity is achieved. The road side units were introduced as an important role in this model which receives the pseudonyms from trusted authority. The distributed optimization method was developed for shuffling process and also new technique was introduced for vehicles to change their pseudonyms.

ISSN (online) : 2277-5390
ISSN (Print) : 2277-5382

2. Comparison of pseudonym management systems

Ref. No.	Title	Merits	Demerits
[4]	Impact of pseudonym changes on geographic routing in VANETs	Routing efficiency is improved	Pseudonymity is not completely tackled
[5]	Support of anonymity in VANETs-putting pseudonymity into practice	Cost of pseudonymity is less since less delay	Privacy and security challenges are addressed
[6]	Privacy in VANETs using changing pseudonyms-ideal and real	Pseudonym modifications are masked	Attacker can easilyrecognize the nodes/vehicles
[7]	On the effectiveness of changing pseudonyms to provide location privacy in VANETs	Level of privacy is enhanced	The possibility of varying pseudonyms is high
[8]	An analytical model for random changing pseudonyms scheme in VANETs	Better position privacy, minimum use time	Limited to distributions which are used for pseudonym changes
[9]	Effectively changing pseudonyms for privacy protection in VANETs	Improve changing pseudonyms	Necessary to optimize the changing pseudonyms
[10]	On the age of pseudonyms in mobile ad hoc networks	Achieves more privacy	Requires optimization for pseudonyms changing
[11]	Threshold anonymous announcement in VANETs	Improve reliability, audit ability	Security challenges are addressed
[12]	Pseudonym changing at social spots: An effective strategy for location privacy in VANETs	Location confidentiality is high	Amount of changing pseudonyms must be optimized
[13]	A pseudonym management system to achieve anonymity in vehicular Ad hoc networks	High anonymity	Transmission cost of pseudonym is not reduced

3. Conclusion

There were different approaches developed along with pseudonyms management system for effectively achieving the anonymity or privacy which causes the authentication of vehicles in VANET. The developed techniques should able to improve the anonymity in VANET environment. Finally, the better approach should be selected for improving the privacy or anonymity of vehicles.

4. References

1. A.Prasanna, R. Asha. An Improved Selfish Node Detection in the Mobile Adhoc Network with the Consideration of Malicious Nodes Present in the Network. *Indian Journal of Innovations and Developments*, 2015; 4(4), 1-6.
2. D.Jiang, L.Delgrossi. IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments. In Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE. 2008 May; 2036-2040.
3. M.Raya, J. P.Hubaux. Securing vehicular ad hoc networks. Journal of Computer Security. 2007; 15(1), 39-68.

4. E.Schoch, F.Kargl, T.Leinmüller, S.Schlott, P.Papadimitratos. Impact of pseudonym changes on geographic routing in vanets. In European Workshop on Security in Ad-hoc and Sensor Networks. Springer Berlin Heidelberg.2006 Sep; 43-57.
5. E. Fonseca, A. Festag, R. Baldessari, R. L.Aguiar. Support of anonymity in vanets-putting pseudonymity into practice. In 2007 IEEE Wireless Communications and Networking Conference. IEEE, 2007 March; 3400-3405.
6. M.Gerlach, F.Guttler. Privacy in VANETs using changing pseudonyms-ideal and real. In 2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring. IEEE, 2007 April; 2521-2525.
7. L.Buttyán, T.Holczer, I. Vajda. On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In European Workshop on Security in Ad-hoc and Sensor Networks. Springer Berlin Heidelberg. 2007 July; 129-141.
8. Y.Pan, J.Li, L.Feng, B.Xu. An analytical model for random changing pseudonyms scheme in VANETs. In Network Computing and Information Security (NCIS), 2011 International Conference on IEEE. 2011 May; 2, 141-145).
9. J.Liao, J.Li. Effectively changing pseudonyms for privacy protection in vanets. In 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks. IEEE, 2009 Dec; 648-652.
10. J.Freudiger, M. H.Manshaei, J. Y.Le Boudec, J. P.Hubaux. On the age of pseudonyms in mobile ad hoc networks. In INFOCOM, 2010 Proceedings IEEE. 2010 March; 1-9.
11. L.Chen, S. L.Ng, G.Wang. Threshold anonymous announcement in VANETs. IEEE Journal on Selected Areas in Communications, 2011; 29(3), 605-615.
12. R.Lu, X.Lin, T. H.Luan, X.Liang, X.Shen. Pseudonym changing at social spots: An effective strategy for location privacy in vanets. IEEE transactions on vehicular technology, 2012; 61(1), 86-96.
13. H. Artail, N. Abbani. A pseudonym management system to achieve anonymity in vehicular Ad hoc networks. IEEE Transactions on Dependable and Secure Computing, 2016; 13(1), 106-119.

The Publication fee is defrayed by Indian Society for Education and Environment (iSee). www.iseeadyar.org

Citation:
T. Sivakumar[1], A.S. Nidhin. A Survey on Pseudonym Management Scheme in Vehicular Ad-Hoc Networks. *Indian Journal of Innovations and Developments.* 2016; 5 (6), June.