ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)
Vol. 2, Issue 3 (July - Sept. 2015)
International Journal of Advanced Research in Education Technology (IJARET)

Performance Evaluation of VANET Parameters for Security Enhancement Purposes using LTE

[I]Alisha Siwach, [II]Dinesh Kumar Verma
[I,II]PDM College of Engineering, Bahadurgarh, Haryana, India

Abstract
Vehicular Ad Hoc Networks has mostly gained the attention of today's research efforts, while current solutions to achieve secure VANET, to protect the network from adversary and attacks still not enough, trying to reach a satisfactory level, for the driver and manufacturer to achieve safety of life and infotainment. The need for a robust VANET networks is strongly dependent on their security and privacy features. VANET raises a privacy issue because it can track the location of vehicles and users' identity when a security mechanism is provided. In this paper, we analyze the problem of an existing solution for security requirements required in VANET, and resolve the problem of the existing method when a key management mechanism is provided for the security operation in VANET. Therefore, we show suitability of the Long Term Evolution (LTE) in VANET for the solution of this problem. Various vehicular parameters are evaluated using LTE.

Keywords
VANET, Security, RSU, LTE.

I. Introduction

In VANET, each vehicle is equipped with the technology that allows the drivers to communicate with each other as well as with roadside infrastructure's e.g. base stations also known as Roadside Units (RSUs) located in some critical sections of the road such as at every traffic light or any intersection or any stop sign in order to improve the driving experience and making driving safer. By using those communication devices known as On-Board Units (OBUs), vehicles can communicate with each other as well as with RSUs. VANET is a self-organized network that connecting the vehicles and RSUs and the RSUs can be connected to a backbone network so that many other network applications and services including Internet access can be provided to the vehicles.

There are two services provided by vehicular communication which are safety message and non-safety message. Safety message is mostly transferred by V2V communication, and it is life-critical. To provide the safe service, it should provide authentication and security service. There is a possibility that the message about safe driving is false information or the contents can be manipulated that can cause accidents.

Because of that, it is hard to introduce services from VANET without a proper security mechanism. Therefore, the message authentication should be provided. However, if messages are exchanged by an existing digital signature, that will cause the privacy threats. In terms of VANET, the studies are still being carried out to satisfy these privacy issues and the security mechanism at the same time. In addition, the high cost and the shortage of the RSU at the early stage of introduction become an obstacle for vitalizing vehicular communication. Thus, we choose LTE network as a solution to the privacy and security problem while reducing the initial building cost for vehicular communication system.

In section 2, we discuss about the proposed system LTE in brief. Consideration of VANET security through LTE is described in section 3. The simulators used for the operation are mentioned in section 4. Then the results of the simulations with graphs are shown in section 5. Finally, we conclude this paper in section 6.

II. Proposed System

Due to the Pros-Cons available of the RSU as well as the LTE the proposed work considers the network that consists of RSU as well as LTE. The RSU initiates the communication that can be carried out by the LTE. The LTE covers a greater range as compared to RSU. The proposed system also uses the SHA for the integrity of the DATA. SHA is added to the routing protocol AODV before sending the packet. Due to this data integrity is maintained at the LTE as well as RSU and vehicle also. This confirms the integrity of the data.

In the proposed work Firstly Data initiates from RSU that is passed to vehicles as well as to the LTE. Then each vehicle transmit the data to other, the updating can be done by using the RSU or LTE. LTE also communicate with the other LTE this increase the range of data without increasing the cost. LTE network has the property of transmitting data to far away node with lesser delay and maximum efficiency. Whereas in case of VANET, as the node distance increases, the corresponding delay and efficiency decreases. So it is obvious that LTE network performs well when compared to VANET alone network scenario.

A.) Advantages of LTE

We chose LTE for different reasons:

(i) It is well suited to support the traffic induced by our protocol (a total of 20 kbps for 400 vehicles).
(ii) LTE coverage is about 1to2 Km and is hence adapted to the vehicular network organization/management: about 400 vehicles to manage for a single Node B in an urban area.
(iii) The usage of a centralized mechanism is intuitively better than the usage of decentralized mechanism, since the Node B has a global view of its coverage area which can improve the clusters' management.
(iv) Most of the proposed VANET architectures (like CALM) proposes multiple interfaces in the vehicle, including 802.11p and LTE. This framework can have a lot of applications. Indeed, vehicles have become more sophisticated and are aware of not only their operational state but also of their surroundings, through sensors, radars or GPS receivers.

B.) The possibility of utilizing through the LTE in VANET-

Table I shows performance evaluation result the delay in third-generation (3G) and the fourth-generation (4G) by speed.

Table 1 (The Delay in 3G & 4G)

Speed (Km/h)	4G(LTE) (ms)	3G(HSUPA) (ms)
0	36.7	80
40-50	37.7	82.6
80-90	45	92.2
100-110	64.1	94

According to the performance evaluation result in VANET, both 3G and 4G met the non-safety message's delay requirement, which is under 100ms. However, this test is not considered the operation time because the test is performed by the ping. If the delay added the operation time for cryptography of 20ms about the upper layer, 3G not satisfied. Therefore, it is proved that LTE is proper for providing non-safety application service.

III. Consideration of Vanet Security Using LTE

To provide VANET communication, the cost and time for constructing the infrastructure will be needed. Thus, the using of LTE in VANET is anticipated that the commercialization of VANET is activated more quickly. The Table 2 shows the solution in LTE for the unresolved issues of the security in VANET.

Table 2

No.	Consideration of VANET Security	Solution in the LTE
1.	When the RSU is not sufficiently installed	The HSS sends the IMSI and LTE key to MME when the device is connected in LTE
2.	Problem of Privacy Protection by the exposure of ID	Alternates the IMSI by generating the GUTI that is the temporary ID

1.) According to existing studies about VANET, the key can be generated by RSU. However, the key generation cannot be provided by RSU because the density of RSU placement has not yet been determined. Therefore, if the LTE is used, this problem will be solved through the Authentication and Key Agreement (AKA) protocol. The authentication protocol performs an authentication of device through the key information sent from Home Subscriber Server (HSS). The HSS has the International Mobile Subscriber Identity (IMSI) and the master key of the EPS called LTE key. It sends the key information to Mobility Management Entity (MME) for authentication of the user's device. Even though the RSU is not installed, the key generation is able to make use through an allowed key exchange mechanism that the AKA. Therefore, the LTE is anticipated that it is a suitable for MVNET by generating the key through the AKA authentication protocol.

2.) In LTE, the identifier is used to GUTI (Globally Unique Temporary Identifier) instead of the IMSI for solving the problem of privacy protection. When the device initially connects, it requests the registration as IMSI. And the GUTI is allocated from the MME. After this, if the device re-connects in other networks it can be solved the problem of privacy protection by using the GUTI.

IV. Simulators Used

A. VANET MOBISIM (Mobility Simulator)

MobiSim is an extension of the CANU Mobility Simulation Environment (Canu MobiSim) which focuses on vehicular mobility, and features realistic automotive motion models at both macroscopic and microscopic levels. At the macro-scopic level, VANET MobiSim can import maps from the US Census Bureau topologically integrated geographic encoding and referencing (TIGER) database, or randomly generate them using Voronoi tessellation. At the microscopic level, it supports mobility models such as Intelligent Driving Model with Intersection Management (IDM/IM), Intelligent Driving Model with Lane Changing (IDM/LC) and an overtaking model (MOBIL), which interacts with IDM/IM to manage lane changes and vehicle accelerations and decelerations, providing realistic car-to-car and car-to-infrastructure interactions. VANET MobiSim is based on JAVA and can generate movement traces in different formats, supporting different simulation or emulation tools for mobile networks including ns-2, GloMoSim, and QualNet.

1. The macro-mobility models focuses on the macroscopic point of view, i.e. motion constraints such as roads, streets, crossroads and traffic lights, the generation of traffic such as traffic density, traffic flows and initial vehicle distribution.
2. The micro-mobility model focuses on the microscopic descriptions, i.e. the behavior of each driver individually when interacting with other drivers or with the road infrastructure.

B. Network Simulator (NS2)

Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors.

NS2 is a free simulation tool. It runs on various platforms including UNIX (or Linux), Windows, and Mac systems. Being developed in the UNIX environment, with no surprise NS2 has the smoothest ride there and so does its installation. Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community since its birth in 1989. Ever since, several revolutions and revisions have marked the growing maturity of the tool, thanks to substantial contributions from the players in the field. Among these are the University of California and Cornell University who developed the REAL network simulator the foundation which NS is based on.

V. Results

The following parameters are used for the simulation through which the performance of LTE is shown with RSUs –

a.) Routing Overhead- Nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

b.) Packet Delivery Ratio (PDR) - The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

$\sum$ Number of packet receive / $\sum$ Number of packet send

c.) End-to-end Delay- The average time taken by a data packet to arrive in the destination. It also includes the delay caused by

route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

∑ (arrive time – send time) / ∑ Number of connections

The overall framework of the proposed work is completely understood. Previous work is implemented and studied properly. Proposed work's implementation and simulation is done using AODV protocol with the help of NS2, RSU and LTE are combined using AODV and its performances are analyzed. The resultant snapshots, table and graphs are as follows

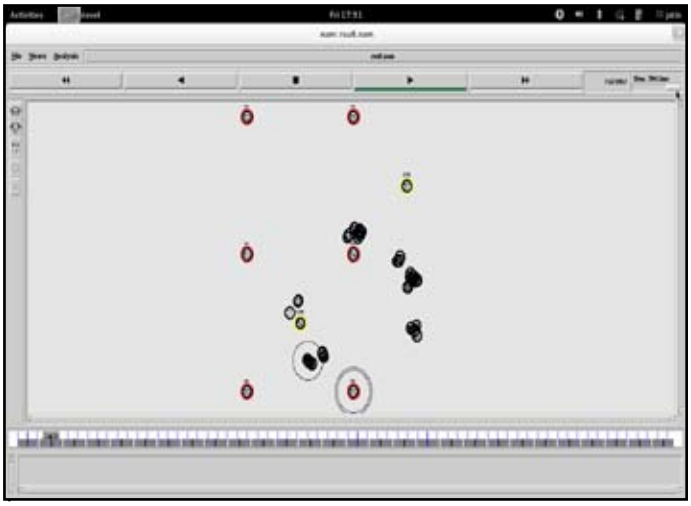

Fig.1 : Communication between RSUs & LTE

The Performance Analysis of Various no. of RSUs with LTE is shown in the following table:

Table 3

No. of RSUs	Routing Overhead	Packet Delivery Ratio (PDR)	Avg. End-to-End Delay (ms)
RSU 3	0.247	99.0415	36.3293
RSU 6	0.376	97.5856	34.6265
RSU 9	0.400	96.3347	34.3652

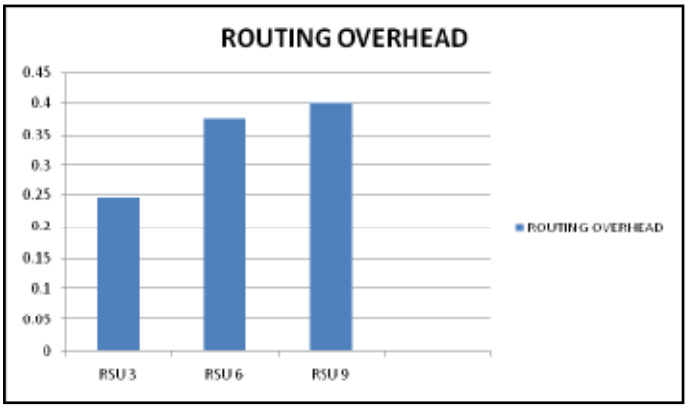

Fig. 2 : Graph Showing the results of Routing Overhead

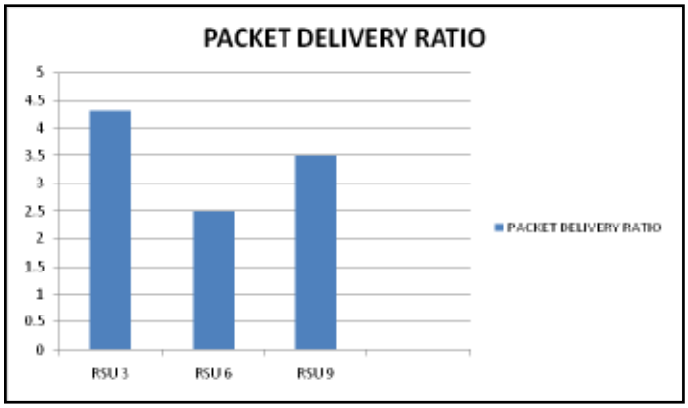

Fig.3 : Graph Showing the Results of Packet Delivery Ratio (PDR)

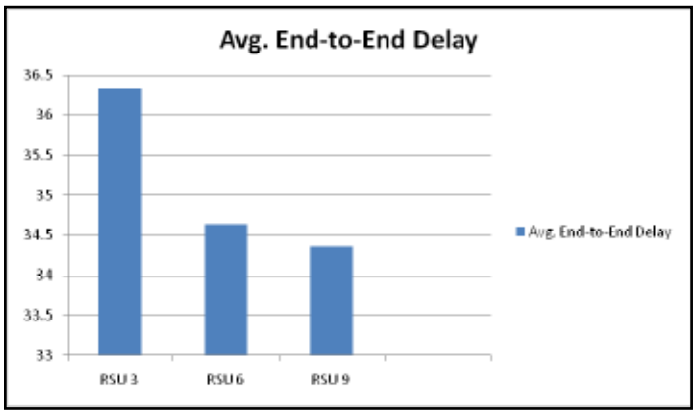

Fig. 4 : Graph Showing the Results of Average End to End Delay

VI. Conclusion

In this paper, we discussed the existing proposed methods for satisfying the security requirement in VANET and described the unresolved problems in VANET. In addition, the key management necessarily needs for this security requirement. Thus, the considerations about the problems among the existing solutions in the key management are also examined. To solve the problems, we looked for the possibility to apply the LTE in the VANET by studying the security of LTE. Research has analyzed the problem of an existing solution for security requirements required in VANET, and resolve the problem of the existing method. The algorithm is showing suitability of the LTE in VANET in the presence of RSU.

References

[1] *Hannes Hartenstein and Kenneth P. Laberteaux, "VANET Vehicular Applications and Inter-Networking Technologies," WILEY, pp299 – 363, Dec. 2009.*

[2] *Michael E. Nowatkowski, "Certificate Revocation List Distribution in Vehicular Ad hoc Network," Georgia Institute of Technology, May. 2010.*

[3] *D. Chaum and E. van Heyst, "Group signatures," Proc. Eurocrypt, vol. 547, pp. 257 – 265, 1991.*

[4] *Shuai Zhang, Jun Tao, Yijia Yuan, "Anonymous authentication-oriented vehicular privacy protection technology research in VANET," International Conference on Electrical and Control Engineering (ICECE), pp.4365-4368, Sept. 2011*

[5] *K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: robust location privacy scheme for VANET", IEEE Journal on Selected Areas in Communications, vol.*

25, no. 8, pp. 1569 – 1589, 2007

[6] Sun-Hee Han, Hun-Jung Lim, and Tai-Myoung Chung "The possibility to resolve the security problems through the LTE in vehicular ad-hoc netwoks", World Academy of Science, Engineering and Technology Vol:6 2012-04-24.

[7] Ho-Yeon Kim, Dong-Min Kang, Jun-Ho Lee "A Performance Evaluation of Cellular Network Suitability for VANET" World Academy of Science, Engineering and Technology Vol:6 2012-04-23

[8] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures "Security Analysis of Vehicular Ad Hoc Networks" 2010 Second International Conference on Network Applications, Protocols and Services.

[9] B. Shrestha, D. Niyato, Z. Han and E. Hossain, "Wireless access in vehicular environments using BitTorrent and bargaining," in Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE, 2008, pp. 1-5.

[10] Y. Gunter and H. Grobmann, "Usage of wireless LAN for inter-vehicle communication," in Intelligent Transportation Systems, 2005. Proceedings. 2005 IEEE, 2005, pp. 408-413.

[11] E. Dahlman, 3G Evolution: HSPA and LTE for Mobile Broadband. Academic Press, 2008. [12] Amendment of the Commission's Rules Regarding Dedicated Short-Range Communications Services in the 5.850-5.925 GHz (5.9 GHz Band) Available: https://www.federalregister.gov [13] D. Jiang and 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, pp. 2036-2040.

[14] Y. Zhang, J. Zhao and G. Cao, "Service scheduling of vehicle-roadside data access, "Mobile Networks and Applications, vol. 15, pp. 83-96, 2010.

[15] R. H. Frenkiel, B. R. Badrinath, J. B. As, and R. D. Yates, "The infostations challenge: Balancing cost and ubiquity in delivering wireless data," IEEE Personal Communications, vol. 7, pp. 66–71, 2000.

[16] K. C. Lee, U. Lee and M. Gerla, —Survey of Routing Protocols in Vehicular Ad Hoc Networks, Information science reference, Advances in Vehicular Ad-Hoc Networks: Developments and Challenges, 2010.

[17] S. Sun, J. Kim, Y. Jung, and K. Kim, —Zone-based Greedy Perimeter Stateless Routing for MVNET, in Proceedings of International Conference on Information Networking (ICOIN 2009), January 2009.

[18] B. Mohandas, and R. Liscano, —IP address configuration in MVNET using centralized DHCP, in Proceedings of 33rd IEEE Conference on Local Computer Networks, Montreal, Canada, October 2008.