ISSN:0975-9646

Comparative Analysis of Performing Vehicle To Vehicle Communication Based On Two Tier Approach with High Security

Aarti R. Thakur
M.Tech, Department of Computer Science and Engineering
Nagpur Institute of Technology
Nagpur, India.

Prof. Jagdish Pimple
Department of Computer Science & Engineering
Nagpur Institute of Technology
Nagpur, India.

Abstract— In wireless networks, the security of data is an important aspect and encryption algorithms play an important role to provide the security to the wireless networks. In wireless sensor network Vehicular adhoc network (VANETs) consist of smart vehicles with sensing, computing and wireless communication capabilities and road side unit (RSUs). The main aim of the cryptography is to enhance the data confidentiality and privacy by making the information unintelligible. Hence the data cannot be interrupted by the intruders. In this paper, we propose a two tier approach for communication. The communication is based on two tier approach for security we have to use RC6 and compression we have to use aggregation of data algorithms. This paper also provides the communication between the vehicles. Suppose the vehicle1 present in one cluster as well as the vehicle12 present in another cluster in that situation using the two tier approach for establishing and performing the communication. The size of data is too large for transferring one cluster vehicle to another cluster in that case chances for data loss. For improving the speed of communication and recovering the loss of data in this paper we have to use the compression techniques.

Keywords— VANETs; RSUs; Cryptography; Encryption techniques; RC6; Aggregation of Data; Decryption techniques; Compression.

I. INTRODUCTION

According to recent technology forecasts [5], vehicles will be equipped with radio interfaces in the near future and vehicle-to-vehicle (V2V) communications will be available in vehicles by 2011. The IEEE 802.11p task group is working on the Dedicated Short Range Communications (DSRC) standard which aims at enhancing the 802.11 protocol to support wireless data communications for vehicles and the road-side infrastructure [39]. Road-Side Units (RSUs) to improve safety, traffic efficiency, driver assistance, and transportation regulation. The RSUs are expected to be located in the critical points of the road, such as traffic lights at road intersections.

Vehicular ad hoc networks (VANETs) consist of smart vehicles with sensing, computing, and wireless communication capabilities, and roadside units (RSUs), which serve as the smart vehicles' access points to the infrastructure network (e.g., the Internet). Both vehicle-to-vehicle (V2V) and vehicle-to-roadside (V2R) communications are based on dedicated short-range communication (DSRC) technology, DSRC also detects and corrects faulty data in the physical and MAC layers, providing valid data to the upper layers with data rates from 6 to 27 Mb/s. With V2V and V2R communications, VANETs promise substantial enhancements in traffic safety, traffic efficiency, and driving experience. Specifically, each node will broadcast beacons containing its driving state, such as location, speed, and heading direction, with a period of 100–500 ms. Thus, enabling each node to learn the driving states of the nearby nodes, VANETs support numerous traffic safety applications, such as collision avoidance and lane merge assistance .

Besides, real-time traffic statistics can be collected based on V2V and V2R communications, which will improve traffic management and efficiency. Last, V2V and V2R communications can support various value added applications to further enrich driving experience, such as automatic survey , advertising , and on-road video game playing . Especially, the potential to improve traffic safety alone is more than enough to justify the cost incurred by the research, development, and deployment of VANETs . Both traffic management applications and value-added applications can be regarded as free-riders. Thus, VANETs may enable more cost-effective solutions to various value-added applications.

Here, we aim to support vehicle performance monitoring and analysis applications based on VANETs. Such applications, including large scale vehicle field testing, after-sale vehicle performance monitoring, and remote vehicle diagnostics, generally rely on the long-term/ large-scale collection and proper mining of in vehicle sensor data. For instance, by collecting the engine states of vehicles of a particular model over (say) five years, extensive data mining can be performed by car manufacturers to gain important insights into the long-term performance of this vehicle model. Nowadays, several commercial vehicular telematics solutions, such as GM On Star and Ford SYNC , can support such applications.

However, these solutions are proprietary systems, which constrain their application scope to specific car manufacturers or fleet owners. Besides, such solutions generally rely on cellular communications (third or fourth-generation, 3G/4G) for data transmission, incurring service fees to the application users. Besides, with free access to all location and speed states, such solutions impose severe privacy risks to vehicle drivers. At the same time, mainly relying on low-rate near-field communications such as RFID and Bluetooth, the existing toll collection systems

are not fit for the long-term and large-scale collection of in-vehicle sensor data either.

Comparatively, VANETs can enable better solutions to these applications with ubiquitous and free V2V and V2R communications. Taking advantage of V2V and V2R communications, Vehicle View can cost-effectively support in vehicle sensor data collection and data mining without requiring additional hardware. Moreover, the relevant security and privacy issues are thoroughly investigated in Vehicle View, with preliminary solutions proposed. Thus, Vehicle View shows salient application potentials and economic prospects by supporting such applications in a cost-effective, secure and privacy-preserving way.

II. LITERATURE SURVEY

The survey is that, we have to provide the high security and the compression technique using that's the vehicles are communicates with each other easily. In VANETs, the *ad hoc domain* consists of vehicular nodes that considered number of vehicles in one cluster as well as the number of vehicles in another cluster. Then consider the vehicles in one cluster in that situation, distance between the vehicles are short or less i.e., the vehicles are communicates with each other easily. But in case of two clusters distance between them are long or high in that situation, vehicles taking more time for communication for this reason, we have to take one base station between the two clusters and using the compression technique. Using this technique optimized the time and efficiency and also increases the throughput.

Ranging from large-scale field testing to remote vehicle diagnostics, vehicle performance monitoring and analysis applications rely on the long-term and large-scale collection of in-vehicle sensor data. With wireless vehicular communications, vehicular ad hoc networks provide a promising platform for such applications. In this, we propose Vehicle View to support the large-scale and long-term collection and mining of in-vehicle sensor data. The system architecture and preliminary procedures of Vehicle View are proposed based on comprehensive considerations on the common functional, performance, and security requirements of such applications. Supporting various vehicle performance monitoring and analysis applications in a cost-effective, secure, and privacy-preserving way, Vehicle View shows great application potential and economic prospects.

Josep Domingo-Ferrer and Qianhong Wu discuss Vehicular *ad hoc* networks (VANETs) will improve traffic safety and efficiency provided that car-to-car communication stays trustworthy. Therefore, it is crucial to ensure that the information conveyed by vehicle-generated messages is reliable. A sensible option is to request that the content of a message originated by a certain vehicle be endorsed by nearby peer vehicles. However, neither message generation nor message endorsement should entail any privacy loss on the part of vehicles co-operating in it. This chapter surveys the available solutions to this security-privacy tension and analyzes their limitations.

P. Caballero-Gil discuss a communication system in wireless sensor network is used for optimizing security issues in vehicle to vehicle communication or vehicular adhoc network. The main goal of these wireless networks will consist in providing safety and comfort to passengers, but their structure will be also taken advantage with many different aims, such as commercial, access to Internet, notification, etc. From a general point of view, the basic idea of a VANET is straightforward as it can be seen as a particular form of Mobile Ad hoc Network (MANET). Consequently, in a first approach we could think on considering well-known and widely adopted solutions for MANETs and install them on VANETs. A VANET is a wireless network that does not rely on any central administration for providing communication among the so-called On Board Units (OBUs) in nearby vehicles, and between OBUs and nearby fixed infrastructure usually named Road Side Unit (RSU). In this way, VANETs combine Vehicle TO Vehicle (V2V) also known as Inter-Vehicle Communication (IVC) with Vehicle TO Infrastructure (V2I) and Infrastructure TO Vehicle (I2V) communications.

Yuh-Shyan Chen, Chih-Shun Hsu and Yi-Guang Siao discuss Routing protocols for vehicular ad hoc networks (VANETs) have attracted a lot of attention recently. Most of the researches emphasize on minimizing the end-to-end delay without paying attention to reducing the usage of radio. This paper focuses on delay-bounded routing, whose goal is to deliver messages to the destination within user-defined delay and minimize the usage of radio. The messages can be delivered to the destination by the hybrid of data muling (carried by the vehicle) and forwarding (transmitted through radio). In the existing protocol, a vehicle may only switch the delivery strategy (mulling or forwarding) at an intersection according to the available time of the next block. To improve previous works, our protocol uses linear regression to predict the available time and the travel distance and thus the vehicle can switch to a proper delivery strategy at a proper moment and can reduce the number of relays by radio. Our protocol contains two schemes: the greedy and centralized schemes. The greedy scheme uses only the local vehicle's speed to predict the available time and decide when to switch the delivery strategy; while the centralized scheme uses the global statistical information to make the decision. Simulation results justify the efficiency of the proposed protocol.

Elmar Schoch, Frank Kargl, Tim Leinm¨uller and Michael Weber discuss Vehicular networks are a very promising technology to increase traffic safety and efficiency and to enable numerous other applications in the domain of vehicular communication. Proposed applications for VANETs have very diverse properties and often require non-standard communication protocols. Moreover, the dynamics of the network due to vehicle movements further complicates the design of an appropriate, comprehensive communication system. In this work, we collect and categorize envisioned applications from various sources and classify the unique network characteristics of vehicular networks. Based on this analysis, we propose five distinct

communication patterns that form the basis of almost all VANET applications. Both the analysis and the communication patterns shall deepen the understanding of VANETs and simplify further development of VANET communication system.

III. PROBLEM STATEMENT

In what follows, the related work on vehicle to vehicle communication is reviewed first. Optimizing the vehicle to vehicle communication based on two tier approach with high security. Communication between the two vehicles are possible when the distance are short but in case of long distance problem occurred in communication. All the above authors trying to solve the problem using different approaches for example communication patterns in VANET, safety and privacy in vehicular communication and optimizing security issues etc.

Using all these approaches we have to resolve only security problems and the problem in that, communication between two vehicles are performed or possible securely but the speed of communication is low and the distance is long, in that situation the overall performance is very poor. We have to solve the problem regarding security and speed using the security and compression approach.

IV. PROPOSED APPROACH

In this, we have to solve the above problem using the security as well as compression technique at a time for improving the speed of communication with high security concept. And also optimized the energy efficiency, optimized the time and increase the throughput all are done with the help of compression. Using the encryption algorithm for encrypting the data with security and compression algorithm for compressed the long size data into short and perform the vehicle to vehicle communication fast. We have to implement the concept of high security using RC6 algorithms and to implement the concept of compression using aggregation of data algorithm for lossless compression data.

. In this, Vehicle View allows customers to derive the required data items based on the application requirements through secure and automatic interactions with VANETs. Besides, Vehicle View supports secure and efficient task dissemination and data collection from the participating vehicles. Eventually, the economical values can be securely and confidentially represented and distributed to all involved parties, to fully realize the economic potential of Vehicle View. Thus, Vehicle View can cost-effectively, flexibly, and securely support vehicle performance monitoring and analysis applications, promising great application significance and economic potential. As the first step, the performance and security (privacy) challenges of Vehicle View are identified, with novel solutions preliminarily proposed.

The two tier approach means:

- ✓ In first approach the communication based on RSUs
- ✓ Second approach after establishing the communication provides the security and compression.

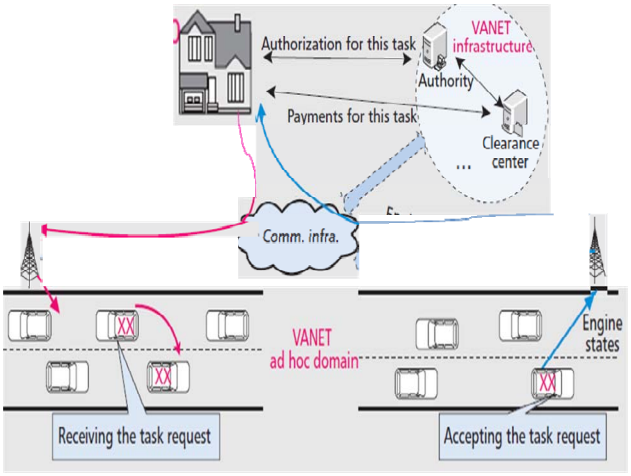

Figure Shows Communication in Infra Structure Domain are assumed to be secure and reliable

In addition to the above centralized authorities, road-side infrastructure can be expected in vehicular *ad hoc* networks. These distributed road-side units are very useful in collecting vehicular communications and optimizing traffic, distributing and relaying safety-related messages, enrolling vehicles from other VANETs and so on. Depending on the designated roles of the road-side infrastructure, the existing proposals assume very diverse numbers and distributions of road-side units. Some proposals require base stations to be distributed evenly throughout the whole road network, others only at intersections, and others at region borders. Due to cost considerations, especially at the beginning it is unrealistic to require vehicles to always have wireless access to road-side base stations.

1. Potential Applications

VANETs have various potential applications including collision avoidance, accident investigation, driving assistance, traffic optimization, traffic regulation, vehicle-based infotainment and so on. Basically, the applications fall into three categories.

Traffic safety related applications: These applications are the main thrust behind VANETs. There are tens of thousands of deaths each year and hundreds 176 J. Domingo-Ferrer and Q. Wu of thousands of people get injured in traffic accidents all over the world. Safety related messages from a road-side unit to a vehicle could warn a driver when she/he enters an intersection. V2V communications can save many lives and

prevent injuries. Some of the worst traffic accidents are due to many vehicles rear-ending each other after a single accident at the front of the line suddenly halts traffic. In this scenario, if a vehicle broadcasts a message about sudden braking to its neighbor vehicles and other receivers relay the message furthermore drivers far behind will get an alarm signal before they see the accident and such type of serious traffic accidents could be avoided. VANETs can also provide driving assistance, *e.g.* violation warning, turn conflict warning, curve warning, lane merging warning etc., to avoid traffic accidents. Many of the accidents come from the lack of co-operation between drivers. By giving more information about the possible conflicts, many life-

endangering accidents can be averted. Furthermore, given that vehicle state information and vehicular communications are accountable, VANETs can help in accident reconstruction and witness collection so that the injured and sacrificed can be compensated fairly in case of casualties.

Traffic optimization: With the increasing number of vehicles, people are experiencing more and more traffic delays during the rush hours. VANETs can greatly reduce traffic delays in several ways. Firstly, vehicles could serve as information source and transmit the traffic condition information for the vehicular network. Then transportation agencies could utilize this information to guide vehicles. This will finally relieve traffic congestion. Secondly, vehicles can also work as information collectors and collect data about weather or road surface conditions, construction zones, highway or rail intersections, emergency vehicle signal preemption, etc., and relay those data to other vehicles. Thirdly, the driving assistance provided by VANETs can also improve traffic efficiency. With that assistance, drivers can enjoy smooth and easy driving by avoiding possible conflicts. Finally, VANETs allow transportation administration authorities to manage vehicles electronically (*e.g.* speed control, permits, etc.), which is much more efficient than traditional manual administration.

Value-added services in VANETs: Since vehicles usually have sufficient computational capacity and power supply, complex protocols can be implemented to provide advanced services in VANETs. By implementing advanced electronic payment protocol in VANETs, one can achieve the convenient and desirable goal of passing a toll collection station without having to reduce speed, wait in line, look for some coins and so on. As GPS systems have become available in many vehicles, it is also possible to realize location-based services in VANETs, for instance, finding the closest fuel station, restaurant, hotel, etc. Other kind of services include infotainment, vehicle-based electronic commerce and so on. All these services lead to a more comfortable driving experience and an easier life for drivers, although they are not the main purpose when designing VANETs.

V. METHODOLOGY

1. Security :-

The demand for the ubiquitous personal communications is driving the development of new networking techniques. In the wireless communication the security of the data plays the vital role. To improve the security of the data being transmitted various techniques are employed. The important method used to provide the confidentiality is the data encryption and decryption technique. Network security becomes more crucial when the volume of the data becomes larger and complex. We have to use the RC6 algorithm is as follows

- ***Rivest Cipher 6 Algorithm:-***

In 1995, RC5 came about from Ronald Rivest, one of the creators of the RSA algorithm (Rivest et al., 1998a). RC5 is a symmetric block cipher that relies heavily on data-dependent rotations (Rivest, 1997). RC5 has been the subject of many studies that have expanded the knowledge of how RC5's structure contributes to its security (Rivest et al., 1998a). With certain architectural constraints by the AES competition, RC5 did not appear to be the best fit. However, in 1998, RC5's successor is born: RC6. Improvements over RC5 include using four w-bit word registers, integer multiplication as an additional primitive operation, and introducing a quadratic equation into the transformation (Rivest et al., 1998a).

Algorithm Details:

RC6, like RC5, consists of three components: a key expansion algorithm, an encryption algorithm, and a decryption algorithm. The parameterization is shown in the following specification: RC6-*w/r/b*, where *w* is the word size, *r* is the non-negative number of rounds, and *b* is the byte size of the encryption key (Rivest et al., 1998a). RC6 makes use of data-dependent rotations, similar to DES rounds (Rivest et al., 1998a). RC6 is based on seven primitive operations as shown in Table 1. Normally, there are only six primitive operations (Rivest et al., 1998a); however, the parallel assignment is primitive and an essential operation to RC6. The addition, subtraction, and multiplication operations use two's complement representations (Rivest, 1997). Integer multiplication is used to increase diffusion per round and increase the speed of the cipher (Rivest et al., 1998a).

Table 1: RC6 Operations (Rivest et al., 1998a)

Operation	Description
`a + b`	Integer addition modulo 2^w
`a – b`	Integer subtraction modulo 2^w
`a` ⊕ `b`	Bitwise exclusive-or (XOR) of w-bit words
`a x b`	Integer multiplication modulo 2^w
`a <<< b`	Rotate the *w*-bit word a to the left by the amount given by the least significant ($\log_2 w$) bits of *b*
`a >>> b`	Rotate the *w*-bit word a to the right by the amount given by the least significant ($\log_2 w$) bits of *b*
Enc: `(A,B,C,D) = (B,C,D,A)` **Dec:** `(A,B,C,D) = (D,A,B,C)`	Parallel assignment of values on the right to registers on the left.

Diffusion

Diffusion involves propagating bit changes from one block to other blocks. An avalanche effect is where one small change in the plaintext triggers major changes in the cipher text. To speed up the avalanche of change between rounds, a quadratic equation is introduced (Rivest et al., 1998a). By increasing the rate of diffusion, the rotation amounts spoiling sooner is more likely, due to the changes from simple differentials (Rivest et al., 1998a). To achieve the security goals for transformation, the following quadratic equation is used twice within each round:

$$f(x) = x(2x + 1)(mod\ 2^w)$$

The high-order bits of this equation, which depend on all of the bits of *x*, are used to determine the rotation amount used (Rivest et al., 1998a). In conjunction with the quadratic equation, the ($\log_2$ w) bit shift complicates advanced cryptanalytic attacks (Rivest et al., 1998a).

Integer multiplication also contributes by making sure that all of the bits of the rotation amounts are dependent on the bits of another register (Rivest et al., 1998a).

2. **Compression:-**

For the compression of data means to reduced the size of data. The communication established between vehicle to vehicle (i.e. source and destination) but the size of data is too long in that case we have to use the compression techniques for reduced or compressed the data size. In this paper for compression we have to use the aggregation of data algorithm

A) Aggregation of data:-

Data aggregation is important in energy constraint wireless sensor networks which exploits correlated sensing data and aggregates at the intermediate nodes to reduced the number of messages exchanged network.

Data aggregation is a type of data and information mining process where data is searched, gathered and presented in a report-based, summarized format to achieve specific business objectives or processes and/or conduct human analysis. In data aggregation it takes only the unique data and remove the duplicate data i.e. after this the size of original data or string are reduced because it takes unique data bits. For example Suppose we have to send data is{1,3,4,2,5,4,6,7,8,9,1,2,3,4} like that the size data is long for sending it consume more time. To remove this problem we are using the data aggregation it takes only the unique data bits i.e.{1,2,3,4,5,6,7,8,9} and it removes the duplicate data so the size of data is reduced and speed is increased.

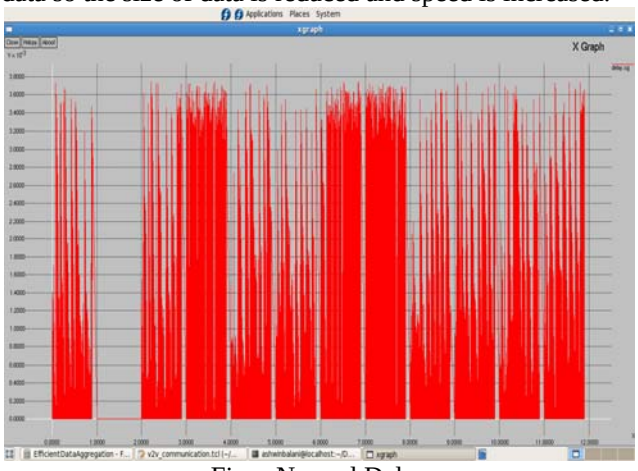

Fig: - Normal Delay

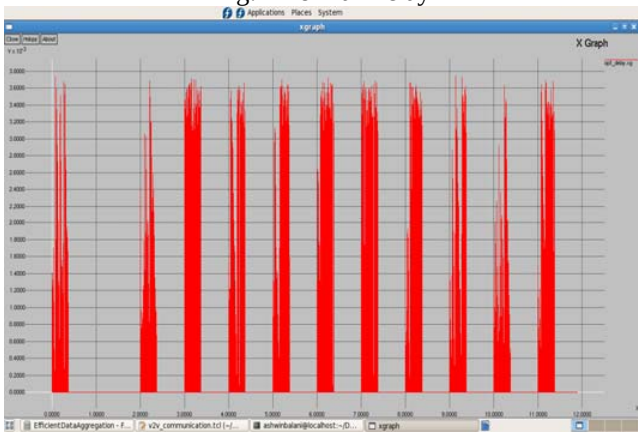

Fig: - Optimized Delay

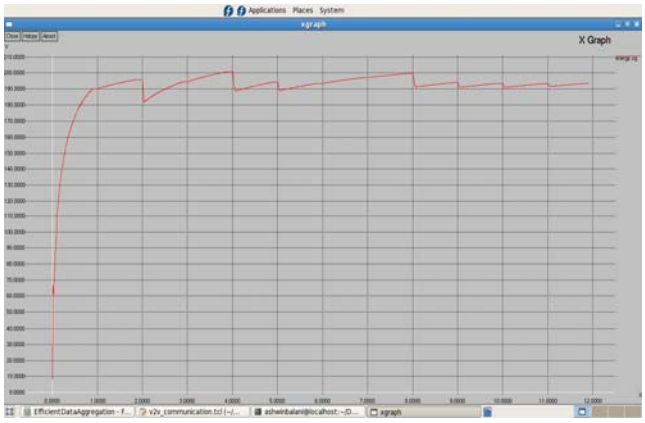

Fig: - Normal Energy

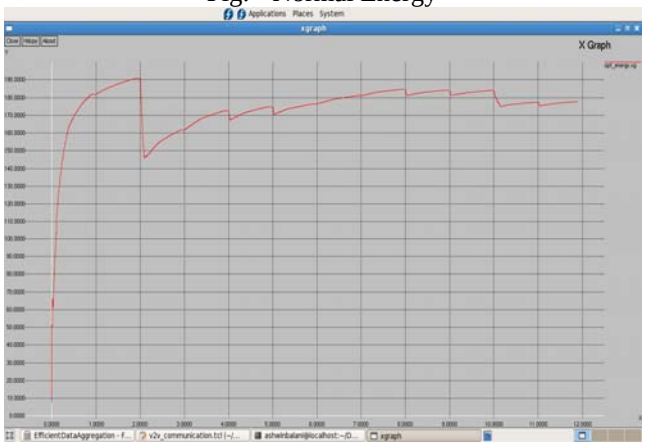

Fig: - Optimized Energy

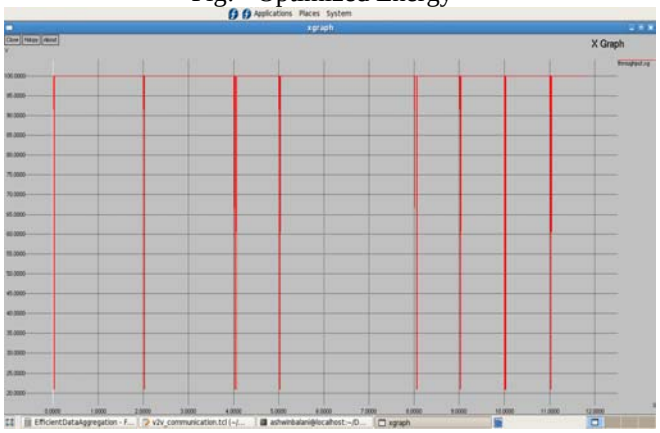

Fig: - Normal Throughput

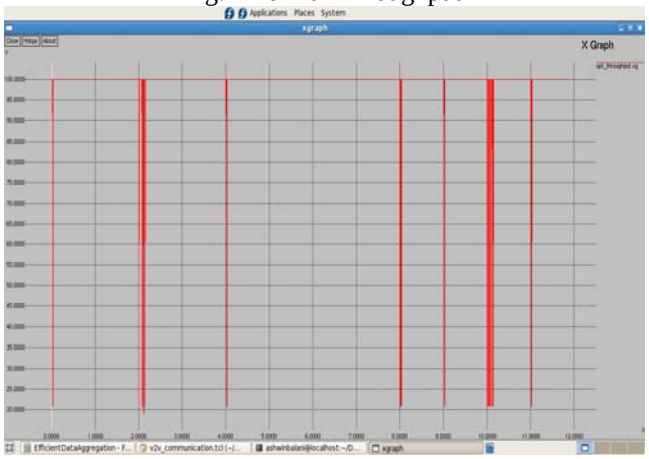

Fig: - Optimized Throughput

VI. CONCLUSION

In this paper, we have briefly reviewed the state of the art in VANETs. We have described their architecture and some of their potential applications, especially car-to-car information sharing in view of increasing traffic safety. We have justified why VANETs should be secure *and* preserve the driver's privacy. Security and privacy countermeasures proposed in the literature have been reviewed. In order to overcome the limitations of existing proposals, we have presented a framework combining both *a security* and *a compression* approaches. The new framework offers a better balance between public safety and driver privacy in VANETs.

Using two tier approach to improve the speed of communication with high security.

There are also other aspects that should receive more attention in the future. We need a more insightful consideration of the relationship between location privacy and anonymity. Anonymity mechanisms make it hard for attackers to link vehicles at specific locations with their identities. However, the location itself can leak information on vehicle identities. Also, content-based security in VANETs should be studied. Messages in VANETs contain much information about driving patterns. It is possible for attackers to extract much private information by collecting and mining vehicular communications. Finally, application-oriented security is also an open-ended line of work: more and more types of applications will appear in VANETs in the future, each bringing its own new security concerns.

REFERENCES

[1] Daza, V., Domingo-Ferrer, J., Sebe, F., Viejo, A.: Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology 58(4), 1876–1886 (2009).

[2] Golle, P., Greene, D., Staddon, J.: Detecting and correcting malicious data in VANETs. In: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, pp. 29–37 (2004).

[3] "Dedicated Short Range Communication (DSRC)," http://grouper.ieee.org/groups/scc32/dsrc/.

[4] Walter Franz, Hannes Hartenstein, and Martin Mauve, "Inter-Vehicle-Communications Based on Ad Hoc Networking Principles" – The FleetNet Project, W. Franz, H. Hartenstein, and M. Mauve, Eds. Universit¨atsverlag Karlsruhe.

[5] "Communication Patterns in VANETs" Elmar Schoch_, Frank Kargl_, Tim Leinm¨uller+, Michael Weber_ _Ulm University, Institute of Media Informatics, {elmar.schoch|frank.kargl|michael.weber}@uni-ulm.de +DENSO AUTOMOTIVE Deutschland GmbH,t.leinmueller@denso-auto.de

[6] Josep Domingo-Ferrer and Qianhong Wu "Safety and Privacy in Vehicular Communications Universitat Rovira i Virgili, UNESCO Chair in Data Privacy, Dept. of Computer Engineering and Mathematics, Av. Pa¨ısos Catalans 26, E-43007Tarragona,Catalonia{josep.domingo,qianhong.wu}@urv.cat

[7] "Linear Regression-Based Delay-Bounded Routing Protocols for Vehicular Ad Hoc Networks" Yi-Guang Siao Institute of Comm. Eng. National Taipei University Taipei 237, Taiwan, R. O. C.

[8] Pranay Meshram,Pratibha Bhaisare, S.J.Karale,",comparative study of selective encryption algorithm for wireless adhoc network" ,IJREAS Volume 2, Issue 2 , in International Journal of Research in Engineering & Applied Sciences.

[9] C. Liu, and C. Chigan, "GPAS: A General-Purpose Automatic Survey System based on Vehicular Ad Hoc Networks," *IEEE Wireless Commun.*, vol. 18, Aug. 2011.

[10] Z. Li, Z. Wang, and C. Chigan, "Security of Vehicular AdHoc Networks in Intelligent Transportation Systems," Ch. 6, *Wireless Technologies forIntelligent Transportation Systems*, 2009, pp. 133–74.