International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume2, Issue 8 (August '2016)

PERFORMANCE EVALUATION OF IMPROVED DIFFIE-HELLMAN ALGORITHM FOR SECURED DATA TRANSMISSION IN VANET

Dr.T.Ramaprabha,
Professor,
Department of Computer Science and Applications,
Vivekanandha College of Arts and Sciences for Women,
Tiruchengode,Tamilnadu,India.

V.Premalatha,
M.Phil Scholar,
Department of Computer Science,
Vivekanandha College of Arts and Sciences for Women,
Tiruchengode,Tamilnadu,India.

Abstract: A Vehicular Ad-Hoc Network is a form of mobile ad hoc network, which provide communications among nearby vehicles and nearest fixed equipment, like traffic sensor. Vehicular network act as an infrastructure to transfer the data between vehicles. Road Side Unit acts as a base station to deliver the data about the path to the vehicles using Diffie-Hellman key exchange algorithm.The Diffie-Hellman Key Exchange is one of the more popular and interesting methods of key distribution. It is a public-key cryptographic system whose sole purpose is for distributing keys and avoiding attackers.It gives high level security and more energy efficient data transmission on the network. Diffie-Hellman key exchange is used to find out another route quickly in case of false route. Diffie-Hellman algorithm can be used to recover the failure nodes. In this paper, we improve the performance and good delivery ratio and we do several processes like throughput, network performance, reliability over VANET.

KEYWORDS: VANET, RSU, OBU Security, Privacy.

I. INTRODUCTION ON VANET

The Vehicular Ad-Hoc Network, or VANET, is a technology that uses moves cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. Vehicular network faces wide range of attacks and the most common attacks are: impersonation, bogus information injection, non integrity, non confidentiality, and Denial of Service (DOS). Two classes of attacks are like to occur in vehicular networks such as

i) external attacks, in which attackers not belonging to the network jam the communication or inject erroneous information.

ii) Internal attacks, in which attackers are internal compromised nodes that are difficult to be detected.

Both types of attacks may be either passive intending to steal information and to eavesdrop on the communication within the network, or active modifying and injecting packets to the network. As a counter-measure against most of these attacks, the following security considerations should be satisfied providing a trusted infrastructure between communicating vehicles, mutual authentication between each communicating pair whether two vehicles or a vehicle and a fixed element of infrastructure, efficient access control mechanisms allowing not only the authorization to the network access but also the authorization to the services' access, confidential and secure data transfer. Since ITS (Information Technology scheme) applications are mainly targeting the peoples' safety on roads, while passengers oriented Non-ITS applications are mostly concerned with commercial services provision on roads, thus Securing inter vehicular communication is different in both cases as shown in figure1.1. As a consequence security requirements are different for each application type. For both types of applications, we found that the non-repudiation, the integrity and the non-traceability is important security requirements for worth considerations.

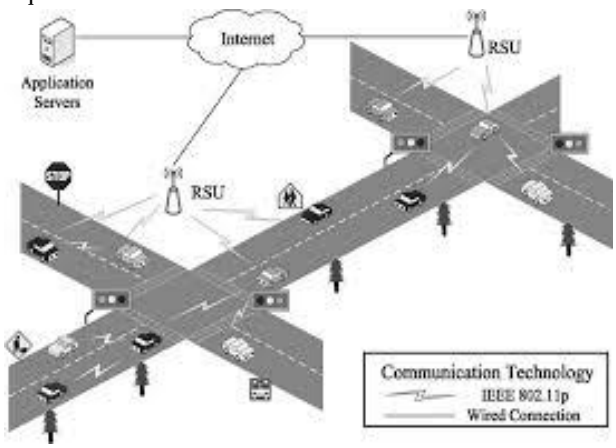

Figure 1: Communication Based on Vehicular Network by using the RSU

IJCRCST © 2016 | All Rights Reserved

Thus a complex problem arises in this issue. In fact, a tough requirement in vehicular networks environments is to manage traceability in terms of allowing this process for the concerned authorities and at the same time assuring the no traceability between mobile client's vehicles themselves. Nevertheless, the latter is difficult to be achieved and so far no promising solutions exist to resolve this issue in the vehicular networks dynamic and open environment. It is noticed that the word traceability can include:

(i) Authentication, Authorization and Access Control
(ii) Vehicular applications and Internet Implementations
(iii) Routable addresses and position based addressing

II. DIFFIE-HELLMAN KEY EXCHANGE ALGORITHM

It should be complemented with an authentication mechanism. In this approach for key distribution in security factors with respect fact that solving attacking problem is very challenging and that the shared key is never itself transmitted over the channel A distributed key management framework has advantage in revocation of malicious vehicles, system maintenance, and the implementation of heterogeneous security policies. A secure key distribution protocol is used with the capability of preventing from misbehaving. The protocol guarantees the traceability of compromised malicious vehicles. Structure of Data Transmission using Diffie-Hellman Algorithm as shown in figure 2.1. An efficient cooperative message authentication protocol is developed, by which cooperative verifiers are intelligently selected to significantly reduce the computation and communication overhead in the group signature based implementation.

A. KEY GENERATING NODE:

Active attackers have the ability to send packets into wireless channels. Global attackers have an unlimited scope which means they can listen to any information in the network. Attackers May have strong transmission power to communicate over long distances. Adversarial parsimony means an attack involving a few malicious nodes is more likely to happen than an attack that requires collusion among a large number of nodes. The key generating node(KGN) will assume that the vehicles will report to authorities when they find that the other vehicle sends a false message. Wired network which connects authorities transmits data securely without packet loss. In the key distribution phase, our protocol is used to moderator whether a vehicle is a legitimate user or not.

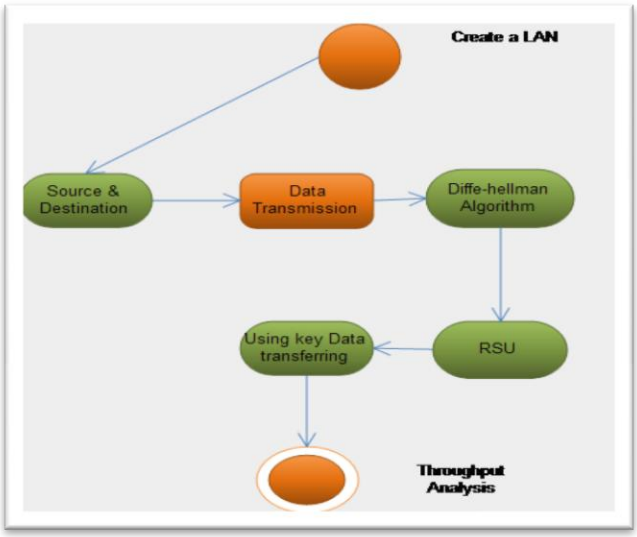

Figure 2: Structure of Data Transmission using Diffie-Hellman Algorithm

Algorithm should be complemented with an authentication mechanism. In this approach for key distribution in security factors with respect fact that solving attacking problem is very challenging and that the shared key is never itself transmitted over the channel.

B. RSU:

The RSU [1] Detection System using the Diffie-Hellman key exchange method used to be one of the most interesting key distribution schemes in use today. However, one must be aware of the fact that although the algorithm is safe against passive dropping, it is not necessarily protected from active attacks distribution to allow malicious nodes to interact within the network for transferring data between sources to destination and hence complete security could not be achieved within the network due to the presence of malicious nodes. In order to provide more secure communication between source and destination, DH uses risk as an input to determine how much source node can be trusted, so that only trusted nodes are allowed to communicate and hence high security can be achieved within VANET. They have to take a throughput, delay and delivery ratio are network performance on the network. It most efficient and security based data transmission.

Advantages:

- Diffie-Hellman algorithm is used to find out another route easily.
- Each user have own time slot.
- Efficient data transformation.
- Data will be transferred without any packet loss.

- Network performance is increased effectively.

III. DIFFIE-HELLMAN ALGORITHM IMPLEMENTATION IN NS-2

NS or the Network simulator (also popularly called ns-2) is a discrete event network simulator. It is popular in academia for its extensibility (due to its open source model) and plentiful online documentation. NS are popularly used in the simulation of routing and multicast protocols among others and are heavily used in ad-hoc networking research. NS supports an array of popular network protocols, offering simulation results for wired and wireless networks alike. It can be also used as limited –functionality network emulator. NS are licensed for use under version 2 of the GNU General Public License. A network simulator is a piece of software or hardware that predicts the behaviour of a network, without an actual network being present. Simulators typically come with support for the most popular protocols in use today, such as IPv4, IPv6, UDP, and TCP. Diffie-Hellman algorithm is implemented in NS-2.

A. NETWORK SIMULATOR 2.28 (NS2):

NS-2.28 is a packet-level simulator and essentially a centric discrete event scheduler to schedule the events such as packet and timer expiration. Centric event scheduler cannot accurately emulate "events handled at the same time" in real world, that is, events are handled one by one. This is not a serious problem in most network simulations, because the events here are often transitory. Nodes do not move significantly over the length of time they transmit or receive a packet. This assumption holds only for mobile nodes of high-rate and low-speed. Consider a node with the sending rate of 10Kbps and moving speed of 10m/s, during its receiving a packet of 1500B, the node moves 12m. Thus, the surrounding can change significantly and cause reception failure. The question of key exchange was one of the first problems addressed by a cryptographic protocol. This was prior to the invention of public key cryptography. The Diffie-Hellman key exchange algorithm is implemented as shown in figure 3. The point is to agree on a key that two parties can use for a symmetric encryption, in such a way that an eavesdropper cannot obtain the key.

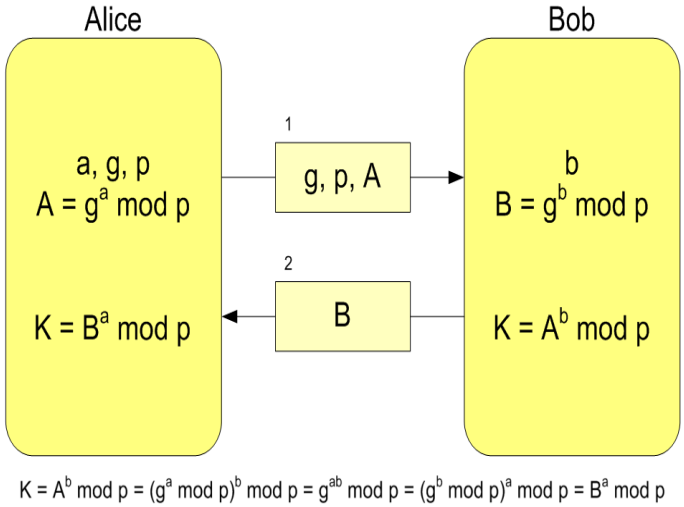

Figure 3: Diffie-Hellman Key Exchange Algorithm

B. STEPS IN THE ALGORITHM:

1. Alice and Bob agree on a prime number p and a base g.
2. Alice chooses a secret number a, and sends Bob (g a mod p).
3. Bob chooses a secret number b, and sends Alice (g b mod p).
4. Alice computes ((g b mod p) a mod p).
5. Bob computes ((g a mod p) b mod p). Both Alice and Bob can use this number as their key. Notice tha t p and g need not be protected.

In this section Table 1 we has compared the two algorithms on certain user defined parameters:

PARAMETERS	RSA	DIFFIE-HELLMAN
Ephemeral Keys	Generating ephemeral keys for RSA is extremely difficult.	Generating ephemeral keys for Diffie-Hellman is extremely easy.
Security	Relies on the difficulty of integer factorization	Relies on the difficulty of discrete logarithm.
Encryption	Encryption is cheaper	Encryption is expensive
Public Key	Public key is	Public key is

Encoding	smaller to encode.	bigger to encode.
Strength	RSA 1024 bits is less robust than Diffie-Hellman	Diffie-Hellman 1024 bits is much more robust
Authentication	Authenticates only the sender	Authenticates both the sender and the receiver.

Table 1: Comparative Study of RSA and Diffie-Hellman Algorithm

IV. EXPERIMENTAL RESULTS

This module figure 4 is developed to node creation and more than 10 nodes placed particular distance. Wireless node placed intermediate area. Each node knows its location relative to the sink. The access point has to receive transmit packets then send acknowledge to transmitter.

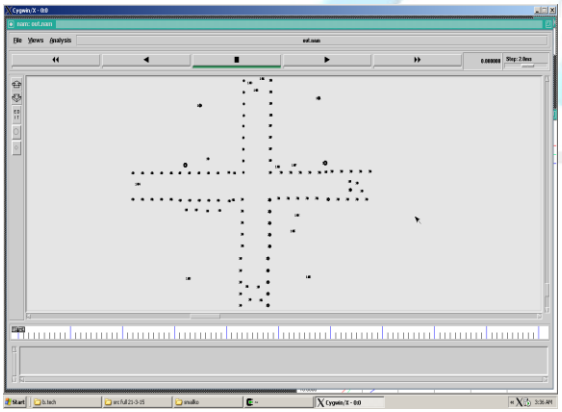

Figure 4: Node Creation

Figure 5 module is developed to Topology design all node place particular distance. Without using any cables then fully wireless sensor equipment based transmission and received packet data. Node and wireless between calculate sending and receiving packets. The cluster head is at the center of the circular sensing area. Intermediate the sender and receiver of this networking performance on this topology.

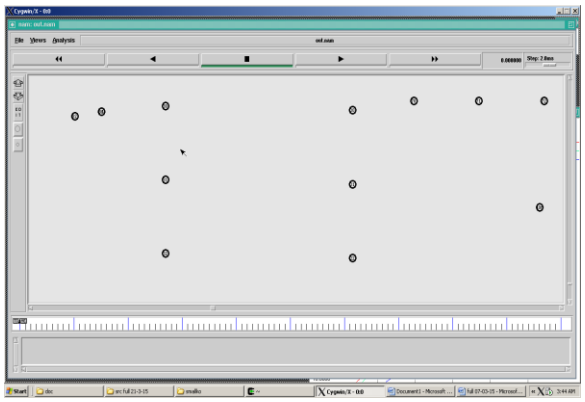

Figure 6: Topology Design

This module figure 7 shows wireless networks to create the no of nodes. The packets to send and receiving through the source to destination. It's based the scheme of packets delivered for ACK packet drop on the nodes. In this network to creating the source and destination node of the network and transmit the data to processing on their whole networking. Wireless networks use some sort of radio frequencies in air to transmit and receive data instead of using some physical cables. The most admiring fact in these networks is that it eliminates the need for laying out expensive cables and maintenance costs.

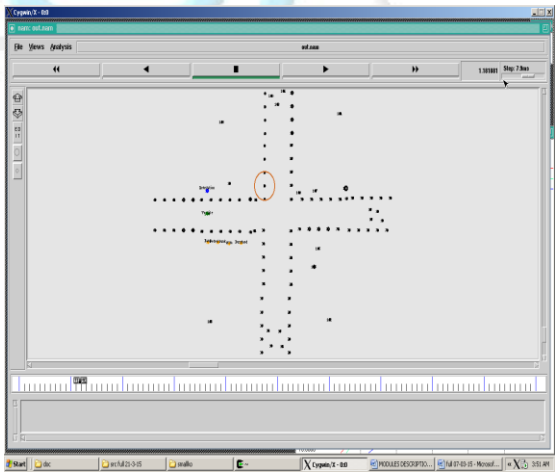

Figure 7: Wireless Network Configure Setting in RSU

This module figure 4.4 shows RSU consider into new way of communication. In this process to maintaining the separate time slot as well as key for every user. Vehicular Ad-hoc networks enable vehicles that are not necessarily within the same radio transmission range to communicate with each other.

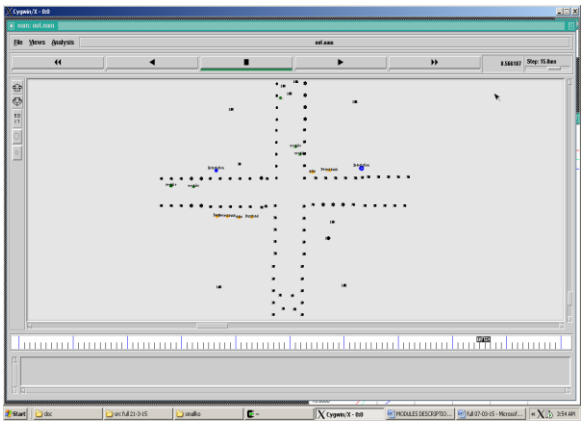

Figure 8: RSU Process

It connects RSU than later connected to the internet, forming a fixed infrastructure that refers then the capability of communicating with each other with roaming vehicles.

A. PERFORMANCE ON TRACE GRAPH

Trace graph figure 9 is a free tool for analyzing the trace files generated by ns2. Trace graph can support any trace format if converted to its own or ns2 trace format. Trace graph runs under Windows, Linux, and UNIX and MAC OS systems.

Some of the program features are as follows:

- 238 2D graphs: Trace graph supports drawing 238 different graphs depending upon different parameters in 2 Dimensional areas.
- 12 3D graphs: Trace graph supports 12 graphs in 3 Dimensions.
- Delays, jitter, processing times, round trip times, throughput graphs and statistics can be plotted with the help of Trace graph.

These are described below:

- Delay: This is the delay encountered between the sending and receiving of the packet.
- Jitter: This is the unwanted variation in the output.
- Processing Time: The time it takes for a node to process the input.
- Round Trip Time: The time required for a signal pulse to travel from a specific source to a specific destination and back again.
- Whole network, link and node graphs and statistics.
- All the results can be saved to text files, graphs can also be saved as jpeg and tiff.
- Any graph saved in text file with 2 or 3 columns can be plotted.
- Script files processing to do the analysis automatically.

The program does have some disadvantages though, such as it hangs or takes a very long time while trying to open large trace files. Also it sometimes hangs after displaying the graph in 3D. The reason why this tool was used in the simulation work is that there are not too many graph plotting tools available in the market.

Graph is an essential part of displaying a result, so we plot a graph to show a various result comparison with packets, throughput, delivery ratio and etc. In X-axis the level of energy will be shows. In Y-axis the lose level will be shows. In this graph, the throughput, packet delay and delivery ratio will be increased step by step. This comparison will be used to analyze the data transmitting level.

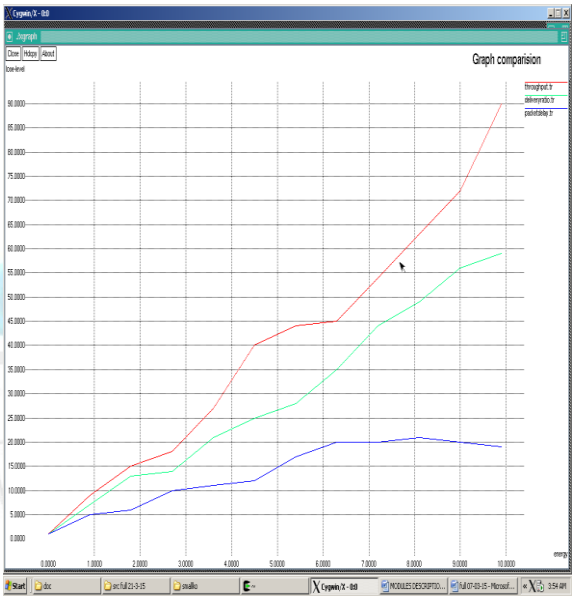

Figure 9: Graph Result for Improving Throughput, Packet Delay and Delivery Ratio

V.CONCLUSION

Driven by the real world implementing VANET with RSU is a compelling task. While the term RSU prepares user data and caches them during free TS before the users connect. Since, this network uses movable nodes from one place to another for preventing data from the attacker. The RSU enables that the sensor nodes can communicate each other securely to increase in network performance. With the use of Diffie-Hellman key exchange it is easy to find out another route quickly in case of false route. To support data transfer in efficient manner high performance networks are required, which impose systematic design on the network to unleash the power of the VANET. Diffie-Hellman algorithm can be used to recover the failure nodes. Finding trusted node is not essential, since all nodes are allowed to communicate. High security, most efficient

throughput, delays and delivery ratio can be achieved within VANET.

VI. REFERENCES

[1] Z. Chen, H. Kung, and D. Vlah, "Ad Hoc Relay Wireless Networks over Moving Vehicles on Highways," Proc. ACM Mobihoc, pp. 247-250, 2001.

[2] F. Bai, D.D. Stancil, and H. Krishnan, "Toward Understanding Characteristics of Dedicated Short Range Communications (DSRC) from a Perspective of Vehicular Network Engineers,"Proc. ACM MobiCom, 2010.

[3] Z. Li, Y. Liu, M. Li, J. Wang, and Z. Cao, "Exploiting Ubiquitous Data Collection for Mobile Users in Wireless Sensor Networks," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 2, pp. 312- 326, Feb. 2013.

[4] M. Li and Y. Liu, "Traffic Management through Inter-Communication between Cars using VANET System," IEEE /ACM Trans. Networking, vol. 18, no. 1, pp. 320-332, Feb. 2010.

[5] L. Chisalita and N. Shahmehri, "Distributed Key Management Techniques for Message Authentication in VANETs," Proc. Fifth IEEE Conf. Intelligent Transportation Systems, pp. 336-341, 2002.

[6] Z. Li, Y. Zhu, H. Zhu, and M. Li, "Compressive Sensing Approach to Urban Traffic Sensing," Proc. IEEE 31st Int'l Conf. Distributed Computing Systems (ICDCS), 2011.

[7] H. Zhu, Y. Zhu, M. Li, and L.M. Ni, "SEER: Metropolitan-Scale Traffic Perception Based on Lossy Sensory Data," Proc. IEEE INFOCOM, 2009.

[8] J. Eriksson, L. Girod, B. Hull, R. Newton, S. Madden, and H. Balakrishnan, "The Pothole Patrol: Using a Mobile Sensor Network for Road Surface Monitoring," Proc. ACM Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys), 2008.

[9] P. Gibbons, B. Karp, Y. Ke, S. Nath, and S. Seshan, "Privacy in Location-based Services: A System Architecture Perspective," IEEE Pervasive Computing, vol. 2, no. 4, pp. 22-33, Oct.-Dec. 2003.

[10] U. Lee, B. Zhou, M. Gerla, E. Magistretti, P. Bellavista, and A. Corradi, "Mobeyes: Smart Mobs for Urban Monitoring with a Vehicular Sensor Network," IEEE Wireless Comm., vol. 13,no. 5, pp. 52-57, Oct. 2006.

[11] I. Leontiadis and C. Mascolo, "GeOpps: Geographical Opportunistic Routing for Vehicular Networks," Proc. IEEE Int'l Symp. World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1-6, 2007.

[12] G. Marfia, M. Roccetti, C.E. Palazzi, and A. Amoroso, "Secure and Efficient Protocol for Vehicular Ad Hoc Network with Privacy Preservation," Proc. ACM MobiHoc Workshop Pervasive Wireless, 2011.

[13] I. Leontiadis, P. Costa, and C. Mascolo, "Silent Cascade: Enhancing Location Privacy without Communication QoS Degradation," Proc. IEEE INFOCOM, 2010.

[14] A. Balasubramanian, B. Levine, and A. Venkataramani, "A secure anonymous communication scheme in vehicular ad hoc networks from pairings," Proc. ACM SIGCOMM, 2007.

[15] J. Leguay, T. Friedman, and V. Conan, "DTN Routing in a Mobility Pattern Space," Proc. ACM SIGCOMM Workshop Delay-Tolerant Networking, pp. 276-283, 2005.