e-ISSN: 2349-9745
p-ISSN: 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

SECURE DATA TRANSMISSION BASED ON THE TRAFFIC DEPENDENCY ON COOPERATIVE ENVIRONMENT

R.Sangeetha [1] ,M.Ramya[2], B.Ranjani[3], A.Suganya[4]

[1] *Assistant professor/IT, Vivekananda College of Engineering for Women*
[2,3,4]*Information Technology, Vivekananda College of Engineering for Women*

Abstract— Currently, variety of networks has been developed in the society. Reliability and security plays a vital role in data transfer through network. Vehicular network is a collection of vehicles that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of change on a continual basis. Road side unit (RSU) which is used to facilitate communication within the network and it act as a base station (BS) as well as RSU maintain time slots and key for each node for gathering information from sender and receiver using Diffie-Hellman key exchange. 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, whereby it is used to exchange a single piece of information and where the value obtained is normally used as a session key for a private-key scheme. The key distribution scheme is based on intrusion detection method for using a data transmission from source to destination on the network. It gives high level security and more energy efficient data transmission on their network. At last several processes are performed to reach better delivery ratio, throughput, network performance, reliability over VANET.

Keywords- Vehicular Network; Road Side unit(base station);Key generating node(KGN); Diffie-Hellman Key Exchange; Key distribution scheme ; Intrusion detection method .

I. INTRODUCTION

Vehicular networks have special characteristics which makes them susceptible to a wide range of attacks. The most common attacks are: impersonation, bogus information injection, non integrity, non confidentiality and Denial of Service (DoS). Two classes of attacks are likely to occur in vehicular networks external attacks, in which attackers not belonging to the network jam. Internal attacks are in which attackers have internally 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, injecting packets to the network. As a counter-measure against most of these attacks, the following security considerations should be satisfied:

- Providing a trust infrastructure between communicating vehicles,
- Mutual authentication between each communicating pair whether two vehicles or a vehicle and a fixed element of the infrastructure,
- Efficient access control mechanisms allowing not only the authorization to the network access but also the authorization to the service access.

Since ITS applications are mainly targeting peoples safety on roads, while passenger oriented Non-ITS applications are mostly concerned with commercial services provision on roads, thus securing inter-vehicular communication is different in both cases. As a consequence, security requirements are different for each application. In fact, source authentication is a major Requirement for ITS applications to achieve the main ITS purpose which is accident avoidance. Source authentication can assure the legitimate safety related messages transfer on one hand and give every vehicle the right to receive safety-related messages on the other hand. Another important requirement

concerns the time-sensitivity during safety-related message transfer, which states that the critical transmission delay for these messages is about 100ms. On the other hand, passenger oriented non-ITS applications necessitate more security requirements, as for instance mutual authentication between each communicating parties such as confidential data transfer, efficient authorization for service access.

For both types of applications, we find that there is no repudiation; the integrity and the non-traceability are important security requirements that worth considered. Although traceability is a legitimate process for some governmental authorities and networks operators, the non-traceability is an important security requirement in order to assure people's privacy. 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 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.

II. RELATED WORK

Vehicular networks have frequent system disruption, fast topological change and mobility indecision and the vehicular trajectory information plays a key position in information delivery. It has made prediction on the flight with coarse-grained patterns such as spatial arrangements giving out the inter-meeting time distribution. By extracting mobility patterns from past vehicular traces, trajectory prediction uses various orders Markov chain process. This process derives packet delivery likelihood with predicted trajectory. Then it contains routing algorithms takes full benefit of predicted probabilistic vehicular trajectories. Finally, trajectory takes out extensive simulation based on big data sets of real GPS vehicular.

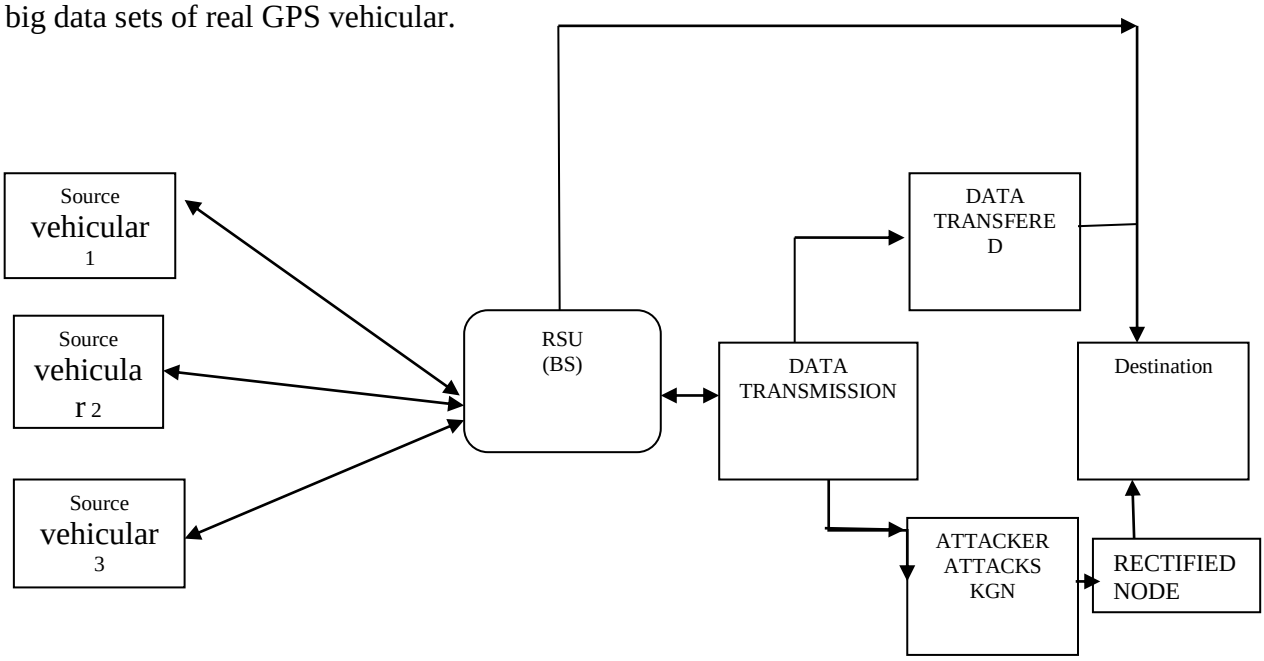


FIGURE 1. Architecture for Diffie-Hellman Key Structure

A. PACKET

A packet is composed of a stack of headers, and an optional data space. A packet header format is initialized when a Simulator object is created, where a stack of all registered (or possibly useable) headers, such as the common header that is commonly used by any objects as needed, IP header, TCP header, RTP header (UDP uses RTP header) and trace header, is defined, and the offset of each header in the stack is recorded. A stack is composed of all register headers which is created when a

packet is allocated by an agent, and a network object can access any header in the stack of a packet it processes using the corresponding offset value.

B. ROAD SIDE UNIT

RSU are important tools to support and extend safety- as well as efficiency applications. This paper depicts beneficial applications and the technological basis for RSU systems.

C. DIFFIE-HELLMAN KEY EXCHANGE

Diffie-Hellman key exchange (D–H) [nb 1] is a specific method of securely exchanging cryptographic keys over a public channel. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communication channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

D. ATTACKER IDENTIFIES KGN

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. 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. 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 MAC layer model is developed to quantitatively evaluate the impact of number of verifiers and the size of authentication messages on network utilization.

III. SCOPE OF THE PAPER

The RSU Detection System uses the Diffie Hellman key exchange method is one of the most interesting key distribution schemes. 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. Then throughput, delay and delivery ratio are network performance on the network are analyzed effectively. The RSU receives more efficient and security based data transmission.

A. Authentication, Authorization and Access Control

Authentication and authorization are important counter-attack measures in vehicular networks Deployment, allowing only authorized mobile nodes to be connected and preventing adversaries to sneak into the network disrupting the normal operation or service provision. A simple solution to carryout authentication in such environment is to employ an authentication key shared by all nodes in the network. Although this mechanism is considered as a *plug and play* solution and does not require the communication with centralized network entities, it is limited to closed scenarios of small number of vehicles, mostly belonging to the same provider. For wide scale commercial deployment of vehicular networks, the shared secret authentication has two main pitfalls: firstly, an attacker only needs to compromise one node vehicle to break the security of the system and paralyze the entire network. Secondly, mobile nodes vehicles do not usually belong to the same community, which leads to a difficulty in installing/pre-configuring the shared keys.

In fact, distributed authentication and authorization schemes with secure key management are required in such environment. A possible approach for distributed authentication is the Continuous discovery and mutual authentication between neighbors whether they are moving Vehicles or fixed architectural elements access points or base stations. Nevertheless, if mobile nodes vehicles move back to the range of previous authenticated neighbors or fixed nodes, it is necessary to perform re-authentication in order to prevent an adversary from taking advantage of the gap between the last association and the current association with the old neighbor to launch an impersonation attack. The re-authentication procedure should be secure and with the minimum possible delay in order to assure services' continuity.

B. Vehicular applications

Vehicles in a grid are only a few hops away from the infrastructure Wi-Fi, cellular, satellite. Protocol and application design must account for easy access to the Internet during normal operation. At the same time, the vehicles are among the few communications nodes that can continue to operate when the Internet goes away, during urban emergency, with enough reserve power to establish a vehicle based emergency network. To this end we examine innovative peer to peer content sharing applications that can still operate with intermittent connectivity and sporadic vehicular traffic and connectivity. Peer to peer applications have so far been confined to the fixed Internet. The storage and processing capacity of modern vehicles make such applications feasible also on mobile platforms. In these dynamic scenarios we must understand the role of the Internet in facilitating the smooth transition from full Internet connectivity to full autonomy. This is a radical concept in ad hoc networks traditionally designed for exclusively autonomous operation and thus unable to exploit the interconnection and resource sharing of the wired Internet. In the sequel, we consider a number of emerging VANET applications and study their interdependence with the Internet.

C. Routable addresses and position based addressing

Addressing is a major challenge in the management of vehicular network mobility and an important enabler of interconnection to and through the Internet. First, we must distinguish between Unique Identifier, license plate; Vehicle-ID, and; Routable Address (geo-coordinates, or; unique ID (typically IP address) for conventional routing AODV. It is becoming apparent that the dominant form of routing in the vehicle grid will be position based routing geo-routing. This is because of the emergence of location aware communications, i.e., the need to establish connections and route packets to entities and resources characterized by location rather than a specific ID. More traditional MANET routing schemes, AODV and OLSR, will also be used in the vehicle grid. These schemes

currently use IP address as the routable addresses to set up/maintain the routes. The IP address is an extremely effective routable address in the static, hierarchical Internet structure enabling, for example, prefix routing. It is not very helpful in finding (hierarchical) routes in a constantly changing network like the vehicle grid unless it is combined with the Mobile IP construct, with provides the desired redirection.

COMPARISION TABLE:

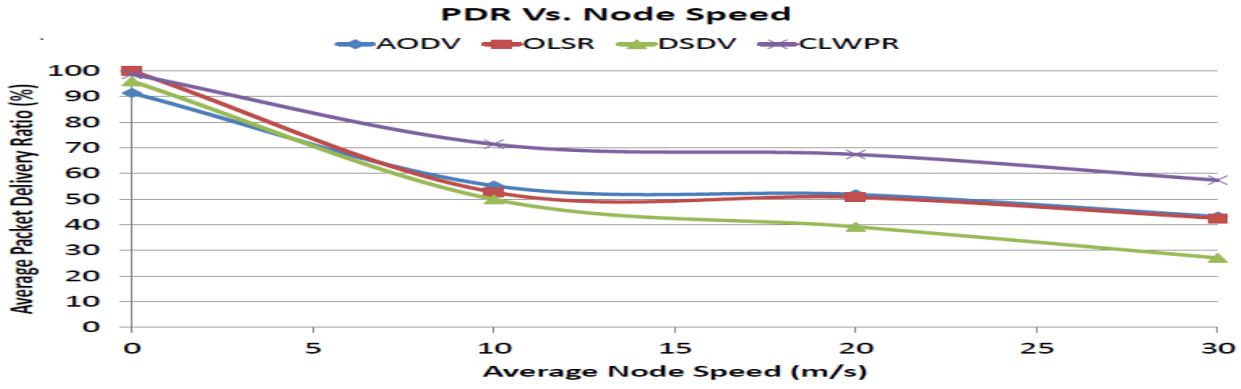
PARAMETERS	MARCOV CHAIN PROCESS	DIFFIE-HELLMAN ALGORITHM
Speed of the node	**56%**	**79%**
Network performance	**67%**	**86%**
Delivery ratio	**66%**	**99%**
Packet delay	**87%**	**23%**
Data loss	**93%**	**-----**

Table 2: ratio analysis of existing and future process

D. TRACE GRAPH

Trace graph 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.



VI. 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 a 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.

REFERENCES

[1] Trupti Gajbhiye, Akhilesh A. Waoo, P.S Pathija, "Traffic Management through Inter-Communication between Cars using VANET System", International Journal on Advanced Computer Engineering and Communication Technology Vol-1 Issue:1 :ISSN 2278 – 5140 ,2009.

[2] Jessy Paul, Elizabeth Saju, Mercy Joseph Poweth," Privacy in VANET using Shared Key Management", International JournalofInnovativeResearchinScience,EngineeringandTechnology*Vol.2,Issue3,March2013*

[3] M. Li and Y. Liu, "Rendered Path: Range-Free Localization in Anisotropic Sensor Networks with Holes,"IEEE /ACM Trans. Networking,vol. 18, no. 1, pp. 320-332, Feb. 2010.

[4] L. Chisalita and N. Shahmehri, "A Peer-to-Peer Approach to Vehicular Communication for the Support of Traffic Safety Applications," Proc. Fifth IEEE Conf. Intelligent Transportation Systems, pp. 336-341, 2002.

[5] 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.

[6] J. Jeong, S. Guo, Y. Gu, T. He, and D. Du, "TBD: Trajectory-Based Data Forwarding for Light-Traffic Vehicular Networks," Proc. IEEE 29th Int'l Conf. Distributed Computing Systems (ICDCS), 2009.

[7] I. Leontiadis, P. Costa, and C. Mascolo, "Extending Access Point Connectivity through Opportunistic Routing in Vehicular Networks," Proc. IEEE INFOCOM, 2010.

[8] 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.

[9] J. Krumm and E. Horvitz, "Predestination: Where Do You Want to Go Today?" Computer, vol. 40, no. 4, pp. 105-107, Apr. 2007.

