Performance Evaluation of Defense Mechanism in VANET

Amanpreet[1], Richa Gupta[2]

[1,2]Department of Cmputer science and Engineering, aman15preet@gmail.com
[2]Department of computer science and Engineering, Reechaaggarwal8@gmail.com
Haryana Engineering College, KUK University, India

Abstract— **VANET is a particular type of mobile ad hoc network which is an upcoming technology and is going to be an essential part of future traffic systems. VANET is basically meant to improve security and safety on the roads. In the present scenario where traffic is increasing on a daily basis and so are the accidents increasing, with the more and more number of vehicles on roads daily, the chances of collision and traffic jams has increased to a large extent. Drivers are unaware of the jams ahead and also of any accident that has occurred ahead. So VANET improves communication among drivers and helps them to find suitable routes. As every coin has two sides, VANET also has security problems due to the constantly changing configuration of the network and many other factors. One such threat is Sybil attack in which a single node claims to be multiple identities and does gives illusion of jam ahead. In this work the existing protocol has been studied and enhanced using timestamp series approach and is made to avoid the compromised node. This aimed to study the performance of protocol with the help of ns2 simulation. Results indicated that after enhancing the protocol, the packet drop ratio improved to a large extent.**

Keywords-Ad hoc Network; VANET; routing protocols; GPSR; Virtual Carrier Sensing;

1. INTRODUCTION

With VANET is abbreviated form of vehicular Ad hoc network. It is a form of Mobile Ad hoc Networks (MANETs), which provides communication between vehicles on road, and nearby fixed units called Road Side Units (RSUs). Every node in VANET i.e., either a vehicle or RSU communicates with any other node in single hop or multi hop. VANETs are designed with the goals of making driving more safe and comfortable. VANET includes the below mentioned communications:

- Inter-Vehicular Communication
- Vehicle-to-RSU Communication
- Inter-RSU Communication

Various communications of VANET are shown in figure 1.1.The channel used for the communication in VANET is DRSC. DSRC/WAVE supports inter vehicular and vehicle-to-RSU communications in Intelligent Transportation Systems ITS. DSRC systems eliminate the drawbacks in the wireless infrastructure by providing very less latency, geographically local, high data rate, and high mobility communications

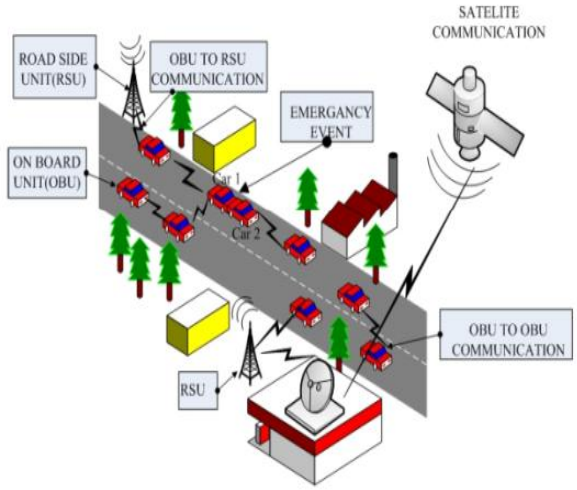

Figure 1.1 VANET Architecture

IEEE 802.11p is an improved version of the IEEE 802.11 standard to provide Wireless Access in Vehicular Environments (WAVE). It provides enhancements for 802.11 and supports Intelligent Transportation Systems applications. This includes exchange of data between highly mobile vehicles and between the vehicles and the RSU in the ITS band of 5.9 GHz. IEEE 1609 is a higher layer advanced standard based on the IEEE 802.11p.

1.1 Why VANET?

VANET is more useful as compared to Mobile Ad hoc Network (MANET) owing to elevated mobility of the nodes and it is also a fact that MANET does not support high movement. When the rate of node is rapid then the topology and arrangement changed quickly which cannot be handled by the mobile ad hoc network MANET so we need the VANET.

1.2 Characteristics of VANET:

- High mobility support
- Almost unbounded network size

- Time-sensitive packet transfer
- Accurate positioning of nodes
- Negligible power related problems
- Deployment in direction of road
- Large connection range and large amount of nodes possible
- Fast changing topology

1.3 Possible Applications of VANET

The most practical application of VANET is the Intelligent Transport System (ITS). ITS is an existent safety application which provides the information of one node to a different node. Given that the pathway of node is predefined so node cannot shift randomly and we can calculate the location of nodes past regular time interval on the base of their individual speed. An additional important and proficient function of VANET is Electronic Toll Collector (ETC). ETC is process of collection of toll electronically without stopping the nodes. Service finder is an application of the VANET. It can offer the location of adjacent filling stations, restaurant, etc.

1.4 Architecture of VANET

The ideology of safety may be précised by hierarchic level of assurance between us or by safety fundamentals as well as genuineness, data consistence confirmation, ease of use, privacy, non- negation and online intimidation.

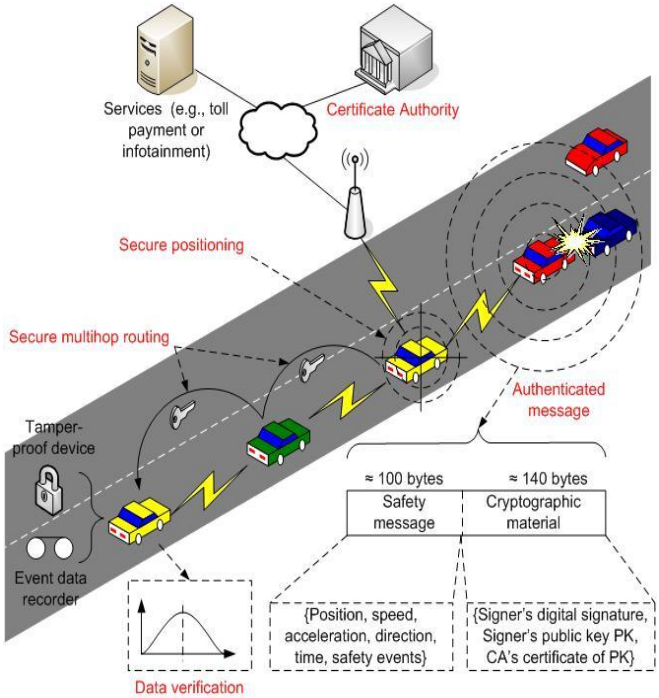

Figure 1.2 Architecture of VANET

Tamper- Proof device (TPD)

It is the safety device installed in the vehicles. It contains all the safety information related to the vehicle, a battery and a watch for management. It participates in all safety actions and it is simply realistic for the authorized person. Working of tamper proof device is shown in figure 1.3.Tamper proof device has communication with all sensors as well as transmission system in VANET.

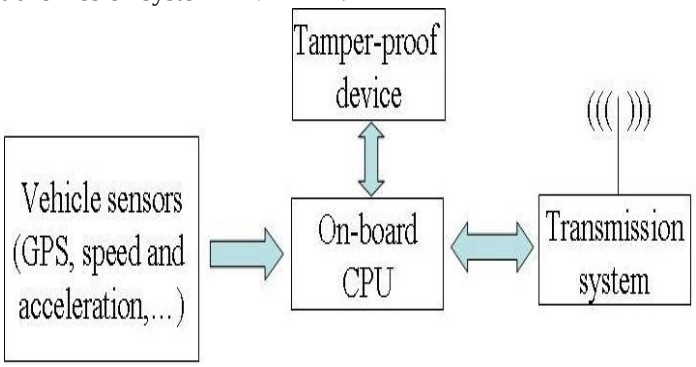

Figure 1.3 Tamper Proof Devices

Digital signatures

- Symmetric cryptography is not appropriate: messages are separate, large size, non-repudiation constraint
- Each message is supposed to be signed with a DS.
- Liability-related messages should be stored in the EDR.
- Structure of digital signatures is shown in figure below. Signer sends a message containing all its information along with cryptographic material and all nearby vehicles verify it.

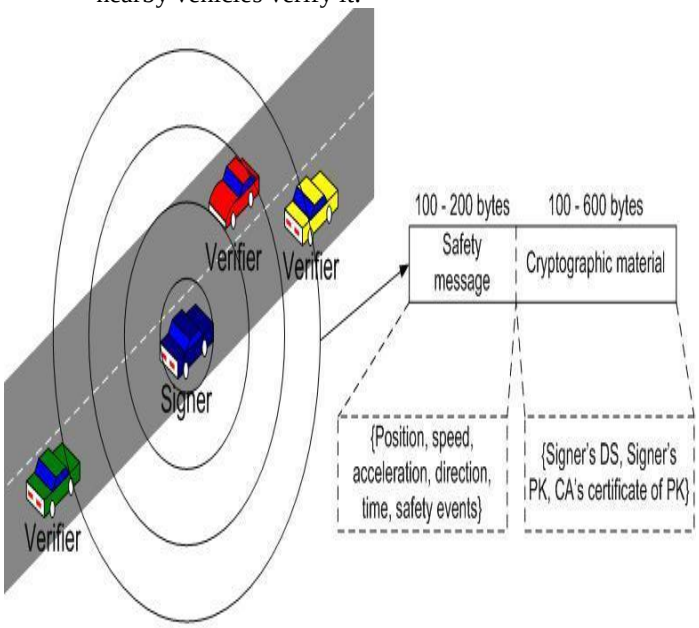

Figure 1.4 Digital Signatures

VPKI (Vehicular PKI)

- Every medium carries inside its Tamper-Proof Device i.e. TPD, A unique and certified identity, Electronic License Plate (ELP)
- Mutual authentication can be done without involving an attendant.

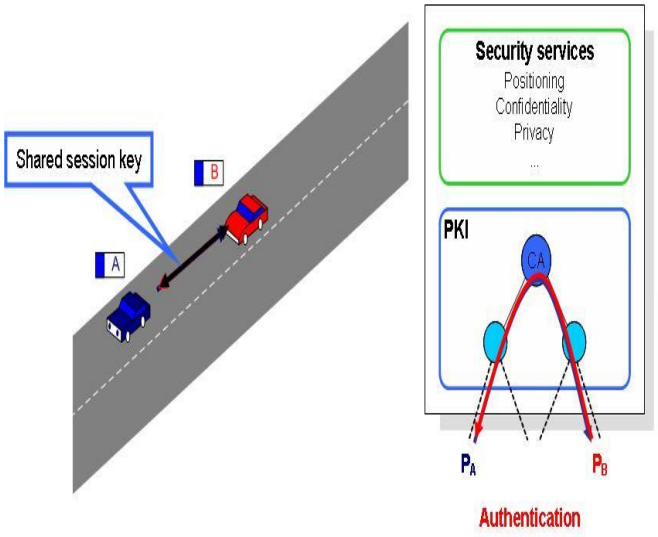

Figure 1.5: VPKI

1.5 Transmission of Packages in VANET

In ITS, it has exchange necessity information between vehicles such as position and speeds in order to guarantee an efficient trip and insurance. The choice of a protocol adjusted for an application of rakes without wires depends on the level of commitment between energy efficiency and flexibility of communication. In contrast of the others we sensory furniture, the vehicles supplies, electric power sufficiently raised, a communication system generally, therefore, the energy consumption, is a secondary factor.

The procedure of admittance to the part MAC is most significant for miscellaneous applications of the rakes without flex. As in all mesh that shares the method of show, etiquette MAC is essential for the achievement of the process of the mesh. The occupation most significant of the etiquette is to stop collisions. Varied obtainable protocols MAC for nets lacking flex endure. However, these protocols hold applied boundaries when to the rakes lacking flex.

The S-MAC looks to be capable in force plummeting (dropping at high speed) the expenditure of the major guilty actions for the vigour carelessness:

- **Collisions**: To choose the crash crisis the S-MAC uses a chat of announcement RTS-CTS-DATAACK for the custody of physical haulier and NAV for custody of practical transporter. This conversation of statement prevents collisions and trouble of hidden fatal In holder that collision occurs, it uses an algorithm to stay a chance point, the BEB.
- **Overhearing**: it snoops to transmissions of moves intended to others lump. The S-MAC separates the radio of the loop when verifying that the image not intended for it.
- **Idle listening**: the knot listening the way of communication unerringly when travel in the arrangement does not exist. The S-MAC uses a cycle of operation with fixed times of doings listen and rest sleep. The commotion point is minor who the rest time (about 10%).

The signalling for the harmonization and direct movies is finished indoors of the canal, having sent a package SYNC in broadcast for all its neighbours. The S-MAC applies the practice of communication passing to reduce the latency throughout the containment in applications that necessitate storeroom of in sequence for processing in the networks (in-network). This technique allows the broadcast of extended mail that are alienated in minute fragments and envoy in gust. This protocol gets considerable decrease of the vigour expenditure, draws out the instance of life of the net.

1.6 Various Attacks in VANET

- **Denial of Overhaul Assault:** This assault is said to contain occurred when the attacker takes control of a vehicles resources or hinders the communication channel used by the Network, this prevents important information from arriving. It also increases the problem for the driver, if it has to depend on the network information.
- **Message Suppression Attack**: An attacker selectively drops few packets from the network, dropped packets may hold important information for the receiver, and the attacker suppresses these attacks. The motive of such an attacker is not to allow registration and insurance authorities to know about collisions involving his vehicle and/or to prevent delivery of collision reports to roadside units.
- **Fabrication Attack**: This attack occurs when attacker transits false information into the network, the information could be corrupted or the transmitter could hide its original identity. This attack includes, warnings, fabricate messages , Identities ,certificates,
- **Alteration Attack:** This attack is said to occur when attacker changes an existing data. It has many forms like delaying the transmission of the data, replaying previous transmission, or changing the actual data transmitted.
- **Replay Attack**: This attack is said to have occurred when an attacker replays the earlier transmission.
- **Sybil Attack**: Sybil attack is the attack where an attacker creates a large number of false names, and behaves like it is more than a hundred vehicles, to show other vehicles that there is congestion or jam ahead, and thus forcing them to take alternate route.
- **Eavesdropping**: It is a very prominent attack against VANETs confidentiality. In this attack attackers can be in form of a vehicle (stopped or moving) or in form of a false RSU. Their aim is to get unauthorized access to confidential information. As confidentiality is must in group communications, techniques should be established to grip such scenarios.

1.7 Security Services in VANET

Security is an important topic for VANET'S. To ensure a secure network, one needs to consider the following attributes

to measure security:

- **Availability**: The availability copes with the network services for all nodes and includes bandwidth and connectivity. In order to solve the availability problem, prevention as well as detection techniques involving group signatures scheme have been introduced. The scheme focuses on the availability of exchange of messages between vehicles and RSUs. When any attack leads network unavailability, the proposed method still prevails due to interconnection using private and public keys between RSUs and vehicles.
- **Confidentiality**: These techniques provide the confidentiality in the communication. The most popular technique "false names" are used toward defend solitude in VANETS. Each node is given multiple key pairs along with encryption. Messages are encrypted using various pseudo and these pseudo have no link to the vehicle node but relevant authority concerned to it. Vehicle needs to obtain new pseudo from RSU before the previous pseudo expires.
- **Authentication**: Authentication is the checking of identity between vehicles and RSUs and the validation of data during the information exchange. Civic or confidential keys with CA are planned to found connection between the nodes and password is used to access the RSUs and AS in authentication method.
- **Integrity**: Data integrity is the guarantee that the data received by nodes is the same as the data which has been generated during the exchange of messages. To protect the reliability of the message, digital signature which is incorporated with password access is used.
- **Non-Repudiation**: It states that sending and receiving the message cannot disagree with ever sending and receiving the message such as accident messages. In some fields, non-repudiation is referred to as audit ability where nodes can prove of message being receive and sent respectively.

2. RELATED WORK

Maria Elsa Mathew et. al (2013) discussed that value-added applications such as online payment services, geographical location identification, etc. in VANET, improve driving safety, passenger comfort, offer great business opportunities, and attract more and more attention in our daily life. VANETs connect vehicles into a huge mobile ad hoc network to share information on a larger scale. By enabling the vehicles to communicate with their neighbors and sharing their driving states, VANETs avoid accidents potentially caused by emergency braking, lane changing, etc. The characteristics of VANET pose both challenges and opportunities in achieving security goals. The various attacks in VANETs are the Sybil attack, DDOS attack, misbehaving and faulty nodes, sinkhole attack, spoofing, traffic analysis attack, position attack, and illusion attack. Providing security to VANET is important in terms of providing user anonymity, authentication, integrity, and privacy of data. In the paper, a comprehensive survey on the threats and vulnerabilities in VANETs are explored and analyzed in detail. The compromised security goals are identified for each threat. The existing solutions for these threats are also discussed in the paper.

Vinh Hoa LA et. al (2014) presents a survey of VANETs attacks and solutions in carefully considering other similar works as well as updating new attacks and categorizing them into different classes. Vehicular Ad hoc Networks (VANETs) have emerged recently as one of the most attractive topics for researchers and automotive industries due to their tremendous potential to improve traffic safety, efficiency and other added services. However, VANETs are themselves vulnerable against attacks that can directly lead to the corruption of networks and then possibly provoke big losses of time, money, and even lives.

Y.Bevish Jinila et. al (2014) Authentication of safety messages in Vehicular Ad hoc Networks (VANET) plays a major role. The time taken for signature generation and verification should be very less, to provide a secure and comfortable transportation to the public. Several signature generation and verification schemes are proposed in the literatures. The author focuses on the usage of Cha Cheon's ID based signature scheme for authentication in vehicular networks. Experimental analysis shows that this signature scheme incurs less signature size, less delay and less overhead in transmission when compared to the existing schemes.

Parul Tyagi et. al (2014) presented a paper and figured out and explained various types of security complications and objections of VANET .VANET has turned into an effective area of research, standardization and advancement, because it has impressive potential to raise vehicle and road safety, welfare, as well as convenience to both drivers and passengers and traffic adaptability. A lot of VANET Research work has been centered on particular areas including broadcasting, routing, surveillance and quality of service. The security benchmarks of vehicular Ad hoc network are examined here. Due to the unguarded nature of the VANET system routing protocols, such networks are also unsafe from the malicious mobile nodes in the structure itself. Hence the fundamental objective of vehicular ad hoc networks (VANETs), i.e., safe transmission of the time critical data, is possible only if a sturdy framework provides this insurance at all times. In this paper, various security protocols for vehicular ad hoc networks and achievement of mechanisms are discussed to give security.

Prakash Tripathi et. al (2014) Emerging Vehicular Ad-hoc Networks have the potential to improve the safety, traffic efficiency and as well as comfort to both drivers and passengers of highways. In the last three decades, various kinds of improvements are made in Wireless Ad-hoc Network and now a day's one of the most attractive research topic is Vehicular Ad-hoc Network (VANET) and become the most relevant form of Mobile Ad-hoc Networks. In the paper author

addresses the Security in Vehicular ad-hoc Network. threats are devised. The author provides a set of security protocols to protect the privacy and analyze the robustness and efficiency. In the paper a security architecture for vehicle communication is proposed. The architecture contains symmetric and asymmetric cryptography mechanism in the vehicular distributed environment for dissemination of information securely and efficiently.

Vivek Chand Dubey et. al (2015) surveyed that there are some possible attacks in the VANET like Sybil attack, Wormhole attack, Sinkhole attack etc and tried to show the effect of different attacks. The author discussed that it is very important to implement Intelligent Transportation System (ITS). There is some security issues and attacks which are associated with the VANET due to its dynamic nature, like changing topology, lack of infrastructure etc. The author aimed to detect and avoid the attacks and enhance the security.

Rohini Avinash Nere et. al(2015) shortly studied real time examples of vanet. There are huge number of accidents that happens at the intersection. Motive of the authors is to prevent accidents at intersection by introducing Intersection RSU in the system. Author has discussed simulators results for the same.

3. PROPOSED WORK

In Sybil attack, the attacker tries to harm the system of a peer-to-peer network by creating a huge number of identities, and using them to create a disproportionately large control. A system's exposure to a Sybil attack depends on how inexpensively identities can be created, the amount to which system accepts inputs from nodes that do not have a chain of trust linking them to a trusted node, and whether the system treats all nodes identically. Studies show that large-scale Sybil attack can be carried out very easily and efficiently.

Network has been denoted as a graph G consisting of vertices (V) and edges (E). There are honest nodes in the network, each with one identity, denoted as a h node in V. There are also one or more compromised nodes in the network, each with a more than one of Sybil identities. Each Sybil node is also donated in V. A relationship between two identities in the network is represented as an edge connecting the two nodes in G. The edges in G are undirected. We name the edge between a Sybil node and an honest node an attack edge.

The algorithm of the procedure is as follows

Step 1: initialize J = {h}
Step 2: for i = 1 to f, do
Step 3:Perform a random walk with length l = logn originating from h
Step 4: J = J ∪ {the ending node of the random walk}
Step 5: end for loop
Step 6: l = lmin
Step 7: while l <= lmax do
Step 8: for i = J.first() to J.last() do
Step 9: Perform R random walks with length l originating from node i
Step 10: Get ni as the number of nodes with frequency no smaller than t
Step 11: end for
Step 12: output hl,mean({ni : i ∈ J}),stdDeviation({ni : i ∈ J})i
Step 13: l = l + 100
Step14: end while
Step 15: while l <= lmax do
Step 16: Perform R random walks with length l originating from u
Step 17: m = the number of nodes whose frequency is no smaller than t
Step 18: Let the tuple corresponding to length l in the outputs of Algorithm 1 be hl, mean, stdDeviation
Step 19: if mean − m > stdDeviation ∗ α then
Step 20: output u is sybil
Step 21: end the algorithm
Step 22: end if
Step 23: l = l ∗ 2
Step 23: end while
Step 24: output u is honest
Step 25: exit

4. SIMULATION RESULTS

In this particular part we will observe the Performance of GPSR Protocol on ns2.34 simulator. A network of 150 nodes is deployed in an area of 1500m*1500m. The main Parameters are described in Table 1.

TABLE 1: SIMULATION PARAMETERS

Parameter	Value
Channel type	Wireless channel
Number of nodes	25
Area (deployment)	1000*1000 M
Max packet in interface queue	50
MAC type	802.11

Antenna model	Omni Direction Antenna
Propagation model	free space/two-ray ground
Queue type	Priority queue
Simulation time	100 S
Routing protocol	AODV
X Dimension	1186
Y Dimension	584

We will compare the existing GPSR protocol with the improved or enhanced GPSR protocol using our proposed technique. From comparative analysis it is clearly shown that by implementing our proposed technique, there is significant improvement in the results as shown in table below.

TABLE 2: PERFORMANCE METRICS

Protocol	Number of nodes	Number of packets sent	Number of packets received	Number of packets dropped	Packet delivery ratio
Gpsr	50	78	36	42	46.15%
Gpsr	100	82	42	40	51.21%
Proposed	25	1242	1234	8	99.35%

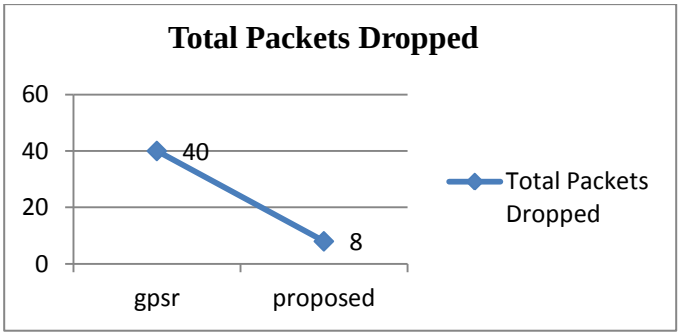

Figure 4.1 Total Packets Dropped

The above Figure 4.1 depicts the graphical view of comparing of total packets dropped in Existing GPSR and Enhanced GPSR.

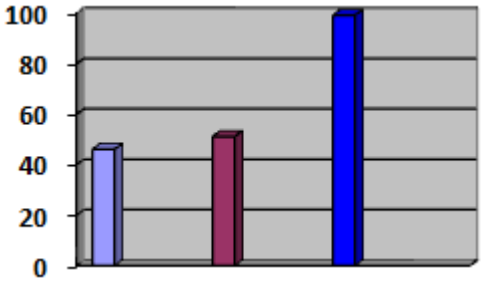

Figure 4.2 Packet Delivery Ratios

The above figure 4.2 shows the graphical analysis of comparing the packet delivery ratio in Existing GPSR and Enhanced GPSR. First bar shows 50 nodes, second bar shows 100 nodes and third bar shows enhanced GPSR. As the protocol will perform better when the value of packet delivery ratio is more and in above graph the PDR value is more as compared to existing.

5. CONCLUSION AND FUTURE SCOPE

The Performance of Vehicular Ad-Hoc Network is enhanced by the proposed algorithm in terms of increasing packet delivery ratio and decreasing the total packets dropped during the execution. The proposed algorithm has shown a significant increase in packet delivery ratio as compared to original GPSR protocol. The calculation of work is done in NS2 and the simulation results indicated that the proposed mechanism has superior performance and provide a significant increase in terms of PDR and decrease in Packets dropped. In future, the work can be extended to improve the lifetime of network by improving the Average Delay and other metrics in the proposed system and by improving packet delivery ratio without any much delay

.

REFERENCES

[1] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, "Security Analysis of Vehicular Ad Hoc Networks (VANET)", International Conference on Network Applications, Protocols and Service,2010

[2] José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda, "Overview of security issues in Vehicular Ad-hoc Networks",2010

[3] Mushtak Y. Gadkari, Nitin B. Sambre," VANET: Routing Protocols, Security Issues and Simulation Tools", IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 3, Issue 3 (July-Aug. 2012), PP 28-38

[4] Ankita Agrawal, Aditi Garg, Niharika Chaudhiri, Shivanshu Gupta, Devesh Pandey, Tumpa Roy,"Security on Vehicular Ad Hoc Networks (VANET) : A Review Paper", International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013)

[5] Maria Elsa Mathew and Arun Raj Kumar P,"Threat Analysis and Defence Mechanisms in VANET", International Journal of Advanced Research in Computer Science and Software Engineering,ISSN: 2277 128X, Volume 3, Issue 1, January 2013

[6] Vinh Hoa LA, Ana Cavalli,"Security Attacks And Solutions In Vehicular Ad Hoc Networks: A Survey", International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014

[7] Y.Bevish Jinila K. Komathy,"An Efficient Authentication Scheme for Vanet Using Cha Cheon's ID Based Signatures", Research papers computer science,Volume : 4,Issue : 6, June 2014 ,ISSN - 2249-555X

[8] Parul Tyagi, Deepak Dembla,"A Taxonomy of Security Attacks and Issues in Vehicular Ad-Hoc Networks (VANETs)",International Journal of Computer Applications (0975 – 8887) Volume 91 – No.7, April 2014

[9] Prakash Tripathi, Dr. Kanojia Sindhuben Babulal, "Security In Vehicular Ad-Hoc Network", International Journal Of Scientific & Technology Research Volume 3, Issue 11, November 2014,ISSN 2277-8616

[10] Rashmi Raiya, Shubham Gandhi, "Survey of Various Security Techniques in VANET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, June 2014, ISSN: 2277 128X

[11] Vivek Chand Dubey, Vinod Kumar ,"Survey: Secure Routing in VANET", International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015), Vol. 3, Issue 1, Jan – Mar 2015

[12] Rohini Avinash Nere, Prof. Uma Nagaraj , "Intersection RSU in VANET", International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 3, Issue 3, March 2015