Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.285 – 295

VPROOF: Enforcing Lightweight Privacy Preserving Vehicle Location Proofs

Ms. Sonea.K[1], Dr. SaravanaSelvam.N [2], Mr. Gowtham.A.R[3]
[1]PG Scholar,Department of CSE,SECE,Coimbatore & Anna university, India
[2]HOD,Department of CSE,SECE,Coimbatore & Anna university, India
[3]Senior Systems Executive,Cognizant Technology Solutions, Coimbatore, India
[1] sonea1210@gmail.com; [2] saravanaselvam.n@sece.ac.in; [3] gowtham.ar@cognizant.com

Abstract— In past few years VANET have received increased attention as the potential technology to enhance active and protective shelter on the road, as well as travel ease. Vehicular Ad-hoc Networks (VANET) applications rely on accurate location information. Generally, attacks cause anomalies to the network functionality. A secure VANET system, while swapping information should guard the system in opposition to unauthorized message injection, message alteration, eavesdropping. To overcome these issues, we present location based security mechanisms specifically designed for VANET. Proposed mechanisms for location range from the use of on-board radar devices and GPS with help of cellular networks to simple methods that depend on information grouping. We also address ways to enhance the availability of location information by selecting and sustaining constant routing paths. Finally, we confer a mechanism that promotes location confidentiality through encryption/decryption of PKI method and access control using geographical information. It identifies the packet drop occurred by the unauthorized vehicles with fake information's. By tracing the network information frequently and sharing in order to improve the security to vehicles in the VANET. The stimulation results show that the proposed mechanism has obtains higher performance in terms of throughput, packet delivery ratio, energy consumption and packets drop than the existing system. However, proposed proactive routing protocol has increased the accuracy and scalability.

Keywords— Vehicular Ad-hoc Networks (VANET), On-Board radar devices GPS, Cellular Network, Public Key Infrastructure and location security mechanism.

I. INTRODUCTION

Vehicular ad hoc network (VANET) can offer various services and benefits to VANET users and thus deserves deployment effort. VANETs with interconnected vehicles and numerous services promise superb integration of digital infrastructure into many aspects of our lives, from vehicle-to-vehicle, roadside devices, base stations, traffic lights, and so forth. A network of a huge number of mobile and high-speed vehicles through wireless communication connections has become electronically and technically feasible and been developed for extending traditional traffic controls to brand new traffic services that offer large traffic-related applications. Safety information exchange enables life-critical applications, such as the alerting functionality during intersection traversing and lane merging, and thus plays a key role in VANET applications. The attractive features of VANETs inevitably incur higher risks if such networks do not take security into an account prior to deployment. For instance, if the safety messages are modified, discarded, or delayed either intentionally or due to hardware malfunctioning, serious consequences such as injuries and even deaths may occur. Unlike

traditionally wired networks are protected by several lines of defense such as firewalls and gateways, security attacks on such wireless networks may come from any direction and target all nodes.Basically,Vehicular ad hoc networks (VANETs), is a subset of Mobile Ad hoc Networks (MANETs), in which vehicles provide communication services among one another or with Road Side Infrastructure (RSU) based on wireless Local Area Network (LAN) technologies.

Therefore, VANETs are susceptible to intruders ranging from passive eavesdropping to active spamming, tampering, and interfering due to the absence of basic infrastructure and centralized administration. Moreover, the main challenge facing vehicular ad hoc networks is user privacy. Whenever vehicular nodes attempt to access some services from roadside infrastructure nodes, they want to maintain the necessary privacy without being tracked down for whoever they are, wherever they are and whatever they are doing. It is considered as one of the important security requirements that should be paid more attention for secure VANET schemes, especially in privacy-vital environment. A number of security threats to vehicular ad hoc networks have been addressed. Ray et al. introduced three kinds of security threats in VANETs, including attacks on safety-related applications, attacks on payment-based applications, and attacks on privacy.

The primary application of a VANET is to allow vehicles to send safety messages that contain various information like vehicle speed, turning direction of vehicle, traffic accident information etc. to other nearby vehicles. It is denoted as vehicle-vehicle or V2V communications and it also send the information to RSU. It is denoted as vehicle-infrastructure or V2I communications. This information send on regular basis so that other vehicles may adjust their traveling routes and RSUs may inform the traffic control center to adjust traffic lights for avoiding possible traffic congestion. The main benefits of VANETs are that they enhance road safety and vehicle security while protecting drivers' privacy from various attacks such as DoS, Sybil, Alteration etc. Security is one of the most critical issues related to VANETs since the information transmitted is distributed in an open access environment.

II. WORKING OF VEHICULAR NETWORKS

Vehicular Networks System consists of large number of nodes (for e.g. vehicles).Here, each vehicle can communicate with other vehicle using short radio signals DSRC (5.9 GHz), within 1 KM range area. The communication between each vehicle is an Ad Hoc communication that means each connected node can move freely, there is no any wires required, the routers used is called cellular networks on-board GPS and transceiver, it works as a router between the vehicles on the road and connected to other network devices. Typically, in a VANET each vehicle is assumed to have an onboard unit (OBU) and there are GPRS that are installed along the roads. A trusted authority (TA) and application servers are installed in the back end. The onboard unit and roadside units communicate with each other by using the Dedicated Short Range Communications (DSRC) protocol over the wireless channel while the on board GPS, TA, and the application servers communicate using a secure fixed network (Internet). In Vehicular Networks System each vehicle has OBU (on board unit), that is connected to the vehicle with GPS via DSRC radios, and another device is TPD (Tamper Proof Device).Tamper Proof Device (TPD) holds the vehicle secrets, that is all the information about the vehicle like keys, drivers identity, trip details of that vehicle, speed of the vehicle, route.

We present validation mechanisms to provide location proof in VANET. In our approach, we use network cells as security as well as communication units. Providing location integrity is thus split into intra-cell integrity and intercell integrity. Intra-cell integrity consists of three mechanisms. First, we assume that all vehicles are endowed with an on-board radar device, a GPS unit and a standard transceiver with connected to cellular networks. To ensure intra-cell position information integrity, we propose an active validation mechanism (called active location integrity) which relies on the help of on-board radar to detect neighbouring vehicles and to confirm their alleged coordinates. Since radar is not currently installed in all vehicles, we propose a second mechanism (called passive location integrity) which relies on information fusion to filter out malicious data and refine low-resolution location information into high-resolution location information. Mindful of the fact that some of the vehicles participating in the traffic may not have any of these devices, we propose a third validation method (called general location integrity) which combines the active and passive location integrity mechanisms. Since VANET applications often need position information of vehicles that belong to different cells, we address inter-cell position information integrity as well. Vehicles request that their neighbors or vehicles in oncoming traffic check the alleged position information of remote vehicles. Both the request and response messages are propagated among cells. The availability of location information is also important in VANET. Because of the high mobility of vehicles, routing paths are often fragile and prone to disconnection. This results in situations where vehicles in different cells may not be able to communicate with each other.

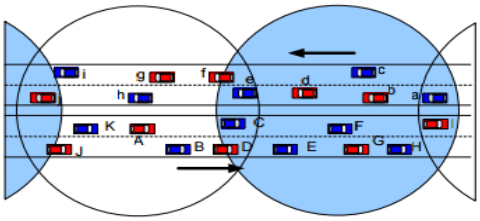

Fig.1 Cellular Networks

We propose a secure light weight scheme that selects and maintains stable routing paths based on a better understanding of the probability distribution of car-to-car communication links under realistic traffic and radio propagation assumptions. Given the insecure nature of wireless communication, we propose VProof, which is a lightweight and privacypreserving location proof solution that verifies if a vehicle's location claims match its historical locations.we propose both encryption/decryption and access control mechanisms to provide location VProof. Often position information from multiple vehicles is aggregated to reduce the number of messages that are sent. In our approach, the aggregated position message is encrypted using a key based on a geographic location that specifies the decryption region under cellular network. Vehicles have to be physically present in the decryption region to decrypt and access the aggregated position information using PKI. We design an efficient algorithm that can reliably determineif two series of packet RSS are similar given potentialpacket losses and inaccurate RSS measurements. The on board GPS based cellular networks is mentioned above is illustrated in Figure 1. By ensuring position information confidentiality, integrity, and availability, we achieve position information security that is compliant with the security requirements outlined in the Confidentiality, Integrity, and Availability information security model.

III. MOTIVATION WORK

A number of works have been done on the area of ad hoc network security especially for detection of attacks by malicious nodes in vehicular ad hoc networks. This section mentions some of these works.

Ho et al. obtained a multi-hop path using the help of structured mobility (e.g., bus systems). However, these schemes are empirical and cannot determine, with any degree of accuracy, the duration of links or the probability of the existence of communication links. Further, these models consider only a few parameters such as radio signal strength or distance between sender and receiver, while ignoring important mobility and radio propagation parameters. In contrast, we assume that the inter-car headway distance (i.e., the instantaneous gap between consecutive vehicles) obeys a log-normal distribution. Using this assumption and a classic radio propagation model, we derive the probability and the mean duration of a link.

Dousse et alproves that the probability of end-to-end connectivity decreases with distance, for one-dimensional network topologies. This implies that it now becomes much easier for a malicious attacker to partition the network. This effect can potentially be addressed by maintaining multiple forwarding nodes for each packet. Hence, if we only have one or a few malicious nodes, the rest of them could potentially maintain the node reliability. However, a synchronized attack by multiple compromised vehicles would be disastrous. This, together with the unreliability of single vehicles, is ideal for applying even simple attacks.

Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhangsays that Vehicular networks have attracted extensive attentions in recent years for their promises in improving safety and enabling other value-added services. Security and privacy are two integrated issues in the deployment of vehicular net-works. Privacy-preserving authentication is a key technique in addressing these two issues. They proposed a random key-set based authentication protocol that preserves user privacy under the zero-trust policy, in which no central authority is trusted with the user privacy However, the attacker has only a limited number of keys.In particular, the application cannot find a signature/nonce combination with the same cryptographic hash value.

K.Sampigethaya et al proposed architecture as Context-Aware Architecture for VANET. Vehicular ad hoc networks (VANET), it is possible to locate and track a vehicle based on its transmissions, during communication with other vehicles or the road-side infrastructure. This type of tracking leads to threats on the location privacy of the vehicle's user. They also studied the problem of providing location privacy in VANET by allowing vehicles to prevent tracking of their broadcast communications. They first, identify the unique characteristics of VANET that must be considered when designing suitable location privacy solutions. Based on these observations, They proposed a location privacy scheme called CARAVAN, and evaluate the privacy enhancement achieved under some existing standard constraints of VANET applications, and in the presence of a global adversary.

J. Freudiger, M. Raya, M. Flegyhzi, P. Papadimitratos, and J.-P. Hubaux, says that Vehicular Networks (VNs) seek to provide, among other applications, safer driving conditions. To do so, vehicles need to periodically broadcast safety messages providing precise position information to nearby vehicles. However, this frequent messaging (e.g., every 100 to 300ms per car) greatly facilitates the tracking of vehicles, as it suffices to eavesdrop the wireless medium. As a result, the driver's privacy is at stake. In order to mitigate this threat, while complying with the safety requirements of VNs, we suggest the creation of mix-zones at appropriate places of the Vehicular Networks. The results show that, although the unlink ability of individual mixzones can be relatively low in some cases, the accumulated unlink ability of the mix-networks is generally very high.

XiaodongLin ,Xiaoting Sun et alsays that first identify some unique design requirements in the aspects of security and privacy preservation for communications between different communication devices in vehicular *ad hoc* networks. Then they proposed a secure and privacy-preserving protocol based on group signature and identity (ID)-based signature techniques. They demonstrate that the proposed protocol cannot only guarantee the requirements of security and privacy but can also provide the desired traceability of each vehicle in the case where the ID of the message sender has to be revealed by the authority for any dispute event. Extensive simulation is conducted to verify the efficiency, effectiveness, and applicability of the proposed protocol in various application scenarios under different road systems. However, some proposed group signature schemes are questionable in the security and anonymity assurance. For instance, many ID-based group signature schemes, such as failed to meet the unlink ability requirement.

Chenxi Zhang et.alintroduce a novel roadside unit(RSU)-aided message authentication scheme named RAISE, which makes RSUs responsible for verifying the authenticity of messages sent from vehicles and for notifying the results back to vehicles. In addition, RAISE adopts thenanonymity property for preserving user privacy, where a message cannot be associated with a common vehicle. In the case of the absence of an RSU, they further propose a supplementary scheme, where vehicles would cooperatively work to probabilistically verify only a small percentage of these message signatures based on their own computing capacity. Extensive simulations are conducted to validate the proposed scheme. The RAISE scheme has many advantages because of its lower computation and communication overhead. RAISE also protects the vehicles privacy by adopting the k-anonymity approach. It is demonstrated that RAISE yields a much better performance than previously reported counterparts in terms of message loss ratio (LR) and delay.

R.VijayaKarthika, P.R.Gomathisays, Vehicular ad hoc networks (VANETs) enable vehicles to communicate with each other but require efficient and robust routing protocols for their success. In this proposed system, we exploit the infrastructure of Road Side units (RSUs) to efficiently and reliably route packets in VANETs. This system operates by using vehicles to carry and forward messages from a source vehicle to carry and forward messages from a source vehicle to a nearby RSU and, if needed, route these messages through the RSU network and, finally send them from an RSU to the destination vehicle. simulation results in shows that DSDV fails to converge if nodes don't pause for at least 300 seconds during movement; the packet delivery ratio is in the range of 70%-92% at higher rate of mobility; packet loss is mainly caused by stale routing entries; in periodic updates transmission, routing overhead is constant with respect to the mobility rate; nearly optimal path can be selected in routing procedure.

Jing Zhao, Guohong Cao says,Multi-hop data delivery through vehicular ad hoc networks is complicated by the fact that vehicular networks are highly mobile and frequently disconnected. To address this issue, we adopt the idea of carry and forward, where a moving vehicle carries the packet until a new vehicle moves into its vicinity and forwards the packet. Different from existing carry and forward solutions, we make use of the predicable vehicle mobility, which is limited by the traffic pattern and the road layout. Based on the existing traffic pattern, a vehicle can find the next road to forward the packet to reduce the delay. The proposed vehicle-assisted data delivery (VADD) is based on the idea of carry and forward. Different from existing carry and forwarding approaches to make use of the predicable mobility, which is limited by the traffic pattern and road layout.

IV. RELATED WORK

Vehicular ad hocnetwork(VANET) have been proven to be a better network structure to implement the vehicle environment scenario. We will use some routing protocols in NS2 for data transfer reliably. So that in order that adhoc on demand distance vector(AODV) is used in this system to improve their performance. Ad hoc on demand distance vector routing (AODV) is the combination of DSDV and DSR. In AODV, each node maintains one routing table. Each routing table entry contains Active neighbor list a list of neighbor nodes that are actively using this route entry. Once the link in the entry is broken, neighbor nodes in this list will be informed. However, the disadvantages are that AODV only accepts bi-directional link and has much delay when it initiates a route and repairs the broken link.

They have proposed accurate algorithm is developed to detect the malicious packet drop. Here detection accuracy is very high which is achieved by finding the correlation of lost packets which is obtained by using the bitmap of packet reception provided by each node. By finding correlation between lost packets we can find whether packet loss is only because of link error or is the effect of combination of both link error and malicious packet drop because both correlations gives different patterns for packet loss. To reduce the computation overhead of the baseline scheme, a packet-block-based mechanism is also proposed, which allows one to trade detection accuracy for lower computation complexity. Through extensive simulations, they verified that the proposed mechanisms achieve significantly better detection accuracy than conventional methods such as a maximum-likelihood based detection. Even though they obtain the highest accuracy in detecting the attackers but they fail to prevent the data from the attackers during the data transmission.

The major limitation in the existing methods, attacks cause anomalies to the network functionality. A lot of previous studies have investigated security vulnerabilities of routing protocols for wireless networks. Also, there are attacks in which malicious nodes advertise fake locations to their neighbor nodes. Malicious attackers may damage the network by announcing fake node locations. Such attacks are even more difficult to mitigate.In existing system leads to higher energy consumption, due to the open nature of wireless medium, a packet drop in the network could be caused by harsh channel conditions by the insider attacker. It provides lesser accuracy in detecting the attackers in vehicular ad hoc networks.

The main objective of this research is to improve the lightweight privacy of a vehicle to avoid fake information and also to improve in terms of overhead, transmission delay, energy conversion and increasing throughput, transmission delay, energy, and reliability. So, in the proposed system an innovative technique is in ITS data collection applications, vehicles sense and collect data about surrounding elements by their add-on vehicle sensors. The sensed data were generated, are uploaded to backend servers located at the infrastructure side, either immediately after they are generated or sometime later when appropriate. The ITS systems operate vehicular networks that enable wireless communication between vehicle and the infrastructure via cellular network. They assume that cellular network are controlled by the ITS operator, and all vehicles are equipped with GPS receivers with cellular towers. They consider the threat that malicious users target at disrupting ITS systems by reporting fake information about numerous places where they did not actually visit. If there is no scheme to allow ITS operators to verify whether the reporting users have actually visited the places indicated in the reported data, a malicious user can easily generate and report bogus data about lots of places without actually visiting those places. The amount of the bogus data could overcome that of the honest data we observe that the RSS of a series of packets received by a vehicle when it passes an cellular network, which is continuously broadcasting packets with fixed power, exhibit similar patterns over time. In the experiments, we deployed a wireless node, which broadcast packets at a rate of 100 packets/s with full transmission power at the roadside of a downtown environment. We drove a car past the roadside wireless node and collected its packets at different times. DSDV has one routing table; each entry in the table contains destination address, number of hops toward destination, next hop address. Routing table contains all the destinations that one node can communicate. When a source A communicates with a destination B, it looks up routing table for the entry which contains *destination* address as B. Next hop address C was taken from that entry. A then sends its packets to C and asks C to forward to B. C and other intermediate nodes will work in a similar way until the packets reach B. DSDV marks each entry by sequence number to distinguish between old and new route for preventing loop, it is demonstrated in Fig.3. DSDV use two types of packet to transfer routing information: full dump and incremental packet. The first time two DSDV nodes meet, they exchange all of their available routing information in full dump packet. From that time, they only use incremental packets to notice about change in the routing table to reduce the packet size. Every node in DSDV has to send update routing information periodically. When two routes are discovered, route with larger sequence number will be chosen. If two routes have the same sequence number, route with smaller hop count to destination will be chosen. DSDV has advantages of simple routing table format, simple routing operation and guarantee loop-freedom. Generally, cellular networkcontinuously broadcast packets that are specifically for the location. Each VPacket is broadcast using a randomly chosen transmission power. Since the transmission power is randomly selected, the RSS of the VPackets received by vehicles exhibit no pattern. Each VPacket includes certain encrypted information that contains the transmission power of the packet.

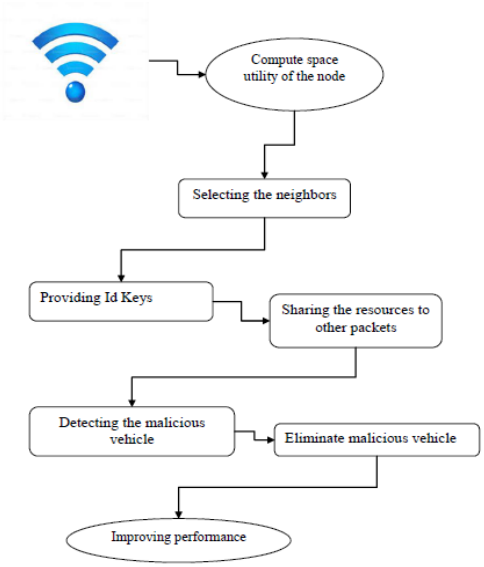

Fig .2 Architecture Diagram

V. SYSTEM ARCHITECTURE

The initially the network is configured with calling the Node configure function with number of nodes. And then Link create will create link, while creating link we need to specify the levels with which the node is associated. Once the network is configured we take up server as the destination and any of the nodes as the sender. Once the network is set we browse for the file we need to send. In the source we split the entire file in to number of packets these packets will be encrypted and Add bit function will help in adding bits to identify the change in number of packets and packet will be forwarded further.

Fig. 3 System architecture

5.1 SYSTEM MODULES

The proposed system contains four modules.

1. Creation of nodes
2. Selection of Qualified neighbors and key generation
3. Authentication Message Verification
4. Fake information detection

5.1.1CREATION OF NODES

An undirected graph G (V, E) where the set of vertices V represent the mobile nodes in the network and E represents set of edges in the graph which represents the physical or logical links between the mobile nodes. Sensor nodes are placed at a same level. Two nodes that can communicate directly with each other are connected by an edge in the graph.

Let N denote a network of m mobile nodes, $N_1, N_2, \ldots\ldots, N_m$ and let D denote a collection of n data items D_1, $D_2, \ldots\ldots, D_n$ distributed in the network. For each pair of mobile nodes N_i and N_j, let t_{ij} denote the delay of transmitting a data item of unit-size between these two nodes.

5.1.2SELECTION OF QUALIFIED NEIGHBORS AND KEY GENERATION

In Distance Vector Routing algorithm, an intermediate node assigns the highest priority to the packet with the closest deadline and forwards the packet with the highest priority first. *Cp*← *SEsUi* ,*t*(*p*). We design an algorithm to allow an cellular network Ci to randomly select a transmission power p from L options: Pf, P1, . . . , PL−1, with Pf being the full power and P1, . , PL−1 being the other L − 1 none full power levels. The algorithm ensures that the cellular network would broadcast VPackets using the same power for a period of time that is larger than coherence time Tolerance. The details of the algorithm are s. After the transmission power p is determined, Ci encrypts p a symmetric-key algorithm SE, with the combination of sCi and time t (i.e., the time when the VPacket is generated) as the cryptographic key RSS instability, we want users to receive n VPackets within a period of coherence time, which is the time duration over which the RSS is considered to be not varying. Then, we can take the average of these n VPackets' RSS as data point in the RSS series VPacket RSS traces in cellular network. In our design, there are N be RSS traces associated with each possible vehicle trajectory around each RSU Ui. Each RSS trace contains an RSS series of VPackets collected by driving a car past Ci on the trajectory. If the location proofs are constructed based on authentic VPackets, an cellular networkCi generates a VPacket authentication Message (VAM) for each VPacket as

VAM ← *H* (*Ci*, *sCi*, *t*, *Cp*)

Square root of (x2-x1)^2+(y2-y1)^2

Where x and y is a node positions

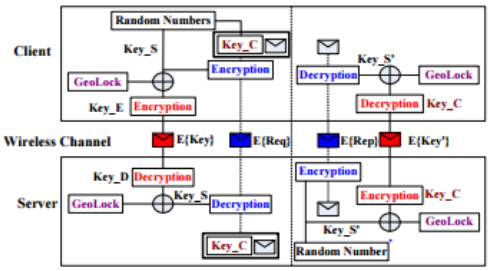

Fig.4 Key Generation and Verification

5.1.3AUTHENTICATION MESSAGE VERIFICATION

The ITS operator verifies the VAM contained in each location proof as follows. ITS computes the message content by using with the parameters Ci t, Cp,andsCi , where Ci, t, and Cp are extracted from the location proof, and sCi is kept by the operator. If the computed content is different from the VAM contained in the location proof,VAM is deemed invalid. An invalid VAM indicates that atleast one parameter of Ci, t, and Cp provided in the location proof has been tampered with. If there exists one location proof containing invalid VAM, the whole batch of location proofs is invalid. Note that a batch of location proofs with valid VAMs does not necessarily mean that the batch of location proofs is valid, because a malicious user can statically collect VPackets, obtain valid VAMs, and present them in the location proofs.

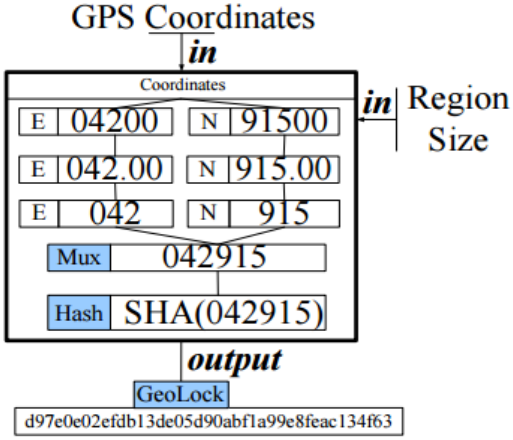

Fig.5 Location based message verification

5.1.4FAKE INFORMATION DETECTION

The vehicular wireless node runs a program that constructs location proofs when VPackets arrive. To study whether hardware differences at the user side have impacts on our scheme, we have used two different wireless 29 cards on the vehicular wireless node, Users can choose to upload the data anytime they feel appropriate, for example, when the uploads will not contend with other important tasks. Our choice of letting the backend server process the location proofs offline conforms to the reality AP is able to change the transmission power for each packet. This per-packet power control is achieved by specifying the desired transmission power in the packet's radiotap structure. With the per-packet transmission power control, it is possible to change VPacket's transmission power randomly while not affecting the normal tasks done by the cellular networks.

5.2PERFORMANCE ANALYSIS

The NS2 tool is used to study the performance of ourVPROOF: Enforcing Lightweight Privacy Preserving Vehicle Location Proof. We employ the IEEE 802.11 MAC with a channel data rate of 11 Mb/s. We compare with the normal existing architecture with proposed architecture in order to prove that proposed simulation results are better in energy consumption as well as provide secure routing path for source to destination.
The coherence time of the wireless channel at each of the experiment locations as Specific, we let the cellular network broadcast small packets (100 bytes/packet) at a very high packet rate (500 packets/s). Then, we measured the RSS differences between different sizes of VPacket windows based on which we determined the coherence time of the channel. We found that the coherence times at our experiment locations were around 100 ms. Thus, in our experiments, we set the VPacket rate to 100 frames/s, To restore the inherent RSS pattern from the RSS of VPackets broadcast using random transmission power levels, our solution relies on the fact that the difference of RSS at the same location between two VPackets that are transmitted by the same cellular network using two different power levels is roughly a constant across the entire communication, of the cellular network. We conducted an experiment to quantify how stable this RSS difference is. In the experiment, we let the roadside wireless AP change between two transmission power levels periodically while broadcasting the VPackets. In the first half of a coherence time period, the VPackets were transmitted using full power, and in the second half, the VPacket transmission power was set to half the full power. The VPacket rate was 100 frames/s.

*5.2.1 Performance Metrics***:** The metrics used to evaluate performance of proposed approach:

a) Throughput: It is defined as the total number of packets received by the destination node andtotal number of packets originated by source node with respectively time period.

b) Delay: This is defined as the average time taken for a packet to be transmitted from the source to the destination.

c)Average energy consumption: It is defined as the average energy required to send the packet and to receive the packet.

d) Packet Delivery Ratio (PDR): It is defined as the total number of packets received by the destination node andtotal number of packets originated by source node

A graph is plotted between time and packet size to study the delay in the proposed system and is shown in Fig. 7.Average energy consumption, Fig.8. packet delivery ratio and Fig 9.packet delay. Theresult shows that VPROOF: Enforcing Lightweight Privacy Preserving Vehicle Location Proofsperformances is better for the detection of malicious node and secure routing path for data transmission.

Parameter	Value
Application Traffic	10 CBR
Transmission rate	4 packets/s
Packet Size	512 bytes
Channel data rate	11 Mbps
Area	700m*700m
Simulation time	800

Table I. Stimulation parameters

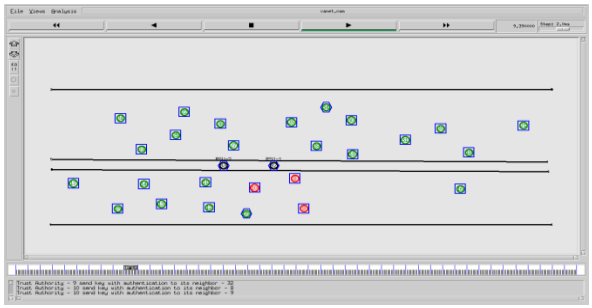

Fig.6 Proposed scheme with cellular network

5.3SIMULATION RESULTS

We used the performance metrics to validate the proposed algorithm with results obtained in this papers are shown in Figure 7 and figure 9.

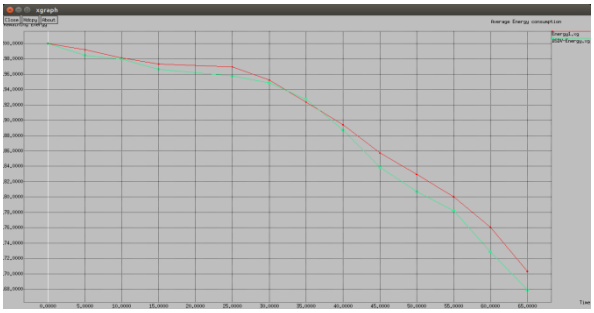

Fig. 7 Average energy Consumption

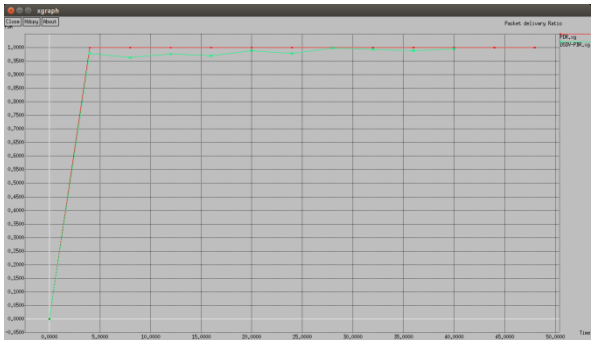

Fig. 8 Packet delivery ratio

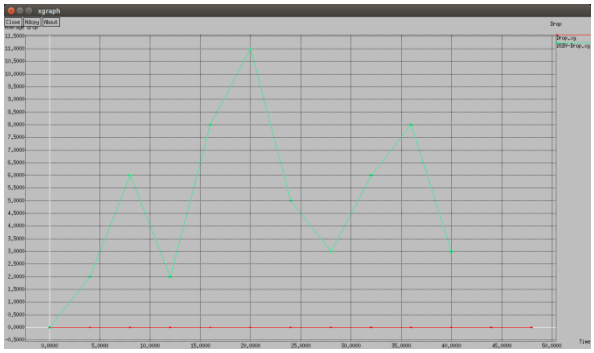

Fig. 9 Packet Delay

Thus the proposed scheme is very significant and effective when comparing with existing methods.

VI. CONCLUSION

In the proposed method, we implement another important routing protocol of NS2 AODV-ADHOC ONDEMAND DISTANCE VECTOR for increase the throughput and fast accessing to find out the reliable path vehicle. Byanalyzing the existing system using graphical representation of important parameter like, delay, drop, throughput, packet delivery ratio and average energy conversion and proving that our future work has successfully improved of the above performances and also find each vehicles individual shortest route to reach required destination by using GPS with the help of cellular networks. Road side unit will be easily hacked as they are not monitored. So we plan to introduce as other device as cellular tower. Thus the result obtained is minimum energy consumption and found unauthorized node by using cellular tower. Thus the future work of the project can be selection of different protocols.

ACKNOWLEDGEMENT

I am thankful to Dr.N.SaravanaSelvam Head Of The Department for his guidance, support and supervision. And also for providing the information and ready to help any time in completion of this paper.

REFERENCES

[1] XiaodongLin,Xiaoting Sun, Pin-Han Ho, **"**GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications**",** IEEE TRANSAs, VOL. 56, NO. 6, NOVEMBER 2007.

[2] Chenxi Zhang, Xiaodong Lin, Rongxing Lu, "An Efficient Message Authentication Scheme for Vehicular Communications", IEEE TRANSAs, VOL. 57, NO. 6, NOVEMBER 2008.

[3] JulienFreudiger, Maxim Raya, **"**Mix-Zones for Location Privacy in Vehicular Networks", vol. 4,pp. 398-415, 2006.

[4] Feeney.L, Cetin.B, Hollos.D, Kubisch.M, Mengesha.S, "Ontheanalysis of the predecessor attack on anonymity systems",in IEEE 802.11WLANS," Proc. Fifth Int'l Conf. Wired/Wireless Internet Comm., 2007.

[5] S.Djahel, J.Murphy "A Comparative Study of Vehicles Routing Algorithms for Route Planning in Smart Cities", in proc. IEEE, vol 20- 20 Nov. 2012.

[6] J. Zhao and G. Cao, "VADD: Vehicle-assisted data delivery invehicularad hoc networks," in *Proc. IEEE INFOCOM*, Barcelona, Spain, Apr. 2006, pp. 1–12.

[7] Liao.H, Tseng.Y.C, and Shih.K.P, "Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks", Proc. IEEE Int'l Conf. Comm., 2002.

[8] Liu.C and Layland.J, "Proving Your Location without Giving up Your Privacy",J. ACM, vol. 20, pp. 46- 61, 1973.

[9] R.Vijayakarthika, P.R.Gomathi "A Cost Effective RSU Placement Strategy for Secured Communication in Vanet", in proc. ICSECSRE, Vol.3,Special Issue 3, April2014. 43

[10] Lu.C, Blum.B, Abdelzaher.T, Stankovic.J, and T. He, "CARAVAN: Providing Location Privacy for VANET",Proc. IEEE Real-Time and Embedded Technology Applications Systems, 2002.

[11] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao. Towards event source unobservability with minimum network traffic in sensor networks. In ACM WiSec, 2008.

[12] S. Saroiu and A. Wolman.Enabling new mobile applications with location proofs. In Proceedings of the 10th workshop on Mobile Computing Systems and Applications, page 3. ACM, 2009.

[13] EmmanouilMagkos Cryptographic Approaches forPrivacy Preservation in Location-Based Services

[14] M. Talasila, R. Curtmola, and C. Borcea. Link: Location verification through immediate neighbors knowledge.

[15] In P. S´enac, M. Ott, and A. Seneviratne, editors, Mobile and Ubiquitous Systems: Computing, Networking, and Services, volume 73 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pages 210–223. Springer Berlin Heidelberg, 2012.

[16] B. Gedik and L. Liu. A customizable k-anonymity model for protecting location privacy. In IEEE ICDCS, 2005

[17] J. Manweiler, R. Scudellari, Z. Cancio, and L.P. Cox. We saw each other on the subway: secure, anonymous proximity-based missed connections. In ACM HotMobile, 2009.

[18] J. Manweiler, R. Scudellari, and L.P. Cox. SMILE: Encounter-based trust for mobile social services. In ACM CCS, 2009.

[19] Dr.SaravanaSelvam.N Ms.Sonea.K Mr.Gowtham.A.R "A Survey on Various Protocols and Security Techniques in VANET" International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.20 (2015)

[20] F.J. Massey Jr. The Kolmogorov-Smirnov test for goodness of fit.Journal of the American Statistical Association, 46(253):68–78, 19.

