Third Party Based Security Method in Vehicular Ad-Hoc Networks

Dinesh Arora, Hardeep Singh Saini, Harbinder Singh

Abstract: Security is the key factor of consideration in the vehicular ad-hoc network (VANET), which is prone to various security dangers. A VANET package gives information on life's essentials and provides security from detrimental external agencies. This paper presents an outsider-based security approach which secures VANETs condition by verification process, where marks are produced and conveyed to hubs and checked at the measure of any transmission. In the suggested approach, the rise in mobility decreases the packet delivery ratio and performance of proposed protocol is approximately 4% improved as compared to other techniques. Moreover, the escalation in mobility increases the average delay and in case proposed protocol is compared with the group based authentication then the improvement in its performance is approximately 50%.Thus, the proposed approach is completely focused on security and consequently secures the system.

Index Terms**: *Ad-hoc network, end to end delay, nodes, packet delivery ratio (PDR), security, VANETs security*****.**

I. INTRODUCTION

Highlight With the quick progression and inescapable arrangement of data and remote correspondence advances, vehicular ad- hoc networks (VANETs) are required to be created soon. A VANET comprises of on board units (OBUs) which are embedded in vehicles serving as mobile nodes and road side units (RSUs). It functions as the information infrastructure located at critical points of the road. VANETs have different potential applications. The primary purpose behind this kind of systems is applications identified with activity security. By providing further data about conceivable clashes, most life-imperiling mischance can be turned away. VANETs likewise encourage movement advancement. Without a doubt, vehicles can gather information about car influx, climate or street surface conditions, development zones, and highway or rail convergences, and so on, and move toward becoming data sources by conveying that information to different vehicles in the VANET. These components empower transportation organization experts to direct vehicles and oversee them electronically (e.g. grants, speed control, etc.), which are extra productive than a customary manual organization. Further to safety related applications VANET also provides value-added services [1 -3].

For those new services to make life less demanding instead of more troublesome, they ought to depend on secure and protection saving conventions that urge clients to take an interest without fear for their well-being or individual security. Thus, security and protection are two basic worries for the designers of VANETs and if overlooked, might prompt the organization of powerless VANETs. Unless legitimate steps are taken, various assaults could without much of a stretch be directed, to be a specific message content change, false information generation, identity theft and propagation and so forth. The cases of some particular attacks are:

- If message respectability is not ensured, a vindictive vehicle could alter the substance of a message sent by another vehicle to influence the conduct of different vehicles. Thus, the malevolent vehicle could acquire lots of advantage while keeping its character obscure. Furthermore, the vehicle that primarily created the message would become in charge of the harm caused.
- If validation is not given, a vindictive vehicle may imitate a crisis vehicle to outperform speed limits without being authorized.
- A false emergency situation could be reported by a malicious vehicle which needs to be checked. In case, it is overlooked, it could be sanctioned.
-

From the past cases, it is noticeably clear that message verification, uprightness, and non-disavowal are essential necessities in VANETs [4]. VANET needs certain system for security, certain methodology and strategies to figure out the genuine sender of the message or whether or not the message has been distorted or changed by the assailant.

VANET is thought to be an extraordinary sort of versatile, specially appointed system with particular attributes [5 - 8]. VANET is an accumulation of remote hubs that can be progressively set up any place and whenever without utilizing any previous system framework [9]. There are some uncommon qualities exhibited in VANETs which are exemptions to general MANETs. These are recorded beneath: - VANETs are conceivably expansive scale systems [10].

Revised Manuscript Received on June 15, 2019.

Dinesh Arora, Department of Electronics & Communication Engineering , Chandigarh Engineering College Landran , Mohali , India.

Hardeep Singh Saini, Department of Electronics & Communication Engineering , Indoglobal College of Engineering & technology Abhipur, Mohali,India.

Harbinder Singh, Department of Electronics & Communication Engineering , Chandigarh Engineering College Landran , Mohali, India.

There are a huge number of vehicles on the streets in many nations [11]. Since each vehicle should be enrolled on the system, there are an extensive number of portable hubs that will be a part of the system. - Road design, activity laws, and speed constraints on streets influence the portability of vehicles [10].

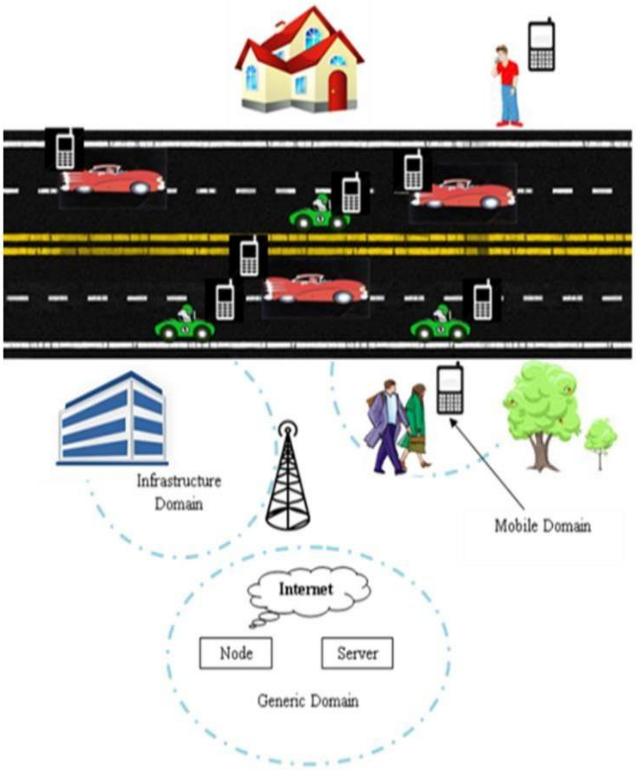
The versatility of vehicles is dependent on the driver's behavior and his interpersonal communication with other drivers. It is a complex job to simulate the vehicle traffic involving applications in transportation engineering. Vehicles provide more resources like batteries, antennas and processing power than typical mobile devices [10]. Thus, preserving these assets in VANETs is not a noteworthy concern. In VANETs, hubs are vehicles which move as per limited portability design in view of many factors, for example, street course, incorporating activity and activity controls [12].

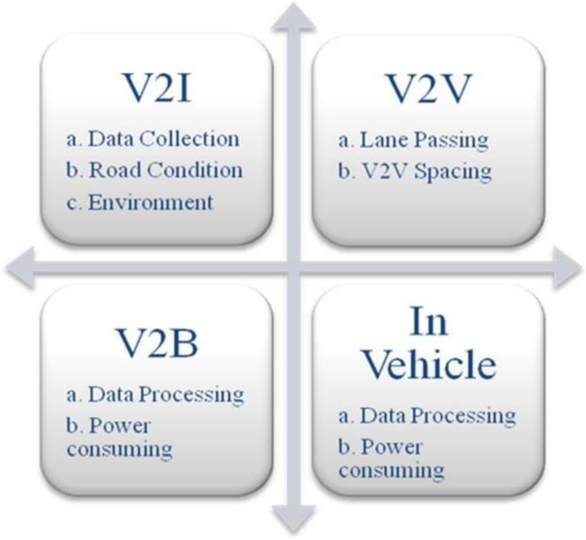
VANET supports correspondences among vehicles by means of inter-vehicle communication (IVC) and among vehicles and fixed RSU equipment through roadside-to-vehicle communication (RVC). RSUs can be conveyed at basic areas, for example, tricky streets, benefit stations, unsafe crossing points or places surely understood for dangerous climate conditions [13]. All things considered, capricious and conflicting relative hub speed may cause discontinuous connection breakages. Besides, a hub in VANETs can be outfitted with a global positioning system (GPS) to effortlessly decide its own area. A standout amongst essential perspectives that decide the achievement of VANET is the dependable message steering from a sourcing hub to a goal hub [9].

II. ARCHITECTURE OF VANET

VANETs architecture is divided into three different domains, namely as (i) Infrastructure domain (ii) Generic domain (iii) Mobile domain. Figure 1 explains the architecture of VANETs. The mobile reign consists of vehicle domain and mobile device domain where vehicle domain contains all types of vehicles and mobile devices contain portable devices [11].

VANETs architecture can also be categorized into four types based on its communication. Figure 2 illustrates the functions of communication types in VANETs. There are four different types of communication-based categories. These are 'In vehicle communication', vehicle to infrastructure (V2I), vehicle to vehicle (V2V) and vehicle to the broadband cloud (V2B). The correspondence system in a vehicle identifies a vehicle's operability and most importantly the driver's fatigue and indifference which are needed for open security. Information-sharing is possible as the data exchange gives an opportunity for the V2V correspondence enabling the drivers to share information and forewarning messages, keeping in mind the end goal to develop the driver help [14]. V2I correspondence engages progressing action/atmosphere revives for drivers and gives characteristic distinguishing and watching. V2B correspondence suggests that vehicles may grant by methods for remote broadband parts, for instance, 3G/4G. As the broadband cloud may consolidate greater development information and watching data and what is more infotainment, this sort of communication will be useful for dynamic driver help and vehicle following.





"Fig. 2. Functions of communication types in VANETs"

III. SECURITY REQUIREMENT IN VANETS

Securing VANET framework must have the capacity to choose errand drivers while maintaining their protection. For example, data about vehicles and their drivers must be secured to guarantee the notwithstanding working of shrewd transportation frameworks. This to a great degree dynamic circumstance set apart by the routinely prompt landing of brief period association lengths, vehicles, and flight, the arrangement of a total security arrangement has been not kidding to façade restriction and particular setups. VANET well-being ought to be a remarkable worry in conventional systems. The crucial security responsibilities, including accessibility, trustworthiness and secrecy are as a matter of first importance association with life well-being. Basic data can't be erased or adjusted by an aggressor [15]. The security-call attention to the message ought to trade safely about the vehicles and their relating drivers.

Before the VANET is conveyed, it ought to fulfill a couple of necessities. A VANET security framework fulfills the accompanying necessities as shown in the Table 1.

“Table 1. Security Requirements”

Requirement	Explanation
Authentication	It ensures that the certified client made the message. In VANET, a vehicle reacts as per data got from alternative vehicles, which fulfil the confirmation
Data verification	To wipe out the false informing, a consistent confirmation of information is required. The message likewise includes their consistency with comparable ones on the grounds that the sender can be true blue, while the message contains the false information
Non-Repudiation	It clarifies that a vehicle can't dismiss the client which does not communicate the message. It may be a basic to finish up the Correct arrangement of crash remaking.
Real time constraints	The most noteworthy paces are run of the mill type in VANET; there ought to be a strict time confinement which regards the Security components.
Data Correlation	The vehicle will make an outcome in the level of consistency and respectability of the data got by utilizing information connection conspire which gathers Information got from different sources.
Availability	It affirms that data ought to be accessible to the bona fide client. Assaults ought to Close down the system so that the data can't be shared.
Secure positioning	There ought to be a genuine necessity to secure position confirmation. As a result of it, vehicle or base-station should affirm and ascertain the position of other Vehicles or base- stations.

A. EXISTING SECURITY MECHANISMS IN VANETS

Security Using Digital Certification: This strategy gives the secure correspondence between vehicles using propelled supports. The transmissions are completed in three stages. The primary correspondence is intervened between a base station (BS) and RSU [16]. BS needs to offer a presentation to RSU in this system. Each vehicle or car is to be enrolled with RSU in the second stage and utilizes the inflexible and open key of the vehicle and eventually RSU sends the demonstration of the car. The vehicle-to-vehicle correspondence is invoked in the third stage and relating vehicles transmit their supports to each other. In this tradition the time multifaceted nature is, θ (10) and moreover it’s economical, in light of the fact that the tradition uses check, statement, and opens key 7.

Position-Based Routing Security: In position-based steering, security is given by utilizing directing message insurance component and hub assessment system. In directing message, insurance component messages are encrypted thus enabling security and it utilizes advanced mark. The mark engulfs the area data of the source, goal, and information [17]. The hub assessment instrument entwines the utilization in three stages. In the initial step, it confirms the mark of the sending hub. After the subsequent stage records, the following bounce advances the packages. In the final stage, the reverse assessment is incorporated and it is the other way around of forwarding assessment.

Preventing Hole Generation Attack*:* This component is utilized to keep the gap era assault and upgrades the directing way in three phases. The stages consist of gap location, data broadcasting and data security. In the starting, identification organizes the vehicle pronounces the limits and it is self-allotted as a limit hub [18]. This hub sends packages to next limit hubs. This procedure proceeds until an opening is reached to and this way is characterized as a gap in the system. The opening data is communicated to every single other vehicle in the second stage and in the third stage is utilized to produce secure directing way. The directing way is developed utilizing MFR conventions until a gap is found in the system. On the off chance that the opening is achieved and it incorporates two operations among which the first is secure module and the other one is recuperation module. Secure is utilized to locate the authentic hub and the recuperation module is utilized to recoup the pernicious hub from aggressors. This convention is utilized to recoup the gap era assault just, it doesn't recuperate different assaults.

MAC Security*:* RSU helped message confirmation conspire gives security safeguarding by asking for RSU for impermanent ID. Transitory ID is also signified as the pseudo ID, which is put away in RSU, is legitimate as long as the vehicle is in that specific scope of RSU. A private key using ECDSA signature and transitory ID is employed by vehicles to send message. The beneficiary vehicle inquiries RSU for the open key of the sender vehicle [19]. When the check sender vehicle conveys the validated message, RSU.

Communicates open key of the sender vehicle. Vehicular hub name-lessly collaborates with different hubs, so that data regarding the client is entirely unknown. Thus, it manifests genuine ID from pseudo ID and checks it by open key affirmation technique

Group-Based Authentication: This system is for the most part utilized for applications such as the conglomeration of military troops and it consists of three different stages. In the introduction stage, the source is verified utilizing TESLA. The reinstatement stage is separated into three phases which includes the sender setup; amass enrollment confirmation, and communication associated with bootstrapping parameters [20]. In sender setup, sender secures the package utilizing a one-way hash chain and relegates the bundles as indicated by the time interim. In gathering participation validation, assemble individuals are allocated with a gathering id and gathering testament. These gathering ids and gathering declaration are composed utilizing MD5 calculation. Bootstrapping transmits the packages utilizing different parameters, for example, current time interim, bundle encryption interim, predefined key, and confer keys. The second stage is an intra bunch correspondence. It is separated into sender operation, recipient operation and gathering participation refresh. In this correspondence sender sends the bundles to gathering individuals and the package is encoded utilizing a conferred key [21]. The beneficiary gets the bundles and the information package is decoded utilizing the submitted key. In gathering enrollment refresh the server produces another keychain and multicasts it to gathering individuals so the gathering individuals are confirmed occasionally with new keychain [22]. The third stage is intergroup correspondence and is partitioned into sender operation and recipient operation. The packages are transmitted to non-amass recipients during the sender operation. The validation key is marked by harsh work and is acquirable only to the collectors. As the different constraints of security are fulfilled the recipients get an information bundle [23].

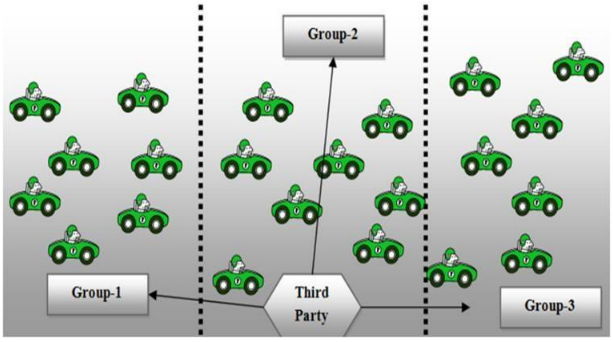
IV. PROPOSED THIRD PARTY BASED SECURITY APPROACH

In this work, a third party based security approach has been proposed with group based authentication mechanism. In this network is divided into different groups and each group has one head that assigns a signature or security key to all the nodes present in their group [24]. Group head gets digital certificates from the third party and then generates a key using that certificate.

A. Simulation Setup and Analysis

For simulation network of 100 nodes is generated. These nodes are spread over the 1600x1000 area with fixed mobility. The simulation setup for the scenario is as given in Table 2. The step wise methodology of the proposed approach given as:

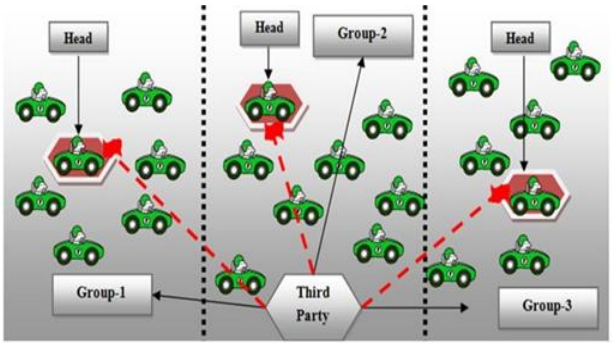
Step 1: The first step of the simulation is to generate network scenario. In this scenario, 100 nodes are generated



in the area of 1600x1000. In this, one node is treated as the third party and other nodes are divided into 3 groups. These 3 groups are generated using range based clustering where network area is subdivided into 3 sub-networks each of 533x1000 as shown in figure 3[25].

Step 2: In the next step, a third party is used here for security purposes. The third party generates digital certificates and distributes it to all the heads where heads will generate their group signature using this certificate. This signature will be used for authentication purposes when communication between the nodes will take place. Figure 4 represents the Group Head Selection.

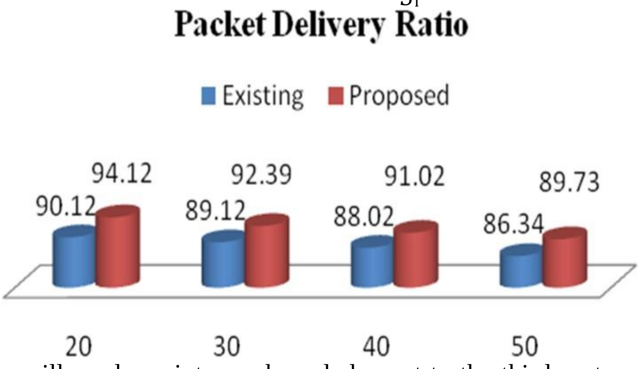
"Fig. 3. Node distribution in groups"



"Fig 4. Group head selection"

Step 3: After receiving authentication keys, nodes will send receipt or acknowledgment to the third party that key has been received. So that authenticated nodes are verified by the third party.

S_i



Step 4: In this scenario, the user will enter source and destination node address it means nodes are selected which he wants to connect for data sharing. In this work, source node firstly sends the request message for establishing connection between two nodes. Both nodes establish a connection only if they were authenticated nodes of the network.

Step 5: When destination receives the request, it waits till default waiting time and replies through authenticated nodes of network.

Step 6: When the source node receives reply packet then it will send its data packet. The data packets are also encrypted before transmitting at the source side. Destination decrypts these data packets using the signature [26].

"Table 2. Simulation Setup"

Parameter	Value
Area	1600 x 1000
Number of Nodes	100
Mobility Model	Random Waypoint
Propagation Model	Two Ray Ground
Antenna Type	Omni Directional
Mobility (m/s)	20,30,40,50
Simulation Time (s)	100
Packet Size (B)	512
Traffic Type	CBR

B. Simulation Results

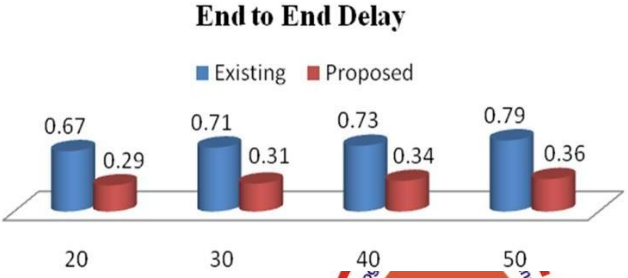
To analyze the performance of the proposed protocol perform -ance matrices, End to End Delay and Packet Delivery Ratio are considered.

Packet Delivery Ratio (PDR): It is referred to as the ratio of data packets actually received at the receiver end to those which were sent by the sender. So, it can also be defined as in equation (1):

$$PDR = R_i / \qquad (1)$$

Where S_i is the aggregate number of information bundles sent by the hubs in the system and though R_i is the aggregate number of information packages got by the collectors. The performance of the proposed protocol is measured by varying node mobility. Figure 5 shows that with the increase in mobility, the packet delivery ratio decreases, but if this proposed protocol is compared with the group based authentication, then the performance of proposed protocol is approximately 4% improved.

"**Fig 5**. Packet Delivery Ratio (PDR)"



“Fig 6. Average end to end delay”

End to End Delay: All the intricacies concerned with buffering during route discovery, latency, and retransmission by intermediate nodes result in delays such as the processing delay, and propagation delay. It is calculated as equation (2):

$$D_i = (Tr - Ts) \qquad (2)$$

In which T_r and T_s are the receiving time and sent time of the packet respectively. Figure 6 shows that with the increase in mobility, the average delay increases, but if this proposed protocol is compared with the group based authentication, then the performance of proposed protocol is approximately 50% improved.

V. CONCLUSION

The vehicular ad-hoc networks (VANETs) are presently vulnerable to numerous security dangers [24]. This paper presents a outsider based security approach which secures VANETs condition by verification process, where marks are produced and conveyed to hubs and checked at the measure of any transmission[25]. It is also concluded that the end to end postponement is likely less in contrast with other existing components. This work establishes that higher package conveyance proportion in contrast with the existing plan even with high portability approach reduces average delay. In the wake of encountering distinctive security procedures, it can be concluded that the proposed 'Outsider based security approach' is the best security arrangement. Thus, this system is completely focused on security and consequently secures the VANET system [26].

REFERENCES

1. Qin B, Wu Q, Domingo-Ferrer J, Susilo W. Robust distributed privacy-preserving secure aggregation in vehicular communication. Control and Cybernetics 2012;42 (2):.277-296.
2. Azogu IK, Ferreira MT, Larcom JA, Liu K. A new ati-jamming strategy for VANET metrics-directed security defence in conference proceedings. IEEE Globecom Workshops; 2013, Atlanta, GA, USA, pp.1344–1349.

   DOI: 10.1109/GLOCOMW.2013.6825181
3. Dhurander SK, Obaidat M, Jaiswal A, Tiwari A, Tyagi A. Vehicular security through reputation and plausibility checks. IEEE Systems Journal 2014;8 (2): 384-394.

   DOI. 10.1109/JSYST.2013.2245971
4. Petit J, Feiri M, Kargl F. Spoofed data detection in VANETs using dynamic thresholds”, IEEE Vehicular Networking ;2011, Amsterdam, Netherlands, pp. 25–32.

   DOI: 10.1109/VNC.2011.6117120
5. Chakroun O, Cherkaoul S. Overhead-free congestion control and data dissemination for 802.11p VANETs. Vehicular Communications 2014; 1 (3): 123–133.

   doi.org/10.1016/j.vehcom.2014.05.003
6. Pari NS, Jayapal S, Duraisamy S. A trust system in MANET with secure key authentication mechanism. Recent Trends Information Technology (ICRTIT);2012, IEEE. Chennai, Tamil Nadu, India, pp.261–265. DOI: 10.1109/ICRTIT.2012.6206818
7. Karger P, Frankel Y. Security and privacy threats to ITS. In Second World Congress on Intelligent Transport Systems 2014; 5: 2452 2458.
8. Raiya R, Gandhi S. Survey of various security techniques in VANET. International Journal of Advanced Research in Computer Science and Software Engineering 2014; 4 (6): 431-433.
9. Dadali AS, Joshi, R. Survey on VANET protocols and security techniques. International Journal of Science and Research 2015; 4 (6):1644-1648.
10. Ribagorda A, Gonzalez-Tablas AI., Ribagorda A. Overview of security issues in vehicular ad-hoc networks. Handbook of Research on Mobility and Computing ; 2010, IGI Global, Hershey, USA.
11. Becker M, Gupta A, Marot M, Singh H. Improving clustering techniques in wireless sensor networks using thinning process. Performance Evaluation of Computer and Communication Systems. Milestones and Future Challenges- Series Lecture Notes in Computer Science ; 2014, Springer, pp. 203-214
12. Bitam S, Mellouk A, Zeadally S. HyBR: A hybrid bio-inspired bee swarm routing protocol for safety applications in vehicular adhoc networks (VANETs). Journal of Systems Architecture 2013; 59 (10B): 953–957.

    doi.org/10.1016/j.sysarc.2013.04.004
13. Chen L, Ng SL, Wang G. Threshold anonymous announcement in VANETs. IEEE Journal on Selected Areas in Communications 2011; 29 (3): 605–615.

    DOI: 10.1109/JSAC.2011.110310
14. Bali RS, Kumar N, Rodrigues JJPC. Clustering in vehicular ad hoc networks: Taxonomy, challenges and solutions. Vehicular Communications 2014; 1(3):134-152.

    doi.org/10.1016/j.vehcom.2014.05.004
15. Katal A,Wazid M, Goudar RH. A cluster based detection and prevention mechanism against novel datagram chunk dropping attack
16. in MANET multimedia transmission. Information & Communication Technologies (ICT) ; 2013, IEEE. Thuckalay, Tamil Nadu, India, pp.479–484.

    DOI: 10.1109/CICT.2013.6558143 Verma K, Hasullah H, Saini HK. Reference broadcast synchronization-based prevention to DoS attacks in VANET. 7th IEEE International Conference on Contemporary Computing ; 2014, Noida, India, pp. 270–275.

    DOI: 10.1109/IC3.2014.6897185
17. Khabazian M, Aissa S, Mehmet-Ali M. Performance modelling of safety messages broadcast in vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems 2013; 14 (1): 380- 387. DOI: 10.1109/TITS.2012.2213595
18. Daeinabi A, Rahbar AG. An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks. Computers & Electrical Engineering. 2014 ; 40 (2) : 517–529.

    doi.org/10.1016/j.compeleceng.2013.10.003
19. Yujin L, Zhao M, Wang W. Internode mobility correlation for group detection and analysis in VANETs. IEEE Transactions on Vehicular Technology 2013; 62 (9):4590-4601.

    DOI: 10.1109/TVT.2013.2264689
20. Wang M, Shan MH, Lu R, Zhang R, Shen X, Bai F. Real-time path planning based on hybrid-VANET-enhanced transportation system. IEEE Transactions on Vehicular Technology 2015; 64 (5): 1664-1678.

    DOI: 10.1109/TVT.2014.2335201
21. Chim TW, Yiu SM, Hui LCK, Victor OKL. VSPN: VANET-based secure and privacy-preserving navigation. IEEE Transactions on Computers 2014; 63 (2): 510-524. DOI: 10.1109/TC.2012.188
22. Song C, Liu M, Gong HG, Chen GH, Cao JN. Utilizing the dropped packets for data delivery in VANETs. The Journal of China Universities of Posts and Telecommunications, Elsevier 2013; 20(3): 48–52. doi.org/10.1016/S1005-8885(13)60048-5
23. Kaur, A., Arora, D.: Survey over VANET routing protocols for vehicle communication. Int. J. Electr. Electron. Eng. **1**, 1–6 (2014)
24. Jain, P., Arora, D.: A

survey on link connectivity of networks. Int. J. of Engineering Applied Sciences and Technology, 2016 Vol. 1, Issue 10, ISSN No. 2455-2143, Pages 156-162 Published Online August - September 2016.

25. P. Jain and D. Arora, "Fuzzification based intravehicular communication in VANETs," 2017 International Conference on I- SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam,2017,pp.223-228.doi: 10.1109/I-SMAC.2017.8058344

.

AUTHORS PROFILE

Dr.Dinesh Arora obtained his Doctorate degree in Electronics & Communication Engineering in December 2012. His Area of Interest is Optical fiber and Wireless communication. .His total experience is 17 years & is presently working as Professor (ECE) in Chandigarh Engineering College (Mohali) PUNJAB (INDIA). He has published 64 papers in national/international journals & has guided 20 M.Tech. Students of K.U.K. & P.T.U. He is a life Member of The Institution of Electronics and telecommunication Engineers and is in the editorial board of various Journals like (IJEEE & IJCSIT etc.).He is a reviewer of International Journal for Light and Electron Optics (ELSEVIER).

Dr..Hardeep Singh Saini obtained his Doctorate degree in Electronics & Communication Engineering in 2012. He holds Master's degree in Electronics & Communication Engineering from Punjab Technical University, Jalandhar passed in 2007. His total experience is 18 years, presently working as Professor (ECE) at Indo Global College of Engineering, Abhipur (New Chandigarh), and PUNJAB (INDIA) since June-2007. His area of expertise includes optical communication. He is author of 6 books in the field of Electronics &Communication Engineering. He has presented 64 papers in international/national conferences and published 41 papers in international journals. He is a fellow and senior member of various prestigious societies like IETE (India), IEEE, IETI China, SCIEI USA and he is also editorial member of various international journals and conferences.

Harbinder Singh has done Ph.D. degree in Electronics and Communication Engineering at the Jaypee University of Information Technology, Waknaghat, India, received the M. Tech degree in Electronics and Communication Engineering from Punjab Technical University, Punjab, the B. Tech degree in Electronics and Communication Engineering from Himachal Pradesh University, Shimla and 3-year diploma in Electronics and Communication Engineering from Punjab State Board of Technical Education. He is the author or co-author of 24 papers published in national, international conferences and journals. He has few patents and book chapters to his credit. His current research interests include diatom analysis based on multifocus image fusion, exposure fusion, edge-preserving filters, high dynamic range imaging and tone mapping. He is currently working as Associate Professor, ECE, Chandigarh Engineering College Landran, Mohali, India