International Journal of Hybrid Information Technology
Vol.8, No.7 (2015), pp.335-344
http://dx.doi.org/10.14257/ijhit.2015.8.7.30

A Novel Approach Of Trust Based Routing To Select Trusted Location In AODV Based VANET: A Survey

Kumud Dixit, Krishna Kumar Joshi, Neelam Joshi

Dept. of Computer Science & Engg
Maharana Pratap College of Technology, Gwalior, India

dixit.kumud20@gmail.com, Krishnakjoshi@gmail.com,Neelam.khemariya@gmail.com

Abstract

During the last few years, a vehicular ad hoc network (VANETs) was extensively focused by researchers. A vehicular ad hoc network (VANETs) is a subclass of Mobile ad hoc networks builds to make sure the safety of traffic. VANET is a type of mobile peer to peer network, although it exhibits some different characters (fast moving, short lived connection etc). VANET is different from MANET due to large scale networks, higher mobility of nodes, geographically constrained topology and frequent network partitioning. In this paper, we present a survey on trust based routing in AODV based VANET to find secure location. In this first discussed about VANETs, their applications, characteristics, attacks, routing protocols and present a review of various researchers on trust based VANET.

Keywords: *VANET; Trust; RSU; TA ; AODV*

1. Introduction

Ad hoc networks are a collection of nodes which establishes a temporary network. There are nodes that communicate with them without any fixed infrastructure. A MANET(Mobile Ad hoc Network) is a self-organized wireless network composed of autonomous nodes that communicate with each other in order to forward the packet from one hop to other hop before it reaches to the required destination by using the routing protocol. VANET (Vehicular Ad hoc Network) is a subgroup of a MANET, where the communication nodes are vehicles and scattered on different roads [14-16].

As mobile wireless devices and networks become increasingly important, the demand for Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (VRC) or Vehicle-to-Infrastructure (V2I) Communication will continue to grow. In vehicular communication it provides secure driving environment, avoid traffic jams, provide accident information, hazards and weather information and decrease travel time. They exchange important safety and warning messages that can be reported ahead of any accident and road traffic congestion. It consists of vehicles (mobile nodes), RSUs (Road side units), TAs (Trusted authorities).Vehicular communication has a capability to exchange a local information in a near real time for enhancing safe driving and improving mobility of nodes. There are many characteristics of VANET like short lived connections, substantial computation power, high mobility, dynamic topology etc. Due to frequently changing topology between vehicles the security for routing protocols has been taken as a challenging task for researches .In VANET a malicious node can alter and diffuse fake messages in the network to cause collisions. There is a need to provide a trust mechanism between nodes to prevent fake messages sharing on VANET.

ISSN: 1738-9968 IJHIT

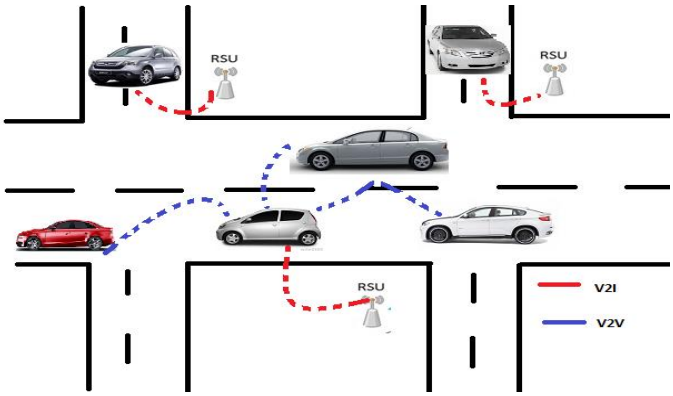

Figure 1. Types Of Communications In VANET

Many secure and trust based routing protocols have been implemented to ensure message integrity and compute the trust value of each message content. Trust model makes a relationship between all neighboring nodes and recommend trust degree. And it also identifies selfish and malicious nodes efficiently and solves the security problems of node failure [17].

2. Overview of Vanet

A. Intelligent Transportation System

Intelligent Transportation System (ITS)[1] is a system in which each vehicle works as a router to broadcast safety and control messages to the vehicular network and ensuring safe and secure driving environment. For obtaining communication between vehicles and RSU(Road Side unit),vehicles must be equipped with some kind of radio interface that forms a short range wireless Ad hoc networks and also fitted with GPS(Global positioning system) that provides a detailed position information of moving vehicle. RSUs must be in place to facilitate communication in the backbone network. The distribution and number of RSUs depend on the communication protocol used.In some protocols it should be distributed evenly throughout the road, some protocols require RSUs only at intervals, while some other protocol requires region wise.In Intelligent transportation system, there are three types of possible communication configurations, vehicle to vehicle, vehicle to roadside unit and routing based. These communications rely on updating information about whole network, which in turn requires the use of a smart communication protocol and positioning systems to exchange information.

B. Inter-vehicle (vehicle to vehicle) communication-

In Vehicle to vehicle communication (Figure 1) vehicle uses a multi hop multicast or broadcast messages to exchange, safety and control information related to traffic to a group of receiver. There are two types of messages i.e. naïve broadcasting and intelligent broadcasting. In naïve broadcasting vehicle exchange updated information at an interval to another vehicle. When message is received if it came from vehicle behind of it ignores the message otherwise it broadcast a message to the vehicle behind it. Intelligent broadcasting addresses an inherent problem of naïve broadcasting with limited messages broadcast for an emergency event. If a vehicle receives same message from behind, then it assumes that one vehicle behind has received this message and want to broadcast and also responsible for sending a message to rest of the vehicles [1,12].

Figure 2 . Vehicle To Vehicle Communication

C. Vehicle to Roadside communication

In vehicle to roadside unit communication (Figure 2) roadside unit (RSUs) uses single hop broadcast message to exchange information to all the vehicles over whole road in the region .In this communication RSUs are distributed over a whole road at every kilometer or less and provide high bandwidth link between RSUs and vehicles and maintain high data rates in heavy traffic. The road side unit periodically broadcast updated information about speed limit if any vehicle violates the desired limit, then warning message will be delivered to that vehicle to reduce his/her speed.

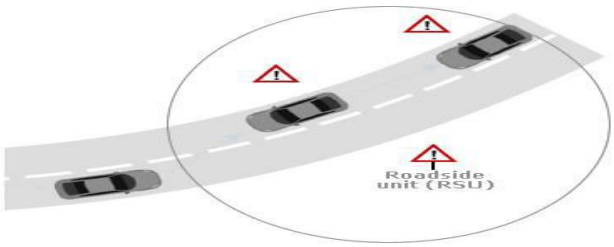

Figure 3. Vehicle To Roadside Communication

D. Routing –Based Communication

The routing-based communication configuration (Figure 3) uses a multi-hop unicast message to exchange information in multi-hop fashion until the vehicle carrying the desired data is received. When the request is received by a particular vehicle owning the desired piece of information, now that vehicle immediately unicast message including information on the vehicle it received the request from, which is then forwarded it towards the query source.

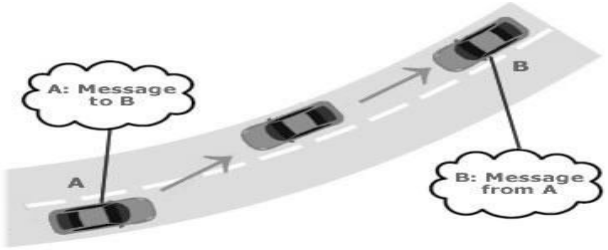

Figure 4. Routing-Based Communication

3. Vanet Applications

A. Safety Related Application

In VANET safety applications[2,13] are very important because it related to directly related to passengers and cars and provide safe and secure driving environment .There are various active safety applications which are based on the safety and control functions with the purpose to exchange status data and sensor information between inter-vehicle and vehicle to infrastructure communication .some example of active application are Antilock Brake system (ABS) and Electronic Stability Program (ESP).Some passive safety applications works inside the car and provide safety against accidents on the road .safety belts and air-begs are passive applications. But passive application cannot avoid accidents like active applications of VANET.

B. Efficiency Application

Efficiency applications are divided into two categories like traffic management and traffic monitoring information. Traffic management information contains intelligent traffic flow control, roadways planning and congested road notification. Traffic monitoring information includes notifications regarding road condition sensing, vehicles and fleet trafficking. These notifications are received by the vehicle, according to the requirement of the condition over the road.

C. Infotainment Application

These infotainment applications utilized to provide many services, except safety related services .It includes peer to peer applications which are used to provide services like sharing multimedia files to other vehicles in the network. It also provides services like internet connectivity all the times constantly to the users and other user based applications like payment services, to locate important destination points over the whole road in the network.

4. Characteristics of VANET

VANET [1] is a subgroup of MANET but it is having some of its own distinct features compare to MANET are as follows-

A. *Dynamic topology*-In VANET nodes are moving with a very high velocity so nodes are changing its positions rapidly.So network's topologies are changing frequently.

B. *High Mobility*-Vehicles are moving over the road with a very high speed so it is very difficult to predict the current position of any vehicle.

C. *Wireless communication*-In VANET all vehicles are connected through a wireless connection and exchanging information through wireless medium. So it's required to put some security measures in the communication.

D. *Real time critical*- Vehicles are moving over the road with a very high speed over the road on the network. So information is exchanged between vehicles in very short span of time and decision regarding to perform any action should be in real time.

E. *Sufficient energy*-There is not any issue regarding energy and resource in VANET because it provides an unlimited computation and transmission power.

F. *Unlimited network size*-VANET can execute over, one city many cities or over a whole country. So it has an unlimited network size.

G. *Good physical protection*-In VANET, nodes are very much protected against geographical attacks and having a better physical protection.

5. VANET Routing Protocol

In VANET vehicles can move rapidly from one place to another .So the path formed by a source may not exist after a short span of time if any intermediate node moves from one network to another. Routing [11] in VANET has been a very challenging task due to its very rapidly changing topology between nodes. The important characteristics of VANET are high mobility, sufficient energy resources, self organization, not an issue of restricted network sizes made this environment is very challenging for establishing an efficient routing protocol in VANET. There are basically routing protocols are categorized in three broad categories-

A. On Demand or Reactive Routing Protocol

In this protocol nodes find their routes only when they need. These protocols first initiate route discovery and roué maintenance. For discovery route it makes use of route request (rreq) and route reply (rrep).Some of the on demand routing protocols are DSR,AODV and TORA.

B. Table Driven or Proactive Routing Protocol

These protocols constantly maintain the network topology. In a network every node contains the information of the neighbors. Unlike on demand routing in this protocol, information about neighbors is stored in different tables and tables are updated periodically according to the changes in the network topologies. Some of the table driven routing protocols are DSDV, DBF, GSR, WRP and ZRP.

C. Hybrid Routing Protocol

The combination of proactive and reactive protocols is a Hybrid protocol. These protocols make use of distance-vector for more precise metrics to establish the best paths to destination networks. The hybrid routing protocol is ZRP.

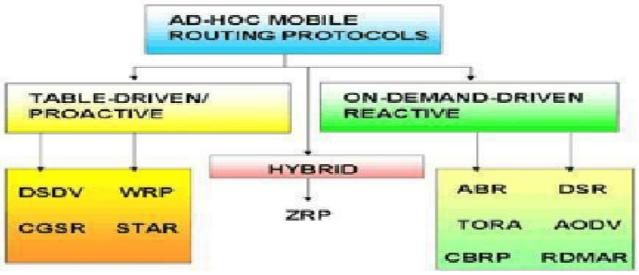

Figure 5. Vanet Routing Protocol

D. Reactive Routing Protocol-

AODV (Ad Hoc On Demand Distance Vector) Routing Protocol-

AODV is an ad-hoc on demand distance vector routing protocol that establishes a route to the destination when it is desired by the source node. It maintains this route as and when needed by the source node. It offers quick adaptation to dynamic link conditions, memory overhead, low processing, low network utilization, and determines routes to destinations over an ad hoc network. In order to communicate between the mobile nodes, Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV[11].

1) Route Discovery-

When any node in the network send a packet to the destination and that particular path does not find in its routing table [11] for the same destination, then that source will initiate route discovery process. Source now broadcast its RREQ (route request) packet to neighbors .In this technique source node searches the destination by a TTL (time to live) value. If any reply does not come in TTL time then it incremented by a value .It will be repeated continuously until the threshold value is reached .If any intermediate node forwards the RREQ ,so the address of the node from which first packet of the broadcast is received, thereby it establishes a reverse path. RREP is unicast to the route towards the source from which it came. In this way when the RREP reaches to the source node, a secure path is established between the source and destination node.

2) Route Maintenance –

Once a route is established between the source and destination node, then it is maintained by the source. But due highly dynamic topology in VANET If the source node moves away from its location, it can again initiate a route discovery for establishing a new route to a specified destination. If the destination and any intermediate node move, the node is entry removes from the routing table and sends a RRER message to that particular damaged upstream link. Now this link propagates this RRER message to the source node [11].

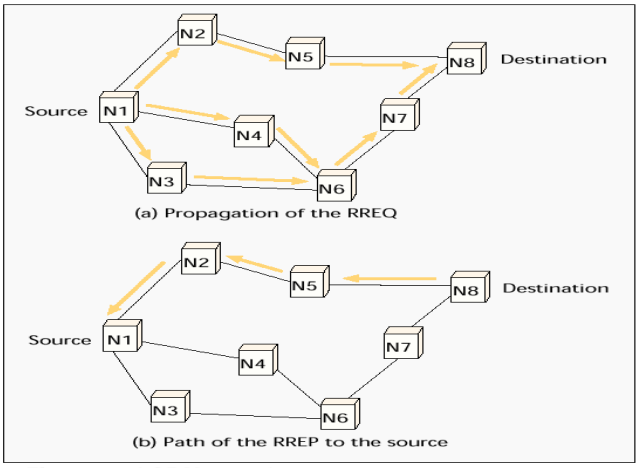

Figure 3. *AODV route discovery.*

Figure 6. AODV Route Discovery

6. Securitty Issues in VANET

Security got more attention in the recent years by researchers. VANET packets include life critical(real time critical) information. Hence it is very necessary to ensure that these packets are not modified and altered by an attacker; at the same time the liability of drivers should also be maintained in such a way that they can inform the traffic environment correctly and within the time [5]. These security problems do not similar to general Ad hoc networks. The size of network, mobility, geographic relevancy, etc. makes the implementation difficult and distinct from other network security.

Security Requirements in VANET

VANET must have some of the following security requirements before they established a communication. There are following security requirements[5]:

1. *Data confidentiality: It means to protest or hide information to the unauthorized users. It is the most important aspect of security, but it is the most which is attacked mostly. Cryptography and encryption are the techniques used to ensure confidentiality.*
2. *Integrity: It is to ensure that the data is secure and unchanged of the original information. This is required to eliminate message delay attacks.*
3. *Non-repudiation: It is to ensure that the one cannot deny the authentication of digital signature to the message or data it has sent or originated. It can be used to find the exact sequence in crash reconstruction.*
4. *Authentication: It should be guaranteed that a message is produced by an authorized user. In VANET message is verified at every vehicle came from another vehicle.*
5. *Availability: It is important to ensure that the data should be accessible to the authorized user at any time. Some types of attacks make the authorized users not to use the data.*

7. Attacks in the VANET

There are many types of attacks of which we must have knowledge about the attacks in VANET [5]. Attacks on different security requirement are as follows

A. *Impersonation*-In this type of active attack attacker take an identity and make an access of the privileges of an authorized user with the purpose to disrupt the normal operations of a network and use the resources which may not be utilized under normal functioning of the network. This type of multilayer attack can affect an application, network and transport layer. It can be of two types-
   a) Sybil attack-In this type of attack, an attacker assumes more than one different identities at the same time.
   b) False identity possession-In this type of attack attacker take some unique property of an authenticated user and after claims that he has sent a message. In VANET by using this attack any vehicle can assume that he is a fire protector and police to free the traffic and cause accidents.

B. *Location Tracking*-An attacker can trace the exact information about driver by analyzing location of a moment over the path followed by a period of time.

C. *Session Hijacking*-All the authentication process is done at the start of any session. So this type of attack hijack a whole session after connection is established between vehicles in VANET.

D. *Eavesdropping*-The main goal of this active attack to take an access of confidential data.

E. *Denial of services attack and flooding*-In this attack, an attacker restricts an authorized user to utilize services from targeted node. It can be achieved by different ways-
   a) SYN flooding-in this type of technique an attacker sends multiple SYN request to victim node so that it spoof the sender address .Now target node sends in rep ACK message to attacker node, but it could not get the a ACK REP in return from the attacker. So now there is only half open connection can be made so authorized users unable to use services from legitimate users.
   b) Jamming-in this mechanism attacker continuously analyses the traffic on the channel and its frequency at which receiving node receives a data. After that he starts to transmit data over the channel so that jam is occurring.
   c) Distributed DoS attack-This is kind of denial of service (Dos) attack in which many attacker nodes restrict the authorized user to utilize services from victim node [5].

F. *Repudiation*-In this type of attack two entities have same identities so it is very difficult to distinguish them.

Routing Attacks in VANET

Routing attacks [5] are those which are used to exploit network layer functionality. It either drops the packets during routing or disrupts the routing process in the network.

1) *Black-hole Attack* –This is an active attack [5] in which a malicious node waits for neighbor to send a route request (RREQ) message. When a malicious node receives a RREQ message from any neighboring node, it immediately reply to route reply (RREP) message without checking its routing table and with a higher sequence number. By receiving this fake message source thinks that route discovery processes completed and send data by this attacker node ignoring other RREP messages. When data comes through this node, then it drops secretly whole data. In this way the attacker node attacks all RREQ messages and takes over all routes in the network.
2) *Worm-hole Attack*-In this type of attack, an attacker place themselves between two normal nodes in the network and continuously hears the wireless data.
3) *Gray-hole Attack*-Gray hole [5] is a special case of black-hole attack which selectively drops data with some probability. In this attack attacker node timely changes its nature between a black-hole node and normal node. It is very hard to find because of its changing behavior.

8. Trust Management and Trust Related Issues

Trust [2] is a key value which is used to create safe and secure driving environment over the road. Trust is defined as a set of relations of all entities participated in a network and maintaining trust in VANET, it would mean that "All entities and objects are communicating with each other in the same manner which is expected from the context of VANET". It is generated by analyzing interactions among entities in the protocol. It is a degree of belief among entities or agents. The goal behind calculating trust value at their neighboring nodes is to build a belief to safe transmission of information to the destination and provide trustable environment which would ensure safer road experience. There are some of the characteristics of trust value as follows [11]-

- It should be dynamic calculated not static.
- It should be subjective.
- It is a method to determine trust in fully distributed environment.
- Trust is not transitive mandatorily like if node A trust node B and node B trust node C so node A may not trust node C.
- In trust decision framework all nodes should cooperative and maliciousness is likely to be prevalent over cooperation.
- Trust is not necessarily reciprocal and it is asymmetric.
- Trust is context-sensitive. A can trust B but not as a car expert.
- Trust is a function of uncertainty

9. Related Work

In VANET (Vehicular Ad Hoc Network) exchanging control and safety messages between vehicles is very crucial in real time environment. An attacker may introduce a bogus message and share with neighbor nodes. Many mechanisms have been proposed to establish trust in vehicular communication. Researchers have made strong efforts in design and implementation of trust computation in VANET. Trust is defined as a set of relations among entities that participate in a protocol. These relations are based on the evidences generated by the previous interactions of entities within a protocol.

Irshad Ahmed et al [2] proposed a TPM (Trusted Platform Module) for building a chain of trust within vehicular communication in VANET. Basically, there are five basic entities of trust and when all modules are trusted only then it worked together for

achieving chain of trust in the whole system. The security level of trust is also categorized into three levels, i.e. (1) Zero trust (COT=0) is the first level of trust at which attacker feel very free to create problem by launching different types of attacks (External & internal). (2) Weak trust is the second level of trust in which an attacker is able to launch different type of attacks but within a some specific region. Only some entities can be trusted here.(3) Strong Trust is the third level in which no attackers can manipulate network and is a very genuine condition that all entities are working properly.

Shekhar Verma et al [3] proposed a mutual authentication technique for RSU and vehicle. This mechanism basically relies on trusted traffic authorities and it maintains a hierarchical structure among central trusted authority, state level trusted authority(STA) and city level trusted authorities(CTA).Vehicle unit and RSU(road side unit) have public - private key pairs. Here each vehicle- CTA and RSU – CTA share a symmetric key. At RSU can be malicious and a vehicle can be malicious and a vehicle can communicate with a CTA only via an RSU and vice-versa. So here every message exchange in the RSU oriented communication between CTAs and vehicles to be confidential. This process is bandwidth efficient and needs only one request-reply message pair between the vehicle and the RSU (RSU- CTA-STA-TA) infrastructure to build a trust between vehicle and RSU unit. The time taken is in the order of millisecond which is a very small part of stay time of any vehicle within the RSU unit infrastructure.

David Antolino Riavas [4] et al proposed a transformation of information in VANET by validating user signatures about points of interest .

Nianhua Yang et al [6] proposed a similarity based trust and reputation management framework based on similarity between messages and similarity between vehicles for VANET. A reputation evaluation algorithm is proposed for a new vehicle based on the similarity theory. Similarities and reputations of recommenders are used as weights for computing comprehensive reputation for the generation of a message. An updating algorithm for calculating reputation in VANET is proposed which is based on similarities between vehicles, messages and other entities. The framework is applied to help the driver to decide whether he should believe the incoming message or not.

Chaurasia et al [7] proposed a reputation assisted trust evaluation framework. In this they have categorized a trust in two types, first one is static trust that depends on the organization of received messages and Second one is dynamic trust that depends on a number of vehicles are moving on the road. In this technique receiver pass message to the neighbor, then trust value will be increased between sender and receiver and if not then trust value will be decreased .The formation of group signature has five phases, i.e. setup, joining, signing, verifying and opening .in this scheme a secure group provides a message integrity which an actual signer cannot provide.

Mayuri Pophali et al [9] proposed a trust model which is a combination of several weak and vulnerable links into one strong link. After that it enhances the link quality. This model uses an opportunistic routing to enhance throughput and performance of routing. This model calculates a degree of trust and makes a relationship between neighboring nodes and desired trust degree. By this model maliciousness can be easily identifiable and solvable.

10. Conclusion

VANET is a very important subpart of MANET which is having some of the important characteristics like self organization, high mobility, no restrictions of network sizes have made very challenging to provide efficient routing environment. In this paper overview of VANET, features, applications and routing protocols have described. There is a need to put a trust between neighboring entities to provide a safe and secure driving environment in a VANET

References

[1] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, **"**Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges", Computer science Journal vol.2, 2007.
[2] Irshad Ahmed Sumra,Halabi Hasbullah, Jamalul-lail, and Masood-ur-Rehman,"Trust and Trusted Computing in VANET," Computer Science Journal Vol. 1, Issue 1, pp. 29-51, April 2011 .
[3] B. K. Chaurasia, and Shekhar Verma, "Infrastructure based Authentication in VANETs," In International Journal of Multimedia and Ubiquitous Engineering, Vol. 6, No. 2, pp.41-54, 2011.
[4] David Antolino Rivas, Manel Guerrero Zapata, "Chains of Trust in Vehicular Networks: a Secure Points of Interest Dissemination Strategy," Journal of Network and Computer Application Vol. 10 Issue 6, pp. 1115-1133, August 2012.
[5] Ram Shringar Raw, Manish Kumar, Nanhay Singh, "SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013.
[6] Nianhua Yang, "A Similarity based Trust and Reputation Management Framework for VANETs," International Journal of Future Generation Communication and Networking Vol. 6, No. 2, pp. 25-34, April 2013 .
[7] B. K. Chaurasia and S. Verma, "Trust Based Group Formation in VANET," In International Journal of Modern Traffic and Transportation Engineering Research (MTTER), Vol. 2, No. 2, pp. 121-125, 2013.
[8] Kapil Sharma, Sonam Soni, Brajish Kumar Chaurasia,"Reputation and Trust Computation in VANETs",IEMCON-14 Conference on Electronics Engineering and Computer Science, pp.118-122 ,2014.
[9] MayuriPophali, ShraddhaMohod,T.S.Yengantiwar,"Trust Based Opportunistic Routing Protocol for VANET Communication" International Journal Of Engineering And Computer Science ISSN:2319-7242 ,Volume - 3 Issue -8 August, 2014 Page No. 7408-7414.
[10] Sonam Soni et al,"Trusted Location Selection in Vehicular ad-hoc Network", American Journal of Advanced Computing, issue1,Vol. II (1), 1-6, 2015.
[11] R.S. Tomar, S.Verma and GS Tomar, "Cluster Based RSU Centric Channel Access for VANETs", Springers Transaction on Computational Science Trans. on Comput. Sci. Vol.17, LNCS 7420, pp. 150–171, 2013.
[12] B.K. Chaurasia, S. Verma, G.S. Tomar, "Intersection Attack on Anonymity in VANET", Springer Trans. on Comput. Sci. Vol.17, LNCS 7420, pp. 133–149, 2013.
[13] GS Tomar, Laxmi Shrivastava, SS Bhadauria, "Load Balanced Congestion Adaptive Routing for Randomly Distributed Mobile Adhoc Networks", Springers International Journal of Wireless Personal Communication, Vol.75, No.2(II), pp 2723-2733, Feb 2014.
[14] Laxmi Shrivastava, SS. Bhadauria, G.S. Tomar, "Influence of Traffic Load on the performance of AODV, DSR and DSDV in MANET", International Journal of Communication Systems and Network Technologies, Vol.1 Issue 1. pp 22-34, Apr 2013.
[15] Laxmi Shrivastava, Sarita S. Bhadauria, G.S. Tomar, "Performance Evaluation of Routing Protocols in MANET with different traffic loads" IEEE International Conference on Communication Systems and Network Technologies CSNT 2011, pp 13-16, 2011
[16] A.Chinnasamy et al,"Enhance Trust based Routing Techniques against Sinkhole Attack in AODV based VANET", International Journal of Computer Applications (0975 – 8887) Volume 65– No.15, March 2013.
[17] Brijesh K Chaurasia, Shekhar Verma, GS Tomar, "Trust Computation in VANETs", IEEE International Conference on Communication Systems and Network Technologies pp 468-471, 2013.

