Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 45 (2015) 592 – 601

Procedia Computer Science

International Conference on Advanced Computing Technologies and Applications (ICACTA-2015)

Trust based approaches for secure routing in VANET: A Survey

Nirav J. Patel[1] , Rutvij H. Jhaveri[2]

Department of computer engineering-IT, Shri S'ad Vidya Mandal Institute of Technology , Bharuch 392-001, Gujarat, India, nirav402@gmail.com[1],

Department of computer engineering-IT, Shri S'ad Vidya Mandal Institute of Technology, Bharuch 392-001, Gujarat, India, rhj_svmit@yahoo.com[2]

Abstract

Vehicular Ad-hoc networks (VANETs) require trusted vehicles to vehicles communication. VANET is multidimensional network in which the vehicles continuously change their locations. Secure routing is imperative during the routing process to incorporate mutual trust between these nodes. Sometimes, the malicious node broadcast the bogus information among other nodes. Establishing trust is a challenge while one or more malicious nodes attempt to disrupt route discovery or data transmission in the network. A lot of research has been carried out for secure routing process with trust-based approaches. In this paper, we present survey of various mechanisms to improve different ad-hoc routing protocols for secure routing process by enhancing the trust among different nodes in VANETs.

Peer-review under responsibility of scientific committee of International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

Keywords: Vehicular ad hoc network, routing protocols, trust management, reputation, security.

1. Introduction

Vehicular ad-hoc network is an emerging area in networking. It is a subset of Mobile ad-hoc networks. Vehicular ad-hoc network that provides Vehicles to Vehicles (V2V), Rode-side Unit to Rode-side Unit(R2R) and Vehicles to rode-site Unit (V2R) communication[30]. In recent years, more accident cases are found significantly. Due to this, roads are found to be more congested and busy. With the help of dedicated short range communication (DSRC) VANETs establishes communication between various vehicles which are changing their direction frequently. Vehicles directly communicate with different vehicles and send information regarding traffic jams, warning messages with road-site unit (RSU) which is fix equipment in roads.

Peer-review under responsibility of scientific committee of International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).
doi:10.1016/j.procs.2015.03.112

VANET is a part of Mobile Ad–hoc network so, all nodes move dynamically within the network area and communicate with each other in single hop or multi hop by utilizing the road-site unit (RSU)[1]. Benefit of VANETs is to enhance safety feature in cars by exchanging warning message between vehicles. VANETs also suffer from different kinds of attacks like denial of service (DOS), message modification, false message sending etc. One of the main concerns of VANET is to enhance the passenger safety, to exchange the safety message among the nodes [2]. VANET Communication architecture describe in Fig. 1. [30]

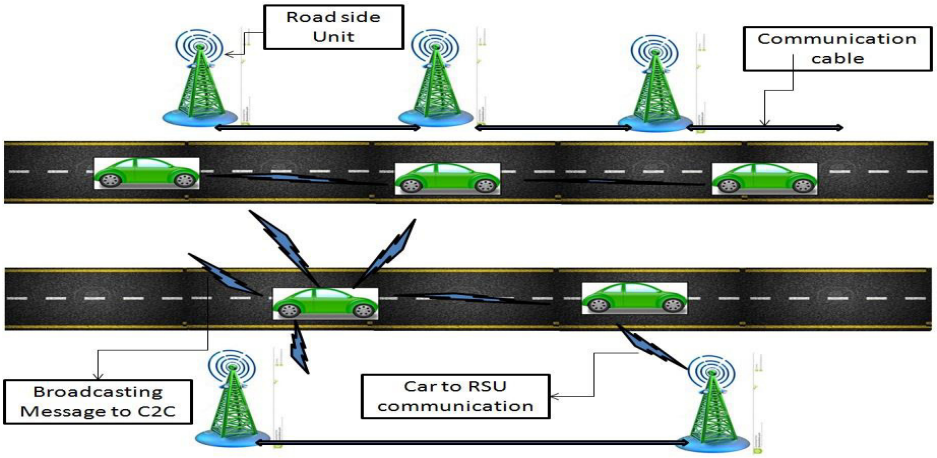

Fig. 1. VANET Communication architecture [30]

Vehicles communicate with another vehicle directly if there is wireless connection available; it's called single hop vehicle to vehicle (V2V) communication. If there is lack of direct connection between them then, forward data one vehicle to other vehicles until it reaches proper destination its called multi-hop vehicle to vehicle (V2V) communication. Vehicles also communicate with Road Site Unit (RSU) that increases range of network for communicating vehicles to RSU for sending, forwarding and receiving data with them [31].

The Security is more crucial in VANETs due to lack of centralization, dynamic topology. Due to this, it is difficult to identify malicious, misbehaving and faulty nodes or cars in network. Mainly trust models are based on verifying vehicles and provide appropriate trust value to all vehicles. Trust should be provided either directly or indirectly. We can classify which node is trustworthy, secure and reliable communication with other nodes in network by utilizing the trust values. The paper proceeds as follow [30].

In section 2, we present various conventional ad-hoc routing protocol for VANETs. The issues of trust management are described in section 3. Section 4 describes the summary of literature survey. Finally, the paper concluded in section 5.

2. Routing protocols for VANETs

A VANETs having dynamic nature of nodes and dynamic topology, Hence the mechanism is to provide optimal path between network nodes by reducing the overhead [3][4]. Basically routing protocols are classified in topology based and position based which show in Fig. 2. [35][23].

2 Topology Based Routing Protocol

Topology based routing protocol is traditional MANET routing protocol. It uses source to destination information that is stored in routing table. There are three types of sub-categories in topology based routing protocol, namely, Proactive, Reactive and Hybrid [35].

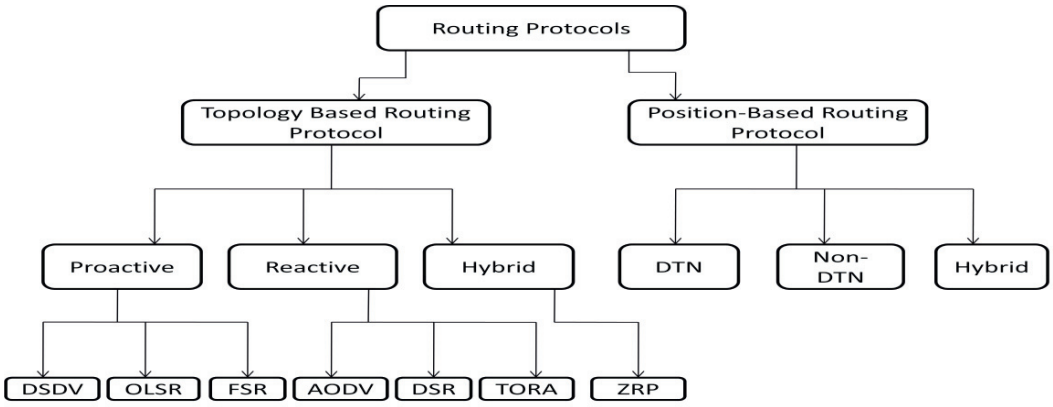

Fig. 2. VANET Routing Protocols [35]

2.1.1 Proactive Routing Protocols

Proactive protocols store route information in routing table for all the network nodes, whether route information is needed or not for communication. Each entry in the routing table contain next hop by providing path to the destination. Routing table updated frequently on dynamic topology. These protocols choose shortest path algorithm for routing [4].

2.1.1.1 Destination Sequence Distance Vector Routing(DSDV)

Destination Sequence Distance Vector Routing protocol is one type of table driven protocol. DSDV provide loop free routing, reducing the extra traffic by utilizing the frequent updating in routing table, It's also reducing routing overhead and it's always choose optimal path with the use of shortest path algorithm. DSDV assign the sequence number to avoid the duplication entry into the routing table. DSDV doesn't provide multi path routing and they don't have any control over network congestion [26].

2.1.1.2 Optimized Link State Routing Protocol

OLSR protocol is implemented with link state policy. In this protocol, all possible route paths are stored in routing table for network nodes traversal. When network topology changes then all nodes sent update routing information to such selected nodes. After those node re-broadcasts that information to next hop. The nodes can read those information and process the packet that is not selected list. OLSR works well in dynamic topology in which low latency is suitable during the data transmission. Network congestion is the limitation of the OSLR [25].

2.1.1.3 Fisheye State Routing(FSR)

FSR is table driven protocol, storing the latest information in to routing table that is received from neighbor nodes. The source transmits the packet to destination by different frequency for neighbors with the use of routing table. It is in not scalable in large network. It maintains neighbor nodes information for routing as accurate manner. Poor performance is found if node is far or long in distance. If the neighbor node is closer than the performance of FSR found to be accurate [35].

2.1.2 Reactive Routing Protocols

Reactive routing protocols also called as on-demand routing protocol. This protocol reduces overhead in the network. When source node need to communicate with destination node than source node starts a route discovery until it reaches destination node. After that, destination node send route reply message (RREP) to source

node using uni-cast communication. Reactive routing protocols are used in large size ad hoc network that is high mobility and dynamic nature topology in network [4].

2.1.2.1 Ad Hoc On-Demand Distance Vector(AODV)

Ad Hoc On-Demand Distance Vector (AODV) routing protocol is reactive (on-demand) protocol. It is proposed for Mobile ad hoc Network. Packet headers not included for routes in AODV. It is highly dynamic in nature and reducing overhead. Routing information is stored in source node, destination node and intermediate nodes along with active routing in data transmission. In AODV, three steps involved for routing, route discovery, route establishment and route maintenance for the communication path. AODV contain three controls message in communication, Route Request (RREQ), Route Reply (RREP), Route Error (RERR) messages for establishing connection with source to destination node. Source node broadcast RREQ to all neighbors node if any node has destination path than intermediate node also broadcast RREQ. If destination found than destination node send RREP to source node with sequence number. Then source node select higher sequence number path for routing path. AODV also support multipath routing for communication. AODV needs extra bandwidth for broadcasting control message [28].

2.1.2.2 Dynamic Source Routing Protocol(DSR)

DSR protocol provide a high on-demand routing process, its low overhead protocol and fast reacts on the frequent changes in network topology. DSR protocol provides successful data packet delivery on change in network nature. DSR allows multi hop routing in dynamic nature of network. Two main processes in this protocol are: Route discovery and Route maintenance. When source node need to communicate with node whose path is unavailable. In this scenario, Source node starts up a route discovery process in which the source node broadcasts route request message. The destination node on receiving a RREQ packet, It sends back route reply message to source node. Source node keeps the route in route catch for future communication. If routing fail than it sends back to route error to the source node. In DSR protocol every packet has intermediate node, source node delete path in cache and then store alternative path for destination [27].

2.1.2.3 Temporally Ordered Routing Protocol(TORA)

TORA is a distributed protocol that is highly scalable, nonhierarchical, multi path routing protocol. It reduces the communication overhead in designing the frequent changes in network. This protocol doesn't follow the shortest path algorithm but, uses directed acyclic graph (DAC) for communication. One of the advantages of TORA is it has available path for all nodes within network and reduce control message for broadcast [35].

2.1.3 Hybrid Protocols

Hybrid protocol is combination of proactive and reactive protocols. Hybrid protocol is used according ad hoc network scenario. The objective of hybrid routing protocol is to reduce the overhead and speedup the packet delivery to destination with the use of reactive protocol. Basically this protocol divides the network in many different zones [4].

2.1.3.1 Zone Routing Protocol(ZRP)

ZRP is developed for hybrid routing that is the combination of proactive and reactive protocols. It divides network in to different zones. In this protocol many factors are included like power transmission, strength of singles, speed, mobility and other factors. We can divide inner zone routing schemes with proactive protocols and outer zone routing schemes with reactive protocols. It uses existing protocols of proactive and reactive protocols for routing. Inner zone keeps the latest route information within inner zone in which source node uses cached routing table to route a destination. In outer zone where source node transmits a route request to last node of that network. Packet includes sequence number of source address and the destination address. Last node of zone receives a route request

packet, if it finds the destination node within own zone than sends route reply packets with sequence number of destination node to source node [29].

2.2 Position-Based Routing Protocol

Position based routing or geographic routing is based on the positional information of nodes in routing process. For utilizing the source node it sends a packet to the destination node using geographic position of individual node. In this protocol each node is able to decide its location and its neighbour node through GPS (global positioning system). It stores destination position of node and attach it in packet header which help to forward packets to the destination without a needs of route discovery, route maintenance. It is commonly classified in three sub categories: Delay Tolerant Network (DTN) protocols, Non Delay Tolerant Network (Non DTN) protocols, hybrid protocols [35][23].

3. VANETs trust management issues

Vehicles in VANET are in roaming area on roads and are highly dynamically change in topologies around city or urban area. According to traffic situation or different types of road, vehicles speed may vary. It is difficult to react on position for higher speed of vehicles. It is important to gain trust and related information about in real time [32]. VANET is decentralized and open system environment. So, there is a possibility that any vehicle can join and leaves the network at any time. There is no mechanism to meet next time within network for after communication with particular vehicle. False information should not be transferred by the neighbor node which affects the overall performance of network. False positioning is received by malicious nodes that affect traffic jams on roads and that increase the probability of collision on roads [7]. High mobility in VANET is due to vehicles random speed i.e., On highway vehicles speed is found up to 60-100 km/hr, Means, vehicles move's fast as it needs high transmission power from node to node [23]. Vehicles move randomly in any direction on roads, so not required long term relationship with other nodes/peers is maintained. Road condition is dynamic so we cannot predict traffic and actual condition of nodes [22]. Node information like time and location information are accurate to all vehicles. Its current location is sent rapidly to other vehicles and RSU unit for establishment of trust value to vehicles.
Trust establishment approaches classification as describe in Fig. 3. [34].

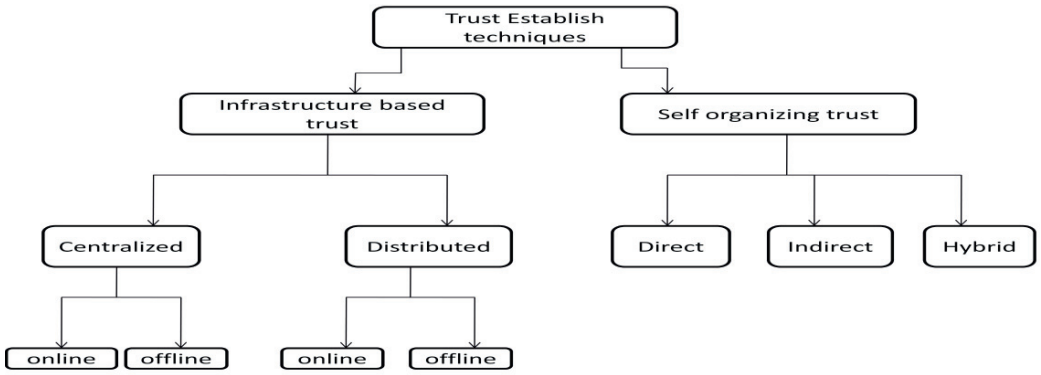

Fig. 3. Trust establishment models [34]

- **Infrastructure models**

Certified Central Authority (CA) provides certificates to all other nodes/vehicles that provide authentication to particular peers/vehicles. The presence of RSU is necessary in infrastructure models for communication [34].

- **Self Organizing models**

Self Organization models are classified in three sub categories: Direct trust model, indirect trust model, Hybrid trust model [34].

- There are several challenges of VANET described as below [36][23]:
  - Network management
  - Congestion and collision control
  - Environmental impact
  - Security
  - Social and Economical challenges
- Trust Establishment techniques for different sources are as below [33]:
  - Cryptographic Authentication (etc. PKI key management)
  - Accurate Source Location
  - Local Sensors for identifying neighbor node
  - Other Vehicles messages transmission
  - Infrastructure Validation as per road map
  - Identify Sender's Repudiation

4. Related Works

In this section, we are describing the existing approaches for trust establishment in VANETs. That follows different trust models and different techniques to establish trust between vehicles.

Hong x. et al. [12], proposed establishing trust management scheme with three aspects, which are policy control, proactive trust establishment, social network impact on the network. Policy control considers entry trust and data trust attributes are used. Proactive trust considers traditional approach according to past communication history of that car/node for the trust value. Social trust consider nearest vehicles opinion and setting up trust among another vehicles.

Jorge h. et al. [19], proposed watchdog algorithm with intrusion detection techniques for establishing trust management. In that source node sent packets to the neighbour node and monitors that node with ids. Its forward that packets than maintain its trust value in trust table otherwise that decrease trust value of that node. Drawback of this technique is to create collision in network, and monitor that node until that forward or drop. It has contained huge monitoring history of neighbour node if it has large number of neighbour nodes.

Cong l. et al. [13], proposed trustworthiness based on incident reports in V2V communication and forward to those vehicles. Crowed sourcing capabilities use for evaluating trustworthiness value for vehicles. Global view can broadcast for individual vehicles trust value in CSC. Future work includes security and privacy issues using unique identification and public key infrastructure mechanism.

Zhou w. et al. [9], proposed establish Dynamic trust token based on method used for co-operation with nodes. Both cryptography mechanism should be included for packet integrity with symmetric and asymmetric algorithm and applies neighbourhood watchdog algorithm which generate tokens for checking packet is either valid or not. In this algorithm protection of packets during communication is increased and latency of network is decreased. It is cooperative packet forwarding schemes applying for communication. It is setup for instant trust at run time communication. Drawback of this technique is not encouraging misbehaving node to well behaving, don't punish malicious node and not reward good nodes.

Subir b. et al. [20], proposed id-based techniques used for verification of cars with public key without certificate. Proxy server provide message authentication and trust management. Safety message delivered though RSU (rode site unit) and id-based signature properties implies on proxy signature with ECDSA. In this technique authentication and trust management is dynamic and un-trustworthiness. Trust management scheme is handled by RSU which had proxy signature pre-stored.

Tahani g. et al. [24], proposed markov chain model for establishing trust management. This model not only considers behaviour of node in dynamic trust metric but that monitor all constraints activity of that node. Each vehicle treated as monitoring an updating trust metric table of its neighbour nodes belong that behaviour. Misbehaving and selfish vehicles identified with this mechanism. It uses time interval and number of transition with other nodes in trust management. This system uses stress and trust evolution system for trust model. In this global trust should not be established which is future scope of this mechanism.

Yu-Chih w. et al. [21], proposed road site unit (RSU) and beacon based trust management system to improve safety and location privacy. This techniques motto is quick message opinion and prevent sending and forwarding from internal malicious node. This technique takes decision quickly and provides opinion in less time.

Drawback of this mechanism is not able to compare trust value with another node.

Felix g. et al. [6], proposed provide trust based on TRIP (Trust and Reputation infrastructure based proposal) algorithm for traffic analyzing. TRIP identify malicious and selfish node which spreading bogus or false information in network. Message and traffic warning message sent to another node that checks reputation and trustworthy value of that node. If node is malicious than reject and drop packets from those nodes/cars. Fuzzy logic classifies and categorizes trust value as per operation and advertisement messages. Reputation score are computes with three information's: previous experience, surrounding vehicles and recommendation of the central authority. Three types of trust values: Not trust-reject all packets, +/- trust-accept but not forward and trusted- accept and forward. Drawback of this mechanism is hard to maintain trust value and behaviour of node and we can't identify the node is honest or malicious.

Sanjay k. et al. [5], proposed overcome event modification message, false event generation in network and data grouping with the use of Vehicular Security throw reputation and plausibility check (VSRP) mechanism. VARs algorithm performs indirect and direct reputation in network. It validate message handling technique like opinion generation, opinion piggybacking and provide node reputation. Identify node false message generation nodes and prevent with plausibility validation model (PVM). If any event occurred that broadcast message to all neighbour. Each node contains all neighbour node trust table that is frequently changing according the reputation of that node. VSRP can mitigate or eliminate malicious nodes in the network. Drawback of this technique is that it has only neighbour node information lack of global network situation. In future implies location based service be added in extended version of VSRP.

Tahani g. et al. [10], proposed trust model depends on public key infrastructure for trust management and distributed cluster algorithm. VANET dynamic demilitarized zone, its set of vehicles of neighbours provide confident and there is registration authority (RA) provide authentication to each vehicles within particular cluster head (CH). This technique prevents malicious and unknown vehicles which are authenticated within cluster. Cluster head define as trust level and vehicles CA. Cluster algorithm is based on two parameters: trust metric used for define trust level of vehicles and mobility metric.

Qing d. et al. [11], proposed event based reputation model for filtering bogus messages. Role-based reputation mechanism is used to determine incoming message is significant and trustworthy to the drivers/cars. It enhances trust for vehicular network. This technique includes random way point which is not sufficient technique for reputation. In future we can imply fuzzy logic for calculating reputation value for an event.

Jian w. et al. [8], proposed trust propagation establishing throw describes new relationship from pre-existing trust relationship. It is novel scheme for enhancing trust propagation scheme in VANETs. Numerical methods include effective performance in trust propagation scheme. This approach improves packet forwarding in multi hop routing and provides reliable packet delivery.

Jetzabel s. et al. [15], proposed geolocation-based trust establish and studies proposing privacy and use of pseudonyms. Privacy mechanism provide with mandatory access control and novel technique for trust information based in vehicles geolocation. Drawback of this approach is not to provide any authorization and authentication collection of data.

Tahani g. et al. [14], proposed hybrid trust model for determines trust metric. Two terms used for monitoring trust: cooperation with other vehicles in network and broadcast legitimate data. Fuzzy based algorithm used to decide the honesty of vehicles and filter out malicious vehicles. One trusted neighbour to issue CA in the PKI is distributed among number of vehicles. Trustworthy value is calculated through monitoring cooperativeness of monitor vehicles and forward calculated trust to neighbour vehicles.

Yi-Ming c. et al. [18], proposed Beacon-based trust management (BTM) techniques prevents the internal attackers from sending false or bogus messages in privacy enhancement in network. Secure beacon based trust protocol is used to evaluate direct and indirect trust management scheme. Direct trust in trustworthiness value and indirect trust opinion transmitted from multiple vehicles. Dempster Shafer evidence theory is used for numerical computation.

Chen c. et al. [16], proposed data aggregation mechanism for establishes trust in network. This is used to check the quality of the message. This method use multiple existing identity based aggregation methods like concatenate signature base, onion signature base, and hybrid signature base combines in to one aggregate signature summing them mathematically. It eliminates signature redundancy of aggregation signature, flexibility to aggregation function no negative effects in network. Drawback of this algorithm is signature size is much higher and no comparative mechanism.

Rashmi s. et al. [17], proposed trust based approach in clustering and ant colony routing, clustering techniques create cluster and consider position, direction and speed of relative vehicles manage networks/cars. Cluster head (CH) considering real time update location and trust value of that vehicles. Direct and Indirect trust mechanism used to establish the trust. Trust management used to find out the most trusted path between two nodes of a VANET.

5. Conclusion and future Scope

Trust management for secure routing over network is most crucial to establish. It makes V2V (Vehicles to vehicles) and V2I (Vehicles to infrastructure) communication secure and maintain privacy between them. Handling false or bogus information is voluminous concern in ad hoc network. For that, trust management is required that make the communication reliable. To evaluate the paper concern, we survey various techniques with their novels ideas as well as we also describe the conventional routing protocols in briefly. Most of the methods are described with direct and indirect trust which is used to calculate the trustworthiness value of node. Several approaches are used cryptography techniques for secure communication over a cluster in ad hoc network in which cluster head (CH) approaches distinguee in small cluster and provide trust throw certificate authority within cluster. Fuzzy Method is used to classify malicious and normal node in network.

In future we try to provide centralized certification techniques for small town or geographical proactive information that used to calculate trust value of particular vehicles.

Appendix A. Table 1. A Survey of trust establishment approaches

Topic Name	Description	Mechanism / Algorithm	Methodology	QoS / Performance
SAT: situation-aware trust architecture for vehicular networks[12]	The SAT is works as a middle layer to establish the trust between nodes, which includes two functions : SAT layer and STL	SAT architecture (Situation-Awareness Trust)	Establish trust based on cryptographic techniques such as data integrity and authentication	Policy control, Trust enhancement, Social network
Evaluating the usefulness of watchdogs for intrusion detection in vanets[19]	Watchdog monitors neighbour node and listen behaviour trust value	Watchdog algorithm with intrusion detection	Neighbours node forward packets ahead and monitor node	Coverage and detection latency, False negative & false positive
Countermeasure uncooperative behaviors with dynamic trust-token in VANETs[9]	DTT provides instant calculated trust at real time performance of the node	Dynamic Trust-Token (DTT)	Symmetric and asymmetric cryptographic for integrity and watchdog used for generating trust token	Protect packet integrity, latency degradation
ID-based safety message authentication for security and trust in vehicular networks[20]	ECDSA is used for RSU unit authentication and verification for message transfer which makes message secure	ID-based proxy signature and ECDSA	Certificate less public key verification for message authentication and trust management	Message transfer with authentication throw trusted RSU
An efficient trust management system for balancing the safety and location privacy in VANETs[21]	RSU decides immediately which message is trust worthier as per opinion sent by other vehicles. Message opinion quickly and prevents internal attacks	Road-side unit (RSU) and Beacon-based trust system (RABTM)	Indirect event based trust used for trust establishment and beacon message and event message to determine the trustworthiness value of that event	Safety and location privacy of vehicles
TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks[6]	Identify malicious and selfish nodes which node broadcast bogus information. Central authority has a malicious database update frequently	Trust and reputation infrastructure based proposal(TRIP)	Fuzzy set classify trust and categorized, servity of previous trust	Identifying malicious and selfish node which spreading false information
Securing vehicular networks: a reputation and plausibility checks-based approach[5]	Opinion generation, opinion piggybacking and provide node reputation is trusted or malicious node. False message generation identifies with PVM	Vehicular Security throws reputation and plausibility check (VSRP), VARs algorithm	VARs algorithm performs indirect and direct trust, Reputation based algorithm	Event Modification, false event generation, data aggregation and data

				Dropping
Secure clustering scheme based keys management in VANETs[10]	VDDZ describes filter certificate request provided by CA in the cluster. It also protects direct communication and differ attacks	VANET Dynamic Demilitarized Zone (VDDZ)	Divide cluster head (CH) of neighbour node and Registration authority(RA) provide the confident to neighbours	Prevent malicious and unknown vehicles within cluster
Reputation-based trust model in vehicular ad hoc networks[11]	All vehicles encounter same traffic event and distinguish differ roles occurred in event	Event based reputation algorithm	Random way point scheme to adopt for identify bogus information	Filter bogus and false warning message, enhance trust
A trust propagation scheme in VANETs[8]	Derive new relationship between pre-existing trust relationship evaluate trust based on forwarding packets of attributes check and calculate similarity between two nodes	Novel scheme for enhancing trust management	Attributes comparison with trust value	Enhancing trust propagation, reliable packet delivery
Geolocation-Based Trust for Vanet's Privacy[15]	Mandatory access control provides trust validation between nodes. Novel technique provides valid trust geographical area	Geolocation based establishment	Pseudonyms used for privacy and MAC trusted location	Privacy mechanism
A trust-based architecture for managing certificates in vehicular ad hoc networks[14]	Certificate authority(CA) provide legitimately to vehicles and fuzzy distinguee honest node and cluster broadcast trust value to neighbour	Fuzzy algorithm, certification authority (CA)	Fuzzy based solution and certificate authority(CA) and PKI scheme	CA within cluster only Co-operation with vehicles and legitimate broadcast data
A beacon-based trust management system for enhancing user centric location privacy in VANETs[18]	BTM establishes and verifies vehicles position and direction. Message transmission send with cryptography and the pseudo identity scheme	Beacon-based trust management (BTM), Dempster Shafer evidence	Beacon establish trust relationship, FSP and RSP location privacy enhancement scheme	internal attacks, bogus message and privacy enhancement
Secure and efficient trust opinion aggregation for vehicular ad-hoc networks[16]	Combine multiple message signature into one signature which used to send to vehicle	Identity based aggregate algorithm	Trust opinion aggregate scheme	Space efficiency and time complexity
A trust based clustering with Ant Colony Routing in VANET[17]	CH is used to partition the network in cluster and that calculate the indirect trust on source node. Ant colony used for secure and optimized routing path	Trust dependent Ant Colony Routing (T ACR), Mobility-aware Ant Colony Optimization Routing (MAR-DYMO)	MAR-DYMO used for routing overhead in the network. CH calculate indirect trust value, MAR-DYMO for optimized routing technique	Scalability, real time updated position and trust value of vehicles

References

[1] Hartenstein, Hannes, and Kenneth P. Laberteaux, "A tutorial survey on vehicular ad hoc networks", Communications Magazine, IEEE 46.6,pp- 164-171, 2008.

[2] Mazilu, Sînziana, Mihaela Teler, and Ciprian Dobre, "Securing vehicular networks based on data-trust computation", In P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2011 International Conference on, pp- 51-58. IEEE, 2011.

[3] Taleb, Tarik, Ehssan Sakhaee, Abbas Jamalipour, Kazuo Hashimoto, Nei Kato, and Yoshiaki Nemoto, "A stable routing protocol to support ITS services in VANET networks", Vehicular Technology, IEEE Transactions on 56, no. 6,pp- 3337-3347,2008.

[4] Fonseca, Emanuel, and Andreas Festag, "A survey of existing approaches for secure ad hoc routing and their applicability to VANETS", NEC network laboratories 28 pp- 1-28,2006.

[5] Dhurandher, Sanjay K., Mohammad S. Obaidat, Amrit Jaiswal, Akanksha Tiwari, and Ankur Tyagi, "Securing vehicular networks: a reputation and plausibility checks-based approach", In GLOBECOM Workshops (GC Wkshps), IEEE, pp- 1550-1554, IEEE, 2010.

[6] Gómez Mármol, Félix, and Gregorio Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks", Journal of Network and Computer Applications 35 springer, no. 3 pp- 934-941,2012.

[7] Huang, Zhen, Sushmita Ruj, Marcos Cavenaghi, and Amiya Nayak, "Limitations of trust management schemes in VANET and countermeasures", In Personal Indoor and Mobile Radio Communications (PIMRC), IEEE 22nd International Symposium on, pp- 1228-1232. IEEE, 2011.

[8] Wang, Jian, Yanheng Liu, Xiaomin Liu, and Jing Zhang, "A trust propagation scheme in VANETs", In Intelligent Vehicles Symposium, IEEE, pp- 1067-1071, IEEE, 2009.

[9] Wang, Zhou, and Chunxiao Chigan, "Countermeasure uncooperative behaviors with dynamic trust-token in VANETs", In Communications, ICC'07, IEEE International Conference on, pp- 3959-3964, IEEE, 2007.

[10] Gazdar, Tahani, Abderrahim Benslimane, and Abdelfettah Belghith, "Secure clustering scheme based keys management in VANETs", In Vehicular Technology Conference (VTC Spring), IEEE 73rd, pp- 1-5. IEEE, 2011.

[11] Ding, Qing, Xi Li, Ming Jiang, and XueHai Zhou, "Reputation-based trust model in vehicular ad hoc networks", In Wireless Communications and Signal Processing (WCSP), International Conference on, pp- 1-6, IEEE, 2010.

[12] Hong, Xiaoyan, Dijiang Huang, Mario Gerla, and Zhen Cao, "SAT: situation-aware trust architecture for vehicular networks", In Proceedings of the 3rd international workshop on Mobility in the evolving internet architecture, pp-31-36, ACM, 2008.

[13] Liao, Cong, Jian Chang, Insup Lee, and Krishna K. Venkatasubramanian, "A trust model for vehicular network-based incident reports", In Wireless Vehicular Communications (WiVeC), IEEE 5th International Symposium on, pp-1-5, IEEE, 2013.

[14] Gazdar, Tahani, Abderrahim Benslimane, Abderrezak Rachedi, and Abdelfettah Belghith, "A trust-based architecture for managing certificates in vehicular ad hoc networks", In Communications and Information Technology (ICCIT), International Conference on, pp-180-185.,IEEE, 2012.

[15] Serna, Jetzabel, Jesus Luna, and Manel Medina, "Geolocation-Based Trust for Vanet's Privacy", In Information Assurance and Security, ISIAS'08, Fourth International Conference on, pp-287-290. IEEE, 2008.

[16] Chen, Chen, Jie Zhang, Robin Cohen, and Pin-Han Ho, "Secure and efficient trust opinion aggregation for vehicular ad-hoc networks", In Vehicular Technology Conference Fall (VTC 2010-Fall), 2010 IEEE 72nd, pp. 1-5. IEEE, 2010.

[17] Sahoo, Rashmi Ranjan, Rameswar Panda, Dhiren Kumar Behera, and Mrinal Kanti Naskar, " A trust based clustering with Ant Colony Routing in VANET", In Computing Communication & Networking Technologies (ICCCNT) Third International Conference on, pp- 1-8. IEEE, 2012.

[18] Chen, Yi-Ming, and Yu-Chih Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs", Communications and Networks, Journal of 15, no- 2 pp- 153-163, 2013.

[19] Hortelano, Jorge, Juan Carlos Ruiz, and Pietro Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in vanets", In Communications Workshops (ICC), IEEE International Conference on, pp- 1-5. IEEE, 2010.

[20] Biswas, Subir, Jelena Misic, and Vojislav Misic, "ID-based safety message authentication for security and trust in vehicular networks", In Distributed Computing Systems Workshops (ICDCSW), 31st International Conference on, pp- 323-331. IEEE, 2011.

[21] Wei, Yu-Chih, and Yi-Ming Chen, "An efficient trust management system for balancing the safety and location privacy in VANETs", In Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 11th International Conference on, pp- 393-400. IEEE, 2012.

[22] Yan, Gongjun, Stephan Olariu, and Michele C. Weigle, "Providing location security in vehicular Ad Hoc networks", Wireless Communications, IEEE 16, no. 6 , pp- 48-55,2009.

[23] Li, Fan, and Yu Wang, "Routing in vehicular ad hoc networks: A survey", Vehicular Technology Magazine, IEEE 2, no. 2,pp- 12-22,2007.

[24] Gazdar, Tahani, Abderrezak Rachedi, Abderrahim Benslimane, and Abdelfettah Belghith, "A distributed advanced analytical trust model for VANETs", In Global Communications Conference (GLOBECOM), IEEE, pp- 201-206. IEEE, 2012.

[25] P. Jacquet, . P Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot, "Optimized Link State Routing Protocol for Ad Hoc Networks" 0-7803-7406-1/01/,2001 IEEE

[26] Khaleel Ur Rahman Khan, A Venugopal Reddy, Rafi U Zaman, K. Aditya Reddy, T Sri Harsha, "An Efficient DSDV Routing Protocol for Wireless Mobile Ad Hoc Networks and its Performance Comparison", Second UKSIM European Symposium on Computer Modeling and Simulation, 978-0-7695-3325-4/08, 2008 IEEE.

[27] Mohamed Aissani, Mustapha Réda Senouci, Walid Demigna, and Abdelhamid Mellouk, "Optimizations and Performance Study of the Dynamic Source Routing Protocol", Third International Conference on Networking and Services(ICNS'07), 0-7695-2858-9/07 ,2007 IEEE.

[28] Prashant Kumar Maurya, Gaurav Sharma, Vaishali Sahu, Ashish Roberts, Mahendra Srivastava, "An Overview of AODV Routing Protocol", International Journal of Modern Engineering Research (IJMER) ISSN: 2249-6645 Vol.2, Issue.3, May-June 2012, pp-728-732.

[29] Sweety Goyal, "ZONE ROUTING PROTOCOL (ZRP) IN AD-HOC NETWORKS", IJREAS, Volume 3, Issue 3 (March 2013), ISSN: 2249-3905.

[30] Zeadally, Sherali, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan ", Vehicular ad hoc networks (VANETS): status, results, and challenges.", Telecommunication Systems 50, no- 4 pp- 217-241, Springer, 2012.

[31] Hartenstein, Hannes, and Kenneth P. Laberteaux. ", A tutorial survey on vehicular ad hoc networks", Communications Magazine, IEEE 46, no- 6 pp- 164-171, IEEE, 2008

[32] Zhang, Jie. "A survey on trust management for vanets.", In Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on, pp- 105-112, IEEE, 2011.

[33] Wang, Dongxia, Tim Muller, Yang Liu, and Jie Zhang. "Towards Robust and Effective Trust Management for Security: A Survey."

[34] Wex, Philipp, Jochen Breuer, Albert Held, T. Leinmuller, and Luca Delgrossi, "Trust issues for vehicular ad hoc networks.", In Vehicular Technology Conference, 2008, VTC Spring IEEE, pp-2800-2804. IEEE, 2008.

[35] Altayeb, Marwa, and Imad Mahgoub, "A survey of vehicular ad hoc networks routing protocols.", International Journal of Innovation and Applied Studies 3, no-3, pp- 829-846, 2013

[36] 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,pp- 95-105, September 2013