WORLD COMPLEXITY SCIENCE ACADEMY JOURNAL| Vol. 1 Issue 2, 18 |Fall 2020

A COMPARATIVE STUDY ON TRUST-BASED SECURITY ROUTING PROTOCOLS FOR VANETS

N.S. Vishnu[1*], Sahil Verma[1*], and Kavita[1*]

[1] School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India

*Correspondent author, N.S. Vishnu - nsvishnu890@yahoo.com; Sahil Verma - sahilkv4010@yahoo.co.in; Kavita - dhullkavita@yahoo.in

Received: 24. June 2020; Accepted: 11. June 2020; Published: 18 September 2020
DOI: https://doi.org/10.46473/WCSAJ27240606/18-09-2020-0018
Category: Research paper

ABSTRACT

Vehicular Ad-Hoc Networks (VANETs) have gained popularity due to their ideal characteristics and wide range of applications. In VANETs, every vehicle is capable of acting as a routing device to transmit the data as well as an endpoint vehicular node for the processing of transmitted data. Various routing protocols were proposed for VANETs to determine the paths between the two vehicular nodes. The majority of these protocols were derived from the protocol designs of MANETs. Due to the distinct traits of nodes in the VANETs, there is the need for appending security features to the existing protocols for reliable and secure communication among the vehicular networks. VANET Secure routing protocols can be of three main classes, namely, Cryptography based, Trust-based and Hybrid protocols. In this paper, we surveyed various Trust-based security mechanisms to actively secure the communications taking place between the vehicular nodes. Also, the surveyed Trust-based protocols were compared to determine the effectiveness and working strategies of each of them.

Keywords: VANETs, Network, Credibility, Cryptography, Routing, Transmission, Security, Privacy.

1. Introduction

Perennially varying Topology, elevated Mobility, and Self- Administration are exceptional traits of Vehicular Ad-Hoc Networks (VANETs) (Mansour et al., 2018). Despite having these remarkable qualities, they also possess some confrontations (Jadhao and Chaudhari, 2018; Li, Song, 2015) . The benefits provided by this networking strategy may degrade its quality deliverance with improper Routing practices (Jadhao and Chaudhari, 2018). The Routing processes which occur between the nodes within the network are normally governed by the

Protocols (Patel and Jhaveri, 2015). So, these protocols must be fabricated carefully to meet the required outcomes eliminating the flaws incurred (Mishra et al., 2016). The essential objective of installing the Security features in any field is to achieve "Confidentiality", "Integrity" and "Availability" (Jadhao and Chaudhari, 2018). As every node present in these kinds on the network doesn't keep any Wired connection with any of its nodes situated beside them, the security concerns are increased while in transmission of essential information among the nodes (Hosmani and Mathpati, 2017). Consider, for example, the fact that to ensure security while a vehicle node A is transmitting a message to another vehicle node B, we need to completely make sure that the message being transmitted between these two nodes must not be altered, should not be accessed by any unauthorized third party individual or any device, and it must not adhere much duration to reach its intended destination (Oluoch, 2016). To attain the feature of Integrity, the device must be able to verify whether the received messages are the exact ones that were sent by the Source device. The nodes should also be concerned whether these data are received from a trusted node or not. Sometimes, the attacker can send the target system with some erroneous data to mislead the device. In Vehicular networks, it is can be very crucial if the messages are not validated because the attacker might transmit fallacious information and this can lead to fatal situations (Mishra et al., 2016). The security mechanisms in the Routing Protocols ensured that the data which is disseminated among the nodes is not lost somewhere in the course of the transmission process (Godse and Mahalle, 2017). It is observed that the adoption of these smart routing techniques can lower the occurrences of accidents. In these networks, the vehicular nodes communicate with its adjacent nodes and go on passing the information. Sometimes, the Road Side Units are also assisted in reducing the delays incurred (Oluoch, 2016). Through the exercise of these networks, vehicular users might be able to communicate with each other and also, they can know the movement of the other vehicles in different lanes. This can be a significant strategy to bring down the accidental cases. Even though the Cellular networks are in existence for the quality communication between the users, this cannot be preferably used in these kinds of networks (Oluoch, 2016).

The cautionary alerts are passed among the nodes to reduce destruction in case of hazardous situations. When a vehicle has an accident, this alert message will be forwarded to the emergency services through the intermediary nodes and the RSU to get the required medical support to the user (Mansour et al., 2018). This can even help some people who are in a hurry by addressing them to take a different route to reach their destination. This prior alerting technique can eliminate the occurrence of the majority of hazardous accidents (Li and Song, 2015) . Public safety was the essential motive behind the development of this kind of network in the vehicles. Comprehending the security features of this networking strategy can further be beneficial in attaining its purpose (Mishra et al., 2016).

2. Literature Survey

Marvy B. Mansour et al. (2018) presented an outlook on the importance of Security and Privacy in the VANETs. The authors have also given the categorization of attacks that can be carried out on these kinds of networks. They suggested that this paper would be an essential overview

for all the researchers working for the fabrication of VANETs security features. Jadhao and Chaudhari (2018) demonstrated the design and analysis of Security Aware Routing mechanisms to enhance the security in VANETs while performing the routing process. The authors had first surveyed the efficacy of previously existing protocols and implemented a novel approach called the "Crypto Security System" to elevate the security functions (Jadhao and Chaudhari, 2018).

Wenjia Li et al. (2015) presented a scheme called "Attack-Resistant Trust Management (ART)" for VANETs. The authors suggested that this scheme would be beneficial in determining the reliability of Mobile nodes in the network. Different kinds of complex experiments were conducted to evaluate the efficacy of the above-discussed ART scheme. Patel and Jhaveri (2015), reviewed a variety of techniques to secure the routing mechanisms by adding security functions into the existing protocols. The authors claimed that securing the routing between the nodes in VANETs can be a challenging task as the attacks are getting evolved day by day (Patel, Jhaveri, 2015). Rashmi Mishra et al. (2016), reviewed the different security threats to which VANETs are vulnerable to. For that, the authors have presented the architecture of the VANETs to give an outlook to the inner mechanism undergoing these kinds of networks.

Sridevi Hosmani and Basavaraj Mathpati (2017) surveyed various Clustering Algorithms used in fabricating the Cluster-based Routing Protocols. The authors have evaluated the surveyed protocols based on the different parameters to study the efficiency staged by the various protocols in diverse situations. Sachin Godse and Parikshit Mahalle (2017) proposed a secure approach of transmitting the message through CBDS. The Authors have examined the performance of this proposed approach in a supported environment and saw the impeccable performance in reducing the latencies incurred. They also surveyed the previously existing secure routing protocols for fabricating a new approach for enhancing the security mechanisms (Godse and Mahalle, 2017). Chun-I Fan et al. (2014) presented with a novel methodology to preserve the privacy of the Driver and vehicular node in the VANETs. The authors proclaimed that their model has displayed elevated performance in maintaining the privacy of the node information without the interruption of routing functions.

Jared Oluoch (2016) implemented a model that can assist in the validation of the nodes in the Road Network through conditional probability methods. They also proposed that their model would be capable of providing an extra reliability check though the Road Side Units (RSUs). They claim that their model attained an accuracy of 90% in determining the malevolent data packer transfers. Osama Abumansoor and Azzedine Boukerche (2012) presented an ideal approach to verify the location of a node accurately utilizing a Cooperative mechanism. The authors evaluated their model against different scenarios for testing its performance. They learned that their model was able to alert the neighboring node at times of NLOS conditions. Tahani Gazda et al. (2012) proposed a model to address the variation in the Trust based Secure Routing Protocols. The authors implemented the mechanism of metric transition variation to monitor the movement of packets within the network of distant nodes. They also have inspected their model by simulating it against complex situations and compared it with other priorly existing similar models.

Sanjay K. Dhurandher et al. (2014) proposed a unique strategy to validate the credibility and the reputation of the sender node through the benign nature of the data packet transmitted. Periodic checks are implemented to have a piece of updated information about the node values. Tahani Gazdar et al. (2017), fabricated a methodology to improve the efficiency of existing Trust based Computing Protocol. The authors suggested a Distributed approach to enhance the functionality and robustness in detecting the malevolent vehicular node in the network.

3. Attacking Strategies in VANETs

Every single node existing in this kind of network needs to do functionalities of the routing devices as well as the functionalities of an End device (Chinnasamy et al., 2013). All the intermediary nodes need to process the information being shares to remain safe from threats and needs to forward the same information to the other vehicles beside them for alerting them (Abumansoor and Boukerche, 2012). In some cases, the information that is being passed through the network can be an illegitimate one and this might lead to unfavorable situations (Abumansoor and Boukerche, 2012). In this section, we will be discussing the different attacks which can be carried out on VANETs by exploiting its working mechanisms (Gazdar and Belghith, 2017).

3.1 Attacks targetting Availability

The availability feature of this system ensures that the required information and services must be accessible to the user in the network at any point of time without any delays (Godse and Mahalle, 2017). If the information is transmitted to the user after the occurrence of an accident, there won't be any benefit of using this technology (Mishra et al., 2016). So, for gaining the complete benefit out of this wireless networking, we need to make sure about lowering its latency levels to a minimum (Godse and Mahalle, 2017). Even little latencies in the case of vehicular networking can be very hazardous. There are many attacks implemented by the attackers to disable the availability feature of this kind of networks. One of the well-known attacks is the "Black Hole Attack" in which the attacker tries to inculcate a few illegitimate nodes into the pre-existing network. At the time of passing the information among the nodes, these nodes deny taking part in the process. In some cases, it might also drop the information packet from being transmitted further (Gazdar, Belghith, 2017). This would cause loss of the information in the routing process and the message wouldn't be reached to the other nodes. Another type of attack which disrupts the services is the "Broadcast Tampering" attack. This attacker is implemented by indulging misinformation in the network. Some other attacks of this category are "Greedy Drivers", "Denial of Service" and "Spamming".

3.2 Attacks targetting Authenticity

It is the process of validating whether a message received from another node during the transmission process is a legitimate user or not (Chinnasamy et al., 2013). It also checks whether the sender node is the same node which it is pretending to be. These attacks are carried out to trick the other users by sending information by spoofing the identity of another node to present

the topography (Gazdar and Belghith, 2017). The procedure of verifying the source is done as the first thing to assure the secure communication between the vehicular nodes. "Masquerading" is one of the well-known attacks which is implemented by compromising authenticity. It even actually absconds the identity of another node and performs the false routing process. Another type of attack which comes under this category is "Replay Attack". In this, the attacker takes hold of the transmitted message by the sender and alter it. After altering the message, it is then forwarded to the destination (Gazdar and Belghith, 2017). The user at the destination node would assume that the message is from a legitimate user. Some other attacks coming under this category are "Sybil attack", "Tunneling" and "Spoofing".

3.4 Attacks targetting Confidentiality

The messages transmitted between the nodes would be of confidential type. It shouldn't be made non- accessible to the attacker as they may take advantage of that. Consider for example, if an attacker is tailgating an individual while traveling through the vehicle. The attacker can gain the route traveled and the location of the victim by getting hold of the messages being transmitted from the victim's vehicle node. This process of illegitimate access to the information can be termed as Eavesdropping. These methods can also be used to gain knowledge about the system version and hardware put in deployment at the target's end. So, preserving the security of the transmitted is considered as a very significant step in secure routing (Gazdar and Belghith, 2017).

3.4 Attacks targetting Non-Repudiation

Every node subsisting in the topological network needs to have a unique identity to ensure that no node can deny their actions. For example, if a user behind a particular node in the topology has committed some illegitimate action and later, they may refuse to have done that action. So, it is essential to allocate a distinct identity address for every node present in the network (Gazdar et al., 2012).

4. Securing Mechanisms

The security in this kind of networking can only be achieved when the vehicular node can validate and process the transmitted data according to the nature of the message and reacting accordingly (Mansour et al., 2018). Individual nodes must efficiently be able to differentiate between the benign and the malevolent messages obtained (Li and Song, 2015) . The mechanisms which are blended in to elevate the security features can be categorized into two main classes of protocols, namely, Cryptography based, Trust-based and Hybrid protocols (Li and Song, 2015) .

5. Cryptography based Security Solutions

The first group of protocols is named after the cryptography, which signifies the art of encoding the messages (Patel and Jhaveri, 2015). This method aims at encoding the code in robust ways to ensure the confidentiality of the message by eliminating the access of illegitimate users

(Mishra et al., 2016). The protocols falling under this class assist the Hashing mechanisms, Digital Signatures, Encoding, and Decoding techniques for assurance of the security traits (Hosmani and Mathpati, 2017). The Cryptographic techniques can be further be classified into Symmetric and Asymmetric methods (Li and Song, 2015) . The Basic difference which exists between them is that the Symmetric Cryptographic methods utilize only one key and the Asymmetric methods utilize two keys, namely, public and private keys. In the first case consisting of only one key, the same key is applied for encoding as well as for the decoding purpose (Hosmani and Mathpati, 2017). But in the case of the second method, the public key is used for the encryption purpose, and for the decryption purpose, the private key is utilized (Mishra et al., 2016). The Private key in this kind of Encryption technique is only known to the corresponding User similar to that of passwords. They are revealed to others (Mishra et al., 2016). But the public key can be revealed to anyone. In the cases where the Asymmetric Cryptographic methods are deployed, the Keys involved in the procedure are managed by a specialized infrastructure known as Public Key Infrastructure (PKI) (Patel and Jhaveri, 2015). These can be referred to as a collection of Software, Hardware, and corresponding procedural elements. The Digital Signatures are blended with the messages before the initiation of transmission for assurance of the Authentication and Non-Repudiation. The Certificates would be unique for every individual and in case of a large number of users, the Certification Authorities (CAs) are put into action for dealing with the management of a large number of certificates (Mishra et al., 2016).

6. Trust-based Security Solutions

The next class of protocols is named after the term trust, which signifies the Reliability based on the protocols deployed (Li and Song, 2015) . It can be considered as an ancillary feature that is attached to the Cryptographic methods to further improve the securing properties in the network (Patel and Jhaveri, 2015). Different protocols falling under this category have been proposed by the various researchers in their work by contemplating the credibility of the “Sensor-Driven Techniques” and “Reputation-Driven Techniques” (Hosmani and Mathpati, 2017). The periodic credibility validations are done on the deployed routing mechanisms to check the effectiveness of Security in the network (Patel and Jhaveri, 2015). The trust mechanisms also implement a neighboring node-based method that works by the exchange of the credit report along its routing path (Patel and Jhaveri, 2015). If any of the nodes come to discover that any particular message being transmitted to be a malevolent one, then it begins to share with its respective nodes about the discovered results and make the whole topology to mark it as an illegitimate packet (Li and Song, 2015) . Even though these mechanisms are not capable of determining the exact identity of the sender to validate its authenticity, it can still be able to differentiate between the malicious and benign packets being routing from one device to another (Patel and Jhaveri, 2015).

7. Composite Security Solutions

Last class of protocols, which is assumed to be the efficient one among the other two for its combined properties of both the above-mentioned classes (Li and Song, 2015) . This is considered to stage better security characteristics because it blends the utilities gained from both the other class of protocols (Li and Song, 2015) . Many research works are still happening to discover these kinds of protocols for salient security maintenance.

8.Trust-based Security Protocols

Different Trust based protocols which enhance the security feature in the VANETs are:

MHLVP

"Multi-Hop Location Verification Protocol" aims to secure the routing procedures by verifying the identity of the other nodes by assisting the location feature (Abumansoor and Boukerche, 2012). This strategy of validating the vehicular node identity is attained by the employment of request exchange between the intermediary nodes until the source node is reached (Abumansoor and Boukerche, 2012). But in most of the cases, it staged the effective performance in the cases of localized transmissions. This type of validating methodology only works when the GPS functionality is enabled on the source node (Abumansoor and Boukerche, 2012). Otherwise, the protocol must be fabricated with distance calculating functions to determine the accurate position of a particular node by taking the number of nodes and the geographical map to considerations. The obstacles falling in between any two nodes may sometimes depreciate the communication channel formed between them (Abumansoor and Boukerche, 2012). This may also cause the stabilized signal loss. The RSD might be deployed to alleviate this problem. Consider an example, in which vehicles P and Q are separated by any obstacle, let's assume that these vehicles to be traveling in different lanes separated by building (Abumansoor and Boukerche, 2012). So, for communication between these two devices, a route path consisting of an intermediate vehicle node R is determined which will be a neighbor of both P and Q. When the Q receives the message through the assistance of the R node, it needs to resend a request to determine the position of the sender node for validation. Based on the node coordinates, an approximated position of the Sender can be determined through the construction of a triangle with three devices as its vertices (Abumansoor and Boukerche, 2012).

DAATM

This is a dynamic tool that can detect and eliminate malicious nodes from the network (Gazdar et al., 2012). It was capable of detecting the difference between the benign and the malevolent one by performing advanced inspection processes on the devices (Gazdar et al., 2012). Distributed Advanced Analytical Trust Model (DAATM) is a trust-based model that assists in dealing with the nodes by inspecting them on a different basis. Only the vehicles which can pass the metric test set up by this protocol will be able to stay within the network topology (Gazdar et al., 2012). The inspecting procedure has consisted of two main phases, namely, the initial examining phase and the provision of the collaboration value phase (Gazdar et al., 2012).

The first phase gets completed when the scan is completed by the protocol and then values called the collaboration value are assigned to every device based on its trustworthiness (Gazdar et al., 2012). This value must be periodically updated to its latest value according to its behavioral nature (Gazdar et al., 2012).

TMAODV

This protocol was presented by Integrating a Trust-based mechanism with the popularly known Routing protocol AODV (Chinnasamy et al., 2013). By utilizing this protocol, the Sinkholes present in the network can be easily identified and this protocol eliminates the utilization of these nodes at the time of the routing process. If these nodes are used in the process of routing (Chinnasamy et al., 2013), that may result in loss of data packets as sink nodes do not forward the packets coming to them (Chinnasamy et al., 2013). For determining the presence of Sinkhole in the network, this protocol sets up a strategy by broadcasting the Request messages to its nearest nodes until the destination is reached (Chinnasamy et al., 2013). In that procedure, the route containing the Sink nodes will not be able to reach the destination node (Chinnasamy et al., 2013). Therefore, those nodes can be avoided during the actual transmission (Chinnasamy et al., 2013).

VSRP

"Vehicular Security through Reputation and Plausibility" is a protocol to which validates the nodes based on some specialized Trust mechanism and Credibility check. When some vehicle needs to transmit any information through the network, the Source undergoes through an initial phase that performs the neighbor discovery process to determine all the neighboring nodes of the source node. Then based on the trust reference tables maintained by the neighboring nodes, it checks for the trust value of the source node. if the Source node is eligible to have a minimum trust level criterion, then the transmission is accepted. Otherwise, it would be denied.

DRS

"Distributed Reputation Scheme (DRS)" protocol was presented by the author for performing a situation-based Awareness activity among the vehicular nodes present in the topology (Oluoch, 2016). This protocol can be immensely beneficial to maintain the dependable values associated with nodes despite their continuous motion over the road (Oluoch, 2016). DRS allows the nodes to calculate the associate values of every corresponding node at all the time detecting for the change in values (Oluoch, 2016). As soon as it detects a change, the changed associate value would be broadcasted to the other nodes to make all the nodes in the network to store the updated value of the Source node (Oluoch, 2016).

EDTCP

EDTCP stands for "Enhanced Distributed Trust Computing Protocol". It is also a distributed structure-based trust validating protocol that assists in determining the credibility of the message being transmitted without the help of a Recommendation based system. This protocol

undertakes enhanced strategies to determine the activity of Eavesdropping and False message Transmission. While it detects the sign of some illegitimate activity to be happening in the network, it would soon eliminate the transmission and shares the information about the malicious node to other legitimate vehicular nodes existing in the network.

CSRP-TDA

"Channel State Routing Protocol Trust based Distribution Authentication" protocol executes by relying on globally available services which can be capable of eliminating the Collision attacks through prior detection of routing paths across the sender and the receiver nodes (Gazdar and Belghith, 2017). The proposed methodology proved to be an effective approach in dealing with the Inter and Intra Vehicular transmission problems. The CSRP present in the CSRP-TDA acts like an add-on for enhancing the quality deliverance during the transmission among the legitimate nodes (Gazdar and Belghith, 2017). "On-Board Units (OBUs)" are employed to recognize all the reliable node paths to use in the transmission process (Gazdar and Belghith, 2017). The state of the Channel is also considered as a significant feature to check for the trustworthiness of a particular node (Gazda and Belghith, 2017). This protocol can also be beneficial to deal with the latency issues and optimal energy consumption rates in the node devices.

Comparative Study of Trust-based Protocols

Table 1. Comparing the Trust-based protocols based on their Securing Mechanism

Protocol	**Securing Strategy Used**
MHLVP (Abumansoor, Boukerche, 2012)	Plausibility Check
DAATM (Gazdar et al., 2012)	Reputation System
TM-AODV (Chinnasamy et al., 2013)	Plausibility Check
VSRP [13]	Plausibility Check Reputation System
DRS (Oluoch, 2016)	Plausibility Check Reputation System
EDTCP [13]	Reputation System
CSRP-TDA (Gazdar, Belghith, 2017)	Plausibility Check Reputation System

Table 2. Comparative Analysis between Trust-based protocols on their PDR, Overload, and Scalability

Protocol	PDR	Overhead	Scalability
MHLVP (Abumansoor, Boukerche, 2012)	High	-	High
DAATM (Gazdar et al., 2012)	High	-	-
TM-AODV (Chinnasamy et al., 2013)	High	Average	-
VSRP [13]	Medium	Low	-
DRS (Oluoch, 2016)	High	-	-
EDTCP [13]	High	-	Low
CSRP-TDA (Gazdar, Belghith, 2017)	High	-	Low

9.Conclusion and Future Scope

VANETs are the vehicular networks consisting of vehicles as nodes for forwarding and processing of information transmitted through the network. There are many Routing protocols proposed for this approach for dealing with the transmission strategies. But the security concerned with these routing processes was a major issue. So, there came the need to introduce protocols to secure the communications taking place among the nodes. First, we have discussed a diverse range of attacking strategies on the VANETs. Then, we have conducted a comparative study between different Trust-based Secure Routing Protocols to determine the efficacy and features possessed by each of them. Even though the field of VANETs has adhered to numerous advancements, still many confrontational issues need to be addressed. One of the well-known issues related to the VANETs is regarding the Privacy of Location issue. The attacker can be able to track the location of a victim's vehicle by becoming a part of the network. Also, another issue is regarding the attacks based on Location spoofing by assisting the GPS facility to manipulate the users by transmitting false information. The protocols for VANETs must be carefully designed by incorporating the security features along with the Routing procedures.

References

Abumansoor, O. and Boukerche A (2012), 'A Secure Cooperative Approach for Nonline-of-Sight Location Verification in VANET', *IEEE Transactions on Vehicular Technology*, Vol. 61 No. 1, pp. 275-285. doi: 10.1109/TVT.2011.2174465.

Chinnasamy, A., Prakash, S., and Selvakumari, P. (2013), 'Enhance Trust based Routing Techniques against Sinkhole Attack in AODV based VANET', *International Journal of Computer Applications,* Vol 65 No. 15., pp. 22-27.

Dhurandher, S. K., Obaidat M. S., Jaiswal A., Tiwari A., and Tyagi, A. (2014), 'Plausibility Checks', *IEEE Systems Journal*, Vol. 8 No. 2, pp. 384–394.

Fan, C., Sun,W., Huan, S., and Huang, J. (2014), Strongly Privacy-Preserving Communication Protocol for VANETs, *2014 Ninth Asia Joint Conference on Information Security*, Wuhan, China, pp. 119-126,

Gazdar, T. and Belghith, A. (2017), 'An Enhanced Distributed Trust Computing Protocol for VANETs', *IEEE Access*, Vol 4c, pp. 1–14. doi: 10.1109/ACCESS.2017.2765303

Gazdar, T., Rachedi, A., Benslimane, A., and Belghith A. (2012), "A distributed advanced analytical trust model for VANETs", *2012 IEEE Global Communications Conference (GLOBECOM),* Anaheim, CA, pp. 201-206,

Godse, S. and Mahalle, P. (2017), "Using CBDS", *2017 International Conference on Computing, Communication, Control, and Automation (ICCUBEA)*, Pune, India, pp. 1–6.

Hosmani, S. and Mathpati, B. (2017), "Survey on cluster based routing protocol in VANET", *International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, Mysuru, India, pp. 1-6.

Jadhao, A. P. and. Chaudhari, D.N. (2018), "Security Aware Routing Scheme In Vehicular Adhoc Network", *2nd International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, India, pp. 1374–1379.

Li, W. and Song, H. (2015), 'ART : An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks', *IEEE Transactions On Intelligent Transportation Systems,* Vol. 17 No. 4, pp. 1–10.

Mansour, B. M., Salama, C., Mohamed, K. H., and Hammad, S. (2018), 'VANET Security and Privacy - An Overview', *International Journal of Network Security & Its Applications*, Vol. 10 No. 2, pp. 13–34. doi: 10.5121/ijnsa.2018.10202.

Mishra R., Singh A., and Kumar R. (2016), "VANET security: Issues, challenges and solutions", *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT),* Chennai, China, pp. 1050-1055.

Oluoch, J. (2016), "A distributed reputation scheme for situation awareness in Vehicular Ad Hoc Networks (VANETs)", *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, San Diego, CA, pp. 63-67.

Patel, N. J. and Jhaveri, R. H. (2015), 'Trust-based approaches for secure routing in VANET : A Survey', *Procedia - Procedia Computer Science*, Vol. 45, pp. 592–601. doi:10.1016/j.procs.2015.03.112