Indian Journal of Science and Technology, *Vol 10(17), DOI: 10.17485/ijst/2017/v10i17/112343, May 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Trusted and Secured Routing Protocol for Vehicular Ad-Hoc Networks

Debasish Roy and Prodipto Das

Department of Computer Science, Assam University, Silchar – 788011, Assam, India; debasish.aucs@gmail.com, prodiptodas@gmail.com

Abstract

Objectives: To establish a trust based secured routing protocol to accurately distinguish malicious nodes that are dropping the important information and modifying the routes. Efforts are made to identify malicious nodes such as route modifiers and packet droppers. **Methods/Statistical Analysis:** Vehicular Ad-hoc NETworks (VANETs) is a modern technology which help a vehicle and a driver in several ways. The main characteristics of VANETs are nodes i.e. vehicles with relatively high mobility and constantly changing topology. In case of data communication in VANETs, a source node must depend on the intermediate nodes to send its data packets to the destination node on multi-hop routes. VANETs can give better performance if all its nodes work properly with full cooperation during the communication. In VANETs, a node can generate and broadcast important and essential messages to other nodes in the network for safety reason. However, the generated message by a vehicle may not be reliable every time. In this paper we have proposed a trusted and secured routing protocol that evaluates the trust of a vehicle and also checks the message reliability. The proposed protocol is named as Trusted Vehicular Ad-hoc On-demand Distance Vector (TVAODV) routing protocol which is the modification of Ad-hoc On-demand Distance Vector routing protocol. Since VANETs are mostly attacked by the malicious nodes; therefore better security solution is needed to stop such attacks. The proposed protocol introduces a trust model to establish a malicious node free route for source node to send its data packets to the destination node on multi-hop routes. **Findings:** The TVAODV protocol is simulated in Network Simulator (NS2) to check the performance and accuracy and also compared to AODV routing protocol. It is found that TVAODV is comparatively better in performance when VANET is in high mobility and versatile topology. The performance of the proposed protocol is evaluated using performance measurement metrics: average end-to-end delay, throughput, routing load and packet delivery ratio. The proposed protocol performance is evaluated in the presence of malicious (route modifiers and packet droppers) vehicles and the results shows that the proposed protocol is achieved better accuracy and it shows better performance compared to AODV routing protocol. **Application/Improvements:** The proposed protocol may be useful in the process of developing a better traffic management and transportation system. In this paper we have proposed a TVAODV routing protocol which includes trust model to evaluate the trust of vehicles as well as to establish a malicious free route.

Keywords: AODV, NS2, Packet Delivery Ratio, Routing Load, Throughput, TVAODV, VANETs

1. Introduction

The part of Mobile Ad-hoc NETwork MANET is Vehicular Ad-hoc NETworks (VANET)[1]. VANETs are composed of roadside infrastructure and sensor nodes are installed within vehicles. VANETs are characterized by high mobility and fast topology change, partitioning or fragmentation frequently etc[2]. For these reasons VANETs require effective security solutions. Security is crucial due to lack of centralization and dynamic topology. One of the main issues in VANETs is security and key element of security is trust[3]. In VANETs to get better security the trust plays an important role. Authentication is one of the security solutions to find the integrity of message transmitted[4]. VENETs are attacked by the malicious nodes[5]. In VANETs vehicles can generate and broadcast messages about road condition, accident and traffic etc[6]. These types of messages are called road related message.

**Author for correspondence*

These are helpful for safety drive and also to take any road related decisions because they already aware of the situation ahead of them. These massages are helpful provided they are not false messages. Therefore, the entire VANET depends on the reliability of the messages or nodes. So, how a vehicle should decide whether the incoming message is true or not? Or whether the vehicle generated message is reliable or not? In VANETs, a malicious node can broadcast false messages and can divert other vehicles in wrong direction. Therefore, to stop such activities an effective trust management scheme is required for VANETs. In this paper we have addressed this problem of selection of reliable or trusty vehicles i.e. to establish a malicious node free route by proposing a trust based model for VANETs. We have evaluated the reliability and trustworthiness of the message or the vehicle based on the trust metrics of that message or the vehicle.

The remaining part of the paper is organized as follows: In section 2 the existing works are reviewed for trust establishment in VANETs. In section 3 we have discussed about the proposed trust model for secure routing in VANETs. In section 4 we have proposed an algorithm for trusted and secured routing in VANETs. In section 5 the simulation and configurations of the simulations are discussed. In section 6 we have discussed about the performance metrics. Section 7 discussed about simulation results and the results are compared with AODV protocol. The theoretical comparisons with other reactive and hybrid protocols are given in same section for better acceptability. Conclusion is given in section8. Finally, the future work is given in section 9.

2. Existing Method

VANETs can make our road journey safe. To deploy VANETs universally, it is important to solve the security issues in VANETs. All the messages must be securely communicated by vehicles. During the past few years, intensive research works has been done by the researchers and numerous research papers have been published addressing the security issues in VANETs. In this section we have discussed some of them.

In[7] proposed an algorithm for Vehicular Security through Reputation and Plausibility (VSRP) check. The VSRP detect and eliminate the malicious node using trust value of the nodes. Neighbor table, Trust table, Req seen table, Data table, Temp table are maintained by the each node in the network. The trust values are changing frequently based on the reputation of that node. The algorithm follows an event oriented approach. Data aggregation and data dropping are also handled by VSRP algorithm. Drawback of this algorithm is that it has information of only the neighboring nodes, whole network situation being not considered. In future the authors wish to extend VSRP to work well in automatic toll collection, entertainment and location based services.

In[8] proposed a trust model which is based on Markov chain. Each vehicle monitoring its neighboring vehicle trust and also update trust based on their behavior in network. Misbehaving and selfish nodes are detected through this model. To manage the trust, two parameters are used: trust interval and number of transactions. The authors plan to establish global trust metric in future.

In[9], proposed a trust propagation scheme in VANETs. The main focus is to enhance the trust propagation in VANETs. They have introduced the attribute similarity concept in case of forwarding the data packets. This scheme improves the packet delivery or the reliability of packet forwarding in multi-hop routing.

In[10] proposed a Dynamic Trust Token (DTT) based scheme for enhancing the cooperation of the nodes in VANETs. It uses both the symmetric and asymmetric cryptography to maintain the integrity of the data packets. It also executes the Neighborhood Watchdog algorithm that generates tokens for identifying the correctness of the packets. Their main focus is set up an instant trust depending on the performance at runtime to enforce well cooperation among nodes, detect the malicious nodes and maintain packet integrity during transmission. It is a passive detect and prevent approach. Drawback of this solution is the transmission range problem i.e. if there is absence of relaying nodes within the transmission range.

In[11] proposed scheme for safety message authentication based on ID-based proxy signature with Elliptic Curve Digital Signature Algorithm (ECDSA) and verification methods. Certificate-less public key verification is done by ID-based method. Proxy signature provides the authentication of message and managing the trust. Safety messages are delivered through Road Side Unit (RSU). Trust is managed by the RSU. Proxy signature is presorted in RSU.

In[12] proposed a dynamic public key infrastructure (PKI) for VANETs which is based on the trust model and distributed clustering algorithm. The clustering algorithm selects the cluster head on the basis of two metrics: security in terms of trust and mobility. Trust metrics represent

trust level of a vehicle and the mobility metric represents a vehicles relative velocity. An approach is used to protect the Cluster Head (CH); it is done through forming a VANET Dynamic Demilitarized Zone (VDDZ) where each vehicle is fully trusted. The Authentication of each vehicle within each CH is provided by the Registration Authority (RA).

In[13] proposed event based reputation model for finding the false information. A dynamic role based reputation mechanism, used to identify the incoming message is significant and trustworthy to the driver. It enhances the trust for VANETs. In future, the authors have a plan to include fuzzy theory to calculate the reputation score of an event.

In[14] proposed to determine the accuracy of the Vehicle to Vehicle (V2V) incident reports based on trust of the report generator and forwarded nodes. To get the detailed view of the vehicle trustworthiness Vehicle to Infrastructure (V2I) communication approach is used to collect the vehicle behavioral information in crowdsourcing fashion. Here each vehicle needs to make decision upon the incident report: Whether to accept and if accepted, an endorsement opinion. These two decisions are made based on the report originator and forwarders trust value. Global trust is aggregated by the central authority in V2I communication. In the future work the authors plan to improve the overhead during communication, impact of unreliable communication channel and infrastructure development cost.

In[15] proposed Vehicle Ad-Hoc network Reputation System (VARS) based on the situation oriented reputation level. They have defined three areas: event area, decision area and distribution area. Event area for recognizing the event, decision area to decide the trustworthiness of event message and distribution area defines how much distance the messages can be distributed. The opinions about the message trustworthiness are collected during the forwarding of message. Every forwarding node will append their own opinion about the message while they distribute it. It is known as opinion piggybacking. Direct and indirect trust is used for getting the reputation information.

In[16] proposed hybrid trust model to determine the vehicles trust metric. Two aspects are used for trust monitoring: vehicle cooperation and broadcast legitimate data. To decide the honesty of the vehicle, fuzzy theory is used. The vehicle having lowest relative mobility is elected as a Certification Authority (CA). Each vehicle monitors all its neighbors and calculates their trust value. The vehicle behavior is evaluated through the monitored vehicle's cooperativeness and the legitimacy of information that it broadcasts.

In[17] proposed geo-location based trust for VANETs and establish a set of privacy requirements, proposing a mechanism beyond pseudonyms. Privacy mechanism is provided through mandatory access control model and a novel method is used to propagate the trust information which is based on vehicle's geo-location.

In[18] proposed a new trust architecture based of the situation called Situation Aware Trust (SAT). It includes three components mainly: attribute based policy control model, proactive trust model and prevent the breakage of existing trust. Identity based cryptography method is used to integrate entity trust, security policy enforcement etc. It uses the proactive approaches for trust establishment. In future, the authors plan to use cloud computing method to deploy global and local trust.

In[19] proposed trust opinion aggregation scheme to establish trust in VANETs. This is used to evaluate the quality of the shared message. They have used multiple existing identity based aggregation methods and combined them into one. This is the extension of existing identity based aggregate signature algorithm, it combines the signatures in multiple messages into one aggregate signature and eliminate redundant signature. Therefore, achieved both time and space efficiency is achieved. In future, the authors plan to use variable length encoding algorithm.

In[20] proposed a protocol for detection of malicious nodes and remove those nodes from the Vehicular Networks (VNs). The method is a combination of: 1. infrastructure based revocation protocols and Revocation of Trusted Components (RTC), Revocation using Compressed certificate Revocation Lists (RC2RL), 2. Misbehavior Detection System (MDS) (c) Local Eviction of Attackers by Voting Evaluators (LEAVE) protocol. Malicious nodes are detected using MDS and a distributed eviction protocol.

In[21] proposed Beacon based Trust Management (BTM) mechanism to stop the internal attacker to spread false information in privacy enhanced VANETs. The method checks both event message and beacon message to decide the message trustworthiness. Cryptography method is used to protect messages and pseudo identity scheme is used to achieve privacy. They have evaluated the system under the Fixed Silent Period (FSP) and Random Silent Period (RSP) scheme. The method is based on evaluating

the direct event based trust, indirect event based trust and combining trustworthiness.

In[22] proposed a trust model based on the ATTACk Resistant trust Management (ART). It is able to find the malicious node and to deal with them. It evaluates trustworthiness of both data trust based on the data sensed, data gathered from vehicles and node trust based on the calculation of functional trust and recommendation trust.

In[23] proposed a trust model for multicast Mobile Ad-hoc NETworks (MANETs). It is two steps authentication approach: to determine the Trust Value (TV) of each one hop neighbor using markov chain trust model and Central Authentication (CA) server is selected within a group based on the node with the highest trust value. Backup CA server is selected based on the second highest trust value to increase reliability.

In[24] proposed trust mechanism RaBTM based on Road Side Unit (RSU) and beacon. The goal is to spread the message opinions quickly and stop the internal attackers from sending or spreading false information. Crosschecking is done on both the beacon and event message to determine the most trust worthier message and instantly send the opinion to others. Trust evaluation is based on: direct, indirect and hybrid. In this method vehicle can get reliable opinion from RSUs. The system used both cryptography and pseudo identity algorithm.

In[25] proposed trustworthy privacy preserving method for the announcements generated by the vehicles. It is secured from the both internal and external attackers. Internal attackers are detected through endorsement method based on the threshold signature. Three types of privacy preserving technique are defined to preserve the privacy of the vehicles during trustworthy announcements. First one is better suited for dense VANETs, whereas in case of fallbacks for sparse VANETs second and third is used. To reduce the verification cost a priori protection paradigm is used.

In[26] proposed Optimize Node Selection Routing Protocol (ONSRP) based on the trust evaluating algorithm. Analyzed the trust computing algorithm to find the time complexity and tries to find the large packet delivery ratio. ONSRP is developed to evade the link failure and routing loops. For each node based on distance it stores a flag trust value in its routing table. To calculate the trustworthiness of data direction and velocity of nodes are used. The method is compared with the Scalable Hybrid Routing (SHR) and finally shows that ONSRP performs better than SHR in presence of link failure with better packet delivery ratio.

In[27] proposed a trust model for effective communication in VANETs. The authors aim was to find out the trustworthiness of the agents of other vehicles. They have developed a multifaceted trust model that consists of role, experience, priority and majority based trust. Future plan as mentioned is to use the commuter pool, the number of agents travel through the same route at the same time.

3. Trust Model for Secure Routing in VANET

3.1 Overview of Trust

Trust[28,29] is the belief that someone or something is reliable, honest etc. The meaning of trust varies with different context. In networks trust is the important part of relationship among nodes. In our trust model, Trust Initiator is the node that is evaluating the trust. Trusty refers to the node whose trust is being evaluated. Recommenders are the expectation of the Trust Initiator nodes those can give honest and unbiased recommendation on a specific Trusty.

3.2 Trust Quantification

Trust quantification means how much trust may have a Trust Initiator node on the Trusty node. In our trust model, we quantified trust value with continuous real number between 0 and 1. The degree of trust is shown in Table 1.

3.3 Trust Computation

In our trust model TVAODV, we have calculated two types of trust. One is direct trust and the other is recommendation trust. Direct trust is calculated based on the

Table 1. Degree of trust.

Trust Level	Trust Value	Semantics
1	0	New or Unknown
2	0.1 – 0.2	Very Low Trustworthy
3	0.3 – 0.4	Low Trustworthy
4	0.5 – 0.6	Medium Trustworthy
5	0.7 – 0.8	High Trustworthy
6	0.9 – 1.0	Very High Trustworthy

direct experience of the trust initiator upon the trusty node. Recommendation trust is calculated based on the recommendation given by the recommender nodes upon the trusty node. The types of trust computations are shown in Figure 1.

In Figure 1 node X represents the Trust Initiator node, node Y represents the trusty node and the node Z represents the recommender node. The dotted lines indicate the indirect path between the trust initiator node and the trusty and it signifies recommendation. The solid line indicates the direct path between the trust initiator node and the trusty and it signifies direct trust.

3.3.1 Direct Trust Evaluation

Direct trust is evaluated based on the direct previous experience that the trust initiator node may have on the trusty node. The trust initiator node may have large numbers of direct experience and these can be either positive experience or negative experience. All the experiences are not having the same importance level. There are some experiences which are having more importance level than that of others. Each message will have some importance or risk. Say, in case of VANET, experience for accidental alert and experience for searching parking slot are not having the same importance level.

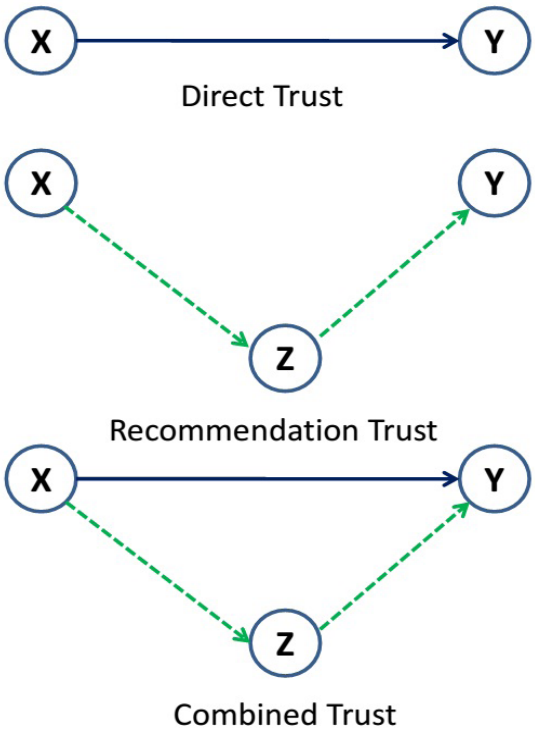

Figure 1. Trust Computation for VANET.

In our trust model TVAODV, the direct trust evaluation TE_D is evaluated through eq. 1 if the value of TE is greater than equal to 1.But if TE<1 then there is no direct previous experience between nodes and in that case the value of TE_D becomes Zero.

$$\mathbf{TE_D} = \mathbf{round}\left(\frac{\sum_{i=1}^{n} \mathbf{W}_i \times \mathbf{PE}_i}{\mathbf{TE}}\right) \quad (1)$$

Where, TE is the total numbers of various experiences that the trust initiator node may have on the trusty node, W_i represents the weight of this experience which reflects the importance level. PE_i represents the number of positive experiences. The value of PE is 1 if experience i is positive.

Here weight W_i place an important role for increasing and decreasing the trust value. The values of W_i lies between continuous real number 0 and 1 ($W_i \in [0,1]$) which is predefined. Important experience with large weight may have larger impact on the trust value even if there are small numbers of such experiences.

About the positive experience say, if the alert message sent by the trusty node is confirmed then the trust initiator node takes this experience as positive experience in its direct trust evaluation. The positive experiences are may not just limited to alert message there are lots of other cases, here it is just only said about one of such case.

The round function is rounding the decimal value to the nearest tenth. The round function is used to make the value within range 0 to 1, as specified in Table 1.

3.3.2 Recommendation Trust from other Surrounding Nodes

When the trust initiator node does not have adequate previous direct experiences with trusty node to satisfy the trust requirements, the trust initiator node may generate queries to other nodes in the network i.e. the recommender nodes to give recommendation about trusty node. Here we have assumed that the recommender nodes are already having some trust value TV_i about trusty node on the basis of its own evaluation. The trust initiator nodes may query several nodes in the network for accurate evaluation. The recommendation trust value TV_R is evaluated using eq. 2.

$$\mathbf{TV_R} = \frac{\mathbf{1}}{n}\sum_{i=1}^{n}(\mathbf{TE_{Di}} \times \mathbf{TV_i}) \quad (2)$$

Where, TE_{Di} is the direct trust value that the trust initiator node has upon recommender node.

3.3.3 Direct and Recommendation Trust Combination

When the trust initiator node has the both direct and recommendation trust upon trusty node then we have used the following combined trust $T_{combined}$ equation to evaluate the trust score.

$$T_{Combined} = TE_D + (1 - TE_D) \times TV_R \quad (3)$$

$$(0 \leq TE_D \leq 1 , 0 \leq TV_R \leq 1)$$

- If TE_D =1, the trust initiator is having sufficient value to satisfy the trust requirements, so it will not depend on the Recommendation Trust value. In that case the trust initiator will not enquiry for recommendation trust value.
- If TE_D =0, the trust initiator node will completely depends on the value given by the recommender nodes about the trusty.
- The more trust value got by the trust initiator node from the direct interaction less recommendation trust value is required for to satisfy the trust requirements and vice versa.

3.3.4 Trust Decision

In our trust model TVAODV, the final trust or trust decision TD is evaluated based on eq. 4.

$$TD = T_{Combined} - TR_{Threshold} \quad (4)$$

Where, $TR_{Threshold}$ is the trust risk threshold value for any ongoing tasks. In other words, how much risk we can take for that ongoing task. So, threshold value is needs to be defined for each task. For example say, every important message like accident alert require at least high trustworthy value which is starts from .7 given in Table 1.

- If TD >= 0, means evaluated trust value satisfies the trust requirement of ongoing task.
- If TD<0, means evaluated trust value does not satisfy the trust requirement of ongoing task.

3.3 Maintaining Trust Information

In our trust evaluation model TVAODV, the trust evaluation is performed by each node locally. The trust information table must be maintained by each node and the table may contain the information about trusty node's ID, Direct Trust Value, Recommendation trust Value and Combined trust value. The trust information may be refreshed periodically. The information will be expired if it is not refreshed within the period of time t as assumed by the network and the corresponding trust value will become Zero i.e. the initial value.

4. Proposed Algorithm

4.1 Direct Trust Calculation

If a source node, say A needs to send information to the destination node say D then source node A or monitored node will evaluate the direct trust to its neighbor node say B using eq. 1.

4.2 Recommendation Trust Evaluation

If a source node or monitored node, say A has more than one hop neighbors between it and the trusty node, then the recommendation trust value will be evaluated through eq. 2.
Else {
Recommendation trust value for trusty node set to 0.
}

4.3 Combined Trust

If a source node or monitored node gets both direct trust and recommendation trust of the trusty node then it will evaluates the trust value using eq. 3.
Else {
Combined trust value set to 0.
}

4.4 Vehicle Behaviour Evaluation Based on Cooperativeness Algorithm

Step 1:
If a monitor node, say X finds a monitored node say Y trusty from the trust table then X will send data packets to Y.
Packet Received = Packet Received + 1.
Else if Y unable to receive then {
Packet Received =Packet Received – 1.
}

Step 2:
If X finds that Y forward the packet successfully then {

Packet Forward = Packet Forward + 1.
}
Else {
Packet Forward = Packet Forward – 1.
}

Step 3:
The Rate of forwarding of data packets F_{Rate} is evaluated using eq. 5.

$$F_{Rate} = \frac{FM}{TM} \quad (5)$$

Where FM represents the number of messages forwarded by the monitored node and TM represents the total number of messages transmitted by the monitor node.

Step 4:
If the value of F_{Rate} is equal to 0, then it indicates the monitored node is malicious node.
Else if the value of F_{Rate} is equal to 1, then it indicates the monitored node is not malicious.
Else {
The monitored node may or may not malicious.
}

4.5 TVAODV Algorithm

An algorithm for trust based and secured routing in VANET.

Step 1:
Route discovery process starts if a source node needs a valid route to some destination nodes. The source node will sense its entire neighbor and take those are having the evaluated Trust Decision (TD) value satisfied the trust requirements. Source node will then broadcast the Route REQuest (RREQ) packet to all such neighbors. The neighboring nodes also does the same process to broadcast its RREQ packet to their neighbor and so on until the destination node reached or an intermediate node with afresh enough route plus TD with satisfied trust requirement to reach the destination node is found.

Step 2:
When the RREQ packet arrives at the destination or intermediates with fresh enough route, the destination or intermediates replied by unicasting a Route REPly (RREP) packet back to the neighboring node from which the RREQ was first received. When the source node received the RREP packet the complete path is established. The source node may now starts data transmission.

Step 3:
Source node sent data packets to the destination node. The destination node will give a confirmation message.

Step 4:
If a source node gets confirmation message from destination node within preferred time interval t.
{
Source node will continue to transmit data through this route.
}
Else {
Check if any intermediate nodes playing the role of malicious using the vehicle behavior evaluation based on cooperativeness algorithm then Set the trust value for that malicious node to 0 (zero).
Else {
Source node will update the trust table with decreasing trust value.
}
Source node will select the next best route to send the data, go to Step 1 and Repeat.
}

5. Simulation Configuration

The performance of the TVAODV protocol is evaluated using the Network Simulator (NS2). To configure the simulation environment the parameter used are given in Table 2.

Simulation scenario with 150 numbers of nodes is shown in Figure 2.

6. Performance Measurement Metrics

To evaluate the performance of proposed model we used the metrics: Average End-to-End Delay, Throughput, Routing Load and Packet Delivery Ratio.

6.1 Average End-to-End Delay

It is the time taken by a data packet to arriveata destination node. It also includes the delay caused by route discovery process, queue in data packet transmission, MAC level retransmission and the time taken during propagation and transfer[30]. The average end-to-end delay is calculated using eq. 6.

Table 2. TVAODV simulation parameter.

Parameter	Value
Routing Protocol	TVAODV
Channel Type	Wireless Channel
Number of Nodes	100, 150, 200
Transport Protocol	UDP
Interface Queue Type	Queue/DropTail/PriQueue
Queue Length	50 Packet
MAC Type	Mac/802_15_4
Mobility	Random way point
Transmission Range	250 meter
Speed	70, 80, 90 and 100 km/h
Area of Simulation	9570 m X 8758 m
Maximum Bandwidth	1Mbps
Simulation Time	500 sec
Traffic	CBR
$TR_{Threshold}$	0.6

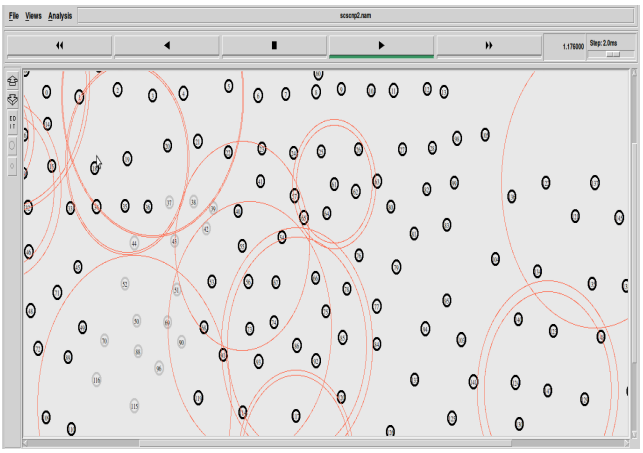

Figure 2. Simulation scenario with 150 nodes.

$$Avg_{EtoE_{Delay}} = \frac{1}{T_{success}} \sum_{i=1}^{n} (rec_i - sent_i) \quad (6)$$

Where $T_{success}$ is the successfully received packets, i is the unique packet identifier, rec_i is the time of i^{th} packet received and $sent_i$ is the time when it was sent.

6.2 Throughput

Number of bits receives by destination node per unit time. It is measured in kilo bits per second (kbps)[31]. The throughput is calculated using eq. 7.

$$\text{Throughput} = \frac{\text{Received Size}}{\text{End Time} - \text{Start Time}} \times \frac{8}{1000} \quad (7)$$

Where, 'End Time-Start Time' is the transmission period of data.

6.3 Routing Load

Number of routing packets transmitted per data packet delivered at the destination[32]. The routing load is calculated using eq. 8.

$$\text{Routing Load} = \frac{\text{No. of Routing Packets Sent}}{\text{Data Packets Received}} \quad (8)$$

6.4 Packet Delivery Ratio

It is the ratios of the number of packets that are successfully delivered to destination compared to the number of packets have been sent by the sender[33].The Packet Delivery Ratio (PDR) is calculated using eq. 9.

$$PDR = \frac{\text{Received Packets}}{\text{Sent Packets}} \times 100\% \quad (9)$$

7. Simulation Results, Analysis and Discussion

Simulation results are shown in Figures 3-8 using gnu plot line graph. In our simulation we have used percentage of malicious node in case of both AODV and TVAODV protocol to compare the performance of both the protocols. As shown in Figure 3, we have evaluated the accuracy, scalability of the TVAODV protocol by increasing the number of malicious vehicles and also by increasing the total number of vehicles. The worst case of the scenario is when 90% of the vehicles are malicious and they are dropping the original message or spreading the false message, in that case our TVAODV protocol is able to achieve accuracy approx 60%, i.e. our TVAODV protocol is able to fairly differentiate approx 60% of the cases. When 10% of the vehicles are malicious, our TVAODV protocol achieves accuracy approx 97%.

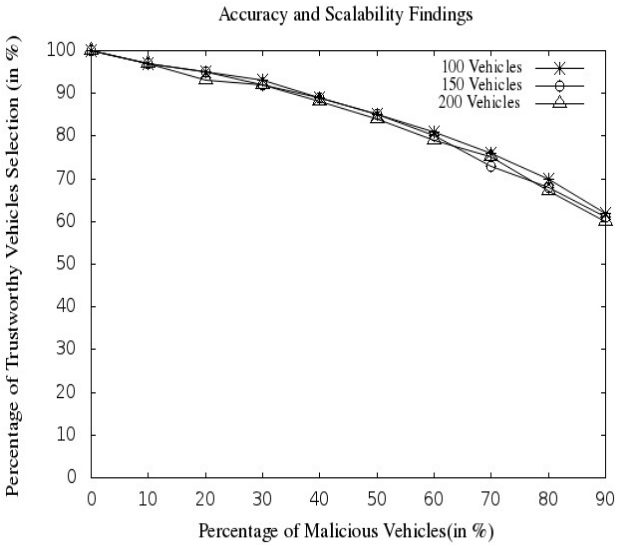

Figure 3. TVAODV accuracy and scalability findings.

As shown in Figure4, we have evaluated the Packet Delivery Ratio of the AODV and TVAODV protocol based on the increase in percentage of malicious (route modifier) vehicles. Figure 4 shows that our TVAODV protocol performs better than AODV protocol because of trustworthy route selection. In the worst case scenario, where 90% of the vehicles are malicious our TVAODV protocol shows Packet Delivery Ratio approx 61%. When 10% of the vehicles are malicious, our TVAODV protocol shows PDR approx 95%.

As shown in Figure 5, we have evaluated the Packet Delivery Ratio of the AODV and TVAODV protocol based on the increase in percentage of malicious (packet dropping) vehicles. Figure5 shows that our TVAODV protocol performs better than AODV protocol because of trustworthy route selection, selection of trusted vehicle. In the worst case scenario, where 90% of the vehicles are malicious our TVAODV protocol shows Packet Delivery Ratio approx 59%. When 10% of the vehicles are malicious, our TVAODV protocol shows PDR approx 94%.

As shown in Figures 6-8, we have evaluated the throughput, End-to-End Delay and Normalized Routing Load of the AODV and TVAODV protocol based on the increase in percentage of malicious vehicles. The Figures 6-8 shows that TVAODV protocol performs better than AODV protocol in all the cases. In the worst case, where 90% of the vehicles are malicious, our TVAODV protocol shows Throughput approx 14 Kbps, End-to-End Delay approx 52 millisecond and NRL approx 65. When 10% of the vehicles are malicious, our TVAODV protocol shows

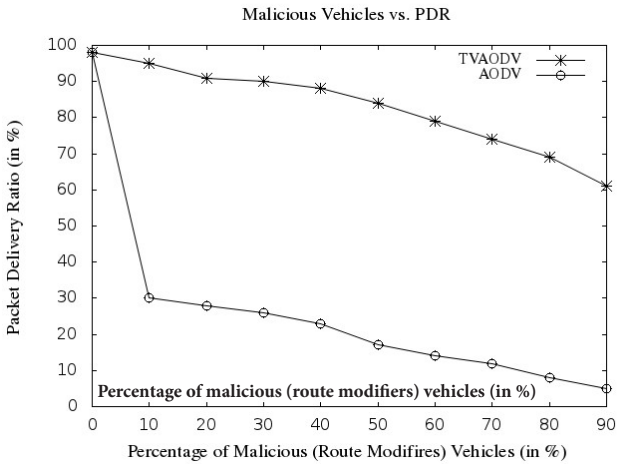

Figure 4. Route modifier vs. PDR.

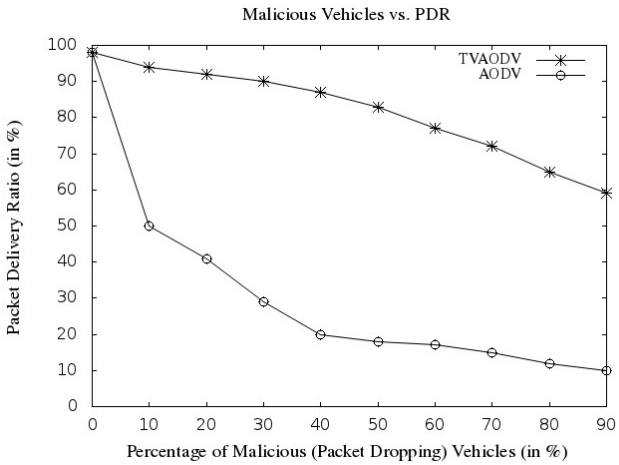

Figure 5. Packet dropping vs. PDR.

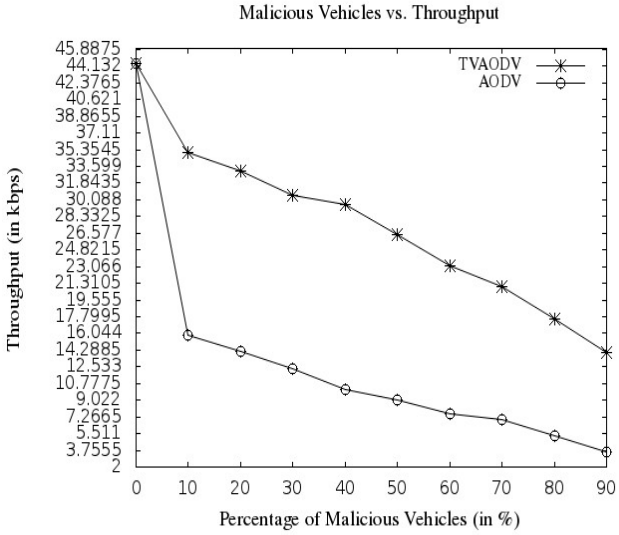

Figure 6. Malicious vehicle vs. throughput.

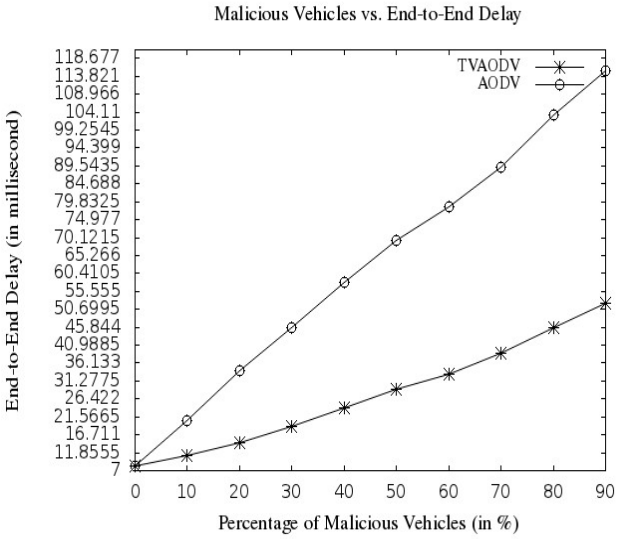

Figure 7. Malicious vehicle vs. end-to-end delay

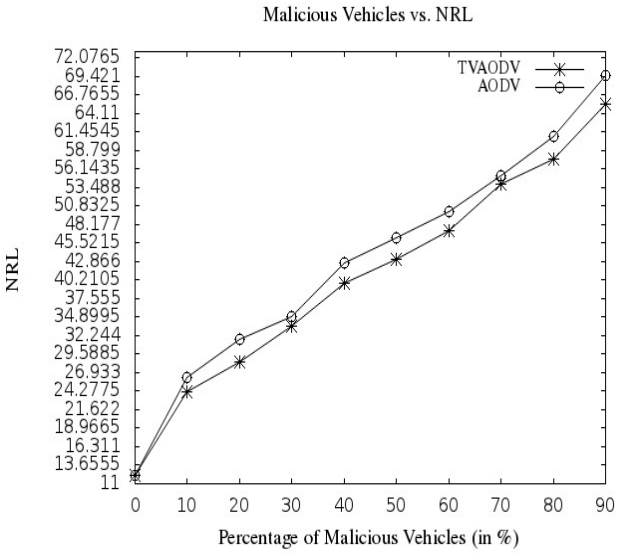

Figure 8. Malicious vehicle vs. NRL

Throughput approx 35 Kbps, End-to-End Delay approx 11 millisecond and NRL approx 24.

8. Conclusion

In this paper we have modified the AODV routing protocol named as TVAODV. Both the AODV and TVAODV protocol are used in vehicular environment to find out the performance. The simulation shows that our TVAODV protocol performs better than AODV protocol. In this paper trust evaluation mechanism is used to avoid routing attacks. In this paper we have presented accuracy, scalability and other performances of the TVAODV routing protocol. The protocol shows approx 60% accuracy in presence of 90% malicious vehicles and approx 97% accuracy in case of 10% malicious vehicles. Regarding scalability, with the increase in size (total number of vehicles) of VANET the accuracy of our TVAODV protocol does not decrease so much, it is nearly the same.

9. Future Work

In future, a more improved trust model can be developed to find the better security. The proposed model can be used in other WSN routing protocols to find out the performances. In future global trust table may be introduced to enhance the proposed model performances. A modified cryptography method may be added along with trust model to achieve more security. A cluster based model can be developed along with the trust model for to get better performance in vehicular communication.

Since TVAODV is a modified version of AODV protocol, TVAODV is also reactive protocol. Therefore it is of no use to compare TVAODV with proactive routing protocols. There are various reactive routing protocols in literature for example Associativity Based Routing (ABR), Dynamic Source Routing (DSR). The TVAODV may be compared with hybrid routing protocols too. Zone Routing Protocol (ZRP) is one of the popular hybrid routing protocols. This comparative analysis can be done as a future work of this paper.

10. Acknowledgments

Our thank to the funding program for research, Rajiv Gandhi National Fellowship (RGNF) for SC/ST Candidate funded by Ministry of Social Justice and Empowerment and Ministry of Tribal Affairs.

11. References

1. Patel NJ, Jhaveri RH. Trust Based Approaches for Secure Routing in VANET: A Survey. Elsevier International Conference on Advanced Computing Technologies and Applications (ICACTA); 2015. p. 592-601. Crossref
2. Blum JJ, Eskandarian A, Hoffman LJ. Challenges of Intervehicle Ad-Hoc Networks, IEEE Transportation Systems. 2004; 5(4):347-51. Crossref
3. Raya M, Hubaux JP. Securing Vehicular Ad-Hoc Networks, Journal of Computer Security. 2007; 15(1):39-68. Crossref

4. Wei YC, Chen YM. Efficient Self-Organized Trust Management in Location Privacy Enhanced VANETs, Springer International Workshop on Information Security Applications WISA, Jeju Island, Korea; 2012, 13. p. 328-44. Crossref
5. Alheeti KMA, Gruebler A, McDonald-Maier KD. An Intrusion Detection System Against Malicious Attacks on the Communication Network of Driverless Cars. IEEE 12th Annual Consumer Communications and Networking Conference (CCNC), Las Vegas, NV; 2015. p. 916-21. Crossref
6. Li Q, Malip A, Martin KM, Ng SL, Zhang J. A Reputation-Based Announcement Scheme for VANETs, IEEE Transactions on Vehicular Technology. 2012; 61(9):4095-108. Crossref
7. Dhurandher SK, Obaidat MS, Jaiswal A, Tiwari A, Tyagi A. Securing Vehicular Networks: A Reputation and Plausibility Checks-based Approach. IEEE Globecom Workshop on Web and Pervasive Security; 2010. p. 1550-54. Crossref
8. Gazdar T, Rachedi A, Benslimane A, Belghith A. A Distributed Advanced Analytical Trust Model for VANETs. IEEE Global Communications Conference (GLOBECOM), Anaheim, CA; 2012. p. 201-06. Crossref
9. Wang J, Liu Y, Liu X, Zhang J. A Trust Propagation Scheme in VANETs. IEEE Intelligent Vehicles Symposium, Xi'an; 2009. p. 1067-71.
10. Wang Z, Chigan C. Countermeasure Uncooperative Behaviors with Dynamic Trust-Token in VANETs.I EEE International Conference on Communications, Glasgow; 2007. p. 3959-64.-Crossref
11. Biswas S, Misic J, Misic V. ID-based Safety Message Authentication for Security and Trust in Vehicular Networks. IEEE 31st International Conference on Distributed Computing Systems Workshops, Minneapolis, MN; 2011. p. 323-31.
12. Gazdar T, Benslimane A, Belghith A. Secure Clustering Scheme Based Keys Management in VANETs. IEEE 73rd Vehicular Technology Conference (VTC Spring), Yokohama; 2011. p. 1-5.
13. Ding Q, Li X, Jiang M, Zhou XH. Reputation-based Trust Model in Vehicular Ad-Hoc Networks. IEEE International Conference on Wireless Communications and Signal Processing (WCSP), Suzhou; 2010. p. 1-6. Crossref
14. Liao C, Chang J, Lee I, Venkatasubramanian KK, A Trust Model for Vehicular Network-Based Incident Reports. IEEE 5th International Symposium on Wireless Vehicular Communications (WiVeC); 2013. p. 1-5. Crossref
15. Dotzer F, Fischer L, Magiera P. VARS: A Vehicle Ad-Hoc Network Reputation System. IEEE 6thInternational Symposium on a World of Wireless Mobile and Multimedia Networks; 2005. p. 454-56. Crossref
16. Gazdar T, Benslimane A, Rachedi A, Belghith A. A Trust-based Architecture for Managing Certificates in Vehicular Ad-Hoc Networks. IEEE 2nd International Conference on Communications and Information Technology (ICCIT), Hammamet; 2012. p. 180-85. Crossref
17. Serna J, Luna J, Medina M. Geolocation-based Trust for Vanet's Privacy. IEEE 4th International Conference on Information Assurance and Security (ISIAS), Naples; 2008. p. 287-90. Crossref
18. Huang D, Hong X, Gerla M. Situation-Aware Trust Architecture for Vehicular Networks, IEEE Communications Magazine. 2010; 48(11):128-35. Crossref
19. Chen C, Zhang J, Cohen R, Ho PH. Secure and Efficient Trust Opinion Aggregation for Vehicular Ad-hoc Networks. IEEE 72nd Vehicular Technology Conference Fall (VTC 2010-Fall), Ottawa; 2010. p. 1-5.
20. Raya M, Papadimitratos P, Aad I, Jungels D, Hubaux JP. Eviction of Misbehaving and Faulty Nodes in Vehicular Networks, IEEE Journal on Selected Areas in Communications. 2007; 25(8):1557-68. Crossref
21. Chen YM, Wei YC. A Beacon-Based Trust Management System for Enhancing User Centric Location Privacy in VANETs, Journal of Communications and Networks. 2013; 15(2):153-63.
22. Li W, Song H. ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad-Hoc Networks, IEEE Transactions on Intelligent Transportation Systems. 2016; 17(4):960-69. Crossref
23. Chang BJ, Kuo SL, Liang YH, Wang DY. Markov Chain-based Trust Model for Analyzing Trust Value in Distributed Multicasting Mobile Ad-Hoc Networks. IEEE Asia-Pacific Services Computing Conference, APSCC '08, Yilan; 2008. p. 156-61. Crossref
24. Wei YC, Chen YM. An Efficient Trust Management System for Balancing the Safety and Location Privacy in VANETs. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool; 2012. p. 393-400. Crossref
25. Daza V, Domingo-Ferrer J, Sebe F, Viejo A. Trustworthy Privacy-Preserving Car-Generated Announcements in Vehicular Ad-Hoc Networks, IEEE Transactions on Vehicular Technology. 2009; 58(4):1876-86. Crossref
26. Jeyaprakash T, Mukesh R. Mathematical Analysis of Trust Computing Algorithms. ELSEVIER Second International Symposium on Computer Vision and the Internet (VisionNet'15); 2015. p. 105-12. Crossref
27. Minhas UF, Zhang J, Tran T, Cohen R. A Multifaceted Approach to Modeling Agent Trust for Effective Communication in the Application of Mobile Ad-Hoc Vehicular Networks, IEEE Transactions on Systems, Man and Cybernetics-Part C: Applications and Reviews. 2011; 41(3):407-20. Crossref

28. Golbeck J. Computing with Trust: Definition, Properties and Algorithms. IEEE Securecomm and Workshops, Baltimore, MD; 2006. p. 1-7.
29. Gai X, Li Y, Chen Y, Shen C. Formal Definitions for Trust in Trusted Computing. IEEE Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, Xian, Shaanxi; 2010. p. 305-10. Crossref
30. Khan MF, Felemban EA, Qaisar S, Ali S. Performance Analysis on Packet Delivery Ratio and End-to-End Delay of Different Network Topologies in Wireless Sensor Networks (WSNs). IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN), Dalian; 2013. p. 324-29.
31. Fabbri F, Riihijarvi J, Buratti C, Verdone R, Mahonen P. Area Throughput and Energy Consumption for Clustered Wireless Sensor Networks. IEEE Wireless Communications and Networking Conference, Budapest; 2009. p. 1-6. Crossref
32. Mahmood D, Javaid N, Qasim U, Khan ZA. Routing Load of Route Discovery and Route Maintenance in Wireless Reactive Routing Protocols. IEEE 7th International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), Victoria, BC; 2012. p. 511-16. Crossref
33. Guo C, Zhou J, Pawelczak P, Hekmat R. Improving Packet Delivery Ratio Estimation for Indoor Ad-Hoc and Wireless Sensor Networks. IEEE 6th Consumer Communications and Networking Conference, Las Vegas, NV; 2009. p. 1-5.