TruVAL: Trusted Vehicle Authentication Logic for VANET

Suparna DasGupta[1], Rituparna Chaki[2], and Sankhayan Choudhury[3]

[1] Department of Information Technology,
JIS College of Engineering, West Bengal, India
suparnadasguptait@gmail.com
[2] Department of Computer Science & Engineering,
West Bengal University of Technology, West Bengal, India
rituchaki@gmail.com
[3] Dept. of. Computer Sc. & Engg. University of Calcutta, West Bengal, India
sankhayan@gmail.com

Abstract. Vehicular ad hoc networks are characterized by nodes with relatively high mobility and comprise of vehicle-to-vehicle and vehicle-to-infrastructure communications based on wireless network technologies. The deployment of vehicular communication systems is strongly dependent upon their underlying security and privacy features. As vehicular ad hoc networks (VANETs) are vulnerable to malicious attacks, the security in VANETs is receiving a significant amount of attention in the field of wireless mobile networking. It has been observed that trust establishment in VANET is a challenging task due to the lack of infrastructure, and the high speed mobile nodes causing frequent changes to the network topology. In this paper we have proposed a Trusted Vehicle Authentication scheme for secured communication in VANET. The use of a layered framework for assigning trust values to a vehicle helps in detecting a node taking part in malicious activity. Conducted simulation experiments on different scenarios show the performance and effectiveness of our new proposed vehicle authentication logic for vehicular ad hoc networks.

Keywords: Vehicular ad hoc networks, Security, Privacy, Trust Value.

1 Introduction

Vehicular ad hoc networks have become a popular area for both the academic research community and automobile industry, with specific attention to improving driving experience and road safety. Prerequisite to communicate within VANETs is an efficient route between network nodes which must be adaptive to the rapidly changing topology of VANET. The VANET consist of vehicles and road side units (RSUs) as network nodes and enables inter-vehicle communications (IVC) along with the road side to vehicle communications (RVC). Each vehicle that is part of a VANET contains an onboard wireless computing unit, commonly known as the onboard unit (OBU). Vehicles can communicate with nearby vehicles known as a vehicle-to-vehicle (V2V) communication and also with road side infrastructure also

S. Unnikrishnan, S. Surve, and D. Bhoir (Eds.): ICAC3 2013, CCIS 361, pp. 309–322, 2013.

known as vehicle-to-Infrastructure (V2I). IVC and RVC can be divided into two categories; safety-related application and information-related application.

The security of VANETs is crucial as their existence relates to critical life threatening situations. The network has to be secure without compromising current transmission quality. Recent studies on VANETs identify several issues, including those in security and privacy, which need to be addressed for widespread adoption. The security algorithm which is to be implemented in VANET, aims for lesser computational cost and should utilize limited resource effectively. Identifying malicious node and preserving privacy are also one of the major aspects of the VANETs security. The security of vehicular ad hoc networks can be affected mostly due to illegal access and impersonation attacks. For avoiding illegal access a vehicle must have a desired trust value and be registered under an authorized registration authority for accessing the network. An attacker can perform much different type of attacks; they can disturb the network topology and attack other node's dataflow by identity spoofing.

Authentication is an important security requirement for VANET. Large number of high speed vehicles and dynamic topology of the vehicular network are some of the key factors which makes authentication task difficult. Many emerging vehicular ad hoc networks use a trust value based mechanism which is dynamic and context dependent.

In this paper we have introduced a new trust based security mechanism to track malicious and misbehavioral vehicles and present new trusted vehicle authentication logic for vehicular ad hoc networks. This proposed scheme consists of two different steps. (i) Registration procedure has been introduced for new vehicles and trust value has been assigned to each registered vehicles. (ii) Trust value updating mechanism has been presented for existing vehicles.

The rest of the paper is organized as follows. Comprehensive surveys of related works of different secure routing protocols for VANETs are discussed in section 2. In section 3 we have presented new trusted vehicle authentication logic for VANET. Intensive performance analysis of our proposed scheme is presented in section 4. We conclude our paper with final remarks in section 5.

2 Related Works

For full deployment of VANETs two paramount issues should be resolved, namely security and privacy. The information communicated by vehicles should be secured. Many researchers have been already published number of research papers, addressing the security issue of vehicular ad hoc networks. In this section we have discussed some of the security related research challenges of VANET.

In [7] B. Aslam et al. proposed a certificate based distributed approach for VANET. The focus of this approach is to achieve the desired security attributes (Privacy, authentication, confidentiality and non-repudiation) during the initial deployment phase of VANET. Architecture has been proposed to achieve desired security requirements and enables service providers to offer incrementally various VANET services with minimal investment thus encourages both service providers and users to try/adopt VANET. According to this protocol when a user wants to participate in a VANET, he/she purchases a payment-processing-device, consists of an associated certificate. At the time of initialization, the device was registered with the user's account. The vehicle's information is maintained by the provider. In this case they need to introduce some roaming or cross certification mechanisms between the service areas.

S. Biswas et al. [17] proposed an ID-based message authentication mechanism for VANETs. This is a safety message authentication scheme for vehicular ad hoc networks using an ID-based signature and verification mechanism. This offers a certificate-less public key verification, while a proxy signature provides flexibilities in message authentication and trust management. An ID-based proxy signature framework with the standard ECDSA for VANET's road-side unit (RSU) has been incorporated in this scheme. RSU originates safety application message. Forwarding of signed messages is specially handled to ensure the trust and authentication of RSU's application messages. In this mechanism the current location information of a signer has been used as the signer's identity in order to sign and verify the proxy signature. An emergency/road-safety application message has been generated by a trusted central authority (e.g. department of transportation), while the issued message is signed and delivered to end users (OBUs) by corresponding road-side units (RSUs) on behalf of the originator of the message. If any OBU is the outside communication range of an RSU, it may receive the broadcast through an intermediate "message-forwarder" OBU. The receiver vehicle checks the signature contents for the verification of the message. One easy way to accomplish for forwarding exactly the same signature materials as received from RSU. The receiving OBU verifies the signature as if it has received the message from the corresponding RSU. This approach is appropriate for authentication and trust management in highly dynamic and untrustworthy vehicular network environment as it is resilient to potential security threats. It is also compatible to the VANET's standard specifications.

In [8] Terence Chen et al. proposed a distributed routing framework for authentication of messages, nodes and routes. The architecture is distributed and uses limited assistance from a Certificate Authority (CA). By using digital signature control messages message integrity and originality can be ensured. A secure neighbor discovery method is included in the node-to-node authentication module. The link status evidence mechanism included in the cumulative routability verification module regulates the behavior of internal nodes. This proposed mechanism is applied to the OLSR [3] routing protocol, resulting in an OLSR extension which guarantees trusted routing using only the routes with verified nodes. The routability verification module adds a substantial amount of overhead, which may result in scalability problems.

Y. Sun et al. [9] Proposed ECHO, an efficient certificate updating scheme by Vehicle-to-Vehicle communications. They had used GPSR [1] for transmitting the message from the source node to the certain location. In case an improved route is discovered, the next relay node prefers the OBUs on the shortest path from source to the destination. The shortest path is calculated based on the selected roads with high traffic density. In this scheme the OBU not only sends the certificate request to an immobile RSU but also inform the RSU where the response message should be sent back. The RSU also issues a new certificate for the legitimate OBU. The OBU receives the response message at the expected callback address if the whole process is success.

In [6] Charles Harsch et al. presented a scheme that secures geographic position-based routing for VC. They design mechanisms to safeguard the functionality of PBR

[4]. A public key infrastructure with a Certification Authority (CA) has been introduced in this routing scheme. CA issues public/private key pairs and certificates containing public key, attribute list, the CA identifier, the certificate lifetime and the CA signature. Each received packet is first submitted to a sequence of plausibility checks using the packet's time and location fields as inputs. If at least one test fails, the packet is discarded. Otherwise, if all checks succeed, the packet is validated cryptographically. First, the certificate is validated, unless it was previously validated and cached. Then, the signature(s) on the packet are validated and, if failed, discarded. Otherwise, the packet is processed further. We have discussed s in more detail the security mechanisms hereafter.

Ming Chin Chuang et al. [18] proposed a decentralized lightweight authentication scheme called Trust Extended Authentication Mechanism (TEAM) for vehicle-to-vehicle (V2V) communication networks. This scheme adopts the concept of transitive trust relationships to improve the performance of the authentication procedure. It also claim to satisfy requirements like anonymity, location privacy, mutual authentication to prevent spoofing attacks, forgery attacks, modification attacks and reply attacks, as well as no clock synchronization problem, no verification table, fast error detection, and session key agreement. The amount of cryptographic calculation under TEAM is substantially less than in existing schemes because it only uses an XOR operation and a hash function.

V. Paruchuri et al. proposed [10] a protocol for anonymous authentication in vehicular Networks (PAAVE) to address the privacy preservation issue with authority traceability in vehicular ad hoc networks (VANETs). This protocol is based on smart cards to generate on-the-fly anonymous keys between vehicles and Roadside units (RSUs). PAAVE [10] is lightweight and provides fast anonymous authentication and location privacy while requiring a vehicle to store one cryptographic key.

In [5] J. Serna et al. proposed a geo-location based trust for VANET's privacy. This paper used as an authorization paradigm based on a Mandatory Access model and a novel scheme which propagates trust information based on a vehicle's geo-location. In this proposed scheme different levels of authorization is defined; Such as; personal (i.e., driver's "consent" is required), emergency (i.e., in this case driver's "consent" is not needed; however the system will require the credential of the entity (i.e. police) accessing the information) and public (i.e., no authorization checks are required). For trustworthiness certifying authority has been presented in this scheme.

Asif Ali Wagan et al. [12] presented a hardware based security framework which uses both standard asymmetric PKI and symmetric cryptography for secure and faster safety message exchange. The paper proposed to develop trust relationship among the neighboring node, finally leading to the formation of trust groups. The trust has been established via Trusted Platform Module (TPM) and group communication. In [12] Wagan et al. proposed an extended version of above discussed security framework. Within these two schemes, one is for efficient group formation for improving life time of a group leader role. They also presented hybrid (symmetric /asymmetric) message dissemination scheme for faster and secure communication.

A trust based privacy preserving model for VANETs has been presented by Ayman Tajeddine et al. [13], which is unique in its ability to protect privacy while maintaining accurate reputation based trust. VANET users are anonymous within their groups and yet identifiable and accountable to their group managers. In this proposed scheme each vehicle is a part of a static group assigned offline and should generate a group signature on each of its outgoing messages and includes with it an authentic group ID. Group Managers (GMs) have the responsibility to admit new vehicles and to evict attacker/malicious vehicles. Every group has a reputation level that accounts for the trustworthiness of the messages signed in the name of this particular group. In this proposed mechanism no scheme has been described for estimation of this reputation level.

In [14] a reputation based trust model has been presented by Qing Ding et al. This is an event based reputation model to filter bogus warning messages. A dynamic role dependent reputation evaluation mechanism has been presented to determine whether an incoming traffic message is significant and trustworthy to the driver. In this proposed scheme initially different roles played by vehicles are defined for reputation estimation. These roles are Event Reporter (ER), Event Observer (EO) and Event Participant (EP). After encountering a traffic event at first ER calculate reputation value of that event. If this value is over the redefined threshold, the event message will be sent to the traffic safety application in the vehicle and to all neighbors in one hop, namely EO. When an EO receives a traffic warning message from an ER, it will first store this message into the event table if there is no the same ID record in the table. Depending on the message truthfulness send by an ER an EO can calculate ER's reputation. EP receives message only form EO's and other EP's. Complex formula for calculating reputation values are given in this paper. Reputations are estimated based on the behavior of vehicles. The behavioral characteristics are not clearly identified.

G. Kavitha et al. [15] introduced a grid based approach for providing a quantitative trust value, based on the past interactions and present environment characteristics. This quantitative trust value has been used to select a suitable resource for a job and eliminates run time failures arising from incompatible user resource pairs. This act as a tool to calculate the trust values of the various components of the grid and there by improves the success rate of the jobs submitted to the resource on the grid. The access to a resource not only depend on the identity and behavior of the resource but also upon its context of transaction, time of transaction, connectivity bandwidth, availability of the resource and load on the resource. The quality of the recommender has been evaluated based on the accuracy of the feedback provided about a resource. The jobs are submitted for execution to the selected resource after finding the overall trust value of the resource. The parameters depend on which trust value of a node has been calculated are not clearly defined in the paper.

Sumit kumar Singh et al. [16] proposed two levels of security based on Signcryption and node trust. Signcryption is less cost effective than Signthenencryption and it also conserved confidentiality and integrity of the message. In [16] authors proposed a network model consisting VANET server, Roadside Unit, On-Board Unit, Source node and Destination node. The VANET server is a trusted entity by all nodes participating in the network. The shared key used between nodes and VANET server cannot be compromised in any conditions. The public and private keys sent from VANET server to nodes are through secure channel and cannot be compromised by any means. The trust value assigned by the destination node is appropriate and depending on this trust value, trust level has been assigned. This proposed mechanism does not focus on the estimation of trust value and the trust value calculation parameters have not mentioned in this research.

The above discussions lead to the conclusion that mainly cryptographic and certificate based techniques are being preferred by the researchers for securing communication within VANETs. The metrics influencing the certificate based technique have not been clearly identified. The cryptographic approaches such as, encryption, digital signature, Signcryption etc. has been introduced additional complexities for key management. Some researchers have chosen trust value based authentication, but the parameters influential in trust value assignment of a vehicle are not properly identified. This paper aims to identify the parameters in a trust based authentication scheme as to ensure authenticity of communication in a VANET.

3 Proposed New Routing Protocol: TruVAL: Trusted Vehicle Authentication Logic for VANET

The previous section leads to the observation of different security related research challenges of VANET. In this section we are going to propose TruVAL: Trusted Vehicle Authentication Logic for VANET. In our proposed solution we have distributed VANET in a layered architecture.

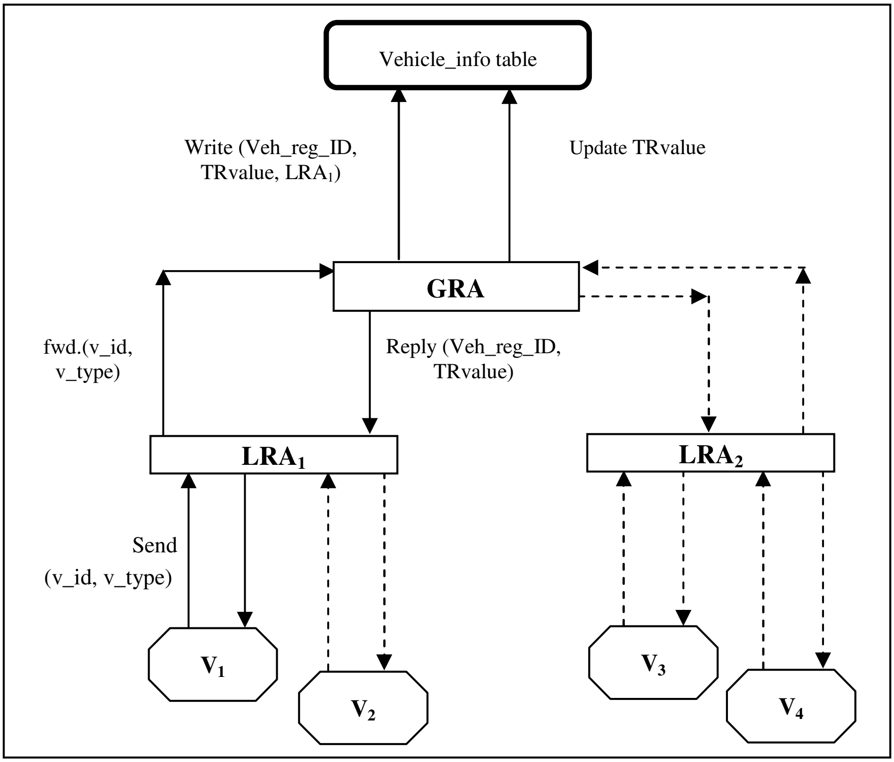

Fig. 1. Modular Diagram of TruVAL

In the lowest layer, all nodes (i.e., vehicles) present in the system. LRA_i (Local Registration Authority) implies a road-side unit that acts as a middle layer element within the framework. LRA_i is responsible for estimating an initial trust value and also updated the trust value based on some pre-defined parameters for that vehicle. The highest layer component, called Global Registration Authority (GRA), is nothing but a repository having all lower layer information. TruVAL consists of two phases: registration procedure and trust value updating mechanism.

I. Registration Procedure

Here we have assumed that all nodes in a VANET are distributed according the proposed layered architecture. On entry of a new vehicle in the system, it requests the LRA_i for a registration certificate. This request is termed as Registered to Communicate (RTC). In this request, new vehicle sends it vehicle number and other details to LRA_i. Depending on that information trust value of that vehicle is estimated. LRA_i forwards vehicle number and trust value to GRA. GRA generates a unique sequence number, i.e., USN for that particular vehicle. This USN acts as Veh_reg_ID for the corresponding vehicle. At the registration time LRA_i have no idea about the behavior of the vehicle. For this reason at this time an initial trust value is given to the vehicle.

❖ Trust Value Initialization

In this subsection we are going to present an algorithm for new vehicle entering in the system. Every new vehicle has to register under its local LRA_i. For this reason it sends a registration request to LRA_i. In this request each vehicle has to send their types and the unique features of it. After receiving the request LRA_i assigns a unique number and a trust value to the requesting vehicle. After initialization of trust value it will forward to GRA and GRA keeps all this information in Vehicle_info table and the corresponding vehicle is registered under the communicating LRA_i.

Table 1. Vehicle_info table

Veh_reg_ID	**LRA_i**	**TR_{value}**

Algorithm 1. Registration_proc

```
New vehicle sends (vehicle_id, v_type) to $LRA_i$
$LRA_i$ call Trust_init_func(vehicle_id, v_type)
$LRA_i$ forward that vehicle_id and TRvalue to GRA
GRA generates a Veh_reg_ID
GRA write Veh_reg_ID, TRvalue and $LRA_i$ in Vehicle_info table.
New vehicle is registered under $LRA_i$
END.
```

After completion of the above discussed procedure, the systems now have a new registered vehicle. Apart from registered a new vehicle and supply information about that registered information, LRA_i have another very important role. LRA_i have to update trust value of every registered vehicle after a certain interval. In the next section we are going to discuss the trust value updating procedure.

II. Trust Value Updating Procedure

After a certain time interval LRA_i updates trust value of every registered vehicle. This mechanism has been done based of some parameters defined by us. Those parameters are as follows:

✓ **Active Factor:** For each communication every sender vehicle maintains a communication counter after every interaction. Every receiving vehicle also maintains a list of name of every sender vehicle. In this way LRA_i can easily know how many times a vehicle have taken part into communication. This can measure by a metric called active factor.

Active factor α is defined as follows: Let cn be the total number of communications in which vehicle v have participated during time interval t, then,

$$\alpha = 1/n \sum_{n=0}^{n} (c_s + c_r) / c_n \tag{1}$$

Where c_s is the value of communication counter maintained by v and c_r denotes the number of times v appeared in the sending vehicle list of other vehicle present in the network. Using equation (i) LRA_i can easily calculate value of active factor for v.

✓**Feedback Factor:** After completion of every communication every vehicle who was taken part in that communication sends feedback [R_S, R_F, R_{PS}, R_{PF}] to LRA_i about its neighbors taking part in that communication. LRAi calculates feedback value from those reports. Feedback value can be calculated using some metrics defined in feedback form.

- Request success ratio (R_S): This is defined as the request success ratio which is calculated based on number of neighboring nodes who have successfully received from the source node which has broadcasted it. Once a vehicle sends a request to its neighbor and gets the acknowledgement within the timeout period, the respective R_S value is incremented by one.
- Request failure ratio (R_F): This is defined as the request failure ratio which is calculated based on number of neighboring nodes which have not received the request.
- Reply success ratio (R_{PS}): This is defined as the reply success ratio which is calculated as successful replies received by source node which has sent the request.
- Reply failure ratio (R_{PF}): This is defined as the reply failure rate which is calculated based on the number of neighboring nodes which have not sent the replies for the request received.

Using these metrics feedback value can be defined. Let feedback value is denoted by f. Then,

$$f = 1/n \sum_{0}^{n} (t_p * \left(\frac{R_S - R_F}{T_{mr}} + \frac{R_{PS} - R_{PF}}{T_{mn}}\right)) \tag{2}$$

Where, t_p is time period, T_{mr} is the total number request sends in that time period and T_{mn} is total number of reply receives in that time period.

✓**Experience Factor:** After successful registration of each new vehicle every LRA_i assigns a timestamp value to them. This value indicates the entry time of the vehicle in the system. From this value LRA_i can easily estimate the duration of the instance of vehicle in the system. According to this time it calculates experience factor which is denoted by € symbol. Let, at time t_0 a vehicle enters in the system.

At time t_n the value of

$$€= (t_n – t_0) \tag{3}$$

Trust updation of a vehicle is done based on this active, feedback and experience factor. The updated trust value (TRvalue) can be estimated using the following equation.

$$TR_{value} = W_1 * \alpha + W_2 * f + W_3 * € \tag{4}$$

Where, W_1, W_2 and W_3 are weighting factors. The multiplying values with different factors actually indicating weight given to that factor. Active, authentic and reliable new vehicle is more desirable than inactive and less reliable vehicle. For this reason more weight is given to α and f than €. The main aim for calculating TRvalue is secure authenticity and reliability in message passing. For this reason highest weight is given to f factor.

Algorithm 2. Trust_val_updt

```
/*updating mechanism of trust value for vehicle v by respective LRA_i */
Calculate active factor, $\alpha = 1/n \sum_{n=0}^{n} (c_s + c_r) / c_n$
Calculate feedback factor,
$f = 1/n \sum_{0}^{n} (t_p * \left(\frac{R_S - R_F}{T_{mr}} + \frac{R_{PS} - R_{PF}}{T_{mn}}\right))$
Estimate experience factor, €.
Update TRvalue = $W_1 * \alpha + W_2 * f + W_3 * €$.
END.
```

After calculation of trust value this value is attached with the vehicle. From the above discussion we can see the trust value is calculated based on some basic behavioral activities of a node. These activities are not immortal. For this reason assigned trust value should be updated by LRA_i, after a certain time interval.

Vehicles are all highly mobile in nature. In a very short time interval it can move from one LRA_i's region to another LRA_i's region. After become registered once all information about the corresponding vehicle is maintained by parent LRA_i. Information of every registered vehicle's is also stored in GRA. GRA actually acts as a global repository of all registered vehicles. LRA_i monitors all vehicles registered under it. When a vehicle moves out of its region it broadcast a message consisting information about that vehicle. In this way the new LRA$_i$ in which region the vehicle enters can know information about it. The information sends by the following message format.

FM$_i$	**Veh_reg_ID**	**TR$_{value}$**	**Parent_LRA**

Fig. 2. Frequent message format

In the above message format FM$_i$ denotes an identifier that uniquely identifies the message. Veh_reg_ID, TR$_{value}$, Parent_ LRA$_i$ denotes registration identifier, trust value and initial LRA$_i$ respectively for the corresponding vehicle. In this way when LRA$_i$ found any new vehicle in its region it also have some essential information about that vehicle. If LRA$_i$ needs more detail information then it can query to GRA and gets required information from it.

Table 2. Data Dictionary

Parameter	**Details**
LRA	Local Registration Authority
GRA	Global Registration Authority
RTC	Registered to Communicate
USN	Unique Security Number
Veh_reg_ID	Vehicle Registration Identifier
TR$_{value}$	Trust Value
Vehicle_id	Vehicle Identifier
V_type	Vehicle Type
FM$_i$	Frequent Message Identifier
α	Active Factor
C_s	Sending Message Counter
C_r	Receiving Message Counter
C_n	Total Number of Communication Maintained Counter
R_S	Request Success Ratio
R_F	Request Failure Ratio
R_{PS}	Reply Success Ratio
R_{PF}	Reply Failure Ratio
T_p	Total Time Period
f	Feedback Factor
€	Experience Factor
W_i	Weighted Factor
T_o	Time of A Vehicle Entering In System
T_{mr}	Total Number of Request Send Within Time Period
T_{mn}	Total Number of Reply Received Within Time Period

IV. Performance Analysis

In our proposed protocol we haven't used any cryptographic techniques like digital signature etc. Thus there is no overhead of maintaining public key and private key. Extra bandwidth is also not needed for transforming the data. The layered network structure helps us to overcome the problems of centralized approach like performance bottleneck, no scalability etc. Based on three clearly defined behavioral parameters of vehicle a trust value is assigned to all registered vehicles. Every node has to maintain this trust value which result to very less overhead. For performance analysis the above discussed trust estimation mechanism is integrated into existing AODV routing protocol. The basic aim is to restrict malicious vehicles to take part in communication.

We choose the NS2 simulator for this analysis because it realistically models arbitrary node mobility as well as physical radio propagation effects such as signal strength, interference, capture effect and wireless propagation delay. Our propagation model is based on the two-ray ground reflection model. The simulator also includes an accurate model of the IEEE 802.11 Distributed Coordination Function wireless MAC protocol.

Using NS2 we evaluate the performance of the proposed protocol TruVAL and present the following metrics for comparing the performance of traditional AODV with the TruVAL. The simulation model consists of a network model that has a number of wireless nodes, which represents the entire network to be simulated.

Table 3. Simulation Environment Parameters

Parameter	Value
Channel type	Wireless Channel
Radio-propagation model	Two Ray Ground
Antenna model	Omni Antenna
Network interface type	Wireless Phy
Mac type	802.11
Number of nodes	25

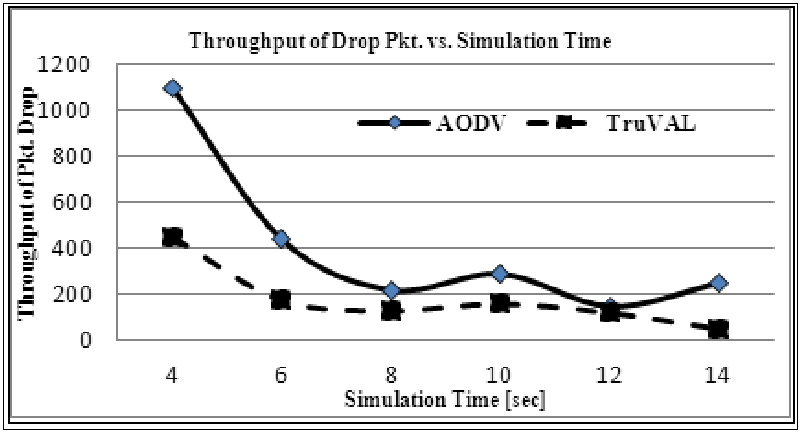

Fig. 3. Throughput of Drop Pkt. vs. Simulation Time

Figure 3 depicts a comparison of AODV and TruVAL with respect to packet dropping in presence of malicious nodes. The graph clearly shows that the number of packets dropped is less in case of TruVAL. Simulation result shows that in the same network scenario, traditional AODV dropped 4628 packets whereas TruVAL dropped 2444 packets.

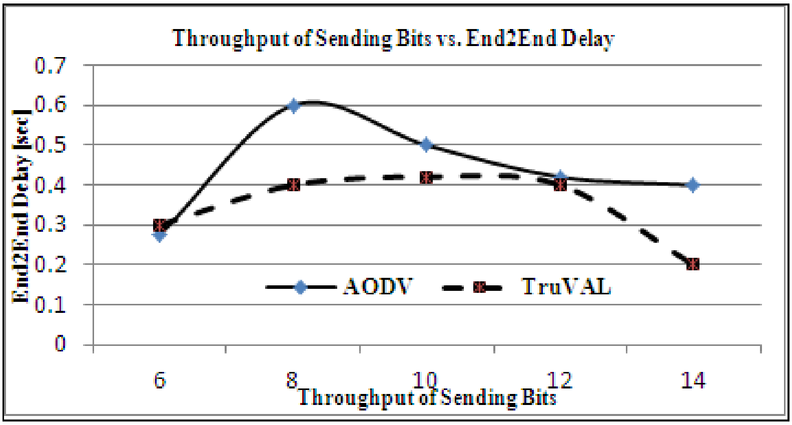

Fig. 4. Throughput of Sending Bits vs. End2End Delay

From figure 4, we have compared end2end delay for packet sending of AODV with TruVAL in same network condition. It is observed from the above graph that the delay for TruVAL is much lesser than AODV. Simulation result show average end2end delay for sending packet for AODV is 0.40226. For TruVAL it is 0.36542. In this case also TruVAL gives a better result than AODV.

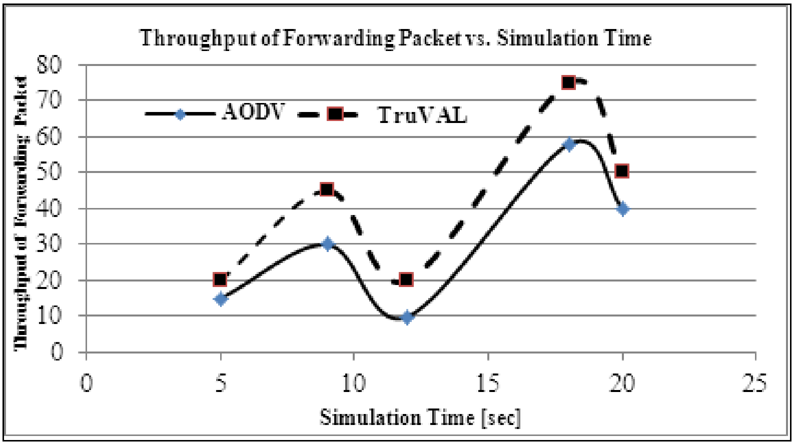

Fig. 5. Throughput of Forwarding Packet vs. Simulation Time

Figure 5 depicts a comparison of AODV and TruVAL with respect to number of forwarding packet in presence of malicious nodes. The graph clearly shows that the number is high in case of TruVAL. Simulation result shows, that in the same network scenario our proposed scheme forwards more bits with respect to traditional AODV.

From the above three comparisons we can see in present of malicious nodes our proposed scheme gives better result than traditional AODV.

4 Conclusions

In this paper we have summarized the generic characteristics of some well-known security approaches for VANETs and proposed a trust based authentication logic for VANET named TruVAL. We presented a layered structure for authenticating vehicles to communicate. A trust estimation mechanism is also proposed for trust calculation. Depending on this estimated trust malicious nodes are detected. In this way malicious nodes can be easily avoided during communication. For performance analysis of TruVAL, a simulation environment is created using NS2. The results show that TruVAL result in lesser number of packet drop and end2end delay as compared with traditional AODV. TruVAL also forward more bits than traditional AODV. In future this scheme shall be extended into a secure routing scheme.

References

1. Karp, B., Kung, H.T.: GPSR: greedy perimeter stateless routing for wireless networks. In: 6th Annual International Conference on Mobile Computing and Networking, pp. 243–254 (2000)
2. Perkins, C.E., Royer, E.M., Das, S.: Ad Hoc on Demand Distance Vector (AODV) Routing. IETF Internet draft, draft-ietf-manet-aodv-08.txt (March 2001)
3. Clausen, T., Jacquet, P.: Optimized Link State Routing Protocol (OLSR). RFC 3626, IETF Network Working Group (October 2003)
4. Namboodiri, V., Gao, L.: Prediction-Based Routing for Vehicular Ad Hoc Networks. IEEE Transaction on Vehicular Technology 56(4) (July 2007)
5. Serna, J., Luna, J., Medina, M.: Geo-location based Trust for Vanet's Privacy. In: Fourth International Conference on Information Assurance and Security, IAS 2008 (2008) 978-0-769-3324
6. Harsch, C., Festag, A., Papadimitratos, P.: Secure Position-Based Routing for VANETs. In: IEEE 66th Vehicular Technology Conference (VTC Fall), Baltimore, USA (2008)
7. Aslam, B., Zou, C.: Distributed Certificate and Application Architecture for VANETs. In: 28th IEEE Conference on Military Communications, MILCOM 2009 (2009) 978-1-4244-5238-5
8. Chen, T., Mehani, O., Boreli, R.: Trusted Routing for VANET. In: 9th International Conference on Intelligent Transport Systems Telecommunications, ITST 2009 (2009) 978-1-4244-5347-4
9. Sun, Y., Zhao, B., Su, J.: ECHO: Efficient Certificate Updating Scheme by Vehicle-to-Vehicle Communications. In: Fourth International Conference on Frontier of Computer Science and Technology, FCST 2009 (2009)

10. Puruchuri, V., Durresi, A.: PAAVE: Protocol for Anonymous Authentication in Vehicular Networks using Smart Cards. In: Proc. GLOBECOM (2010) 978-1-4244-5638-3
11. Wagan, A.A., Mughal, B.M., Hasbullah, H.: VANET Security Framework for Trusted Grouping using TPM Hardware. In: 2010 International Conference on Communication Software and Networks, ICCSN (2010) 978-0-7695-3961
12. Wagan, A.A., Mughal, B.M., Hasbullah, H.: VANET Security Framework for Trusted Grouping using TPM Hardware: Group Formation and Message Dissemination. In: 2010 International Symposium in Information Technology, ITSIM (2010) 978-1-4244-6716-711
13. Tajeddine, A., Kayssi, A., Chehab, A.: A Privacy-Preserving Trust Model for VANETs. In: 10th IEEE International Conference on Computer and Information Technology, CIT 2010 (2010) 978-0-7695-4108-2
14. Ding, Q., Jiang, M., Li, X., Zhou, X.H.: Reputation-based Trust Model in Vehicular AdHoc Networks. In: IEEE Conference on Wireless Communications and Signal Processing, WCSP (2010) 978-1-4244-7555
15. Kavitha, G., Sankaranarayann, V.: Secure Resource Selection in Computational Grid Based on Quantitative Execution Trust. International Journal of Computer and Information Engineering (2010)
16. Singh, S.K., Vijayan, R.: Enhanced Security for Information Flow in VANET using Signcryption and Trust level. International Journal of Computer Applications (0975-8887) 16(5) (February 2011)
17. Biswas, S., Misic, J., Misi, V.: ID-based Safety Message Authentication for Security and Trust in Vehicular Networks. In: 31st International Conference on Distributed Computing Systems Workshops (2011)
18. Chuang, M.C., Lee, J.F.: TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks. In: International Conference on Consumer Electronics, Communications and Networks, CECNet (2011) 978-1-61284-459