Trust Based Group Formation in VANET

Brijesh Kumar Chaurasia¹, Shekhar Verma²

ITM University, Gwalior, (M.P.), India
Indian Institute of Information Technology, Allahabad, (U.P.), India
¹ bkchaurasia.itm@gmail.com; ² sverma@iitta.ac.in

Abstract- In this paper, we present a reputation assisted trust management mechanism for vehicular ad hoc network (VANET) using privacy preserving trusted group formation. In VANETs, vehicles or road side units can be malicious or malfunction making security essential. A distributed trust management provides a lightweight security alternative to existing security techniques especially in VANETs. The trust mechanism framework is based on group formation which is multi step process. Once a group is formed, the group manager tracks the behavior of vehicles and changes their trust value in accordance to its current behavior which is essential in large scale road transportation. It can also admit new vehicles and eject old vehicles depending on their current trust values. Simulation results indicate the time taken for the process of group maintenance is small and is in the order of milliseconds. This time is sufficiently small and the spread of malicious messages can be prevented.

Keywords- Trust management; VANET; Group Signature

I. INTRODUCTION

VANET is a network of vehicles moving on the road supported by fixed infrastructure [1]. Vehicles have On Board Units (OBUs) that are equipped with communication equipment that allow them to exchange messages between each other (V2V communication) and also exchange messages with a roadside infrastructure (RSUs) (V2I and I2V communication). In VANETs, RSUs are located along the roads at regular intervals. Vehicles travel longitudinally at different speeds in restricted geographical strait jackets (roads) with restricted lateral motion except at junctions or during a lane change manoeuvre. VANETs are self-organized and distributed. Vehicles do not usually have energy constraints and they can be equipped with high computing and communication capabilities. They also equipped with an event data recorder (EDR) and global positioning system (GPS) and some additional equipment [2].

A bandwidth of 75 MHz has been allocated in the 5.850-5.925 GHz band and vehicles use dedicated short range communications (DSRC) protocol for communication [3],[4].

DSRC classifies two classes of applications: safety related applications and non-safety related applications [5]. For safety applications, [6] warning messages like lane changing, intersection collision warnings etc. are broadcast by the vehicle. Non safety applications [7] related to passenger comfort and efficiency of the transportation system such as toll collection, parking management and location-based services etc. are broadcast by infrastructure. The DSRC recommends [8] a transmission range between 300-1000 m, signal bandwidth of 10 MHz and data rate from 3-27 Mbps.

The stay period of vehicles under a RSU is very small with members (vehicles) joining / leaving a RSU membership as they move on the road. VANets also have some unique characteristics which differentiate them from other ad hoc networks such as high mobility, predictable topology and high density network.

In a VANET, information is exchanged over the shared wireless medium within limited communication range. It is expected to support safety as well as other messages like accident reporting, traffic management, electronic toll-tax collection etc. The safety related messages broadcast by vehicles are used by other vehicles to make critical decisions. This may trap a vehicle taking wrong decision with dire consequences. Moreover, a malicious vehicle may inject false messages with different identities. This necessitates that messages and vehicles be trusted, especially during V2V communication. The trust management system should simple (not complex), accurate, scalable, resilient so that the trust estimation is possible in minimal time.

Trust is a process by which relationships develop [9]. In wireless ad hoc networks, trust avoids the central trusted authority and used to record feedback about the security evaluations of other entities in the networks [10]. In VANETs, trust is a relationship between two vehicles such that one vehicle believes, expects, and accepts that the other trusted vehicle will act or intend to act beneficially [11],[12]. For example, let us assume that between two vehicles x and y, the trust of x to y is $T_{(x,y)}$ and the trust of y to x is $T_{(y,x)}$. If vehicle $x$ successfully forwards a packet for vehicle $y$, then vehicle x is considered to be an honest vehicle for y vehicle. Vehicle y will increase its trust value $T_{(y,x)}$ for good behavior of x vehicle. Otherwise, vehicle y will decrease its trust value $T_{(y,x)}$ for suspicious behavior of x vehicle. Trust management is a separate component of security services in networks which provides a unified approach for establishing a relationship [13]. In VANETs, trust management is a system to track behaviors of every vehicle and decide on rewarding an honest vehicle or to detect false information provided by malicious vehicles and make inform other vehicles for driving decisions. Existing literature has very few trust models for VANETs. In [14], trust models are categorized into three types: entity-oriented, data-oriented and combined trust model.

Entity oriented trust model is based on the modeling of the trustworthiness of peers. It is categorized in two types. The sociological trust model [15] uses the principle of trust and confidence tagging. The second model is the multi-faceted trust management model [16] based on role based and experience based approach for trustworthiness of vehicles in VANET. Some other role based trust models are presented.
in [17], [18], [19]. Data oriented trust model focuses on the evaluating the trustworthiness of data reported by other vehicles instead of trust of vehicles of themselves in VANET. The use of event specific trust metrics along time and location closeness is proposed in [19]. In [20], the detection and correction of malicious data problem in VANET is proposed. However, it requires that every vehicle to have global knowledge of the network. Combined trust model evaluates trustworthiness of data and maintains vehicle trust at the same time. Distribution reputation system is proposed in [21] using piggybacking approach. In [22], pre-authenticated anchor node is used to provide trustworthiness and identified malicious node. Another trust based message propagation model is proposed in [23]. The features of the existing trust models for VANET is summarized in Table I.

The trust management mechanism in VANET should be distributed, event / task & location / time specific, sensitive to privacy for vehicles, scalable and robust etc. Moreover, the mechanism should not affected by attacks as Sybil, newcomer, camouflage, on-off or betrayal, inconsisteny, collusion and bad mouthing / ballot stuffing etc. In the present work, a group based trust management is proposed. The mechanism is based on group formation with pre-trusted vehicles as group managers. The group formation is a five phase process which preserves the privacy of the vehicles. The associated inclusion and exclusion of vehicles in the group is based on dynamic trusted value. The membership depends on the current trust value of a vehicle which is compared to a threshold which is prefixed by the group manager. However, for such a mechanism to be effective, the time taken for group formation and maintenance should be small so that transmission and dissemination of malicious messages can be prevented.

### TABLE I FEATURES OF THE EXISTING TRUST MODELS FOR VANET

<table>
<thead>
<tr>
<th>Mechanisms</th>
<th>[24]</th>
<th>[25]</th>
<th>[20]</th>
<th>[21]</th>
<th>[16]</th>
<th>[23]</th>
<th>[22]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decentralized</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Dynamics</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Scalability</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Sparsity</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Confidence</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
</tbody>
</table>

The remainder of the paper is organized as follows. In Section II, proposed scheme is presented. Group formation of trusted vehicles is presented in Section III with simulation results and discussion in Section IV. Section V presents the conclusion.

II. PROPOSED REPUTATION ASSISTED TRUST EVALUATION FRAMEWORK

In the proposed scheme, trust level is of two types: static and dynamic reputation. Static trust level depends on an organization and the static trust value increases or decreases on the basis of observation of received messages (reputation based). Dynamic reputation increases or decreases when vehicles are moving on the road. Dynamic reputation depends on the reputation tag value based on its own tag and given by other vehicles over a period of time t on messages received and forwarded. This value becomes zero after some time to reduce the possibility of a collusion attack. Moreover, members of a group cannot increase the trust value of other members of their group.

**Algorithm for Trust value computation:**

The receiver vehicle will observe the received messages.
- If receiver vehicle forwards the message to other vehicles then trust value will increase of both the vehicles (sender vehicle and forwarder vehicle).
- If receiver vehicle found after sometime received message is wrong then trust value will decrease (both of the vehicles). Two cases are possible here:
  - **Case 1:** If receiver vehicle founds after t time received message is wrong and forwarder vehicle information is right then trust value will increase of forwarder vehicle and trust value will decrease of receiver value.
  - **Case 2:** If receiver vehicle founds after t time received message is right and forwarder vehicle information is wrong then trust value will decrease of forwarder vehicle and trust value will increase of receiver value.
- At the time of re-authentication trust value will be zero. Same as the original static value will also.

III. GROUP FORMATION OF TRUSTED VEHICLES

In this section, the process of group formation and its maintenance through pre-trusted vehicles is presented. Pre-trusted vehicles are police vans/cars, ambulances and other government vehicles which can be trusted a priori. A pre-trusted vehicle will act as a group manager and initiates the formation of a group of vehicles moving on the road. The group member vehicles are selected using their current trust value. Initially when a vehicle starts on the road, its trust value is equal to the static trust value. After sometime, the trust value of a vehicle may get updated according to its dynamic reputation. When evaluated current trust value becomes more than a prefixed threshold value, the group manager will include the vehicle(s) as a group member. Similarly, when evaluated trust value becomes less than the threshold value, its group manager will remove the vehicle(s) from the group.

The formation of a group signature has five phases and algorithms [26], [27] of these phases are discussed below:

**Setup:** The group manager is a pre trusted vehicle. The pretrusted selects an input a security parameter k and uses a probabilistic algorithm to calculate the group public key PK and the secret key of the group manager, SK respectively.

\[ PK = \{n,e,e,g,y,h,C,l_0,?,l_1,l_2\}; \ SK = \{p',q',x\} \]

To calculate PK and SK the group manager selects two prime numbers \(p'\) and \(q'\), which is calculated from \(p = \]

MTTER Volume 2, Issue 2 April 2013 PP. 121-125 www.vkingpub.com ©American V-King Scientific Publishing
2p' + 1 and q = 2q' + 1, n = pq, l_n is the bit length of n, e > 1, e is relative prime to φ(n), g is an element of ℤ_n^* of order n, G = < g, h ∈ G, C = ℤ_n^*.

The group manager selects value x and calculates the value of y = g^χ(mod n), H: {0, 1}^* → {0, 1}^* which is collision-resistant hash function, and security parameters ? > 1, l_1, l_2 are set.

**Join:** This is an interactive protocol between the group manager and a user that results in the user becoming a new group member on the basis of evaluated trusted value of vehicles by group manager. The algorithm of this protocol assigns the certificate and the private key by the group manager.

Certificate of the group member U_j is the combination of two calculated integers as \( (A_j, X_j) \) where

\[
X_j = C + \delta (mod n),
\]

\( \delta \) is also belong to \( [2^{l_1}, 2^{l_2} + 2^{l_2} - 1] \)

\[
A_j = (C + X_j)^2 (mod n)
\]

\( x_j \) is also belong to \( [2^{l_1}, 2^{l_2} + 2^{l_2} - 1] \)

**Sign:** This algorithm creates the group signature with many integers and with multiple mod function s of integers. This interactive protocol between group manager and user uses a probabilistic algorithm. The inputs to this protocol are group public key, a membership certificate, a membership secret key and a message \( m \) with group signature \( \text{Sign} \) of \( m \) as the output.

Group signature is: \((c, s_1, s_2, s_3, s_4, s_5, A, B, D)\) Where

\[
c = H(m g / h / y / A / B / D / d_1 / d_2 / d_3 / d_4)
\]

Every group member can send the message through group signature. Every group member is treated as trusted vehicle for intra group member due to its group identity.

**Verify:** This protocol is known as algorithm of establishing the validity of the group signature, a given public key and signed message \( m \). Inputs of this protocol are group public key, the \( \text{Sign} \) of \( m \) and output is 1 or 0. If and only if \( c = c' \) then signature verification is successful and group signature is acceptable. When group member will broadcast a message to other vehicles within transmission range then the other intra group member vehicles can trust in the absence of infrastructure.

**Open:** This protocol is known as deterministic algorithm that, given message and group secret key, determines the identity of the signer. Inputs of this protocol are message \( m \), signature \( \text{Sign} \) of \( m \), and the secret key \( S \) of the group manager. The output of this protocol is 1 or 0 (identity or failure). When group manager will find that trusted value of any group member is below the threshold value or any misbehavior nature of the group member then group manager will remove the vehicle (group member) from the group.

A secure group is able to provide anonymity, where, actual signer cannot be identified from the group; unlinkability of two different signatures of the same group member; However, the group manager can always reveal the identity of the group member and finally no non member can forge and sign a message on behalf of the group. Different members of a group including the group member cannot collude and sign for a member.

**IV. RESULTS AND DISCUSSION**

In this section, the proposed trust management for VANET has been evaluated through simulation of real traffic scenarios \[28\]. A road with multiple unidirectional lanes is considered. The vehicles move in a single direction with different speeds and multiplicity of the lanes allows vehicles to overtake each other without any restriction in the number of lanes. The total length of the road is taken as 18 km with segments of 3 km each. In our experiment, we have taken 20% of malicious vehicles and 70% of malicious vehicles to evaluate efficacy of proposed trust management framework respectively. Fig. 1 shows that trust level of vehicle in VANET increases in three phases. The first phase is linear while other phases are exponential in nature. This nature is vice versa i.e. when trusted vehicle will increase around the vehicle then trust level will increase, similarly when malicious vehicle will increased around the vehicle then trust level will decrease in same three phase manner.

![Trust values curves in a VANET](image)

![Number of vehicle](image)
Fig. 3 Number of vehicles (malicious vehicle 20%), Speed = 10 m/s & Acc./Dec. = 5 m/s²

Fig. 4 Number of vehicles (malicious vehicle 70%), Speed = 10 m/s & Acc./Dec. = 5 m/s²

Fig. 2 and Fig. 3 show that at distance 9 km, the number of trusted vehicles is decreasing and malicious vehicles are increasing. In this case intra vehicle cannot trust any vehicle around itself but at this time a vehicle can trust the proposed trusted group vehicle’s messages and group formation is also possible at this time. Fig. 4 and Fig. 5 show that for high percentage of malicious vehicles i.e. 70% around the vehicle, the initial peak is lower than the 6th, 12th and 18th km distance peaks where the number of malicious nodes can be seen to be increasing. Evidently, the malicious node population steadily increases as we move towards the last junction. In this case, a trusted group is essential to provide trust in vehicles among themselves.

V. CONCLUSION

The present study dealt with the challenge of trust management using reputation based trust group formation. The scheme achieves formation of dynamic trusted groups around pre-trusted vehicles regardless of the percentage of malicious vehicles. The group formation mechanism is distributed and independent of the roadside infrastructure. It provides anonymity and traceability of group member vehicles in VANET. This makes the scheme viable for implementation in VANET environment. However, further research is required to formation of group on demand and also when pre-trusted vehicles are not present in a region.

REFERENCES


**Brijesh Kumar Chaurasia** is pursuing Ph.D. from Indian Institute of Information Technology, Allahabad, India. He received his M. Tech. Computer Science and Engg. from D.A.V.V., Indore, India. His research interest areas are Security in Wireless Ad-hoc Networks and Wireless Sensor Networks.

**Shekhar Verma** received his Ph.D. degree from IT, BHU, Varanasi, India in Computer Networks. He is Associate Professor at Indian Institute of Information Technology, Allahabad, India. His research interest areas include Computer Networks, Wireless Networks and Communication, Wireless Sensor Networks, Information and Networks Security.