Design Secure Connectivity Protocol to mitigate malicious activity using Game Theory in VANET

DR.J.NASKATH
Assistant Professor (SG),
,Department of Computer Science and Engineering,
National Engineering College, Kovilpatti, Tamilnadu, India.

DR.NITHYANANTHAM SAMPATH KUMAR
Assistant Professor,
School of Engineering,
Department of computer science and Engineering, Presidency University,
Bangalore,Karnataka, 560064

M.PAPPATHI JANCY RANI
Research Scholar,
Department of Computer Science and Engineering,
National Engineering College, Kovilpatti, Tamilnadu, India.

Abstract:

Nowadays, Governments, academic institutions, and the corporate sector are fascinated by the new ad hoc type of Intelligent Transport System (ITS) known as Vehicular Ad Hoc Networks (VANET). A VANET network has a significant demand for security due to the sensitive nature of the data it transmits. Hence, it is obligatory to design a secure connectivity conventionality to safeguard the normal vehicles from malicious attacks. Game theory assists to solve selfishness issues between the vehicles that deal with the rational and strategic behavior of the vehicles. Perfect Bayesian equilibrium (PBE) gives a solution for flagging games to solve the problem of inadequate data by joining methodologies and result of players that establish agreement. To identify and visualize this malicious activity, the proposed game theory model portraits a Bayesian signaling game to induce better data exchange and communication.

Keywords: *security protocol, Perfect Bayesian equilibrium, game theory, Bayes rule, connectivity conventionality, belief update, VANET*

INTRODUTION

The rapid arise of wireless communication networks has lead to the development of more secure VANETs. Wireless Networks are computer networks without any cabling. Mobile Ad-Hoc Network (MANET) is a group of nodes or terminals that communicates and exchanges information with each other without any centralized administrator. VANET falls under the category of Ad-hoc Networks and plays a vital role in Transportation and Traffic Management. VANET is a mechanism that considers each vehicle as a node, induces communication and exchanges information with each other in Vehicle-to-Vehicle Communication (V2V) and Vehicle to Road Side Communication (V2R). VANETs are a sub domain of MANETs (Mobile Ad-hoc Networks) generally providing communication services between two or more vehicles and between vehicles and Road Side Units. The main role of these components is to provide secure communication. Although VANETs plays a key role in the deployment of science and research, they have many issues and challenges in real

https://doi.org/10.37896/pd91.5/9154

world. One of them is Secure Connectivity. VANETs are an open network where any vehicle is allowed to join the network. There is no certain mechanism, that can ensure the trustworthy nature of the vehicles. Therefore, security becomes a major concern for researchers as communication between vehicles happen over a wireless medium where any node can transfer malicious data and may cause significant harm to other vehicles. Traditional connectivity algorithms are not prescribed due to the mobility[33] and dynamic nature of the vehicles in VANET architecture[34]. Usage of innovative algorithms stays as a challenge in VANET. Game theory is a game where multiple players interact with each other and one player's payoff is affected by the decision made by the other players [19,21 & 22]. It has two main branches: Non - Cooperative game and cooperative game. Non - Cooperative game theory covers competitive social interactions with some winners and some losers. The Prisoner's Dilemma by embedding 5G networks in VANETs, it can ensure high reliable and safe data forwarding. However, security threats can also prolong with these advantages. In work [1], a Puzzle Based Co-Authentication (PCA) scheme is discussed to overcome authorization and authentication difficulties. The hash functions incorporated can slower the process as only a checksum hash is used. Data communication in VANETs still remains a challenge with dynamic topology [2]. VANSec, a new trust management approach is more resistive to different kinds of network layer attacks [18]. Data theft and networks eavesdropping lead to huge risk in real time world entities. Hence, in study [3] the passive and active attack scenarios are discussed to mitigate data security issues. An attack and defense game is proposed to analysis the strategic behavior of each vehicle and based on the final strategy the malicious activity is visualized [29 & 30]. In the proposed system, dynamic Bayesian signaling game [31] is used to analyze the strategy profile of the regular and malicious vehicles. Collaboration between vehicles is the most problematic issue for forwarding packets between vehicles. To overcome this drawback an algorithm is designed to find the finest response strategy and the belief strategy pairs in the game. First, it formulates a two - player dynamic Bayesian signaling game for the sender and receiver. Pure strategy, mixed strategy and Perfect Bayesian Equilibrium (PBE) are the Nash equilibrium strategies to be analyzed to find the best strategic interaction outcome of the players. Then, the payoff is calculated for sender and receiver vehicles for motivating the particular vehicles that are misbehaving [24]. Based on the action picked and message sent by the players, the belief update is calculated for each vehicle using Bayes rule. The probability of the vehicle's type is determined by the strategy picked by the players. Finally, countermeasures are taken to distinguish regular vehicles from malicious vehicles and malicious attacks are predicted to improve efficiency. The rest of the paper as organized as follows. The various contributions of other authors are illustrated in Section II. In Section III, an algorithm is proposed to determine the vehicle's strategy and articulate the payoff matrix. It also determines to find the finest response strategy and the belief strategy pairs in the game. The various performance analyses regarding average utility, the strategy of vehicles, throughput, routing overhead and routing latency are discussed in Section IV. Finally, the result is concluded in section V.

RELATED WORKS

Data exchange and communication between the nodes is complex in the presence of malicious activity. Regular nodes stand in a pivotal space to support and secure data access. In study [4], the paper accentuates a framework to represent the false actions of the malicious nodes, also favoring high network utility. A decision making model is designed to visualize and locate the malicious and regular activities. The behavioral pattern of the abnormal and malicious nodes is simulated by monitoring the trends of the node's strategy. In the proposed approach, detection or identification of a specific malicious node is not considered, which remains as a drawback.

Network layer plays a vital role in data dissemination in VANETs. Data communication between the vehicles differs in various parameters. In work [5] the authors discussed about the network layer attacks and game theory techniques used in VANETs [23 & 25]. This study deals with both co-operative and non- cooperative gaming approaches to ensure security. In spite of various approaches, the solutions to overcome security issues are still limited and less identified.

Malicious nodes exhibit an incredible behavior similar to regular nodes. Due to this confusing behavior, visualizing these malicious nodes through traditional simulation techniques is complex. In [6] the authors discussed a game theory multi-attacker collusion approach to identify the unpredictable behavior of the malicious nodes in various aspects. Here a strategic decision making algorithm is designed to analysis the behavior of the nodes. Also, PBE model is initiated to sketch the wrestling between the malicious and regular nodes. The outcome of the above approach is simulated only in the case of single attacker nodes.

Co-operative Intelligent Transport System (CITS) are extensions of VANET, where communication in between the vehicles is autonomous. In this type of unique driving, vehicles can sense information with the help of various sensors. The authors in [7 ,26 & 27] design a game theory algorithm to detect the insider attackers present within the dynamic network. This algorithm classifies the behavior and past information of the attackers. The CITS model supports all the basic components in VANET architecture. The Medium Access Control and Physical layers are specified in IEEE 802.11p structure. Moreover, an efficient clustering model is organized to save energy and time delay. The main drawback of this clustering approach is to maintain equality within the vehicles.

In cooperative game theory, the two players must deliver equal amount of trust for secure communication. Trust management in VANETs is still difficult to achieve due to the change in the network topology during mobility[39]. In [8] the authors design a robust approach to monitor the communication between the players. A payoff matrix is calculated based on the chances of the action and reaction link. It is a defend and attack security model to detect the abnormal nodes. This algorithm simulates better results in performance and other metrics. This approach is not suitable for non-cooperative games with multiple players.

Vehicle mobility and speed mainly affects the network security in both rural and urban areas [33]. Clustering with an enhanced topology overcome the adversities due to some physical parameters[34]. The proposed system in [9] improves the Signal-to-Noise Ratio (SNR) and capacity of the channel by designing a potential clustering model in VANETs. The vehicles with similar characteristics are grouped into clusters. Based on the SNR value, the coalition value is formulated. This model is significant for unreliable and low communicative vehicles.

Enhancing securities in dynamic networks is tedious in changing infrastructure. In [10] the authors accentuate an Optimized Link State Routing Protocol (OLSR).The proposed system incorporates a co-operative approach with many players and multiple interactions. Every node monitors the Cooperation Rate (CR) of the other nodes and checks the activity log frequently .This CR value is also reported to the other neighbor nodes and hence the malicious node's activity and movement is prevented. Parameters like overhead, routing latency, energy etc. are not considered while implementing this propose model[35]. Safe data exchange or packet delivery in VANET is feasible when interactions among the vehicles are secure [35 & 36]. To overcome the challenge of handling vehicles with incomplete information, Public Goods Game (PGG) is preferred in areas of high vehicle density. In [11] the paper focused on the issue of enhancing co-operation in VANETs. A Greedy Neighbor Selection (GNS) is chosen instead of a regular static strategy. The defectors and contributors follow the GNS strategy and the probability greedy value is calculated for each node. Then grouping mechanism is carried out to group the regular nodes in the network. Hence, this reputation system increases the co-operation rate between the vehicles. This algorithm is highly efficient but does not support the system to be scalable.

The regular duty of a regular node is to monitor the surroundings and identify abnormal activities. The malicious node attacks the normal node with maximum time intervals to avoid arresting by the normal node. The authors in [12 & 32] deal with a game model to cooperate and decline in the wireless infrastructure. The concept on Markov Perfect Bayesian Nash Equilibrium is produced to update the belief of the nodes. This models the delay of the malicious node attack. The distinct characteristics of each attack and essential techniques differs in nature, hence this proposed system is not applicable [28]. In [13], an Efficient Computational Modeling (ECM) approach is introduced to induce better collaboration among the regular nodes and detect the malicious nodes. The framework analysis a dynamic multi-stage Bayesian signaling game which employs a decision making model to determine the actions performed by the nodes. The main drawback is the time factor, which is to be classified into separate slots making the proposed study tedious. Occurrence of observation errors is high.

Beacon collision generally takes place in areas with large vehicle density. Channel overloading, path location and transmission delay also lead to beacon collision. In order to avoid high collision, a decision-making algorithm is designed considering the model of Medium Access Control [14]. As the vehicles are aware of each other's type, Bayes rule is played and the response strategy is calculated. The packets in this proposed system are transmitted based on channel gain and threshold value. The packets are independent of the Congestion Window (CW) size, as it results in long delay periods. The optimum and sub-optimum values for co-operative game theory vehicles were not discussed in this existing approach.

Unmanned Aerial Vehicles (UAV) are vehicles mannered by a remote control or onboard system. They are revolutionary in areas of high security concerned needs. These vehicles are also termed as drones or Remotely Piloted Aerial Systems (RPAS).This paper deals with enhancement of network and other performance metrics with UAV's[15]. Nash bargaining solution (NBS) is formulated in these drones to determine the close period of the probability encounter value. Using NBS, only the solution with optimal efficiency while considering equal fairness is achieved.

Clustering or grouping is categorized into Single-hop clustering, Multi-hop clustering. In this mechanism, the nodes depend on mediatory nodes for path selection and communication. Preservation of resources such as energy and bandwidth. is a challenging task in dynamic networks. To overcome these challenges, the authors in [16] centralize a scheme to avoid the problem of route fiddling. In this model, a dynamic theory to give differential punishment mechanism for fiddling nodes is deployed. Based on both local reputation information and global reputation information the misbehaving nodes are classified and the Dynamic Chips Allotment (DCA) mechanism is applied [24]. These mechanism portraits only the direct misbehavior of the node and the more challenging indirect behavior is not focused.

Tracking of nodes in mobility is not scalable. Enhancing cooperation and achieving connectivity among the nodes is a key factor in VANETs [37 & 38]. In [17] the authors presented a Public Goods Game (PGG) to simulate better cooperation in VANETs. Abnormal nodes try to flip out from the model to preserve their resources. Using this decision model, it is compulsory for nodes or vehicles to take part in the game. Acquiring this PG game also gives greater efficiency with low cost contribution. The final benefit is calculated as the total of all the contributions. The same is applied to both rural and urban environment and simulations are carried out[36 & 37]. Even though this model is appropriate in all types of network, optimization results are complex.

PROPOSED WORK

Routing and network performance are the main constraints to be considered while designing VANETs. As malicious nodes are termed to degrade the performance of VANETs, dynamic Bayesian signaling game is used to reveal vehicles with normal and abnormal activities. In this approach, co-operative game theory is chosen. Fig.1. gives the detailed flow diagram of the proposed system. The game consists of two players Vehicle 1 (V1) Vehicle 2 (V2) where V1 acts as the Sender and V2 as the Receiver. Here V1, V2 are not aware of each other's type. A = $[a_1, a_2 \ldots a_j]$ is the set of messages from which V1 chooses a message and sends it to V2. Finally V2 fixes the required action from the action space B = {Cooperate(C), Decline(D)}. Perfect Bayesian equilibrium (PBE) is a strategy in which V1 chooses the message and V2 chooses the action. The node's strategy is determined by the payoff calculation and belief update mechanism. It can be either pure, mixed, or PBE. In the case of pure strategy, the vehicle's type cannot be altered or changed. In PBNE (Perfect Bayesian Nash Equilibrium) based on the type of the other players, the strategy profile and the beliefs are specified for each player. In this approach, some of the sender and relay vehicles exhibits abnormal activities and are termed as malicious. This information about the malicious nodes is reported to the neighbor vehicles.

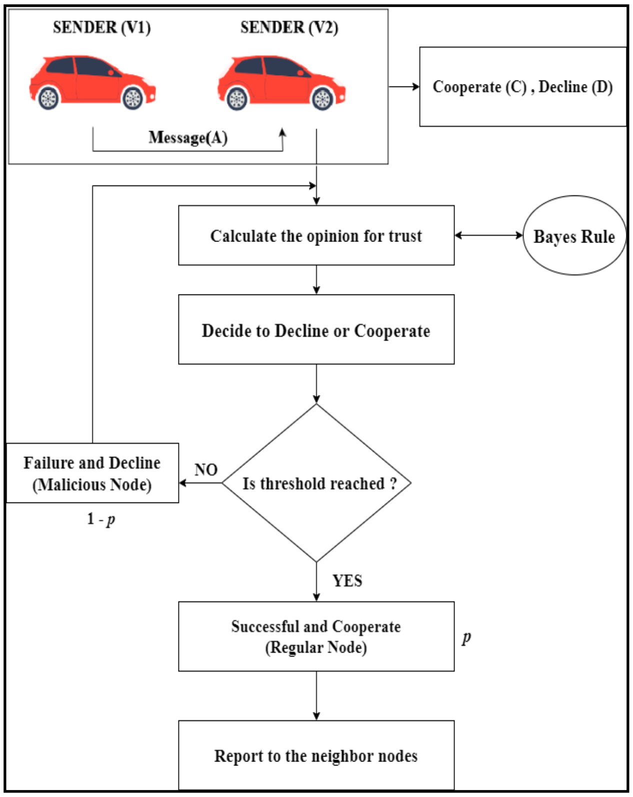
SENDER (V1)
SENDER (V2)
Message(A)
Cooperate (C) , Decline (D)
Calculate the opinion for trust
Bayes Rule
Decide to Decline or Cooperate
Is threshold reached ?
NO
Failure and Decline (Malicious Node)
1 - p
YES
Successful and Cooperate (Regular Node)
p
Report to the neighbor nodes

Fig.1 Flow diagram of Proposed System

A. Algorithm to choose feasible action for players.

```
Input: Two players [Sender (V1), Receiver (V2)]

Output: Project the malicious activity

Start:

    Initiate Vehicle (V1) and Vehicle (V2)

    Define the strategy profile of the players.

    Determine the vehicle's type {Regular or Malicious}

    Apply Bayes rule and analysis the belief for the vehicles.

Apply Bayes rule and analysis the belief for the vehicles.

    Intend the optimal payoff for V1 and V2.

    Find the operable action{C or D}
```

```
if not operable then
    Convey to other vehicles/nodes as malicious
else
    Choose to Cooperate or Decline (C or D)
end if
Stop
```

The sender V1 has type δ = {Regular, Malicious}. The receiver V2 trusts its own type as probability of p(δ) is 1.The sender V1, observes the information about its own type and decides to choose an action. Similarly, V2 checks the action chosen by V1 and chooses a reaction. Here, $x_i(c, d, \delta)$ denotes the payoff of the sender vehicle V1, $p_1(\delta)$ denotes the probability distribution for the sender's strategy over the action Cooperate (C) and ρ_2 (y_1) denotes the probability distribution over the action Decline (D).

Sender's payoff is calculated in Equation (1)

$$x_1(\rho_1, \rho_2, \theta) = \sum_{y_1} \sum_{y_2} \rho_1 (y_1|\delta) \rho_2(y_2|y_1) x_1(y_1, y_2, \delta) \qquad (1)$$

Receiver's payoff is calculated in Equation (2)

$$x_2(\rho_1, \rho_2, \theta) = \sum_{\delta} p(\delta) \sum_{y_1} \sum_{y_2} \rho_1 (y_1|\delta) \rho_2(y_2|y_1) x_1(y_1, y_2, \delta) \qquad (2)$$

where y_1 and y_2 are the actions chosen by V1 and V2.

$$P_{V1} : \forall\ \delta,\ x_1(\rho_1^*, \rho_2, \theta) \geq x_1(\rho_1^*, \rho_2, \theta), \qquad (3)$$

$$P_{V2} : \forall, y_1 x_2(\rho_1^*, \rho_2, \phi) \geq x_2(\rho_1^*, \rho_2, \phi^*), \qquad (4)$$

$$P_Q: \phi^*(\delta|y_1) = \frac{p(\delta)\rho_1^*(y_1|\delta)}{\sum p(\delta')\rho_1^*(y_1|\delta')} \qquad (5)$$

where $\phi^1$is uncertainty of nodes and P_{V1} , P_{V2} are the perfect Bayesian Equilibrium for the sender and receiver. The belief of type δ is given by P_Q . In case of mixed strategy, the stranger can have two types: {Regular, Malicious}. The probability for stranger vehicles to be determined as malicious and its action space is given as {Attack, Normal}. P_{V1} always behaves normally as it's probability is determined to be regular. {Doubt, Trust} are the two actions the neighbor nodes may perform on the stranger. When a 'Doubt' arises, the neighbor's help is asked to find the trustworthiness of the stranger.

B. Payoff Articulation

Generally, payoff ate the outcomes of the players in the game. It is usually a number. The brief procedure is as follows:

1. *Consider a stranger to be a regular vehicle, 'g' amount of payoff will be obtained by the target if it trusts, where* $g > 0$.

2. Consider a stranger to be a malicious vehicle; an amount of harm 'h' is caused to the target, if the target is attacked successfully. $0 < h < 1$

3. Consider the stranger being doubted by the stranger, then it costs 1.

4. Consider the stranger to be a malicious vehicle but pretends to be a normal one. In this case, the cost is more for the target to doubt, but the target may threaten the stranger more frequently.

5. For invaluable trust, the payoff lost by the target is 'h' amount.

As in dynamic Bayesian signaling game, decline is a strategy dominated by cooperate, (D) is the best result.

C. Pure Strategy:

In pure strategy, the vehicle chooses the strategy those outcome the highly beneficial payoffs. This strategy provides at most profit to the players. The Nash Equilibrium is an action profile in which a vehicle is restricted to increase or decrease its payoffs. Consider the strategies {Attack, Doubt} and {Normal, Trust}. If the receiver response to the sender as “Doubt”, then the sender vehicle is aimed to show malicious activity. Similarly, if the receiver vehicle response to the sender vehicle as “Trust” then the sender vehicle is aimed to show normal activities.

D. Mixed Strategy:

In the case of mixed strategy, the vehicle chooses more than one action based on the probability value in the strategic game. Here one of the two players plays a randomized strategy.

Definition 1: A mixed strategy is a neutral strategy for players to choose n number of actions dependent over the probability distribution, where $\mathrm{n} = (\mathrm{n}_1 + \mathrm{n}_2 \ldots \ldots \mathrm{n}_\mathrm{k}) = 1$.

E. Perfect Bayesian Equilibrium:

PBE, a strategy profile whose payoff is dependent on its own belief and other players belief, regarding to update beliefs based on Bayes rule. The strategy is given by $\rho = (\rho_1 - \rho_2)$ and the fact set is given by $\mathrm{X} = \{\mathrm{x1}, \mathrm{x2}, \mathrm{x3}\}$. Equations (6), (7) and (8) calculates the probability distribution on X.

$$\phi(x1) = \alpha q, \qquad (6)$$

$$\phi(x2) = \alpha(1-q), \qquad (7)$$

$$\phi(x3) = 1 - \alpha \,. \qquad (8)$$

The payoff of the receiver and the differential coefficient is calculated in the equations (9) and (10).

$$\phi(\rho) = (3h-g)\alpha q t + (g-h)\alpha q + (g\alpha - h\alpha - 1)t + g(1-\alpha). \quad (9)$$

$$\frac{\partial \phi}{\partial q} = (3h-g)\alpha t + (g-h)\alpha \,. \quad (10)$$

Finally it $^{\text{is}}$ concluded as if q increases, the expected payoff the receiver(V1) will increase .

$t > \frac{g-h}{(g-3h)}$, considering the Equation (9) < 0.

E. Calculating the payoff

Payoff of the regular and malicious vehicles constitutes the player's vantage point. This payoff depends on the player's action and the action of its neighbors. Fig.(2) portraits the payoff calculation of each vehicle. Based on the expected payoff value, corresponding action is chosen by the sender and the receiver. Decline (D) is categorized for a node that is rejected for participating in packet forwarding. Cooperate(C) means that the vehicle can cooperate for packet forwarding.

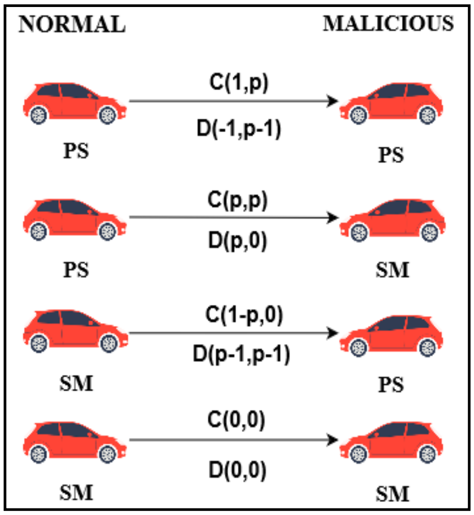

Fig.2 Payoff Calculation

Here, the sender receives a certain amount of payoff if it attacks the receiver. In the case of Decline (D), the regular vehicle has zero gain. If the receiver finds the sender to be malicious, it reports to the neighbors and fetches the gain Signaling Malicious(SM). Here PM (Prefer to Send) and SM are the profit gained to report and cooperate. (PSPS, C) and (SMSM, D) are the Nash Equilibrium for Perfect Bayesian Game. In the first case, (SMSM, D) - the sender avoids to send the message and checks in for decline. In the second case, (PSPS, C) - the sender sends the message and as the final step the receiver chooses to cooperate or decline. Hence based on the vehicle's type payoff is calculated.

F. Belief Update Mechanism

Malicious vehicles can raise the overhead and this leads to performance degradation while communicating. Belief updating needs to be carried out to avoid this issue. It is given by

$$p(\theta|a) = \frac{p(\theta')\rho(a|\theta)}{p(\theta)\rho(a|\theta)}$$

where ρ denotes the action and a is the message that the sender sends. The trust opinion is determined using Bayes rule. Decline(D) is categorized for a vehicle that is rejected for participating in packet forwarding. Cooperate(C) means the vehicle can cooperate for packet forwarding. Malicious and regular vehicles are determined by the belief update process. The following algorithm finds the belief strategy pairs for the PBE strategy.

INPUT: Incomplete information of the Sender (V1) and Receiver (V2).

OUTPUT: Belief strategy pairs for PBE.

MAIN:

Find the $Type\ t_n$ for $V1_n$ from $type$ = {T,……T_L} based on the distribution p(t_n), where p(t_n) > 0V_i and $\sum_L$ p(t_n) =1. $V1_n$ sends message $A_{sg_j}$from A ={$a_1 \ldots\ldots a_j$} depending on the observed T_n. $V2_n$ chooses a reaction $V2B_k$ from B ={$V2B_1$…..$V2B_k$} depending on the observed A_{sg_j}

Calculation of payoffs for Sender ($POV1$) and Receiver ($POV2$):

$POV1_n(t_n, A_{sg_j}, V2B_k)$, $POV2_n(t_i, a_j, x_k)$

$V2_n$ has a belief ϕ($t_n|A_{sg_j}$)

```
**for** each $A_{sg_j}$ ϵ A, V2B * $A_{sg_j}$; **do**
    max $a_j$ ϵ A $V1_n(t_n, A_{sg_i}, a_k)$
**end for**
**for** each $t_n$ ϵ $Type$, $A_{sg}$* $t_n$ do
    max $A_{sg_j}$ ϵ $A\ \sum t_n$ ϵ $Type$
**end for**
```

Pure strategies:

$$ϕ(t_n|A_{sg_j}) = \frac{p(t_n)}{\sum t_n\, \epsilon\, Type} = p(t_n)$$

Belief strategy pairs (PBE):

[A_{sg}* t_n ,V2B * A_{sg_j} ϕ($t_n|A_{sg_j}$)]

Performance Analysis

In this analysis section, various parameters are assessed using NS-2 simulation. Pure, mixed and PBE strategies of regular and malicious vehicles are evaluated. Table 1 depicts the various parameters used in this simulation. Nearly 45 percent of the vehicles are analyzed to show malicious activity. The proposed approach is compared with two more existing approaches and the results are simulated.

PARAMETER	VALUE
Simulation area	1000 m× 500 m
Simulation Time	1000 s
Density of vehicles	50-80 vehicles
Transmission range	50 m
Mobility model	Freeway model
Speed of Vehicle	[20-60] m/s
Packet size	512 bytes
Pause Time	400 s

Table 1. Parameters for Simulation

Node Utility:

Node utility shows the final value of payoff of the vehicles. The payoff matrix gives the value of the expected payoff. The expected payoff is the product of type of node of payoff of the action in probability. Based on this payoff, related action is chosen by the sender and the receiver. Figs. (3) and (4) simulates the respective strategy with each vehicle's utility. In both the cases, the vehicle's strategy is high when following the PBE strategy.

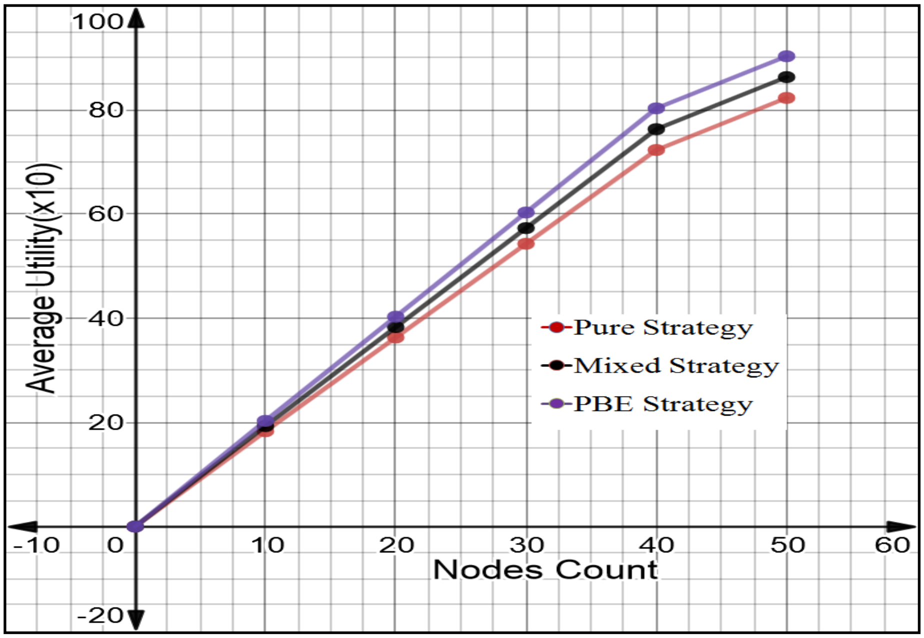

Fig. 3. Utility of regular vehicle in malicious vehicle strategy.

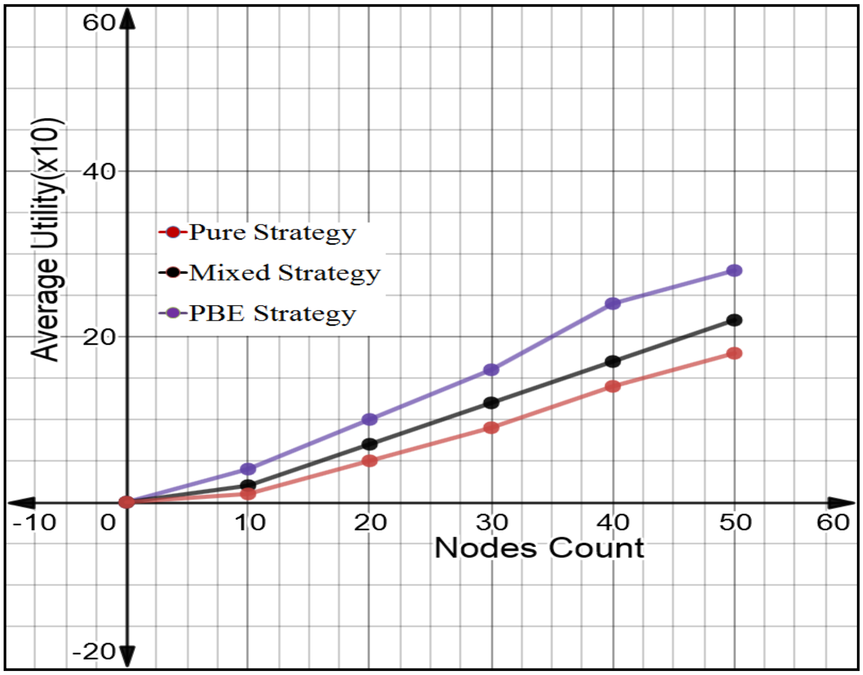

Fig. 4. Utility of malicious vehicle in malicious vehicle strategy.

Strategy of Nodes:

The node's strategy is determined by the payoff calculation and belief update mechanism. It can be either pure, mixed, or PBE.In fig. (3), the regular or normal vehicle's utility is maximum obtaining PBE. As regular vehicles, co-operate securely with other regular nodes, the utility result is high. Similarly in fig. (4), the malicious nodes utility in PBE high. When comparing with both pure and mixed strategy. As the regular vehicle, reduces he expected payoff of the malicious vehicles they can be easily detected. This happens as a regular node has the ability to choose both mixed and pure strategies. The final utility value of the malicious vehicle is the least. This information about the malicious nodes is reported to the neighbour nodes by the regular node in the PBE strategy.

Throughput:

Throughput is termed as the amount of data packet transmitted from one vehicle to another. It is generally represented as data packets per second (pps). In this paper, various existing simulation algorithms like AODV, ECM- GT is analyzed with the results of the proposed approach (SCP). Fig (5) depicts the simulation results dealing with throughput in decimals. In our proposed system, the test is simulated with 45 vehicles. For each 5 percent of vehicles in count, the throughput value is plotted. The total simulation time is 1000 sec and pause time is around 400 seconds. The throughput value has a constant decrease with increase in the number of nodes. Considering the first 5 vehicles

https://doi.org/10.37896/pd91.5/9154

the result decrease from 0.9 to 0.88 having a fall of 2 percentage. For the next 20 percent vehicles, the result falls for nearly 6 percentage . The final decrease is only 10 percentages.

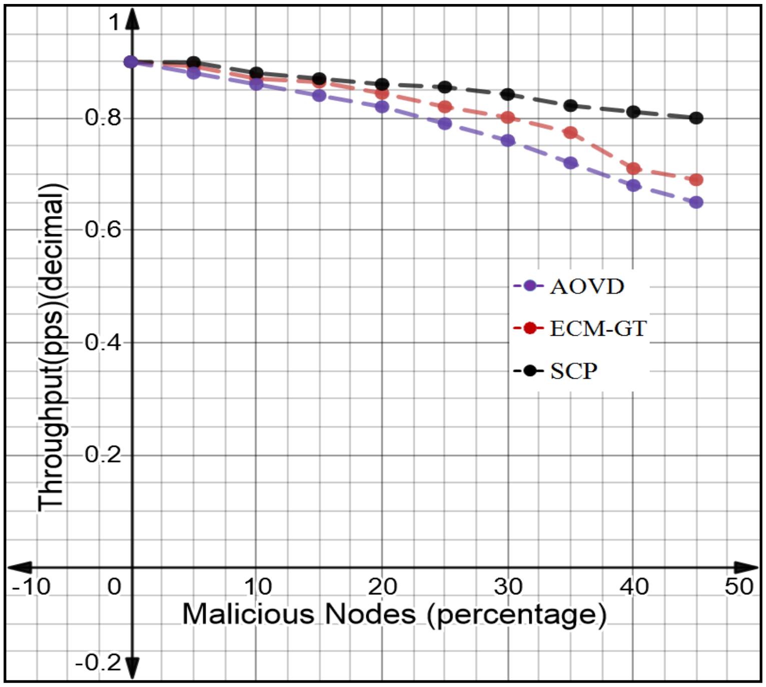

Fig. 5. Throughput with malicious vehicles.

Comparing with the other two existing approaches, Secure Connectivity Protocol (SCP) has high throughput having low fall percentage , whereas AODV has 25% and ECM- GT has 21 % as their existing fall percent.

Routing Overhead Analysis:

The count of routing data packets essential for a network for data communication is termed as routing overhead. Generally, higher efficiency is achieved with low routing overhead. Fig (6) shows how routing overhead is graphed for the three comparative models. It is clear that the proposed algorithm (SCP) has lower routing overhead value [19 & 20]. Compared to the other two approaches the routing overhead range is maximum for AODV approach hence it is causes time delay in data transfer. Initially the routing head value is equal for all the approaches. For the pause time of 400 seconds and first 10 percent of vehicles the algorithms depicts the percentage of 96, 90 and 82 respectively . In the stage of next 20 the algorithms are routed in a ratio of 1:2:2:5. In the final stage of routing overhead analysis, the proposed (SCP) model has the lower decimal value of 0.54, suffixed by ECM - GT with 0.6 (60 %) and AODV with 0.72 (72 %).

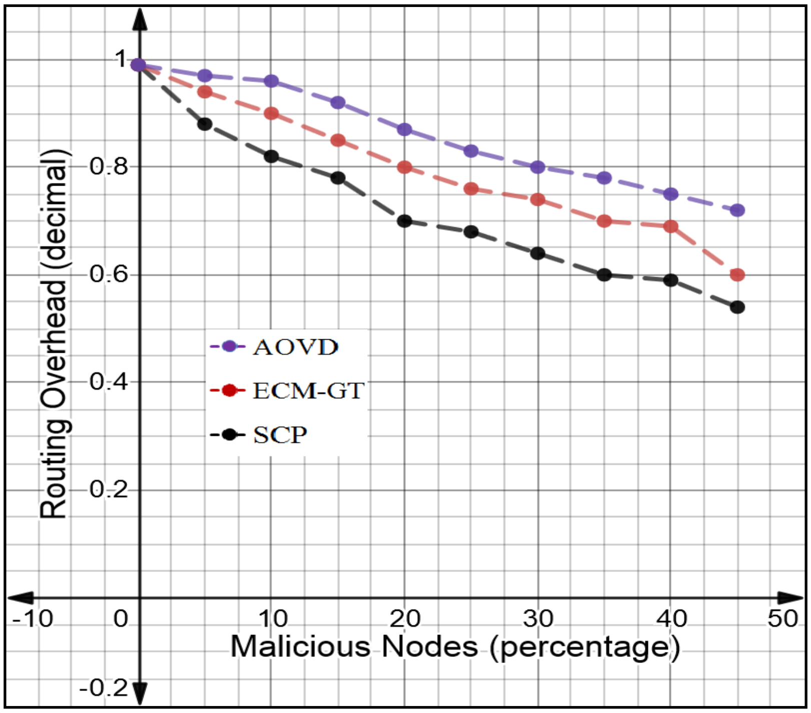

Fig. 6. Routing overhead with malicious vehicles

Routing Latency:

It is defined as the amount of time a sender takes to travel towards the processing sender. Fig (7) shows the routing latency comparison for AODV, ECM-GT and SCP approaches. In the proposed system, the routing latency has higher results than the other approaches. As this approach does not allow the malicious vehicles to forward packets, performance is high and efficient. The routing latency is nearly 99 percent at the initial stage. For the first 20 percent of malicious vehicles there is a tremendous decrease of percent to 85.Furthur for 45 percent of vehicles to misbehave, the routing latency pins with 0.78 in decimal. Hence, the proposed model shows a high percent of efficiency.

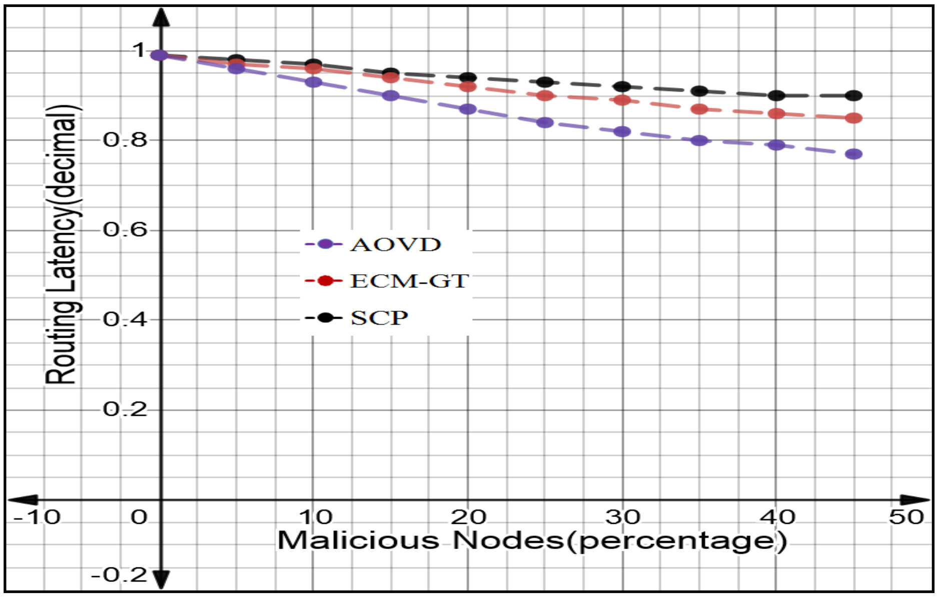

Fig. 7. Routing latency with malicious vehicles.

In this performance analysis, utility of regular vehicles and routing latency are seemed to be above 90% in comparison with other two models. It is also graphed that the proposed system has higher throughput than AODV and ECM-GT. Table 2 describes the comparison metrics of existing and proposed system.

METRICS	AODV (%)	ECM-GT (%)	SCP (%)
Utility of regular vehicles	82.4	86.2	90.5
Utility of malicious vehicles	28.1	22.5	18.0
Throughput	65.8	69.0	80.2
Routing Overhead	60.7	72.9	54.8
Routing Latency	77.7	85	90.1

Table 2. Performance metrics comparison

CONCLUSION

In order to reduce the abnormal activity of the malicious vehicles, an optimal secure connectivity protocol is designed. This proposed system visualizes and simulates the interactions between regular and malicious vehicles. To find the best outcome of the strategic interaction between the sender and the receiver, three Nash equilibrium strategies were analyzed. Malicious vehicles can raise the overhead and this leads to performance degradation while communicating. To avoid this issue, each vehicle updates its belief and reports to the other neighboring vehicles. If the vehicle has a type regular, co-operation is enhanced. If the vehicle is predicted to be malicious, it degrades the network performance with high packet drop.The PBE model adopted gives a positive solution to detect unexpected attacks from malicious vehicles and reduce eavesdropping. Thus, the system graphs far better results than the other existing approaches with high reliability and security.

REFERENCES:

[1] Muhammad Sameer Sheikh and Jun Liang, "A Comprehensive Survey on VANET Security Services in Traffic Management System," Journal of Wireless Communications and Mobile Computing, vol. 2, 2019.

[2] Yusor Rafid Bahar Al-Mayouf, Omar Adil Mahdi, Namar A. Taha, Nor Fadzilah Abdullah, Suleman Khan and Muhammad Alam, "Accident Management System Based on Vehicular Network for an Intelligent Transportation System in Urban Environments," Journal of Advanced Transportation, vol. 15, 2018.

[3] Garima Dhawan and Shilpa Nagpal, "An Overview and Evolution of the Intelligent Transportation System as VANETs," International Journal of Engineering and Computer Science, vol 5, 2016.

[4] Mohammed Saad Talib, Aslinda Hassan, Burairah Hussin, Ali Abdul-Jabbar Mohammed, Ali Abdulhussian Hassan and Ammar Awad Mutlag, " Vehicular Ad hoc Network for Intelligent Transport System: A review," International Journal of Engineering and Technology, vol. 7, 2018.

[5] HamssaHasrouny, Abed EllatifSamhat, CaroleBassil and AnisLaouiti, " VANet security challenges and solutions: A survey," Journal of Vehicular Communications, vol. 7, 2017.

[6] Rakesh Shrestha , Rojeena Bajracharya and Seung Yeob Nam, " Challenges of Future VANET and Cloud-Based Approaches," Wireless Communications and Mobile Computing, vol. 15, 2018.

[7] Shubham Kapoor , Surjeet, “VANETs: Basics, Issues and Challenges in its Practical Deployment,” International Journal of Engineering Trends and Technology, vol.57, 2018.

[8] Muhammad Sameer Sheikh, Jun Liang 2, and Wensong Wang, “A Survey of Security Services, Attacks and Applications for Vehicular Ad HocNetworks (VANETs),” Journal of Sensors, vol. 19, 2019.

[9] Gurpreet Singh, “ Overview of Challenges in VANET,” International Journal of Innovative Research in Science and Engineering, vol. 2, 2016.

[10] Qazi Ejaz Ali, Naveed Ahmad, Abdul Haseeb Malik, Gauhar Ali and Waheed ur Rehman, “Issues, Challenges, and Research Opportunities in Intelligent Transport System for Security and Privacy,” Journal of Applied Sciences, vol. 6, 2018.

[11] Kun Hua, Xing Liu, Zheyi Chen, and Mingyue Liu, “A Game Theory Based Approach for Power Efficient Vehicular Ad Hoc Networks,” Journal of Wireless Communications and Mobile Computing, vol. 1, 2017.

[12] Sri K.C.Kullayappa Naik, Madala Lakshmi Durga, Dr.Ch.Balaswamy, “Efficient Resource Allocation in VANET,” International Journal of Engineering Science Invention, vol. 6, 2017.

[13] Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang and Rongfang Bie, “Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends,” International Journal of Distributed Sensor Networks, vol. 2, 2015.

[14] VanDung Nguyen, Tran Anh Khoa , Thant Zin Oo, Nguyen H. Tran, Choong Seon Hong and Eui-Nam Huh, “Time slot utilization for efficient multi-channel MAC protocol in VANETs,” Journal of Sensors,vol. 9,2018.

[15] Xiaofeng Liu and Arunita Jaekel, " Congestion Control in V2V Safety Communication: Problem, Analysis, Approaches," Journal of Electronics, vol. 4, 2019.

[16] Muhammad Arshad1, Zahid Ullah, Naveed Ahmad, Muhammad Khalid and Haithiam Criuckshank, " A survey of local/cooperative-based malicious information detection techniques in VANETs," EURASIP Journal on Wireless Communications and Networking, vol.18,2018.

[17] G.Md.Nawaz Ali,Edward Chan and Wenzhong Li, " On scheduling data access with cooperative load balancing in vehicular ad hoc networks (VANETs)," The Journal of Supercomputing, vol. 7, 2015.

[18] Puguang Liu, Bo Liu, Yipin Su, Baokang Zhao1 And Ilsun You, "Mitigating DoS Attacks against Pseudonymous Authentication through Puzzle-based Co-authentication in 5G-VANET," IEEE Transactions on Aerospace and Electronic Systems, vol. 6, 2017.

[19] Yunhua He, Limin Sun, Weidong Yang and Hong Li, "A Game Theory-Based Analysis of Data Privacy in Vehicular Sensor Networks," International Journal of Distributed Sensor Networks vol.10, 2015.

[20] Sheeraz Ahmed, Mujeeb Ur Rehman, Atif Ishtiaq, Sarmadullah Khan, Armughan Ali and Shabana Begum, "VANSec: Attack-Resistant VANET Security Algorithm in Terms of Trust Computation Error and Normalized Routing Overhead," Journal of Sensors, vol. 4, 2018.

[21] Burhan Islam Khan, Rashidah F. Olanrewaju, Roohie Naaz Mir, Asifa Baba, Balogun Wasiu Adebayo, "Strategic Profiling for Behaviour Visualization of Malicious Node in Manets using Game Theory," Journal of Theoretical and Applied Information Technology, vol. 77-2, 2015.

[22] A. Ilavendhan and K. Saruladha, "Comparative study of game theoretic approaches to mitigate network layer attacks in VANETs," ICT Express, vol. 4-1, 2018.

[23] B. U. I. Khan, R. F. Olanrewaju, M. M. U. I. Mattoo, A. A. Aziz and S. A. Lone, “Modeling malicious multi-attacker node collusion in MANETs via game theory”, Middle-East Journal of Scientific Research, vol. 25- 3, 2017.

[24] Rens W. van der Heijden, Stefan Dietzel, Tim Leinmüller, Frank Kargl, “Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems ,” International Journal of Computer Science Issues, vol. 8-4, 2018.

[25] Muhammad Mohsin Mehdi, Imran Raza and Syed Asad Hussain, “A game theory based trust model for Vehicular Ad hoc Networks (VANETs),” Journal of Computer Networks , vol. 121, 2017.

[26] Selo Sulistyo , Sahirul Alam, and Ronald Adrian, “Coalitional Game Theoretical Approach for VANET Clustering to Improve SNR,” Journal of Computer Networks and Communications, vol.3, 2019.

[27] Hicham Amraoui, Ahmed Habbani, Abdelmajid Hajami and Essaid Bilal, “Security-Based Mechanism for Proactive Routing Schema Using Game Theory Model,” Journal of Mobile Information Systems, vol.2, 2016.

[28] Qing Ding , Xikai Zeng, Xinming Zhang and Dan Keun, “A Public Goods Game TheoryBased Approach to Cooperation in VANETs Under a High Vehicle Density Condition,” IEEE Transactions on Intelligent Transportation Systems, vol. 20-11, 2019.

[29] Wenjing Wang, Mainak Chatterjee, Kevin Kwiat and Qing Li, A game theoretic approach to detect and co-exist with malicious nodes in wireless networks, International Journal of Computer Networks, vol. 71, 2015.

[30] Burhan Ul Islam Khan, Rashidah Funke Olanrewaju, Farhat Anwar, Roohie Naaz Mir, “ECM-GT: Design of Efficient Computational Modelling based on Game Theoretical Approach Towards Enhancing the Security Solutions in MANET,” International Journal of Innovative Technology and Exploring Engineering, vol.8-7, 2019.

[31] Y. H. Kwon1 and B. H. Rhee, “ Bayesian Game-Theoretic Approach based on 802.11p MAC protocol to alleviate beacon collision under Urban Vanets,” International Journal of Automotive Technology, vol. 17-1, 2016.

[32] Mbazingwa E. Mkiramweni, Chungang Yang, Jiandong Li, Zhu Han, “ Game -Theoretic Approaches for Wireless Communications with Unmanned Aerial Vehicles,” International journal of Wireless Communications, vol. 12, 2018.

[33]Naskath, J, Paramasivan, B, et al. (2020) A Study on Modeling Vehicles Mobility with MLC for enhancing vehicle-to-vehicle connectivity in VANET. Journal of Ambient Intelligence and Humanized Computing, Springer, ISSN: 1868-5137, https://doi.org/10.1007/s12652-020-02559-x.

[34]J Naskath, B Paramasivan, B Shunmugapriya, Hamza Aldabbas, “Dynamic Cluster Based Connectivity Approach for Vehicular Adhoc Networks”,International Conference on Information, Communication and Computing Technology187-197,Springer, Cham. 2019.

[35] Anjali Anand, Himanshu Aggarwal, and Rinkle Rani, “Partially Distributed Dynamic Model for Secure and Reliable Routing in Mobile Ad hoc Networks,” International Journal of Communications and Networks, vol. 18, 2016.

[36]Zhihua Cui, Fei Xue, Xingjuan Cai, Yang Cao, Gai-ge Wang, Jinjun Chen, “Detection of malicious code variants based on deep learning”,IEEE Transactions on Industrial Informatics Volume 14,Issue 7,Pages3187-3196,2018.

[37]Naskath, J., Paramasivan, B., Mustafa, Z. et al. Connectivity analysis of V2V communication with discretionary lane changing approach. Journal of Supercomputing, https://doi.org/10.1007/s11227-021-04086-8,2021.

[38]J. Naskath et al. (2018). Location optimization for road side unit deployment and maximizing communication probability in multilane highway. International Journal of Heavy Vehicle Systems, Vol. 25, Nos. 3/4.

[39] Smitha Shivshankar and Abbas Jamalipour, “An Evolutionary Game Theory-Based Approach to Cooperation in VANETs under Different Network Conditions,” IEEE Transactions On Vehicular Technology, vol. 64-5, 2015.