International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 4, Issue 5, May – 2020, Pages: 21-32

Cooperation Methods in Vehicular Social Networking: A Survey

Lema Misgan[1*], Andualem Chekol[2]
[1,2]Department of information technology, institute of technology, Woldia University/ WLDU, Woldia, Ethiopia
Email: lemabest@gmail.com[1*], andualemchekol@gmail.com[2]

Abstract**:** *The main objective of this paper is to fill the gap of the current state of the arts in vehicular social networking cooperation methods and to indicate open issues that researchers should work on. Vehicular Social Network (VSN) is a cutting-edge communication system that provides an Intelligent Transportation System (ITS) services to the vehicles for providing fast information transmission and safety. VSN communications systems are mainly Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V), which employs wireless short-range protocols. In Vehicular Ad hoc Network (VANET), every node is armed device called On-Board Unit (OBU) and set of unwired sensors for node communication. A communication that mostly used for road safety application for example for collision avoidance is V2V. On the other hand non-safety applications for example navigation assistance and advertisement are handled with V2I communication. Vehicular Social Networking (VSN) formation is for three major reasons that are: (1) for an emergency, (2) for utility, and (3) for entertainment purposes. In VSN communication, there are Selfish vehicles that continuously trying to save their energy by deliberately fall the messages. To inspire these selfish nodes in forwarding packets, several credit-based and reputation-based stimulating protocols are suggested. Due to the exceptional features of Delay Tolerant Networks (DTNs), including the huge variation in network conditions and lack of periodic path, still it's difficult to detect DTN nodes' misbehave conducts. The major cooperation methods in VSN include punishment-based, incentive-based, reputation-based and misbehavior detection-based approaches. We collected a total of 70 papers and after doing exclusion criterion 38 papers were reviewed.*

Keywords: Cooperation methods, Emergency, Incentive, Misbehavior nodes, VSN

1. INTRODUCTION

1.1 Message Forwarding Schemes of Vehicular Social Networking

Road traffic accidents (RTAs) are a main community health fear, resulting in an millions of deaths and millions of injuries worldwide each year (Beshah, 2010, March) and (Authority, E. R., 2005).. The Rapid advancement of infrastructure and technology has prepared our lives calmer. The advancement of technology has also augmented the traffic risks and the road accident take place frequently which effects enormous loss of life and property due to the weak emergency services (Thakre, 2014).

The social car concept taken from the hypothesis that all drivers can exchange information with other nearby nodes based on mutual interests, for example, Ford concept car Evos can openly create a social network communication system with the driver's friends (Vegni, 2015).

Vehicular Social Network (VSN) is a cutting-edge communication system that provides an Intelligent Transportation System (ITS) services to the vehicles for providing fast information transmission and safety. Numerous routing protocols have developed for the implementation of routing in Vehicular Ad hoc Network (VANET). Maybe MANET routing protocols used to implement VANET but because of its high mobility, it is difficult to implement VANET using the same topology-based routing protocols (Bhoi, 2013)**.**

According to (Lu, 2010), VSN communications systems are mainly Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V), which employs unwired short-range protocols, then data transmission is vital to effectively exchange the information among vehicles. Consequently, most routing protocols of VANET are proposed and focused on exchanging data by totally exploiting unwired short-range information transmissions (Nitti, 2014).

To prioritize the highly relevant safety packets a multi-channel model and some Access Classes (ACs) can be used by IEEE 802.11p standards to ensure messages can be exchanged timely in a compact scenario (Eichler, 2007).

In VSN, for nodes communication nodes are equipped with an On-Board Unit (OBU) and many of unwired sensors by forming a mode of communication called V2V or in V2I like communication vehicles could communicate with a Road Side Units (RSU) (Barskar, 2015). The vehicles can then participate in intelligent transportation system where with the RSU located alongside the road. The RSU might be equipped by a trivial battery in non-urban areas with shortage of power (Nguyen, 2011).

"V2V communication is commonly used in road safety applications for example collision prevention. V2I communication, contrary is applied in non-safety related application or non-critical for example traffic update, navigation assistance, advertisement and therefore V2I way of communication may allow some delays (Ali, 2016). Message transmission in V2V

way of communication can be broadcast, multicast or multi-hop mode, on the other hand V2I uses single hop (Barskar, 2015).
Figure 1 Showed the V2I and V2V communications.

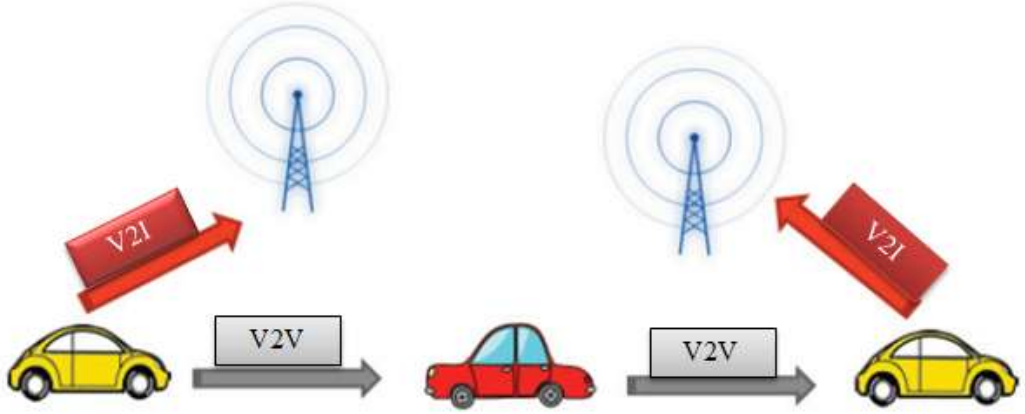

Figure 1. Modes of Vehicle communication in VSN (Hua, 2017)

Different from MANET, the mobility of the vehicles in VSN is roads restricted. Moreover, the mobility of nodes are also significantly influenced by the synchronization and operation of traffic lights. Consequently, the routing protocols developed for main road settings might not be proper for the traffic in town areas (Viriyasitavat, 2009). On the road there are at least 2 types of vehicle nodes that are bus and car. Therefore, the protocol developers should deliberately consider these conditions during routing protocol development for VSN (Luo, 2010). Routing protocols in VSN can be classified into 6 types which are Position-based, Topology-based, Broadcast-based, Geocast-based, Infrastructure-based and Cluster-based (Benamar, 2013).

Nearby to real-world mobility model must be considered during evaluation of routing protocol, (Fiore, 2007). In-vehicle to vehicle communications, multicast or broadcast schemes should be more applicable than unicast protocols especially if the message is accident-related messages, then it had to reach to all vehicles or nodes around the accident area to avoid chain accidents (Chen, 2011).

2. METHODOLOGY

2.1 Why VSN

As it is stated by researchers vehicular social networking (VSN) formation is for three major reasons that are: (1) for an emergency, (2) for utility, and (3) for entertainment purposes.

Vehicular social networks can become mainly valuable in the occasion of emergency. The emergency-based vehicular social networks could assist in a way for human to request for and give support to one another in serious circumstances like road accidents and street assist. There are vehicular social networks developed to exchange info about roadway events such as congestion, accidents, etc. Utility-based vehicular social networks are designed to simplify helpful but non-critical networks to occur. For instance, towns might launch vehicular social networks to exchange info about remarkable local events or critical things along main highways, for that passengers might ask questions for assistance in choosing a local hotel or restaurant. Refreshment-based vehicular social networks are designed for people to exchange common interests, such as, to discuss latest political and social concerns, sports, and many other refreshment issues (Smaldone, 2008).

2.2 PRISMA Diagram

As indicated in the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) flow-chart diagram bellow, a total of 70 papers were collected from Google scholar indexed databases and publisher. After applying exclusion criterion then a total of 38 papers was fully reviewed. The whole process is depicted in the fig 2, bellow.

PRISMA Diagram

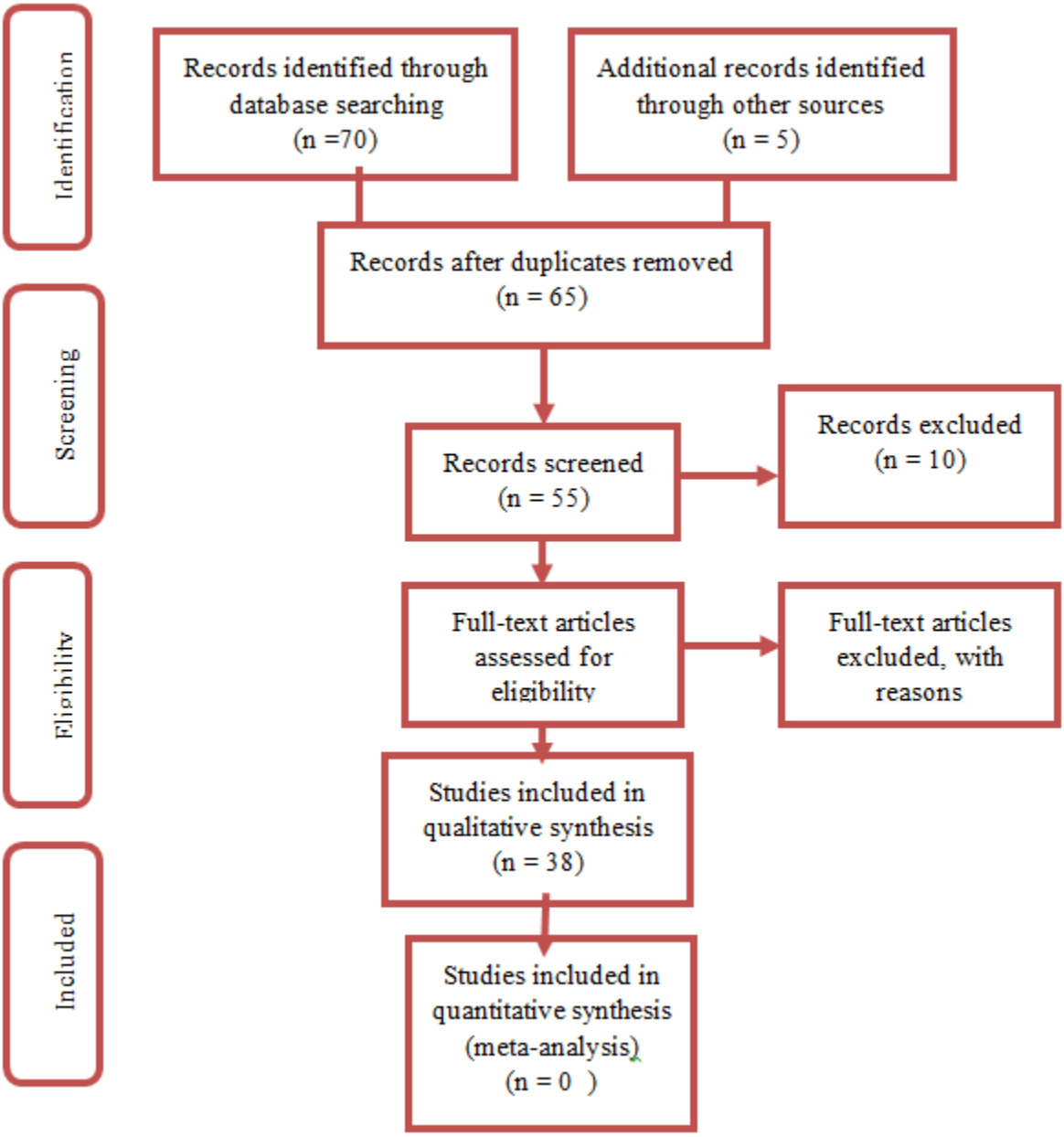

Fig2. PRISMA diagram of the review

2.3 **Payment Methods**

To inspire the selfish nodes in forwarding bundle, various "credit-based and reputation-based incentive protocols" have proposed. But, due to the exceptional characteristics of DTNs, such as the high variation in network conditions and lack of periodic path, it is difficult to detect delay tolerant networks nodes' misbehave conduct or prearrange a routing path. Thus, these difficulties in detect delay tolerant networks make the MANET incentive protocols, not applicable to DTNs (Lu, 2010).

The "intermittent connectivity and the opportunistic encounters between nodes within the communication system are a typical features of Vehicular ad hoc network" (Gong, 2014)**.**

2.3.1 Major Cooperation methods In VSN

In current years, we had seen several works stimulating vehicle's cooperation in VSN. Many popular methods for example reputation and incentive-based methods would use a centralized technique to handle a vehicle's reputation considering its past behavior & rewards the vehicles consequently (Shivshankar, 2014).

All the cooperation approaches are drawn in the fig3 bellow and the description of all the methods are stated after the taxonomy.

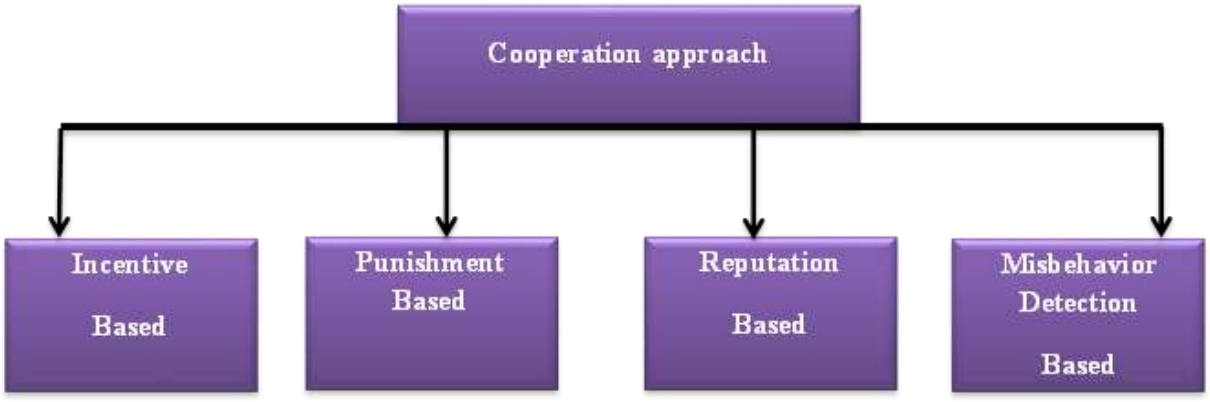

Fig3. Types of VSN cooperation approaches

2.3.1.1 Incentive-Based Cooperation method

In good condition, VANET design treats all vehicles in the system reasonably and accepts each vehicle would partake in message sending. Be that as it may, VANET is in some cases working in a harsh condition, for example, high vitality utilization and low data transfer capacity accessibility, bringing about certain vehicles declining to advance the message from different hubs. Such vehicles are called selfish vehicles, which consistently augment their benefit and would cause genuine deferrals and in the end influencing the whole execution of the system. Motivating forces or rewards can be given to stimulate collaboration. Different kind of impetus based collaboration has proposed as follows.

(Li, 2009), Proposed a strategy called FRAME to determine overspending and decency issues. FRAME involves two parts: A sweepstake segment and a weighted rewarding segment. A Weighted rewarding segment works so that each source must submit a fixed measure of rewarding Fr to the weighted reward. Accordingly, the nodes that take part in the bundle sending would acquire a portion of the prize. At the point when a packet has arrived at its goal, an affirmation will be dispersed over the VSN and put away in the proof assortment focuses. Subsequently, the sending organization authority will gather the proof, develop a tree, compute every node's evidence dependent on the weight of every node, lastly nodes would receive the grant.

The simulation outcomes of FRAME demonstrate the average prize increased as the nodes' participation increased. The FRAME design additionally demonstrates that it has a superior sending motivating force than the Proportional rewarding. Other than that, the conveyance proportion and entrance proportion with the FRAME plot is additionally higher than Receipt Counting and Proportional Rewarding strategies.

(Zhu, 2014), Proposed an inventive method to stimulate selfish vehicles by giving rewards to selfish vehicles and urge misbehave vehicles to transfer other vehicle's packets and reports their receipts genuinely. This is attainable by assigning out a credit value "C" to the last vehicle who sending the bundle to the goal node. The credit value "P" is assigned out to the previous vehicles. Consequently, if C<P, it infers that the previous vehicle isn't transmitting any packet and the Payment System (PMS) won't pay any credit an incentive to the vehicles that are not participate in information transmission. To dispose of cheating in the system, PMS would require the sending vehicles for an additional credit value if the goal vehicle doesn't report the receipts. The finding indicates that by stimulating the misbehave vehicles with motivating incentives, rather than punishing the misbehave vehicles can viably control the quantity of selfish vehicles in the VSN. Notwithstanding, the downside of this strategy is more vehicles will in general become selfish.

Receipt counting technique has proposed an adaptable motivating incentive strategy in light of the fact that the source vehicle could reclaim the beneficiaries before the message arrives at the goal vehicle. Nonetheless, it reveals overspending issues for the source vehicle for the most part because of the explanation that the source vehicle doesn't have power over the measure of reward

as the number of vehicles in the tree can't be predicted. To solve this issue, another motivating incentive strategy called the Proportional Rewarding technique was proposed. Proportional Rewarding technique just fixes the aggregate sum of the reward and remunerates the vehicles taking part in the transmission as indicated by their relative commitment. As the number of participants vehicles increment, the prize extent for a vehicle is diminished. This has brought about the middle vehicle that may want to keep its credits instead of sending the bundles.

To implement collaboration and fairness in LTE downloading among the vehicles in VSN, scheduling, and an incentive is required. (Wu, 2015), Proposed a game-theoretic technique of the group downloading as well as sharing, and a server helped key administration scheme where the friend association is kept up centrally and the information is transmitted through the of minimal cost Vehicles to Vehicles(V2V) transmission.

Table1. Incentive-Based Cooperation methods

Researcher	Proposed research	Technique	Remark
(Lu, 2010)	Pi: A Practical Incentive Protocol for Delay Tolerant Networks	Reputation-based and Credit-based incentives	If the bundle is not successful, no incentives for intermediate nodes
(Zhu, 2014)	Credit-Based Incentive in VANETs	Incentive-Based collaboration	The cooperative vehicles would become a misbehave vehicle deliberately of the rewards.
(Gong, 2014)	Social Contribution-Based Routing Protocol for Vehicular Network with Selfish Nodes	Social contribution	Social contribution is used as the incentive to incentivize misbehave vehicle to encourage its cooperation and the packet sending probability is determined by the social relations created among vehicles.
(Li, 2009)	FRAME: an incentive method in vehicular communication	Incentive-Based collaboration	Calculate every node's weight (forwarding contribution) and allocate rewards with the highest weight first basis.
(Zhu, 2009)	SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks	profit-sharing based incentive	Profit-sharing model: intermediate nodes participated in a effective packet transmission will be incentivized with a dividend of the sum of the credit given by the source node.
(Wu, 2015)	Incentive-based LTE Content transmission in vehicular ad hoc networks	Incentive-Based collaboration	At the first stage low throughput as many vehicles doesn't have the keys to encode the information they receive.
(Dias, 2015)	A Hybrid System to Stimulate misbehave vehicles to collaborate in Vehicular DTNs	Incentive-Based collaboration	Due to an growing numbers of nodes from the source to the destination, there is delay in information delivery.

2.3.1.2 Punishment-Based Cooperation approaches

Rather than rewarding incentives, a few investigations have proposed an increasingly intense approach to advance collaboration in VSN. These methodologies examine the vehicles, punish the selfish or misbehaved vehicles by including them into the boycott, and reject them from the system.

(Jesudoss, 2015), Proposed a collaboration approach by incentivizing truth-telling among the vehicles by means of punishing and rewarding (hybrid) approaches. Bundle transferring duty tumbles to Gateway and Cluster Head vehicles only. Watchdog is utilized to control the presentation of these transfer vehicles and to recognize on the off chance that they are helpful or non-agreeable vehicles. Installment will at that point be offered by the decision. Three vehicles go about as watchdogs for each hand-off, one is the predecessor of the hand-off vehicle, 2nd is the ACH & the 3rd vehicle is the part vehicle chose in a round-robin design. To prevent bundle content from being altered by bundle forwarder, each transferring vehicle creates a hash of the information bundle and keeps it before disseminating it to the following hop.

To separate legitimate and untrustworthy watchdogs, this methodology applies a hybrid Trust on Important Factor (CIF) as watchdogs may unjustifiably guarantee a forwarder as a cooperative vehicle. Watchdog is additionally qualified for a payment based on every trust report. On the off chance that the last trust score determined by the CH equals the trust report, at that point, the watchdog is expected as authentic. Else, it is expected as a selfish watchdog.

VSN collaboration techniques are required to guarantee the right activity and to shield the system from over-burden and misbehave vehicles. In this manner, (Shivshankar, 2012), built up a bundle sending model dependent on Public Goods game hypothesis with contingent Tit-for-Tat procedure and unlimited selflessness with punishment chances.

In this methodology, a collection of vehicles going at a similar speed inside a similar direction is designed. The information transmission is done utilizing a Multicast Routing Protocol (SMRP). A novel ID is given out to the node and can't re-join for a second time utilizing a similar ID after the node leaving the team. The ID is put away in the lookup table.

Information bundle is taken as an open decent. The way, router is framed which has the root hub that sends the packet and nodes at the middle for dissemination. Every vehicle is taken in to account once in the tree, with timestamp and directions showing its position. There could be more than 1 transmission whenever. Vehicles that hesitant to collaborate make a social quandary circumstance. The reward is considered regarding throughput. The conduct of helping other people with some expense gain for the activity is called altruism. In this methodology, the altruist vehicles attempt to contribute better than expected regarding bundle sending to repay the conduct of misbehave vehicles and in this way the system could perform better. Be that as it may, pure altruism doesn't keep going long as altruist vehicles would come up short on cost and data transfer capacity. In this manner, a bundle time cutoff time must be fixed & a separation measure to recognize the misbehave vehicles. The punishment instrument is acquainted with change and stimulate the conduct of the misbehave vehicles to collaborate in VSN.

As indicated by the public goods game hypothesis, commitment past the time limit and doesn't add to the group ought to be viewed as invalid and should be punished. To adequately analyze the commitment of the misbehave vehicles that are lower than normal, a more drawn out cutoff time for comfort application and a littler cutoff time for a safety application is indicated. Another metric is distance Ij, among source and goal, and max distance Dj where the data is viewed as valuable by the recipient. Since data about an occasion created in one area may not be valuable for sending to an area outside the radius.

In light of the components above, misbehave vehicles will be punished on the off chance that they keep the bundle after the time limit. At the point when a vehicle punishes a misbehave vehicle, it advises different vehicles in the network about the misbehave vehicle.

Table2. Punishment Based Cooperation approaches

Researcher	Proposed research	Technique	Remark
(Jesudoss, 2015)	Motivating cooperation and truth-telling among vehicles in VSN via punishment and payment technique	cooperation method using Punishment mechanism	All the cluster design will down if ACH and CH both leave the group at one time with no possibility of re-grouping.
(Shivshankar, 2012)	Consequence of Punishment and Altruism on misbehave behavior for collaboration in Vehicular communication systems.	cooperation method using Punishment mechanism	

2.3.1.3 Reputation-Based Cooperation approaches

Another old style method for stimulating collaboration in VSN is via a vehicle's reputation assessment. vehicles with a decent reputation that have added to the system can utilize the assets while vehicles with a terrible reputation will be avoided from the system. The reputation assessment is finished by controlling the nearby vehicle one hop separated. Since a vehicle can confide in

no one however just itself, more weight is considered to direct perception or direct data. Along these lines, distinguishing the getting into mischief vehicles would be progressively exact if the checking segment is reliable (Abbas, 2010). (Michiardi, 2002), Proposed a methodology called Collaborative Reputation (CORE) to implement participation in MANET. CORE depends on the vehicle's reputation & can be incorporated into any system functionality, such as router disclosure, network control, and bundle sending. CORE comprises of a watchdog for management and routing table which utilizes a negative to positive range to survey reputation. The reputation feature is gathered by the information being checked by the neighborhood substance and different vehicles that have cooperated in the system. Misbehave vehicles who have participated in the system will have their own reputation rating expanded from terrible to great.

There are three kinds of reputation in cooperative Reputation. Abstract reputation is determined privately dependent on direct perception. Then again, in indirect reputation data is recovered by different vehicles. Since indirect reputation would just take positive reputation esteems, attacks like denial-of-service (DoS) activated by a misbehave vehicle dependent on false-negative reputation worth can be stopped. In conclusion, functional reputation refreshes the reputation dependent on specific functions where each function is given a weight.

This method settled the participation concerns between the misbehave vehicles in the system yet has made another conceivable disadvantage. Malevolent vehicles could develop a decent reputation before they begin their selfishness again. CORE likewise does not think about another opportunity technique and henceforth when a failing vehicle recuperates from the transient issue, it can't regain its reputation once more (Marias, 2006).

With no need for a unified server, the Cooperative Watchdog System (CWS) is utilized to battle misbehave vehicles in VSN to distinguish the non-collaborated vehicles. For CWS to well function, every vehicle in the system keeps up a score, to decide the level of percentage might be imparted to other people. Before all else, all vehicles have a score equivalent to 50 and may change after some time somewhere in the range of 0 and 100. At the point when vehicle experience with each other, the data about the past vehicle are exchanged and saved in a neighbor reputation table kept up by all the system vehicles. This data is likewise gathered by the CWS so it knows about the performance of every vehicle in the system. The reputation scores are refreshed by taking the accompanying consideration: a vehicle reputation score saw by its neighbors, a collaborative worth appointed by the watchdog and a vehicle reputation score saw by the vehicle itself (Dias, 2015).

(Buchegger, 2002), Proposed other reputation based collaboration method called CONFIDANT, which distinguishes and disengages got selfish vehicles from the system. In this technique, every vehicle watches and learns the conduct of its neighbor vehicles. In CONFIDANT, every vehicle comprises a screen, a trust chief, a reputation framework, and away manager. The screen is otherwise called Neighborhood Watch in which it works as a watchdog and watches the neighbor's conduct. The trust director assesses the reliability of the alerts got. Thusly, the trust supervisor could alarm others on dishonest vehicles and guarantee the got information is reliable.

The reputation framework is liable for the vehicle evaluations where a table is kept up comprising of the appraisals of every vehicle. In conclusion, the patch director will decide the best way as indicated by the reputation and rejects the vindictive vehicle. All solicitations got from the noxious hub will likewise be disregarded.

In CONFIDANT, every vehicle controls its neighboring vehicles and reports to the reputation framework if suspicious practices are distinguished. The reputation framework will at that point play out a couple of checks to decide whether the revealed vehicle has gotten selfishness for more than a predefined limit. On the off chance that the rating result is negative, the malicious vehicle data will be passed to the path director and all ways containing the malicious vehicle will be expelled. Path supervisor to every vehicle in the system at that point sends an ALARM message, which contains the data, for example, the address of the revealing vehicle, the sort of protocol infringement, the goal address, and others. At the point when a vehicle gets an ALARM message, the message is first assessed by the trust director to distinguish the reliability of the source vehicle. The message will be saved in the ALARMS table on the off chance that it is trusted. The data with respect to the vehicle will be sent to the reputation framework and play out a similar rating capacity again when there is adequate proof to decide a vehicle revealed in the ALARM is malicious.

The huge accomplishment of the CONFIDANT method is its enormous decrease rate in bundle loss when contrasted with the system without CONFIDANT, which lost around 70% of the bundle. This is on the grounds that the malicious vehicles are prohibited and consequently the bundles can be sent all more proficiently.

(Safaei, 2009), the outcome shows that the bundle overhead has decreased contrasted with the methodology where no action is made against the misbehave bundles. By removing the misbehave vehicles, the bundles are just sent to vehicles that are eager to send to the goal node. Vehicles' asset utilization is additionally decreased since less dissemination is expected to convey the bundles.

Table3. Reputation-based collaboration methods

Researcher	Proposed research	Technique	Remark
(Michiardi, 2002)	a Collaborative Reputation (CoRe): mechanism to put in force vehicle collaboration in MANET	Reputation Based collaboration	Malicious vehicles could gain a decent reputation in advance they shift to selfishness once more.
(Buchegger, 2002)	CONFIDANT's Performance Study of the Protocol (Fairness in the collaboration of vehicles in DAT (Dynamic Ad-hoc Networks)	Reputation Based collaboration	The Paths to packet transmission will be narrow when malicious vehicles in the path are removed from the network.
(Dias, 2015)	A Vehicular DTNs Collaboration Strategies	Reputation Based collaboration	There is no reinforcement for the collaborative vehicles.
(Safaei, 2009)	to Enforce collaboration in Mobile ad hoc networks an effective Reputation-Based method	Reputation Based collaboration	

2.3.1.4 Misbehavior nodes Detection mechanism

(Vulimiri, 2010), proposed a collaboration enforcement system called 3CE (3-Counter Enforcement) for CLA-S (Connectionless Approach for Street). In CLA-S, each bundle disseminated between vehicles is inspected by the vehicles' 3C building block. A 3C building block comprises three counters, Location Discover Counter, Forward Counter, and Forward Request Counter which are likewise kept up by the vehicle's 3C building block with the goal that they can't be undermined by malicious vehicles.

This technique is additionally permitting a malicious vehicle to re-join the system by expanding its forwarding counter when takes part in sending the bundles for different vehicles. At the point when a selfish vehicle's proportion of Request Forward Counter to forwarding Counter transcends a limit A, and it's a proportion of Location Discover Counter to forwarding Counter demolishes underneath threshold T, the selfish vehicles can then re-join the system and its neighboring vehicles would assist with sending its Location Discovery bundle.

The experiment outcome of this technique shows that the rate of forwarding more information is expanded hugely as vehicles are required to take part in bundle sending, which is about 25% in excess of the scheme with no identification or prevention system. The selfish vehicle discovery proportion is likewise extremely encouraging at an 87% detection rate.

Security and collaboration concerns are consistently the major worry in VSN. misbehave vehicles are continually attempting to save their energy and deliberately drop the bundles. A behavior called Byzantine, for the most part, shows in an ad hoc system in which vehicles will change, drop, or wrongly route the bundles (Ho, 2008). Thus, the robustness and availability of the system are intensely affected and consequently it is constantly qualified to catch the selfish vehicles since counteraction is in every case superior to fix.

(Wang, 2007), proposed a technique called Dynamic Trust Token (DTT). In the DTT method, a token bundle is sent together with the information parcel, node by node so its accuracy can be assessed. DTT consolidates both asymmetric and symmetric encryption for security. DTT doesn't depend on past records for reputation however run-time execution to arrangement moment reputation for the vehicles. In this manner, just bundles with the right data will be disseminated in VSN. The choice to acknowledge the bundle is made by the token-demonstrated assessment.

Every hub in DTT assumes 3 logical jobs: Predecessor, Relayer, and Successor. The predecessor is the one-bounce upstream hub of relayer and fills in as a watchdog to create trust token while Successor is the one-jump downstream hub of Relayer and accountable for concluding whether to acknowledge the got bundle or not. Relayer is accountable for bundle sending. Every

vehicle additionally keeps up a parcel buffer to store bundles temporarily for additional processing and sending. In the wake of taking care of the information parcel with the trust token, the successor will possibly keep the valid bundles and forward them whenever required.

The initiator begins parcel transmission and requests all its downstream vehicles passing the bundle to their neighboring vehicles inside one Transmission Session (TS).

The majority of the VSN collaboration methods concentrate on distinguishing misbehave vehicles however much of the time, the vehicles would send incorrect data in view of their self-centeredness. A misbehave vehicle would likewise make false traffic warning info to different vehicles and affecting the traffic data exactness in VSN. (Grover, 2011), Proposed a reputation management based on misbehavior detection System to distinguish and used to identify fake data in VSN. The proposed work comprises of rebroadcast, misconduct detection, and global expulsion algorithm.

In a traffic occasion life cycle, an occasion reporter recognizes an occasion by its sensors and makes a traffic occasion and sends it to nearby vehicles. On the off chance that an occasion spectator is inside one hop away, the occasion onlooker would then be able to watch the conduct of the occasion reporter which it got the message from. It performs selfishness detection by utilizing the selfish nodes detection algorithm to identify the false alert messages and the misbehavior vehicles by watching their activity by factor accuracy rough sets. Occasion members are hubs or vehicles past one hop away from occasion reporter along these lines they couldn't recognize the conduct of the occasion reporter.

At the point when the occasion member gets an alarm message from the occasion controller or other occasion members, the receiving member at that point recognizes the selfish vehicle J by utilizing outlier detection techniques and adds node J in the local blacklist of the receiving members.

When an occasion member experiences a Road Side Unit (RSU), the hub transfers its local blacklist to believe registration authority (RA). The trust authority at that point refreshes the global blacklist and uncovers the genuine character of the selfish vehicles. The outcome shows that the methodology can distinguish selfish vehicles by outlier discovery strategies.

malicious hubs may give fake data, for instance, make a misconception of traffic congestion by imagining different nodes and afterward dispatch Denial of Service Attack. The security dangers presented by these malicious vehicles may decrease the VSN efficiency and put the traveler's life at serious risk.

(Wahab, 2014), Proposed an artificial intelligence (AI) technique, and is utilized to separate great and terrible vehicles. It utilizes classifier and the precision of an AI classifier is impacted by the inducer algorithm that is utilized to create the classifier. mainly the kind of characteristics that used to represent the attributes. Every classifier would perform distinctively when various inducers and attributes produce it. For example, Instance-Based Learner (IBK), Naïve Bayes, Random Forest, and Decision Tree are some of the classifiers. Various classifiers are smarter to group a vehicle whether it is a collaborative or selfish vehicle. The result of the classifiers is then consolidated utilizing a smart combination technique into one overall outcome.

This methodology utilized the dominant voting scheme to advance the discovery precision. The vehicles in VSN are arranged by the class that gets the most elevated number of votes. This strategy is known as the basic ensemble method(BEM or plurality vote (PV).

Old style Tit-for Tat encounters a couple of restrictions, for instance, vehicle-to-vehicle collaboration decision, ambiguous controlling, and fake alert. The collaboration decision is done locally and consequently if a vehicle acted mischievously it only be punished by its adversary. Because of bundle collision, a few parcels are not identified. These collisions may be done deliberately or unintentionally as certain vehicles may disseminate parcels simultaneously and different vehicles transmitting the bundles to dispatch a crash attack. False alert could occur and may erroneously perceive the collaborative vehicles as selfish vehicles and the other way around.

To solve the issue of ambiguous controlling, (Kim, 2012), proposed a Dempster-Shafer Tit-for-Tat methodology where every single neighboring vehicle manage the conduct of the MPR vehicles. From that point forward, the Tit-for-Tat procedure is applied to authorize the participation by rewarding the collaborative vehicles or punishing the selfish vehicles.

Five stages are associated with Dempster-Shafer based Tit-for-Tat approach.

The 1st part known as reputation calculation, every vehicle is allocated a worth called reputation with default esteem 100 and is expanded after some time at whatever point it gets installment from its voters. The vehicles once chose as Cluster Head (CH) or Multi-Point Relays (MPRs) get the payment. The reputation esteem is collected after some time yet in the event that a misbehaving vehicle would just collaborate for a short period will have its reputation decreased from time to time. System administrations are allowed to the vehicles relative to their reputation esteems.

The 2nd part is known as watchdog monitoring where the group individuals become watchdogs and MPR vehicles are controlled by these watchdogs. The watchdogs keep up as of late sent and received bundles to identify whether it matches. If correct, this suggests the bundles have sent by the MPR vehicle. Something else, the MPR vehicle is selfish.

The 3rd part includes vote aggregation where the perceptions from numerous watchdogs are aggregated to frame the last decision. A nearby voting procedure among the watchdogs arranging in a similar group is launched.

The 4th part includes the Tit-for-Tat collaboration guideline where an aggregated decision is utilized to choose the participation among the vehicles. The 5th stage includes Information transmission thus after an ultimate conclusion aggregated, each CH disseminates the voting outcomes to its group individuals. At the point when the first CH meets the second CH, the vote results are broadcast among themselves and afterward, the second CH will broadcast the outcome to its group individuals. This guarantees the group individuals won't participate with the disseminating selfish vehicles.

Table4. Misbehavior detection technique

Researcher	Proposed research	Technique	Remark
(Ho, 2008)	Vehicular Networks collaboration Enforcement	Misbehavior identification	When the nodes speed increased then false accusation ratio become higher.
(Wang, 2007)	punish Un-collaborative Behaviors using Dynamic Trust-Token in VSNs	Misbehavior identification	Lack of rewarding methods to motivate collaborative vehicles and transmission range problem.
(Kim, 2012)	Misbehavior – detection based Reputation monitoring technique for VSNs	Misbehavior identification	
Grover, 2012)	Selfish nodes Detection, based on Ensemble Learning in VSN.	Misbehavior identification	Naïve Bayes has the lowliest performance.
(Wahab,2013)	Tit-for-Tat technique to Control the collaboration in VSN utilizing QoS-OLSR Protocol	Misbehavior identification	

3. CONCLUSION

This paper has presented a review of VSNs cooperation approaches. Road traffic accidents (RTAs) are a major public health concern, resulting in an estimated millions of deaths and millions of injuries worldwide each year. Vehicular social network (VSN) is a cutting-edge communication platform that offers an Intelligent Transportation System (ITS) services to the nodes for offering fast information sharing and safety. Comparisons among cooperation approaches of VSNs have outlined. VSN communications are Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V). Every collaboration methodology holds its attributes, models, and shortcomings. In VSN, every node is furnished with a lot of remote sensors and a gadget called Onboard Unit (OBU) for vehicular information dissemination. Vehicle's collaboration is one of the principal problems being looked at in VSN.

Later on, we are expecting further developed and solid vehicle collaboration methods that don't just assist in motivating misbehave vehicles collaboration yet additionally diminishing the expense of bundle routing.

Finally, we saw that most of the incentive mechanisms lack fairness in paying an incentive for cooperated nodes thus we recommend paying per packet incentive method is needed and we will work on it in the future.

4. FUTURE DIRECTIONS

1) **Fair Incentive Mechanism of cooperative nodes:** We can totally claim that VSNs cooperative nodes needs a fair payment method because, if cooperative nodes are not paid back for every packets they transfer then they may be become a selfish node in the middle of communication.
2) **Security issues in VSNs**: In VSN, a multiple of systems both the safety and non-safety related is enabled by V2I and V2V communications. But, the curl of VSNs including, security and privacy preservation issues are in question.
3) **Connectivity development in DTN:** in order to moderate continuous disconnections in VSNs and provide full coverage in all part of the network further research is needed.
4) **Selfishness factor in VNS:** Since the selfishness factor of misbehave drivers is unequal, then to stimulate most of the nodes in the network further work is needed.

5. REFERENCES

1. Abbas, S., Merabti, M., & Llewellyn-Jones, D. (2010, June). A survey of reputation based schemes for MANET. In *The 11th Annual Conference on the Convergence of Telecommunications, Networking & Broadcasting (PGNet 2010), Liverpool, UK* (pp. 21-22).
2. Ali, G. M. N., Chong, P. H. J., Samantha, S. K., & Chan, E. (2016). Efficient data dissemination in cooperative multi-RSU vehicular ad hoc networks (VANETs). *Journal of Systems and Software*, *117*, 508-527.
3. Authority, E. R. (2005). How Safe are Ethiopian Roads. *Midterm Review of RSDP II. Planning and Programming Division. Ministry of Infrastructure, Ethiopia*.
4. Barskar, R., & Chawla, M. (2015). Vehicular ad hoc networks and its applications in diversified fields. *International Journal of Computer Applications*, *123*(10).
5. Benamar, M., Benamar, N., Singh, K. D., & El Ouadghiri, D. (2013, May). Recent study of routing protocols in VANET: survey and taxonomy. In *WVNT 1st International Workshop on Vehicular Networks and Telematics*.
6. Beshah, T., & Hill, S. (2010, March). Mining road traffic accident data to improve safety: role of road-related factors on accident severity in Ethiopia. In *2010 AAAI Spring Symposium Series*.
7. Bhoi, S. K., & Khilar, P. M. (2013). Vehicular communication: a survey. *IET networks*, *3*(3), 204-217.
8. Buchegger, S., & Le Boudec, J. Y. (2002, June). Performance analysis of the CONFIDANT & protocol. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking computing* (pp. 226-236).
9. Chen, W., Guha, R. K., Kwon, T. J., Lee, J., & Hsu, Y. Y. (2011). A survey and challenges in routing and data dissemination in vehicular ad hoc networks. *Wireless Communications and Mobile Computing*, *11*(7), 787-795.
10. Dias, J. A., Rodrigues, J. J., Kumar, N., & Saleem, K. (2015). Cooperation strategies for vehicular delay-tolerant networks. *IEEE Communications Magazine*, *53*(12), 88-94.
11. Eichler, S. (2007, September). Performance evaluation of the IEEE 802.11 p WAVE communication standard. In *2007 IEEE 66th Vehicular Technology Conference* (pp. 2199- 2203). IEEE.
12. Fiore, M., Harri, J., Filali, F., & Bonnet, C. (2007, March). Vehicular mobility simulation for VANETs. In *40th Annual Simulation Symposium (ANSS'07)* (pp. 301-309). IEEE.
13. Gong, H., Yu, L., & Zhang, X. (2014). Social contribution-based routing protocol for vehicular network with selfish nodes. *International Journal of Distributed Sensor Networks*, *10*(4), 753024.
14. Grover, J., Laxmi, V., & Gaur, M. S. (2011, December). Misbehavior detection based on *and* ensemble learning in vanet. In *International Conference on Advanced Computing, Networking Security* (pp. 602-611). Springer, Berlin, Heidelberg.
15. Ho, Y. H., Ho, A. H., Hamza-Lup, G. L., & Hua, K. A. (2008, June). Cooperation enforcement in vehicular networks. In *2008 International Conference on Communication Theory, Reliability, and Quality of Service* (pp. 7-12). IEEE.
16. Hua, L. C., Anisi, M. H., Yee, L., & Alam, M. (2017). Social networking-based cooperation mechanisms in vehicular ad-hoc network—A survey. *Vehicular Communications*, *10*, 57-73.
17. Jesudoss, A., Raja, S. K., & Sulaiman, A. (2015). Stimulating truth-telling and cooperation among nodes in VANETs through payment and punishment scheme. *Ad Hoc Networks*, *24*, 250-263.
18. Kim, C. H., & Bae, I. H. (2012). A misbehavior-based reputation management system for vanets. In *Embedded and Multimedia Computing Technology and Service* (pp. 441-450). Springer, Dordrecht.
19. Li, F., & Wu, J. (2009, June). Frame: An innovative incentive scheme in vehicular networks. In *2009 IEEE International Conference on Communications* (pp. 1-6). IEEE.
20. Luo, J., Gu, X., Zhao, T., & Yan, W. (2010, April). A mobile infrastructure based VANET routing protocol in the urban environment. In *2010 International Conference on Communications and Mobile Computing* (Vol. 3, pp. 432-437). IEEE.
21. Lu, R., Lin, X., Zhu, H., Shen, X., & Preiss, B. (2010). Pi: A practical incentive protocol for delay tolerant networks. *IEEE Transactions on Wireless Communications*, *9*(4), 1483-1493.

22. Marias, G. F., Georgiadis, P., Flitzanis, D., & Mandalas, K. (2006). Cooperation enforcement schemes for MANETs: A survey. *Wireless Communications and Mobile Computing*, *6*(3), 319-332.
23. Michiardi, P., & Molva, R. (2002). Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Advanced communications and multimedia security* (pp. 107-121). Springer, Boston, MA.
24. Nitti, M., Girau, R., Floris, A., & Atzori, L. (2014, May). On adding the social dimension to the internet of vehicles: Friendship and middleware. In *2014 IEEE international black sea conference on communications and networking (BlackSeaCom)* (pp. 134-138). IEEE.
25. Nguyen, T. D., Vo-Nguyen, Q. B., Vo, M. T., & Mai, L. (2011, August). Energy efficient cooperative communication techniques for Intelligent Transport System. In *The 2011* 80). *International Conference on Advanced Technologies for Communications (ATC 2011)* (pp. 76-IEEE.
26. Safaei, Z., Sabaei, M., & Torgheh, F. (2009, October). An efficient reputation-based mechanism to enforce cooperation in MANETs. In *2009 International Conference on Application of Information and Communication Technologies* (pp. 1-6). IEEE.
27. Shivshankar, S., & Jamalipour, A. (2012, August). Effect of altruism and punishment on selfish behavior for cooperation in vehicular networks. In *2012 1st IEEE International Conference on Communications in China (ICCC)* (pp. 653-658). IEEE.
28. Shivshankar, S., & Jamalipour, A. (2014). An evolutionary game theory-based approach to cooperation in VANETs under different network conditions. *IEEE Transactions on Vehicular Technology*, *64*(5), 2015-2022.
29. Smaldone, S., Han, L., Shankar, P., & Iftode, L. (2008, April). Roadspeak: enabling voice chat on roadways using vehicular social networks. In *Proceedings of the 1st Workshop on Social Network Systems* (pp. 43-48).
30. Thakre, N., Raut, N., & Shaik, A. (2014). Design and development of automatic vehicle accident detection & localization of automobile using Bluetooth technology. *International Journal of Advanced Research in Computer and Communication Engineering*, *3*(3), 5343-5345.
31. Vegni, A. M., & Loscri, V. (2015). A survey on vehicular social networks. *IEEE Communications Surveys & Tutorials*, *17*(4), 2397-2419.
32. Viriyasitavat, W., Tonguz, O. K., & Bai, F. (2009, June). Network connectivity of VANETs in urban areas. In *2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks* (pp. 1-9). IEEE.
33. Vulimiri, A., Gupta, A., Roy, P., Muthaiah, S. N., & Kherani, A. A. (2010, May). Application of secondary information for misbehavior detection in VANETs. In *International Conference on Research in Networking* (pp. 385-396). Springer, Berlin, Heidelberg.
34. Wahab, O. A., Otrok, H., & Mourad, A. (2014). A dempster–shafer based tit-for-tat strategy to regulate the cooperation in vanet using qos-olsr protocol. *Wireless personal communications*, *75*(3), 1635-1667.
35. Wang, Z., & Chigan, C. (2007, June). Countermeasure uncooperative behaviors with dynamic trust-token in VANETs. In *2007 IEEE International Conference on Communications* (pp. 3959-3964). IEEE.
36. Wu, C., Gerla, M., & Mastronarde, N. (2015, June). Incentive driven LTE content distribution in VANETs. In *2015 14th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC- NET)* (pp. 1-8). IEEE.
37. Zhu, Y., Liu, L., Panneerselvam, J., Wang, L., & Li, Z. (2014, April). Credit-based incentives in vehicular ad hoc networks. In *2014 IEEE 8th International Symposium on Service Oriented System Engineering* (pp. 352-357). IEEE.
38. Zhu, H., Lin, X., Lu, R., Fan, Y., & Shen, X. (2009). Smart: A secure multilayer credit-based incentive scheme for delay-tolerant networks. *IEEE Transactions on Vehicular Technology*, *58*(8), 4628-4639.