2017 IEEE 7th International Advance Computing Conference

Impact of Malicious Node on Secure Incentive Based Advertisement Distribution (SIBAD) in VANET

V Padmapriya, Smitha S, D N Sujatha
Department of Computer Applications, B M S College of Engineering
Bangalore, India
Email:priya.venkatesh09,smitha3393,dnsbms@gmail.com

Venugopal K R
University Visvesvaraya College of Engineering
Bangalore, India
Email: venugopalkr@gmail.com

***Abstract*—Last decade has seen an increasing demand for vehicle aided data delivery. This data delivery has proven to be beneficial for vehicular communication. The vehicular network provisions safety, warning and infotainment applications. Infotainment applications have attracted drivers and passengers as it provides location based entertainment services; a value add to the traveling experience. These infotainment messages are delivered to the nearby vehicles in the form of advertisements. For every advertisement disseminated to its neighboring vehicle, an incentive is awarded to the forwarder. The incentive based earning foresee a security threat in the form of a malicious node as it hoards the incentives, thus are greedy for earning incentives. The malicious behavior of the insider has an adverse effect on the incentive based advertisement distribution approach. In this paper, we have identified the malicious nodes and analyzed its effect on incentive based earning for drivers in vehicular networks.**

***Keywords*-Advertisement, Infotainment applications, Incentive, Malicious Node, Security**

I. Introduction

Cities are moving towards smart infrastructure with a strong telematics support. Intelligent Transportation System (ITS) is working towards providing this smart, innovative and feasible transportation solutions. ITS resolves the growing demand of the safer, well coordinated and efficient traffic management needs [1]. ITS technology embraces the communication mechanism which gathers collective intelligence from various sources spanning the road side infrastructure, number plate recognition systems, vehicle bound navigation assistants, on board units and Global Positioning System (GPS) units. ITS promotes exchange of information between vehicles and the fixed infrastructure located along the roads like the road side units [2]. The success of this system is a well coordinated effort of governmental agencies, transport department and telematics service providers. Intelligent Transportation System is the backbone for Vehicular Ad Hoc Networks (VANETs) [3]. VANET is aimed to improve safety features to driver, assist in better traffic management, improve traffic efficiency, provide location based information, handle advanced traveler information system and aid in vehicle health monitoring with comfortable driving experience on the go [4]. VANET depends on the radio services for communication using its specialized technologies ranging from the short range communication mechanism like Dedicated Short Range Communication (DSRC) to todays 3G and 4G mobile networks. In VANET, vehicles form the nodes of communication. The communication in this network is realized as successful, if all its components like the On Board Unit (OBU), Global Positioning System (GPS), Electronic License Plate (ELP), front and rear cameras of the vehicles and antennas are assisting the nodes to gather the information. However, existence of all these components though not mandatory, are desirable to make all the functions available to different category of vehicles even to the ones which are economically priced [5].

Vehicular Ad Hoc Network (VANET) is a special category of Mobile Ad Hoc Network (MANET). It is a small network of self-managed, self-organized, featured by highly mobile nodes and thus, has dynamic topology. VANET supports communication between vehicles (V2V), vehicle to nearby roadside infrastructure (V2I), vehicle to pedestrians (V2P) or any other communicating entity across road (V2X). The communication among vehicles facilitating V2V communication in VANET is made possible using the radio interface range with a spectrum of 5.850 - 5.925 GHz and with a bandwidth of 75 MHz. This frequency range is allocated by Federal Communication Commission (FCC) called as *Dedicated Short Range Communication (DSRC)* [6]. This range varies across the globe with the United States in 75 MHz range, Japan and Europe in 700 MHz range and is yet to be adopted in India. DSRC has allocated 6 service channels for non - safety applications and one exclusive control channel for safety applications. This control channel is regularly monitored by all vehicles for safety related information. The Road Side Unit (RSU) has privilege to use this control channel to disseminate several safety related service announcements to the vehicles approaching its radius [7]. DSRC supports short range communication, but considering the extensive applications supported by VANET, there is a need to adopt other wireless technologies like Bluetooth, WiFi, Cellular Automata, and WiMax for a wider reach of communication.

Since 1998, researchers across globe have been work-

978-1-5090-1560-3/17 $31.00 © 2017 IEEE
DOI 10.1109/IACC.2017.50

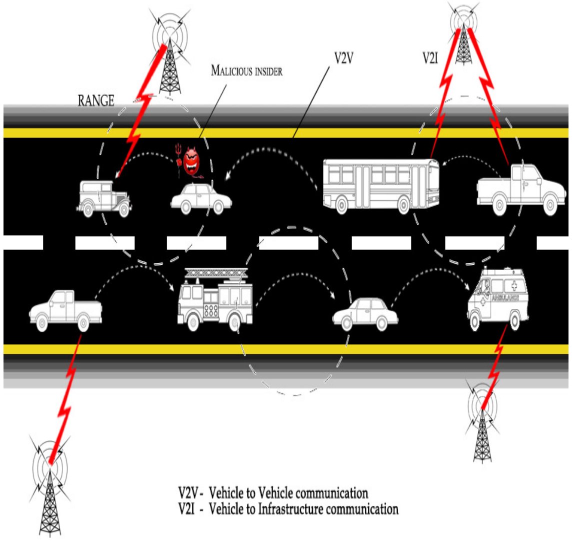
RANGE
MALICIOUS INSIDER
V2V
V2I
V2V - Vehicle to Vehicle communication
V2I - Vehicle to Infrastructure communication

Fig.1: Malicious Node in VANET

ing on various projects in VANET. Some of them are PROMETHEUS [8], PATH [9], FLEETNET [10], CarTalk [11], SAFESPOT [12], PReVENT [13], COMeSafety [14], SEVECOM [15], Car2Car [16]. One of the major research challenges identified in vehicular networks is the security issue [17], [18], [19]. The basic security requirements includes the authentication of the vehicles participating in the information exchange, establishing trust among the nodes to cooperate and disseminate the information. Additionally, the factors like key management and non-repudiation further strengthen the security aspect. Vehicular networks adopts several heterogeneous wireless media for communication. This communication is limited to the wireless coverage area. Vehicular networks have many applications which disseminate information to the commuters on road. This information becomes a prime candidate for the attacker. One of the challenging tasks here is to secure this communication from attackers [20]. The attacker is either an authenticated trusted insider or a malicious outsider. Fig. 1 depicts a scenario where a malicious node is the car representing an attacker passing a fabricated or modified information to the jeep following the car. The information which was passed from the bus about the traffic, road condition or the weather condition is either modified, fabricated or impersonated to avert the traffic following the malicious car. This poses threat to the communication in vehicular network as it is sending false information on the network which probably never existed at all. Finding a malicious insider who poses threat of impersonation, modification and fabrication of the information elevates the security issue to the next level.

VANET supports several applications [21]. It embraces many protocols which improves traffic management and support safety and convenience in the transportation system, thus in turn supports diverse applications in vehicular network. These applications range from general, safety to warning which assist in providing adaptive driving environment to the vehicles on road [22]. These applications provide information to the driver on the traffic, road, weather conditions, user centric and infotainment services to the passengers. The wireless medium embraced by these applications cover a radius of 10 m to 1000 m. The drivers can distribute these infotainment messages, location based information in the form of advertisements to the nearby vehicles.There has been considerable amount of research efforts put in the area of content distribution and incentive based earnings in vehicular ad hoc networks [23] and the details of the work carried out in this area is discussed in section III.

Vehicles in VANET communicate with each other adopting the short range communication and various other medium to long-range wireless off-the-shelf enablers like Bluetooth, ZigBee, WiFi, WiMAX etc. These wireless enablers are used by applications as one of the modes of communication in vehicular networks. One of the most popular category of application for commercial purpose is the advertisement distribution. This category of application provides a means of additional income to the drivers in the form of incentive [24]. Incentive is a motivating factor for promoting cooperative behavior. In reality, incentives cannot be generalized and there is a need to fine tune based on the applications. The drivers who participate in the commercial / comfort advertisement distribution to the vehicles in its periphery are awarded an incentive for every forward of the advertisement [25]. In this context, the major challenges are to control the amount of incentives earned by every driver and to evade the malicious and selfish nodes in vehicular networks. We have proposed a Secure Incentive Based Advertisement Distribution (SIBAD) approach [26] which provides a platform for secure incentive based earning by distributing the advertisements in VANET. The details of this model is described in section IV. The information exchanged by these applications anticipates potential security threat of being impersonated, fabricated or modified leading to breach of integrity and trust. In this work, we have identified the malicious nodes which earn the incentive and prevent other nodes from earning the incentives by channelizing all the incentives to a predefined set of nodes.

II. Motivation

Driving on urban roads is quite a tough assignment for drivers. Drivers on roads wait in long traffic jams, steer through congested roads, bear and adjust with erring drivers, handle different road conditions or wait around for passengers to board the vehicle. There is an endless effort for earnings. An additional earning in the form of incentive is a reward to them. Drivers are encouraged to utilize the idle time in disseminating useful information to commuters on road in the form of advertisements delivered to other vehicles and earn incentive. Our motivation for this work, are all those drivers who spend ample of time handling different situations on road but get meagerly paid. Incentive is perceived to be their additional income without compromising on the safety of driving and being distracted when on wheels.

The rest of the paper is organized as follows. In section III we discuss various research work carried out related to incentive based schemes. The section IV describes our proposed scheme for the incentive based earning. The section V highlights the simulation setup and discussion of simulation results. The paper concludes in section VI.

III. Related Work

In this section we discuss some of the work related to cooperative behavior, security issues and incentive based schemes adapted in VANET. Zhao and Cao [27] have proposed a carry and forward technique where a vehicle holds the packet i.e.,*carries* the packet till a node gets a receiver in it neighborhood and then *forwards* it to its neighbor. They have used predictable vehicle mobility model which is limited by the traffic pattern and road layout.

In the work by Li et al. [28], authors have adopted a scheme that supports secure ad dissemination. They have arrived at an efficient secure and privacy preserving scheme called *Incentive Cash-In* to support financial transactions based on Distance - Based gradient Algorithm (DBA) relying on ad posting patterns. The work highlights the cost requirement from the ad service provider perspective.

The paper on Social - Contribution by Gong et al. [29], spotlights the greedy nodes in the vehicular network contributing to the delivery of data. The greedy nodes thus impair the network performance. The authors have arrived at new protocol called as *Social Contribution - based routing protocol* for these greedy nodes. The forwarding decision in this technique is based on the delivery probability to the destination and the social contributions of the relay node. The scheme has refined the decision of choosing the next hop candidate as the one which has higher delivery probability and lower social contribution.

The rewarding scheme proposed by Salem et al. [30] are for the nodes which participate in cooperative and collaborative packet forwarding scheme. Authors have implemented the charging scheme which justifies that, user uses the services and is charged for the services for only those he has requested for. The schemes ensures that the users are aptly charged by the service provider. The incentives are called *Double Edge Swords*, which means that the monetary rewards in the system will act as reward but a poorly designed system shall lead to cheating.

Liu et al. [31], in their work have focused on risk assessment, harm prediction, predictive / proactive cyber defense for specific ad hoc applications. The idea is based on the concept that the incentives can unify a large variety of attacker intent.

Buchegger et al. [32] have arrived at a protocol based on altruism and utilitarianism called as the *Cooperation Of Nodes: Fairness In Dynamic Adhoc NeTworks (CONFIDANT)*. This protocol is designed to detect and isolate the misbehaving nodes and thus make cooperation in the network. The effect of misbehavior of the node earns it a negative reputation.

A novel method of customizing the incentive scheme is proposed by Huang et al. [33]. The authors in their work have discussed that the incentive based scheme should not vary with streams and stages of adoption. They are to be tailored to the needs of each individual application rather than using a generalized approach.

Li et al. [34] have framed a novel *Fair Reimbursement and Motivating swEepstake (FRAME)* scheme. FRAME is a weighted rewarding and sweepstake scheme for all the vehicles participating in the packet forwarding in VANET. This scheme calculates the probability of the vehicle being the winner in this forwarding process.

IV. Proposed Model

Vehicular Network is a hub of information exchange on the road. It uses broadcast and multicast techniques to leverage its benefits to group of users on the go. Generally, all the nodes in the vehicular network are desired to be participative and cooperative to completely reap its benefits. Drivers are vehicle bound and spend ample amount of time on urban road handling different traffic situations, passing through narrow lanes, managing different road and weather conditions. Drivers on the urban roads pass through various commercial hubs like spots of entertainment, malls, food joints, theme parks and tourist spots. These business spots show their presence by means of advertisements. These advertisements are well received if they are displayed or disseminated to the vehicle bound passengers visiting or passing through these spots. Our proposed model, called as *Secure Incentive Based Advertisement Distribution* (SIBAD) approach takes care of the advertisement distribution initiated by drivers on the road.The SIBAD approach is depicted in Fig. 2. The participating entities in this approach are Advertisement Content Server (ACS), Advertisement Distribution Point (ADP) and vehicles on the road.

The ACS is the first point of this advertisement distribution and it houses all the advertisements. ACS is hosted on the prime locations on the urban roads catering to both commercial and non-commercial advertisement to be disseminated to the vehicular traffic. The ADP which is the advertisement distribution point is generally present as part of the fixed infrastructure RSU. The ADP uses wireless medium to reach the nearest vehicle in its range. ADP initiates the information exchange by a handshake mechanism established with the drivers smartphone. This handshake process initiates the chain of advertisement distribution. The driver is authenticated and identified by a unique identification number P_i. P_i is a combination of driver's mobile phone number, engine number and chassis number of the vehicle he drives. For every advertisement a driver D_i forwards to his neighbor, the forwarder earns an incentive. Incentives in this approach are in the form of food coupons or fuel recharge cards or mobile currency recharge points.

The node D_i, which begins the advertisement distribution is the potential candidate for being a malicious node. It can compromise with friend node D_f and form a tunnel to create an illusion that the network is busy and the advertisements are distributed to many nodes. As a result of this tunnel, a set of forwarder nodes earn more incentives compared to the other nodes in the network. This malicious forwarder node is an insider to the approach and it thus stands a very less chance of being identified as the attacker. One of the toughest challenge is to identify this incentive grabbing nodes as the malicious node, which on contrary is a cooperative set of nodes. In this approach, we have introduced a set of nodes which exhibit the malicious behavior and analyzed their impact on SIBAD. Further, this approach does not involve any game theoretic techniques or any other Public Key Infrastructure (PKI) mechanism for authentication, but uses the dual authentication mechanism with the P_i to handle the legitimate advertisement disseminator. The incentive reimbursement in this approach is handled by ACS, which keeps track of number of incentives earned by a P_i reflecting the number of forwards made by a D_i.

The SIBAD approach foresee a potential threat from intruders, masqueraders and eavesdroppers. The security mechanism in SIBAD approach is handled in two folds. First, in order to secure the communication between ACS and ADP, it employs a certification process by a third party Certification Authority (CA). However the CA's trustworthiness is one of the major concerns in the vehicular network. Further, it is obligatory that CA's are being chosen by the governmental agencies which follows procedure and policies in the selection process and thus prevent automotive industry or private companies in choosing CA's. Second level of security threat anticipated in SIBAD approach is on the loss of driver's mobile phone or handling the fake identity of the driver. In order to prevent these kinds of situations, SIBAD sets forth a next level of security by introducing another authentication body called the Advertisement Authentication Authority(AAA). The AAA is a specialized body for handling the second level of authentication mechanism to evade fake identities of the drivers and the deal with the economics of advertisement distribution. AAA handles features of the advertisement like the category of advertisement, base cost, lifetime, coverage area and redemption modes of incentives.

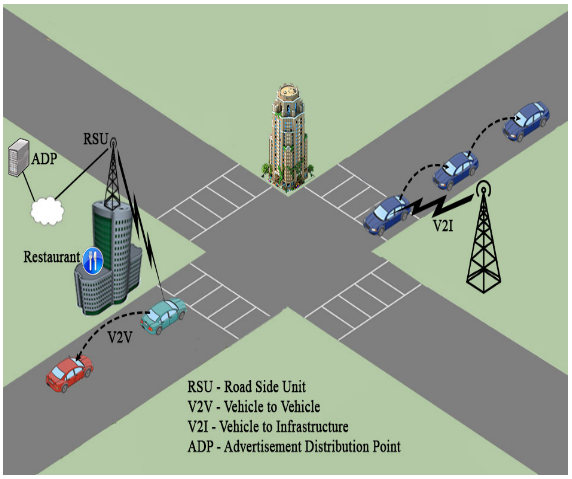
ADP
RSU
Restaurant
V2V
V2I
RSU - Road Side Unit
V2V - Vehicle to Vehicle
V2I - Vehicle to Infrastructure
ADP - Advertisement Distribution Point

Fig. 2: Secure Incentive Based Advertisement Distribution (SIBAD)

V. Simulation and results

A. Discussion on SUMO and MOVE

Simulation is the popular means for depicting the behavior of vehicular networks. Simulation helps to model, analyze and test the performance of the vehicular networks which is generally not feasible in the real world scenario. It aids in evaluating the traffic scenarios both at microscopic and macroscopic levels [35]. In this paper, we have used free, open microscopic traffic simulator Simulation of Urban Mobility (SUMO) [36]. SUMO is a microscopic traffic simulator which helps in visualizing the traffic system with roads, traffic lights, routes management and emission calculation. The microscopic model feature followed by SUMO gives the minute details of vehicles like the car overtaking, lane changing etc. These details reflect the mobility situation of the vehicles as seen on the road but in the simulated environment.

VANETs have mobile devices and on board units which are vehicle bound. The pattern of movements of the nodes is well captured by its mobility model. The mobility models give significant information about the location of the vehicle, velocity and change in position varying with time. These mobility patterns have great impact on the performance of the vehicular networks. In our work, we have adopted Random Waypoint Mobility Model [37]. The Random Waypoint Model works well with the nodes which move independently to a random destination and with random velocity. This model is driven by the previous history of the node to the destination or has fair knowledge of its neighbor. With these distinguishing feature, the Random Waypoint mobility model is a popular choice in many simulators used in the

Table I
SIMULATION PARAMETERS

Parameter	Value
Traffic Simulator	SUMO
Mobility Modeler	MOVE
Trace Analyzer	ns-2
Number of Lanes	4
Number of Vehicles	58
Number of Malicious Nodes	10
Malicious Node Color Code	Red
Non Malicious Node Color Code	Yellow
Average speed of Malicious Nodes	4 Km/hr
Average speed of Non-Malicious Node	18 Km/hr
Protocol	AODV
Packet Size	1000 bytes
Simulation time	0-750 ms
Sending Rate	64 Kb
Range of communication	1000 m

area of vehicular networks. Further in this work, we have used the MObility model generator for VEhicular networks, MOVE [38]. MOVE is compatible with SUMO. MOVE includes two editors MAP Editor and Vehicular Editor. The Map Editor collects the details of nodes, edges, edge type and maps the configuration to generate road maps for the simulation setup. On the other hand the Vehicular Editor helps in generating the vehicular movements with details of start point, routes, end point, vehicle arrival time, departure time, maximum speed etc. The output generated by MOVE is analyzed by the network simulators like ns-2 [39].

B. Simulation Setup

The simulation here depicts the impact of the incentive hogging malicious nodes in the SIBAD approach. The traffic simulator SUMO is used to set up the traffic visualization with roads, lanes and vehicles. Our setup has a bi-lane roads. Nodes are numbered either even or odd based on the direction of travel. All the even numbered nodes travel from left to right (denoting left driving lane) and all odd numbered nodes are set to travel from right to left (denoting right driving lane). Further, the malicious nodes are denoted by red color and non malicious ones in yellow color. Red vehicles V_r are the first one to get authenticated from the ACS with required authentication credentials, whereas the V_y, the yellow ones are the ones which receive the advertisements from the red ones. V_r sends the advertisements to all the vehicles in its range, and for every advertisement sent, driver earns an incentive. We have 58 nodes participating in this advertisement distribution. The simulation is set between 0 ms to 750 ms. MOVE handles the mobility parameters and network setting which include protocol type, antenna type, packet type, simulation time settings etc.The results of the simulation is obtained in the form of trace file. The simulation parameter details are shown in Table I.

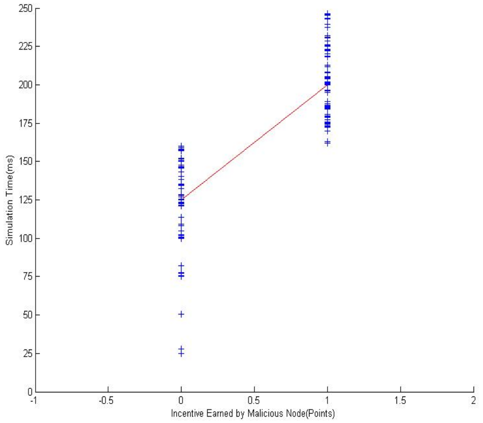

Fig. 3: Incentive earned by Malicious Nodes in 250 ms

C. Results

In this section, we present the impact of introducing malicious node on our SIBAD approach.The results are evaluated on the following assumptions:

- Simulation Time: Time of the simulation varying from 0 ms to 750 ms. The malicious node behavior is recorded for simulation run time of 250 ms, 500 ms and 750 ms.
- Malicious Nodes: Nodes which are colored red and are greedy to hog the incentives.
- Handoff Points: The points where the malicious node handoff the channel to its friend node to earn incentive, thus forming a tunnel between the two nodes.

The graph in Fig. 3, depicts the incentive earned by the malicious nodes at time between 0 ms to 250 ms. In this simulation run, there are 28 nodes and the nodes numbered 0 and 1 represent malicious node. The blue points on the graph represent the incentive earned by the malicious nodes. In this graph, the node 0 starts earning the incentive at 25 ms continues up to 160 ms.The handoff point to node 1 is at 123 ms of the simulation time. The red line in the graph shows the tunneling activity between node 0 and 1.The tunneling is here inversely proportional to time. It implies that, smaller the simulation time larger the tunneling activity.

The graph in Fig. 4, represents the points earned as incentives by malicious nodes 0, 1, 14, 15, 28 and 29. These 6 nodes are set to be the forwarders of the advertisements. This simulation run is set to 500 ms with 38 nodes participating in advertisement distribution on SIBAD approach. In this graph, it is observed that node 0 starts earning incentive at 25 ms and handoff the channel to node 1 at 100 ms, thus reducing the tunneling time by 23 ms compared to the simulation run of 250 ms. Similarly, the handoff between nodes numbered 14 and 15 is at 250 ms. The next handoff

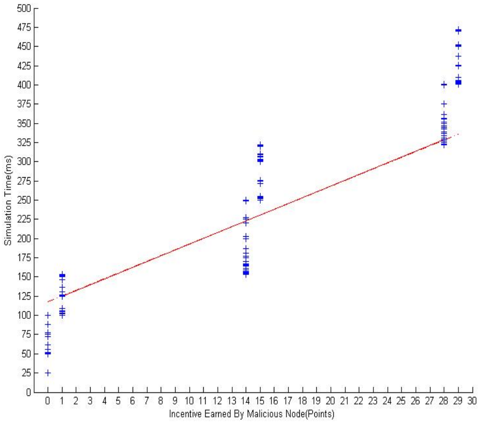

Fig. 4: Incentive earned by Malicious Nodes in 500 ms

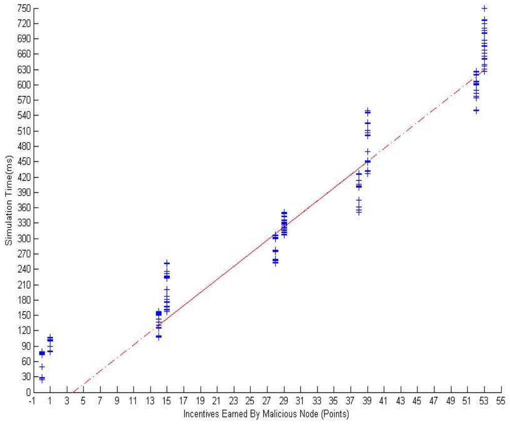

Fig. 5: Incentive earned by Malicious Nodes in 750 ms

between nodes numbered 28 and 29 is at 397 ms. It is observed that all other32 nodes are receivers and never gets an opportunity to earn incentives. Fig. 5 represents the graph of points earned by 10 malicious nodes 0, 1, 14, 15, 28, 29, 38, 39, 52 and 53. There are 58 nodes engaging in the SIBAD approach for the simulation run set to 750 ms. The graph depicts that the malicious node 0 starts earning incentive at 25 ms, node 1 at 85 ms, 14 at 86 ms, node 28 and 29 at 225 ms and 229 ms respectively. Further, the next two sets of malicious nodes 38, 39 and 52, 53 starts earning incentives at 345 ms, 421 ms, 540 ms and 632 ms respectively. The graphs affirm that, there is a smooth handover of the advertisement distribution through the pre-established tunneled path to its friend nodes and no other node in this group gets the control of advertisement distribution.

VI. Conclusion

In this paper, we have introduced malicious nodes in the Secure Incentive Based Advertisement Distribution approach.We have analyzed that the malicious nodes becomes more greedy and prevent other nodes from earning incentive. This behavior of malicious node degrades the performance of incentive based earning and promotes non-cooperation. Thus, in our future work we plan to devise a mechanism to restrict the amount of incentive earned per node and thwart the incentive hogging by a group of malicious nodes. Further, we plan to develop a mobile application adopting this approach. This application will promote a fair earning of incentives for all the participating nodes.

References

[1] [Online]. Available: http://deity.gov.in/content/intelligent-transportation-system-its

[2] F. J. Martinez, C.-K. Toh, J.-C. Cano, C. T. Calafate, and P. Manzoni, “Emergency services in future intelligent transportation systems based on vehicular communication networks,” *Intelligent Transportation Systems Magazine, IEEE*, vol. 2, no. 2, pp. 6–20, 2010.

[3] A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, “Vehicular ad hoc networks: A new challenge for localization-based systems,” *Computer Communications*, vol. 31, no. 12, pp. 2838–2849, Jul. 2008.

[4] R. Sen and B. Raman, “Intelligent transport systems for indian cities,” in *6th USENIX/ACM Workshop on Networked Systems for Developing Regions*, 2012.

[5] J. Blum and A. Eskandarian, “The threat of intelligent collisions,” *IT Professional*, vol. 6, no. 1, pp. 24–29, Jan 2004.

[6] Q. Xu, T. Mak, J. Ko, and R. Sengupta, “Vehicle-to-vehicle Safety Messaging inDSRC,” in *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*, ser. VANET ’04, 2004, pp. 19–28.

[7] M. L. Sichitiu and M. Kihl, “Inter-vehicle Communication Systems:A Survey,” *IEEE Communications Surveys Tutorials*, vol. 10, no. 2, pp. 88–105, Second 2008.

[8] M. Williams, “Prometheus- The European research programme for optimising the road transport system in Europe,” in *Driver Information, IEE Colloquium on*, Dec 1988, pp. 1/1–1/9.

[9] [Online]. Available: http://www.path.berkeley.edu/

[10] W. Enkelmann, “Fleetnet - Applications for inter-vehicle communication,” in *Intelligent Vehicles Symposium, 2003. Proceedings. IEEE*, June 2003, pp. 162–167.

[11] D. Reichardt, M. Miglietta, L. Moretti, P. Morsink, and W. Schulz, “Cartalk 2000: safe and comfortable driving based upon inter-vehicle-communication,” in *Intelligent Vehicle Symposium, 2002. IEEE*, vol. 2, June 2002, pp. 545–550.

[12] G. Vivo, P. Dalmasso, and F. Vernacchia, "The european integrated project "safespot"- How ADAS applications co-operate for the driving safety," in *2007 IEEE Intelligent Transportation Systems Conference*, Sept 2007, pp. 624–629.

[13] [Online]. Available: http://www.prevent-ip.org

[14] [Online]. Available: http://www.comesafety.org

[15] [Online]. Available: http://www.transport-research.info/project/secure-vehicle-communication

[16] [Online]. Available: http://www.car-to-car.org

[17] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *Communications Magazine, IEEE*, vol. 46, no. 6, pp. 164–171, 2008.

[18] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[19] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Workshop on hot topics in networks (HotNets-IV)*, 2005, pp. 1–6.

[20] I. A. Sumra, I. Ahmad, H. Hasbullah, and J.-l. B. A. Manan, "Classes of attacks in VANET," in *Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International*, 2011, pp. 1–5.

[21] U. Lee, R. Cheung, and M. Gerla, "Chapter 1 :Emerging Vehicular Applications."

[22] R. Karim *et al.*, "Vanet: Superior system for content distribution in vehicular network applications," *Rutgers University, Department of Computer Science, Tech. Rep*, 2008.

[23] N. B. Salem, L. Buttyán, J.-P. Hubaux, and M. Jakobsson, "A charging and rewarding scheme for packet forwarding in multi-hop cellular networks," in *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking*, ser. MobiHoc '03, 2003, pp. 13–24.

[24] S. B. Lee, J. S. Park, M. Gerla, and S. Lu, "Secure Incentives for Commercial Ad Dissemination in Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 6, pp. 2715–2728, July 2012.

[25] E. Huang, J. Crowcroft, and I. Wassell, "Rethinking Incentives for Mobile Ad Hoc Networks," in *Proceedings of the ACM SIGCOMM Workshop on Practice and Theory of Incentives in Networked Systems*, ser. PINS '04, 2004, pp. 191–196.

[26] V. Padmapriya and D. N. Sujatha, "A futuristic approach for Secure Incentive Based Advertisement Distribution in VANET," in *Indian Technology Congress (ITC-2015)*, 2015.

[27] J. Zhao and G. Cao, "VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 3, pp. 1910–1922, May 2008.

[28] Z. Li, C. Liu, and C. Chigan, "On Secure VANET-Based Ad Dissemination With Pragmatic Cost and Effect Control," *IEEE Trans. Intelligent Transportation Systems*, vol. 14, no. 1, pp. 124–135, 2013.

[29] H. Gong, L. Yu, and X. Zhang, "Social Contribution-Based Routing Protocol for Vehicular Network with Selfish Nodes," *IJDSN*, 2014.

[30] N. B. Salem, L. Buttyán, J. Hubaux, and M. Jakobsson, "A charging and rewarding scheme for packet forwarding in multi-hop cellular networks," in *Proceedings of the 4th ACM Interational Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc 2003, Annapolis, Maryland, USA, June 1-3*, 2003, pp. 13–24.

[31] P. Liu, W. Zang, and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives, and strategies," *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 1, pp. 78–118, 2005.

[32] S. Buchegger and J. L. Boudec, "Performance analysis of the CONFIDANT protocol," in *Proceedings of the 3rd ACM Interational Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc 2002, June 9-11*, 2002, pp. 226–236.

[33] E. Huang, J. Crowcroft, and I. Wassell, "Rethinking Incentives for Mobile Ad Hoc Networks," in *Proceedings of the ACM SIGCOMM Workshop on Practice and Theory of Incentives in Networked Systems*, ser. PINS '04, 2004, pp. 191–196.

[34] F. Li and J. Wu, "FRAME: An Innovative Incentive Scheme in Vehicular Networks," in *Proceedings of IEEE International Conference on Communications, ICC, 14-18 June*, 2009, pp. 1–6.

[35] D. Yin-fei, Z. Ying-yong, and L. Nian-feng, "Research Overview on Vehicular Ad Hoc Networks Simulation," *International Journal of Control and Automation*, vol. 8, no. 3, pp. 207–216, 2015.

[36] [Online]. Available: http://www.sumo.dlr.de/userdoc/Tutorials.html

[37] A. H. FanBai, "A survey of mobility models in wireless ad hoc networks," *University of Southern California, USA*.

[38] F. K. Karnadi, Z. H. Mo, and K. c. Lan, "Rapid Generation of Realistic Mobility Models for VANET," in *2007 IEEE Wireless Communications and Networking Conference*, March 2007, pp. 2506–2511.

[39] [Online]. Available: http://www.isi.edu/nsnam/ns/