COMPARATIVE ANALYSIS OF IDENTIFICATION OF MALICIOUS NODE IN VANET USING FFRDV AND ERDV ROUTING ALGORITHM

Archana Harit[1], N C Barwar[2]

[1]ME Scholar, [2]Professor , Department of Computer Science & Engineering,
MBM Engineering College, JNVU, Jodhpur, Rajasthan

ABSTRACT

A vehicular ad hoc network (VANETs) is an ad hoc wireless communication system setup between multiple vehicles.The vehicles communicate to each other to share the information. There are some malicious nodes whose behaviour is not proper. A misbehaving vehicle can raise an alert even if there is no crash or it can falsely divert the traffic in wrong direction and create jams or create any hazard. The misbehaviour can have many causes. So there is a requirement of an algorithm that can identify the misbehaving node. Research have proposed a new Modified Sybil Attacked Node Identification Algorithm (MSANIAlgorithm) is proposed. This algorithm identifies the misbehaving node and does not interactwith these nodes. This decreases the packet congestion in the network. The algorithm uses the ERDV and FFRDV for the routing in the VANET. The QoS performance of new algorithm is analysed in ERDV and FFRDV. The paper briefly presents detection and prevention from Sybil Attack.

I. INTRODUCTION

Wireless technologies are shaping the beginning of the new millennium. The principle of computing anytime anywhere is becoming reality. Computer network, traditionally viewed as infrastructure of a fixed form, has evolved into combinations of wired and wireless networks to suit today's need of mobile communication. As the mobility of users continues to increase, a special type of network will be gaining more and more attention, which is mobile ad hoc network (MANET).

Vehicular ad hoc networks (VANETs) are special class of MANETs. Vehicular ad-hoc network (VANET) is an ad-hoc network which is an important approach used in the intelligent transportation system (ITS). VANET is growing rapidly to support the wireless products that can be used in vehicles like personal digital assistance (PDAs), laptops, remote keyless entry devices and mobile telephones. VANET has the number of features such as quick changes in the network topology, high mobility etc. VANET allows inter- vehicle communication to enhance the driving experience and road safety. It can be used for safety and non-safety applications such as vehicle safety, traffic management, automatic toll payment, navigation, location-based services i.e. finding closest fuel station or restaurant [1].

VANET is characterized by infrastructure free, wirelessly connected and distributed systems with no central administration for controlling different operations in network. Every node are equipped with wireless sensors and on board units (OBUs) to make wireless communication with vehicles and their environs. Every node has capabilities as packet sender, receiver and router which helps in providing multi hop communication among nodes which don't have direct link as shown in figure 1.

There are constraints in ad hoc networks i.e. limited battery backup, radio range, and heterogeneity of devices. (VANETs) is an ad hoc wireless communication system setup between multiple vehicles in a neighbourhood. The communication can be only vehicle-to- vehicle (V2V) or may also involve some roadside infrastructures.

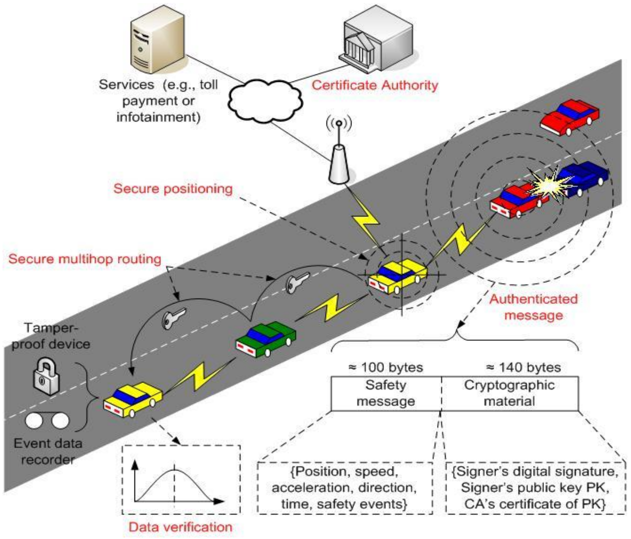

Figure 1: Vehicular Ad-hoc Network

II. GEOCAST ROUTING PROTOCOL

It is also known as location based routing. In this routing protocol, path is constructed based on the location. It monitors vehicle's location on the basis of (GPS). It uses vehicle's location information of source node, destination node and next-hop node. It does not require to maintain any routing table for path. Routing is carried out through two steps, first is path selection, the routing path is constructed based on Dijikstra algorithm and second in shortest path, it computes the shortest path between the source and destination node. It is as further classified as Non-Delay tolerant network (Non-DTN) and Delay tolerant network (DTN).

The goal of Non-DTN routing protocol is to transmit information or packets as soon as possible without any delay. DTN It is based on a store-and forward policy by overlaying a protocol layer, called bundle layer which is to provide internetworking on heterogeneous networks operating on different transmission media. Some DTN based routing protocol are fastest-ferry routing DTN (FFRDV) and enhanced DTN based routing (ERDV).

a. Fastest-Ferry Routing in DTN-enabled in VANET (FFRDV)

It is a unicast routing scheme for VANET. It inlets message ferrying technique and selects vehicle based on velocity of vehicle. It divides road into logical blocks and at the beginning of each block initial ferry chooses the next ferry by comparing its speed with other ferries in that block and forwards the packet to the fastest ferry [2]. If initial ferry does not get any ferry with higher speed, it carries the message till next logical block this process continues till the destination node.

b. Enhanced Routing in DTN in VANET (ERDV)

It divides the road into blocks of variable size based on speed of vehicle [3]. The size of block is inversely proportional to the speed of the vehicle. Each vehicle has its own logical block based on its speed. Whenever vehicle enters into logical block it broadcasts HELLO message, each HELLO message contains speed and direction of vehicle. HELLO message gives information about speed of vehicle, on the basis of this initial ferry selects its next ferry and forwards message to it. The best feature of this routing is that it provides minimum end-to-end delay because it is not bound by fixed size of block.

III. NEED FOR SECURITY

The security of VANETs [7] is an important as it relates to the critical life situations when any misbehaviour occurred. It is imperative that vital information cannot be inserted or modified by a malicious node. The system must be able to determine the liability of node while still maintaining their privacy. These problems are difficult to solve because of the network size, the speed of the vehicles, their relative geographic position, and the randomness of the connectivity between them. An advantage of vehicular networks over the more common Ad hoc networks is that they provide ample computational and power resources. For instance, a typical vehicle in such a network could host several tens or even hundreds of microprocessors.

IV. SECURITY ATTACK IN VANET

If a node or vehicle modifies message, drops message in between, do not send message on time or affects the network to harm the user in any way.The attacks can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behaviour of the attack i.e. Passive or Active attack. To work correctly and effectively, it must follow some security majors as authentication, integrity, confidentiality, privacy to protect vehicles and vehicles information from the attackers. There are several attacks:

i. **Masquerading:** It can be easily performed on VANET. An attacker can easily enter into network and misguide other vehicles by sending false messages.

ii. **Replay Attack:** An attacker re-send the previously received message to the network and can poison a node's location table by replaying beacons.

iii. **Message Tampering:** An attacker modifying the message exchanged in vehicle-to-vehicle or vehicle-to-roadside unit communication in order to falsify transaction

iv. **Global Positioning System (GPS) Spoofing:** The GPS maintains a location table with the geographic location and identifies all vehicles on the network. An attacker can fool vehicles by manipulating reading of GPS device.

v. **Certificate Replication:** An attacker can undermine the system by duplicating a vehicle's identity across several other identity specially in hit-and-run events.

vi. **Sybil Attack:** In this attack, attacker creates a malicious node that broadcasts the false information to the network to harm other users for their personal interest. A vehicle declares to be several vehicles either at the same time or in succession. This attack is very dangerous since a vehicle can claim to be in different positions at the same time, thereby creating chaos and huge security risks in the network. The Sybil attack damages network topologies and connections as well as network bandwidth consumption.. The node spoofs the identities of other nodes is called as malicious or Sybil node. In this malicious or Sybil node gives the illusion of traffic jam or accident so that other vehicles change their route for the benefit of others.

V. MOVEMENT ABNORMALITY EVALUATION MODEL PREVENTION AGAINST SYBIL ATTACK –

The traffic moves in the two directions in the typical VANET model. Each direction has two lanes the vehicles in the first lane are marked with green and the second lane vehicles have been marked with the orange colour as shown in figure 6. The red colour vehicle in the bottom lane has been defined as the attacker node, which inject the false information in the cluster to launch the sybil attack to take the advantage by making its way clear in order to facilitate the hassle free movement by influentially changing the driving direction or lane of the other vehicles in the cluster. The red node have plotted the grey colour Sybil node in the front of the green vehicle and have slowed down the speed, which forced the green vehicle to change its lane to obtain the obstacle free movement, which directly gives the way to the red vehicle in the fast lane.

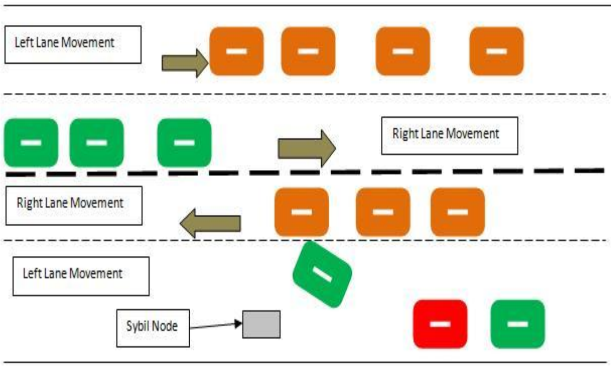

Figure 6: Demonstration of the Sybil attacks with single node.

In this work, a scenario is created upon the VANET security issue of Sybil Attack. In this attack one or more VANET nodes propagates their false location and direction to other nodes in the cluster, which may cause accident or traffic jam. This attacking mechanism can be utilized by terrorist or selfish driver to mandate their intensions. The solution suggested is applicable to the VANET cluster without any traditional setup of Road Side Units. The model is to protect against the fake information injection because the fake information injection attacks (E.g. Sybil Attack, etc.) are dangerous and can cause various false implications in the VANET cluster.

The minimum criteria has been defined to protect the vehicular network from the false information injection attacks. The false information injection attacks are initially found with the minimum originality criteria, which verify the behaviour of the vehicular node in the VANET cluster. If the minimum originality criteria are met, the node is declared as the authentic and permitted to join the VANET cluster. In case the originality criteria is not met, the vehicular node is verified more deeply for its movement, speed displacement, direction or driving, which gives us the better perspective about the authenticity of the vehicular node.

VI. PROPOSED MODIFIED SYBIL ATTACKED NODE IDENTIFICATION ALGORITHM (MSANI ALGORITHM) –

The nodes has the location and denoted by the X and Y coordinates. The node has coordinate (Xp,Yp) and the Centre node (Xc,Yc). Each vehicle node has the speed. Each vehicle has antenna mounted on the vehicle. Its range is R meter. Now the nodes are identified that are in the antenna range. Nodes that are not in the range of antenna, are removed. Now the node whose behaviour is not correct is identified. The direction of the node is received from the node by centre node. It is also calculated by the centre node also. If both matches then it indicates that the node location is correct. If not matches then it means that the node is attacked node and it is removed from the network. Now the packets are transferred using the ERDV protocol and FFRDV protocol.

VIII. SIMULATION AND EXPERIMENT

To simulate MSANI implementation, here MATLAB 7.0 is used for simulation and getting experimental results. The simulation is carried out using wireless network IEEE protocol 802.11 in MATLAB.The advantage that MATLAB offers is that it is widely available, continuously updated and has wider reach. To simulate a scenario is created with Experimental Area 500 meter length and 100 meter breadth road. A scenarios is created one for Sybil Attack

In the scenarios we are using two routing protocols Fastest Ferry Routing in DTN enabled VANET (FFRDV) and Enhanced Routing in DTN enabled VANET (ERDV) for transferring packet. The packets are transferring with the speed of 11 MBPS and size of packet is 512 kb. We are sending only two packets in our experiment. The block size for FFRDV is 100 meter. We are considering that each vehicle is equipped with GPS and Omni direction Antenna of range 250 meter.Generally each vehicle on road moves with the speed between 30 km per to 100 km per hour, using speed of vehicle between 30-100 km/h. We are performing our experiment on different number of vehicles like 10, 25, 50, 100, 150, 200.

In this section we are going to present simulation scenario aimed at stimulating the network performance through network throughput and average packets end to end delay.

i. MSANI with ERDV

We are taking the number of packet = 2 and node 10, 25, 50, 100, 150 and 200. The Delay, % of node attacked and throughput is shown in table 5.3. From the table 5.3, the minimum delay is 31.5543 sec and maximum delay is 35.92 sec. The minimum attacked node is 35.75% and maximum is 40.02%. The minimum throughput is 27.04 % and maximum is 34.56 %.

Table 1: MSANI algorithm with ERDV

Node	Packet per Node	Delay	% of Node attacked	Throughput
10	2	35.569	35.75	34.56
25	2	34.4414	40.02	27.77
50	2	33.6318	37.59	32.07
100	2	35.92	37.9	28.69
150	2	34.3401	39.84	27.04
200	2	31.5543	37.59	32.25

Figure 7 shows delay in sending packet from sender to receiver with ERDV algorithm.

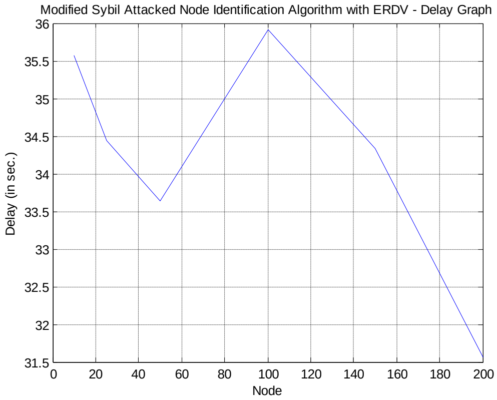

Figure 7: Delay Graph of MSANI with ERDV

Figure 8, shows number of packet attacked by malicious nodes with ERDV algorithm.

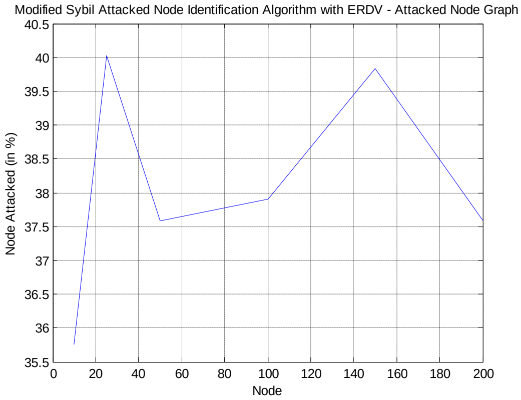

Figure 8: percentage of nodes attacked Graph of MSANI with ERDV

Figure 9, shows throughput of sending packets on network with ERDV

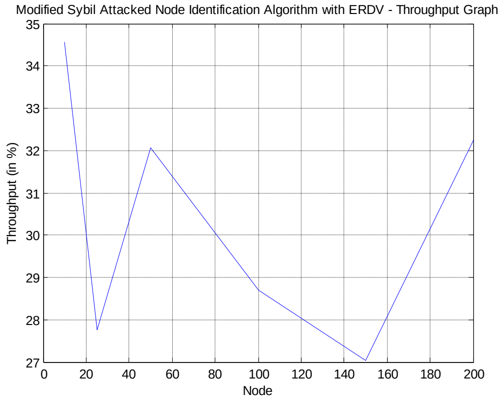

Figure 9: Throughput Graph of MSANI with ERDV

ii. MSANI algorithm with FFRDV

We take the number of packet = 2 and node 10, 25, 50, 100, 150 and 200. The Delay, % of node attacked and throughput is shown in table 4.2. . From the table 4.2, the minimum delay is 32.6407 sec and maximum delay is 36.3403 sec. The minimum attacked node is 35.69 % and maximum is 40.56 %. The minimum throughput is 27.44 % and maximum is 31.44 %.

Table 2: MSANI algorithm with FFRDV

MSANI Algorithmwith FFRDV				
Node	Packet per node	Delay	% of Node attacked	Throughpu t
10	2	36.340	37.48	29.99
25	2	33.990	37.75	28.69
50	2	34.16	35.81	31.44
100	2	34.776	39.67	27.44
150	2	32.640	40.56	31.08
200	2	32.895	35.69	30.6

Figure 10, shows delay in sending packet from sender to receiver with FFRDV algorithm.

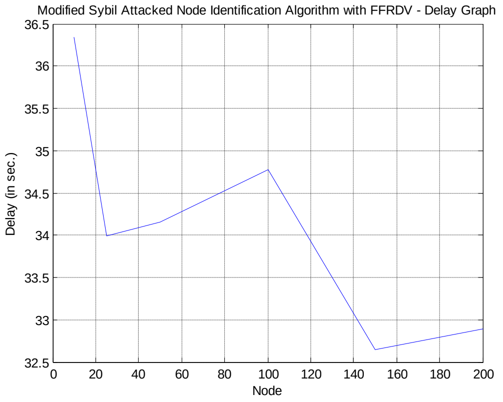

Figure 10: Delay Graph of MSANI with FFRDV

Figure 11 , shows number of packet attacked by malicious nodes with FFRDV algorithm

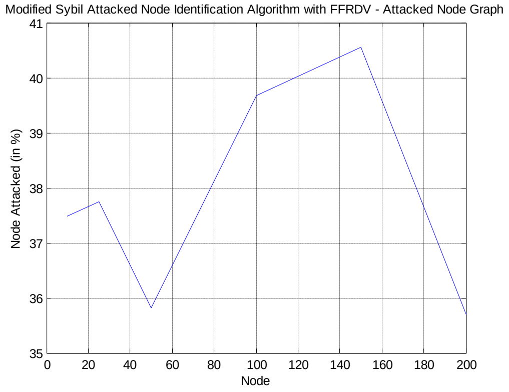

Figure 11: percentage of nodes attacked Graph of

MSANI with FFRDV

Figure 12, shows throughput of sending packets on network with FFRDV

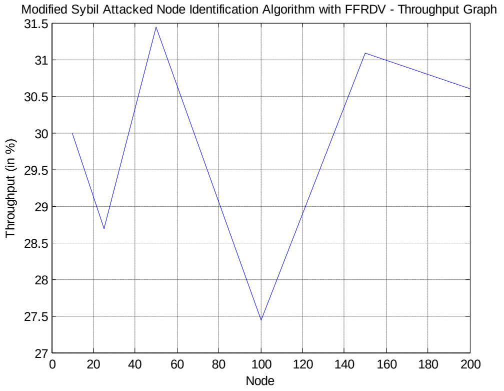

Figure 12: Throughput Graph of MSANI with FFRDV

iii. *Comparative Analysis of Results –*

a. Delay Analysis –

The delay analysis for MSANI Algorithm for ERDV and FFRDV is shown in the figure 13. In figure 13, it is observed that the delay is more in FFRDV for node 10, 50 and 200 while delay is more for ERDV for node 100 and 150. When see the graph, it is analysed that ERDV gives the minimum delay than the FFRDV.

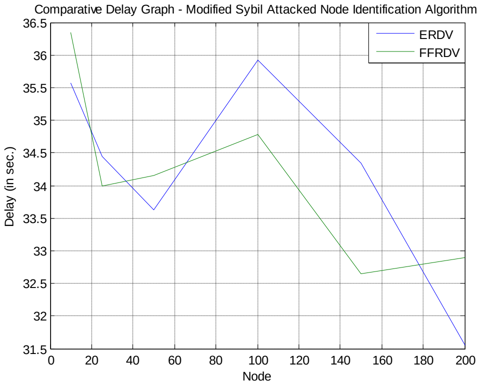

Figure 13:Comparative Delay Graph - MSANI Algorithm

b. Attacked Node Analysis –

The attacked node analysis for MSANI Algorithm for ERDV and FFRDV is shown in the figure 14. In figure 14, it is observed that there is more attacked node in FFRDV than in the ERDV.

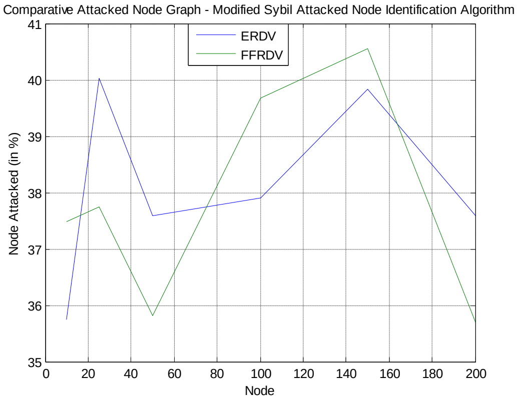

Figure 14: Comparative Attacked Node Graph – MSANI algorithm

c. Throughput Analysis –

The throughput analysis for MSANI Algorithm for ERDV and FFRDV is shown in the figure 15. In figure 15, it is observed that MSANI algorithm has more throughputs with ERDV than with FFRDV.

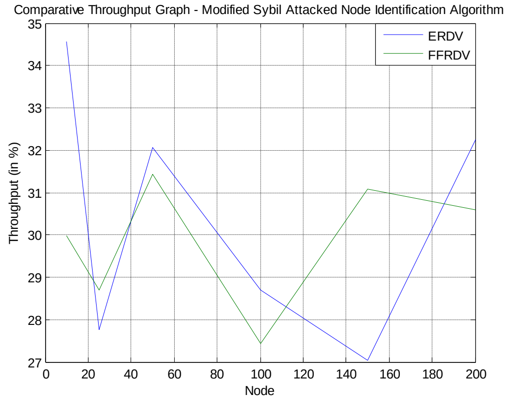

Figure 15: Comparative Throughput Graph - MSANI Algorithm

VIII. CONCLUSION

This paper includes Sybil Attack in VANET and its detection mechanism with FFRDV and ERDV routing protocol. The simulation is performed on MATLAB.

The delay, number of attacked node and throughput is obtained. From the analysis it is found that ERDV gives the minimum delay than the FFRDV. There is more attacked node identified in FFRDV than in the ERDV. MSANI algorithm has more throughputs with ERDV routing protocol than with FFRDV protocol. The results show that MSANI algorithm gives better results with ERDV than FFRDV.

IX FUTURE WORK

VANET have various kinds of attacks and one single solution does not work for all. In this work, ERDV and

FFRDV routing protocols are considered. The delay and throughput are taken in to account. Still there is delay while transferring packets from sender to destination. Many routing protocols were designed for VANET but because of its highly dynamic nature, none is able to work perfectly.

In the future, other routing protocols can be implemented. Other quality of service parameters can be considered. To solving these problems, the VANET network can be further secured and improved.

REFERENCES

1. Sherali Zeadally , Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, **“**Vehicular ad hoc networks (VANETS): status, results, and challenges”, August 2012, Volume 50, Issue 4, **pp 217-241, http://link.springer.com/article/10.1007%2Fs11235-010-9400-5**
2. Danlei Yu, Young-Bae Ko, “FFRDV: Fastest-Ferry Routing in DTN-enabled Vehicular Ad Hoc Networks”, Nov 2014 IEEE Publication.
3. Arun Kumar, “Enhanced Routing in Delay Tolerant Enabled Vehicular Ad Hoc Networks”,International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012.
4. Stampoulis, A. & Chai, Z., “A Survey of Security in Vehicular Networks”, http://zoo.cs.yale.edu/~ams257/projects/wireless-survey.pdf. (accessed: May 29, 2010).
5. Mainak Ghosh, Anitha Varghese, Arzad A. Kherani and Arobinda Gupta, “Distributed Misbehavior Detection in VANETs” , 2009 IEEE
6. Uzma Khan, Shikha Agrawal and Sanjay Silakari, “A Detailed Survey on Misbehavior Node Detection Techniques in Vehicular Ad Hoc Networks”, © Springer India 2015
7. Kadam, M., Limkar, S.: D and PMV: “New approach for detection and prevention of misbehave/malicious vehicles from VANET”. In: Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013. AISC, vol. 247, pp. 287–295. Springer, Heidelberg (2014)
8. Omar Abdel Wahaba, Hadi Otrokb and Azzam Mourada, “A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles”, Computer Communications 41 (2014) 43–54, at elsevier publication
9. Sonali Swetapadma Sahu and Manjusha Pandey,School of Computer Engineering, Kalinga Institute of Industrial Technology (KIIT), “Distributed Denial of Service Attacks: A Review”, I.J. Modern Education and Computer Science, 2014, 1, 65-71
10. Ashish Vulimiri, Arobinda Gupta, Pramit Roy, Skanda N. Muthaiah, Arzad A. Kherani, “Application of Secondary Information for Misbehavior Detection in VANETs”, HAL Id: hal-01059125 https://hal.inria.fr/hal-01059125

Submitted on 29 Aug 2014

11. Ghosh, M., Varghese, A., Gupta, A., Kherani, A., Muthaiah, S.: “Misbehavior detection scheme with integrated root cause detection in VANET”. In: VANET’09, 6th ACM International Workshop on Vehicular Internetworking. (2009)

12. Thaneswaran Velauthapillai, Aaron Harwood and Shanika Karunasekera," Global Detection of Flooding-Based DDoS Attacks Using a Cooperative Overlay Network", Fourth International Conference on Network and System Security, IEEE, 2010.
13. Huey-Ing Liu, Kuo-Chao Chang," Defending Systems against Tilt DDoS Attacks", The 6th International Conference on Telecommunication Systems, Services, and Applications, IEEE, 2011.
14. Al-kahtani, M.S.: "Survey on security attacks in vehicular ad hoc networks (VANETs)". In: 6th IEEE International Conference on Signal Processing and Communication Systems (ICSPCS), pp. 1–9 (2012)
15. Harit, S.K., Singh, G., Tyagi, N.: "Fox-hole model for data-centric misbehavior detection in VANETs". In: 3rd International Conference on Computer and Communication Technology (ICCCT), pp. 271–277 (2012)
16. Ghosh, M., Varghese, A., Kherani, A., Gupta, A.: "Distributed misbehavior detection in VANET". In: IEEE Wireless Communication and Networking Conference. (2006)
17. M. Milton Joe, R.S. Shaji, K. Ashok Kumar, "Establishing Inter Vehicle Wireless Communication in Vanet and Preventing It from Hackers", I. J. Computer Network and Information Security, 2013
18. P. Luo, H. Huang, et al. "Performance Evaluation of Vehicular DTN Routing under Realistic Mobility Models" IEEE Communication Society, WCNC 2008
19. Z. Zhang, Q. Zhang, "Delay/Disruption Tolerant Mobile Ad Hoc Networks: Lastest Developments" Wirel. Commun. Mob. Comput. 2007
20. L. Franck. (2007). Using Delay Tolerant Networks for Car2Car Communication. Proc. of ISIE2007, (pp. 2573 – 2578).