World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:14, No:5, 2020

Malicious Vehicle Detection Using Monitoring Algorithm in Vehicular Adhoc Networks

S. Padmapriya

***Abstract*—**Vehicular Adhoc Networks (VANETs), a subset of Mobile Adhoc Networks (MANETs), refers to a set of smart vehicles used for road safety. This vehicle provides communication services among one another or with the Road Side Unit (RSU). Security is one of the most critical issues related to VANET as the information transmitted is distributed in an open access environment. As each vehicle is not a source of all messages, most of the communication depends on the information received from other vehicles. To protect VANET from malicious action, each vehicle must be able to evaluate, decide and react locally on the information received from other vehicles. Therefore, message verification is more challenging in VANET because of the security and privacy concerns of the participating vehicles. To overcome security threats, we propose Monitoring Algorithm that detects malicious nodes based on the pre-selected threshold value. The threshold value is compared with the distrust value which is inherently tagged with each vehicle. The proposed Monitoring Algorithm not only detects malicious vehicles, but also isolates the malicious vehicles from the network. The proposed technique is simulated using Network Simulator2 (NS2) tool. The simulation result illustrated that the proposed Monitoring Algorithm outperforms the existing algorithms in terms of malicious node detection, network delay, packet delivery ratio and throughput, thereby uplifting the overall performance of the network.

***Keywords*—**VANET, security, malicious vehicle detection, threshold value, distrust value.

I. Introduction

VANET is an infrastructure-less wireless network and are created by applying the primary principles of MANET. The main key component of VANET is Intelligent Transportation System (ITS) which enables various users to be more cooperative with better information exchange, thereby forming a safer and smarter transport network [1]. The term VANET is synonymous with the generic term Inter Vehicle Communication (IVC). Such system examines the capacity of the vehicles to communicate, not only between them but also with the infrastructure [2].

All information is collected and processed to offer useful services. VANET supports short range technologies like Wireless Fidelity (WiFi), Infrared, Bluetooth and Visible light communication. Also cellular technologies like Long Term Evolution (LTE), Worldwide Interoperability for Microwave Access (WiMax) are supported by VANET. The default data rate of VANET is 6 Mbps. Two types of communication are carried in VANET [3]. The first one is Vehicle to Vehicle communication (V2V), in which the vehicles participate only in the transmission of message in order to reach the destination [4].

The second is Vehicle to Road side unit communication (V2R), and the communication is established between vehicle and the RSU. For getting any safety message, vehicles communicate with these RSUs and only the header vehicle or the base source vehicle is allowed to communicate with this RSU [5]. V2V is a robust communication when compared to V2R [6]. The main characteristic challenges of VANET are high mobility of vehicles and crucial effect of security and privacy [7]-[9]. The nature of VANET could lead to some malicious attacks and the attackers break the whole system just by feeding false or dummy information and by making the system to overflow. As VANET relies on vehicle to vehicle communication, security becomes the major concern. This is due to the reason that any vehicle can be easily hacked by the hacker for their selfish motives. Hence in this paper, Certificate authority algorithm is proposed through Monitoring Algorithm that identifies malicious vehicles in the network. The proposed network follows both V2V and V2R communications.

II. Related Work

In order to protect the valuable information, security is an important issue in routing. The study in [10] presents Secure and Intelligent Routing (SIR) protocol, where data are transmitted through authenticated vehicles in a quickest path. Also, selecting the authenticated vehicles in the quickest path secures the system from malicious attacks. Data transmission is provided through most connected path as minimum link connection enhances the system performances. In [10], weight (W) is calculated for every neighbouring junction $J_{neighbour}$ by using the safety message transmission model, link connectivity model, delay model and vehicle position model.

The $J_{neighbour}$ with minimum W is selected as the junction through which the data are forwarded to the destination D. Based on group signature, an efficient privacy preserving authentication scheme is made in vehicular networks. Though group signature is often used in VANETs to realize authentication, such schemes suffer from high computation delay in the checking the certificate revocation list and in the signature verification process. This leads to high message loss. As a result, they cannot meet the need of verifying hundreds of messages per second in VANETs. Also, [10] formulated a scheme to divide the precinct into several domains, in which RSUs are responsible for distributing group private keys and for managing vehicles in a localized manner. Hash Message Authentication Code (HMAC) is implemented in [10] to avoid

S. Padmapriyais with Electronics and Communication Engineering Department of Manakula Vinayagar Institute of Technology, Puducherry, India (phone: +91-8608259050; e-mail: padmaece.r@gmail.com).

time-consuming verification of Certificate Revocation List (CRL) and to ensure the incorruptibility of messages before batch group authentication. Finally, a cooperative message authentication algorithm is adopted to reduce the authentication burden. All the vehicles are made to verify fixed number of messages to avoid overloading a particular vehicle. Also, the scheme in [10] is comparatively efficient in terms of authentication speed and conditional privacy in VANETs.

Safety applications should also be designed for VANETs as the network may have vehicles that are involved in transmitting false or inaccurate information. Design of mechanisms that detect such misbehaving nodes is an important issue in VANETs. In [11], the authors investigate the use of correlated information, called "secondary alerts", created in return to another alert, called as the "primary alert" to verify the truth or falsity of the primary alert received by a vehicle. The author in [11] presented a framework to model how such correlated secondary information observed from more than one source can be unified to generate a "degree of belief" for the primary alert. Then, an instantiation of the model is presented in [11] for the specific cases such as Post-Crash Notification and Slow/Stopped Vehicle Advisory. Post-Crash Notification is the primary observant notification and the Slow/Stopped Vehicle Advisory is the secondary alerts.

Design and evaluation of a misbehaviour node detection scheme for VANET is required with Post Collision Notification (PCN) strategy. As each vehicle cannot be a source of all messages in VANET, most of the communication depends on the information received from other vehicles. To protect VANET from malicious action, each vehicle must be able to calculate, decide and react locally on information received from other vehicles. Message verification is more challenging in VANETs, since the privacy and security of the participating vehicles is the major concern. The Certificate Authority (CA) algorithm [12] uses detection of malicious node in the network based on the threshold range with that of the decision parameter of individual vehicle. VANET relies on node to vehicle communication, and hence the threshold range will vary. This is one of the main drawbacks of CA algorithm.

Each vehicle needs to verify the accuracy of the message and needs to verify whether the received message is from a reliable and legitimate vehicle. In [13], an algorithm to secure vehicular communication is presented with the help of the trust value measured for the given period using a probabilistic approach. This algorithm secures VANET against the untrustworthy drivers.

VANET also faces challenge of security breach due to the presence of wireless channel and several known security holes in the network. To protect against such attacks, methods and some additional abilities are developed in [14]. The Intrusion Detection System (IDS) [14] detects malicious or false actions made to the system. In VANETs, IDSs are in charge of examining incoming and outgoing packets to identify malicious signatures. IDS also adapts a decision making protocol for security information in VANETs. As well, two IDS approaches are studied in [14]. Based on speed, the vehicles are classified and IDS is deployed. The IDS are installed on the vehicles in the first one, whereas in the second method, IDS are installed and initialized on the RSU. Verification of an attack is based on a probabilistic model. The level of attack is computed by the number of vehicles or RSUs that has reported the signature of the attack. The dynamic topology of VANET provides a strong prevention towards attacks by transmitting the information through a verification protocol that also alerts neighboring clusters [15].

Detecting misdeed such as transmissions of false information in VANETs is a very serious problem in the networks with wide range of vehicles that in turn impart network bottle neck. In [16], authors discussed several limitations of existing MDS designed for VANETs. Most VANETS are disturbed with detection of malicious nodes. In certain situations, vehicles would send wrong or false information because of its selfish owners who intent to capture access to a particular lane. It is therefore more important to detect and identify false information than that of identifying misbehaving nodes. Also they introduce the concept of data-centric misbehavior detection and propose an algorithm which identifies false alert messages and misbehaving nodes by observing their actions after sending out the active messages. With the data-centric Misbehaviour Detection Scheme (MDS), each node can take decision on whether the information received is true or false.

The decision is based on the texture of recent messages and new alerts with estimated vehicle positions. No voting or majority decisions are needed, making the MDS resilient to Sybil attacks. After misbehavior detection, it does not revoke all the secret credentials of misbehaving or duplicate nodes. Instead, fine is imposed on misbehaving nodes and such nodes are dejected to act on their own. This reduces the communication costs and computation involved in repealing all the secret credentials of misbehaving nodes.

Vehicular Security through Reputation and Plausibility Checks (VSRP) [17] for VANETs are essentially used to communicate with real-time traffic and safety information. In [17], vehicular security algorithm is presented in terms of reputation and plausibility checks to address the most important problem of security in VANETs. The algorithm provides security against the attacks of data dropping, data aggregation, false event generation and event modification. It performs not only detection in the network, but also isolates malicious nodes in vehicular network. The algorithm employs sensors in a reputation-based system and yields a sensible yet cost efficient approach as it utilizes just V2V communication. Hence, the security issues and the cost associated with the RSU infrastructure are reduced. Reference [17] studies various scenarios that are noted to be very efficient and effective in terms of the percentage of malicious nodes detected, average time taken to detect malicious nodes, number of control packets transmitted after the detection of malicious nodes, number of packets dropped during transmission, and the number of packets received by malicious nodes in the network.

Security remains the major aspect for VANET application

due to time constrains. Researchers have proposed a number of solutions to counter such attacks in the network and also to improve certain aspects of security i.e. privacy, authentication, non-repudiation etc. Some of the solutions obtained are based on group formation concept. Disseminating messages in a secured manner over an applicable geographical area is another challenge for VANET. Work in [18] proposed two schemes, one for efficient group formation that enhances life time of a group leader and the second scheme is a hybrid (symmetric/asymmetric) message broadcasting scheme for faster and secured communication.

III. Proposed Model

VANET consists of vehicles and RSU which can communicate with other vehicles by means of short range radio communication. For security purpose, VANET will have third party agency called CA which has a major decision making capability about the malicious vehicles. These authorities are responsible for managing identity of the vehicles in the network. Based on the misbehaviour verification reports, the CA modifies the distrust value of the vehicles.

For each vehicle, two lists are given, one is a white list and the other is a black list.

i. White list is provided by the cluster head vehicle. The neighbouring nodes residing in the cluster will request for certificate from their respective cluster head, and
ii. Black list contains the ID of all malicious vehicles that are identified so far. Black list will be sent by the CA to all the vehicles. Based on the number of packets dropped/ destroyed/duplicated by a vehicle, the distrust value of that particular vehicle is incremented. Vehicles with higher distrust value are added in the black list and isolated from the network.

With such network model, we propose Monitoring Algorithm that compares the distrust value (number of packets dropped) and the threshold values to identify the malicious vehicle thereby isolating such nodes from the network.

Information disseminated by the vehicles in the network is analysed and compared with information received by the other vehicles to verify the originality about the alert message. Our proposed Monitoring Algorithm improves the effectiveness of selecting the authority vehicle or the cluster head in the vehicular network and improves the network performance by advance detection of malicious vehicles. Monitoring Algorithm gives better performance than the other two existing algorithms presented in [12] and [17]. This algorithm also improves throughput with better packet delivery ratio. By detecting malicious node in a short span, the proposed Monitoring Algorithm (MA) reduces the Network delay.

a. *Distrust value (D_v):* Distrust value is broadcasted by CA to all the vehicles in the network. Initial distrust value is given as 1. As the communication period proceeds, malicious vehicles are detected and isolated from the network. This distrust value may either increaseor remain the same based on the monitoring process done by the CA. If any misbehaving node is identified, the vehicle's distrust value is increased by 1. This distrust value is stored in the cluster head of the network also.
b. *Threshold value (T_v):* Threshold value is calculated for each vehicle in order to compare the value with the obtained distrust value. Threshold value is calculated using (1), and compared with D_v

$$T_v = 1 + (1 - P_c)^{\beta-\gamma}(P_c)^{\gamma} \quad (1)$$

where, T_v - threshold value; P_c - probability of missing or duplicating packet; β - number of transmitted packet per sec.; γ - number of drops or duplicates packets.

c. *Verifier:* Verifiers are vehicles elected by the cluster head. Verifiers act based on distrust value. Verifier selection is based on the area of the network represented by,

$$Area(V) = tr(V) - pl(S_{\max} - S_{\min}) \quad (2)$$

where, $tr(V)$ - transmission range of vehicle; pl - packet latency; $S_{\max}$ - maximum speed of vehicle; $S_{\min}$ - minimum speed of vehicle.

The vehicle with minimum distrust value is elected as a verifier by the cluster head. The cluster head will receive all the information about the vehicle from the CA. In MA, the verifier does the process of monitoring the vehicle that enters the area "Area (V)". During the monitoring process, if any vehicle shows misbehaviour indications such as dropping the packets, duplicating the original packets or destroying the packets intentionally, then the verifier reports such misbehavior activity to the corresponding cluster head. Consequently, the cluster head modifies the distrust value of such misbehaving vehicle. Once the distrust value is changed, it is compared with the threshold value of the vehicle. If the distrust value is greater than the threshold value, then the vehicle is identified and tagged as malicious vehicle, thereby isolating such nodes from the network.

d. *Black list (BL):* Black list of MA is maintained by the cluster head. It stores all the ID of malicious vehicles send by the verifier to BL, i.e. if the distrust vector is greater than the threshold value, ($D_v > T_v$), such vehicle's ID is moved to the BL of the corresponding cluster head.
e. *White list (WL):* In proposed MA, white list is maintained by all the vehicles in the network. If the threshold value is greater than the distrust value, then the vehicle's ID is shared to all the associated neighbours within the cluster, i.e. if $D(v) \leq T(v)$, the ID of vehicle is kept in neighbour's WL.

Fig. 1 shows the flowchart of MA in which the monitoring process for vehicle V. The steps involved in MA are presented below:

Step1. Form cluster and distribute the cluster keys to the vehicles in Area (V).
Step2. Allocate initial distrust value for all the vehicles in the network.
Step3. Monitor the vehicle's packet drop rate through the verifiers.
Step4. Determine abnormal behavior of a vehicle with the

help of neighbor.

Step5. Determine threshold value for the vehicle which has abnormal behavior.

Step6. Update BL of the cluster head and WL of the neighboring vehicles based on D_v.

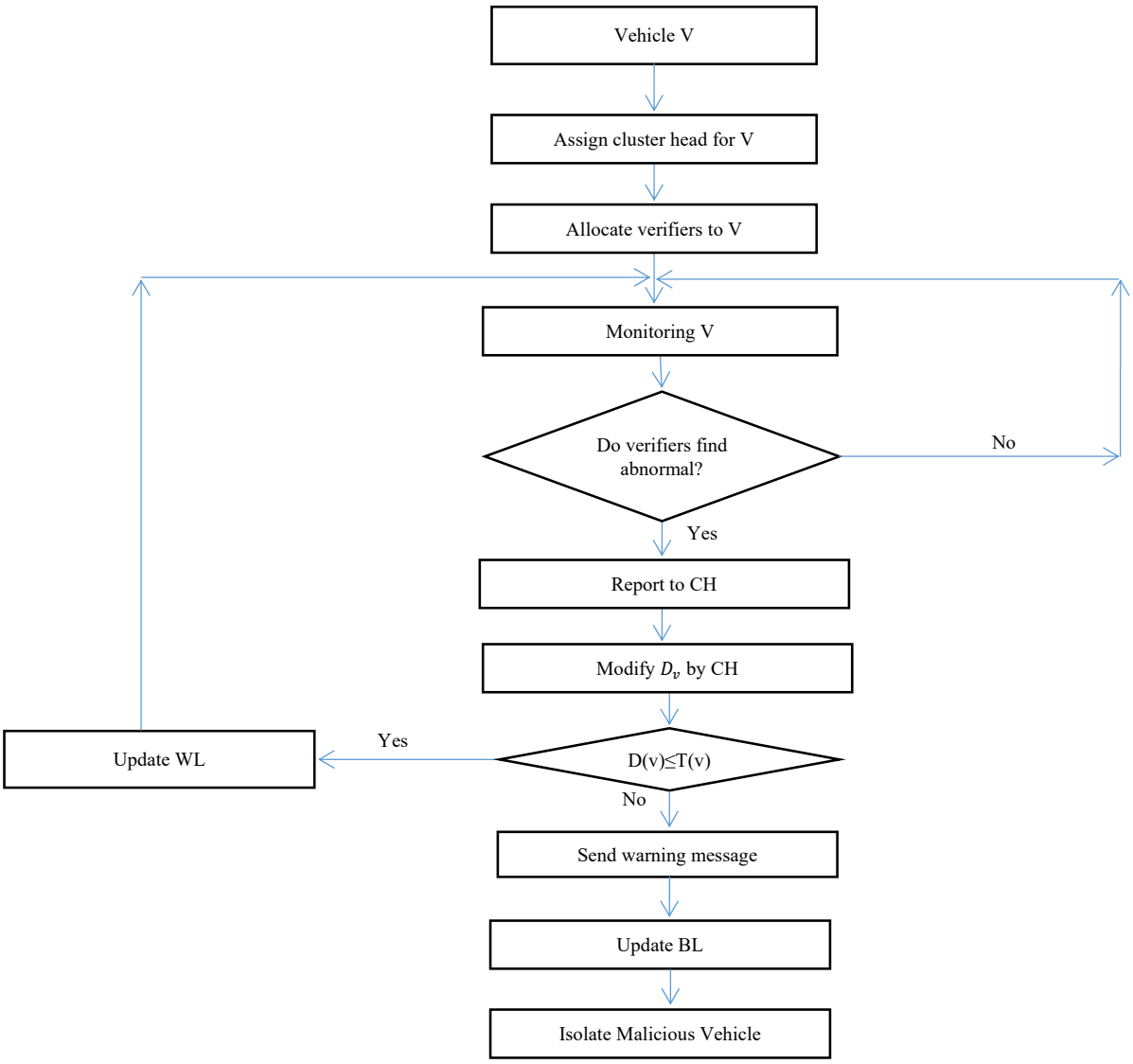

Fig. 1 Flowchart of MA

When a vehicle enters a network, the CH obtains the cluster keys from the cluster authority and it allocates a verifier to monitor the vehicle. During the monitoring process, if the verifier detects any abnormal events such as packet duplication or packet loss, then the verifier reports the CH to modify the $D_v$which is then compared withT_v.

If D_v>T_v, then warning messages are sent to all vehicles in the network by updating the BL of CH. The Malicious vehicle is isolated from the network. If $D_v \geq T_v$, then BL and WL of all the neighbour vehicles are updated and the next vehicle monitoring process continues. Thus, through such multilevel verifications, the proposed MA outperforms the existing algorithms in terms of delay, packet drop ratio, average number of packets transmitted successfully and throughput.

IV. Simulation Results and Discussions

Performance analysis for the proposed model is studied for 40 vehicles using NS2 tool and the metrics like delay, malicious node detection, packet delivery ratio and throughput are analysed. The proposed MA is compared with the existing CA [12] and VSRP [17] algorithms.

End to end delay is defined as difference between the packet delivery time at destination and the packet origination time at source.

$$\text{End to End Delay} = \text{Packet delivery time at destination} - \text{Packet origination time at source}$$

Delay must be minimum in the network in order to have proper and correct time of packet reception in real time cases.

Fig. 2 shows the characteristics of End to End delay for the three algorithms discussed. The verifier reports the start time and end time of the packet to the cluster head and hence the cluster head will calculate the delay of the network. Based on the calculated delay, the cluster head immediately checks for the prevalence of malicious modes. If any such node is detected, cluster head immediately black lists the corresponding node and communicates the same to all other associated nodes thereby regaining the network speed. Hence, from Fig. 2, it is evident that the proposed algorithm has minimum delay when compared to the other two existing algorithms.

Fig. 2 End to End delay

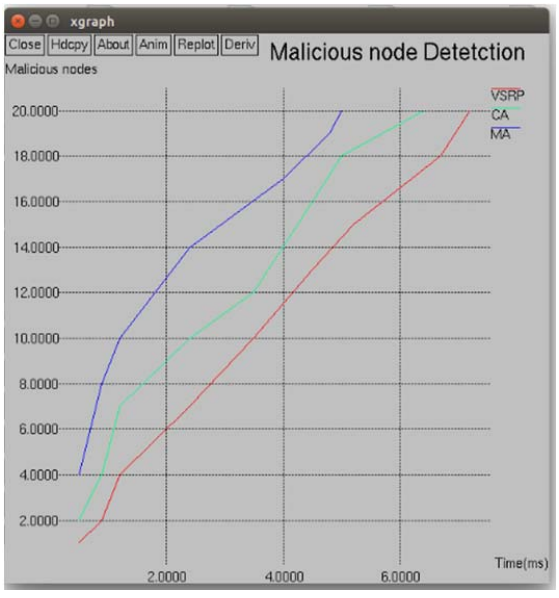

Fig. 3 Malicious node detection

Malicious node detection is analysed over 6,0000 ms. For consideration, 20 vehicles (out of 40 vehicles) are blacklisted as malicious nodes and the time is noted to detect those 20 malicious vehicles. On comparison, proposed algorithm consumes less time to detect the malicious node in the network. This is due to the reason that the cluster head and verifier (CA) jointly act to detect the malicious nodes and the black list is simultaneously shared to all the nodes in the network. Such countermeasure protects the network from further packet drop. Hence, malicious node is detected in a small duration of time as shown in Fig. 3, whereas the existing VSRP and CA algorithms take extra time than the proposed algorithm to detect all 20 nodes.

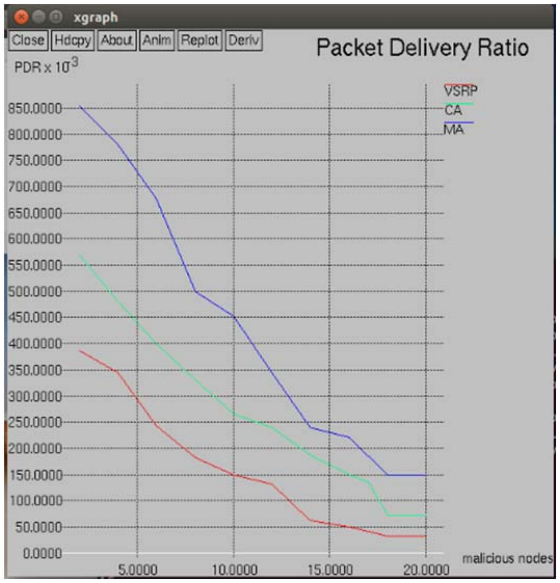

Fig. 4 Packet delivery ratio

Packet delivery ratio is defined as the ratio of successful data packets received by destination to the data packets generated by the source.

$$\text{Packet Delivery Ratio} = \frac{\text{Data packets received by destination}}{\text{Data packets generated by the source}}$$

The verifiers in the network monitor the packets transmitted between the nodes. These verifiers report about the data packets to the cluster head. After comparison, the cluster head will send a report about the vehicle to the verifier itself. Such strategy helps the MA to improve packet delivery ratio. The packet delivery ratio of the proposed MA is much better when compared to the existing techniques.

Packet delivery ratio is plotted between the number of malicious nodes in the network and the successful packet transmission between them as shown in Fig. 4. As the number of malicious nodes increases, packet delivery ratio of the network decreases.

Throughput is defined as the ratio of total packets received to the difference between stop time and start time of the packets. As the active time of the network increases (for fixed set of nodes), the successful packet transmission rate increases. The verifier in the network will report about the total received packets, start time and stop time of each packet to the cluster head. The cluster head calculates the throughput as,

$$\text{Average Throughput} = \frac{\text{Total Received packets}}{\text{Stop time} - \text{Start time}}$$

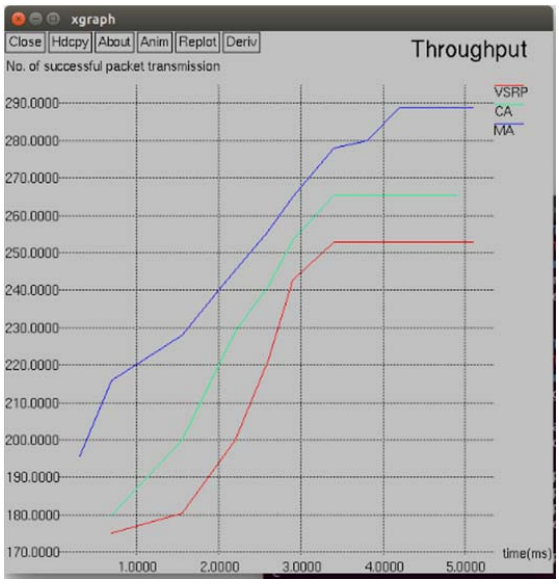

Fig. 5 Throughput comparison

Based on the throughput value, the cluster head dynamically changes the choice of CA, BL, WL and RSU. From the comparison, it is clearly evident that the proposed MA model yields better throughput than the two existing techniques as shown in Fig. 5. Hence, the proposed MA is much efficient and better than the two existing CA and VSRP algorithms.

TABLE I
PERFORMANCE COMPARISON

Metrics	Malicious Node Detection	Delay	Packet Delivery Ratio	Throughput (Packets/sec)
VSRP Algorithm	15 nodes	13ms	38%	253
CA Algorithm	18 nodes	10ms	57%	265
MA	20 nodes	7ms	85%	300

Table I illustrates that the proposed MA is much better than the two existing CA algorithm and VSRP algorithm. To withstand the performance analysis, 20 malicious vehicles are detected at 5 ms in MA and only 18 and 15 malicious vehicles are detected in CA and VSRP algorithms respectively. Also delay is much lesser in MA than the two existing algorithms discussed. 85% packet delivery ratio is achieved in MA whereas only 57% is obtained in CA algorithm and 38% is attained in VSRP algorithm. Throughput is nearly 300 packets/sec for the MA and for VSRP algorithm, the throughput is 253 packets/sec. Therefore, the above discussions show that our proposed MA is efficient and has minimum delay with better throughput and high speed of malicious vehicles detection than the two existing VSRP and CA algorithms.

V. CONCLUSION

In this paper, an algorithm called MA is proposed to detect the malicious vehicle in VANET. This algorithm uses pre-selected threshold value and distrust value for comparison and the false vehicle is detected with the joint effort of CA and CH. MA is more efficient than VSRP and CA algorithms which are used in existing method. Simulated results show that the proposed algorithm will have lesser delay and better throughput when compared to conventional methods present in VANET based literatures.

REFERENCE

[1] M. Raya, J. Pierre, Hubaux, "Securing vehicular ad hoc Networks" Journal of Computer Security,vol.15, pp: 39-68,jan 2007.
[2] Saurabh Kumar Gaur, S.K. Tyagi and Pushpender Singh, VANET System for Vehicular Security Applications, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.
[3] Kamran Zaidi, Milos Milojevic, Veselin Rakocevic and Muttukrishnan Rajarajan, Data Centric Rouge Node Detection in VANETs, International Conference on Trust Security and Privacy, IEEE 2014.
[4] Xiaoyan Zhu, Shunrong Jiang, Liangmin Wang, and Hui Li, ―Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks, IEEE Transactions on Vehicular Technology, vol. 63, no. 2, February 2014.
[5] M. Bharat, Dr. K. Santhi Sree and T .Mahesh Kumar, Authentication Solution for Security Attacks in VANETs, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 8, August 2014.
[6] Mahsa Ghaznavi and Azizollah Jamshidi, A Reliable Spectrum Sensing Method in the Presence of Malicious Sensors in Distributed Cognitive Radio Network, IEEE Sensors Journal, Vol. 15, No. 3, 2014.
[7] Jia-Lun Tsai, An Improved Cross-Layer Privacy-Preserving Authentication in WAVE-Enabled VANETs, IEEE Communications Letters, Vol. 18, No. 11, November 2014.
[8] Ajay Rawat, Santosh Sharma, Rama Sushil, "VANET: Security Attack and its Possible Solutions", Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, pp-301-304, 2013.
[9] Vishal Kumar, Shailendra Mishra, Narottam Chand, "Applications of VANETs Present & Future", *Communications and Network*, 2013, 12-15.
[10] Sourav Kumar Bhoi, Pabitra Mohan Khilar, SIR: a secure and intelligent routing protocol for vehicular ad hoc network, IET Network., vol. 4, no. 3, pp. 185–194, 2014.
[11] Asif Ali Wagan, Bilal Munir Mughal & Halabi Hasbullah, VANET Security Framework for Trusted Grouping using TPM Hardware, IEEE Conference on Communication Software and Networks,2010.
[12] Omar Abdel Wahab, Hadi Otrok, Azzam Mourad, A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles, Elsevier,2013.
[13] Romain Coussement, Boucif Amar Bensaber and Ismail Biskri, Decision Support Protocol for Intrusion Detection in VANETs, ACM 978-1-4503-2359-8/13/11,Barcelona, Spain, November 2013.
[14] Norbert Bi Bmeyer, Joël Njeukam, Jonathan Petit and Kpatcha M. Bayarou, Central Misbehavior Evaluation for VANETs based on Mobility Data Plausibility, Low Wood Bay, Lake District, UK, June 2012.
[15] Gongjun Yan, Danda B. Rawat, Bhed Bahadur Bista and Earl F. Shaner, General Active Position Detectors Protect VANET Security, IEEE International Conference on Broadband and Wireless Computing, Communication and Applications, 978-0-7695-4532-5/11,2011.
[16] Danda B. Rawat, Bhed B. Bista, Gongjun Yan, and Michele C. Weigle, Securing Vehicular Adhoc Networks against Malicious Drivers: A Probabilistic Approach, International Conference, IEEE, 2011.
[17] Sanjay K. Dhurandher and Mohammad S. Obaidat, Vehicular Security through Reputation and Plausibility Checks (VSRP), IEEE Systems Journal, vol. 8, no. 2, June 2014.
[18] Jeong-Ah Jang "A Fixed Sensor-Based Intersection Collision Warning System in Vulnerable Line-of-Sight and/or Traffic-Violation-Prone Environment", IEEE Transactions on Intelligent Transportation Systems, pp 1-11, 2011.