Indian Journal of Science and Technology, *Vol 8(35), DOI: 10.17485/ijst/2015/v8i35/79955, December 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

An Efficient Neighbor Discovery and Aloha based Collision Detection and Correction in VANET

K. Chandramohan[1]* and P. Kamalakkannan[2]

[1]Department of Computer Science and Engineering, Gnanamani College of Engineering, Namakkal - 637018, Tamil Nadu, India; chandramohancse@gmail.com
[2]Department of Computer Science, A. A. Government Arts College, Namakkal - 637002, Tamil Nadu, India; kamal_karthi96@yahoo.co.in

Abstract

Objectives: This paper proposes a novel method to addresses the problem of detecting and correcting collision attack in VANET and enhances the security of the nodes. **Methods:** The proposed Collision detection-based neighbor discovery model uses local monitoring to observe the behavior of neighborhood node. The collision detection is then shared with the immediate neighbors using warning message and propagated to a neighboring region with aiming at improving the broadcasting rate. In addition, proposed NDA-CDS uses Aloha-based Collision Correction which enables a randomized model that provides redundant information, allowing each individual node to process data packet using time slots to reduce time delay in correcting the colliding nodes which in turn maximizes the security of the nodes. The results are simulated in NS2 with each data packet size is differing from 7-49 byte. **Findings:** The NDA-CDC framework based on their immediate neighbors enhances the security of the nodes (i.e., vehicles) and reduces the delay time for detecting collision attack. The experimental results demonstrated that the proposed NDA-CDS model out performed than the existing state of the art works in terms broadcast rate, security and delay time for detecting and correcting collision. **Improvement:** The simulation result shows that proposed NDA-CDS method has advantages over the other existing system in terms of reducing the delay time for detecting collision attack and improving the security.

Keywords: Aloha-Based Collision Correction, Collision Attack, Message Authentication Protocol, Mix-Zone, Neighbor Discovery, Vehicular Ad Hoc Network

1. Introduction

Attack-Resilient Mix-zones over Road Networks (ARM-RN)[1] used mix-zone construction methods to avoid attacks by maintaining higher level of anonymity. Expedite Message Authentication Protocol (EMAP)[2] for Vehicular Ad Hoc Networks applied Hash Message Authentication Code to ensure security for packets being transmitted. However, both the methods were not based on the trajectory patterns which increased the time for detection.

The proposed framework addressed delay time by applying Aloha-based collision correction. Effective data aggregation[3] was performed in the presence of colliding attacks using Iterative Filtering. Another method designed in[4] was called as non-parametric approach for effective traffic classification[5] that reduce delay time using Nearest Neighbor classifier. However, with the absence of beacon messages, though delay time was reduced, acknowledgement of receipt of data packets was not made in between the nodes. Inter-Vehicular communication[5] was introduced to provide dynamic beaconing ensuring latency.

One of the emerging applications in Vehicular Ad hoc Network (VANET) is Intelligent Transportation Systems

*Author for correspondence

(ITS). Direction based Hazard Routing Protocol[6] was designed using Road Side Units (RSUs) in VANET to improve the number of vehicles received at RSU and minimize the dissemination delay. However, measures were not introduced to address the same issues with different traffic and security remained unaddressed. To solve the issues related to security in VANET, authentication mechanisms[7] were introduced that minimize the rate of false positive condition by improving the trust level practically. However, effective collision detection technique was not introduced. The proposed framework addresses this issue by introducing a Poisson approximation to improve the collision detection rate.

Collision probability estimation scheme[8] were used Cooperative Awareness Message for measuring inter vehicle communication to reduce collision attack. However, possible trajectories remained unaddressed. The framework NDA-CDC uses neighborhood node to determine the trajectories. Based on the trajectory of neighborhood node, Nash Bargaining from game theory[9] was introduced to improve the bandwidth utilization in VANET. A survey of misbehaving nodes in VANET[10] was presented to improve the safety on roads and driving conditions.

Road traffic simulation for Inter Vehicle Communication (IVC)[11] was designed with the objective of improving the average speed and coverage of network in the presence of attack. Another IVC method[12] was designed with the objective of improving the service coverage. In addition, Bilinear Diffie Hellman method[13] was developed to increase the message integrity in VANET. However, differentiation between normal and malicious nodes was not made in an efficient manner.

Based on the time of collision, Early Warning Intelligent Broadcasting algorithm[14] was introduced to improve the broadcasting rate. However, the road conditions were not considered during broadcasting. An efficient cluster authentication scheme[15] was introduced to ensure secure data packet transmission in the presence of replay attack. However, security remained unaddressed. The framework NDA-CDC applied Neighbor Discovery algorithm for secure data packet transmission in VANET.

The information regarding malicious node by the surrounding vehicles is enabled by in-vehicle sensors and VANETs. Information hiding techniques[16] contains two hiding techniques namely, subliminal channels and steganogrpahy that improve the robustness against communication errors. A survey regarding adaptive beaconing[17] was presented to improve the transmission of beacons using Adaptive transmission and Adaptive contention window. However, collision detection remained unaddressed. Furthermore, eMAC protocol and Energy-VeMAC[18] was introduced to prevent the collision and to improve the rate of throughput in message transfer between the vehicles. Collision detection and prevention for Unmanned Ground Vehicle in military battlefield using WSN based VANET[19] was developed to improve driving safety. Inter-Vehicular Collision avoidance system[20] was designed to perform safety communication with each other which can alert the drivers before accidents.

A novel MCBA architecture[21] was introduced for protecting applications against memory corruption attacks by incorporating efficient encoding of memory contents that reduced execution and protected the storage overhead. The centralized FEC algorithm[22] was more adaptive in adjusting and controlling the data redundancy across the network for static and dynamic channel fluctuations. Proactive parking based data replication method[23] was developed to improve the data accessibility in VANET. TPM-based Architecture[24] was designed in VANET which used a TPM component embedded in vehicles to improve security and anonymity of VANET communication.

In this paper we present NDA-CDC, a collision detection and correction framework in VANET to protect data packets and traffic. Compared to the existing methods, the NDA-CDC framework has a number of unique features. First, the NDA-CDC framework collision detection is developed based on the neighbor region and location information in assessing the neighbor nodes. This in turn improves the broadcast rate. Second, we introduce a Neighbor Discovery Algorithm based on local monitoring to improve the security of the data packets being transmitted by vehicles and therefore avoiding collision attack in VANET. Third, we develop a Aloha-based Collision Correction model to reduce the delay time in identifying the colliding nodes at an early stage. We formally analyze and experimentally validate the robustness of our NDA-CDC framework against collision timing attacks.

2. Design of Neighbor Discovery based Collision Detection and Aloha-based Collision Correction

In this section we introduce our Neighbor Discovery based Collision Detection and Aloha-based Collision

Correction framework for VANET in detail. We also present Neighbor Discovery (ND) algorithm in details. The NDA-CDC framework is implemented under the neighborhood region framework and employs neighboring region to observe the behavior for efficient collision detection and correction in VANET. The Block diagram of Neighbor Discovery based Collision Detection and Aloha-based Collision Correction is shown in the Figure 1.

As shown in Figure 1, the NDA-CDC framework to detect and correct the colliding attack in VANET is designed. The proposed Neighbor Discovery based Collision Detection and Aloha-based Collision Correction (NDA-CDC) framework uses sensor data collected by vehicles in VANET with the objective of reducing the delay time for collision detection and correction. The framework with the objective of improving the security of data packets being transmitted shares with immediate neighbors, and propagates them to a neighboring region. The validity of the sensor data is checked by individual vehicles in VANET with the objective of checking the validity of the data packets. NDA-CDC framework is split into three parts namely 1. Collision Detection-based Neighbor Discovery, 2. Neighbor Discovery algorithm based on location and 3. Aloha-based Collision Correction. The design of three parts is discussed elaborately in the following sections.

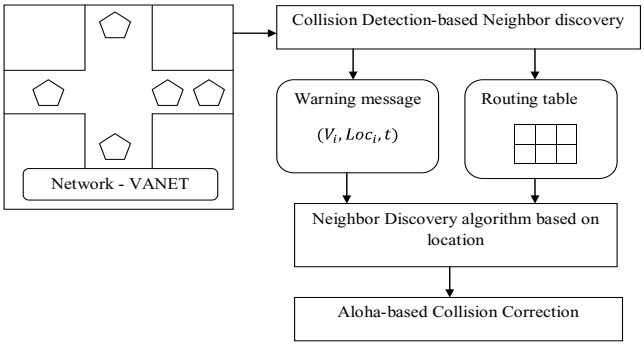

Figure 1. Block diagram of Neighbor Discovery based Collision Detection and Aloha-based collision correction.

2.1 Collision Detection-based Neighbor Discovery

One of the popular methods for detecting collision attacks in VANET is performed by observing the neighborhood node (i.e., vehicle) behavior or local monitoring of vehicles. Local monitoring by a vehicle efficiently monitors the data traffic or message transmission performed in and out of its neighbors. This is a join detection model where the process of monitoring is designed in such a way that the data packets or vehicles are verified by seeing to that they are being faithfully forwarded without any modification.

Let us consider a design of vehicular ad hoc network that consists of a set of nodes (i.e., vehicles) '$V_i = V_1, V_2, \ldots V_n$,' , a set of Road Side Units (RSUs) '$RSU_i = RSU_1, RSU_2, .. RSUn$,' and Certificate Authority '*CA*'. Suppose a node 'V_i' sends a warning message 'WM_i' at time 't' and is formulated as given below.

$$\sum_{i=1}^{n} V_i \rightarrow (WM_i, t) \quad (1)$$

Once a node 'V_j' receives warning message 'WM_i' from 'V_i, then the NDA-CDC depends upon the sensor data, collected by nodes that are shared with immediate neighbors, and passed to the neighboring region. The warning message consists of three tuples and is formulated as given below

$$\sum_{i=1}^{n} WM_i \rightarrow (V_i, Loc_i, t) \quad (2)$$

From Equation (2) the warning message 'WM_i' includes the vehicle from where the warning message originated 'V_i' the location of the vehicle 'Loc_i' and the time, '*t*' at which the warning message originated. After an interval of time '*t+i*', when 'V_i' receives a beacon message from vehicle 'V_j', checks for the validity of location. Upon successful validity of location data packet transmission is performed between the vehicles. Figure 2 shows the neighbor discovery based on changed location (Figure 2 (a)) and without changes in location (Figure 2 (b)).

Let us consider Figure 2 (a) with two vehicles 'V_1, V_2'. The vehicle 'V_1' sends a warning message 'WM_1' to vehicle 'V_2' at time '*t*'. After an interval of time '*t+i*', when vehicle 'V_1' receives a beacon message from vehicle 'V_2', the vehicle 'V_1' checks whether it is the neighboring node using location information.

As shown in Figure2 (a), the location of the vehicles has been changed whereas in Figure 2 (b) the location remains unchanged. In the NDA-CDC, with the objective of improving the broadcasting rate, the information regarding collision is shared with immediate neighbors and propagated to the neighboring region. The NDA-CDC then includes a routing table that consists of details including sensed node (i.e., vehicle), location and detected node which is maintained by '*CA*'. Table 1 shows the description of routing table.

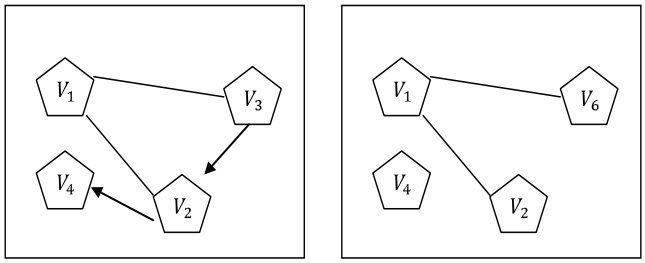

Figure 2. Shows the neighbor discovery based on changed location. (a) Changed location. (b) No changes in location.

As shown in Table 1, the nodes observe the sensed nodes that have been already detected successfully with immediate neighbors. With the aid of the above routing table, local monitoring by a vehicle is made in an efficient manner, aiming at improving the broadcasting rate. The NDA-CDC using neighbor discovery with the help of routing table checks to see if the location is contradictory. If both the location of the sensed node and detected node are contradictory, the detected nodes location in addition to the node is sent to the RSU by '*CA*'. As a result, only non-contradictory detected nodes are further considered in the network for data packet transmission. This in turn increases the broadcasting rate.

Table 1. Structure of routing table

Sensed Node	Location	Detected Node
V_1	(10,15)	V_6
V_2	(10,35)	V_7
V_3	(10,45)	V_8
V_4	(20,55)	V_9
V_5	(40,65)	V_{10}

2.1.1 Neighbor discovery algorithm

With the objective of improving the security in the NDA-CDC, a neighbor discovery algorithm is designed using local information. With the assumptions that data packet communication over long distances is limited in bandwidth, the NDA-CDC uses the neighbor propagation model. Figure 3 shows the Neighbor Discovery (ND) algorithm. The ND algorithm works with the objective of improving the security of the nodes which sends data packet to the destined or detected node. The ND algorithm works with the principle that the nodes share data packet with only the immediate neighbor nodes with the assumption that the neighboring nodes are valid nodes than the distance nodes which are considered as collided nodes.

Initialize Vehicles '$V_i = V_1, V_2, \ldots, V_n$', Warning Message '$WM_i$', Time '$t$' Road Side Units '$RSU_i = RSU_1, RSU_2, \ldots, RSU_n$'

Output: Collision detected node

Step 1: **Begin**

Step 2: **For** each vehicle V_i

Step 3: Sends a warning message 'WM_i' at time 't' using () to vehicle V_j

Step 4: Vehicle V_j checks for the warning message using (2) based on location

Step 5: **If** location (V_i) = location (V_j) **then**

Step 6: Detected node is neighbor node

Step 7: Perform data packet transmission

Step 8: **Else**

Step 9: Detected node is not neighbor node

Step 10: Detected node is colliding node

Step 11: **End if**

Figure 3. Neighbor discovery algorithm.

Figure 3 illustrates the algorithmic description of neighbor discover using local monitoring. Whenever a vehicle wants to send a data packet, the immediate neighbor nodes are detected and the location of the detected nodes is matched with the sender node's location. Efficient broadcasting takes place only the detected nodes location is same to that of the sender node's location. If both the location does not match, the detected node is not the node that the sender node has intended to send and is considered as the colliding node. This effective differentiation of normal nodes and colliding nodes helps in improving the security against colluding adversaries. Therefore detection and correction of malicious data is ensured.

2.2 Aloha-based Collision Correction

In the previous section, Collision Detection-based Neighbor Discovery using Local Monitoring assumed that the location information send in the warning message is correct. However, a colliding node with the intention of performing collision attack also sends wrong location

information, along with the false warning message. In this section we see, how to detect incorrect location information using Aloha-based Collision Correction model.

The NDA-CDC considers the Aloha-based Collision Correction model when all the '*n*' vehicles in VANET are arranged in a group. In Aloha-based Collision Correction model, we consider a slot where time interval '*T*' is divided into slots. Therefore, each message (i.e., data packet) transmission starts when the slot is initiated and lasts the entire duration of the slot.

Figure 4 shows the Aloha-based random model where the vehicle sends a data packet independently in a time slot '*T*' with probability '$P_{neighdis}$'. The aloha-based random model includes two self-loops, one with labels '$P_{neighdis}$ *and 1*' and another with labels '$P_{neighdis}$ *and 0*'.

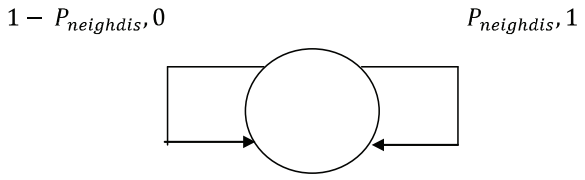

Figure 4. Aloha-based random model.

The Aloha-based Collision Correction in NDA-CDC framework is a randomized model that operates as follows. During each slot, a vehicle transmits a SAFETY message broadcast announcing its ID, with probability of proximity '$P_{neighdis}$'. It listens with the probability of proximity '1-$P_{neighdis}$' , where the SAFETY message broadcast is performed in a given slot only if exactly one vehicle sends data traffic in that slot.

Let '$V_i(t)$' be a random variable that represents the total successful data packet transmissions in VANET by vehicle '*i*' in the first '*T*' slots. By applying Poisson approximation in the NDA-CDC the success data packet transmissions in '*T*' slots is as given below:

$$P\left(V_i(t)\right) = \frac{e^{-a} * e^{n}}{n!} \tag{3}$$

From Equation (3), the probability of successful data packet transmission at time slot '*t*' is equal to the ratio of product of the event '*e*' that discovered the vehicle '*i*' and '*a*' representing data packet '*p*' at time slot ''. With this Aloha-based Collision Correction model, the probability of collision is detected at an early stage. Therefore, the delay time in identifying the collision is reduced in the NDA-CDC using randomized Aloha model.

3. Experimental Settings

In this section we evaluate the performance of NDA-CDC via simulation. NDA-CDC has been compared to Attack-Resilient Mix-zones over Road Networks (ARM-RN)[1] and Expedite Message Authentication Protocol (EMAP)[2] for Vehicular Ad Hoc Networks. The simulation parameter used for effective data transmission is given below (Table 2). The vehicles in NDA-CDC are positioned in uniform topology.

Table 2. Simulation parameters

Parameters	Values
Network area	1500 m * 1500 m
Vehicle density	10,20,30,40,50,60,70
Number of data packets i.e., number of data block	5,10,15,20,25,30,35
Size of data block (i.e., packet)	7 – 49 bytes
Range of communication	50 M
Speed of node	0 – 10 m/s
Simulation time	500 ms
Number of runs	7

The network consists of 70 vehicles, placed in a random manner in the Vehicle Ad hoc Network that generates traffic for every 10 m/s. The neighboring vehicle (i.e., node) collects the data packets of range 5-35 and forwards the data with each data packet size differing from 7-49 bytes. The simulation time varies from 100 simulation milliseconds to 500 simulation milliseconds and the following metrics like broadcast rate, security and delay time for detecting and correcting colliding nodes in VANET are measured.

The broadcast rate measures the amount of data packet received successfully. The broadcast rate is the ratio of data packets received to the data packets sent in VANET. It is measured in terms of percentage (%)

$$BR = \frac{DP_r}{DP_s} * 100 \tag{4}$$

From Equation (4), the broadcast rate '*BR*', measures the ratio of data packet received 'DP_r' and data packets sent 'DP_s'. Security with respect to data packets is measured on the basis of data packets received at the neighboring node in VANET. Therefore, security is the difference between the total packets sent to the packets not received in the neighboring node.

$$S(DP) = DP_s - DP_{nr} \quad (5)$$

From Equation (5), 'DP_s' refers to the data packets sent and 'DP_{nr}' refers to the data packets not received in the neighboring node in VANET. It is measured in terms of packets per second (pps). Delay time is the time taken to identify the collision in VANET with respect to varied node density. It is measured in terms of milliseconds (ms). Delay time is the product of time taken to identify the colliding node with respect to node density.

$$DT = Time\ (CN) * ND \quad (6)$$

From Equation (6), '*DT*' refers to the delay time with respect to colliding node '*CN*' and node density '*ND*'.

4. Discussion

The result analysis of Neighbor Discovery based Collision Detection and Aloha-based Collision Correction (NDA-CDC) framework is compared with the existing Attack-Resilient Mix-zones over Road Networks (ARM-RN)[1] and Expedite Message Authentication Protocol (EMAP)[2] for Vehicular Ad Hoc Networks.

Table 3 represents the broadcast rate obtained using NS2 simulator and comparison is made with two other methods, namely ARM-RN[1] and EMAP[2]. Figure 5 shows the result of broadcasting rate efficiency that measures the amount of data packet received successfully in VANET versus the varying number of data packets in the range of 7-49 bytes. To better perceive the efficacy of the proposed NDA-CDC framework, substantial experimental results are illustrated in Figure 4 and compared against the existing ARM-RN[1] and EMAP[2] respectively. The broadcast rate efficiency for different observations made by several nodes is performed at different time interval is shown above. Higher, the number of data packets being sent (i.e., the observation), more successful the framework is. The results reported here confirm that with the increase in the number of data packets, the broadcast rate efficiency also increases. The process is repeated for 35 different data packets.

As illustrated in Figure 5, the proposed NDA-CDC framework performs relatively well when compared to two other methods ARM-RN[1] and EMAP[2]. The broadcasting rate efficiency using NDA-CDC framework is improved with the application of Collision

Table 3. Broadcast rate with respect to number of data packets

Number of Data Packets	Broadcast Rate (%)		
	NDA-CDC	ARM-RN	EMAP
5	78.52	58.34	40.33
10	81.29	69.29	64.21
15	83.16	71.16	66.08
20	80.22	68.22	63.14
25	84.31	72.31	67.24
30	81.35	69.35	64.29
35	85.89	73.89	68.81

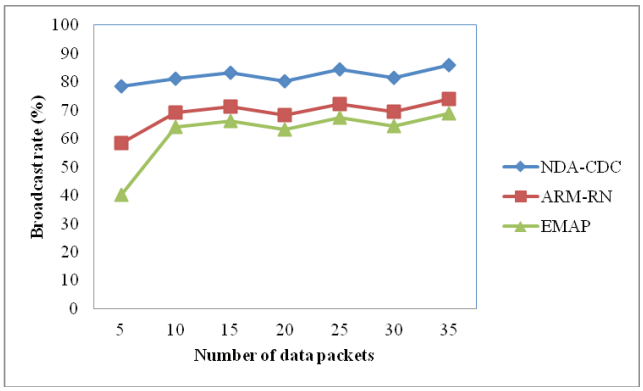

Figure 5. Measure of broadcast rate.

Detection-based Neighbor Discovery where message transmission is performed in and out of its neighbors. As a result, by applying local monitoring for each vehicle based on the neighboring node, results in the improvement of broadcasting rate efficiency using NDA-CDC framework by 19.83% and 34.25% compared to ARM-RN[1] and EMAP[2] respectively.

In Table 4 we compare the security with different number of data packets in VANET setting. The experiments were conducted with 35 observations (i.e., data packets) and the security obtained is measured in terms of packets per second (pps). In order to improve the security while observing the neighboring nodes that does not receive the data packets, the data packets sent and data packets not received is considered. In the experimental setup, the number of data packets ranges from 5 to 35 is illustrated in Figure 6. The security using the NDA-CDC framework provides comparable values than the state-of-the-art methods.

The targeting results of number of data packets sent to measure the security using NDA-CDC framework is compared with two state-of-the-art methods ARM-RN[1] and EMAP[2] in Figure 6. Our framework NDA-CDC

Table 4. Security with respect to number of data packets

Number of data packets	Security (pps)		
	NDA-CDC	ARM-RN	EMAP
5	4	3	3
10	7	6	4
15	11	10	9
20	17	16	13
25	20	19	17
30	22	20	19
35	27	23	21

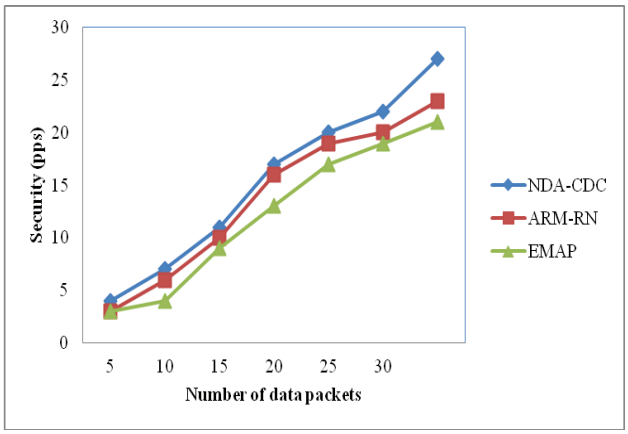

Figure 6. Measure of security.

differs from the ARM-RN[1] and EMAP[2] in that we have incorporated Neighbor Discovery algorithm where immediate neighbors are identified based on the location using warning message and checks for the validity of location. Based on the location validity, the results are generated and stored in routing table which is sent to RSU and maintained by CA. As a result, the security is improved by 15% and 28.24% compared to the ARM-RN[1] and EMAP[2] respectively.

Table 5 shows the delay time for collision detection and correction with respect to node density of size 70 vehicles in VANET. Figure 7 given shows the delay time for collision detection and correction for NDA-CDC framework, ARM-RN[1] and EMAP[2] versus seven different nodes (i.e., vehicles). The delay time returned over NDA-CDC framework increases gradually though not linear for differing node size because of the dynamic changes in the network and topology in VANET.

Table 5. Delay time with respect to node density

Node Density	Delay Time (ms)		
	NDA-CDC	ARM-RN	EMAP
10	220	260	295
20	235	265	300
30	249	279	312
40	240	270	278
50	255	285	293
60	242	272	280
70	249	279	287

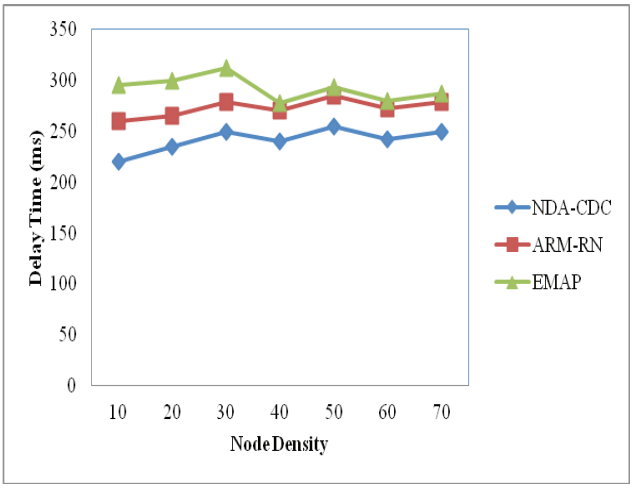

Figure 7. Measure of delay time.

From Figure 7, it is illustrative that the delay time is reduced using the proposed framework NDA-CDC. For example with node density 30, the delay time was 249 ms using NDA-CDC whereas ARM-RN[1] recorded 279 ms and 312 ms using EMAP[2]. Though the delay time for measuring collision detection and correction using all the three methods increase gradually, but using the proposed NDA-CDC, it is comparatively less. This is because with the application of Aloha-based Collision Correction. With the help of Aloha-based Collision Correction, a randomized model applies Poisson approximation that helps in identifying the collision at an early stage in an extensive manner. This in turn helps in reducing the delay time by 14.97% compared to ARM-RN[1]. In addition, by applying randomized Aloha model helps in improving the probability of successful data packet transmission using Poisson distribution and therefore reducing the delay time for collision detection and correction by 24.49% compared to EMAP[2].

5. Conclusion

Neighbor Discovery based Collision Detection and Aloha-based Collision Correction (NDA-CDC) framework in VANET to reduce the delay time for collision detection and correction and improve security for vehicles on dynamic observations is introduced. We then showed how this framework can be extended to incorporate Collision Detection-based Neighbor Discovery model to improve the broadcast rate based on neighbor node by propagating with neighboring regions. The Collision Detection-based Neighbor Discovery model also provided efficient mapping of vehicles using warning message based on the location and hence improved the data packet transmission efficiency in VANET. This location information were arrived by determining the location using the routing table maintained by CA that in turn increases the broadcasting rate efficiency. Next, the introduced Neighbor Discovery algorithm reduces the data packet drop rate using local monitoring to improve the rate of security of nodes carrying data traffic in the network. This local monitoring and location information improves the security of vehicles. The results show that NDA-CDC framework offers better performance with an improvement of broadcast rate efficiency on data packets being traversed in VANET by 27.04% compared to the state of the art works.

6. References

1. Palanisamy B, Liu L. Attack-resilient mix-zones over road networks: Architecture and algorithms. IEEE Transactions on Mobile Computing. 2015 Mar; 14(3):495–508.
2. Wasef A, Shen X. EMAP: Expedite Message Authentication Protocol for vehicular ad hoc networks. IEEE Transactions on Mobile Computing. 2013 Jan; 12(1):78–89.
3. Rezvani M, Ignjatovic A, Bertino E, Jha S. Secure data aggregation technique for wirelesssensor networks in the presence of collusion attacks. IEEE Transactions on Dependable and Secure Computing. 2015 Apr; 12(1):98–110.
4. Zhang J, Xiang Y, Wang Y, Zhou W, Xiang Y, Guan Y. Network traffic classification using correlation information. IEEE Transactions on Parallel and Distributed Systems. 2013; 24(1):104–17.
5. Sommer C, Joerer S, Segata M, Tonguz OK, Cigno RL, Dressler F. How shadowing hurts vehicular communications and how dynamic beaconing can help. IEEE Proceedings INFOCOM; Turin. 2013. p. 110–4.
6. Berlin MA, Anand S. Direction based Hazard Routing Protocol (DHRP) for disseminating road hazard information using road side infrastructures in VANETs. Berlin and Springer Plus. 2014; 3:1–12.
7. Pattnaik O, Pattanayak BK. Security in vehicular ad hoc network based on intrusion detection system. American Journal of Applied Sciences. 2014; 11(4):37–46.
8. Joerer S, Segata M, Bloessl B, Cigno RL, Sommer C, Dressler F. A vehicular networking perspective on estimatingvehicle collision probability at intersections. IEEE Transactions on Vehicular Technology. 2014; 63(4):1802–12.
9. Schwartz RS, Ohazulikey AE, Sommerz C, Scholten H, Dresslerz F, Havinga P. On the applicability of fair and adaptive data dissemination in traffic information systems. Ad Hoc Networks. 2014; 13(Part B):428–43.
10. Khan U, Agrawal S, Silakari S. A detailed survey on misbehavior node detection techniques in vehicular ad hoc networks. Information Systems Design and Intellignet Applications, Springer. 2015; 339:11–9.
11. Sommer C, German R, Dressler F. Bidirectionally coupled network and road traffic simulation for improved IVC analysis. IEEE Transactions on Mobile Computing. 2011; 10(1):3–15.
12. Malandrino F, Casetti C, Chiasserini C-F, Sommer C, Dressler F. The role of parked cars in content downloading for vehicular networks. IEEE Transactions on Vehicular Technology. 2014; 63(9):4606–17.
13. Huang MW, Wu HT, Horng G-J, Hsieh W-S. Using BDH for the message authentication in VANET. Mathematical Problems in Engineering. 2014; 2014:13.
14. Bae IH. An intelligent broadcasting algorithm for early warning message dissemination in VANETs. Computational Science and its Application-ICCSA. Switzerland: Springer International Publishing; 2014. p. 668–81.
15. Jeon YB, Lee KH, Park DS, Jeong C-S. An efficient cluster authentication scheme based on vanet environment in m2m application. International Journal of Distributed Sensor Networks. 2013; 2013:9.
16. de Fuentes JM, Blasco J, Gonzalez-Tablas AI, Gonzalez-Manzano L. Applying information hiding in vanets to covertly report misbehaving vehicles. International Journal of Distributed Sensor Networks. 2014; 2014:15.
17. Bouk SH, Kim G, Ahmed SH, Kim D. Hybrid adaptive beaconing in vehicular ad hoc networks: a survey. International Journal of Distributed Sensor Networks. 2015; 2015:1–16.
18. Santhosh DD, Krishnaveni A. Effective collision detection using E-VeMAC in VANET. International Journal of Advanced Research in Computer Science and Software Engineering. 2014; 4(3):128–31.
19. Thakur N, Kumar P. A cooperative strategy for collision detection and prevention for unmanned ground

vehicles in military applications using WSN based VANET. International Journal of Computer Applications. 2014; 102(14):20–6.
20. Devdhara G, Gohil D, Akhade P, Vala M. Inter-vehicular collision detection and avoidance using ad-hoc network. International Journal for Research in Emerging Science and Technology. 2015; 2(2):1–7.
21. Robert E, Hemalatha. Epidemic dynamics of malicious code detection architecture in critical environment. Indian Journal of Science and Technology. 2014; 7(6):770–5.
22. Lakshmi, Banu W. Centralised enhanced forward error correction mechanism on the contention window to improve the transmission quality in vehicular ad hoc networks. Indian Journal of Science and Technology. 2015; 8(20):52680.
23. Ghavifekr MH, Khosrowshahi AC. Parking based data replication in VANET. Indian Journal of Science and Technology. 2015; 8(27):70054.
24. Suresh JS, Jongkun L. A TPM-based architecture to secure VANET. Indian Journal of Science and Technology. 2015; 8(15):IPL034.