[Downloaded from www.aece.ro on Friday, July 04, 2025 at 03:06:56 (UTC) by 108.162.241.188. Redistribution subject to AECE license or copyright.]

Emergency-Aware Irresponsible Message Forwarding for Vehicular Communications

Mohammad Jan HAIDARI, Zeki YETGIN, Abdullah ELEWI
Department of Computer Engineering, Mersin University, 33343, Mersin, Turkey
zyetgin@mersin.edu.tr

***Abstract*—Message forwarding schemes allow vehicles to exchange messages for various purposes such as safety, entertainment and traffic efficiency in vehicular ad hoc networks (VANETs). This paper addresses the problem of message dissemination under emergency situations in the context of vehicle-to-vehicle communication along the roads. The paper proposes a new forwarding scheme for both hazardous and normal traffic messages. The proposed scheme improves the irresponsible forwarding probability in case of both emergency and non-emergency situations. Furthermore, the scheme uses adaptive broadcast range rather than using static one and thus more appropriate for practical applications. In our work Veins-SUMO-OMNeT simulation platform has been used. The simulation results show that the proposed forwarding algorithm outperforms the other dissemination techniques in terms of message losses and data dissemination success for normal messages and emergency messages.**

***Index Terms*—ad-hoc networks, algorithm, emergency services, simulation, vehicles.**

I. Introduction

The vehicular ad-hoc network (VANET) is a kind of wireless ad hoc network that enables vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications to exchange messages for various applications. The main objective of VANET is to allow the vehicles and road side units (RSUs) to set up and maintain a wireless communication network. Message dissemination among vehicles is crucial for traffic safety using VANETs where vehicles can broadcast messages about traffic and road states to nearby vehicles and propagate them further using message dissemination techniques. These messages can include information related to accidents, broken vehicles, icy roads or any hazardous weather conditions that can affect traffic safety.

VANETs can divide the overall load of the network using infrastructure road side units. This enhances the network efficiency to some extent but programming the network intelligence still remains challenging [1]. For example, in order to inform vehicles about road conditions, the V2I communications can be exploited. However, keeping the network in consistent state, such as keeping road information correctly updated by message exchanging among vehicles and with RSUs seems difficult. Furthermore, current internet of things (IoT) technologies are merged with VANETs, which introduce the internet of vehicles (IoV) concept. The IoV seems to play an important role in developing the intelligent transport systems (ITSs) as an integral part of forthcoming smart cities. Thus, VANET applications need to be more intelligent by incorporating contemporary artificial intelligence technologies.

Since the implementation of such applications practically requires infrastructures and high expenses, simulators are utilized. Numerous VANETs simulators have been proposed. Generally, VANET simulators are developed from three categories: i) traffic simulators (e.g., SUMO [2] and STRAW [3]) ii) network simulators (e.g., ns3 [4] and OMNeT++ [5]), iii) hybrid platforms (e.g., Veins [6] and TraNS [7]. However, there is no universally accepted simulator for VANETs. Usually, available traffic simulators and network simulators are integrated into hybrid platforms.

Veins has an increasing popularity among integrated schemes. The Veins platform combines the popular SUMO traffic generator and the OMNeT++ network simulator together. Both OMNeT++ and SUMO are well-known simulators and they are commonly used in literature due to their efficiency in terms of stability, portability and mobility [8]. Thus, we used Veins-SUMO-OMNeT simulation platform for the implementation of our message dissemination technique in this paper.

Many data dissemination protocols and techniques have been developed for VANETs, such as flooding, probability-based, counter-based, and irresponsible techniques. In this paper, we proposed a new message dissemination algorithm namely emergency-aware irresponsible forwarding in VANETs. The proposed technique gives priority to messages according to the traffic pattern. It favors emergency messages over normal messages in case of emergency situations and disfavors repeated messages in both emergency and normal situations.

The rest of the paper is organized as follows: Next section explores related work. Third section presents basic messages forwarding techniques. Fourth section clarifies the proposed scheme. Fifth section provides performance analysis and comparisons of basic message dissemination schemes with our proposed algorithm. The last section draws a conclusion and presents future directions.

II. Related Work

Message dissemination in VANETs is an active area of research with many techniques for effective data dissemination. First, broadcasting techniques have appeared in [9] where flooding, counter-based, distance-based and probability-based forwarding schemes have been proposed for mobile ad-hoc networks (MANETs) originally. However, many clustering techniques and routing protocols have been adopted for VANETs also. In [10], a time barrier based emergency message dissemination technique has been proposed in VANETs. The technique aims to disseminate information about the road situation with minimum delay

Digital Object Identifier 10.4316/AECE.2020.04008

1582-7445 © 2020 AECE

[Downloaded from www.aece.ro on Friday, July 04, 2025 at 03:06:56 (UTC) by 108.162.241.188. Redistribution subject to AECE license or copyright.]

and reduce the network congestion. A novel emergency message dissemination scheme has been proposed in [11] to disseminate messages in high mobility situations with dynamic topologies. This scheme has used clustering technique to reduce the message loss and delay in the congestion situation to enhance the connection lifetime in vehicular networks. A scheme to enhance safety with a better management of road traffic has been presented in [12]. The proposed scheme can detect hazardous events and notify neighboring vehicles to reduce traffic jams.

The authors in [13] have proposed a black-burst and multi-channel based multi-hop broadcast (BMMB) protocol to disseminate emergency messages in VANETs. In this protocol, vehicles can transmit and sense black-burst at different channels simultaneously using multiple antennas. In [14], the authors have proposed a hybrid emergency message transmission (HEMT) to utilize the flexibility of inter-vehicle communication. For this goal, they have used SDN-enabled hybrid emergency message transmission architecture to support reliable and fast transmission of emergency messages in the context of internet of vehicles. The SDN (software-defined networking) is a structure designed for simplifying and improving network management with high flexibility by splitting control plane and data plane [15]. The authors in [16] have proposed a dynamic partitioning scheme (DPS) for emergency message dissemination in VANETs. The scheme is useful in terms of delay in both light and dense traffic scenarios.

In [17], the authors described a message forwarding scheme for emergency conditions in VANETs. They have used AODV (ad-hoc on-demand distance vector) and GPSR (greedy perimeter stateless routing) routing protocols to reduce the radio channel load by targeting specific nodes instead of flooding the network by broadcasts. The authors in [18] have proposed a ready-to-broadcast-emergency-message and clear-to-broadcast-emergency-message (RBEM/CBEM) handshake mechanism to improve one-hop broadcast reliability of emergency message dissemination in VANETs. In [19], an efficient broadcast protocol (EBP) has been proposed for warning message dissemination in VANETs. Their protocol focuses on enhancing the transmission time and number of transmissions to decrease communication overload and to achieve better results for safety-related data dissemination.

The authors in [20] have proposed an adaptive beacon-based data dissemination (ABDDis) scheme to disseminate the warning message with low overhead and high delivery ratio. This scheme has proposed a novel store-carry-forward (SCF) mechanism to overcome the network partition problem. In [21], the authors have proposed a beaconless multi-hop decentralized dissemination of warnings (DDW) mechanism for warning message dissemination in VANETs. In this mechanism, nodes are capable to generate early warnings about dangerous pollution levels, which are then packed inside the warning messages and forwarded toward the static monitoring units (SMU). However, there are many other studies [22], [23] related to VANETs in literature.

Most of the aforementioned techniques are proposed for general-purpose data dissemination and have no awareness about the type of the message whether an emergency message or a normal one. Emergency-aware approaches usually use complex clustering or network partitioning techniques for nodes in VANETs adding more complexity to their schemes. Thus, they are more theory-oriented rather than practical ones. For example, irresponsible forwarding based approaches use static radio coverage range. However, radio range is highly variable depending on the nature of the geographical objects where signal is refracted or reflected in complex way. Clustering-based approaches trust in cluster heads or leaders. Also, keeping clusters in consistent state and recovering the clusters when the leaders die imposes further practical considerations. Our proposed scheme is completely distributed, emergency-aware and practical. It has an asymmetric nature according to the message type whether emergency or non-emergency messages.

III. Message Dissemination in VANETs

Message dissemination is an important issue in VANETs. A lot of research has been conducted in this area and many dissemination techniques have been proposed. Basic forwarding techniques are presented here.

A. Flooding Algorithm

Flooding is a pure broadcast-based approach. According to flooding algorithm, when a vehicle receives a message for the first time, it broadcasts it immediately to all neighboring vehicles. Thus, same messages are retransmitted to many vehicles with the same ID around the same time. Clearly, this causes power consumption of n transmissions for a network of n vehicles. The main problem with such techniques is the excessive use of the bandwidth by repeating messages, causing a form of message storm.

B. Probability-Based Algorithm

One effective way to limit the extra broadcasts caused by traditional flooding technique is to consider randomized approach where upon receiving a message for the first time, the message is retransmitted with some probability P. Clearly, when $P = 1$, this approach becomes equal to the blind flooding [24]. In pure probabilistic scheme, each vehicle rebroadcast the message using a uniform probability. However, several probability-based techniques, including irresponsible forwarding, aim to find a suitable formulation for P. For example, one major class in formulating P is to consider the distance to the message originator, where the larger the distance, the larger the forwarding probality. Another major class is to consider the density around the receiving vehicle, where the higher the density, the lower the forwarding probability. For many other techniques, distance and density are considered with other considerations in formulating the forwarding probability.

C. Counter-Based Algorithm

When a vehicle attempts to retransmit a message, the message could be blocked due to back-off procedure caused by busy medium, or buffering in message queues. This increases the chance of having duplicated messages from other hosts before starting the message transmission. Counter approach advantageously uses the idle time, when hosts wait to transmit the next message in the queue, to count the number of message clones. When waiting time is over, the vehicle retransmits the message if the number of message clones is less than a threshold k or neglects it

[Downloaded from www.aece.ro on Friday, July 04, 2025 at 03:06:56 (UTC) by 108.162.241.188. Redistribution subject to AECE license or copyright.]

otherwise.

Much research takes into account the number of replicated massages with or without a thresholding approach. Counter based approach needs a delay to count messages. Thus, they seem to expose additional latency. However, from the practical consideration, it does not seem such a big problem since random waiting time between transmissions positively affects the bandwidth usage, and small latency can also be ignored in practice.

D. Distance-Based Algorithm

In this algorithm, the node calculates the distance to the message originator (transmitter not forwarder) when it receives the message. A global positioning system (GPS) is usually used to determine the position of a node. Let d denote the distance between the originator and the receiver. The receiving node forwards the message if d is greater than a threshold d_{min} and discards it otherwise. Also, many researchers consider the distance to the originator in their approach without using a thresholding approach such as irresponsible forwarding scheme. Thus, distance-based approaches are one of the major classes and are usually used in hybrid forwarding schemes, with other metrics also.

E. Irresponsible Forwarding Algorithm

Irresponsible forwarding [25] is a hybrid scheme of probabilistic and distance-based rebroadcast schemes. This approach computes the forwarding probability by considering both the density around the receiving vehicles and the distance to the originator. According to irresponsible forwarding approach: i) The spacing between the vehicles follows exponential distribution where ρ_s represents the spatial density (rate) of vehicles. ii) Vehicles have fixed coverage range, denoted by z. iii) Vehicles have GPS sensors to compute their own positions at any time.

In this approach, each vehicle calculates the forwarding probability by considering the likelihood of finding another vehicle in the remaining coverage to rebroadcast the message. Upon receiving a message, vehicles compute the forwarding probability as follows:

$$p = e^{-\rho_s (z-d)/c} \tag{1}$$

where, d is the distance between the vehicle and the message originator and $c \geq 1$ is a coefficient to shape the likelihood of forwarding in the forward segment where the higher the c value is, the higher the likelihood of forwarding is for any position d. A particular case is when $c = 1$ where the situation becomes equivalent to the one with no vehicle in the forward segment within the interval ($z - d$).

IV. Proposed Forwarding Algorithm

The proposed Emergency-aware Irresponsible Forwarding (EIF) is a probabilistic scheme incorporating the behavior of irresponsible forwarding. It is also an asymmetric model that behaves differently depending on the type of messages whether emergency or not. Three types of messages, namely *emergency*, *data* and *beacon*, are considered. The forwarding probability of the proposed approach is formulated as follows:

$$p = \begin{cases} (1+EP)e^{-\frac{n_1}{R}(R-d)/C} & in\ case\ of\ emergency \\ (1-EP)e^{-\frac{n_2}{R}(R-d)/C} & otherwise \end{cases} \tag{2}$$

where, EP is the emergency probability, which is the ratio of emergency messages over total messages in the current period, n_1 is the number of neighboring vehicles in the current period, n_2 is the number of replicas of the current message, R is the adaptive radio coverage range in meter, d is the distance to the originator node in meter and C is an adjusting parameter.

The algorithm has two main parameters *period* and C. Although the initial value of R, denoted as R_0, is given and fixed (200 meter in our simulation), R is dynamically adjusted by the algorithm. The parameter *period* is the time interval during which the node can observe the recent emergency state to compute the forwarding probability p. The proposed forwarding algorithm is given as a detailed flowchart in Fig. 1.

Letting *MQueue* denotes the multi queue of all received messages such that *MQueue[mid]* denotes the queue of all replicas of the same message with the message ID *mid*, receiving time *time* and message type *type* as some attributes. The number of messages of given type t, denoted as N_t, in the current period is formulated in (3), where union operator selects the matched records in queue, while the EP formula is given in (4).

$$N_t = \left| \bigcup_{for\ each\ mid} \left(\bigcup_{time \geq (now - period) \wedge type = t} MQueue[mid] \right) \right| \tag{3}$$

$$EP = \frac{N_{emergency}}{N_{emergency} + N_{data}} \tag{4}$$

Letting *NQueue* denotes a neighbor table keeping track of all vehicle IDs of the neighbors in current *period*, taken from the received messages, such that *NQueue[vid]* shows the time stamp of the last message belonging to the vehicle ID *vid*. The queue is dynamically updated such that the records that are too old, out of the *period*, are dropped or otherwise updated with the new time stamps. Then, n_1 and n_2 are formulated in (5) and (6) respectively where *mid* is the ID of the received message.

$$n_1 = |NQueue| \tag{5}$$

$$n_2 = |MQueue[mid]| \tag{6}$$

The radio coverage R is dynamically updated, rather than fixed as considered in irresponsible forwarding scheme while the vehicle moves. As shown in Fig. 1, when the vehicle changes its road, R is replaced with the default R_0 (initial R value) due to the fact that the vehicle has no information related to the distance to its neighbors on this road.

As the vehicle moves, it can find the furthest neighbor (neighbor in the current broadcast domain) by analyzing the distance to the sender, denoted d_{sender}, when any message is received from the vehicle neighbors. The update of R is defined in (7).

$$R = \begin{cases} R_0 & if\ road\ just\ changed \\ \max(R,\ d_{sender}) & otherwise \end{cases} \tag{7}$$

[Downloaded from www.aece.ro on Friday, July 04, 2025 at 03:06:56 (UTC) by 108.162.241.188. Redistribution subject to AECE license or copyright.]

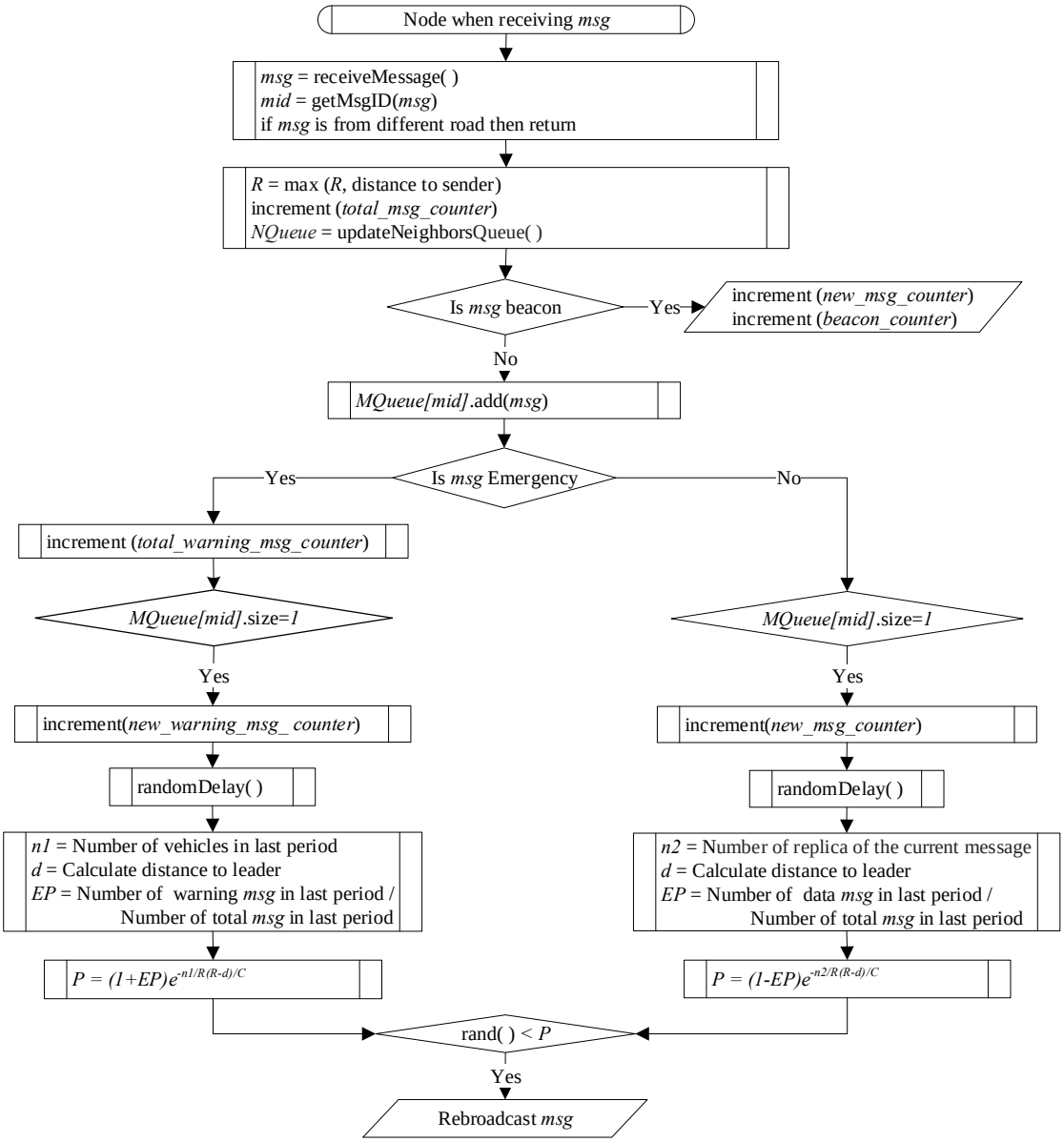

Figure 1. Proposed emergency-aware irresponsible forwarding

From the implementation point of view, the update $R = R_0$ is done when the vehicle moves and changes road. The other update can easily be handled with R = max (R, d_{sender}) for every received message of any type. Thus, the proposed algorithm has functional components in Fig. 1 and Fig. 2, where Fig. 1 handles receiving message and Fig. 2 handles the update of R when the road is changed.

A. Data Traffic Scenario

In this scenario, vehicles generate three types of messages, beacon, data and emergency. The flow of message traffic is generated as shown in Fig. 2, where only the update to R is the part of our proposed forwarding scheme and the rest is related to the simulation of message traffic flow. We assume that beacon messages are sent per second and vehicle average speed is computed between consecutive beacon times. In order to generate realistic emergency or warning messages, we used the critical distance, which is the displacement between the node's breaking and stopping positions. The critical distance is dependent on the node velocity and its deceleration coefficient. Deceleration value is dependent on the brake mechanism and is considered constant for each type of vehicle. If the gap between the node and its leader is less than the critical distance of the former, the likelihood of the crash is further increased when the leader slows down or the node accelerates. Every vehicle generates data message randomly, possibly after sending beacon or emergency message. As shown in Fig. 2, the network is made highly overloaded with data messages in order to evaluate the warning message dissemination under heavy data traffic.

V. Results and Discussion

A. Simulation Setup

Simulations are performed using Veins platform, which integrates the network simulator OMNeT++ with the mobility model SUMO. Veins controls both the OMNeT++ and SUMO using TCP connection as a standard for the traffic control interface (TraCI). Using TraCI protocol, vehicle movements in SUMO application are reflected as node movements in an OMNeT++ application. The mobility model of our simulation is based on random trips with high vehicle traffic on main roads of Mezitli map in Mersin, Turkey, extracted from OpenStreetMap (OSM), Fig. 3.

[Downloaded from www.aece.ro on Friday, July 04, 2025 at 03:06:56 (UTC) by 108.162.241.188. Redistribution subject to AECE license or copyright.]

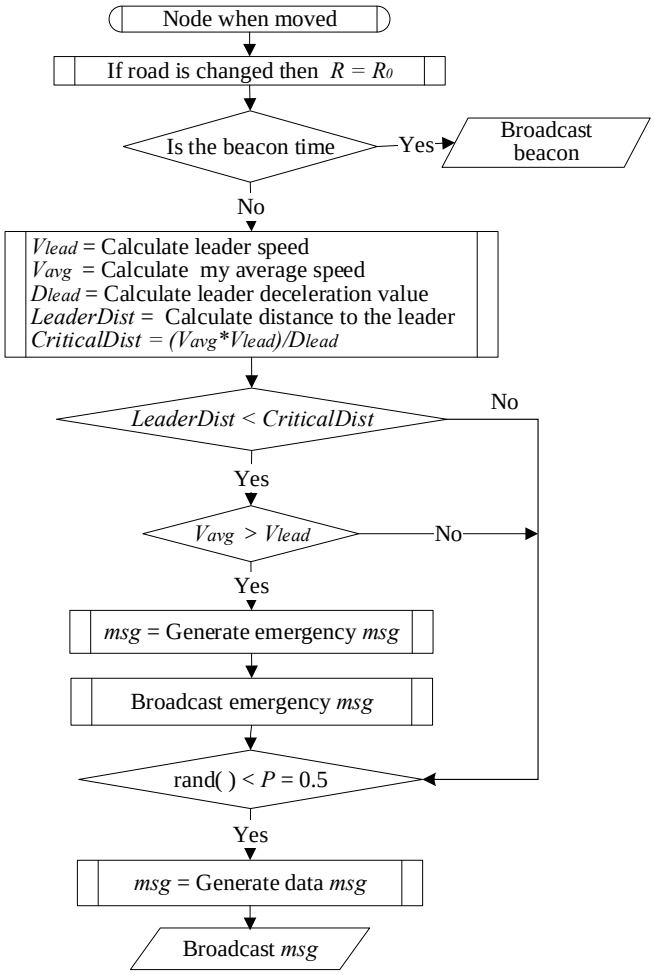

Figure 2. Data traffic scenario used in simulation

Table I shows the parameters used in this simulation such as simulation area, simulation times and etc.

B. Simulation Results

We analyzed the performance of five forwarding algorithms separately and compared their best results. Table II shows the performance metrics used to evaluate the performance of the dissemination algorithms. The *new warning* and *new message* metrics show the actual performances achieved to disseminate *warning messages* and *data messages* respectively since the *all warning* and *all message* metrics also count the replicas.

Figure 3. Map used in the simulation, part of Mezitli, Mersin, Turkey

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Simulation area	13 * 13 km
MAC	IEEE 802.11p WAVE
Look ahead	200 m
Message size	166 bytes
Simulation times	35s
Accident start	17s
Accident duration	18s
Maximum speed	55.5 m/s
Maximum acceleration	2.6 m/s^2
Maximum deceleration	4.5 m/s^2
Minimum Vehicle gap	2.5 m
Road side unit (RSU)	No
Dedicated beacon channel	False
Vehicle generation period	0.5 s
Vehicle routes	Random trips
Transmission data rate	18Mbps
Transmission power	20mW

However, replication contributes more in tolerating the message losses and security. Also, the *total loss* metric gives important information about network conditions of the channel where a single channel is used for all messages.

TABLE II. PERFORMANCE METRICS

Metric	Explanation
all message	Total number of received messages, including beacons and replicas
new message	Number of unduplicated received messages
all warning	Total number of received warning messages, including replicas
new warning	Number of unduplicated received warning messages
total loss	The number of all lost messages including beacons and others.

1) Flooding Algorithm

Fig. 4 shows the simulation results of this scheme. In this scheme, since all received messages are rebroadcasted, the network is congested with many replicas. Thus, the total number of lost messages, including beacons and other types, seems high. The beacon channel and data channel are assumed to be united in the simulation. This in turn further increases the channel congestion. Also, since the flooding is not aware of the warning messages, it seems very poor to disseminate the warning messages. The majority of warning messages seem to be lost due to heavy data traffic. Furthermore, all replicas of the received warning messages also seem lost. The total loss is higher than the total message since the losses are packets that are not received whereas the other metrics deal with the received packets.

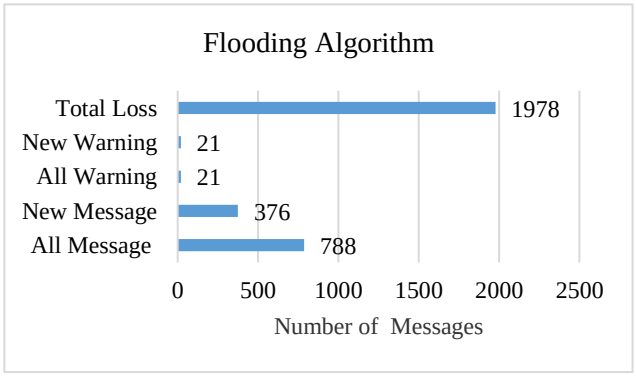

Figure 4. Results of flooding algorithm

[Downloaded from www.aece.ro on Friday, July 04, 2025 at 03:06:56 (UTC) by 108.162.241.188. Redistribution subject to AECE license or copyright.]

2) Probability Algorithm

In this scheme, a node receiving a message for the first time will rebroadcast it with probability *p*. In this simulation, various *p* values are tested but only *p = 0.4* is used for demonstration purposes. The results of probability algorithm are shown in Fig. 5. Similar to the flooding algorithm, the majority of warning messages and all their replicas are lost due to heavy data traffic. When *p=1* the scheme becomes exactly equal to flooding. When *p* is reduced, the performance is also reduced since only selected nodes become forwarders, unlike flooding.

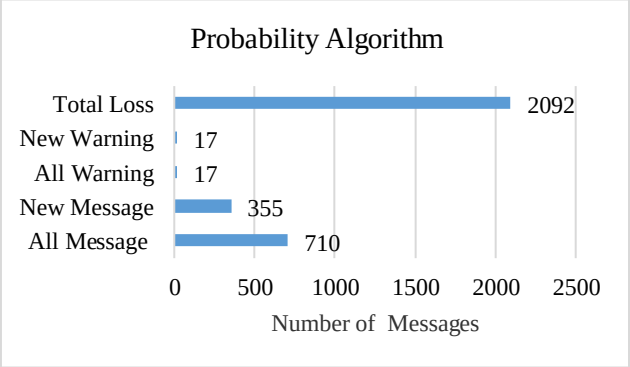

Figure 5. Results of probability algorithm

3) Counter Algorithm

In this scheme, each node initiates a counter *c* that will record the number of times the same message received, after that each node increments its *c* by one each time it receives the same message and compares its *c* with a predefined counter threshold *C*. If *c* < *C*, the node rebroadcasts the message. In this simulation, the threshold *C* takes four values *2, 3, 4* and *5*, respectively. Fig. 6 shows the best results of this scheme in this simulation.

The counter algorithm seems effective in dissemination of different messages since it doesn't attempt to forward the highly repeated message. This will also reduce the *total loss*. However, increasing the counter threshold doesn't surely increase the performance. Small and high threshold values seem not effective and a tradeoff among metrics arises. For example, when *C=3* the dissemination of different messages seems to be the best with the cost of worst dissemination of different warning messages. Talking in general, the counter-based approach contributes more to the total loss due to fact that replications are elaborately disfavored

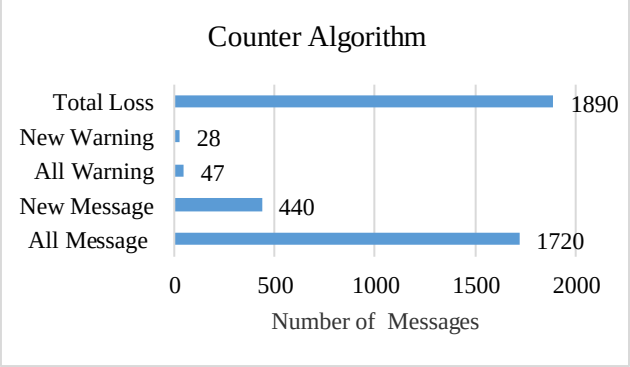

Figure 6. Results of counter algorithm

Irresponsible Forwarding

In this method, forwarding probability depends on the distance to the originator, vehicle density per m^2 in the region from the node towards to its coverage range, and the coefficient *C*. We tested various *C = 1-13* values and Fig. 7 shows the best results of them.

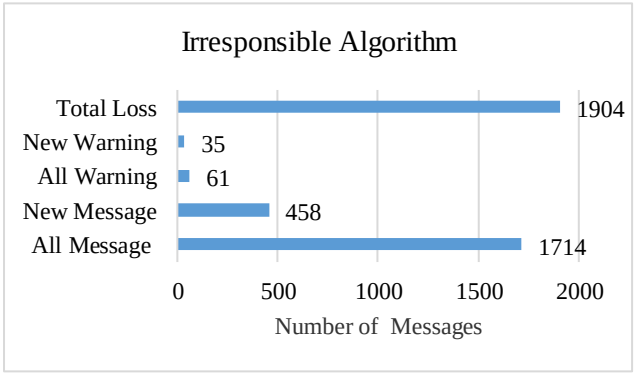

Figure 7. Results of irresponsible forwarding algorithm

Since irresponsible forwarding considers the likelihood of finding any forwarder in further distance, it effectively increases the message dissemination performance. From the results, one can generalize that increasing the C value to some extent positively affects all the metrics such as total losses and data dissemination performances. However, increasing the *C* value further will decrease the performance. According to Fig. 7, considering the total loss and dissemination performance together, the best results are acquired at *C=13*.

4) Proposed Algorithm

The proposed forwarding algorithm is a parametric model dependent on the coefficient *C* inherited from irresponsible forwarding and it behaves differently according to the message type. As shown in Table III, the results highly differ depending on the coefficient *C* value, changing from *1* up to *13*. It seems difficult to establish a relation between the coefficient *C* and the performance of any metric. One possible explanation is that the proposed approach adds additional factors to irresponsible forwarding, such as emergency probability, period, and both message and traffic densities around the node. Also, it behaves differently depending on the message type. Fig. 8 shows the best performance achieved by the proposed algorithm on the basis of each metric.

Considering message dissemination performance and total loss together, best results with the proposed approach seems to occur at *C=1*. Although, better results for warning message dissemination has been achieved at *C=13* and total loss at *C=8*, their score seems close to the one at *C=1*.

TABLE III. SIMULATION RESULTS OF PROPOSED ALGORITHM

	all message	**new message**	**all warning**	**new warning**	**total loss**
C= 1	1249	461	49	42	1853
C= 2	1212	389	35	27	1993
C= 3	1421	420	34	27	2050
C= 4	1529	412	23	18	1872
C= 5	1407	401	49	33	2065
C= 6	1472	423	59	30	2072
C= 7	1500	423	39	26	2040
C= 8	1643	440	45	25	1841
C= 9	1553	414	29	22	1987
C=10	1574	429	21	17	1938
C=11	1554	413	26	17	2049
C=12	1652	440	13	12	2015
C=13	1406	394	96	44	1970

[Downloaded from www.aece.ro on Friday, July 04, 2025 at 03:06:56 (UTC) by 108.162.241.188. Redistribution subject to AECE license or copyright.]

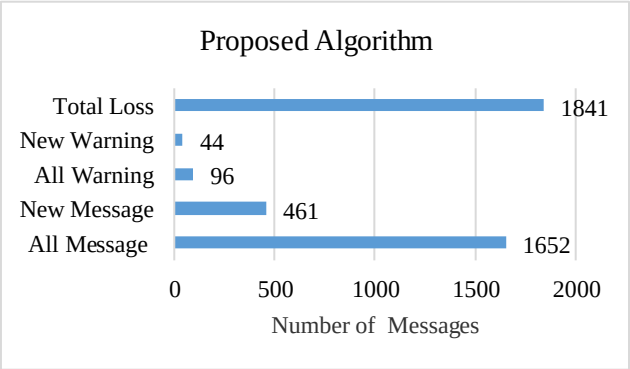

Figure 8. Results of proposed algorithm

5) Comparison of All Algorithms

The dissemination performance of *new warning* messages is important in emergency situations. Fig. 9 shows the result of dissemination performance of *new warning* messages. The results show that the proposed scheme is the best in rebroadcasting the warning messages with minimal replicas. The worst performance occurs with probability and flooding algorithms as expected.

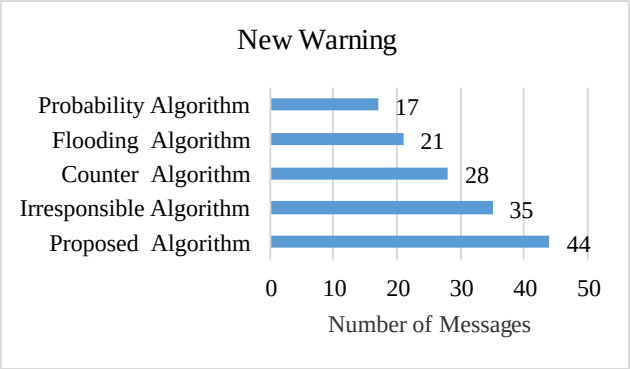

Figure 9. Results of new warning metric in all algorithms

The second metric used in this experiment is the *new message* metric, which shows the ability of the forwarding scheme to disseminate a message of any type with no duplication. According to Fig. 10, the proposed scheme also disseminates higher number of different messages than the other schemes. As the figure shows, the order of schemes in disseminating the *new messages* is the same as the one for the *new warning*.

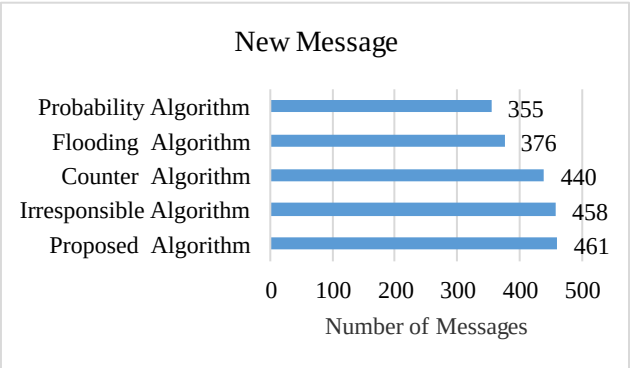

Figure 10. Results of new message metric in all algorithms

The other important metric used in the experiment is the *total loss* metric, which shows the ability of the forwarding scheme in using the bandwidth efficiently. Our proposed scheme has lowest loss values than other schemes. One can notice that the order of schemes with respect to the total loss is the same as the dissemination performances, shown in Fig. 11. Thus, the dissemination performances and *total loss* could be correlated.

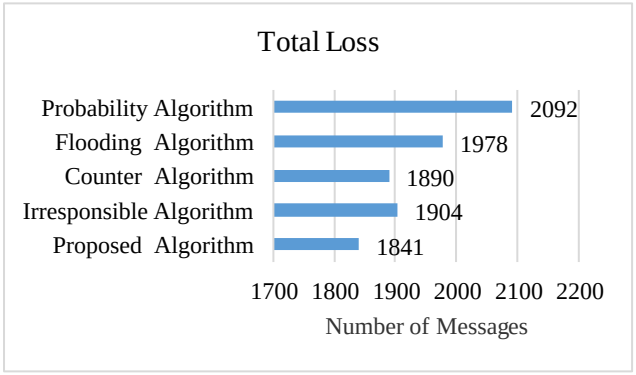

Figure 11. Results of total loss metric in all algorithms

The other metrics, *all warnings* and *all messages* show the ability of the forwarding algorithms to disseminate the total warning messages and the total messages, without caring whether the message is a new one or a replica. These metrics contribute very little to message dissemination performance in that receiving many replicas of the same message for one vehicle has no much impact on performance. However, replicas can sometimes be used to increase reliability when messages are lost due to channel conditions. But, sending many replicas could sometimes be the sole cause of losses.

Thus, there seems a tradeoff between *all messages* and *new messages* metrics, and having higher values for *all messages* metric does not mean to disseminate all messages better. The low values of *all messages* and *all warning* metrics are more indicative for dissemination performance. Low values of these metric mean bad performance in disseminating the message indicated by the metric. Therefore, a good dissemination approach should achieve at least an average value for these metrics but not low.

According to Fig. 12 and Fig. 13, the proposed scheme disseminates above the average number of total warning messages and total messages. The order of the forwarding schemes according to the performance of these metrics is the same as the others.

The results altogether show that the proposed forwarding scheme achieves better than the other schemes from the five metrics point of view. However, a further study is required to investigate the proposed dissemination scheme from other metrics point of view, such as latency.

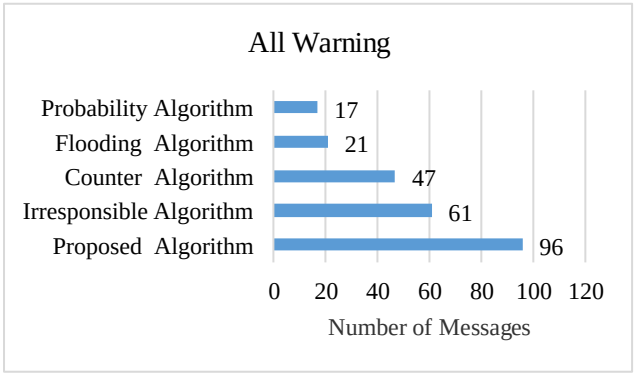

Figure 12. Results of all warning metric in all algorithms

[Downloaded from www.aece.ro on Friday, July 04, 2025 at 03:06:56 (UTC) by 108.162.241.188. Redistribution subject to AECE license or copyright.]

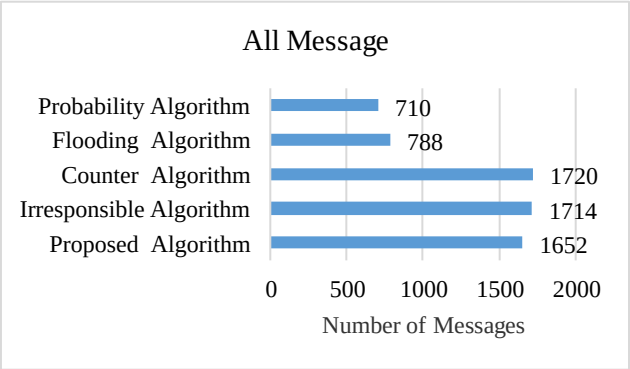

Figure 13. Results of all message metric in all algorithms

Finally, the performance still needs to be improved more under large scale test scenarios. Furthermore, comparisons of the proposed approach with more state-of-the-art data dissemination techniques are needed and thus motivated as future work for researchers.

VI. Conclusion

In this paper, a new message forwarding algorithm was proposed for VANETs. The proposed forwarding scheme forwards the incoming message based on its emergency state, which is monitored. Thus, the scheme behaves differently according to the emergency degree of the incoming message. The proposed algorithm also provides a practical scheme by the dynamic adaptation of the radio coverage range. This allows the algorithm to be applied to vehicle traffic in urban streets and/or high ways, using a traffic scenario, in which warning messages are generated in a realistic way. The proposed scheme was tested across five performance metrics, and comparisons of five forwarding techniques were given.

The results showed that the proposed forwarding scheme disseminates messages more efficiently, particularly emergency messages. It achieved emergency message dissemination at least 26% better than the other dissemination techniques. Moreover, it achieved better with respect to the other utilized performance metrics, such as total loss. However, in future work, comparisons could be extended to cover recent forwarding algorithms such as cluster-based ones. Also, more performance metrics, such as latency, could be investigated.

References

[1] S. Latif et al., “Industrial internet of things based efficient and reliable data dissemination solution for vehicular ad hoc networks,” Wireless Communications and Mobile Computing, pp. 1-16, 2018, doi:10.1155/2018/1857202

[2] D. Krajzewicz, “Traffic simulation with SUMO – simulation of urban mobility,” in Fundamentals of Traffic Simulation, Springer, New York, pp. 269–293, 2010, doi:10.1007/978-1-4419-6142-6_7

[3] Y. Tao, L. Kong, Y. Wang, H. Jian-Bin, and C. Zhong, “PKU-STRAW-L: A simulative platform evaluate the power-saving rate of the intelligent street lamp system,” in 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing, Sep. 2012, pp. 525–532, doi:10.1109/UIC-ATC.2012.116

[4] W. Liu, X. Wang, W. Zhang, L. Yang, and C. Peng, “Coordinative simulation with SUMO and NS3 for vehicular ad hoc networks,” in 22nd Asia-Pacific Conference on Communications (APCC), Aug. 2016, pp. 337–341, doi:10.1109/APCC.2016.7581471

[5] Xiaodong Xian, Weiren Shi, and He Huang, “Comparison of OMNET++ and other simulator for WSN simulation,” in 3rd IEEE Conference on Industrial Electronics and Applications, Jun. 2008, pp. 1439–1443, doi:10.1109/ICIEA.2008.4582757

[6] R. Riebl, H.-J. Günther, C. Facchi, and L. Wolf, “Artery: Extending Veins for VANET applications,” in 2015 International Conference on Models and Technologies for Intelligent Transportation Systems, Jun.2015, pp.450–456, doi:10.1109/MTITS.2015.7223293

[7] M. Piórkowski et al., “TraNS: realistic joint traffic and network simulator for VANETs,” ACM SIGMOBILE Mobile Computing and Communications Review, vol. 12 no. 1, pp. 1–4, 2008, doi:10.1145/1374512.1374522

[8] M. J. Haidari and Z. Yetgin, “Veins based studies for vehicular ad hoc networks,” in 2019 International Conference on Artificial Intelligence and Data Processing Symposium, Sep. 2019, pp. 1–7, doi:10.1109/IDAP.2019.8875954

[9] Y. Tseng, S. Ni, Y. Chen, and J. Sheu, “The broadcast storm problem in a mobile ad hoc network,” Wireless Networks, vol. 8, pp. 153–167, 2002, doi:10.1023/A:1013763825347

[10] S. S. Shah, A. W. Malik, A. U. Rahman, S. Iqbal, and S. U. Khan, “Time barrier-based emergency message dissemination in vehicular ad-hoc networks,” IEEE Access, vol. 7, pp. 16494–16503, 2019, doi:10.1109/ACCESS.2019.2895114

[11] M. Ali, A. W. Malik, and A. U. Rahman, “Position-based emergency message dissemination for Internet of vehicles,” International Journal of Distributed Sensor Networks, vol. 15, no. 7, pp. 1–12, 2019, doi:10.1177/1550147719861585

[12] A. F. Santamaria, “Managing emergency situations in VANET through heterogeneous technologies cooperation,” Sensors, vol. 18 no. 5, pp. 1–24, 2018, doi:10.3390/s18051461

[13] W. U. Libing, N. I. E. Lei, F. A. N. Jing, H. E. Yanxiang, L. I. U. Qin, and W. U. Dan, “An efficient multi-hop broadcast protocol for emergency messages dissemination in VANETs,” Chinese Journal of Electronics, vol. 26, no. 3, pp. 614–623, 2017, doi:10.1049/cje.2017.03.001

[14] W. Zhu, D. Gao, W. Zhao, H. Zhang, and H. Chiang, “SDN-enabled hybrid emergency message transmission architecture in internet-of-vehicles,” Enterprise Information Systems, vol. 12, no. 4, pp. 1–21, 2017, doi:10.1080/17517575.2017.1304578

[15] R. Masoudi and A. Ghaffari, “Software defined networks: A survey,” Journal of Network and Computer Applications, vol. 67, pp. 1–25, 2016, doi:10.1016/j.jnca.2016.03.016

[16] M. S. Rayeni, A. Hafid, and P. K. Sahu, “Dynamic spatial partition density-based emergency message dissemination in VANETs,” Vehicular Communications, vol. 2, no. 4, pp. 208–222, 2015, doi:10.1016/j.vehcom.2015.07.002

[17] T. Petrov, P. Kortis, and T. Kovacikova, “Evaluation of packet forwarding approaches for emergency vehicle warning application in VANETs,” in 2018 ELEKTRO, 2018, pp. 1–5, doi:10.1109/ELEKTRO.2018.8398258

[18] W. Zhu, D. Gao, C. H. Foh, W. Zhao, and H. Zhang, “A collision avoidance mechanism for emergency message broadcast in urban VANET,” in IEEE 83rd Vehicular Technology Conference, 2016, pp. 1–5, doi:10.1109/VTCSpring.2016.7504057.

[19] O. Mahma, A. Korichi, and A. Bourouis, “EBP: An efficient broadcast protocol for warning message dissemination in VANETs,” Journal of Computing and Information Technology, vol. 26, no. 3, pp. 157–166, 2018, doi:10.20532/cit.2018.1004247

[20] T. D. T. Nguyen, Q. Huynh, and H. Pham, “An adaptive beacon-based scheme for warning messages dissemination in vehicular ad-hoc networks,” in 2017 Int. Conf. Adv. Comput. Appl. ACOMP, 2017, pp. 47–53, doi:10.1109/ACOMP.2017.19

[21] M. Milojevic and J. A. Barria, “Early warnings dissemination for urban micro-scale monitoring using vehicular sensor network,” in 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), 2017 pp. 244–249, doi:10.1109/MTITS.2017.8005674

[22] J. Alves Junior, E. C. G. Wille, "Exploiting the inherent connectivity of urban mobile backbones using the P-DSDV routing protocol," Advances in Electrical and Computer Engineering, vol.20, no.1, pp.83-90, 2020, doi:10.4316/AECE.2020.01011

[23] S. M. M. Langari, S. Yousefi, S. Jabbehdari, "Fountain-code Aided File Transfer in Vehicular Delay Tolerant Networks," Advances in Electrical and Computer Engineering, vol.13, no.4, pp.117-124, 2013, doi:10.4316/AECE.2013.04020

[24] A. T. Giang, A. Busson and V. Vèque, “Message dissemination in VANET: protocols and performances,” in Wireless Vehicular Networks for Car Collision Avoidance, Springer, New York, pp. 71–96, 2013, doi:10.1007/978-1-4419-9563-6_3

[25] S. Panichpapiboon and G. Ferrari, “Irresponsible forwarding,” in 8th International Conference on ITS Telecommunications, Thailand, November 2008, pp. 1–6, doi:10.1109/ITST.2008.4740277