

Optimal Threshold Analysis for Triggering Fail-Safe Mechanism in Vehicular Ad Hoc Networks

Kumar Sharshembiev*, Seong-Moo Yoo*, Yong-Kab Kim**, Geun-Ho Jeong**

*Electrical and Computer Engineering Department, The University of Alabama in Huntsville, USA

**School of Electrical Information Communication Engineering, Wonkwang University, Korea

kbs0010@uah.edu, yoos@uah.edu, ykim@wku.ac.kr, rootbig@nate.com

Abstract— A novel approach is proposed to estimate the optimal threshold of broadcast messages in vehicular ad hoc networks in order to detect misbehaving nodes and prevent broadcast storms. This threshold value is estimated based on the number of incoming and outgoing data statistics and metrics to be used to judge if the node is behaving properly. To avoid misjudgement and false alarms, the accuracy of the estimate of the threshold value is very important. Our method and detection technique are based on the IEEE 802.11p MAC protocol and weighted p -persistence routing protocol. The main contribution of this paper is proposing an analytical model to accurately estimate the optimal threshold value to trigger the fail-safe mechanism for misbehaving cars. Computer simulation results using Veins simulator show that analytical models work properly.

Keywords— Vehicular ad hoc networks, misbehaving node, IEEE 802.11p, probabilistic routing protocols, threshold value.

I. INTRODUCTION

One of the main issues in vehicular ad hoc networks (VANETs) today is the problem of broadcast storms. In order to efficiently disseminate safety messages across all vehicles, most of the routing protocols are categorized into probability-based and timer-based. These protocols in both categories allow the concept of intelligent flooding, where the broadcast is distributed in a systematic way as opposed to general flooding.

In probability-based routing each vehicle makes a decision to rebroadcast based on some fixed or dynamic probability value. The value could be calculated based on the distance, as in the case of the weighted p -persistence implementation, or some other parameter such as the signal strength. To achieve maximum packet penetration rate, the simplest case would flood the network, but that could lead to a minimum of 60% packet loss ratio [1], which is unacceptable for safety applications. Weighted p -persistence algorithm is one of the main techniques in probabilistic rebroadcasting. Here, the core idea is to calculate the probability-based on the distance between the communicating nodes while applying certain fixed delays. The timer-based techniques are based on the slotted time and continuous time. Wisitpongphan et al. [1] proposed slotted techniques called slotted 1-persistence and p -persistence techniques, where each vehicle rebroadcasts with probability 1 or p based on the assigned time slot. The

continuous timer version works by not rebroadcasting the frame immediately, but waiting for a certain time before the decision of rebroadcasting.

The efficient emergency information dissemination is the focus of our research. To achieve maximum reach of all neighbours, many VANET broadcasting protocols today employ the concept of intelligent flooding. Under the intelligent flooding, affected vehicles broadcast the emergency message out to all of its neighbours, but those neighbours will perform a probabilistic rebroadcast instead of 1-persistent rebroadcast as in the case of basic flooding. Our model and simulation results provide a number of insights into the detection of misbehaviour under probabilistic broadcasting protocols in VANETs.

Our results show that accurate and timely detection of misbehaviour during emergency broadcasts significantly decreases chances of broadcasting storms, and helps keeping the delay and drop rates tolerable. Upon misbehaviour detection, our algorithm will cause the misbehaving node to go into a fail-safe mode, and allow other vehicles to continue operating under the broadcast routing protocol. We use the simulation and analytical model results to validate and do a performance evaluation of our fail-safe misbehaviour detection technique.

The rest of this paper is organized as follows. In the next section the related work is introduced. Section III presents the analytical model based on the two queues, fail-safe detection technique, and performance evaluation parameters. Simulation details and paper results are shown in Section IV. Conclusion and is given in Section V.

II. RELATED WORK

Here we discuss previous methods that have been implemented to determine the mean waiting, response time and the packet loss for ad hoc networks. Qiu, et al [2] presented an analytical model using a Markov chain to compute functions of packets such as the packet transmission probability, broadcasting efficiency, and the throughput performances of the IEEE 802.11p protocol. Ma and Chen [4-5] developed an analytical model for evaluating the performance of vehicle-to-vehicle safety related services in dedicated short range communication (DSRC) system on a highway. Their model is based on the functionality of

802.11a-based channel to simulate the harsh DSRC highway scenarios. Eckhoff and Sommer [3] extended the well-established Veins framework to include a multi-channel simulation model for the IEEE 1609.4/802.11p, allowing the simulator to realistically provide the distinctive properties of the envisioned radio technology.

Another analytical model was presented by Hafeez et al. [6-7] which took into account the impact of mobility on the density of vehicles around the transmitter, the impact of the transmitter's and receiver's speeds on the system reliability, the impact of channel fading by modeling the communication range as a random variable, the hidden terminal problem and transmission collisions from neighboring vehicles. Li et al. [8] proposed a 2-dimensional (2-D) Markov chain queuing model with finite buffer under finite load to characterize the IEEE 802.11p broadcast scheme for VANETs. Their analyses revealed that the lack of binary exponential back-off and retransmission in the 802.11p system results in poor QoS performance during heavy traffic load, particularly for large VANETs.

Zheng, Wu [9] studied the performance modeling of the IEEE 802.11p enhanced distributed channel access (EDCA) mechanism and develops performance models to analyze the access performance of the IEEE 802.11p EDCA mechanism. They constructed a 2-D Markov chain to model the back-off procedure of an access category (AC) queue and establish a relationship between the transmission probability and collision probability of the AC queue.

Our proposed model is used to estimate the optimal threshold values to detect misbehaviour during the probabilistic emergency broadcast. The model is built on top of the Veins simulator environment with stochastic traffic model and Markov chain to represent the MAC layer contention mechanism. This is closer to reality when environmental noise is not considered.

III. ANALYTICAL MODEL AND PERFORMANCE PARAMETERS

We assume that the emergency packet generation occur at rate λ_e according to a Poisson process and the service times have a general distribution. Our assumption is that each vehicle either generates its own emergency packet according to the aforementioned rate or will receive the emergency packet from a neighbour for the purpose of rebroadcasting. This means, each vehicle will have to operate two separate queues: one for the self-generated emergency packets and the other for incoming neighbour broadcast packets. There are no buffer or population size limitations and the service discipline is first come, first served (FCFS). 802.11p adopts the enhanced distributed channel access (EDCA) from 802.11e [3], which utilizes four access classes (ACs) to schedule arrived packets. Packets from different ACs within a node contend internally, and only the winner will participate in external contention.

A. System Model

In this study, IEEE 802.11p and weighted p -persistence with fail-safe are used as the MAC and routing protocols,

respectively. The contention parameters (e.g., the contention window size and arbitrary inter-frame space (AIFS) shown in Table I are configured so that highly important messages (such as safety broadcast) falling in AC3 are most likely to win the internal contention as shown in Figure 1.

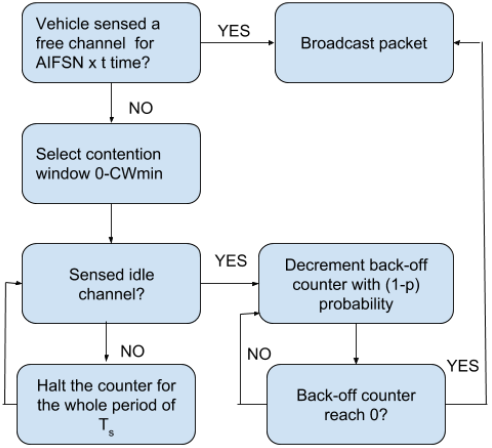


Figure 1. 802.11p back-off process/contention window logic.

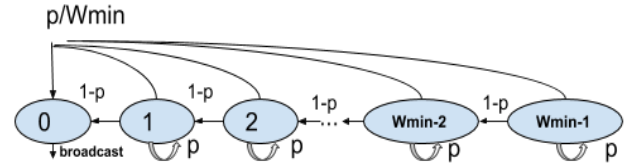


Figure 2. Emergency packet back-off process Markov chain.

Due to the nature of broadcasts in VANETs, there is no acknowledge process for the emergency broadcast packets in our case. Nodes are distributed randomly in a mixed urban/suburban area with a stochastic traffic model. Our assumption that all vehicles in an area R have the same sensing range $l_{cs} = [R, 2R]$. We assume that the queue for the self-generated emergency packets is an M/G/1 queue with λ_e rate of generation. When the emergency packet comes from a neighbour, it has a probability p (weighted p -persistence) of being rebroadcasting by the receiving vehicle. We assume this as a G/G/1 queue with average inter-arrival and service times. Following sub-sections provide more details to derive our two main metrics to do a performance evaluation of the fail-safe extension to the rebroadcasting protocol.

B. MAC Protocol

IEEE 802.11p is an approved enhancement to the 802.11 standard to add wireless access in vehicular environments (WAVE). It supports data exchanges between highly mobile vehicles and the road side infrastructure. The standard is licensed ITS band of 5.9 GHz. IEEE 1609 is a higher layer standard based on the IEEE 802.11p. MAC and physical layer specifications of 802.11p are the part of a whole protocol stack IEEE 1609 WAVE family of standards. The MAC layer of 802.11p has the distributed coordination function (DCF) from 802.11.

When considering a model for the back-off counter process, we are mainly concerned about the safety channel or AC3 and two queues (M/G/1 and G/G/1). If the broadcast channel is free for a period of $AIFSN \cdot \delta$, where AIFSN is the AIFS-number associated with the AC3 and δ is the length of the time slot, which can range from 13-16 μ s, the vehicle will immediately broadcast the packet if available from the queue. However, if the channel is busy during that time, it will select randomly a back-off counter from a contention window from 0 to 3 in the case of AC3 listed in Table I. The process will decrement the back-off counter with probability $(1-p)$ if it senses an idle channel. If the channel is not idle, it freezes the counter and waits for the ongoing transmission time T_t as expressed in (8) until the channel becomes idle again. After the counter reaches 0, the emergency packet gets broadcasted. As mentioned previously, there will be no acknowledgment of this packet and no retransmission tries in case of delivery failure. We use the Markov chain in Figure 2 to derive the probability of sending an emergency packet in a randomly selected slot as shown in the next subsection.

C. M/G/1 queue

Our assumption is that there is a broadcast message sent if certain emergency event happens among vehicles, thus packet generation process is with rate λ and service time is of general distribution due to the nature of the packet processing. We assume that the vehicle's arrival process is represented as a Poisson point process with density β and thus the probability of finding i vehicles in an area A is

$$P(i, A) = \frac{(\beta A)^i e^{-\beta A}}{i!} \quad (1)$$

$$N_t = 4\beta A \quad (2)$$

Based on the same assumptions, the average number of vehicles in the sensing range l would be

$$N_{cs} = 2\beta l_{cs} \quad (3)$$

Figure 1 and 2 provide a Markov chain diagram for the emergency packet's MAC layer back-off counter process. Based on that state transition logic, the probability that the process is in transmission state can be expressed as

$$b_0 = \frac{2(1-p)}{2-3p+pW_s} \quad (4)$$

Once the emergency packet is processed at the queue and ready to be transmitted, according to Poisson properties of probability of the first arrival

$$P(T_1 < t) = 1 - P(N_t = 0) = 1 - e^{-\lambda t} \quad (5)$$

Although the packet is ready, it needs to reach the transmission state with probability $(1-p)$, so having all as an independent set, we have the probability that the vehicle transmits local emergency packet as

$$\tau_s = \frac{2(1-p)^2}{2+pW_s-3p} (1 - e^{-\lambda T_{ss}}) \quad (6)$$

Here, T_{ss} is the average service time needed to process in the upper layer since it has arrived, and p is the probability that the channel is sensed busy during AIFSN and can be expressed as

$$p = 1 - e^{-(N_t-1)(\tau_s+\tau_{ws})} \quad (7)$$

where τ_{ws} is the probability of retransmission/rebroadcast of

a neighbor generated emergency packet derived in Lemma 1. Regardless of whether it is a locally generated emergency packet within the current vehicle or incoming neighbor packet retransmitted, both would have a transmission time T_t which depends on the message and header sizes, arbitrary inter-frame spacing (AIFS) and slot time σ , so the transmission time can be a sum of all the participating elements:

$$T_t = L/r + T_{AIFS} + \sigma \quad (8)$$

where L is the packet size in bits, r is the transmission rate listed in Table II.

When studying the effects of the fail-safe extension, we are concerned about the end-to-end delay for the emergency packets, which consists of the queue delay (either M/G/1 or G/G/1), back-off mechanism delay and the transmission delay. $T_{service}$ is the total end-to-end delay for the emergency packets generated by the sending vehicle and is based on the M/G/1 queue, thus it can be a sum of delay due to the back-off process, T_t , and T_{queue} - delay due to the queue.

$$T_{service} = T_{bo} + T_t + T_{queue} \quad (9)$$

Based on the Pollaczek-Khintchine formula mean time spent at the queue has a general distribution with $E[X]$ and $E[X^2]$,

$$W = \frac{\lambda E[X^2]}{2(1-\rho)} = T_{queue} \quad (10)$$

where $\rho = \frac{\lambda}{\mu} = \lambda E[X]$, thus similarly based on P-K formula

$$T_{queue} = \frac{\lambda_s E[T_{service}^2]}{2(1-\lambda_s T_{service})} \quad (11)$$

Since each of the emergency packets experiences the MAC layer back-off delay, the average delay $E[T_{ef}]$ can be derived as in [3], [7]

$$E[T_{ef}] = \sum_{i=0}^{W_s-1} \frac{p}{W_s} \sum_{k=0}^i (p T_t) = \frac{p^2 T_t (W_s-1)}{2} \quad (12)$$

Thus, overall locally generated emergency packet's end-to-end service time will be different from the service time of the emergency packet coming from a neighbor via a rebroadcast, which is represented as a G/G/1 queue as stated in the next subsection. Another important metric to measure the threshold of the fail-safe mechanism is probability of successful reception.

Due to the nature of broadcast communication in 802.11p/WAVE, there is no acknowledgement, RTS/CTS or retransmission of emergency broadcast packets. Since we only consider one safety channel and only emergency packets generated locally and incoming from neighbors, similar to [7], probability of successful reception of the emergency packets is derived in Theorem 1.

D. G/G/1 queue

Since emergency packets coming from neighbours for rebroadcast have unknown inter-arrival time distribution, we assume it is of general distribution. In addition, due to the nature of weighted p -persistence algorithm, packet history affects whether the current packet will be rebroadcasted or not, so we consider the queue as a G/G/1. The exact number of

mean packets in the queue for this type is unknown, so we will use Marchal formula [11] definitions referred in Table II.

$$\text{Definition 1: } C_s^2 = \frac{\sigma_s^2}{(\bar{s}/\mu)^2} \quad (13)$$

$$\text{Definition 2: } C_a^2 = \frac{\sigma_a^2}{(\bar{a}/\lambda_{wa})^2} \quad (14)$$

Definition 3: Utilization of the server for outside broadcasts

$$\rho = \frac{\lambda_{wa}}{\mu_{wa}} \quad (15)$$

Definition 4: The approximate mean number of packets in the queue is

$$L_q = \frac{\rho^2(1+C_s^2)(C_a^2+\rho^2C_s^2)}{2(1-\rho)(1+\rho^2C_s^2)} \quad (16)$$

We add another independent event to each emergency packet sent by the vehicles. As described in the previous subsection, the probability of each vehicle transmitting an emergency packet consists of having the packet ready for the transmission and the back-off counter reaching state b_0 with probability $(1-p)$, but our case would add another independent probability from the weighted p -persistence schema. As described in [1], weighted p -persistence schema allows the vehicle to decide whether to rebroadcast or not based on the distance between the neighbors. When the tagged vehicle generates randomly an emergency packet due to some accident, that event can be assumed independent of the rebroadcast of a neighbor emergency packet, but both events have similar MAC layer processing. Thus, we have:

Lemma 1: Let τ_e be a probability that a vehicle might send out an emergency packet at the MAC layer once it is ready to be sent and d_{ij} distance between communicating vehicles i and j . Then, the probability τ_{wa} that the vehicle is able to rebroadcast the incoming emergency packet from a neighbor is

$$\tau_{wa} = \frac{2(1-p)^2}{2+pW_0-2p} * (e^{-\lambda_e T_{service}}) * \left(\frac{d_{ij}}{R}\right) \quad (17)$$

where $T_{service}$ is given by (9).

Proof: Based on (4), we know that the probability for any higher level packet to be in Markov process state b_0 but in our case, we have two inflows of emergency packets. First, there is a general case when the vehicle itself experiences an accident and sends an emergency with probability according to (6). Second, if any of the neighbors sends out emergency, the sending vehicle also receives multiple emergency packets from neighbors. Therefore, we have local and foreign emergency packets competing for the MAC layer broadcast. Foreign emergency packets in this case would be packets coming from neighborhood rebroadcasts and local emergency packets are those generated by the tagged vehicle itself. Thus, τ_{wa} represents the probability that the incoming broadcast from neighbors will be sent out when there are no emergency packets from the receiving vehicle itself.

Lemma 2: Let T_{eq} be queuing delay for local emergency packets, then the average delay for foreign emergency packet due to weighted p -persistence algorithm is based on G/G/1 queue. Thus the mean waiting time in the queue is

$$T_{waq} = L_q / \lambda_{wa} \quad (18)$$

where λ_{wa} is the arrival rate of foreign emergency packets

and L_q - mean number of packets in the queue.

Proof: According to G/G/1 characteristics and (16), we have L_q , where C is coefficient of variation of random variable and $C = \frac{\text{Variance}}{(\text{Mean})^2}$. In this case, we have to assume a series of arrival rates and mean service rates to experiment based on the traffic intensity during the intelligent flooding.

Theorem 1: Average emergency packet's time delay for the incoming neighborhood broadcast is:

$$T_{waes} = E[T_{ef}] + T_t + T_{waq} \quad (19)$$

Proof: Based on Lemma 2, we know the wait time in G/G/1 queue for the incoming packets T_{waq} . The time of successful transmission T_t is based on (6). The back-off delay will be the same for both types of emergency packets and is based on (11).

TABLE I. CONTENTION PARAMETERS FOR DIFFERENT ACCESS CATEGORIES IN 802.11p [3]

AC	Data Class	CWmin	CWmax	AIFS
0	Background Traffic	15	1023	9
1	Best Effort	7	15	6
2	Voice	3	7	3
3	Safety Related	3	7	2

E. Fail-safe mechanism and performance evaluation

For the performance analysis of emergency packets, we will mainly use two metrics. Delay for the generated emergency packet is calculated based on equations (9) and (12). Although there is no packet acknowledgement in 802.11p/WAVE, we can still measure the success based on the packet loss. We will then further prove the model by running extensive simulations as described in section IV.

Moreover, these two main metrics will tell us about the effects of having or not having the fail-safe mechanism built into the broadcasting protocols. Under the fail-safe mechanism, each vehicle will continuously monitor the network to detect any misbehavior. Each vehicle needs the following function to determine the misbehavior properly via a calculated weighted score $\omega = F_{fs}(R_{br}, T_{delay}, \varphi_{total}, \gamma)$. Here R_{br} is the ratio of all received broadcasts versus sent broadcasts per each vehicle, and T_{delay} is the average delay each packet experiences at the MAC layer. If the delay average is significantly higher than the standard deviation of the delay previously measured, that would add to the fail-safe detection more weight. φ_{total} is the total number of SNIR/RXTX lost packets during the broadcast communication between vehicles, and γ is the number of times MAC layer goes into back-off if there is any misbehaving vehicle [5]. During the normal operation, the first indicator of the misbehavior will be the excess of delay in multiples of the standard deviation T_{delay} . In addition, to make sure the mechanism does not detect a false positive, other input parameters will be inspected to validate, each adding about the same amount of weight. Algorithm 1 describes the full fail-safe mechanism with the use of the

above input parameters. Refer to Table II for the input parameters of Algorithm 1.

Algorithm 1 Fail-safe mechanism

```

Initial setup
Set  $T_{delay}$  according to (13)
Set score  $\omega \leftarrow 0$ 
Set  $R_{br} = N_{rb} / N_{sb}$ 
Set  $\phi_{total}$  based on the acceptable 10% drop rate
Set  $\lambda_{all}$  - could be correlated with delay or independent
for every incoming message
if  $T_{delay} \geq 3 \times$  standard deviation of delay averages
     $\omega \leftarrow \omega + 0.1$ 
if  $R_{br} \leq 1$  AND  $R_{br} > 0$  (received same or less than sent)
     $\omega \leftarrow \omega + 0.2$ 
if  $\phi_{total} \geq 10\%$  lost rate
     $\omega \leftarrow \omega + 0.1$ 
if  $\lambda_{all} \geq \lambda_{limit}$  (based on the simulation data)
     $\omega \leftarrow \omega + 0.1$ 
if  $\omega \geq 0.5$  Fail-safe = true
else Fail-safe = false

```

TABLE II. NETWORK MODEL PARAMETERS

N	Number of vehicles
λ_{we}	Arrival rate of the incoming neighbor broadcast
λ_j	Arrival rate of each connection
L_q	mean number of packets in the queue
l_{cs}	Sensing range for each vehicle
L	the packet size in bits
r	the transmission rate
σ	Slot time for the MAC layer
P_{ber}	Bit error rate
R	Transmission range
A	i vehicles in an area A
T_{IFS}	Arbitrary inter-frame spacing
β	Vehicle density for the area A
d_{ij}	Communication distance between vehicle i and j
C_s^2	Coefficient of variation of service time for G/G/1
C_a^2	Coefficient of variation of inter-arrival time
R_{br}	Ratio of all received vs sent broadcasts per car
T_{delay}	Acceptable delay threshold limit
ϕ_{total}	SNIR/RXTX lost packets during the broadcast
λ_{all}	Total arrival of packets combined
N_{rb}	Number of received broadcasts per vehicle
N_{sb}	Number of sent broadcasts per vehicle
ω	Weighted score determining the fail-safe mechanism
N_t	Number of vehicles in the range of the transmission

IV. SIMULATION

In this section, the validity of the model is demonstrated by comparing analytical results with those obtained from VEINS simulations that employ standard MAC (IEEE

802.11p) and weighted p -persistence broadcasting protocol [10]. The traffic and scenario patterns are randomly made. The simulation parameters are listed in Table III.

TABLE III. SIMULATION PARAMETERS

Simulation parameter	Value
Simulation time limit	3000 s
Playground size X,Y	6000 m
Playground size Z	2150 m
Channel frequency	5.890e9 Hz
Header length	256 bit
Message size	160 bytes
802.11p sensitivity	-89dBm
802.11p thermal noise	-110dBm
1609.4 TX power	20mW
Data priority	2
Maximum offset	0.005 s
Number of vehicles	100
Weighted p probability	0.5
N misbehaving vehicles	1-3

A. Simulation Parameters

In the model we simulate here, we consider a network of N nodes (100 vehicles) that are uniformly and independently distributed over a 6000 m $\times$ 6000 m area. SUMO tool generates the random vehicular traffic, while Veins simulator produces packets of length 160 bytes at the rate of λ packets per second. Destinations are chosen randomly, and the first emergency message is generated by a random car if it stops for more than ten seconds. The traffic is routed to the destination using weighted- p persistence protocol with $p=0.5$. Code implementation for the routing and fail-safe decisions is done at the application and MAC layer. The area was a typical mix of urban and suburban area generated with OpenStreetMap export tool. The simulation time for each run is 3000 seconds. We are interested mainly in delay and packet loss in this case.

B. Comparing the Analytical Results with Simulation Results

Figure 3 compares the average MAC layer processing delay when there is no misbehaving vehicle, i.e., the routing protocol is operating normally, and when there are two misbehaving vehicles. The highest delay is experienced by the misbehaving vehicles and the closest neighboring vehicles, and although other vehicles' processing delay remains the same, this parameter helps the algorithm to detect when the routing protocol starts failing.

Figure 4 and 5 show how the misbehaviour affects all other vehicles in terms of keeping the communication channel busy. This is the time in seconds that the MAC layer considered the channel as busy, thus had to back-off. Under the misbehaviour, MAC at each vehicle had to wait up to one second versus up to 6 milliseconds under the normal behaviour.

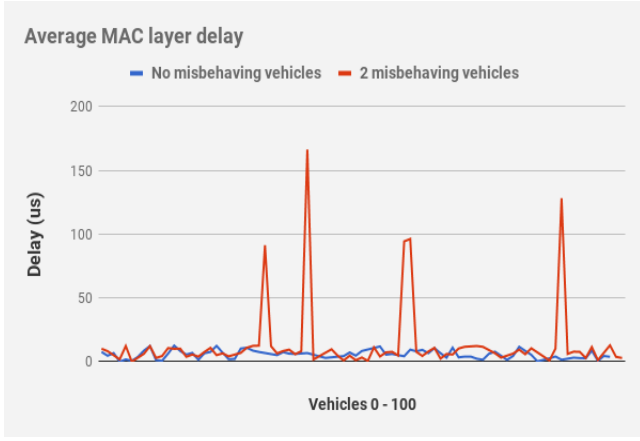


Figure 3. Average MAC layer delay.

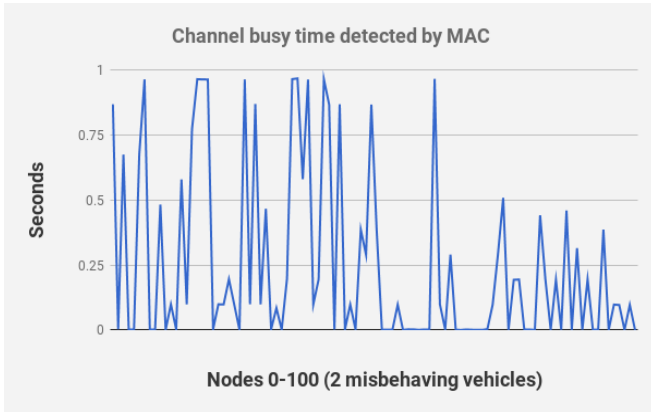


Figure 4. Channel busy time with two misbehaving vehicles.

Figure 6 also shows how the misbehaviour affects the overall packet loss at each vehicle. On average the number of lost packets at each vehicle could increase 80% due to the misbehaviour. Figure 8 shows the same conditions, but with fail-safe mechanism active, thus we can observe that the mechanism stabilizes the routing protocol. Figure 7 shows how the fail-safe mechanism can stabilize the time the MAC layer considers the channel as busy. The mechanism allows the routing protocol operate normally as before, once detected by the algorithm mentioned above. This then affects the overall delay and performance of the system.

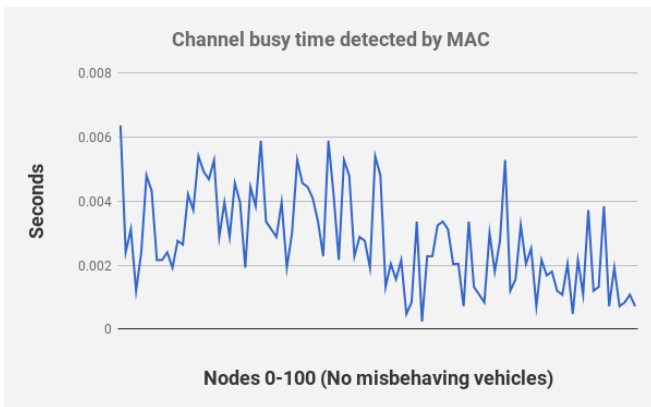


Figure 5. Channel busy time with no misbehaving vehicles.

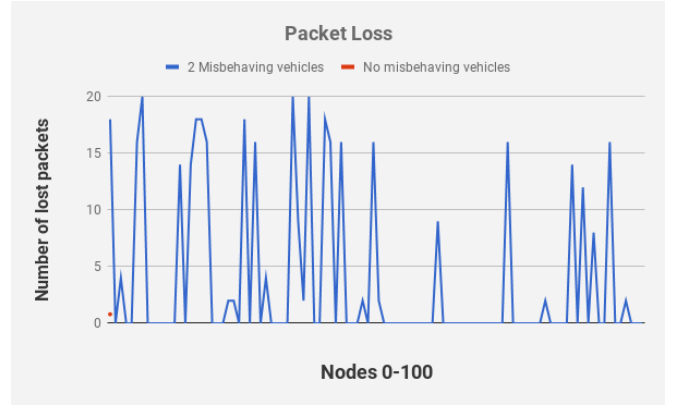


Figure 6. Packet loss with two vs. zero misbehaving vehicles.

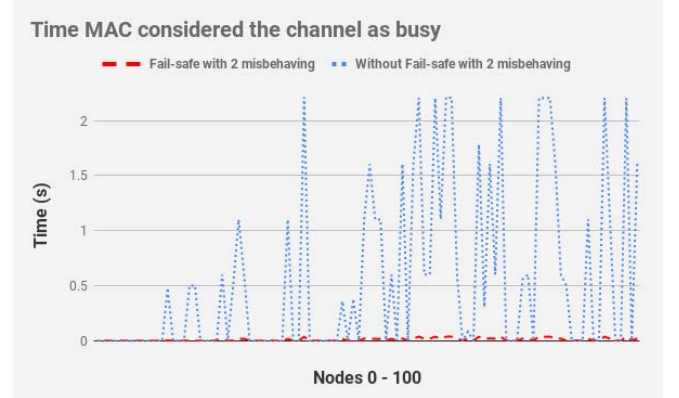


Figure 7. Channel busy time with and without fail-safe mechanism.

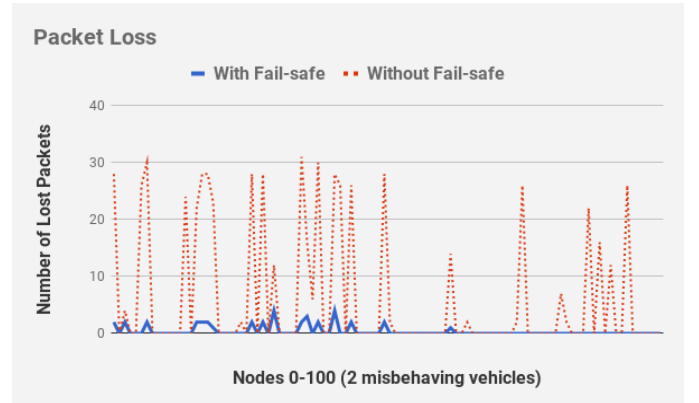


Figure 8. Packet loss with fail-safe active and inactive.

V. CONCLUSION

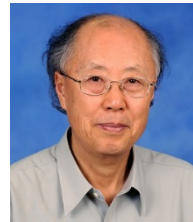
The proposed fail-safe algorithm can be an effective mechanism in stabilizing the probabilistic routing protocol during the emergency message broadcast. The detection process can use multiple internal parameters and metrics to accurately predict when there is a routing misbehaviour happening at each vehicle participating in the emergency broadcast. This paper demonstrated how misbehaviour can turn the normal probabilistic routing protocol into the worst case of flooding the network with large delays and significant packet loss. If the routing protocol or the MAC layer has the

built-in fail-safe mechanism, it is possible to detect and prevent such type of misbehaviour.

We are developing a prototype to find an optimal threshold value for triggering fail-safe mechanism in vehicular ad hoc networks.

REFERENCES

- [1] N. Wisitpongphan, O. Tonguz, J. Parikh, P. Mudalige, F. Bai, and V. Sadekar, "Broadcast storm mitigation techniques in vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 14, no. 6, pp. 84–94, Dec. 2007.
- [2] Qiu, Harry JF, et al. "A methodology for studying 802.11 p VANET broadcasting performance with practical vehicle distribution." *IEEE transactions on vehicular technology* 64.10 (2015): 4756-4769.
- [3] Eckhoff, David, and Christoph Sommer. "A multi-channel IEEE 1609.4 and 802.11 p EDCA model for the veins framework." *Proceedings of 5th ACM/ICST international conference on simulation tools and techniques for communications, networks and systems: 5th ACM/ICST international workshop on OMNeT++*, (Desenzano, Italy, 19-23 March, 2012). OMNeT. 2012.
- [4] X. Ma, X. Chen and H. H. Refai, "Unsaturated Performance of IEEE 802.11 Broadcast Service in Vehicle-to-Vehicle Networks," 2007 IEEE 66th Vehicular Technology Conference, Baltimore, MD, 2007, pp. 1957-1961. doi: 10.1109/VETECE.2007.411
- [5] X. Ma and X. Chen, "Delay and Broadcast Reception Rates of Highway Safety Applications in Vehicular Ad Hoc Networks," 2007 Mobile Networking for Vehicular Environments, Anchorage, AK, 2007, pp. 85-90. doi: 10.1109/MOVE.2007.4300809.
- [6] Hafeez, Khalid Abdel, et al. "Performance analysis and enhancement of the DSRC for VANET's safety applications." *IEEE Transactions on Vehicular Technology* 62.7 (2013): 3069-3083.
- [7] K. A. Hafeez, L. Zhao, Z. Liao and B. N. W. Ma, "Performance Analysis of Broadcast Messages in VANETs Safety Applications," 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, FL, 2010, pp. 1-5. doi: 10.1109/GLOCOM.2010.5683612
- [8] B. Li, G. J. Sutton, B. Hu, R. P. Liu and S. Chen, "Modeling and QoS analysis of the IEEE 802.11p broadcast scheme in vehicular ad hoc networks," in *Journal of Communications and Networks*, vol. 19, no. 2, pp. 169-179, April 2017.
- [9] Zheng, Jun, and Qiong Wu. "Performance Modeling and Analysis of the IEEE 802.11 p EDCA Mechanism for VANET." *IEEE Transactions on Vehicular Technology* 65.4 (2016): 2673-2687.
- [10] Christoph Sommer, Reinhard German and Falko Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing*, vol. 10 (1), pp. 3-15, January 2011
- [11] J. Shortle, J. M. Thompson, D. Gross, C. M. Harris, "Approximations," in *Fundamentals of Queueing Theory*. Hoboken, NJ: John Wiley & Sons, 2018, pp 370-380



in Computer Science at the University of Texas at Arlington. His research interests include computer network security, wireless network routing, and parallel computer architecture. He has co-authored over 100 scientific articles in refereed journals and international conferences. He is a senior member of IEEE and a member of ACM.



Yong-Kab Kim received his Ph.D degree in Electrical & Computer Engineering in North Carolina State University. He is currently in Professor at School of Electrical Information Communication Engineering, Wonkwang University, Korea. His research interests are Remote sensing for Visible Communication, Optical Fiber Sensing, Intelligent Control, and Advanced Computational Intelligence.



Geun-Ho Jeong received his BS degree and currently pursues MS degree in Electrical Engineering in Wonkwang University. His research interests are Electric Machinery, Electronic Circuit, and Light source of LED.



Kumar Sharshembiev is an Assistant Professor at the American University in Central Asia. Currently working towards completing his PhD degree at the University of Alabama in Huntsville (UAH). Before starting his PhD degree, he did his Bachelor and MS in Computer Science at the Old Dominion University, Virginia and worked as a software engineer in New York.

Research interests include vehicular networks, network security, machine learning in vehicular networks, and efficient routing protocols.

Seong-Moo Yoo is an Associate Professor of Electrical and Computer Engineering at the University of Alabama in Huntsville (UAH). Before joining UAH, he was an Assistant Professor at Columbus State University, Columbus, Georgia –USA. He earned MS and PhD degrees