Cluster-Based Irresponsible Forwarding

Stefano Busanelli, Gianluigi Ferrari, and Sooksan Panichpapiboon

1 Introduction

In the last decades, Inter Vehicular Communication (IVC) systems have attracted a significant attention from universities, public administrations, and automotive companies. Despite huge efforts, these applications have not yet found the way to the market, but the intensity of the research activity still remains high. As for other ICT technologies, the success or the defeat of IVC systems depends on the appearance of killer applications. Today, the most promising areas seem to be related to accident prevention and vehicular traffic optimization. Due to the their high dynamical nature and the lack of fixed infrastructure (also for economic reasons), typically IVC systems are exploited by the so-called Vehicular Ad-Hoc Networks (VANETs).

In order to satisfy the requirements of the aforementioned applications, several authors have proposed broadcast transmission techniques, but the design of an efficient and reliable broadcasting forwarding protocol is not an easy challenge [1]. Among the various approaches, we focus on two categories of forwarding protocols, namely probabilistic and cluster-based, and we try to merge them. From pioneering works, such as [2], cluster-based networks have found a fertile application ground in the field of wireless sensor networking. In fact, in these applications, cluster-based approaches are beneficial from several points of view: they allow to reduce network congestion, to increase the spectral efficiency, and to simplify routing issues, data aggregation and dissemination. Despite their evolution and their potential advantages, cluster-based networks have not been able to obtain the same success in VANETs. The high dynamism of these networks is one of the main obstacles

S. Busanelli (✉) and G. Ferrari
Department of Information Engineering, CNIT Research UNIT, University of Parma, Parma, Italy
e-mail: busanelli@tlc.unipr.it; gianluigi.ferrari@unipr.it

S. Panichpapiboon
Faculty of Information Technology, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand
e-mail: sooksan@alumni.cmu.edu

D. Giusto et al. (eds.), *The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications*, DOI 10.1007/978-1-4419-1674-7_6,

against the implementation of cluster-based networking protocols. In fact, the high dynamism leads to a very short lifetime of the clusters, thus yielding a high overhead for cluster construction and maintenance, partially vanishing their potential benefits. Besides these problems, there are nonetheless good reasons for employing cluster-based approaches. One of the strongest motivations is provided by [3], where the authors show that, according to realistic mobility models, VANETs naturally evolve to clustered configurations. Among the more recent cluster-based protocol proposed in VANETs, some interesting approaches can be found in [4, 5]. In the latter work, communications are typically broadcast but, when possible, short-lived clusters are created to constitute a backbone. It is then possible to employ unicast communications among the nodes of the backbone, leading to a higher reliability without sacrificing network performance.

In [6], the authors propose an innovative probabilistic forwarding technique, named irresponsible forwarding (IF), in which every node properly computes its own transmission probability in a per-packet manner, taking in account the vehicle spatial density and the distance from the source. From the simulation analysis of the IF protocol, in IEEE 802.11 networks [7], performed in [8], it emerges that IF is a quite promising approach to broadcasting. Being a probabilistic protocol, however, its reliability is not perfect. Hence, in this work, we apply the concept of IF to derive a new broadcast technique, denoted as cluster-based irresponsible forwarding (CIF), that integrates the probabilistic approach of the original IF protocol with a cluster-based structure, to improve its performance. The key characteristic of CIF is that a clustered structure is not imposed. Rather, CIF opportunistically exploits the "ephemeral" clusters that appear in VANET.

After a short description of the IF protocol in Sect. 2, we will describe the CIF protocol in Sect. 3. In Sect. 4, we will define the simulation setup. Finally, in Sect. 5, we will present and discuss some simulation results, which will highlight the improvement brought by intelligent exploitation of "ephemeral clusters." Sect. 6 will then conclude the chapter.

2 Irresponsible Forwarding

In order to understand the basic operational principle of the IF protocol, we sketch its behavior in a one-dimensional network with a single source placed on the leftmost margin (this is the case, for instance, of a highway lane). After the initial packet transmission from the source, denoted as the 0th hop transmission, the packet is then received by a subset of the source neighbors, that are the potential rebroadcasting nodes. Their union constitutes the so-called 1st transmission domain (while the source itself identifies the 0th *transmission domain*). Every node of the 1st transmission domain extracts a value p uniformly distributed in the interval [0, 1], and then it rebroadcasts it only if $\Delta p \triangleq p_{\text{th}} - p > 0$, where p_{th} is given by the following probability assignment function, originally presented in [6]:

$$p_{\text{th}} = e^{-\frac{\rho_{\text{s}}(z-d)}{c}} \tag{1}$$

where d is the distance between the sender and the receiver (dimension: [m]), ρ_s is the one-dimensional vehicle spatial density (dimension: [veh/m]), z is the node transmission range (dimension: [m]), and c is a shaping coefficient (adimensional). If an intermediate node receives more than one copy of a packet, it makes the rebroadcast decision only upon the reception of the first copy of the packet. All the successive copies are automatically discarded to reduce the network traffic and avoid self-loops. All the nodes that receive a "fresh" packet by a node belonging to the 1st transmission domain contribute to form the 2nd transmission domain. This happens recursively, until the packet is not rebroadcast or reaches the physical network limit.

In [8], the performance of the IF protocol is investigated in a realistic IEEE 802.11 network environment, considering some important performance indicators, introduced in [9], such as the REachability (RE), the number of Saved ReBroadscast (SRB), and the end-to-end delay. The obtained results show that while the IF protocol significantly outperforms a simple flooding protocol in terms of rebroadcast (and energy) savings, it does not guarantee a sufficient reliability to warrant its use in safety-sensitive applications. A simple strategy to increase the reliability would consist of tuning the shaping parameter c in (1) in order to "artificially" increase the number of retransmissions. This approach allows to maintain a short the end-to-end delay, but unfortunately it is feasible and effective only when the traffic load is low. In fact, as shown in [8], when the traffic load is high, even an accurate tuning of the parameter c does not offer significant advantages. This has motivated the integration of the IF protocol with an efficient cluster-based architecture.

3 Cluster-Based Irresponsible Forwarding: The Idea

As previously mentioned, a multihop broadcast protocol can be evaluated according to three strictly correlated metrics: the end-to-end delay, the reliability (here expressed in terms of RE), and the Transmission Efficiency (TE). The goal of the CIF protocol is which of obtain a better tradeoff with respect to the IF protocol.

In order to increase the reliability of the IF protocol, still maintaining its low latency, we propose a hybrid approach that combines the probabilistic broadcast nature of the IF protocol with a "loosely clusterized" VANET structure. Our philosophy is to establish a weak artificial packet flow, having the task of discovering the presence of naturally formed clusters, exactly as the water flow in a river highlights the presence of underwater rocks thanks to the generation of a wave signature. Then, we exploit this informations in order to optimize the forwarding procedure, increasing the reliability and the transmission efficiency, but without building up a true clustered infrastructure. Therefore, we introduce the concept of *Ephemeral Cluster* (EC), that is a short-lived cluster of nodes that is recognized and exploited for a limited period of time (just the duration of a packet retransmission). To clarify the concept, in Fig. 1 we show two typical transmission domains at a given hop. The upper transmission domain is *sparse*, since there is no node aggregation. In this situation, the IF protocol performs generally well, since the probability assignment function is sufficiently "steep" to effectively select the best retransmitting nodes. The lower transmission domain, instead, contains two ECs, one near to the source and one much farther. As shown in [8], in this scenario, the performance degrades since the probability assignment function tends to be similar for all nodes of a cluster, thus yielding to congestion and collisions. This problem is important especially when the cluster is far from the source, since the presence of several nodes, with roughly the same high retransmission probability (p_{th}), will probably lead to several retransmissions of the same packet.

After this preliminary introduction, we now present the forwarding procedure used by the CIF protocol. At the (generic) ith hop, it can be summarized in four steps, graphically represented in Fig. 2.

1. A packet transmission of a node of the $(i - 1)$th transmission domain identifies the ith transmission domain.

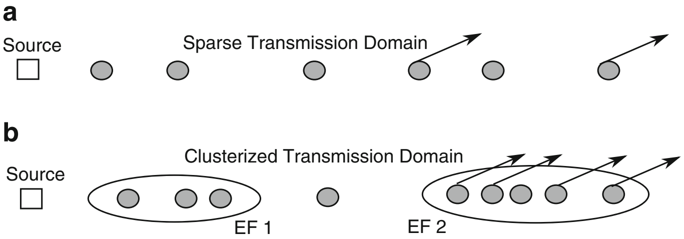

Fig. 1 Two transmission domains (**a**) the upper is *sparse*, while (**b**) the lower contains two ECs

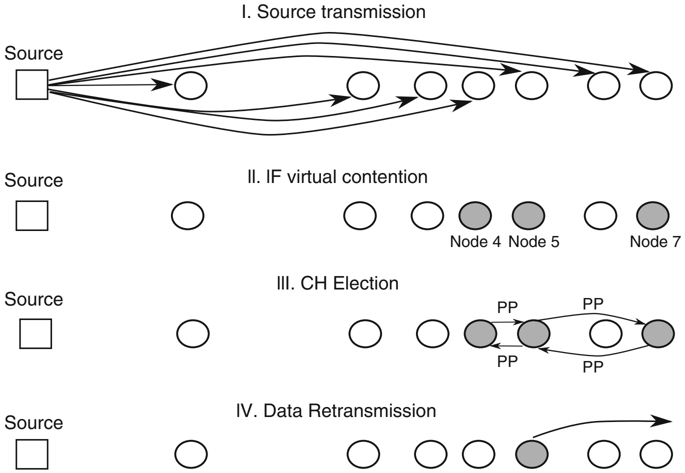

Fig. 2 Forwarding procedure of the CIF protocol

2. The second step derives directly from the IF protocol and is a sort of "virtual contention." In particular, every node in the ith transmission domain decides to become or not a potential forwarder performing the same election mechanism, described in Sect. 2, of the IF protocol. The winners of this contention will begin the third step, while the others will simply discard the packet.
3. The third step derives from the concept of "ephemeral cluster." Once a node wins the first virtual contention, it schedules the retransmission of a very short packet, denoted as probe packet (PP). A PP bears just two information (1) the unique identification (ID) number of the packet to be retransmitted; (2) the instantaneous difference $\Delta p = p_{\mathrm{th}} - p$. The PPs are intrinsically single hop, i.e., they are not forwarded. A PP is transmitted with a low-transmission power, since a node is interested only in signaling its presence to its neighbors, and with a high priority, in order to reduce the overall latency. Moreover, a low transmission power allows to reduce channel interference. The specific power and priority setting of a PP have to be tuned according to the used medium access control (MAC) protocol, and their values in the scenarios of interest will be given in Sect. 5. After winning the virtual contention, every potential forwarder sends a PP. It then waits for a short prefixed interval, denoted as T_{w}: if, within this interval, it receives at least a PP containing a value of Δp larger than its own, it stops and discards the packet (in fact, there is some other better forwarder); conversely, it retransmits the packet. In the worst case, when a collision between two or more PPs happens, this selection mechanism fails and no node of the cluster is elected. In this case, all nodes will retransmit in order to guarantee a high reachability.
4. The fourth step corresponds to the transmission act from the designated forwarding nodes.

4 IEEE 802.11 Network Simulation Setup

We use the IEEE 802.11 model present in Network Simulator 2 (ns-2.31 [10]), sending small size packets (105 B) in order to prevent fragmentation, using the default values of the vanilla ns-2 installation that refers to the IEEE 802.11b standard. On top of the IEEE 802.11 MAC layer, we insert the IF forwarding protocol. Since this work does not focus on physical layer issues, we adopt a simple Friis free-space propagation model [11]. We also consider a static scenario, where the nodes are placed along a straight line of length L (dimension: [m]) and their positions are generated according to a Poisson distribution of parameter ρ_{s} (dimension: [veh/m]) – this is representative of highway scenarios with cars moving at similar speeds. In order to have a fair comparison between the results obtained with different values of z (dimension: [m]), we vary the network length proportionally to the transmission range, setting $L = 8z$. For instance, with a transmission range $z = 500$ m we consider a portion of road of 4 km in front of the source vehicle.

As in [6], there is a single source placed on the left vertex of the linear network, so that packets flow from left to right. For every (ρ_{s},z) pair, there is a nonzero

Frequency	2.4 GHz
Channel bandwidth	2 MHz
PLCPDataRate	1 Mbps
Data rate	1 Mbps
CW_{MIN}	31
SlotTime	$20\mu s$
SIFS	$10\mu s$
PreambleLength	144 bit
PLCPHeaderLength	48 bit

Fig. 3 Parameter of the IEEE 802.11b standard used in the simulations

probability of having a distance d between two consecutive nodes, say k and $k+1$, larger than the transmission range z, since d is exponentially distributed. If $d > z$, the $(k+1)$th node is unreachable and the kth one becomes the last reachable node (lrn) of that particular scenario. When lrn$\neq N$ the network is said topologically disconnected, whereas if lrn$= N$, the network is topologically connected.

The source sends a burst of 1,000 packets using a Poisson distribution with parameter λ (dimension: [pck/s]).[1] We use a value of λ equal to 100 pck/s, so that considering the packet size of 105 bytes leads to an average load of 84 kbps, that is significant with respect to the available data rate that is of 1 Mbps, as shown in Fig. 3. Two values of the parameter c, namely 1 and 5, are adopted, representing, respectively, weak and aggressive rebroadcasting policies. The results are obtained for a fixed node density value $\rho_{\text{s}} = 0.01$ vehicle/m, while the transmission range z assumes the values in the set $\{0.1, 0.3, 0.5, 0.75, 1, 1.5, 2, 3\}$ km, in order to have the desired value of the product $\rho_{\text{s}} z$. Clearly, the transmission range is obtained setting the suitable value of the transmission power. For small values of z, the network is rarely connected since $Pr\{d > \rho_{\text{s}}{}^{-1}\}$ is relatively high. On the other end, the network gets connected with a high probability (almost 1), if z is larger than 750 m.

Clearly, the IEEE 802.11 interfaces operate in the ad-hoc mode, and they send packets in a broadcast fashion. In this configuration, the distributed coordination function (DCF) cannot exploit the ready-to-send/clear-to-send (RTS/CTS) mechanism, since the latter is a viable strategy only for unicast communications. For the same reason, the ACK messages are also ineffective and, therefore, they are disabled. Hence, the hidden terminal problem is unsolved and retransmissions cannot happen at the MAC layer, since the sender cannot get information about the status of its communications. Without retransmissions, the contention window (CW) of the carrier sense multiple access with collision avoidance (CSMA/CA) MAC protocol is never increased and always assumes its initial value specified by the parameter CW_{MIN} of the IEEE 802.11 standard [7]. The parameters of the IEEE 802.11 standard relevant for the simulations are listed in Fig. 3.

[1] Our simulations show that the numbers of the generated scenarios (1,000) and of the transmitted packets (1,000) are sufficient to guarantee an interval of confidence greater than 95%; thus, we will omit any error considerations in our results analysis.

Finally, the CIF protocol foresees the use of two types of packets, data and probe, which require two different services from the lower layers. In particular, a PP requires a higher transmit priority and a lower power than a data packet . In order to obtain a higher priority, we set CW_{MIN} to 7, instead of the value of 31 used for data packets. On the other hand, as will be shown in Sect. 4, the transmit power can be set to different values to vary the transmission range. In all cases, PPs are transmitted with a power equal to 20% of the transmit power used to send data packets. The waiting time T_{w} is set to 10 ms.

5 Numerical Results

In Sect. 3, it was anticipated that three metrics will be used to assess the behavior of the CIF protocol: RE, TE, and end-to-end delay. The latter is the duration of the packet traveling time between its transmission instant at the source and its reception instant[2] at the lrn. The end-to-end delays of the IF and CIF protocols, with two different values of c (1 and 5), are shown in Fig. 4 as functions of the product $\rho_{\mathrm{S}}z$. As expected, the introduction of an election procedure increases the overall latency for both values of c. However, the delay still remains acceptable. In fact, according to [12], a good latency value for the prevention of chain car collision is about 0.1 s and from Fig. 4 one can observe that the overall latency for all $\rho_{\mathrm{S}}z$ values is lower or very close to this value. One has to keep in mind that the end-to-end delay is measured at the lrn that could be considerably far from the source, i.e., for a transmission range

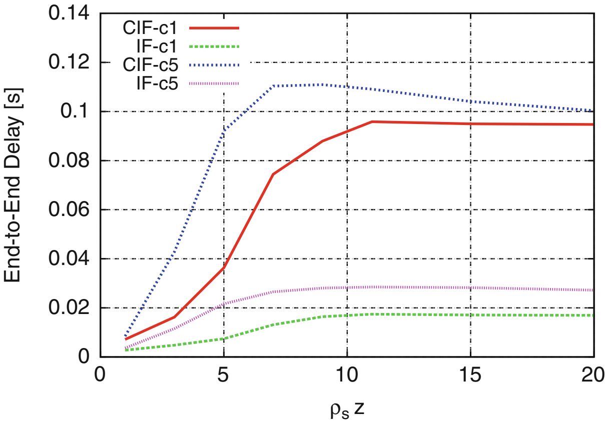

Fig. 4 End-to-end delay as function of the product $\rho_{\mathrm{S}}z$ for various combination of protocols and values of c. In particular, for both IF and CIF protocols two values of c are considered (1 and 5)

[2] We remark that only the packets received correctly at the lrn are considered in the end-to-end delay evaluation phase; hence, this metric is an upper bound of the end-to-end delay experienced by the network nodes.

of 1 km ($\rho_s z \leq 5$) the network dimension is $L = 8$ km. Finally, one can observe that for small values of the product $\rho_s z$ (e.g., 10), the latency is small. In fact, in this region, the network has a limited connectivity and the lrn could be in the proximity of the source, whereas in the other cases its distance is comparable with L.

The RE, introduced in [9], corresponds to the fraction of nodes that receive the source packet among the set of reachable nodes, i.e., those topologically connected to the source. In our case, the number of reachable nodes coincides with lrn. Intuitively, the RE is inversely proportional to the distance from the lrn, since the farther is the lrn, the larger is the number of hops required to reach it. Clearly, since IF is a probabilistic protocol, at every hop there is a nonzero probability of no effective transmission, thus cutting off the packet flow. This induces a singular consequence: with the same value of $\rho_s z$, less connected networks (with a smaller lrn) could have a higher RE since the number of hops required to reach the lrn reduces.

The TE is a novel metric, here introduced for the first time, that is somehow related to the concept of Saved REbroadcasts (SRB), originally introduced in [9]. In particular, for a given packet, we define the TE as the ratio between its RE and the overall number of retransmissions that is experienced during its trip towards the lrn. For instance, given a network with lrn $= 100$, a packet that reaches 80 nodes, through an overall number of retransmissions equal to 20, will lead to measure a value of RE equal to $80/100 = 0.8$ and a value of TE equal to $0.8/20 = 0.04$. Roughly speaking, an ideal forwarding protocol for safety-related vehicular applications should minimize the latency, still guaranteeing the highest possible RE. Instead, the TE is an indicator of the ability of the protocol of selecting the optimal forwarding node. Figures 5 and 6 show, respectively, the REs and TEs obtained with the IF and CIF protocols, using two different values of c (1 and 5) as functions of the product $\rho_s z$. From Fig. 5, one can observe that the classical IF protocol performs very poorly with the selected traffic load of 100 pck/s. In particular, when

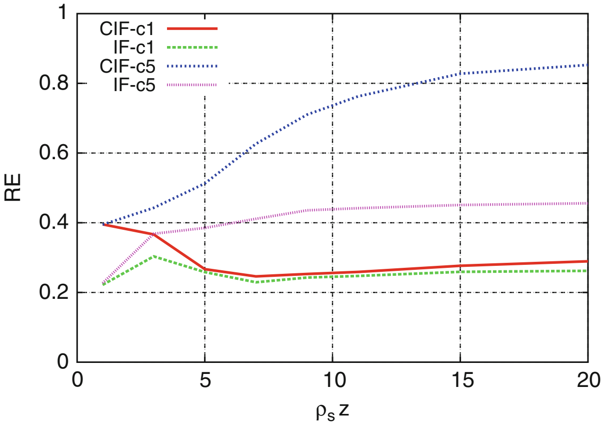

Fig. 5 RE as function of the product $\rho_s z$ for various combination of protocols and values of c. In particular, for both IF and CIF protocols two values of c are considered (1 and 5)

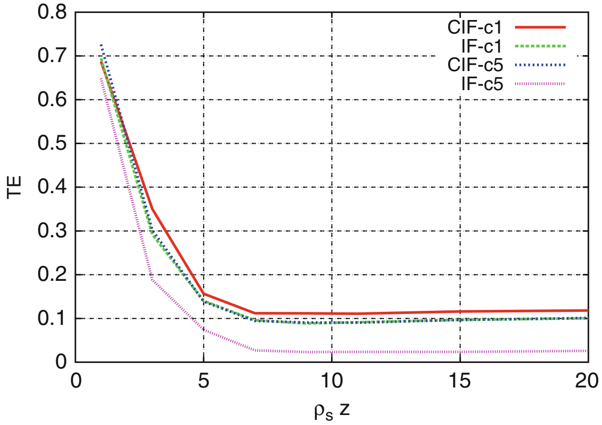

Fig. 6 TE as function of the product $\rho_s z$ for various combination of protocols and values of c. In particular, for both IF and CIF protocols two values of c are considered (1 and 5)

$c = 1$, the IF protocol cannot self-sustain itself and the RE remains around 0.2. With $c = 5$, the behavior is slightly better but the RE is still limited by collisions and congestion. The CIF protocol shows a similar behavior when $c = 1$. In fact, in this case, the improved relay selection mechanism does not offer a significant advantage, since the average number designated by the virtual contention is small (on average around 1, as shown in [6]). Conversely, CIF offers a significant improvement when $c = 5$, since it reduces the congestion of the channel, thus limiting the number of the data packet transmissions by substituting them with quick and low-power PP transmissions. Finally, Fig. 6 shows similar results. In particular, the CIF protocol outperforms the IF protocol for both values of c, but especially when c is equal to 5, where the improvement is particularly evident. Counterintuitively, the TE assumes higher values in the scarcely connected region. This is motivated by the fact that in this region, the single retransmission has a stronger impact on the RE since the lrn and the number of hops are typically small.

6 Conclusions

In previous works [6, 8], we have shown that the IF protocol can offer a high reachability when the shaping factor c is sufficiently high to self-sustain the protocol (typically, $c = 5$ is a good value). Unfortunately, the RE of the classical IF protocol degrades when the network traffic load increases, since a high value of c leads to a high number of retransmissions. In order to reduce the congestion, we have presented a novel approach to exploit the ephemeral clusterization that naturally emerges in VANETs, thus leading to a novel probabilistic forwarding protocol, denoted as CIF. The adopted approach brings significant benefits, in terms of RE and of TE, with respect to the IF protocol. We also observed that the latency remains within the limit imposed by the target applications (safety-related applications in VANETs). Finally, we emphasize that one of the strengths of the CIF protocol is the limited required amount of information on the network topology. In particular, it requires the knowledge of just one topology parameter, the vehicular spatial density ρ_s, that could be obtained combining long-term statistics about the vehicular traffic and local estimations of the density. Hence, unlike other approaches (see, for example, [13]), the CIF protocol represents an efficient event-driven forwarding protocol, without the need of an auxiliary logical channel for exchanging local information between the nodes.

References

1. Li F, Wang Y (2007) Routing in vehicular ad hoc networks: a survey. IEEE Mag Vehicular Technol 2(2):12–22
2. Lin CR and Gerla M (1997) Adaptive clustering for mobile wireless networks. *IEEE J Sel Areas Commun* 15(7):1265–1275
3. Fiore M and Härri J (2008) The networking shape of vehicular mobility. In: Proceedings of the ACM international symposium on mobile ad hoc networking and computing (MobiHoc '08), New York, ACM, pp 261–272
4. Wang Z, Liu L, Zhou M, Ansari N (2008) A position-based clustering technique for ad hoc intervehicle communication. IEEE Trans Syst Man Cybern C: Appl Rev 38(2):201–208
5. Bononi L, Felice MD (2007) A cross layered MAC and clustering scheme for efficient broadcast in VANETs. In: IEEE internatonal conference on mobile adhoc and sensor systems (MASS 2007), Montreal, QC October 2007, pp 1–8
6. Panichpapiboon S, Ferrari G (2008) Irresponsbile forwarding. In: *Proceedings of the IEEE, 8th international conference on intelligent transport system telecommuniction* (ITST'08). Phuket, Thailand, October 2008, pp 311–316
7. Insitute of Electrical and Electronics Engineers (2007) IEEE Std 802.11TM-2007. Part 11: wireless LAN medium access ontrol (MAC) and physical layer (PHY) specifications
8. Busanelli S, Ferrari G, Panichpapiboon S (2009) Efficient Broadcasting in (IEEE) 802.11 Networks through Irresponsible Forwarding. Proc. IEEE Global Telecommun. Conf. (GLOBECOM), Honolulu, HI, USA, October 2009
9. Ni S, Tseng Y, Chen Y, Sheu J (1999) The broadcast storm problem in a mobile ad hoc network. In: Proceedings of the ACM international conference on mobile computing and networking (MOBICOM), Seattle, WA, pp 151–162
10. Network Simulator 2 (ns-2). [Online]. Available: http://isi.edu/nsnam/ns/
11. Rappaport TS (2002) Wireless communications. In: Principles & Practice, 2nd edn. Prentice-Hall, Upper Saddle River, NJ
12. Biswas S, Tatchikou R, Dion F (2006) Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. IEEE Commun Mag 44(1):74–82
13. Torrent-Moreno M, Mittag J, Santi P, Hartenstein H (2009) Vehicle-to-Vehicle Communication: Fair Transmit Power Control for Safety-Critical Information. IEEE Trans. Veh. Technol, September 2009, 58(7):3684–3707