ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 2009. No. 8(96)
ELEKTRONIKA IR ELEKTROTECHNIKA

TELECOMMUNICATIONS ENGINEERING
T 180
TELEKOMUNIKACIJŲ INŽINERIJA

Inter-Vehicle Communication: Emergency Message Delay Distributions

A. Kajackas, A. Vindašius, Š. Stanaitis
Telecommunications Engineering Department, Vilnius Gediminas Technical University,
Naugarduko str. 41, LT-03227 Vilnius, Lithuania, e-mail: algimantas.kajackas@el.vgtu.lt, antanas.vindasius@el.vgtu.lt, sarunas.stanaitis@gmail.com

Introduction

Road accidents and traffic jams are two most important problems on the roads. Most road accidents happen because of human error and could be avoided if drivers would be informed about the accident ahead at least several seconds before. Traffic jams could be decreased if traffic management organizations could receive detailed information about vehicles and their destinations and advise the driver to take alternative routes.

The answer for the mentioned problems above is inter-vehicle communication – wireless access in vehicular environments (WAVE). Recently WAVE is attracting much attention from industry and academia. The base for WAVE is IEEE 802.11p standard draft, which together with IEEE 1609.1/2/3/4 describes inter-vehicle communication. IEEE 802.11p amendment is intended for highly mobile vehicular environments with fast moving nodes. Communication mode is also different from usual Wi-Fi. In 802.11p not just different radio channels are defined, but also there is time division into two time channel slots: control channel (CCH) and service channel (SCH). Synchronization of CCH and SCH is done using Global Positioning Systems (GPS) receiver's universal time clock (UTC) signals.

Using inter-vehicle communication the car suffering from accident or the car passing the accident is sending warning messages. There are several communication scenarios and one of them is multi-hop communication, where information travels from accident place to the cars which will cross it. This information routing is called geounicast, because information is sent to the relevant cars using travel path and current coordinates from GPS.

The most important task for the emergency warning system is to deliver warning messages on time. There can be several warning message types, but sudden brake or crash in front warning messages have to be delivered soonest. To calculate the permissible delivery time we refer to the recommendation to drivers to keep the distance from the front car same as half of the cars speed, which brings time between vehicles positions equal to 1.8 s. That means that after the crash in 1.8 s the following car should stop. The average reaction time of the drivers to accidents on the road is 1.8 s. Warning messages should arrive to the destinations faster than 1.8 s (how much faster should be answered by doing investigation on driver reaction to emergency warnings in the car). This principle is used by analyzing simulation results.

In this paper we analyze the delay values of multi-hop link, based on legacy IEEE 802.11 and emerging IEEE 802.11p standard. The results, obtained from simulations in NCTUns 5.0 environment, show delay distributions of emergency messages, broadcasted in multi-hop manner.

Related Work

Multi-hop chain research is presented in [1] and is based on experiments with real cars using IEEE 802.11b technology. Different scenarios have been tested and results analyzed. Using 3 and 6 cars in the multi-hop chain is shown influence of hop count. Authors concludes, that multi-hop chain suites the needs of VANET. Though optimistic results, there are no hints to IEEE 802.11p, which differs from IEEE 802.11b. There were no background traffic generated, which influence the performance of network.

Packet delay in legacy IEEE 802.11 is analyzed in [2]. Two transmission scenarios are presented: single-hop and multi-hop. Theoretical curves are compared with simulated. Therefore, there are some differences from inter-vehicle communication. The received packets are acknowledged, which is not the case in WAVE, where information is broadcasted.

Information dissemination in the network should be considered by building up the WAVE communication scenarios. A unified approach for disseminating data about different types of events in a vehicle network is presented in [3]. This approach is not concentrating to a specific type of information, but it is unified approach based on encounter probability calculation, which gives a reason for simulated network described in this paper.

Two MAC methods have been evaluated according to their ability to meet real-time deadlines in [4]. IEEE 802.11p carrier sense multiple access (CSMA) was examined through simulation and conclusion was made, that CSMA is unsuitable for real-time data traffic. The

second evaluated algorithm self-organizing time division multiple access (STDMA) will always grant channel access regardless of the number of competing nodes. Regardless the results of [4], we show that standard CSMA suits the needs of WAVE (real-time deadlines is important, but we show, that the time limits are quite high for emergency messages to be transferred).

GeoMAC protocol, presented in [5], exploits spatial diversity, inherent in a vehicular channel. Forwarder selection for transmission over the next hop is enabled in a distributed manner via geobackoff, which selects forwarders in decreasing order of spatial progress. Simulated network consists just of one hop chain, which does not answer to real life situation, but gives a clear overview of the possibilities of GeoMAC.

IEEE 802.11p

The upcoming IEEE 802.11p standard PHY has some differences of other IEEE 802.11a/b/g standards. As stated in [4], IEEE 802.11p will make use of the PHY supplement IEEE 802.11a and the MAC layer QoS amendment from IEEE 802.11e. WAVE PHY uses Orthogonal Frequency Division Multiplexing (OFDM). Radio frequency is similar to IEEE 802.11a and is allocated from 5.85 to 5.925 GHz into several 10 and 5 MHz channels. For USA communication channels are already defined and can be found in IEEE 802.11p standard and for Europe channel allocation is still in progress.

WAVE MAC is also specific and is described in IEEE 1609.4 standard. There is timing allocation of channels. Control Channel (CCH) is defined for emergency message transmission and for service advertisement and Service Channel (SCH) is responsible for all other information transmission. In the CCH time frame all stations should stop transmission and listen to this channel and receive/transmit emergency messages. During SCH channel time frame stations can use all other radio channels to transmit all types of information. Channels are divided into 50 ms frames. Time synchronization of channels is done using GPS universal time clock (UTC) signal. Emergency messages are sent by using WAVE Short Message Protocol (WSMP) described in IEEE 1609.3 standard.

The communicating nodes in VANET are moving fast and they should be ready for transmission as soon as possible. The WAVE Basic Service Set (WBSS) provider first transmits WAVE Announcement action frames, for which the WBSS users listen. That frame contains all information necessary to join a WBSS. Unlike infrastructure and ad-hoc 802.11 BSS types, the WAVE users do not perform authentication and association procedures before participating in the WBSS. To join the WBSS, only configuring according to the WAVE Announcement action frame is required. In addition, a node in WAVE mode shall generate a Clear Channel Assessment (CCA) report in response to a CCA request to know the time-varying channel state precisely.

Simulation Scenario and Initial Assumptions

Scenario of 5 lanes highway (Fig. 1) is used in this research. Following the idea of [4], that vehicle velocity is different in different lanes, following velocities are used: 19.4 m/s (70 km/h), 25 m/s (90 km/h), 30.5 m/s (110 km/h), 36.1 m/s (130 km/h) and 41.6 m/s (150 km/h).

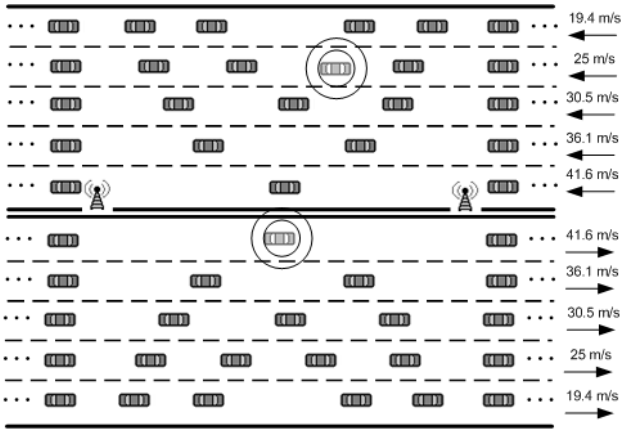

Fig. 1. Highway scenario (5 lanes)

According to described conditions there are ~100 vehicles in one communication range and this number is reflected in the simulation.

Simulations were performed in NCTUns 5.0 network simulation tool [6] under Linux Fedora Core 9 OS. NCTUns was chosen for its advanced IEEE 802.11 model library and ability to integrate with any Linux networking tools.

With the simulations we intend to investigate the delays experienced by the multi-hop link in vehicle ad-hoc scenarios. All simulations are based on IEEE 802.11a PHY and MAC, however the inferences about 11p performance can be drawn as well, since the contention mechanism is the same. In our scenarios only one type (priority) emergency message transmission is simulated, no other non-critical data transmissions are used; therefore the behavior of IEEE 802.11a and IEEE 802.11p/IEEE 1609 is very similar. WSM transmission method is broadcasting, which does not require acknowledgements. WSMs in IEEE 802.11p/IEEE 1609 case may be transmitted in both CCH and SCH using legacy CSMA/CA. Thus, considering contention only between emergency messages, the results are valid both for legacy IEEE 802.11a and IEEE 802.11p/IEEE 1609.

The delays, introduced by CSMA/CA, theoretically can be evaluated by time expenditures calculation [7]. EDCA access mechanism is used for uncoordinated transmission [8]. In this case, time required to send the packet consists of actual packet transmission duration, inter-frame times and medium access delay:

$$t_{exp} = t_{AIFS} + \text{rand}(CW) \cdot t_{slot} + t_{packet}, \quad (1)$$

where t_{exp} represents total time expenditures for one packet transmission, t_{AIFS} – time required for Distributed Inter Frame Space ($t_{\text{AIFS}} = 9 \cdot t_{\text{slot}}$ for IEEE 802.11e AC0), CW –

Contention Window, t_{slot} – slot time (t_{slot} = 9 μs for OFDM, IEEE 802.11a), t_{packet} – time required for data and overhead transmission consisting of preamble, 30-byte MAC header transmission time – t_{MAC} and 4-byte Frame Check Sequence – t_{FCS}:

$$t_{packet} = t_{PLCP} + t_{MAC} + t_{MSDU} + t_{FCS}. \quad (2)$$

Since no acknowledgement is required for broadcasting, no other expenditures take place.

Contention window defines the set of possible delays for back-off algorithm. Every collision in wireless channel results congestion window to double, shifting from minimum value of CW_{min} = 15 to maximum of CW_{max} = 1023 slots for AC0 access category.

IEEE 802.11a PHY was modified to support IEEE 802.11p PHY rates. In simulations we use the lowest possible - 3 Mbps PHY rate. Lowest modulation gives the best reliability and transmission range. Considering always changing radio environment on the roads due to unexpected obstacles (large vehicles, blocking the signal, rapid fading due to movement, etc.), the ability to use higher modulations is unpredictable and may lead to failure of transmission, thus the simulations are designed for worst-case radio transmission scenario. However, the presented results can be theoretically recalculated for any other PHY rate.

Emergency messages are simulated as 500 byte UDP packets. Following the idea of [4], packet length of 100 bytes is just long enough to distribute the position, direction and speed, but due to security overhead, the packets are likely longer. According to that, packet length of 500 bytes is chosen. Messages are routed through the network using IPv4. Since no movement is simulated whatsoever, we use static routes to make controllable transmission through hops. Because all simulations are generally done on IP network, the initial TTL value is modified to make hopping through large number (greater than 64) of hops possible.

All the transmissions in the simulated network use layer 2 broadcasting.

Theoretically, using PHY rate of 3 Mbps and 500 byte payload (plus 8 byte UDP header, 20 byte IPv4 header and 8 byte LLC to form single MSDU), according to formulas 1 and 2, time expenditures for single emergency message delivery can vary from 1,621 ms to 1,756 ms if no collisions effect contention window and wireless medium is always free to access. With more hops, the variation is higher.

Single Emergency Message Transmission Simulation

First scenario (Fig. 2) simulates single emergency message transmission through multi-hop chain. All nodes are located within radio transmission range and operating in the same radio channel, therefore they share the channel with equal rights. Since all the packets are being transmitted as broadcasts, they are received by all stations and not acknowledged. To control the "hopping" to one direction and to avoid broadcast storms, we filter packet forwarding and route them hop-by-hop.

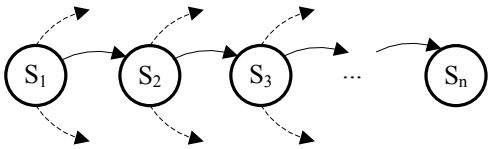

Fig. 2. Single emergency message transmission through multi-hop chain

The delay was measured at every node and delay distributions are presented in Fig. 3. The mean delay for 100 hops reaches 189.3 ms, minimum and maximum values respectively 184.4 ms and 194.0 ms. The delay and delay fluctuations are relatively small due to low channel utilization. There is only one packet in the system at any given moment, therefore no contention takes place.

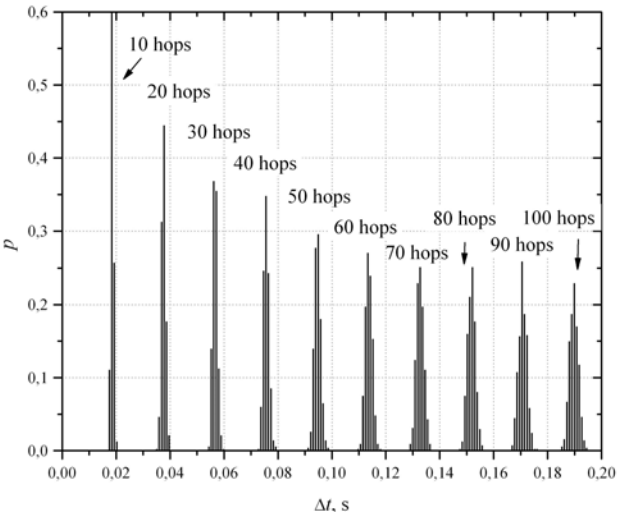

Fig. 3. Delay rate distributions for different hop number

However, this scenario is not realistic in VANETs and is presented to give understanding of transmission delays in perfectly controlled environment and to evaluate the minimal influence of MAC layer and physical transmission of signals. This scenario can be considered as a worst-case for reliability and a best-case for traffic load.

Another set of simulations demonstrates how channel utilization influences the delay spread.

There are many investigations on efficient message broadcasting, and for the simulations we take into account, that data dissemination with broadcasts can be controlled in the network [6 – 8].

Our presented simulations are broadcasting solution independent and may be used to evaluate solution influence on transmission delay over different number of hops. The concept of "background traffic" has to be understood as an overhead, created by broadcasting method. Network topology remains the same, but more traffic is introduced into network as background traffic along with emergency message stream. Background traffic is generated by neighboring nodes on the same radio channel and has the same characteristics as measured (emergency message) traffic.

One of the problems in emergency message transmission in VANETs is reliable and at the same time efficient and robust broadcasting. Inevitably it has to have significant overhead to ensure guaranteed reception. On

the other hand, the overhead has to be reduced in order not to over utilize the radio channel, which will eventually lead to reception failures or extreme reception delays. Guaranteed reception can be achieved by acknowledging, however the messages have to spread fast, therefore there is no time for seeking best route in node mesh or confirming the reception. Broadcast messages cannot be acknowledged, thus the reliability has to be ensured by repeated broadcasts and neighbor retransmissions. This way the channel can be easily flooded with broadcasts degrading network performance with excessive delays.

Fig. 4 shows delay distributions for different number of hops when light background traffic of 100 kbps has been applied. The delays are more spread and shifted, however the influence is relatively small due to low channel utilization: for 100 hops the mean delay increases by 12 ms and maximum delay – by nearly 30 ms. By increasing the background traffic further, delay distributions shift and spread more.

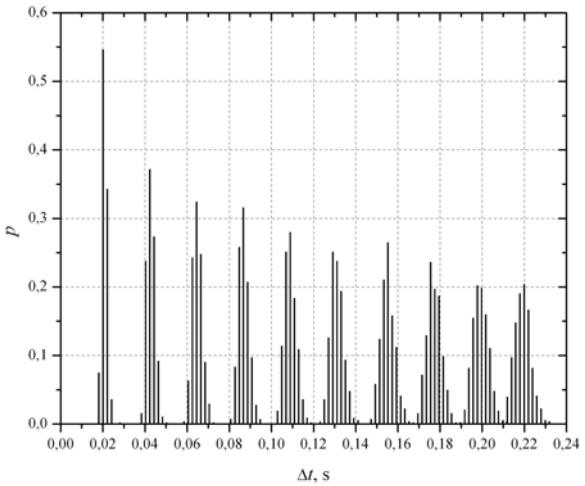

Fig. 4. Delay rate distributions for different hop number with 100 kbps background traffic

Fig. 5 shows delay distributions with 1 Mbps background traffic and Fig. 6 – with 2 Mbps background traffic. Those graphs do not include lost packets. With significant background traffic, the contention for transmission becomes harsh and collision probability increases causing packet loss. Since broadcast packets are never acknowledged, lost packets are not resent and hopping through node chain brakes. Fig. 7 shows the probability for packet to survive different number of hops.

The summary of results for 100 hops is presented in table 1. It is shown, that by increasing background traffic the mean delay is growing proportional, but standard deviation is increasing. This means, that with growing background traffic the delay can vary in wider time range.

Table 1. Results summary for 100 hops

Back-ground traffic, kbps	Mean delay, s	Minimum delay, s	Maximum delay, s	Standard deviation
0	0,189	0,184	0,194	0,00173
100	0,218	0,209	0,230	0,00383
1000	0,386	0,355	0,411	0,00839
2000	0,523	0,458	0,603	0,03083

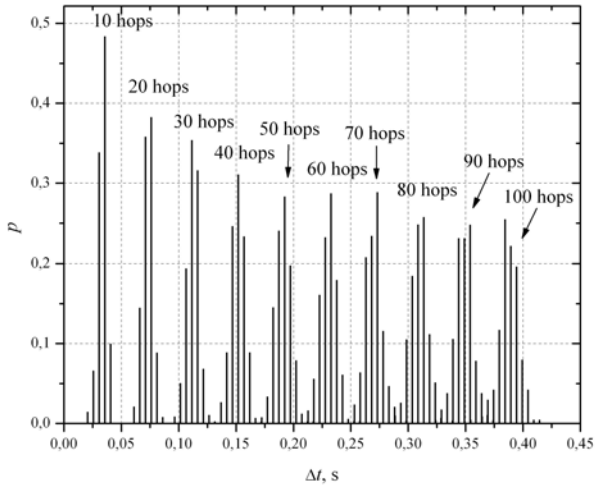

Fig. 5. Delay rate distributions with 1 Mbps background traffic

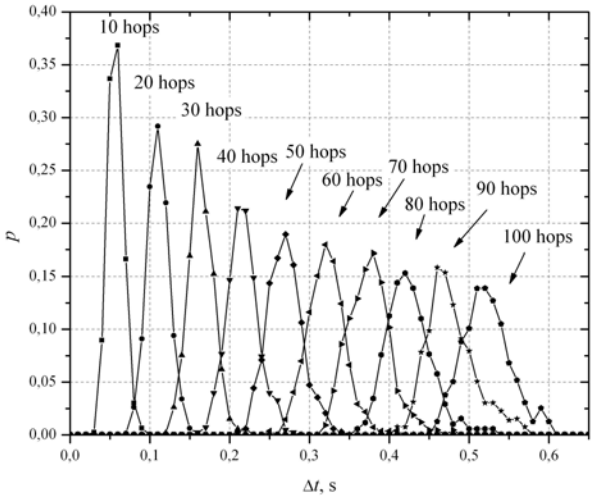

Fig. 6. Delay rate distributions with 2 Mbps background traffic

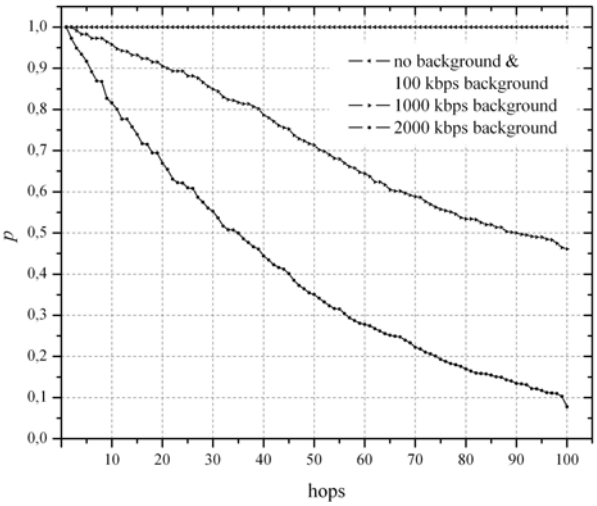

Fig. 7. Packet survive probability for different hop number

Controlled Flood Scenario

One of the ways to improve reliability of multi-hop links is to make redundant paths to every node of the network. Flooding the network with broadcasts may seem the reliable way to ensure message reception for every network node. Since the transmit range is not always

known due to ever-changing environment, every node in the network has to retransmit (rebroadcast) emergency message assuming that it may be at the transmission range edge of the message initiator. For this scenario an algorithm, controlling the floods must be employed, otherwise packet loops will cause broadcast storms (similarly as in looped Ethernet) which eventually will lead to channel congestion. One of the ways to avoid loops could be GPS coordinate tracking and making sure, that broadcasts are being forwarded only in one direction (similar as in [5]). This can be tricky considering vehicle movement. Another simple way – logging retransmitted node IDs: all nodes, retransmitting broadcast packets, put their ID into the frame body; before resending received packet, node always searches this ID list; if own ID is found, the packet is dropped assuming it is in the transmission loop.

We implement this controlled flood scenario in NCTUns 5.0 using same nodes and traffic characteristics as defined in previous chapter. The network topology is depicted in Fig. 8.

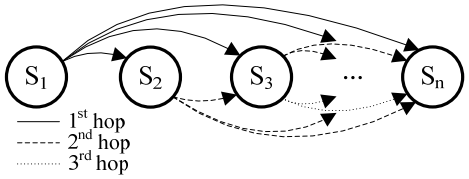

Fig. 8. Controlled flood scenario

S_1 is the originator of emergency message, which is broadcasted through the network. Every other node broadcasts the same message again following basic rule: if source ID is lower than own ID, then message should be broadcasted. Otherwise – received packets have to be dropped.

This way the network is flooded with the message copies, but no broadcast loops appear. This scenario can be considered as a worst-case for traffic load and a best-case for reliability.

Delay distributions for 10 and 20 hops scenario are presented in Fig. 9 and Fig. 10. The delays were measured at every node.

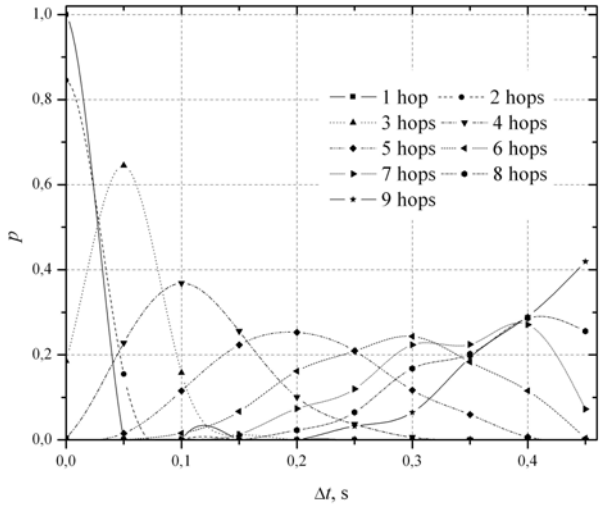

Fig. 9. Delay rate distributions in 10-node controlled flooded scenario

Since the broadcasts from any node are received by all other nodes and retransmitted by all with the ID higher than source ID, increasing node (hop) number, the packet copies in the system grows exponentially. It can be seen (Fig. 9, Fig. 10), that 10 node scenario shows quite reasonable delays, reaching 500 ms for all 9 hops, however doubling node number in the scenario results in excessive delay increase, mean value reaching almost 4 seconds for 9 hops and 7 seconds for 19 hops.

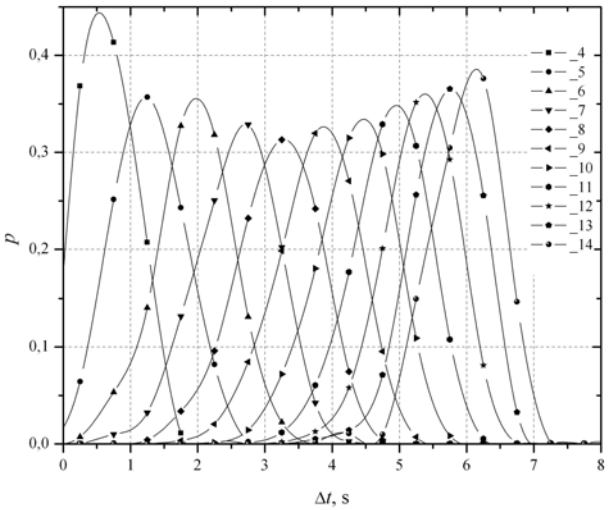

Fig. 10. Delay rate distributions in 20-node controlled flooded scenario

Results Overview

Permissible delay for the first car line (closest to accident place), is less than 1.8 s. This time is the reference for result analysis.

There is just one packet in the multi-hop chain in single message transmission simulation scenario. In this scenario, even with a big background traffic (2 Mbps) the maximal delay is 0.6 s, witch is in permissible range – less than 1.8 s.

Analyzing controlled flood scenario simulation results, delay up to 7 s is found. The results for 10 nodes chain (Fig. 9) can come up to 0.5 s and are satisfying the permissible delay. But for the 20 node chain (Fig. 10), the delay can come up to 7 s. Analyzing Fig.10 can be seen, that just communication path of 4 nodes satisfies the permissible delay. This means, that for the 20 nodes scenario the first car, following crashed car, should get the emergency warning maximum after 4 nodes in multi-hop chain. If the car after accident is in the second row, the permissible time grows up to 3.6 s. This means, that second car can get the emergency message from the chain of maximum 7 nodes.

Conclusions

The delay in IEEE 802.11 multi-hop transmission depends on following major components: physical signal transmission, which depends on PHY rate and distance; and contention, which depends on channel utilization. The problematic of emergency message transmission is two-

fold: transmission has to be reliable and transmission delays have to stay in strict limits.

Presented three sets of simulations show the emergency message delay dependency on hop count in channel utilization best-case, delay dependencies on different loads and reliability best-case.

Simulations show, that single message propagation is in permissible range even for 100 nodes. For controlled flood scenario node number increases delay exponentially. Therefore growing node number influences the delay time and the chain for emergency message transmission is getting smaller to satisfy the permissible delay results. Communication chain length is also dependent on the car position from the accident place.

Message broadcasting methodology has to be chosen carefully, taking into account the traffic overhead. We illustrate this problem with controlled flooding scenario.

References

1. **Jerbi M., Senouci S. M.** Characterizing Multi–Hop Communication in Vehicular Networks // IEEE Wireless Communications and Networking Conference, WCNC 2008. – P. 3309–3313.
2. **Khalaf R., Rubin I.** Throughput and Delay Analysis in Single Hop and Multihop IEEE 802.11 Networks // Broadband Communications, Networks and Systems, 2006, BROADNETS 2006. – P. 1–9.
3. **Cenerario N., Delot T., Ilarri S.** Dissemination of information in inter–vehicle ad hoc networks // IEEE Intelligent Vehicles Symposium, 2008. – P. 736–768.
4. **Bilstrup K., Uhlemann E., Strom E. G., Bilstrup U.** On the Ability of the 802.11p MAC Method and STDMA to Support Real–Time Vehicle–to–Vehicle Communication // EURASIP Journal on Wireless Communications and Networking. – Vol. 2009, Article ID 902414, 13 pages, 2009.
5. **Kaul S., Gruteser M., Onishi R., Vuyyuru R.** GeoMAC: Geo–backoff based co–operative MAC for V2V networks // IEEE International Conference – Vehicular Electronics and Safety, 2008. – ICVES 2008, – P. 334–339.
6. **Wang S. Y., Lin C.C.** NCTUns 5.0: A Network Simulator for IEEE 802.11(p) and 1609 Wireless Vehicular Network Researches // Vehicular Technology Conference, 2008, VTC 2008. –Fall, – P. 1–2.
7. **Kajackas A., Pavilanskas L.** Analysis of the Connection Level Technological Expenditures of Common WLAN Models // Electronics and Electrical Engineering, 2007. – No. 2(74). – P. 63–68.
8. **Kajackas, A.; Vindašius, A.** Applying IEEE 802.11e for Real–Time Services // Electronics and Electrical Engineering, 2009. – No. 1(89). – P. 73–78.

Received 2009 05 14

A. Kajackas, A. Vindašius, Š. Stanaitis. Inter-Vehicle Communication: Emergency Message Delay Distributions // Electronics and Electrical Engineering. – Kaunas: Technologija, 2009. – No. 8(96). – P. 33–38.

Road accidents and traffic jams are most important problems on the roads. To decrease the mentioned problems wireless inter-vehicle communication – WAVE can be used. The nearby cars send the emergency warning messages about their actions. In this paper, using NCTUns 5.0 environment, are analyzed the delay values of emergency message transmission in multi-hop link, based on legacy IEEE 802.11 and emerging IEEE 802.11p standard. Simulations show, that single message propagation is in permissible range even for 100 nodes. For controlled flood scenario node number increases delay exponentially. Ill. 10, bibl. 8, tabl. 1 (in English; abstracts in English, Russian and Lithuanian).

А. Каяцкас, А. Виндашюс, Ш. Станайтис. Связь между автомобилями: распределение времен передачи аварийных сообщений // Электроника и электротехника. – Каунас: Технология, 2009. – № 8(96). – С. 33–38.

Аварии и последующие столкновения автомобилей на дорогах – нерешенные актуальные проблемы**.** Для предупреждения водителей и предотвращения аварийных ситуаций между автомобилями могут быть применены средства радиосвязи – WAVE**.** В такой системе автомобиль, оказавшись в аварийной ситуации, посылает сообщение тревоги**.** Все другие автомобили, приняв сообщение тревоги, его ретранслируют**.** В настоящей статье представлен анализ времен задержки, возникающих при многократной ретрансляции, с применением сетей стандартов IEEE 802.11 и IEEE 802.11p**.** Анализ произведен путем моделирования с применением пакета NCTUns 5.0**.** Результаты моделирования подтверждают гипотезу о возможности предотвращения столкновения автомобилей путем передачи сообщений тревоги по цепи вплоть до 100 станций**.** Если по той же сети станций передаются и другие сообщения, то задержки в цепи возрастают экспоненциально с ростом числа станций. Ил. 10, библ. 8, табл. 1 (на английском языке; рефераты на английском, русском и литовском яз.).

A. Kajackas, A. Vindašius, Š. Stanaitis. Ryšys tarp automobilių: pavojaus pranešimų vėlinimų pasiskirstymas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2009. – Nr. 8(96). – P. 33–38.

Avarijos ir spūstys yra pagrindinės kelių eismo problemos. Siekiant sumažinti šių problemų sukeltas pasekmes gali būti panaudotas ryšys tarp automobilių – WAVE. Greta esantys automobiliai vieni kitiems siunčia pavojaus pranešimus apie savo veiksmus. Šiame straipsnyje, naudojant NCTUns 5.0 modeliavimo aplinką, yra išanalizuoti pavojaus pranešimų perdavimai daugelio šuolių grandine (angl. *multi-hop*), remiantis įprastiniu IEEE 802.11 ir naujai kuriamu IEEE 802.11p standartais. Modeliavimo rezultatai patvirtina hipotezę, kad automobilių susidūrimų galima išvengti perduodant pavojaus pranešimus iki 100 stočių grandine. Jei kuriuo nors stočių tinklu perduodami ir kiti pranešimai, vėlinimas grandinėje eksponentiškai padidėja didėjant stočių skaičiui. Il. 10, bibl. 8, lent. 1 (anglų kalba; santraukos anglų, rusų ir lietuvių k.).

DOI: 10.5755/j02.eie.9956