社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－MBL－35（14）
2005－ITS －23（14）
2005／11／17

Analysis of Characteristics of Flooding for Inter-Vehicle Communications

Peter Davis, Satoko Itaya, Jun Hasegawa, Akio Hasegawa, Naoto Kadowaki, Akira Yamaguchi, Sadao Obana
ATR Adaptive Communications Research Laboratories
2-2-2 Hikaridai, Keihanna Science City, Kyoto 619-0288

Abstract:
We analyse the characteristics of wireless packet broadcast using multi-hop relay to reach nodes which are not within direct radio range of the broadcast source. In particular, we report that in an experimental system using over 50 personal computing devices equipped with standard wireless modules and multi-hop relay software, flooding of packets containing 140 bytes of data over 5 hops was possible within 20 milliseconds. This demonstrates that flooding is a promising way to share real-time information among a large number of mobile vehicles.

車車間アドホック通信のためのフラディング特性の解析

デイビス・ピーター，板谷聡子，長谷川淳，長谷川晃朗，門脇直人，山口明，小花貞夫
ＡＴＲ適応コミュニケーション研究所
〒619-0288 **けいはんな学研都市光台** 2-2-2

概要：
安全運転のための緊急情報などをすばやく共有するために，車車間の通信を直接アドホック無線通信で行うシステムが検討されている．本稿では，フラッディング方式を用いた情報配信の特性について報告する． 具体的には，５０ノードのアドホックテストベッド実験において１４０バイトのデータを２０ミリ秒で配信することが可能であることを示す．

Introduction

Inter-vehicle communications have great potential for improving driving safety and convenience by allowing vehicles to share information about their driving environment. Ad hoc wireless communications directly between vehicles is an attractive method of communication as it does not require roadside infrastructure to relay packets and can avoid bottlenecks associated with concentration of traffic at roadside access points. By adding a packet relay function to the wireless communication modules on each vehicle, it becomes possible for vehicles to relay the packets of other vehicles so that communication is possible even between vehicles which are not close enough for direct transmissions.

It is expected that communication between cars will support many applications, including access to the internet and various information services. Some of these communications will require sending specific messages or data to specific destinations. On the other hand, for some other applications it will be necessary to broadcast the same information to many vehicles. For example, a core scenario for vehicle safety is sharing information about position and velocity. This allows vehicles to be aware of approaching vehicles and other road hazards. Another scenario is propagation of warning signals, for example generated by a vehicle braking suddenly or crashing. In each of these scenarios, it is necessary to broadcast the same information to many nodes. Moreover, due to the limited range or poor coverage of direct transmissions, it is useful for vehicles to re-transmit the broadcast packets that they receive, so the packets can propagate to all vehicles in the network. This mode of wireless communication is called flooding [1-6].

In this paper we evaluate the performance of flooding in a real-world network using standard IEEE 802.11 WLAN modules [7]. The 802.11 incorporates an ad hoc mode of communication which allows direct wireless communication between close terminals, within tens to hundreds of meters depending on the propagation environment. 802.11 is now increasing popular as a wireless access system.

Hence it is natural to consider the ad hoc mode of IEEE 802.11 as a candidate for standard inter-vehicle communications. One new version of 802.11, known as 802.11p which is being considered in IEEE for intelligent vehicle systems, specifies a control channel with usage guidelines to prevent degradation of performance due to congestion. However, all versions of 802.11 are based on CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance) which itself has no explicit restrictions on the number of nodes trying to access the medium, and hence only has probabilistic guarantees on performance.

From the point of view of vehicle safety, it is important to know how long it takes for packets to disseminate to neighbors, and what is the reliability of the packet delivery - for example the likelihood of a packet being delivered to all nodes within a certain distance. To examine these issues using practical equipment, we implemented a flooding application using standard 802.11 WLAN modules on a large number of PCs and PDAs in an experimental network test-bed.

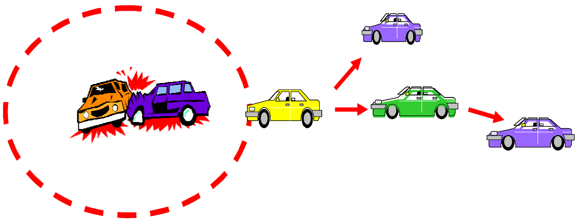

Figure 1. Roadway communication scenario using multi-hop packet relay

Reference Scenario

Figure 1 shows an example of a roadway communication scenario which uses multi-hop relay of broadcast packets, that is flooding. In an emergency situation, a vehicle broadcasts a packet containing its own state information. This information may have various priorities. For example, position, velocity, brake information will have high priority, and various other application information, such as the offer of an on-board camera service, will be of lower priority. Nearby vehicles re-transmit some or all of the broadcast packets so the information can propagate to other vehicles which are not within range of the source vehicle.

Figure 2 shows a typical procedure for relaying a flooding packet. In so-called "pure flooding", each node re-transmits just once any flooding packet that it receives. To avoid loops, it is essential to check for packet duplication. Checks on the number of hops or TTL to restrict the range or time of propagation may also be useful in large systems. Filtering or priority relay scheduling can also be implemented.

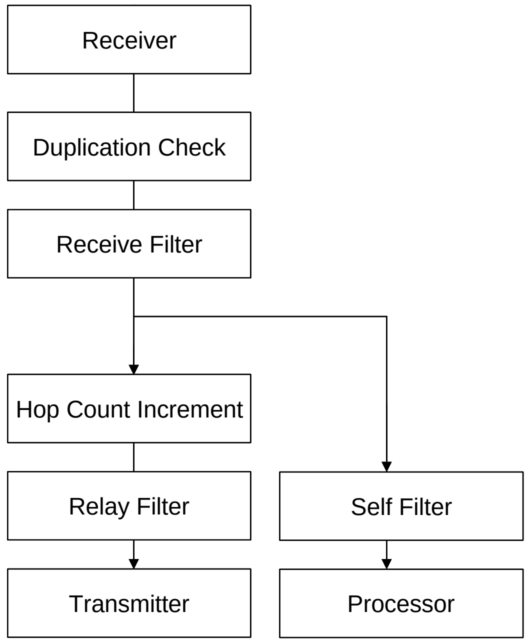

Figure 2. Procedure for Packet Relay for Flooding

Related Work

The issue of fast packet delivery in ad hoc networks was previously studied by Itaya *et al*, who compared the speed and reliability of unicast and broadcast methods when sharing information among many nodes using 802.11 [8-11]. Unicast requires a separate transmission to each neighbor. Broadcast on the other hand is received by all nodes within range of the transmission. Itaya *et al* showed that for more than ten nodes, faster and more reliable distribution could be obtained by broadcast that by unicast.

As for multi-hop flooding, a large number of theoretical studies have been reported [1-6]. For example, the paper by Ni *et al* provides a review of flooding methods and their relative merits [2]. In particular, this paper reviews the issue of "broadcast storm", whereby the relay of packets by a large number of neighbor nodes leads to an increase of traffic which saturates the available transport capacity.

In contrast to the large number of theoretical studies, few implementations of flooding have been reported. Kosuga *et al* developed the "Coconut" software platform for ad hoc networking based on flooding [13-14]. They focused on distribution of presence information and service discovery. Poupyrev *et al* used the Coconut platform to test the time required for mutual distribution of presence information [15]. This work focused on adjusting the rate of packet generation to maintain scalability of applications on the time scale of seconds to minutes in very large systems.

Table 1. Transmission times for 192 Byte packets using 802.11

802.11	Raw delay (DIFS+Preamble)	Total Transmission Time (192 Bytes)	
		Broadcast	Unicast
a	**112us** DIFS=34us Preamble=78us (Slot=9us)	**0.37 msec**	**0.24 msec**
b	**242us** DIFS=50us, Preamble=192us (Slot=20us)	**1.0 msec**	**0.63 msec**
g	**242us** DIFS=50us, Preamble=192us (Slot=20us)	**1.0 msec**	**0.48 msec**

Estimates of Delivery Time and Reliability

In this section we provide more detailed specifications of our model system and a rough theoretical estimates of performance. As a basic case, we assume one vehicle generates a single packet and consider the propagation of this information throughout the system.

First, let us consider the time required to transmit UDP broadcast packets. To be specific, we consider packets of 192 Bytes, which corresponds to 140 Bytes of data with UDP, IP and MAC headers. The minimum time required to transmit a single packet using 802.11 can be estimated from the 802.11 specifications [7] as shown in Table 1. It can be seen that the minimum time to transmit a 192 byte packet using 802.11b is 1 ms. As each node relays the packet just once, the maximum time to flood the whole network is simply proportional to the number of nodes. Hence, a rough estimate of the delivery time can be obtained as

$$T = n \times 1\ ms, \qquad (1)$$

where n is the total number of nodes in the system. Since some of the relay transmissions will take place simultaneously, the actual effective time could be less than this value. On the other hand, packets which are transmitted simultaneously may collide destructively at some receivers, and so not be received there. Note that many packet transmissions will be redundant as it is sufficient that each node received just one copy of each packet generated by the source. However, without specific topology information, it is impossible to know which packet transmissions are redundant. Hence, we can usually only expect a statistical tradeoff between reliability and dissemination time.

Now, let us consider the packet loss due to collisions between packets relayed by different nodes at the same time. Due to the carrier sense mechanism, the re-transmissions become highly synchronized. If the medium is not-idle when the nodes are ready-to re-transmit, they choose a random slot number and may till the medium becomes idle. Let the number of slots be m and the number of relay nodes be k. Let the independent packet success ratio be g. Then the probability of success is:

$$P_{success} = g.k(1-1/m)^{(k-1)} \qquad (2)$$

Note that this success probability initially increases with k but then decreases with k for large k. This decrease with large k due to collisions by the large number of highly synchronous re-transmissions is known as the “broadcast storm” problem. In 802.11 implementations the number m for broadcast packets is typically fixed at $m=32$. The optimal success ratio is obtained for $m \sim n$. If m could be changed adaptively, so $m \sim k$, then high success ratio could be maintained, but the time taken to complete the transmissions would also increase proportionally.

On the basis of this analysis, we can say that to optimize the reliability of delivery, relay density of more than $m=32$ nodes should be avoided. If the channel is shared with other traffic, the density should be reduced further. One way to reduce relay density is to introduce constraints which prevent all nodes from re-broadcasting. This can be done with a number of different filtering methods, either deterministic or stochastic [2, 16].

Experimental Tests

We implemented flooding on a set of Linux PC and measured propagation characteristics. Details of the system are as follows. The PC operated with Red Hat Linux 9 (Kernel version 2.4.25). The WLAN card was an 802.11b card (either the Planex

GW-CF11H, or BUFFALO WLI-PCM-L11GP) with Orinoco_cs0.13d driver. Data packets are transmitted as UDP broadcast packets, typically at 2Mbps. The 802.11 modules all have the same ESSID and default channel, and they do not use the sleep option, so no association or synchronization is necessary before the nodes are ready to receive broadcast packets. Packets containing *140* Bytes of data were generated at a single source at *5* sec intervals. (Data packets consisted of user data 100 Bytes, Route Info 40 Bytes, IP header 20 Bytes, UDP header 8 Bytes, MAC header 24 Bytes) In our test-bed the maximum number of nodes is *50* nodes. Nodes were positioned so as to have a density of more than *10* nodes.

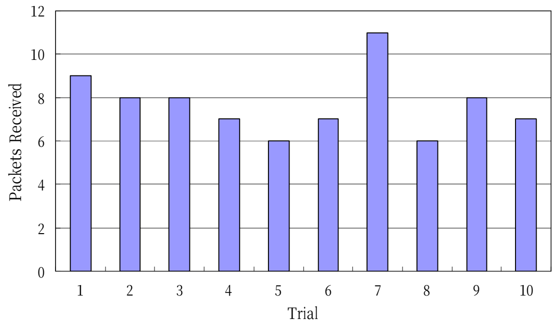

Figure 3. Number of Received Packets
(10 relay nodes, single relay)

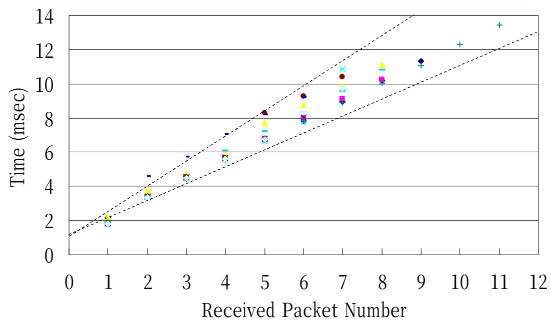

Figure 4. Relay Times
(10 relay nodes, single relay)

We tested two types of flooding implementations. Flooding-1 is pure flooding implemented as IP routing. Flooding-2 is implemented at a higher layer as application middleware. It allows more versatile manipulation of the flooding contents, including various content filter operations.

First, we consider the performance of Flooding-1. Figure 3 shows the the number of packets received by a single node in a cluster of 10 nodes which are all within range of the source node. The figure shows the results for 10 successive trials ie. when the source emits 10 packets in succession, at 5 sec intervals. The maximum number of packets expected is *11* – the first packet plus *10* relay packets. The average number of packets received is consistent with Eqn. 1 which includes losses due to accidental collision.

Figure 4 shows the times of transmissions for each relay packet. The results for the multiple trials are superposed. Times are measured from when the initial send command is executed. The dotted lines are for reference, and correspond to *A+B.k*, where offset *A* is *1* msec, *k* is packet number, and transmission-time-per-packet *B* is *1* msec and *1.5* msec respectively for the lower and upper lines. The first transmission recorded is the initial packet broadcast by the source node. This is finished receiving roughly *2* msec after the send command is initiated. The second packet recorded is the first relay packet. This is detected roughly *1.5* msec after the first packet. Included in this time is the time to process the relay packet. Subsequent packets are received at intervals typically *1~1.5* msec. This is consistent with the estimate of transmission times in Eqn. 1 which was obtained from the specifications of 802.11. Note also the fewer data points for larger packet numbers, indicating a loss of packets.

Figure 5 shows the flooding time distribution for *50* nodes spread over a larger area. Roughly *20~25* nodes were within direct range of the

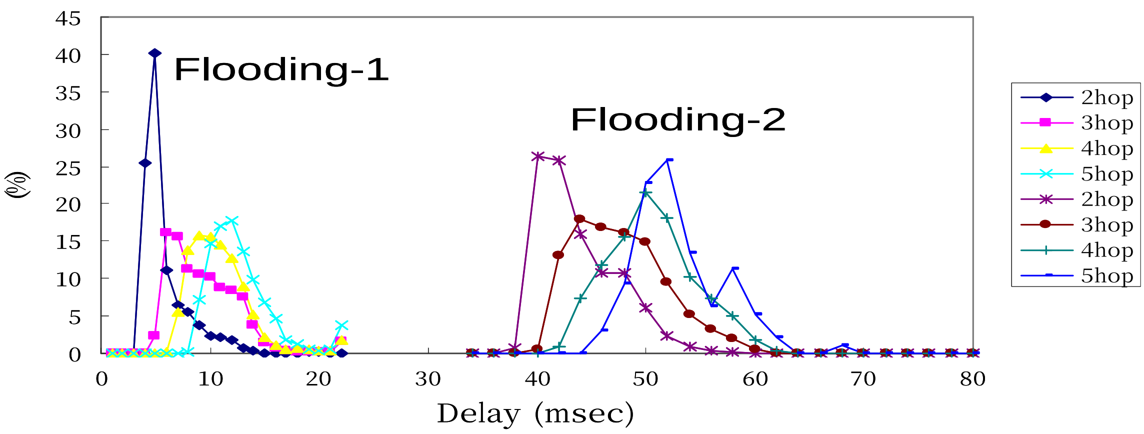

Figure 5. Flooding Time Distribution (50 nodes, multi-hop)

source. The remaining nodes could only be reached by multi-hop relay. Packets were generated at a single source with the same parameters as in the previous case of Figures 3 and 4. Times of arrival of packets at a particular sink node were measured to obtain the data shown in Figure 5. Packets travel to the sink node from the source node via a variety of paths, so they have differing numbers of hops. For Flooding-1, the relay time is roughly *2* milliseconds per hop. Flooding-2 is much slower due to extra processing delay. We also point out the existence of a long tail in the distribution, due to the competition with re-transmissions by other nodes. That is, nodes transmitting packets with different hop numbers competing for access to the wireless medium. Notice also that the Flooding-1 is much sharper than Flooding-2 – the extra processing involved in Flooding-2 also results in a bigger spread of delay times.

Discussion

The theoretical analysis and the experiments consistently indicate that propagation times of the order of *10s* of milliseconds are quite practical for flooding packets. Note that a car travelling at *108* km/hr travels *3* meters in *100ms.* Theoretically, the minimum time for broadcast of a 140 byte data packet using 802.11 is *1* millisecond, which suggests that *100* relay events can be handled within *100* milliseconds. However, the differences between time required by Flooding-1 and Flooding-2 show that fast flooding requires optimization of the packet handling. In particular, as the number of sources had relay nodes increases, the time needed to check packets for redundancy and other filter conditions, can become a bottleneck requiring more efficient memory access and matching algorithms. Whether or not processing is done by processors dedicated to relay or handled by a general purpose computer sharing time with other tasks will also be a key issue for practical systems.

Conclusions

In conclusion, we analysed the delivery times and reliability for multi-hop flooding using 802.11 ad hoc mode. We showed fundamental estimates of flooding time and pointed out that it was necessary to avoid broadcast storm phenomena by constraining the density of relay nodes. Moreover, we examined the delivery time and reliability of flooding in a real-world 50 node network using 802.11 and showed reliable delivery times less than *20* msec can be achieved with efficient relay software. These results are very promising for practical implementation of flooding in practical roadway situations.

Acknowledgements

This work is part of "Ubiquitous ITS" granted by National Institute of Information and Communications Technology (NICT).

References

[1] C. Ho, K. Obraczka, G. Tsudik, and K. Viswanath, "Flooding for reliable multicast in multi-hop ad hoc networks", in Proceedings of the International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communication (DIALM) pp. 64-71, 1999.

[2] S. Y. Ni, Y. C. Chen, J. P. Shen, J. P. Sheu, "Broadcast storm problem in a mobile ad hoc network", in Proceedings of Mobile Computing (MobiCom), pp. 151-162, August 1999.

[3] Y.C. Teng, S. Y. Ni, and E. Y. Shih, "Adaptive approaches to relieving broadcast storms in wireless multihop mobile ad hoc networks", in Proceedings IEEE 21st International Conference on Distributing Computing Systems, pp. 481-488, 2001.

[4] B. Williams, T. Camp, "Comparison of broadcasting techniques for mobile ad hoc networks", MobiHoc, 2002.

[5] C. Cordeiro, H. Gossain and D. P. Agrawal, "Multicast over Wireless Mobile Ad hoc Networks: Present and Future Directions," IEEE Network, January/February 2003, pages 2-9

[6] W. Peng and X. Lu, "On the reduction of broadcast redundancy in mobile adhoc networks", MobiHoc 2000.

[7] I.S. Committee, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. In IEEE 802.11 Standard, IEEE, New York, 1997. ISBN 1-55937-935-9.

[8] S. Itaya, M. Kosuga, P. Davis, "Estimating jitter for real time applications in ad hoc wireless groups using CSMA/CA", International Journal of Wireless and Mobile Networking (to appear 2005).

[9] S. Itaya, P. Davis, "Robust, low latency wireless transmissions for real-time interaction in small ad hoc groups", The 6th International Symposium on Wireless Personal Multimedia Communications WPMC'03, (Yokosuka, October 2003) Vol. 2, pp. 497-501.

[10] S. Itaya, M. Kosuga, P. Davis, "Simulation and analysis of UDP packet exchange in wireless ad hoc groups", CNDOS (San Diego, January 2004).

[11] S. Itaya, M. Kosuga, P. Davis, "Evaluation of packet latency and fluctuation during UDP packet exchange in ad hoc wireless groups", 24th International Conference on Distributed Computing Systems Workshops (ICDCSW'04) (Tokyo, March 2004) pp. 684-689.
[12] **小菅 昌克**, **板谷 聡子**, Peter Davis, **梅田 英和** (**スカイリー・ネットワークス**)「**アドホックネットワークが開く新しい世界（前編）**」 **情報処理学会会誌** 2003.10.1
[13] **小菅 昌克**, **門 洋一**, **田中 信介**、「**無線アドホックネットワークにおけるフラッディングを用いた情報配信方式の一検討**」**電子情報通信学会、情報ネットワーク／モバイルマルチメディア通信／マルチメディア・仮想環境基礎研究会** 2002.11.14
[14] **門 洋一**、「**無線フラッディングにおける中継データおよび発信データの多重化方式**」**電子情報通信学会、情報ネットワーク／モバイルマルチメディア通信／マルチメディア・仮想環境基礎研究会** 2002.11.14
[15] P. Poupyrev, M. Kosuga, P. Davis, "Analysis of wireless message broadcasts in large ad hoc networks of PDAs", IEEE Fourth International Conference on Mobile and Wireless Communication Networks (Stockholm, Sept. 2002).
[16] P. Davis, A. Hasegawa, N. Kadowaki, S. Obana, "Self-organization of activity in wireless sensor networks", Proceedings of the 2004 Intelligent Sensors, Sensor Networks and Information Processing Conference, ISSNIP 2004 (Melbourne, December 2004) pp. 103-106.