Performance Evaluation of a Wireless Ad Hoc Network: Flexible Radio Network (FRN)

Masashi Sugano†, Tsutomu Araki††, Masayuki Murata††,
Takaaki Hatauchi†††, and Yohei Hosooka†††

†Osaka Prefecture College of Health Sciences.
3–7–30 Habikino, Habikino,
Osaka 583–8555, Japan

††Dept. of Informatics and Mathematical Sci.
School of Engineering Science, Osaka University
1–3 Machikaneyama, Toyonaka,
Osaka 560–8531, Japan

†††Multimedia and Wireless Dept., Technology Development Office,
Energy and Electrical Systems Company,
Fuji Electric Co., Ltd., 1 Fuji, Hino, Tokyo 191–8502, Japan

ABSTRACT

In an ad hoc wireless network system, wireless terminals can autonomously construct a network and directly communicate with each other without using wired network. A Flexible Radio Network is one of the ad hoc wireless network systems which has been operational in a recent few years. In the Flexible Radio Network, an original communication protocol is implemented to obtain the reliability of the communication. In this paper, we evaluate the performance by means of simulations for data-link protocol and routing protocol of the Flexible Radio Network. We first show the performance when system parameters are changed to examine how these parameters affect the system performance. Furthermore, we investigate the performance improvement by changing the network configuration.

1. INTRODUCTION

An ad hoc wireless network is a self-organizing and rapidly deployable network, in which neither a wired backbone nor a base station is necessary. The network node can communicate with one another over wireless channels in a multi-hop fashion. From these characteristics, ad hoc networks have been considered suitable for a military communication or an emergency operation. Furthermore, many studies have been dedicated to evaluate the property of the ad hoc network [1, 2], especially for the routing protocol suitable for the ad hoc network system [3-5].

In recent years, its scope is spreading, and the application to various fields is considered. Bluetooth [6] is one such a system that builds a comparatively small-scaled network under the mobile environment. The objective of Bluetooth is a replacement of many proprietary of cables with one universal short-range radio link. In such a system, a network is mainly built by various mobile devices, e.g., a cellular phone and a Personal Data Assistant (PDA). The easy data transfer between these equipments are realized. A large-scale network with stationary terminals has also useful application fields. Flexible Radio Network (FRN) is one such a product developed for the communication system where any cabling is difficult. Without necessity of wired cabling, installation and maintenance can be easily performed. In addition, the network can be extended only by adding the radio terminal if needed. The system is now used for data collection from a lot of ski-lifts scattered in a skiing area, or collection of a sales account or monitoring information of the vending machines in a parking area of the expressway.

FRN adopts a proprietary protocol so that it can efficiently take an action against the failure of a radio terminal or the change of the network configuration. However, it is not clear enough what system parameter affect the performance; such as a throughput, in the current system, these are decided through the process of trial and error. Moreover, for applying FRN to other systems than above-mentioned systems, the influence of network configuration on a basic property should be identified. In order to clarify the scope of this system, it needs to be evaluated using network parameters.

In this paper, we focus on the performance of the data-link protocol and the routing protocol defined in FRN. We will first reveal how the parameter value defining system operation affect the throughput and the average packet delay to show a basic property of the system. We then investigate how network configuration affects the performance, and discuss about arrangement of the radio terminals for improving the performance.

The remainder of this paper is organized as follows. Section 2 briefly introduces Flexible Radio Network and its data-link and routing protocols. In Section 3, we present performance results obtained by simulation and some discussions. Finally, we describe the concluding remarks and future work in Section 4.

2. SYSTEM DESCRIPTION

2.1 Configuration of Flexible Radio Network

The components of FRN is shown in Fig. 1. In FRN, the radio terminal with transmission and reception and the relay function of packets is called *node*. The adjacent nodes can be

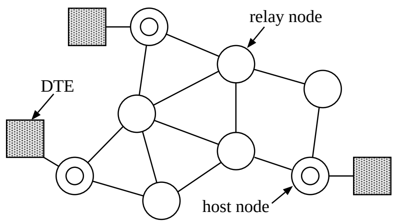


Figure 1: Components of Flexible Radio Network

Dest. ID	Priority of route selection		
0	$\mathbf{R}_{01}$	$\mathbf{R}_{02}$	$\cdots$
1	$\mathbf{R}_{11}$	$\mathbf{R}_{12}$	$\cdots$
2	$\mathbf{R}_{21}$	$\mathbf{R}_{22}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$

Table 1: Configuration table

communicated directly from a certain node. The node linked to DTE (Data Terminal Equipment), which performs generation and reception of data, is called a *host node*, and the other nodes are called *relay nodes*. Each node is assigned a unique ID number.

Each node maintains the network information in the *configuration table* as shown in Table 1. The configuration table contains the route information from the node itself to destination nodes. An element $\mathbf{R}_{ij}$ in the configuration table of node n consists of the following items:

- Adjacent node ID for sending packets through j-th route destined for node i
- The number of hop counts from the adjacent node to the destination node i
- Reliability of the radio channel between node n and the adjacent node of j-th route

The order of route selection for packets destined for node i is $\mathbf{R}_{i1}$, $\mathbf{R}_{i2}$, $\cdots$. Its determination is described in Subsection 2.3.

Each node generates a *configuration-control packet* for obtaining the shortest hop count to all nodes. It is transmitted without specifying a destination node for every fixed time called *configuration-control cycle*. The node which received the configuration-control packet improves and reconstructs its own configuration table on the basis of the information. The configuration-control cycle needs to be determined so that it can react against changes of network status quickly and does not overload the network.

The *reliability* is a value showing the success probability of the packet transmissions between nodes. If the configuration-cycle in which a certain packet was received is a Y time during X cycles, the reliability is calculated as Y/X. Then, if the reliability larger than the prescribed threshold value, the node is recognized as the adjacent node and it registers with the configuration table. If the reliability is below threshold, it is not recognized as a adjacent node and does not register with a configuration table.

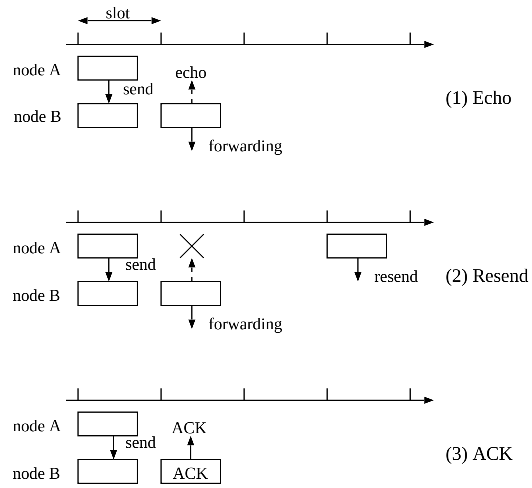


Figure 2: Time chart of packet transmission

2.2 Data-link Protocol

Radio channel is divided into fixed-length time slots. In order to avoid packet collision, each terminal first senses the carrier at the beginning of the slot. When the carrier of other packets is detected, the sender takes a back-off time to retransmit the packet.

In FRN, each of nodes covered by the area in which the radio wave is attainable can receive the packets even when it is not the source/destination of the packet. In FRN, this property is utilized for the acknowledgment of the packet. More specifically, the packet transmitted by some node i is received by the adjacent node j, and it is further relayed to the other node k, the relayed packet can be received by node i. If it is successfully received by node i, it is recognized as a successful transmission of the original packet from node i to node j. It is called *relay echo* (or simply *echo*). The destination host node does not return the echo, in order not to perform packet relay. Then, ACK should be explicitly returned. If the node does not receive an echo or ACK within a fixed time interval after packet transmission, it resends a packet.

The process explained above is illustrated in Fig. 2. Figures 2(a) and (b) show the case where node B is a relay node. That is, the packet is transmitted from node A to node B, and node B performs relay transmission. Figure 2(a) shows the case where transmission of the packet and reception of the echo at node A are successful. The case where node A fails in reception of the echo is shown in Figure 2(b). Figure 2(c) shows the case where node B is a host node. Therefore, node B has sends ACK to node A.

To avoid a loop of the packet forwarding and to sustain the traffic load increase, the maximum survival time is defined for every packet. When the packet is generated, an initial value is set. Then for every time slot, it is decreased by one. Choosing the initial value of the maximum survival time is one of key issues for obtaining good performance of FRN. We will investigate it through simulation in the next section.

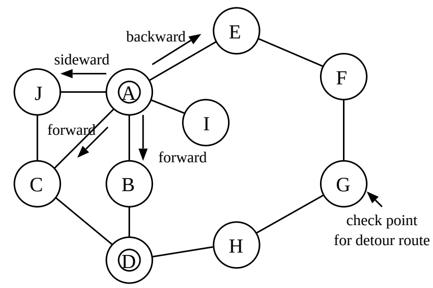


Figure 3: Selection of route for retransmission

2.3 Routing Protocol

The routing protocol is important to attain reliability in packet forwarding especially in the environment of the radio channel. In FRN, the route (i.e., the next hop of the packet at each node) is determined by the configuration table shown in Subsection 2.1. If the node fails to transmit the packet on the first node, another route should be chosen immediately. That reason determined the structure of the configuration table of FRN.

As described in the previous Section, each node maintains the routes to all other nodes in its configuration table. These routes are classified into the following three kinds according to the number of hops:

Forward route: The one or more routes on which the number of hops to the destination node is the shortest.

Sideward route: The one or more routes on which the number of hops to the destination node is the shortest hop number plus one.

Backward route: The one or more routes on which the number of hops to the destination node is the shortest hop number plus two or more.

The transmitting priority is determined in the order of forward routes, sideward routes, and backward routes. If several nodes exist within the same category, the reliability value of the channel in taken into account, by which the flexible and robust routing protocol is realized. In particular, packet collision takes place continuously, the next hop easily changed by utilizing the configuration table of FRN.

The backward route ensures the reliability by using it when forward and sideward routes become unreliable temporarily according to a failure of a channel or a node. The *checkpoint* of a detour is necessary in this case. Based on the configuration table, each node searches for the detour route for all nodes periodically, and determines the checkpoint as a course target.

3. SIMULATION RESULTS AND DISCUSSIONS

In simulation experiments, we introduced the following assumptions.

- The configuration of the network is fixed. Thus, transmission of configuration-control packets are not considered. In an actual system, the configuration-control cycle is enough large compared with the length of one time slot, and therefore the the influence to the load of a network is negligible.
- In a actual system, the radio channel is influenced by fading and/or shadowing, and transmission characteristic is changed, and the burst transmission error takes place intermittently. However, in our simulation, the property of the radio channel is not changed and given based on the reliability values given beforehand.
- When the packet with strong radio power arrives early, and the packet with weak radio power (due to e.g., long distance from the transmitter), the latter packet is lost. On the other hand, when the packet with strong radio power arrives later than the packet with weak radio power, all packets are lost. The strength of the radio power is dependent on the distance between the nodes.
- The time interval for resending the packet is fixed and assumed to be two slots.

We will use the following performance measures.

(a) Throughput
The average number of transmitted packets successfully per one slot time. between host nodes in simulation time.

(b) Packet loss rate (PLR)
The ratio of the packet not reaching the destination. In our simulation, the following packets are considered as the lost packet:
(1) The packets which exceeded the maximum survival time.
(2) The packets which remained in buffer at each node when the simulation has finished.
(3) The packets which arrived at the destination but discarded due to too much delay.

(c) Average packet delay
Packet delay is expressed as the time duration from the packet generation at source host node to the arrival at destination host node.

In order to asses accuracy of simulation, 95% confidence intervals are computed on throughput and average packet delays in each simulation experiment.

3.1 Evaluation of basic property of Flexible Radio Network

In order to evaluate the basic property of the FRN, the simulation was performed using the network model created by arranging nodes at random on a grid. If the distance between nodes is below a threshold value, the error is assumed not to occur. When exceeding a prescribed value with respect to the distance, The packets do not reach at all. That is, when the distance between nodes is below a threshold, reliability is set to 100%, and it becomes 0% when exceeding the threshold. In our simulation, the threshold value is set to be 2.6. The arrangement of the nodes and the connection of each node determined by the threshold value are shown in Figure 4.

In this network model, three host nodes transmit and receive packets mutually. The packet generation rate in each host node per one slot is assumed to be same. When a packet

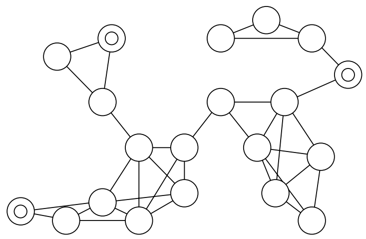
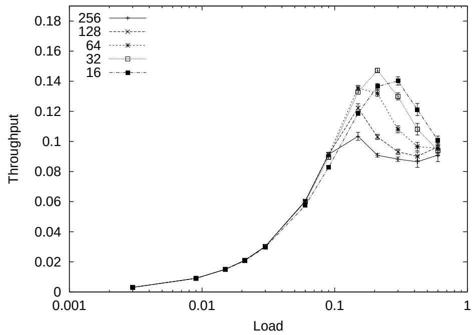
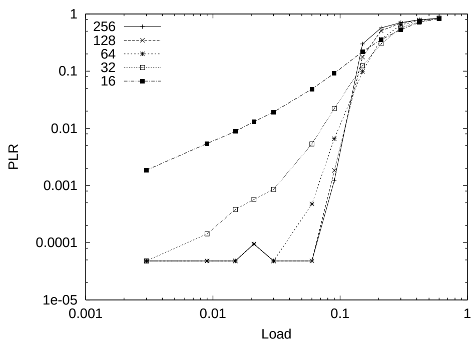


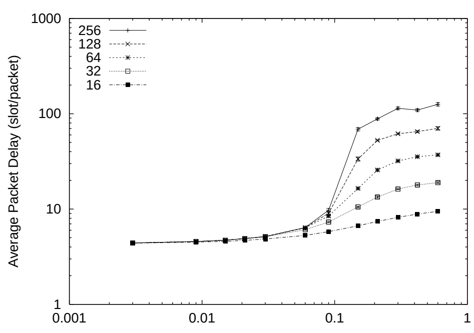
Figure 4: Simulation model with three host nodes



(a) Throughput



(b) Packet Loss Rate

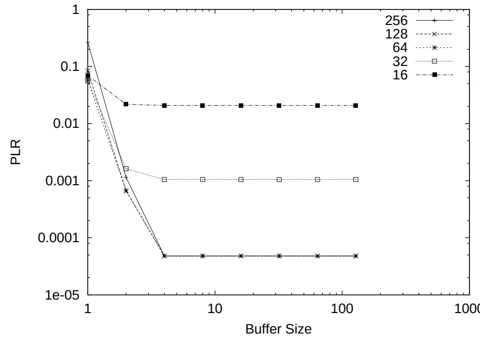


(c) Average Packet delay

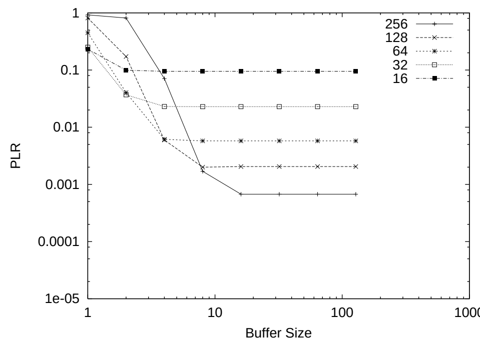
Figure 5: Basic system property and influence of maximum survival time

is generated at host nodes, either of the other two host nodes is randomly chosen as destination. The traffic load is defined as the number of packets generated in per one slot in the whole network (i.e., the sum of the packet generation rate at the three nodes).

First, each performance measure dependent on the traffic load is shown in Figure 5, for five different values of the maximum survival time; 256, 128, 64, 32, and 16. Here, the buffer size of each node is assumed to be infinite. It is shown in the figure that the optimum maximum survival time differs according to the traffic load. That is, since a possibility of being canceled before reaching the destination node will become high if the maximum survival time is small when load is low, the rate of packet loss increases. Conversely, if the maximum survival time is large, it can reduce the rate of packet loss since such a possibility becomes low. On the other hand, in the case where load is high, the maximum survival time should be small so that the network congestion is avoided by canceling packets. When the maximum survival time is set to be large, packet collision increases and smooth communication is prevented.



(a) Load: 0.03



(b) Load: 0.09

Figure 6: Estimation of sufficient buffer size

Next, we investigate the influence of buffer size on the performance. Figure 6 shows the packet loss rate at the time of changing buffer size about the case where load is high (0.09), and the case of being low (0.03). It is shown that as the buffer size is set to be large, PLR becomes settled depending on the traffic load and the maximum survival time. For example, when the maximum survival time is 64 for the traffic load of 0.09, the buffer size of eight packets is enough.

3.2 Configuration of the network for improving a performance

The objective of this subsection is to investigate a performance is influenced by the network configuration. For this, we used four network configurations shown in Figure 7. Other

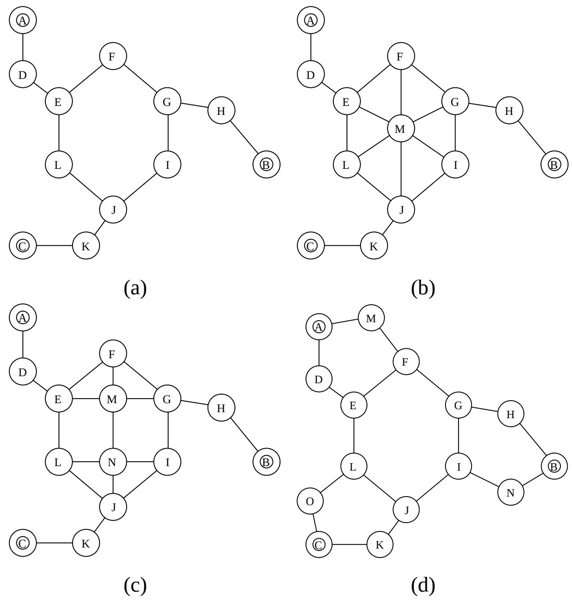


Figure 7: Network Configuration

simulation settings are just same as in the previous subsection.

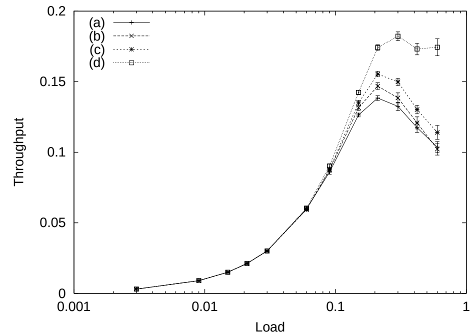
First, one may think that packet collision rarely occurs in the network of Figure 7(a) because each node has a few number of adjacent nodes. However, when a collision occurs at nodes E, G, and J, it will fall into a deadlock for a while. Suppose the packets of nodes L to J and nodes K to J collide, a detour route does not exist for the packet of K to J. Moreover, only one detour exists which goes via G for the packet of L to J. Then, throughput and packet loss rate are lower than other cases as shown in Figure 8(a) and (b).

With the network configuration of Figure 7(b), node M can be used for detour routes to avoid a packet collision at nodes E, G, and J. Therefore, when load is low, the improvement can be observed. However, since node M has many adjacent nodes, it is easy to get overloaded under the high load. Central nodes of M and N in the network configuration of Figure 7(c) can share the role of detours. The frequency of collision is then expected to become low. However, as load is high, it is shown that performance is degraded similarly. In Figure 7(d), the large improvement about the throughput and the packet loss rate in Figures 8 (a) and (b). This is because the number of hop counts between host nodes is decreased. Furthermore, a collision can be reduced by providing two routes in the central area of the network. In such a network configuration, the improvement in the packet loss rate is remarkable under the low load, since transmission passing through the detour from every host node is possible.

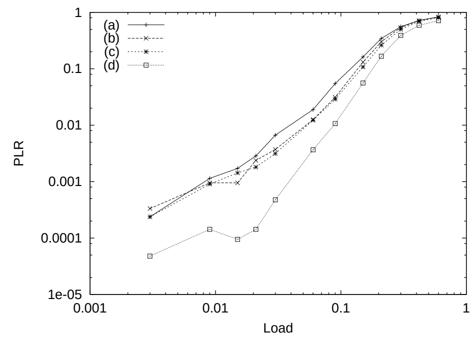
4. CONCLUSION

In this paper, the performance evaluation by simulation was performed for FRN by carefully modeling its unique features of the data-link protocol and the routing protocol. We have investigated how the parameter values of FRN affect the performance measures; such as a throughput and average packet delay. Furthermore, we have shown how various network configuration affect the performance, and the adequate network configuration for improving the performance was discussed.

As a future subject, performing the simulation on many network configuration further, and clarifying the more general improvement techniques are necessary.



(a) Throughput



(b) Packet Loss Rate

Figure 8: Performance variation by different network configurations

REFERENCES

[1] M. Gerla and J. T.-C. Tsai, "Multicluster, mobile, multimedia radio network," *Wireless Networks*, vol. 1, pp. 255–265, May 1995.

[2] K. Nakano, M. Sengoku, and S. Shinoda, "Fundamental Characteristics of Multi-hop Wireless Communication Networks," in *Proceedings of 11th ITC Specialist Seminer*, pp. 293–301, Oct. 1998.

[3] J. Broch, D. B. Johnson, and D. A. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks." Internet Draft, draft-ietf-manet-dsr-03.txt, Oct. 1999.

[4] Z. J. Haas, "A New Protocol for the Reconfigurable Wireless Networks," in *Proceedings of IEEE ICUPC'97*, pp. 562–566, Oct. 1997.

[5] Y. B. Ko and N. H. Vaidya, "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks," in *Proceedings of ACM Mobicom'98*, pp. 66–75, Oct. 1998.

[6] P. Johansson, N. Johansson, U. Körner, J. Elg, and G. Svennarp, "Short Range Radio Based Ad-hoc Networking: Performance and Properties," in *Proceedings of IEEE ICC'99*, pp. 1414–1420, June 1999.