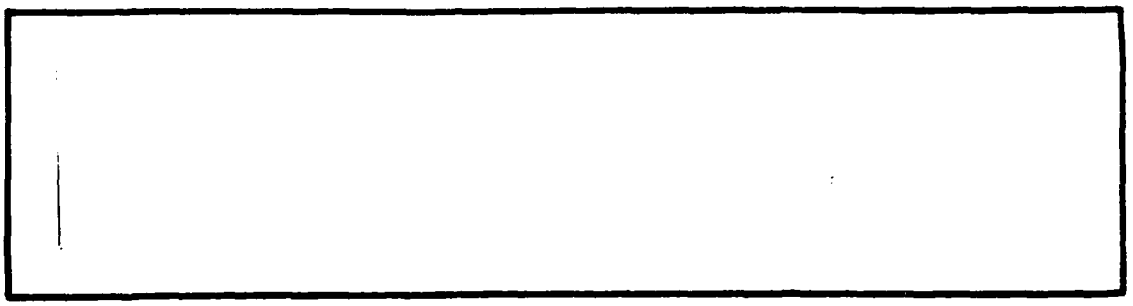
ARO 24649.3-EL-S

(2)



Axiomatix

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER ARO 24649.3-EL-S	2. GOVT ACCESSION NO. NA	3. RECIPIENT'S CATALOG NUMBER NA
4. TITLE (and Subtitle) SIMULATION STUDY OF PERIODIC JAMMING OF ADAPTIVE NETWORKS		5. TYPE OF REPORT & PERIOD COVERED Technical 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Unjeng Cheng		8. CONTRACT OR GRANT NUMBER(s) DAAL03-87-C-0007
9. PERFORMING ORGANIZATION NAME AND ADDRESS AXIOMATIX 9841 Airport Blvd., Suite 912 Los Angeles, CA 90045		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS NA
11. CONTROLLING OFFICE NAME AND ADDRESS U. S. Army Research Office P. O. Box 12211 Research Triangle Park, NC 27709-2211		12. REPORT DATE June 29, 1988 13. NUMBER OF PAGES
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

NA

18. SUPPLEMENTARY NOTES

The view, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy, or decision, unless so designated by other documentation.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Adaptive Networks, Code-Division-Multiple-Access (CDMA), Communications, Networks, Network Simulation, Packet Radio, Periodic Jamming, Spread Spectrum

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

A periodic jamming attack is more harmful to the networks with the adaptive routing algorithms than the static jamming attack, since the latter can be detected by the communicators and the appropriate actions can be taken to alleviate its effectiveness. The non-existence of the equilibrium state makes the analytical and simulation study difficult. Although the equilibrium state does not exist, the time-average of various entities, such as the packet delay and the node queue size, are valid performance measures. In this report, we use simulation techniques to investigate the behavior of networks under the periodic jamming attack.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE 10

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

SIMULATION STUDY OF PERIODIC JAMMING OF ADAPTIVE NETWORKS

Interim Technical Report

Unjeng Cheng

June 30, 1988

U. S. Army Research Office
P. O. Box 12211
Research Triangle Park, NC 27709-2211

Contract No. DAAL 03-87-C-0007

Axiomatix
9841 Airport Boulevard
Suite 912
Los Angeles, CA 90045

APPROVED FOR PUBLIC RELEASE
DISTRIBUTION LIMITED

Axiomatix Report No. R8806-1

TABLE OF CONTENTS

LIST OF FIGURES

SIMULATION STUDY OF PERIODIC JAMMING OF ADAPTIVE NETWORKS

I. INTRODUCTION

The nonstationary jamming attack is more harmful to the networks with the adaptive routing algorithms than the static jamming attack. Static jamming can be detected by the communicators and the appropriate actions can be taken to alleviate its effectiveness. The network behavior under the nonstationary jamming attack is nonstationary. Thus, the equilibrium state does not exist, making the analytical and simulation study difficult. The performance measures for the networks under the static jamming attack are based on the equilibrium and are not valid in the nonstationary jamming environment. Therefore, new performance measures must be identified.

A simple form of the nonstationary jamming is the periodic jamming in which the jammers use a fixed set of jamming topology in a fixed time pattern periodically. The network behavior under the periodic jamming attack is periodic. Although the equilibrium state does not exist, the time-average of various entities, such as the packet delay and the node queue size, are valid performance measures. In addition, we can also use the window-average technique to study the time-varying network behavior. The response speed of the adaptive routing algorithm and the time-variation of the node traffic intensity can be found in this way. In this report, we simulate the behavior of networks under a periodic jamming attack. The results provide the basis for the future investigation.

In this investigation, we demonstrate the window-average technique and the time-average technique. We show that the window-average technique is a way to study the dynamic network behavior. The action of the adaptive routing algorithm and its effect on the network performance can be seen explicitly. The worst case jamming period of the periodic jammer can be found by both the window-average technique and the time-average technique.

The worst case jamming period is a function of the jamming topology and the traffic distribution. Suppose that the traffic distribution is not uniform over the network. If the jammed node is close to the nodes having heavy traffic, the worst case jamming period should be short; on the other hand, if the jammed node is far away from the nodes having heavy traffic, the worst case jamming period should be long.

In Section II, we describe the simulation model in detail. In Section III, we delineate the window-average technique and the performance measures. In Section IV, we consider two simple networks under the periodic jamming attack. In Section V, we present the conclusion and the future research.

II. SIMULATION MODEL

The simulation program comprises seven components, namely,

(1) the external packet generator,

(2) the node transmission simulator,

(3) the spread-spectrum multiple-access channel simulator,

(4) the transit packet handler

(5) channel quality monitoring,

(6) routing information exchange, and

(7) routing table update.

The first four components was described in our previous report [1]. The last two components are delineated in this section.

The simulation results in this report are obtained for the following model:

(1) the slotted-ALOHA transmitter-based code multiple-access,

(2) the geometrical external packet arrival, and

(3) the same transmission and re-transmission probabilities.

Note that the above model was also used in studying static jamming. In this investigation, we concentrate on the issues regarding the adaptive routing algorithm and only the aforementioned model is considered. Other models can be incorporated into the simulation programs in the future.

In the nonstationary jamming environment, the adaptive routing algorithm plays the central role of network performance. It comprises three components, namely,

(1) channel quality monitoring,

(2) routing information exchange, and

(3) routing table update.

The adaptive routing algorithm described in [2] is considered here. Each node maintains a table of distant packet radio (PR) identifications (ID), each with (1) the ID of the next PR in the route to it and (2) the length of the route, i.e., the number of links to be traversed to reach it. The routing information packet broadcasted by each node contains (1) the link quality measurements for all outgoing links to its neighbors, (2) the change of its routing table, and (3) the correct packet counts for all incoming links from its neighbors.

Channel quality monitoring

The detection of jammer existence is through the channel quality monitoring. The technique used in the current PRnet technology is adopted in this simulation study. Each node keeps track of the number of correctly received packets from each of its neighbors in every T_{cm} slots of interval (referred to as the channel monitoring interval). These counts will be included in the next routing information packet.

On the other hand, a node computes the percentage of correct packets in the last channel monitoring interval along an outgoing link after it receives the correct packet count from the corresponding neighbor. If the percentage exceeds a pre-selected threshold, the outgoing link is declared good; otherwise, it is declared bad. If the node does not receive

the correct packet count from a neighbor at the scheduled time, the link is also declared bad. The link quality assessment will be contained in the next routing information packet.

It is possible that no data packet goes through a particular node in a monitoring period. In order to keep monitoring the channel in this situation, we use the concept of I-AM-HERE packets. An I-AM-HERE packet is broadcasted by a node if in the last T_{IAH} slots, no packet (data or routing information) was broadcasted by it. In this simulation study, we choose $T_{IAH} = 100$.

Note that the packet count and the correct packet count includes the data, I-AM-HERE, and routing information packets.

Routing Information Exchange

The channel monitoring interval is synchronous for all nodes. However, each node is assigned to a unique slot in a monitoring period to broadcast its routing information packet. This approach is used to avoid collisions of the routing information packets among neighbors. When a node is being scheduled to transmit its routing information packet in the current slot, the neighbors of this node will delay their data packet transmission to the latter time.

Routing Table Update

A node updates its routing table immediately after it receives the routing information packet from a neighbor. This method is chosen in this study because of its simplicity. Note that there are other ways to update the routing tables. For instance, a node can update its routing table at the end of each channel monitoring interval so that all routing information packets received can be considered simultaneously.

If the outgoing link to a neighbor is declared bad, the length of all routes using that link is updated to be infinite. If the outgoing link is declared good, the routing table is updated by incorporating the new routing table (which is contained in the received routing information packet) of the corresponding neighbor. If the routing information packet from

a neighbor is not received at the scheduled time, the length of all routes using that link is updated to be infinite. The new routing table is contained in the next routing information packet.

III. PERFORMANCE MEASURES AND WINDOW-AVERAGE TECHNIQUE

The performance statistics of the network under the periodic jamming attack is also periodic. The performance measures such as the node busy probability and the node packet delay are functions of time. A straight-forward extension from the static jamming case to the periodic jamming case is to consider the time-average measures such as the time-average node busy probability and the time-average node packet delay. In the next section, we will show that they are indeed useful entities to determine the effectiveness of jamming.

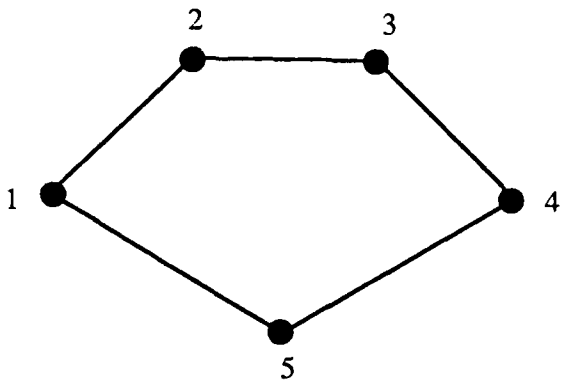
In many situations, however, we may also be interested in the detail network behavior. For instance, we may want to know which node is most busy in which time interval. In order to present this type of information, we can use the window-average technique as follows: we partition each jamming period into small intervals, referred to as windows. The statistics of the observables are collected window-by-window. The simulation program is running continuously and the data collected in many jamming periods are accumulated. The performance measures in each window are computed from the statistics collected in that window. The size of windows determines the resolution. If the window size is equal to the jamming period, the window average is the same as the time average. If the window is small, the number of simulation periods required to get the good estimate can be excessive long. A natural choice of the window size is T_{cm} (the channel monitoring interval) because it is the network action clock time. The simulation results in this report are obtained for this window size.

IV. SIMULATION RESULTS

Two networks are considered in this section. They are shown in Figures 1 and 2, respectively. For network A, nodes 3 and 5 are jammed alternatively with equal duration, which is a multiple of T_{cm}. The only traffic flow is from node 1 to node 4. Two routes are available, namely, 1-5-4 and 1-2-3-4. For network B, nodes 4 and 6 are jammed alternatively with equal duration. The only traffic flow is from node 1 to node 5. Two routes are available, namely, 1-7-6-5 and 1-2-3-4-5. For both networks, the role of the adaptive routing algorithm is to direct the traffic to the unjammed route. After the jamming topology changes and before node 1 directs the traffic to the alternate route, the traffic continues to flow into the blocked route. Since the adaptive routing algorithm does not create a temporary loop during updating the routing tables in these two examples, the traffic are accumulated only in the nodes along the route. On the other hand, the network C shown in Figure 3 is more complex. Suppose that nodes 6 and 8 are jammed alternatively. Let us consider the traffic flow from node 1 to node 7. As node 8 is jammed, the shortest-distance route 1-10-9-8-7 is disturbed and some blocked traffic may flow to nodes 11, 12, and 13 due to the temporary loop created by the adaptive routing algorithm. This certainly affects the local traffic condition around nodes 11, 12, and 13. Network C will not be addressed in this report.

Network A

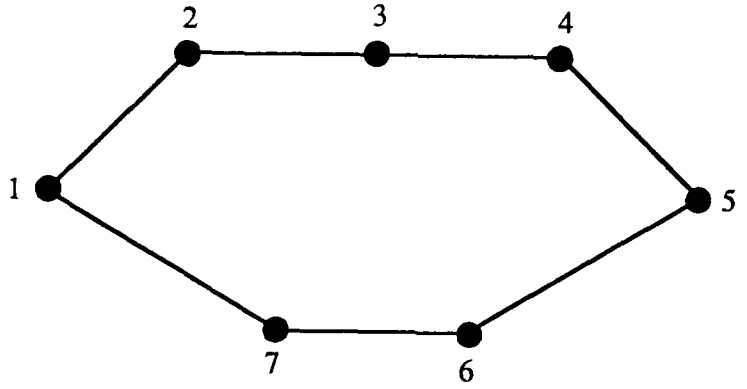
In Figure 4, we show the busy probabilities at all nodes except node 4 versus the time. In window #0 through #2, node 3 is jammed, while in window #3 through #5, node 5 is jammed. The jamming period is $6T_{cm}$ = 4500 slots. Let us consider the activity of node 2 first. In window #0 node 2 is busy because the packets in its buffer cannot be received by node 3 successfully. In window #1, node 2 becomes busier because that, in spite of the jamming situation, node 1 is still sending packets to it. In window #2, node 2 begins to be released from the backlogged traffic because (1) node 1 sends packets to



$\lambda_{14} = 0.012$

$\lambda_{ij} = 0 \quad \text{if } (i, j) \neq (1, 4)$

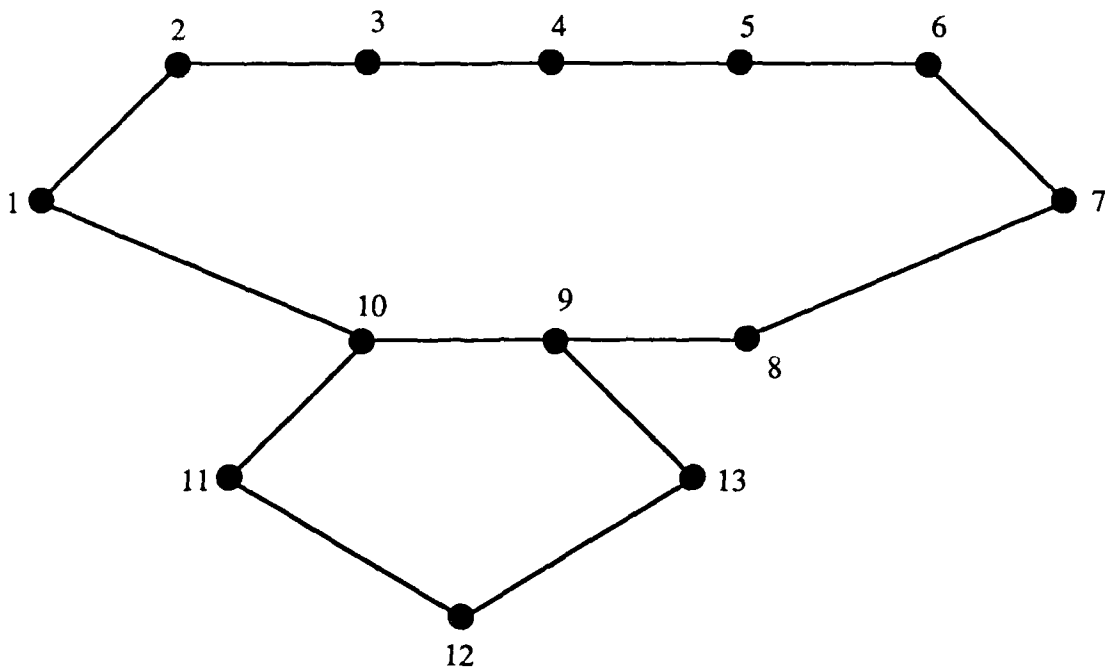
Figure 1. Network A.



$\lambda_{15} = 0.012$

$\lambda_{ij} = 0 \quad \text{if } (i, j) \neq (1, 5)$

Figure 2. Network B.



$\lambda_{17} = 0.012$

$\lambda_{ij} = 0$ if $(i, j) \neq (1, 7)$

Figure 3. Network C.

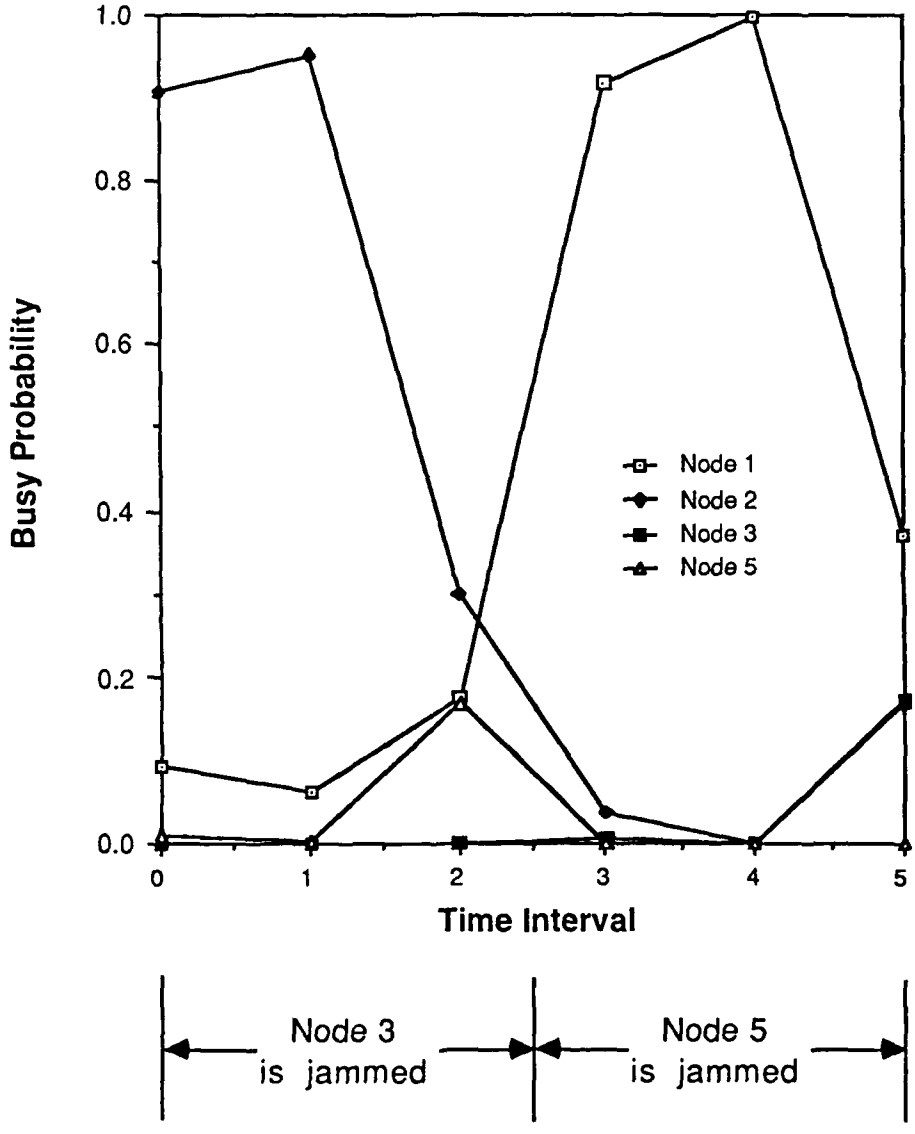


Figure 4. Busy Probability versus Time for Network A.

node 5 and (2) node 2 sends the backlogged packets to node 1. In window #3 and #4, node 2 has very light traffic because (1) node 1 sends packets to node 5 and (2) node 2 sends the backlogged packets to node 3. In window #5, node 2 has increasing traffic because node 1 knows that node 5 is jammed and sends packets to node 2 again. Secondly, let us consider the activity of node 1. In window #0 and #1, node 1 has normal activity since all packets are sent to node 2. In window #2, node 1 sends all packets to node 5. The reason of increasing activity is because it has to handle both the new external arrivals and the backlogged packets from node 2. In windows #3 and #4, its activity increases drastically because node 5 is now jammed. In window #5, node 1 begins to be released from the backlogged traffic because it sends packets to node 2. Node 5 has significant traffic only in window #2 because (1) in windows #0 and #1, traffic goes through node 2 and (2) in windows #3, #4, and #5, it is jammed and, therefore, no traffic can reach it. Node 3 has very light traffic in windows #0, #1, and #2 because it is jammed. Node 3 has no traffic in windows #4 because all traffic goes through node 5. In window #5, node 3 has the same traffic as node 2 because all traffic passing node 2 must also pass it. Node 3 has some traffic in window #3 because the channel monitoring has a small probability to fail to detect the existence of the jammer, and hence node 3 must handle both the backlogged packets and new external arrival in this window. Finally, node 4 always has zero traffic activity because it is the destination of all packets.

In Figure 5, we show the busy probability of node 1 versus time with the jamming period as the parameter. It shows that the most effective jamming period is $4T_{cm} = 3000$ slots. This is the expected result. As we saw before, it takes two channel monitoring intervals for node 1 to learn the jamming situation and to take appropriate action.

In Figure 6, we show the mean packet delay at all nodes (except node 4) versus the time. Let us first examine the mean packet delay at node 2. The packet delay in window #0 is about 1400 slots which is slightly less then $2T_{cm}$. This is because the packets arriving at node 2 in window #0 cannot be sent back to node 1 until the new

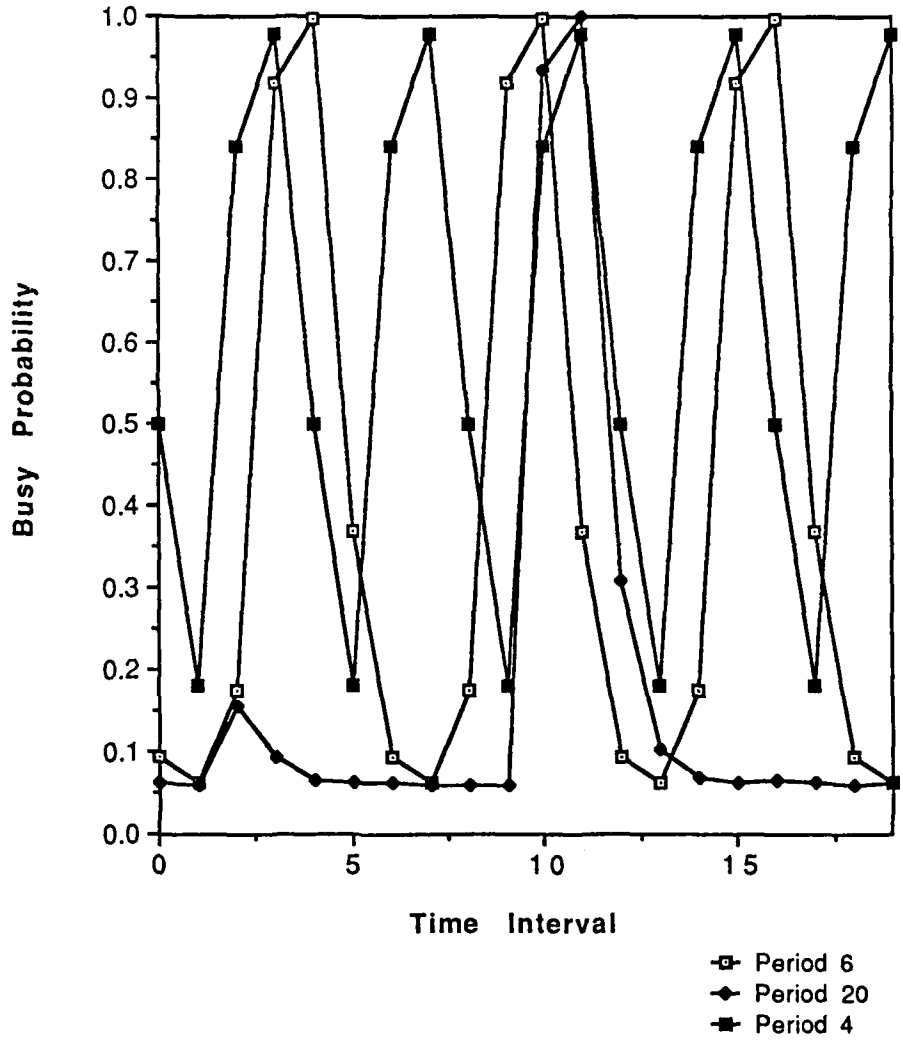


Figure 5. Busy Probability of Node 1 versus Jamming Period for Network A.

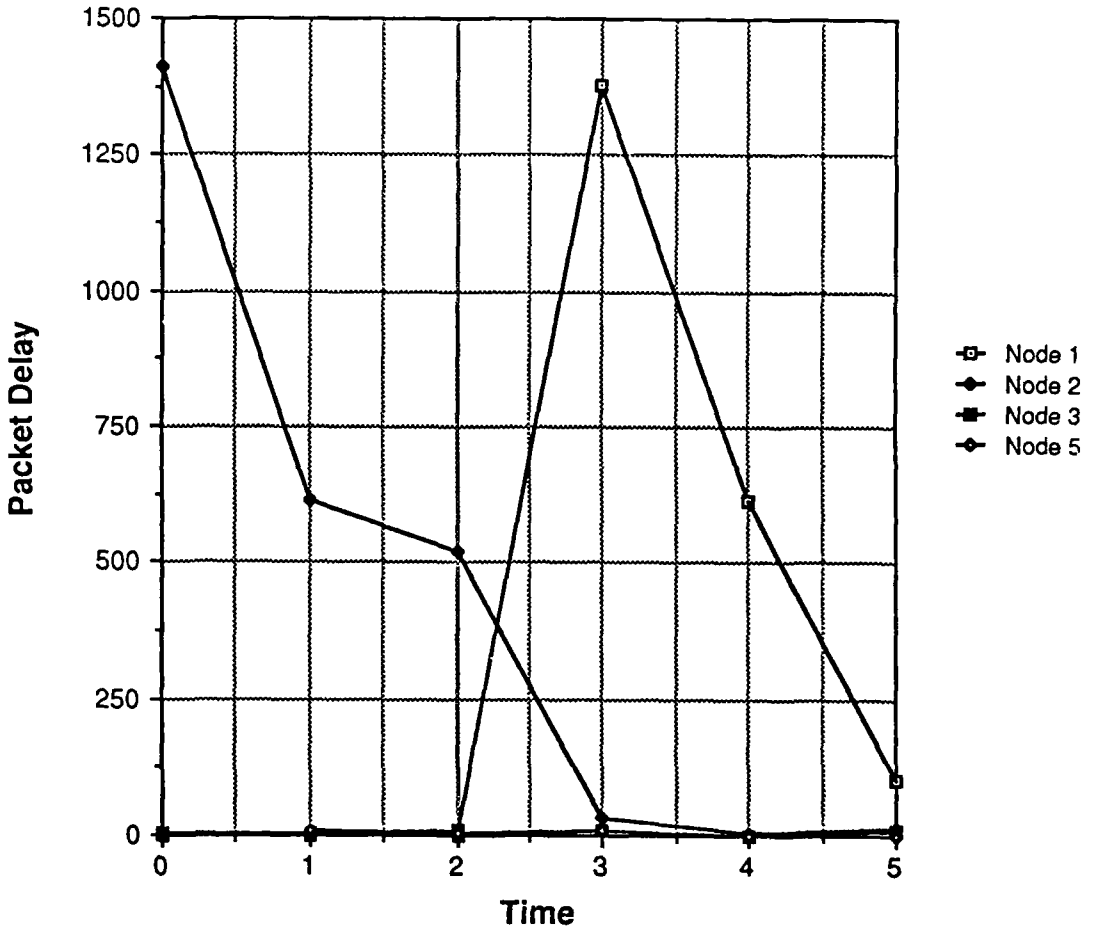


Figure 6. Mean Packet Delay versus Time for Network A.

routing table is derived in window #2. For the same reason, the packet delay in window #1 is about 610 slots which is slightly less then T_{cm}. As mentioned before, there is a small probability that channel monitoring fails to detect the existence of the jammer and thus some traffic may flow to node 2 in window #2. These packets are accounted for the mean packet delay in window #2. As we see, these packets can be transmitted successfully until node 3 is not jammed. In addition, the packets arriving at node 2 in window #2 can be sent only after all packets arriving at it in window #0 and #1 are sent successfully. This explains why the mean packet delay in window #2 is longer than $T_{cm}/2$. Secondly, let us consider the mean packet delay at node 1. The packet delay is small in windows #0, #1, and #2 because all packets arriving at it in these windows can be sent to either node 2 or node 5. In windows #2 and #4, node 1 has large packet delay because the 1-5-4 route is chosen, but node 5 is jammed in these two windows. The packet delay decreases drastically in window 5 because the 1-2-3-4 route is chosen in this window. The packet delay in nodes 3 and 5 is always small because as long as the packets arrive at one of them, there is no difficulty for them to reach node 4.

In Figure 7, we show the time-average busy probabilities of all nodes except node 4 versus the jamming period. It again shows that the most effective jamming period is $4T_{cm} = 3000$ slots. Node 1 is busier than node 2 for all jamming periods. Nodes 3 and 5 are equally busy. This is the expected result since node 1 sends packets to nodes 3 and 5 with roughly equal duration.

Network B

In Figure 8, we show the node busy probabilities at all nodes except node 5 versus the time. We see that the nodes immediately next to the jammed node are the busiest nodes; they are nodes 3 and 7 in this case. We also see that node 3 is busy in a three window period, but node 7 is busy only in a two window period. This is simply because node 3 is one hop further away from node 1 than is node 7. Therefore, it takes one more window

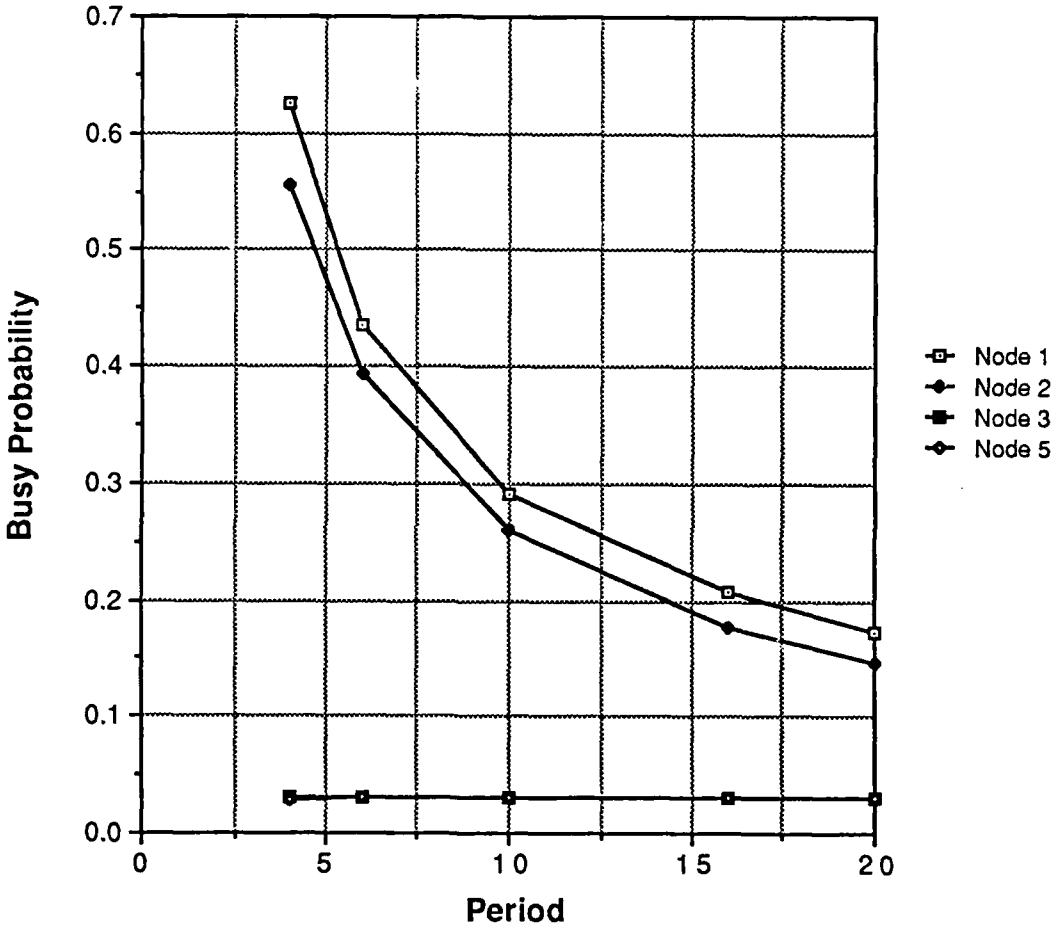


Figure 7. Time Average Busy Probability versus Jamming Period for Network A.

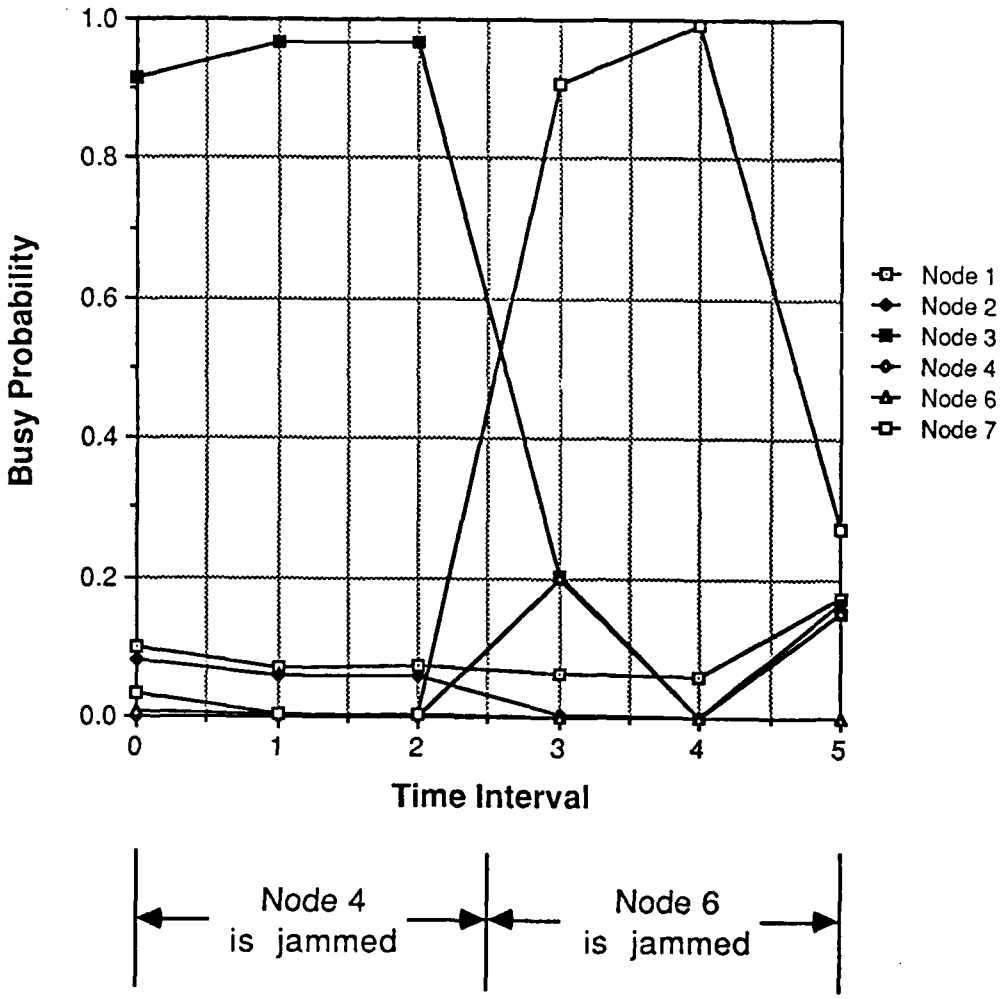


Figure 8. Busy Probability versus Time for Network B.

for node 3 to inform node 1 of the jamming situation. Node 1 has roughly uniform traffic because it can send packets either to node 2 or to node 7. Note that the traffic intensity at node 1 is between 0.1 and 0.2, which is about ten times that of the external packet arrival rate, namely, 0.012. The significant high traffic intensity is due to the backlogged packets. Node 2 has light traffic in windows #3 and #4 because most of the traffic goes through node 7. Node 7 has light traffic in windows #1 and #2 because most of the traffic goes through node 2.

In Figure 9, we show the time-average busy probability of all nodes except node 5 versus the jamming period. It shows that the most effective jamming period is $6T_{cm} = 4500$ slots. It is interesting to see that node 1 is not the busiest node since it can always send packet to either node 2 or node 7 regardless of the jamming situation. Node 3 is busier than node 7 for all jamming periods. This is due to the network asymmetry. It takes longer for node 1 to learn the jamming situation of node 4 than the jamming situation of node 6. Therefore, more traffic flows to node 3. Node 2 is less busy than node 1 because node 2 can always send packets to node 3 or node 1 and every packet must go through node 1 but not node 2. Nodes 4 and 7 are roughly equal busy for long jamming periods. When the jamming period is short, node 4 is busier than node 7.

In Figure 10, we show the time average packet delay at all nodes except node 5 versus the jamming period. As we expect, only nodes 3 and 7 suffer large packet delay. The most effective jamming period is about $6\ T_{cm} = 4500$ slots, which is longer than that for network A. This result suggests that the worst case jamming period is a function of the jamming topology and the traffic distribution. Roughly speaking, if the jammed node is close to the node having heavy traffic, the jamming period should be short. Alternately, if the jammed node is far away from the node having heavy traffic, the jamming period should be long. Note that node 7 has smaller packet delay than node 3 when the jamming period is $4T_{cm}$ and the reserve is true when the jamming period is $6T_{cm}$. This result is expected because it takes a two window period for node 1 to know node 7 is being jammed

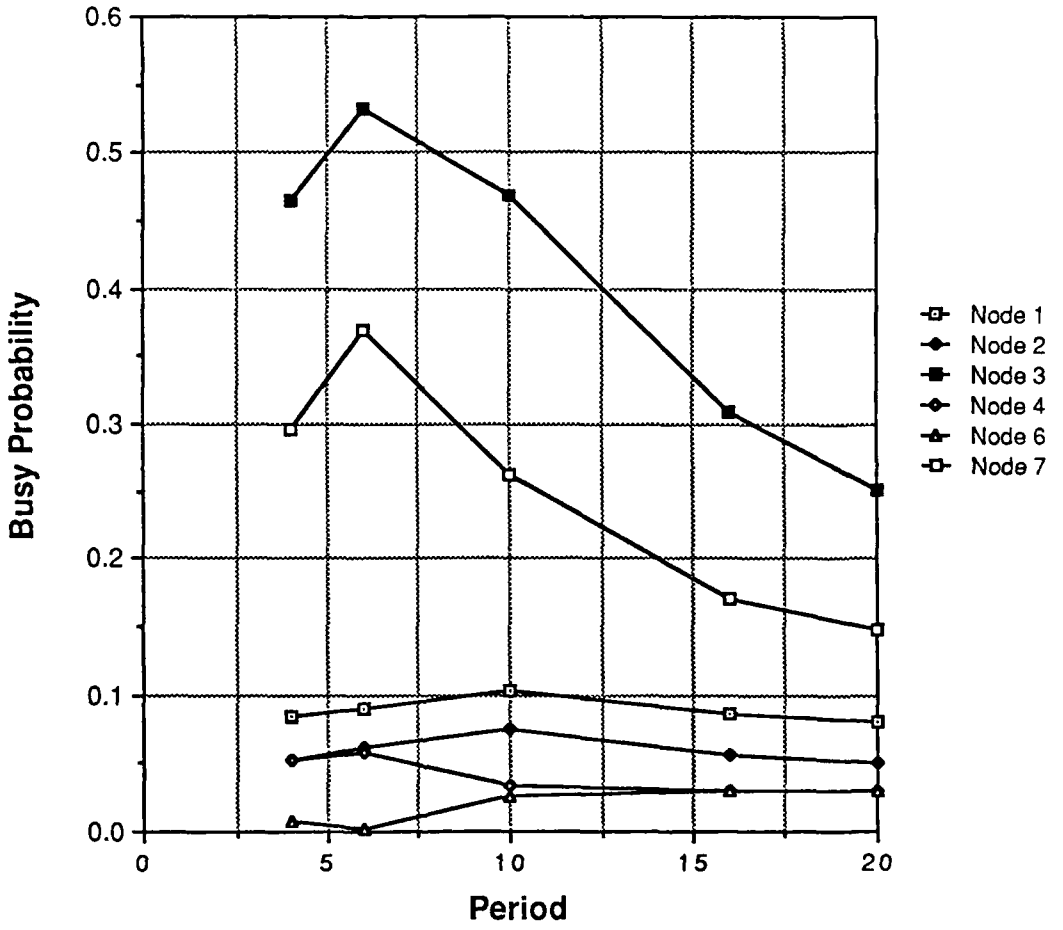


Figure 9. Time Average Busy Probability versus Jamming Period for Network B.

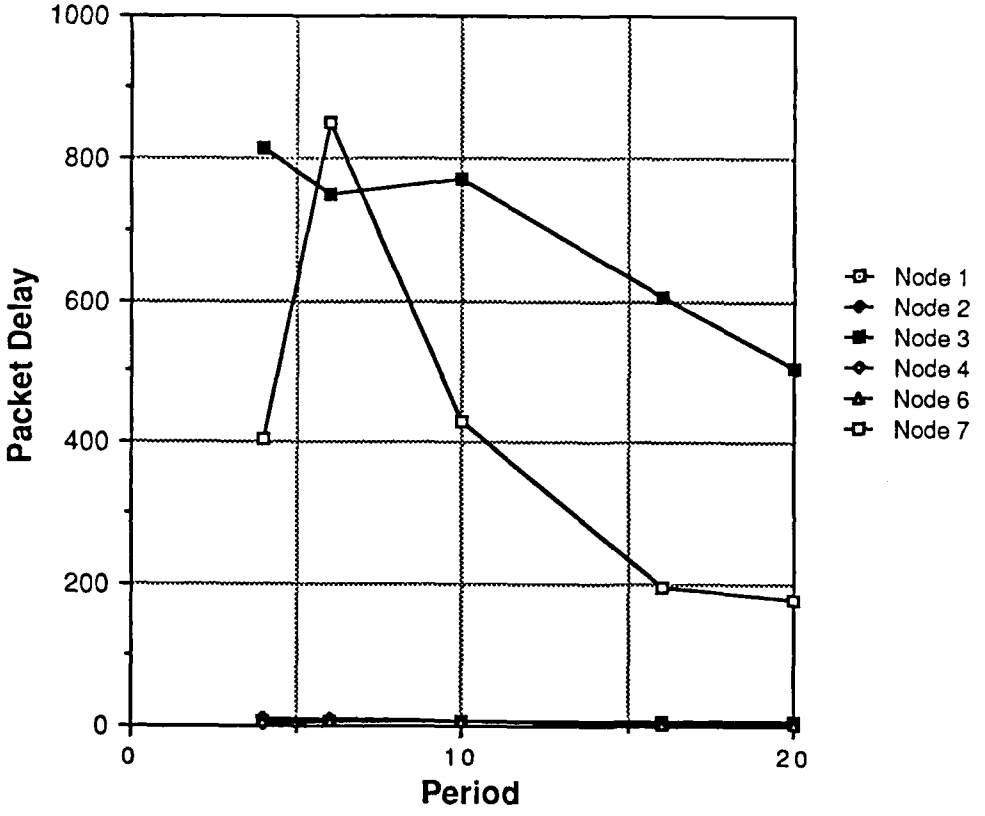


Figure 10. Time Average Packet Delay versus Jamming Period for Network B.

and takes a three window period for node 1 to know node 4 is being jammed. When the jamming period is longer than $6T_{cm}$, node 3 always suffers longer packet delay than node 7 does because of the network asymmetric. Note that periodic jamming forces more traffic flows through the longer route.

V. CONCLUSION AND FUTURE RESEARCH

In this investigation, we demonstrate the window-average technique and the time-average technique for the periodically-jammed networks. It is shown that the window-average technique is a way to study the dynamic network behavior. We have shown that the worst case jamming period is a function of the jamming topology and the traffic distribution. Two simple networks were considered in this study. An immediate extension of this study is to apply the aforementioned techniques to the more complex networks as well as the more sophisticated nonstationary jamming. The derivation of certain form of the analytical tools for studying the nonstationary-jammed networks is another important research problem. The simulation results presented in this report will be useful to evaluate the accuracy of the analytical results.

REFERENCES

[1] U. Cheng, "Static and Dynamic Jamming of Networks," Axiomatix Report No. R8712-6, December 23, 1987.

[2] J. Jubin, "Current Packet Radio Network Protocols," Proceedings of INFOCOM '85, pp. 86 – 92, April 1985.