International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 3, Issue 3 (May-June 2015), PP. 102-105

AN EFFECTIVE APPROACH FOR ALLOCATION OF ROUTING PATH TO MAXIMIZE THE OVERALL THROUGHPUT

Devendra Kumar, Mr. Atma Prakash Singh
C.S Department,
Azad Institute of Engineering & Technology, Lucknow.
devendraiet7316@gmail.com, talk2aps@gmail.com

Abstract- Jamming point-to-point transmissions in a wireless mesh can have debilitating effects on data transport through the network. At the physical layer the impact of jamming resonates through the protocol stack, providing an effectual denial-of-service (DoS) attack on end-to-end data communication. The simplest techniques to protect a network against jamming attacks embrace physical layer solutions such as spread-spectrum or beamforming, forcing the jammers to disburse a greater resource to reach the same objective. Nevertheless, recent work has demonstrated that intellectual jammers can integrate cross-layer protocol information into jamming attacks, tumbling resource disbursement by numerous orders of enormity by targeting certain link layer and MAC implementations as well as link layer error revealing and correction protocols. Hence, more sophisticated anti-jamming methods and defensive measures must be incorporated into higher-layer protocols, for example channel surfing or routing around jammed regions of the network

I. INTRODUCTION

The popular anti-jamming techniques make use of multiplicity. For example, anti-jamming protocols may utilize manifold frequency bands, diverse MAC channels, or various routing paths. Such multiplicity techniques assist to restrain the impact of the jamming attack by requiring the jammer to act on many resources at once. In this research, we consider the anti-jamming multiplicity based on the use of manifold routing paths. Using multiple-path variants of source routing protocols such as Dynamic Source Routing (DSR) or Ad-Hoc On- Demand Distance Vector (AODV), for example the MP- DSR protocol, each source node can ask for several routing paths to the destination node for concurrent use. To make effectual use of this routing diversity, however, each source node must be able to make an intellectual allocation of traffic across the available paths while considering the probable impact of jamming on the resulting data throughput. In order to characterize the impact of jamming on throughput, each source must collect information on the impact of the jamming attack in various parts of the network. However, the extent of jamming at each network node depends on a number of unidentified parameters, including the strategy used by the individual jammers and the relative location of the jammers with respect to each transmitter-receiver pair. Hence, the impact of jamming is probabilistic from the perspective of the network, and the characterization of the jamming impact is further complicated by the fact that the jammers' strategies may be dynamic and the jammers themselves may be mobile. In order to capture the non-deterministic and dynamic impact of the jamming assault, we model the packet error rate at each network node as a random process. At a given time, the randomness in the packet error rate is due to the uncertainty in the jamming parameters, while the time-variability in the packet error rate is due to the jamming dynamics and mobility. Since the impact of jamming at each node is probabilistic, the end-to-end throughput achieved by each source-destination pair will also be non-deterministic and, hence, must be studied using a stochastic framework.

In this paper, we thus investigate the ability of network nodes to characterize the jamming impact and the ability of multiple source nodes to reimburse for jamming in the allocation of traffic across multiple routing paths. Our contributions to this problem are as follow:

- We devise the dilemma of allocating traffic across multiple routing paths in the presence of jamming as a lossy network flow optimization problem.
- We devise the centralized traffic allocation problem for multiple source nodes as a convex optimization hitch.
- We recommend methods which permit individual network nodes to locally characterize the jamming impact and aggregate this information for the source nodes.

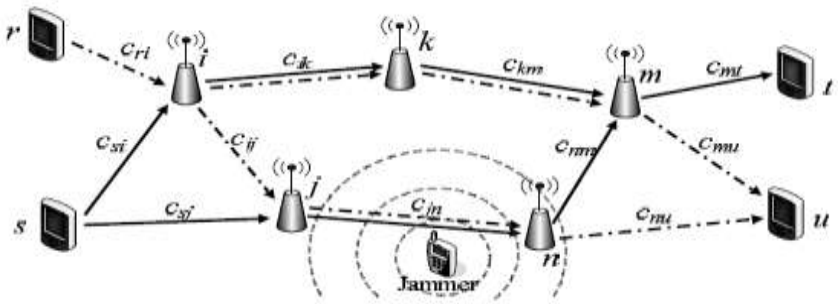


Fig. 1: An example network with sources S = {r, s} is illustrated. Each unicast link (i,j) ∈ E is labeled with the corresponding link capacity.

II. CHARACTERIZING THE IMPACT OF JAMMING

In this section, we suggest techniques for the network nodes to guesstimate and characterize the effect of jamming and for a source node to include these estimates into its traffic allocation. In order for a source node s to incorporate the jamming effect in the traffic allocation problem, the effect of jamming on transmissions over each link (i, j) ∈ E_s must be estimated and relayed to s. However, to capture the jammer mobility and the dynamic effects of the jamming attack, the local estimates need to be continually updated. We begin with an example to illustrate the possible effects of jammer mobility on the traffic allocation problem and motivate the use of continually updated local estimates.

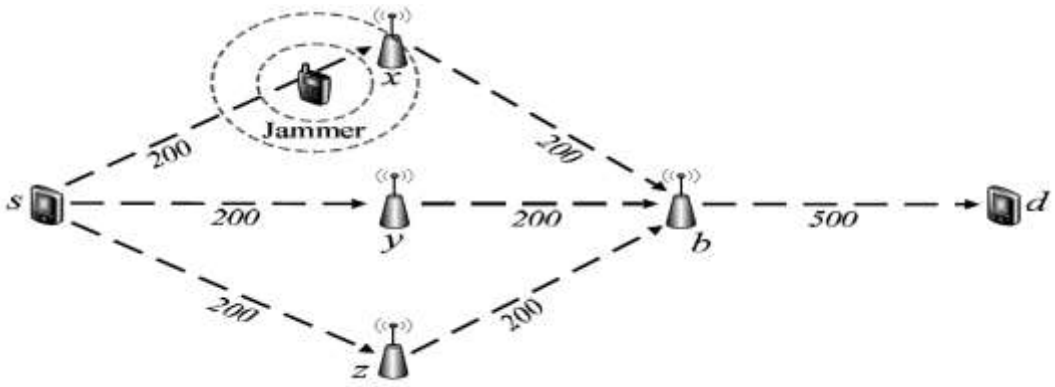


Fig. 2. Illustrates a single-source network with three routing paths.

III. ILLUSTRATING THE EFFECT OF JAMMER MOBILITY ON NETWORK THROUGHPUT

Figure 3 illustrates a single-source network with three routing paths $p_1 = \{(s, x), (x, b), (b, d)\}$, $p_2 = \{(s, y), (y, b), (b, d)\}$ and $p_3 = \{(s, z), (z, b), (b, d)\}$. The label on each edge (i, j) is the link capacity c_{ij} indicating the maximum number of packets per second (pkts/s) which can be transported over the wireless link. In this example, we assume that the source is generating data at a rate of 300 pkts/s. In the absence of jamming, the source can continuously send 100 pkts/s over each of the three paths, yielding a throughput rate equal to the source generation rate of 300 pkts/s. If a jammer near node x is transmitting at high power, the probability of successful packet reception, referred to as the packet success rate, over the link (s, x) drops to nearly zero, and the traffic flow to node d reduces to 200 pkts/s. If the source node becomes aware of this effect, the allocation of traffic can be changed to 150 pkts/s on each of paths p_2 and p_3, thus recovering from the jamming attack at node x. However, this one-time re-allocation by the source node s does not adapt to the potential mobility of the jammer. If the jammer moves to node y, the packet success rate over (s, x) returns to one and that over (s, y) drops to zero, reducing the throughput to node d to 150 pkts/s, which is less than the 200 pkts/s that would be achieved using the original allocation of 100 pkts/s over each of the three paths. Hence, each node must relay an estimate of its packet success rate to the source node s and the source must use this information to reallocate traffic in a timely fashion if the effect of the attack is to be mitigated. The relay of information from the nodes can be done periodically or at the instants when the packet success rates change significantly. These updates must be performed at a rate comparable to the rate of the jammer movement to provide an effective defense against the mobile jamming attack.

Next, suppose the jammer continually changes position between nodes x and y, causing the packet success rates over links (s, x) and (s, y) to oscillate between zero and one. This behaviour introduces a high degree of variability into the observed packet success rates, leading to a less certain estimate of the future success rates over the links (s, x) and (s, y). However, since the packet success rate over link (s, z) has historically been more steady, it may be a more reliable option. Hence, the source s can choose to fill p_3 to its capacity and partition the remaining 100 pkts/s equally over p_1 and p_2. This solution takes into account the historic variability in the packet success rates due to jamming mobility. In the following section, we build on this example, providing a set of parameters to be estimated by network nodes and methods for the sources to aggregate this information and characterize the available paths on the basis of expected throughput.

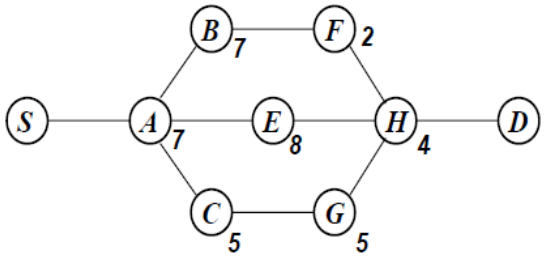
IV. PROPOSED MODEL

Numerous routing protocols are proposed for ad hoc networks. No existing protocol however, considers the load as the primary route selection criteria. Using only the shortest delay as the route metric can lead to network congestion and long delays (because of congestion). Additionally, most on-demand protocols use caching mechanisms for intermediate nodes to reply from cache, resulting routing load to concentrate on certain nodes. Recent simulation studies have shown that on-demand protocols that use shortest paths suffer from performance degradation as network traffic increases.

We present Dynamic Jamming-Aware Routing protocol that considers intermediate node routing loads for route selection metric. The protocol also monitors the congestion status of active routes and reconstructs the path when nodes of the route have their interface queue overloaded.

A. Route Selection Algorithms

We introduce the algorithm in selecting the least loaded route. We use Figure 3.3 as an example network to describe each scheme.



Route *i* : *(S - A - B - F - H - D)*
Route *j* : *(S - A - E - H - D)*
Route *k* : *(S - A - C - G - H - D)*

Figure 3: Exemplar network.

Scheme 1 of proposed algorithm simply adds the routing load of each intermediate node and selects the route with the least sum. If there is a tie, the destination selects the route with the shortest hop distance. When there are still manifold routes that have the least load and hop distance, the path that is taken by the packet which arrived at the destination earlier is chosen. In the exemplar network, route i has the sum of 20 (i.e., 7 + 7 + 2 + 4 = 20), route j has the sum of 19 (i.e., 7 + 8+ 4 = 19), and route k has the sum of 21 (i.e., 7 + 5 + 5 + 4 = 21). Therefore, route j is selected and used as the route.

Scheme 2 of proposed algorithm is similar to scheme 1. However, instead of using the sum of number of packets queued at each intermediate node's interface as in scheme 1, scheme 2 uses the average number of packets buffered at each intermediate node along the path. We can use the shortest delay as a tie breaker if needed.

Considering the example in Figure 3.3 again, route i has the average value of 5 (i.e., 20 / 4 = 5), route j has the value of 6.67 (i.e., 19 / 3 = 6.67), and route k has the value of 5.25 (i.e., 21 / 4 = 5.25). Route i is thus selected.

Scheme 3 of proposed algorithm considers the number of congested intermediate nodes as the route selection metric. Basically, it selects the route with the least number of intermediate nodes that have their load higher than the threshold value t . In our exemplar, if t is five, route i has two intermediate nodes (i.e., nodes A and B) that have the number of queued packets over the threshold, route j has two (i.e, nodes A and E), and route k has one (i.e, node A). Hence, route k is selected using this algorithm. This scheme applies the same tie breaking rule as in scheme 1.

Table 1: Route qualities based on each scheme

	Scheme 1	Scheme 2	Scheme 3
Route(i)	20	5	2 (A and B)
Route(j)	19	6.67	2 (A and E)
Route(k)	21	5.25	1(A)
Selection	Route(j)	Route(i)	Route(k)

Table 1 summarizes the route qualities in Figure 3 by applying each algorithm.

V. IMPLEMENTATION AND RESULT

In this section, we simulate various aspects of the proposed techniques for estimation of jamming impact and jamming- aware traffic allocation. The simulation results presented herein are obtained using the following simulation setup. A network of nodes is deployed randomly over an area, and links are formed between pairs of nodes within a fixed communication range. The set S of source nodes is chosen randomly, and the destination node d_s corresponding to each source $s \in S$ is randomly chosen from within the connected component containing.

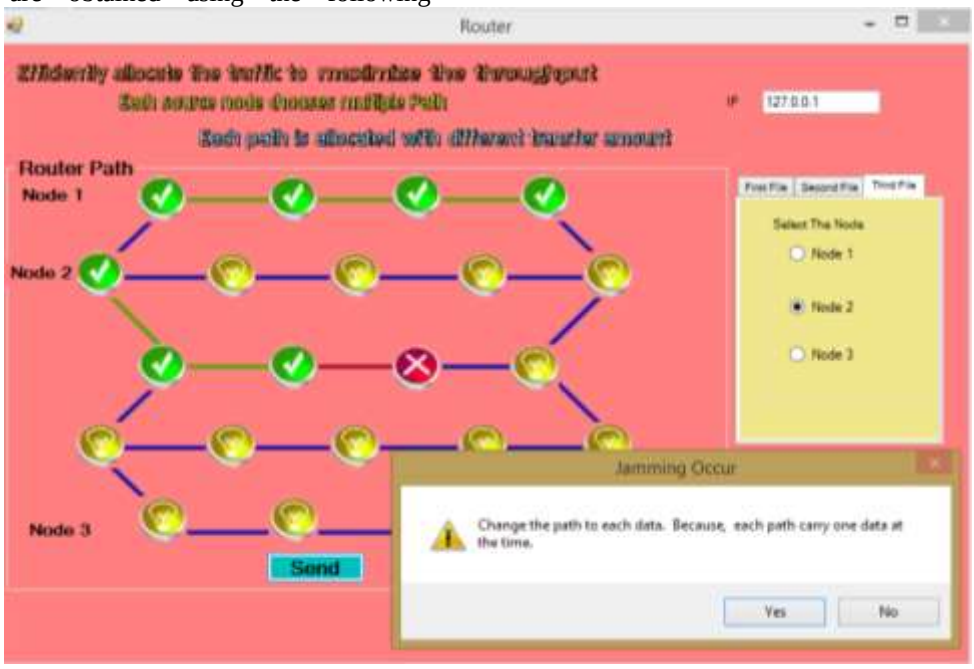


Figure 4.9: Router module

We have implemented the jamming aware traffic allocation concept in c# using .Net environment. The simulation shows that a source node is able to allocate traffic to different paths in the context of multiple-path source routing. The source node is jamming aware.

In order for a source node s to incorporate the jamming impact in the traffic allocation problem, the effect of jamming on transmissions over each link must be estimated. We develop a set of constraints imposed on traffic allocation solutions and then formulate a utility function for optimal traffic allocation. In order to define a set of constraints for the multiple-path traffic allocation problem, we must consider the source data rate constraints, the link capacity constraints, and the reduction of traffic flow due to jamming at intermediate nodes. Due to jamming at nodes along the path, the traffic rate is potentially reduced at each receiving node as packets are lost.

VI. CONCLUSION

This chapter characterized the impact of jamming in wireless sensor network. A Dynamic Jamming-Aware Routing protocol was presented in this chapter that considers intermediate node routing loads for route selection metric. The protocol also monitors the congestion status of active routes and reconstructs the path when nodes of the route have their interface queue overloaded.

REFERENCES

[1] D. Braginsky and D. Estrin, "Rumor Routing Algorithm for Sensor Networks," in Proceedings of the first Workshop on Sensor Networks and Applications, 28 Sept. 2002, Atlanta, USA, 2002, pp. 22–31.

[2] C. Schurgers and M.B. Srivastava, "Energy efficient routing in wireless sensor networks", in Proceedings of the IEEE Military Communications Conference (MILCOM), 28-31 Oct. 2001, Washington, USA, vol. 1, 2001, pp. 357–361 .

[3] R. C. Shah and J. Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks," in Proceedings of the IEEE Wireless Communications and Networking Conference, 17-21 Mar. 2002, Orlando, USA, vol. 1, 2002, pp. 350–355.

[4] C. Chong and S. P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges," in Proceedings of the IEEE, vol. 91, no. 8, pp. 1247–1256, Aug. 2003. [14] S. Mahlknecht, "WSSN (Wireless Self-sustaining Sensor Network) Project," 2005, http://www.ict.tuwien.ac.at/wireless/.

[5] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Computer Networks (Elsevier), vol. 38, pp. 393-422, 2002.

[6] G. Karayannis, "Emerging Wireless Standards: Understanding the Role of IEEE 802.15.4 & ZigBee in AMR & Submetering," 2003, http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=820.

[7] J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," IEEE Wireless Communications, vol. 11, no. 6, pp. 6–28, Dec. 2004.

[8] A. El-Hoiydi, "Spatial TDMA and CSMA with Preamble Sampling for Low Power Ad Hoc Wireless Sensor Networks", in Proceedings of the IEEE Symposium on Computers and Communications (ISCC), 1-4 July 2002, Taormina/Giardini Naxos, Italy, 2002, pp. 685–692.

[9] Chiang, J. T., & Hu, Y. Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks. IEEE/ACM Transactions on Networking, 19(1), 286-296.

[10] Jiang, S., & Xue, Y. (2009, October). Providing survivability against jamming attack for multi-radio multi-channel wireless mesh networks. Journal of Network and Computer Applications, 34(2), 443-454.

[11] Fu, Y., Yang, J., Xiao, P., Luan, L., & Peng, L. (2011, June). Research on Detection Scheme for Denial of Service Attacks in Wireless Mesh Networks. International Journal of Digital Content Technology and its Applications, 5(6), 290-296.

[12] Beg, S., Ahsan, F., & Mohsin, S. (2010, October). Engaging the Jammer on the Jammed Channel in MANET. International Conference on Emerging Technologies, 6, 410-413.