ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 8, October 2012

Avoid Impact of Jamming Using Multipath Routing Based on Wireless Mesh Networks

M. KIRAN KUMAR[1], M. KANCHANA[2], I. SAPTHAMI[3], B. KRISHNA MURTHY[4]
[1, 2], M. Tech Student, [3]Asst. Prof
[1, 4], Siddharth Institute of Engineering & Technology, Puttur, Andhra Pradesh, India.
2,3, Viswodaya Engineering College, Nellore, Andhra Pradesh, India.

Abstract---In this we address the dynamical jamming problem in wireless mesh networks and although some research has been conducted on countering Jamming attacks. Generally Multipath source routing protocols allow a data source node to distribute the total traffic among available paths. We consider the problem of jamming-aware source routing in which the source node performs traffic allocation based on empirical jamming statistics at individual network nodes. In this we formulate this traffic allocation as a lossy network flow optimization problem using portfolio selection theory from financial statistics. We demonstrate the network's ability to estimate the impact of jamming and incorporate these estimates into the traffic allocation problem. Finally, we simulate the achievable throughput using our proposed traffic allocation methods by using dynamic source routing protocols in centralized manner.

I. INTRODUCTION

Jamming point-to-point transmissions in a wireless mesh network or underwater acoustic network can have debilitating effects on data transport through the network. The effects of jamming at the physical layer resonate through the protocol stack, providing an effective denial-of-service (DoS) attack on end-to-end data communication.

The simplest methods to defend a network against jamming attacks comprise physical layer solutions such as spread-spectrum or beam forming, forcing the jammers to expend a greater resource to reach the same goal. However, recent work has demonstrated that intelligent jammers can incorporate cross-layer protocol information into jamming attacks, reducing resource expenditure by several orders of magnitude by targeting certain link layer. Source Routing (DSR) or Ad Hoc On-Demand Distance Vector (AODV) for example the MP-DSR protocol each source node can request several routing paths to the destination node for concurrent use. To make effective use of this routing diversity, however, each source node must be able to make an intelligent allocation of traffic across the available paths.The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration.

The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source *routes* to arbitrary destinations in the ad hoc network. The use of source routing allows packet routing to be trivially loop-free, avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded, and allows nodes forwarding or overhearing packets to cache the routing information in them for their own future use. Routing in wireless ad-hoc networks has received significant attention from recent literature due to the fact that the dynamic behavior, Though on-demand routing approaches have been shown to perform well, they generally lack the support for Quality-of-Service (QoS) with respect to data transmission. In order to select a subset of end to-end paths to provide increased stability and reliability of routes, a new QoS metric, end-to-end reliability, is defined and emphasized in this paper.

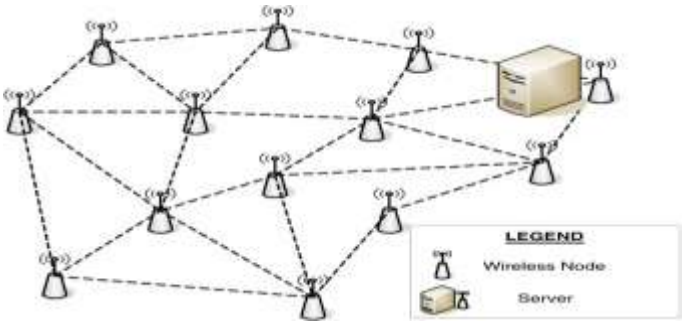

Fig.1 An example network with sources

A simulation study is performed to demonstrate the effectiveness of our proposed protocol, particularly the fact that MP-DSR achieves a higher rate of The majority of anti jamming techniques make use of diversity. For example, anti jamming protocols may employ multiple or multiple routing paths. Such diversity techniques help to curb the effects of the jamming attack by requiring the jammer to act on multiple resources simultaneously.

In this paper, we consider the anti jamming diversity based on the use of multiple 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 request several routing paths to the destination node for concurrent use. To make effective use of this routing diversity however, each source node must be able to make an intelligent allocation of traffic across the available paths while considering the potential effect of jamming on the resulting data through put. In order to characterize the effect 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 unknown 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,1 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 nondeterministic and dynamic effects of the jamming attack, I 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 effect of jamming at each node is probabilistic, the end-to-end throughput achieved by each source–destination pair will also successful packet delivery than existing best-effort ad-hoc routing protocols, such as the Dynamic Source Routing (DSR). Thus investigate the ability of network nodes to characterize the jamming impact and the ability of multiple source nodes to compensate for jamming in the allocation of traffic across multiple routing paths. My contributions to this problem are as follows.

We formulate the problem of allocating traffic across multiple routing paths in the presence of jamming as a lossy network flow optimization problem.

• We map the optimization problem to that of asset allocation using portfolio selection theory.

• We formulate the centralized traffic allocation problem for multiple source nodes as a convex optimization problem.

• We show that the multisource multiple-path optimal traffic allocation can be computed at the source nodes using a distributed algorithm based on decomposition in network utility maximization (NUM)].

• We propose methods that allow individual network nodes to locally characterize the jamming impact and aggregate this information for the source nodes.

• We demonstrate that the use of portfolio selection theory allows the data sources to balance the expected data throughput with the uncertainty in achievable traffic rates.

II. SYSTEM MODEL AND ASSUMPTIONS

The wireless network of interest can be represented by a directed graph. The vertex set represents the network nodes, and an ordered pair of nodes is in the edge set if and only if node can receive packets directly from node. I assume that all communication

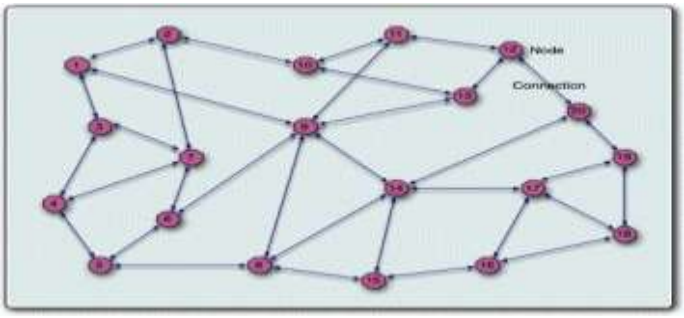

Fig.2. Example network with sources is uni cast over the directed edges, i.e., each packet transmitted by node is intended for a unique node with. The maximum achievable data rate, or capacity, of each uni cast link in the absence of jamming is denoted by the predetermined constant rate in units of packets per second.

In this paper, I assume that the source nodes in have no prior knowledge about the jamming attack being performed. That is, I make no assumption about the jammer's goals, method of attack, or mobility patterns I assume that the number of jammers and their locations are unknown to the network nodes. Instead of relying on direct knowledge of the jammers,

$$Gs = (Ns = \sum_{i=1}^{Ls}) \{j: (i,j) \epsilon Psl\}, es = \sum_{i=1}^{Ls} Psl)$$

We suppose that the network nodes characterize the jamming impact in terms of the empirical packet delivery rate. Network nodes can then relay the relevant information to the source nodes in order to assist in optimal traffic allocation. Each time a new routing path is requested or an existing routing path is updated, the responding nodes along the path will relay the necessary parameters to the source node as part of the reply message for the routing path. Using the information from the routing reply, each source node is thus provided with additional information about the jamming impact on the individual nodes.

III. CHARACTERIZING THE IMPACT OF JAMMING

We propose techniques for the network nodes to estimate and characterize the impact of jamming and for a source node to incorporate these estimates into its traffic allocation. In order for a source node to incorporate the jamming impact in the traffic allocation problem, the effect of jamming on transmissions over each link must be estimated. and relayed to. However, to capture the jammer mobility and the dynamic effects of the jamming attack, the local estimates need to be continually updated. I 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.

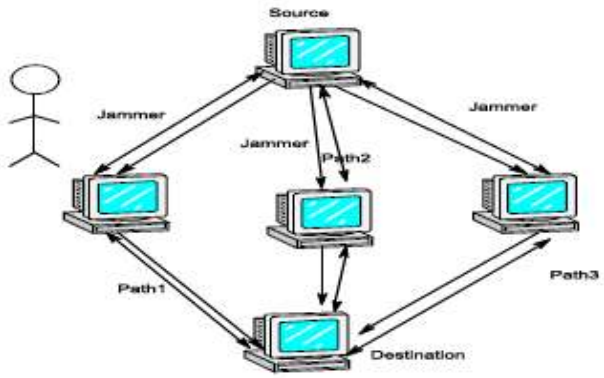

Fig.3. Example network with sources is uni cast over the directed edges

A. Illustrating the Effect of Jammer Mobility on Network Throughput.

Fig. illustrates a single-source network with three routing paths, and. The label on each edge is the link capacity indicating the maximum number of packets per second (pkts/s) that can be transported over the wireless link. In this example, I 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 is transmitting at high power, the probability of successful packet reception, referred to as the packet success rate, over the link drops to nearly zero, and the traffic flow to node 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 thus recovering from the jamming attack at node. However, this one-time reallocation by the source node does not adapt to the potential mobility of the jammer. If the jammer moves to node the packet success rate over returns to 1, and that over drops to zero, reducing the throughput to node 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 , 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 and, causing the packet success rates over links and to oscillate between zero and one. This behavior 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 and . However, since the packet success rate over link has historically been more steady, it may be a more reliable option. Hence, the source can choose to fill to its capacity and partition the remaining 100 pkts/s.In the following section.

B. Estimating Local Packet Success Rates

I denote the packet success rate over link at time, noting that can be computed analytically as a function of the transmitted signal power of node , the signal power of the jammers, their relative distances from node , and the path loss behavior of the wireless medium. In reality, however, the locations of mobile jammers are often unknown, and, hence, the use of such an analytical model is not applicable. Due to the uncertainty in the jamming impact, I model the packet success rate as a random process and allow the network nodes to collect empirical data in order to characterize the process. The shorter update period of s allows each n characterize the variation in over the update relay period of s, a key factor in . I propose the use of the observed packet delivery ratio (PDR) to compute the estimate .This PDR can be used to update the estimate at the end of the update period. In order to prevent significant variation in the estimate

$$PSEij([r-R,r]) = \frac{Vij([T-T,t])}{rij([t-T,t])}$$

and to include memory of the jamming attack history, I suggest using an exponential weighted moving average (EWMA). to the corresponding destination is negligible compared to the update relay period , I drop the time index and address the end-to-end packet success rates in terms of the estimates and. The end-to-end packet success rate for path can be expressed as the product which is itself a random variable due to the randomness in each. I let denote the expected value of , and denote the covariance of and for paths , .Due to the computational burden associated with in-network inference of correlation between estimated random variables, I let the source node assume the packet success rates as mutually independent, even though they are likely correlated.

We maintain this independence assumption throughout this work, yielding a feasible approximation to the complex reality of correlated random variables, and the case of in-network inference of the relevant correlation is left as future work. Under this independence assumption, the mean is equal to the product of estimates as

$$\square sl = \sum_{j=1}^{Psl} \mu ij$$

IV. OPTIMAL JAMMING-AWARE TRAFFIC ALLOCATION

In this section, we present an optimization framework for jamming-aware traffic allocation to multiple routing paths in for each source node. We develop a set of constraints imposed on traffic allocation solutions, and then formulate a utility function for optimal traffic allocation by mapping the problem to that of portfolio selection in finance. Letting denote the traffic rate allocated to path by the source node , the problem of interest is thus for each source to determine the optimal rate allocation vector subject to network flow capacity constraints using the available statistics and of the end-to-end packet success rates under jamming.

A. Traffic Allocation Constraints

In order to define a set of constraints for the multiple-path traffic allocation problem, I must consider the source data rate constraints, the link capacity constraints, and the reduction of traffic flow due to jamming at intermediate nodes. The traffic rate allocation vector is trivially constrained to the nonnegative or than , i.e., , as traffic rates are nonnegative.

B. Optimal Traffic Allocation Using Portfolio Selection

Theory In the distributed formulation of the algorithm, each source determines its own traffic allocation, ideally with minimal message passing between sources. By inspection, I see that the optimal jamming-aware flow allocation problem in is similar to the NUM formulation of the basic maximum network flow problem.

V.PERFORMANCE EVALUATION

In this section, we simulate various aspects of the proposed techniques for estimation of jamming impact and jamming-aware traffic allocation.

VI. CONCLUSION

In this paper, we studied the problem of traffic allocation in multiple-path routing algorithms in the presence of jammers whose effect can only be characterized statistically. I have presented methods for each network node to probabilistically characterize the local impact of a dynamic jamming attack and for data sources to I presented simulation results to illustrate the impact of jamming dynamics and mobility on network throughput and to demonstrate the efficacy of our traffic allocation algorithm. I have thus shown that multiple-path source routing algorithms can optimize the throughput.

REFERENCES

[1] R.A.Poisel,Modern Communication Jamming Principles and Tech- niques. Artech House, 2004.
[2] I.F.Akyildiz,X.Wang, and W. Wang, "Wirelessmeshnetworks:Asurvey,"Comput. Netw., vol.47, no. 4, pp. 445–487, Mar. 2005.
[3] E. M. Sozer, M. Stojanovic, and J. G. Proakis, "Underwater acoustic networks," IEEE J. Ocean. Eng., vol.25, no.1, pp. 72–83, Jan.2000.
[4] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. NewYork: Wiley, 2001.
[5] J. Bellardo and S. Savage, "802.11 denial-of-Service attacks: Real vulnerabilities and practical solutions," in Proc. USENIX Security Symp.,Washington, DC,Aug. 2003, pp. 15–28.
[6] D. J. Thuente and M. Acharya, "Intelligent Jamming in wireless networks with applications to 802.11 b and other networks," in Proc. 25th IEEE MILCOM, Washington, DC, Oct. 2006, pp. 1–7
[7] A. D.Wood and J. A. Stankovic, "Denial of service in sensor networks," Computer, vol. 35, no. 10, pp. 54–62, Oct. 2002