International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 1, January - 2014

Multiple-Path Routing to Avoid Congestion in Wireless Traffic Using Portfolio Selection Theory

Seemanaaz Khan
4th semester *M.E.(VLSI & Embedded system)*
NBN sinhgad school of engineering, Ambegaon,Pune,India

Prof. S. D. Sawant
M.Tech(Power Electronics)

Abstract

Wireless mesh networks (WMNs) consist of mesh routers and mesh clients, where mesh routers have minimal mobility and form the backbone of WMNs. In this paper, we consider the problem of jamming-aware source routing in which the source node performs traffic allocation based on experimental jamming statistics at individual network nodes. We formulate this traffic allocation as a lossy network flow optimization problem using portfolio selection theory in the form of financial flow of assets. We show that in multisource networks, the optimization of a single network problem can be solved using a distributed algorithm based on decomposition in network utility maximization (NUM).

1. Introduction

Jamming in a wireless mesh network [2] can have debilitating effects on data transport through the network. The effects of jamming at the physical layer arise through the protocol stack, providing an effective denial-of-service (DoS) attack on end-to-end data communication. The simplest methods to protect 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 and MAC implementations as well as link layer error detection and correction protocols. Hence, more sophisticated anti jamming methods and defensive measures must be incorporated into higher layer protocols. Using multiple-path variants of source routing protocols such as Dynamic Source Routing (DSR) [7] or Ad Hoc On-Demand Distance Vector (AODV) [6][7], 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 throughput. 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, 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.

We assume that the network does not rely on a jamming detection, localization, or tracking infrastructure [5]. We note that factors other than jamming that similarly impact throughput can be included as well. We focus on jamming in this work as it is likely the prominent source of packet loss. To capture the nondeterministic and dynamic effects of the jamming attack, 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 effect of jamming at each node is probabilistic, the end-to-end throughput achieved by each source destination pair will also be nondeterministic and, hence, must be studied using a stochastic framework.

2. Related Work

Wireless networks are susceptible to numerous security threats due to the open nature of the wireless medium [2]. Anyone with a transceiver can eavesdrop on ongoing transmissions, inject spurious messages, or block the transmission of legitimate ones. One of the fundamental ways for degrading the network performance is by jamming wireless transmissions. In the simplest form of jamming, the adversary corrupts transmitted messages by causing electromagnetic interference in the network's operational frequencies, and in proximity to the targeted receivers.

For an adversary agnostic to the implementation details of the network, a typical jamming strategy is the continuous emission of high-power interference signals such as continuous wave tones, or FM modulated noise [5]. However, adopting an "always-on" jamming strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of high interference levels makes this type of jamming easy to detect. Third, these attacks are easy to mitigate either by spread spectrum communications, spatial retreats, or localization and removal of the jamming nodes.

Continuous jamming has been used as a denial-of-service (DoS) attack against voice communication since the 1940s. Recently, several alternative jamming strategies have been demonstrated. Xu et. al. categorized jammers into four models,

(a) a constant jammer that continuously emits noise,

(b)a deceptive jammer that continuously broadcasts fabricated messages or replays old ones,

(c)a random jammer that alternates between periods of continuous jamming and inactivity,

(d)a reactive jammer who jams only when transmission activity is detected.

Hopping between radio channels, controlled at the software-level, has been proposed to mitigate jamming in wireless sensor networks and 802.11 networks for nodes equipped with one radio [2]. So far, proactive, or periodic, hopping has received more attention because of its implementation simplicity and the overhead and difficulty of jamming detection.

Reactive strategy is one of the most used in multi radio networks to detect jamming. In the reactive strategy, each radio stays at its current channel until it detects jamming. It then switches to a different channel selected uniformly at random using a securely seeded random-number generator. We consider the case where only the sender has to detect jamming, because the receiver (e.g., the base station) has enough transceivers to always listen to all the channels. Jamming may keep the wireless medium busy, resulting in a long waiting-time to access the channel, or may corrupt packets by causing high interference at the receiver, resulting in excessive retransmissions. We use a simple jamming detection algorithm: if the waiting-time for a free channel or the number of transmissions exceeds a threshold, jamming is assumed and the radio hops to a different channel.

Proactive defense strategy is also used for jamming detection. In the proactive defense strategy, radios switch channels according to a pseudo-random schedule pre-loaded off-line [6]. Periodically, all the radios switch to different channels. The proactive strategy is oblivious to jamming status, so un jammed radios may be triggered to switch and jammed ones may be kept. Clock-synchronization is a requirement of the proactive strategy. However, loose clock synchronization is not difficult to achieve among radios on the same device (synchronization between sender and receiver is not needed in our model because the base station has enough transceivers to cover all possible channels).

Channel migration is also proposed as an alternative method to mitigating wireless jamming attacks. For resilience against jamming attacks, this scheme exploits the multiple wireless channels typically available on most wireless platforms. Each node estimates the qualities of the channels that it has a chance to observe. If it detects poor quality on its main communication channel, it leaves for a different channel for communication. As a result, a node currently on a jammed channel can continue communication with its neighbors on other available channels. A nice property of the channel migration scheme is that it does not depend on any single, fixed channel and executes in a decentralized and independent way on each wireless node.

To improve channel synchronization between neighbors, they developed an advertisement mechanism, which enables each node to periodically inform its neighbors using different communication channels about its current main communication channel. Such a mechanism enables each node to keep track of the statistics of different channels. When switching its main communication channel, each node uses the channel statistics to select the one where it possibly gets the most benefit.

The goal of a jammer is to prevent the wireless nodes within their signal range from receiving messages from their neighbor nodes. We assume that each jammer has the ability to sense and jam multiple channels of her choice concurrently, but cannot jam all available channels at the same time. In addition, we assume that the jammer dynamically switches channels she senses and jams, but stays on a channel at least for a certain amount of time, during which legitimate nodes on other available channels can transmit and receive one or more packets.

3. Research Methodology

A jammer may constantly, randomly, or reactively jam multiple channels at the same time. We assume that the source nodes have no prior knowledge about the jamming attack being performed. That is, we make no assumption about the jammer's goals, method of attack, or mobility patterns. We assume that the number of

jammers and their locations are unknown to the network nodes. Instead of relying on direct knowledge of the jammers, 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. Based on this information about each link, a source node gets the idea of probable packet error rate due to jamming at each link.

When source wants to send traffic, it must find all the paths to send the traffic at the first stage. Then it applies optical traffic allocation algorithm to split the traffic and send across the multiple paths found. Optimal traffic allocation policy applied for this follows from the Portfolio selection theory in finance domain proposed by Markowitz.

In Markowitz's portfolio selection theory [8] an investor is interested in allocating funds to a set of financial assets that have uncertain future performance. The expected performance of each investment at the time of the initial allocation is expressed in terms of return and risk. The return on the asset corresponds to the value of the asset and measures the growth of the investment. The risk of the asset corresponds to the variance in the value of the asset and measures the degree of variation or uncertainty in the investment's growth. We equate the solution proposed by Markowitz for investment split across multiple schemes [9], to be used for the case of splitting the traffic across multiple paths.

4. Distributed Jamming Aware Traffic Allocation Algorithm

Initialize n=1 with initial link prices $\alpha 1$

1. Each source s independently computes

$\beta^*_{s,n}=\arg\max (\mu_s^T - \alpha_n^T W_s)\, \beta_s - K_s \beta_s^T \Pi_s \beta_s^T$

2. Source exchange link usage vectors

$u_{s,n}=W_s \beta^*_{s,n}$

3. Each source likely updates link prices as

3. Each source likely updates link prices as

$\alpha_{n+1}=[\alpha_n - a(c - \Sigma u_{s,n})]$

4. If $|\beta^*_{s.n} - \beta^*_{s.n-1}| > \varepsilon$

For any s, increment n and go to step 1 where 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 Ds corresponding to each source s € S is randomly chosen from within the connected component containing s. Each routing path in the set S is chosen using a randomized geometric routing algorithm which chooses the next hop toward the destination Ds from the set of neighboring nodes that are closer to in terms of either distance or hop-count. Nodes transmit using fixed power Pt.

Table .1.Parametrs for traffic allocation

Traffic allocation	
Source data rate	S_d
Routing paths	P_s
Expected packet success rate	$\mu_{s,l}$
Traffic allocation	β_s
Mean throughput	$\mu_s^T \beta_s$
Estimation variance	$\beta_s^T \Pi_s \beta_s$

A. Characterizing the 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.

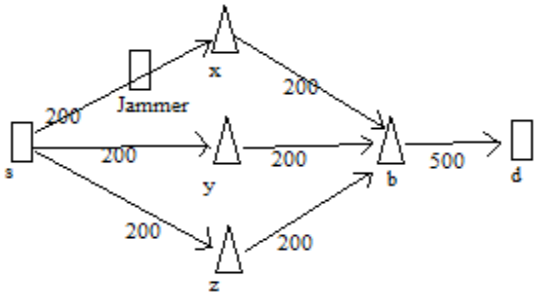

Figure1: Example network that illustrates a single-source network with 3 routing paths.

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 (i,j) belongs to ε_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. In the figure each unicast link (i,j) is labeled with the corresponding link capacity $C_{i,j}$ in units of packets per second. The proximity of the jammer to nodes a and b impedes packet delivery over the corresponding paths, and the jammer mobility affects the allocation of traffic to the three paths as a function of time.

B. Jammer Mobility on Network Throughput

Fig.1 illustrates a single-source network with 3 paths p1={(s,x),(x,b),(b,d)} p2={(s,y),(y,b),(b,d)} and p3={(s,z),(z,b),(b,d)}. 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, 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 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 paths p1 and p2, 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 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 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 s and x. However, since the packet success rate over link has historically been steadier, it may be a more reliable option. Hence, the source can choose to fill to its capacity and partition the remaining 100 pkts/s equally over s and b. 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**.**

REFERENCES

[1]Patrick Tague, Sidharth Nabar, James A. Ritcey, and Radha Poovendran" Jamming-Aware Traffic Allocation for Multiple-Path Routing Using Portfolio Selection",IEEE/ACM Transactions On Networking, Vol. 19, No. 1, Feb 2011.

[2] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," *Comput. Netw.*, vol. 47, no. 4, pp. 445–487, Mar. 2005.

[3] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11 b and other networks," in *Proc. 25thIEEE MILCOM*, Washington, DC, Oct. 2006, pp. 1–7.

[4]A. D.Wood and J. A. Stankovic, "Denial of service in sensor networks,"*Computer*, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[5] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Netw.*, vol. 20, no. 3, pp. 41–47,May/Jun. 2006.

[6] E. M. Royer and C. E. Perkins, "Ad hoc on-demand distance vector routing," in *Proc. 2nd IEEE WMCSA*, New Orleans, LA, Feb. 1999, pp. 90–100.

[7]C.SivaRam Murthy and B.S.Manoj, "Ad-Hoc Wireless Networks, Architectures and protocols", 2003

[8] H. Markowitz, "Portfolio selection," *J. Finance*, vol. 7, no. 1, pp. 77–92, Mar. 1952.

[9] W. F. Sharpe, *Investors and Markets: Portfolio Choices, Asset Prices, and Investment Advice*. Princeton, NJ: Princeton Univ. Press, 2007.

[10] Harry Markowitz, *Portfolio Selection theory* Wikipedia, the free encyclopedia.