ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

Interference Awake Trade Allotment for Multipath Routing Using Reinforcement Learning Algorithm

SangeethaPriya Mohan[1] , Saradha Sekar[2] , Devipriya Chinnasamy[3] , Lavanya Krishnasamy[4]

Master of Engg., Computer Science Engg. Department, SECE, Coimbatore, India[1]

Master of Engg., Computer Science Engg. Department, SECE, Coimbatore, India[2]

Master of Engg., Computer Science Engg. Department, SECE, Coimbatore, India[3]

Master of Engg., Computer Science Engg. Department, SECE, Coimbatore, India[4]

Abstract – Multiple-path source routing protocols allow a data source node to distribute the total traffic among available paths .This paper proposes technique 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. And we have shown that in multi-source networks, this centralized optimization problem can be solved using a distributed algorithm based on decomposition in network utility maximization. We formulate this traffic allocation as a lossy network flow optimization problem using portfolio selection theory from financial statistics which 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.

Keywords: Jamming, Traffic, Optimization, Multi-Source Network, Rate Adaptation.

I.INTRODUCTION

A jamming attack can cause the following effects in an 802.11 network: 1) due to carrier sensing, co channel spreaders defer their packet transmissions for prolonged periods; and 2) the jamming signal collides with legitimate packets at receivers. Frequency-hopping techniques[6] have been previously proposed for avoiding jammers. Such schemes, however, are not effective in scenarios with wideband jammers. Furthermore multiple jamming devices operating on different channels can significantly hurt performance in spite of using frequency hopping. Measurement- driven system, which detects the presence of jammers and invokes rate adaptation and power control strategies to alleviate jamming effects[4]. Clearly, not much can be done to mitigate jammers with unlimited resources in terms of transmission power and spectrum efficiency. Note, however, that in a plurality of cases the jamming device can be resource-constrained, with capabilities similar to that of the legitimate device.2 Portable, battery-operated jammers are typically configured[11] to transmit intermittently and sometimes at low power in order to conserve energy and harm the network for extended periods of time. In addition, misconfiguration of "legitimate" devices can transform them to resource-constrained jammers. In such cases, ARES can effectively fight against the harmful entity, as we discuss later. Our contributions are the following. Understanding the impact of jammers in an 802.11 network with rate/power control[12].

First, we perform an in-depth measurement-based experimental study on our indoor test-bed
to quantify the impact of jamming when employing rate and/or power switch. To the best of our information, there are no such studies to date. With rate control, a spreader can increase or decrease its spread rate depending on the observed packet delivery ratio (PDR)[6] at the receiver. With power control, nodes may increase their transmission powers
and/or clear channel assessment (CCA)[15] thresholds in order to increase the probability of successful packet reception. The design of ARES is driven by two key investigational notes.

Designing ARES, a novel anti-jamming system. The above observations drive the design of ARES. ARES primarily consists of two modules. The rate control module chooses between fixed-rate assignment and rate adaptation, based on channel conditions and the jammer characteristics. The primary objective of this module is to effectively utilize the periods when a jammer is asleep. The power control module adjusts the CCA threshold to facilitate the transmission and the reception (capture) of legitimate packets during jamming[9]. Care is taken to avoid starvation of nodes due to the creation of asymmetric links. This module is used to facilitate successful communications while the jammer is active. Although rate and power control have been proposed as interference alleviation techniques, their behaviour has not

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

been studied in jamming environments. To our knowledge, our work is the first to conduct such a study. Implementing and experimentally validating ARES. We implement and evaluate the modules of ARES on real hardware, thereby making ARES one of the few anti-jamming system implementations for 802.11 networks[11]. ARES relies on the existence of an accurate jamming detection module. It is beyond the scope of our work to design a new detection scheme, and thus we incorporate a mechanism proposed previously in [14]. To demonstrate the effectiveness and generality of our system, we apply it on three different experimental networks: an 802.11n WLAN with multiple-input–multiple-output (MIMO)-enabled nodes, an 802.11a/g mesh network with mobile jammers, and a static 802.11a WLAN with uplink TCP traffic[17]. Our measurements demonstrate that ARES provides performance benefits in all the three networks. Throughput improvements of up to 150% are observed.

A. *Types of Jamming Attacks*

1) *Nonstop Jamming*: Constant jammers continuously emit electromagnetic energy on a channel. Nowadays, constant jammers are commercially available and easy to. While constant jammers emit no readable messages, deceiving jammers transmit seemingly legitimate back-to-back dummy data packets. Hence, they can mislead monitoring systems and other nodes into believing that legitimate traffic is being sent.

2) *Intermittent Jamming*: As the name suggests that these jammers are active intermittently; the primary goal is to conserve battery life. And the random jammer typically alternates between the sleeping periods and uniformly distributed jamming. It jams for s, and then it sleeps for s. A reactive jammer starts emitting energy only if it detects traffic on the medium. This makes the jammer difficult to detect the jamming and implementing reactive jammers can be a challenge.

II. SYSTEM MODEL

The wireless model of network can be defined by a directed graph as G=(N,S). The vertex N represented the network nodes and the ordered pair (i,j) is the edge set.

We assume that every transmission of packets are unicast over the directed edge graph. The maximum capacity and achievable data rate ,of each unicast link is(i,j).

This is an example network with source node *S*={r,s}.

And the sub graph Gr consists of the two routing path

Pr1= {(r,i),(i,k),(k,m),(m,u)}

Pr2= {(r,i),(i,j),(j,n),(n,u)}

The sub graph Gs consists of the two routing path

Sr1= {(s,i),(i,k),(k,m),(m,t)}

Sr2= {(s,j),(j,n),(n,m),(m,t)}

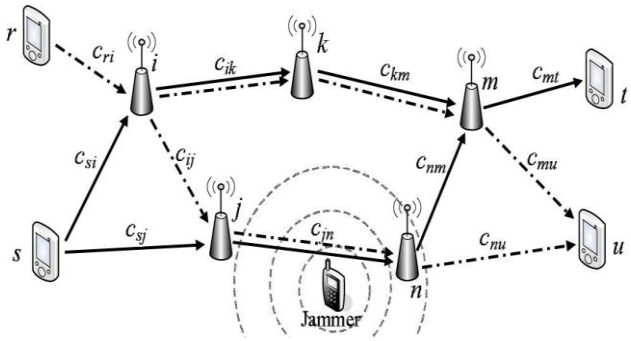

Fig:1 Example network with source node *s,r*.

A. *Impact Of Jamming*

In this the network nodes should characterize the impact of jamming. The source node *S* is to calculate the jamming impact in the traffic allocation problem. And also the effect of jamming is transmitted over a link (i,j) with respect to *S*.

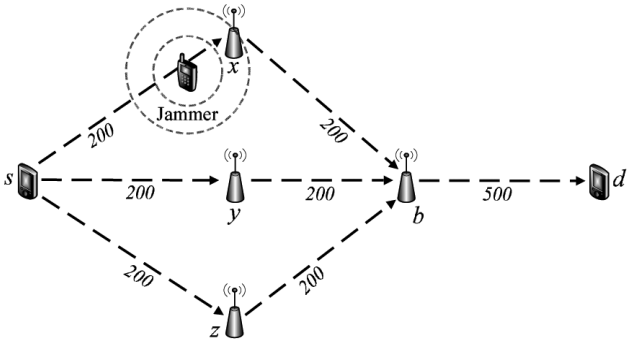

Fig:2 Example network with single source and three routing paths

The jammer mobility on network nodes can be calculated using above figure. Which illustrate the single source with three routing paths.

The routing paths are

P1= {(s,x),(x,b),(b,d)},

P2= {(s,y),(y,b),(b,d)},

P3= {(s,z),(z,b),(b,d)}.

The source node can send only the minimum amount packets at the time with any of these paths.

B. *End-to-End Packet Success Rates*

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

The packet success rate can estimates μ_{ij} and σ_{ij}^2 for the link(i,j) in the given routing path p_{sl}. And the source node *S* to estimate the end to end packet success rate to determine the traffic allocation in the routing path.

The end-to-end packet success rates y_{sl} for path p_{sl} can be expressed as the product,

$$y_{sl} = \prod_{(i,j)\varepsilon P_{sl}} x_{ij}$$

γ_{sl} represent the expected value of y_{sl}

$$\gamma_{sl} = \prod_{(i,j)\varepsilon P_{sl}} \mu_{ij}$$

W_{slm} denotes the covariance of y_{sl} and y_{sm} for paths p_{sl} and p_{sm}

covariance $w_{slm} = E[y_{sl}\, y_{sm}] - E[y_{sl}]E[y_{sm}]$ is given by,

$$w_{slm} = \prod_{(i,j)\varepsilon P_{sl}+P_{sm}} \mu_{ij} \prod_{(i,j)\varepsilon P_{sl}\Pi P_{sm}} (\sigma_{ij}^2 + \mu_{ij}^2) - \gamma_{sl}\,\gamma_{sm}$$

III.GUIDELINES FOR RATE ADAPTATION *[REINFORCEMENT LEARNING ALGORITHM]*

Rate adaptation algorithms are utilized to select an appropriate transmission rate as per the current channel conditions. As interference levels increase, lower data rates are dynamically chosen. Since legitimate nodes consider jammers as interferers, rate adaptation will reduce the transmission rate on legitimate links while jammers are active. Hence, one could potentially argue the rate control for the legitimate links increases reliability by reducing rate and can thus provide throughput benefits in jamming environments.

A. *Details on the Experimental Process:*

We perform experiments with both single-hop and multi hop configurations. In each experiment, we first load the particular rate-control Linux-kernel module on the wireless cards of legitimate nodes. We initiate data traffic between the nodes and activate the jammer after a random time. We collect throughput measurements on each data link once every 500 ms. we use the following terminology.

1) Fixed transmission rate (R_f): This is the nominal transmission rate configured on the wireless card.

2) Saturated rate (R_s): It is the rate achieved when R_f is chosen to be the rate on the wireless card.

In order to compute R_s, for a given R_f, we consider links where the PDR is 100% for the particular setting of R_f. We then measure the rate achieved in practice. We notice that for lower values of the specified rate is actually achieved on such links. However, for higher values of (as an example, Mb/s), the achieved data rate is much lower; this has been observed in other work. Derived from measurements on our test-bed, between and .Application data rate: This is the rate at which the application generates data.

It is difficult (if not impossible) to a priori determine the best fixed rate on a link. Given this, and if we let be the set of all possible fixed transmission rates,

$$R_f = \{\min_{x\in R} x : x \geq R_a\}$$

which is the maximum rate that is required by the application (we discuss the implications of this choice later). Our key observations are summarized as follows.

•Rate adaptation algorithms implement poorly on high-quality links due to the long times that they incur for converging to the appropriate high rate.

•On lossless connections, the fixed rate is better, while rate adaptation is beneficial on lossy links.

We defer defining what constitute lossless or lossy links. Conceptually, we consider lossless links to be those links that can achieve higher long-term throughput using a fixed transmission rate. And Rf rather than by applying rate adaptation.

B. *Single-Hop Configurations*:

Our experiments with one-hop connectivity involve 80 sets of sender–receiver pairs and one jammer per pair. We enforce that a jammer interferes with one link at a time and that the legitimate data links do not interfere with each other. Thus, we perform 20 different sets of experiments, with four isolated data links and four jammers in each experiment.

C. *Rate Adaptation*:

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

Wireless test-bed and the experimental methodology are used. The faced and the design decisions that we had to make based on technical reasons, and some other times due to practicalities. These design tests involve:

1. The accessibility to the software, in order to modify and implement various functionalities
2. physical extend ability, in order to add hardware in the future
3. And manageability, in order to configure and update the software quickly and easily for all the nodes in the network. We explain the hardware and software design choices that we make in order to enable these requirements.

For ease of maintenance and convenience, each node is diskless, and we utilize power-over-ether net through an Ethernet connection with a centralized server. We confirm that the software can be easily modified; this provides for easier module implementation and parameter tuning. We explain the different ways of node arrangement, results that we make on power settings and discuss how and why the receiver sensitivity affects deployment decisions. At the last, we present our observations based on a set of measurements to quantify the stability of the links in our test bed.

Rate Adaptation Consumes a Significant Part of the Jammer's Sleep Time to Converge to the Appropriate Rate: As soon as the jammer "goes to sleep," the quality of connection improves, and thus there will be progressive increase in the rate control algorithm. However, since the purpose of a jamming attack is to corrupt as many transmissions as possible, the jammer will typically not sleep for a long time. In such a case, the sleep duration of the jammer will not be enough for the rate control to reach the highest rate possible. To illustrate this, we choose two links on our test-bed, one that can support 12 Mb/s and the other that can support 54 Mb/s. Fig. 2 depicts the results. We observe the following: 1) irrespective of whether Sample Rate or a fixed rate plan is used, during jamming, the throughput drops to values close to zero since the jammer blocks the medium for the sender; and 2) the through put achieved with Sample Rate is fairly low, and much lower than if we fix the rate to the constant value of 12 Mb/s. Note that we have observed the same behaviour with AMRR and One.

Fixed Rate Assignment Outperforms Rate Adaptation on Lossless Links: As was alluded to, in order to find the best rate on a link after a period where there is no throughput due to a jammer, the rate adaptation mechanisms gradually increase the rate, invoking transmissions at all the lower rates interim, until the best rate is reached. For links that can inherently support high rates, this process might consume the sleep period of the jammer (as suggested by the results in Fig. 2). If the priori language of rate for a link is known, at the case that the jammer goes to snooze, transmissions may be invoked at that rate. This would utilize the sleep period of the jammer more effectively. As observed the throughputs achieved with fixed rate assignment are much higher than those achieved with rate adaptation on such links.

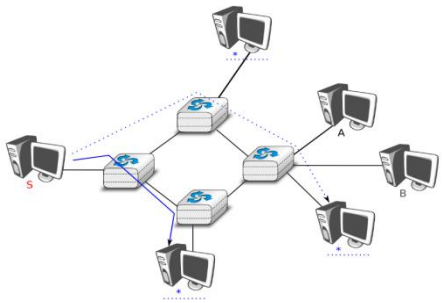

Fig:3 Single source with no.of Receiver

D. *Determining the Right Transmission Rate Policy*:

1. Implications of Setting:

$$R_f = \{\min_{x \in R} x : x \geq R_a\}$$

The application does not require the link to sustain a higher rate, the highest throughput for that application rate is reached either with this choice of or with some rate that is lower than. If the rate adaptation algorithm converges to a rate that results in a throughput that is higher than with the chosen, then the adaptive rate strategy should be used. If instead, during the jammer's sleep period, the rate adaptation technique is unable to converge to such a rate, the fixed rate strategy is better.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

2. Analytically Determining the Right Rate: In order to determine whether it is better to use a fixed- or an adaptive-rate approach for a given connection, we make an analysis based on the following parameters:
1) The supply of the jammer's active and sleep periods (we call this the jammer's distribution).
2) The application data rate .
3) The performance metric on the considered legitimate link, i.e., PDR, link throughput, etc.
4) The rate adaptation scheme that is employed, i.e., One, Sample Rate, etc. The key scheme-specific factor is the transition time from a lower rate to the next higher rate under conducive conditions.
5) The effectiveness of the jammer, measured by the achievable throughput while the jammer is on. The lower the throughput, the more effective the jammer.

E. ***Validation of Our Analysis***

In order to validate our analysis, we measure on 80 different links in the presence of a balanced jammer. We then compare them against the values computed with our analysis. Note here that the study itself depends on measured values of certain quantities (such as the jammer distribution and the function). In this experiment, we consider the Sample Rate algorithm and measure the values of and. The jammer's sleep time follows, and the jamming time follows. plots the values of function for different values of R_f.
The theoretically computed PDR thresholds to the ones measured on our test-bed for various values of R_f. We observe that the thresholds computed with our analysis are very similar to the ones measured on our test-bed. There are slight discrepancies since our analysis is based on using measured average values that may change to some extent over time. We wish to stress that while we verify our analysis assuming that the jammer is active and idle for uniformly distributed periods of time, our analysis depends only on expected values and is therefore valid for other jammer distributions. the advantage of using a fixed rate approach over Sample Rate for various PDR values and with Mbps. We observe that Sample Rate provides higher throughput only for very low PDR values. The jammer's sleeping and jamming time from distributions like that of the frequent jammer, we essentially construct a constant jammer. With frequent jammers, the difference in the performance between fixed rate assignment and rate adaptation is larger, while for a rare jammer this is smaller. This is because with rare jamming, rate adaptation has more time to converge and therefore often succeeds in achieving the highest rate possible; one observes the opposite effect when we have a frequent jammer.

F. ***Random Jamming in Multi hop Topologies***

We experiment with 15 different routes on our test-bed. We fix static routes of various lengths (from two to four links per route) utilizing the route Unix tool in order to modify the routing tables of nodes. We place a jammer such that it affects one or more links. Along each route, links that are not affected by the jammer consistently use a rate adaptation algorithm. On the links that are subject to jamming, our analysis dictates the decision on whether to use fixed or adaptive rate assignment. We measure the end-to-end throughput on the route. We show our results for routes on which, in the absence of a jammer, end-to-end throughput of 6 and 12 Mb/s was observed. From, we see that the throughput trend with rate adaptation on multi hop routes in the presence of a random jammer is the same as that on a single-hop link. In particular, with low data rates, a sufficiently high PDR has to be sustained over the links that constitute the route in order for a fixed-rate approach to perform better than rate adaptation. On the other hand, when routers care high data rates, fixing the rate on the individual links (that are affected by the jammer), as per our logical framework, delivers higher benefits.

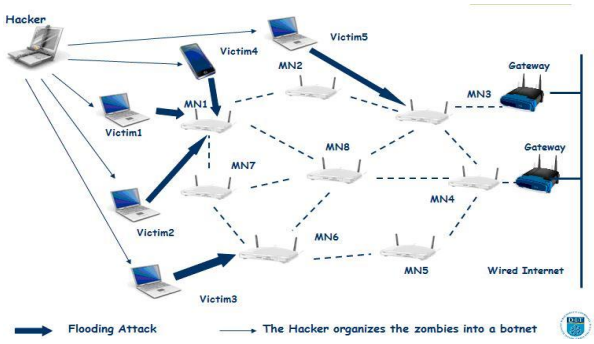

Fig:4 Example for flooding networks

G. ***Choosing the Right Policy in Practice*****:**

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

To summarize our findings, our analysis demonstrates that using a fixed rate may be attractive on lossless links, while it would be better to use rate adaptation on lossy links. However, as discussed, determining when to use one over the other in real time during system operations is difficult. The purpose requires the knowledge of and estimates of how often the jammer is lively/asleep on average.

legitimate transmissions are invoked at the most recent rate used during the previous sleeping cycle of the jammer. We also perform offline measurements by directly using our analytical formulation (with knowledge of the aforementioned parameters). These measurements serve as benchmarks for evaluating the efficacy of MRC.

V. PERFORMANCE EVALUATION

In this section, we simulate various aspects of the proposed techniques for estimation of jamming impact and jamming-aware traffic apportionment. We first describe the simulation setup, including descriptions of the assumed models for routing path construction, estimate updates, packet success rates, jammer mobility. We then simulate the process of computing the estimation statistics $\mu_{ij}(t)$ and variance $\sigma_{ij}^2(t)$ for a single link **(i,j)** . Next, we illustrate the effects of the estimation process on the throughput optimization, both in terms of optimization objective functions and the resulting simulated throughput. Finally, we simulate a small-scale network similar to that in above figure while varying network and protocol parameters in order to observe performance trends.

Thus, we choose a simpler practical approach that we call MRC for Markova an rate control. We will describe MRC in detail later (in Section VI), but in a nutshell, MRC induces memory into the system and keeps track of the feasible rates during benign jamming-free periods. As soon as the jammer goes to sleep,

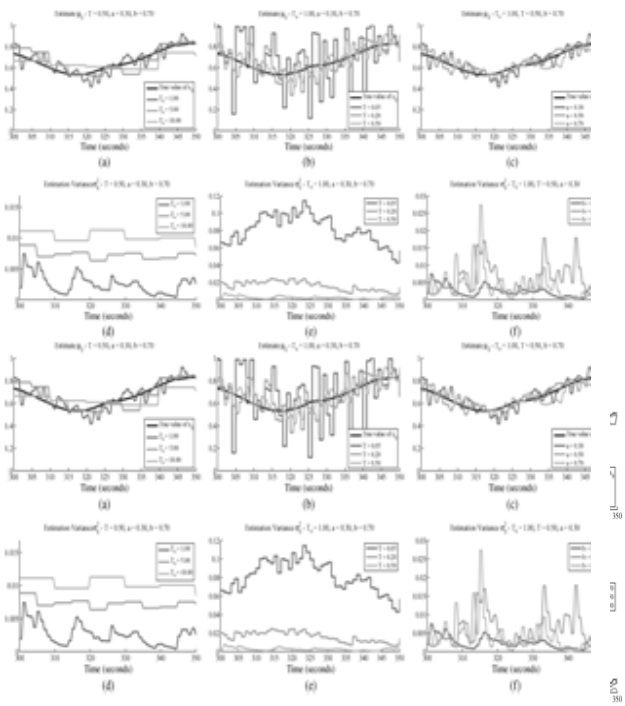

Fig:5 Throughput Analysis

A. *Simulation Setup*

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 $s \varepsilon S$ is randomly chosen from within the connected component containing. Each routing path in the set P_S is chosen using a randomized geometric routing algorithm which chooses the next hop toward the destination d_s from the set of neighbouring nodes that are closer d_s to in terms of either distance or hop-count. Nodes transmit using fixed power P_t.

B. *Simulation Of Estimation Process*

First simulate the process of computing the estimate $\mu_{ij}(t)$ and the variance $\sigma_{ij}^2(t)$ over a single link **(i,j)** Figure shows the true packet success rate $x_{ij}(t)$ with the estimate $\mu_{ij}(t)$ and the estimation variance $\sigma_{ij}^2(t)$ for various parameter values. By inspection of Figure, we see that a shorter update relay period and a longer update period T yield a more consistent estimate $\mu_{ij}(t)$ with less variation around the true value of $x_{ij}(t)$. In addition, a smaller value of allows the estimate $\mu_{ij}(t)$ to reflect rapid changes in $x_{ij}(t)$, while a larger value of smooth's the estimate $\mu_{ij}(t)$ over the sampled PDRs. We similarly see that a shorter update relay period T_S and a longer update period yield a lower estimation variance $\sigma_{ij}^2(t)$. In

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

addition, a smaller value of the EWMA coefficient β allows the estimation variance $\boldsymbol{\sigma_{ij}^2}$ **(t)** to primarily reflect recent variations in the sampled PDRs, while a larger value of β incorporates PDR history to a greater degree.

TABLE I
SUMMARY OF SIMULATION PARAMETERS

Parameter	Value
Network Area	500m x 500m
Radio Range	100m
Number of sources	$\|S\|$
Number of nodes	$\|N\|$=200
Maximum source data rate	R_s=200pkts/s
Maximum number of paths	$\|Ps\| \leq 5$
Transmission power	P_t=1 mW (0 dBm)
Link capacity	C_{ij}=500 pkts/s
Jamming Transmission Power	P_j=1 mW(0 dBm) V_{max}=5 m/s
Maximum jammer mobility speed	Ɛ=1.16
Packet error rate parameter	P=2.5 x 10^{-4}
Path-loss constant	*v*=2.7
Path-loss exponent	N=10^{-10}mW (-100 dBm)
Receiver Noise	α=0.7,β=0.3
EWMA coefficients	T=0.05s
Update period	T_s=2s
Update relay period	

C. *Network Simulation*

We next simulate the jamming-aware traffic allocation using the estimated parameters $\boldsymbol{\mu_{ij}(t)}$ and $\boldsymbol{\sigma_{ij}^2}$ **(t)** as described in Section V-A. To observe the effects of the jamming-aware formulation and the estimation process, we first compare the optimal expected throughput and the actual achieved throughput**.**

D. *Simulation Of Parameter Dependence*

Next evaluate the effect of varying network and protocol parameters in order to observe the performance trends using the jamming-aware traffic allocation formulation. In particular, we are interested in the effect of the update relay period $\mathbf{T}_S$ and the maximum number of routing paths $\mathbf{P}_S$ on the performance of the flow allocation algorithm. In order to compare trials with different update times or numbers of paths, we average the simulated results over each simulation run, yielding a single value for each trial.

VI. CONCLUSION

The problem of traffic in multi path routing algorithm with the presence of jammers. We introduce the method to each network node to characterize the jamming impact of dynamic jamming attack. And also data source to include this information into the routing algorithm. We express the multipath traffic allocation in multisource networks. It can be express as a lossy network flow optimization problem using the function based on reinforcement learning algorithm. This optimization problem can be solved using rate adaptation algorithm based on the Network Utility Maximization (NUM). We offered simulation results to show the impact of jamming and mobility on network throughput and to prove the effectiveness of our traffic allocation algorithm. And we shown the multipath traffic allocation algorithm is optimize the throughput performance by successfully including the empirical jamming impact with the traffic allocation into the set of routing paths.

REFERENCES

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," Comput. Netw., vol. 47, no. 4, pp. 445–487, Mar. 2005.
[2] 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.
[3] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. New York: Wiley, 2001.
[4] 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.
[5] 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.
[6] A. D.Wood and J. A. Stankovic, "Denial of service in sensor networks,"Computer, vol. 35, no. 10, pp. 54–62, Oct. 2002.
[7] G. Lin and G. Noubir, "On link layer denial of service in data wireless LANs,"Wireless Commun. Mobile Comput., vol. 5, no. 3, pp. 273–284, May 2005.
[8] 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.
[9] D. B. Johnson, D. A. Maltz, and J. Broch, DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks. Reading,MA: Addison-Wesley, 2001, ch. 5, pp. 139–172.
[10] 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.
[11] R. Leung, J. Liu, E. Poon, A.-L. C. Chan, and B. Li, "MP-DSR: A QoS-aware multi-path dynamic source routing protocol for wireless ad-hoc networks," in Proc. 26th Ann. IEEE LCN, Tampa, FL, Nov.2001, pp. 132–141.
[12] H. Markowitz, "Portfolio selection," J. Finance, vol. 7, no. 1, pp.77–92, Mar. 1952.
[13] S. Boyd and L. Vandenberghe, Convex Optimization. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[14] D. P. Palomar and M. Chiang, "A tutorial on decomposition methods for network utility maximization," IEEE J. Sel. Areas Commun., vol. 24, no. 8, pp. 1439–1451, Aug. 2006.
[15] M. Evans, N. Hastings, and B. Peacock, Statistical Distributions, 3rd ed. New York: Wiley, 2000.
[16] S. W. Roberts, "Control chart tests based on geometric moving averages," Technometrics, vol. 42, no. 1, pp. 97–101, Feb. 2000.
[17] I. R. James, "Products of independent beta variables with applications to Connor and Mosimann's generalized dirichlet distribution," J. Amer. Stat. Assoc., vol. 67, no. 340, pp. 910–912, Dec. 1972.
[18] W. F. Sharpe, Investors and Markets: Portfolio Choices, Asset Prices, and Investment Advice. Princeton, NJ: Princeton Univ. Press, 2007.