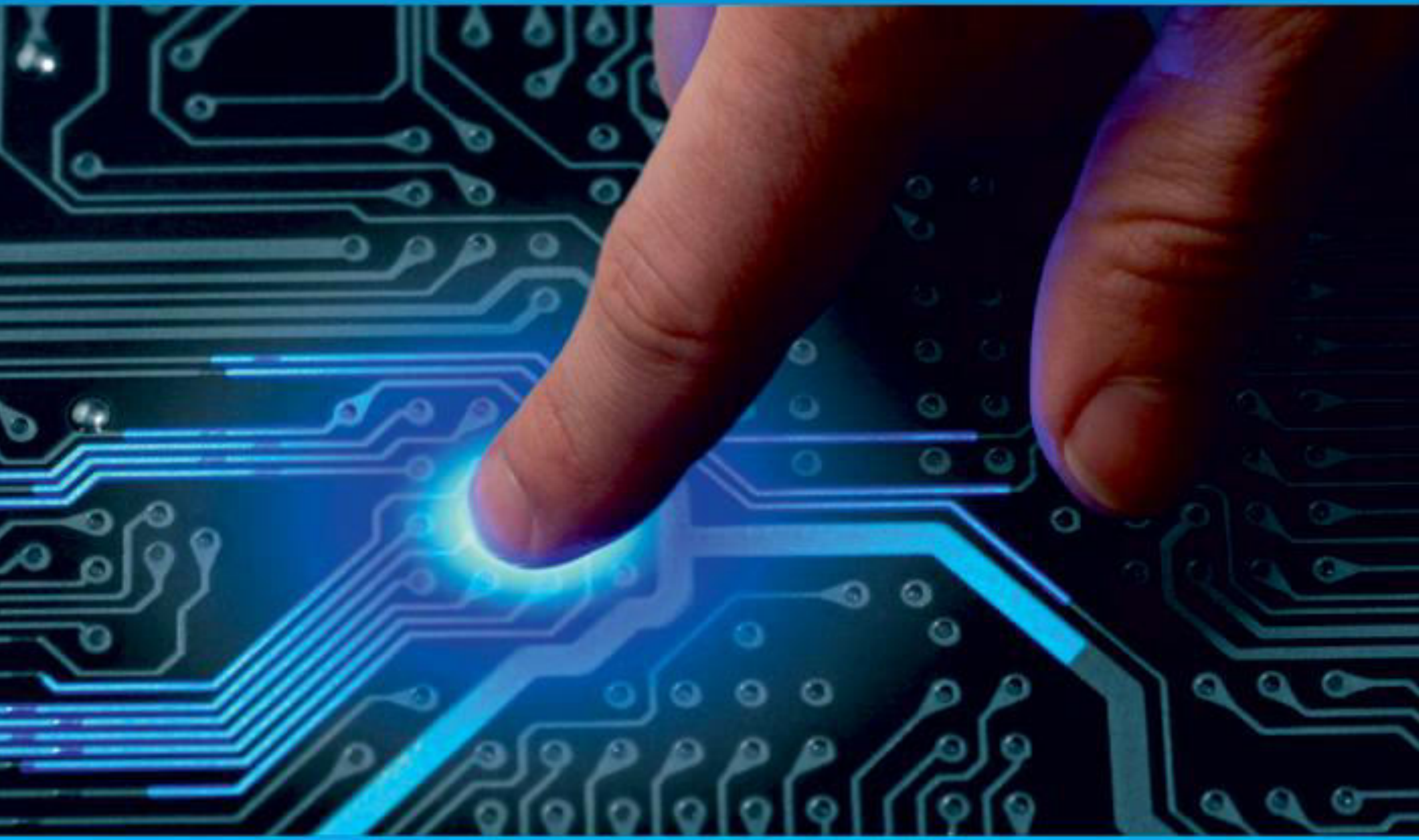
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.165

A Worm Detection System Based on Deep Learning

B.Manjubashini, S.Balaji, M. Mani, S. Gokulakrishnan, S. Mohamed Sharuk

Assistant Professor, Department of CSE, Mahendra Institute of Technology, Namakkal, India

Department of CSE, Mahendra Institute of Technology, Namakkal, India

Department of CSE, Mahendra Institute of Technology, Namakkal, India

Department of CSE, Mahendra Institute of Technology, Namakkal, India

Department of CSE, Mahendra Institute of Technology, Namakkal, India

ABSTRACT: In this article, we consider the problem of jamming-aware source routing and avoiding jamming by spliting data rate. The open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming. This intentional interference with wireless transmissions can be used as a launchpad for mounting Denial-of-Service attacks on wireless networks. Typically, jamming has been addressed under an external threat model. We addressed the problem of selective jamming attacks in wireless networks. We considered an internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. We showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. We evaluated the impact of selective jamming attacks on network protocols such as TCP and routing. Our findings show that a selective jammer can significantly impact performance with very low effort. We developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Our schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical-layer characteristics. We analyzed the security of our schemes and quantified their computational and communication overhead.

KEYWORDS: Deep learning, Network utility maximization. denial-of-service, wireless networks, packet classification.

I.INTRODUCTION

Jamming over point-to-point transmissions in a wireless mesh network can affect 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 beamforming, forcing the jammers to expend a greater resource to reach the same goal. However, recent work has demonstrated that intelligent jammers can incorporate crosslayer protocol information into jamming attacks, reducing resource expenditure by several orders of magnitude by targeting certain link layer and MAC implementation as well as link layer error detection and correction protocols. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support websites.

A network is any collection of independent computers that communicate with one another over a shared network medium. A computer network is a collection of two or more connected computers. When these computers are joined in a network, people can share files and peripherals such as modems, printers, tape backup drives, or CD-ROM drives.

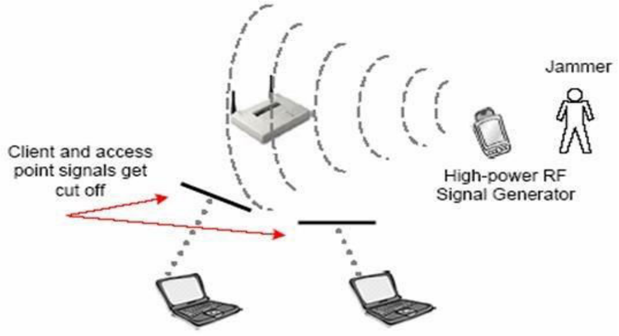

Jammer
Client and access point signals get cut off
High-power RF Signal Generator

Fig: Effect of jamming in wireless network

When networks at multiple locations are connected using services available from phone companies, people can send e-mail, share links to the global Internet, or conduct video conferences in real time with other remote users. When a network becomes open sourced it can be managed properly with online collaboration software.

- Anti-jamming techniques = diversity
    - Multiple frequency bands
    - Different MAC channels
    - Multiple Routing paths

II. BACKGROUND WORK

In this section we outline the basic wireless network and jamming models that we use throughout this paper.

A. Network Model

A wide variety of wireless networks have emerged, ranging from wireless sensor networks, mobile ad hoc network, to mesh networks. The broad range of choice implies that there are many different directions that one can take to tackle the problem of localizing jammers. Devising a generic approach that works across all varieties of wireless networks is impractical. Therefore, as a starting point, we target to tailor our solutions to a category of wireless networks with the following characteristics.We assume that once deployed, the location of each wireless device remains unchanged.

III. METHOLODIES

Neighbor-Aware.

Each node in the network has a number of neighbors, and it maintains a neighbor table which records their information of its neighbors, such as their locations or activeness. Such a neighbor table are maintained by most routing protocols, and it can be easily achieved by periodically broadcasting hello messages.

Location-Aware.

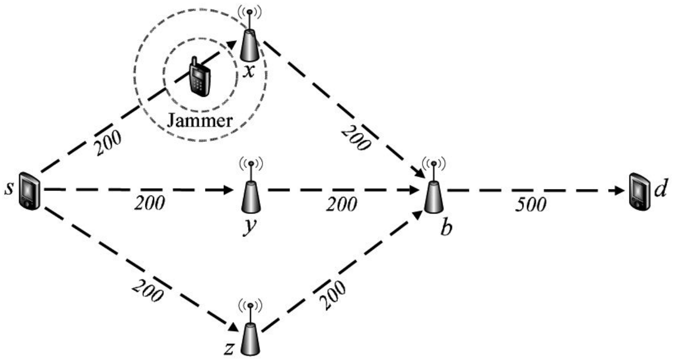
Each node knows its location coordinates and its neighbors' locations. This is reasonable assumption as many applications require localization services.

Able to Detect Jamming.

In this work, we focus on locating a jammer after it is detected. Several jamming detection approaches have been proposed, ranging from measuring simple properties to more complicated consistency checks.

Every network includes:

At least two computers Server or Client workstation. Networking Interface Card's (NIC) A connection medium, usually a wire or cable, although wireless communication between networked computers and peripherals is also possible.
Network Operating system software, such as Microsoft Windows NT or 2000, Novell NetWare, Unix and Linux.



System architecture of multiple-path routing algorithms in the presence of jammers

1. Allocation of traffic across multiple routing paths

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 which allows individual network nodes to locally characterize the jamming impact and aggregate this information for the source nodes.

***2.* Characterizing the Impact Of Jamming**

In these Module 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 s to incorporate the jamming impact in the traffic allocation problem, the effect of jamming on transmissions over each link must be estimated. However, to capture the jammer mobility and the dynamic effects of the jamming attack, the local estimates need to be continually updated.

***3.* Effect of Jammer Mobility on Network**

The capacity indicating the link maximum number of packets persecond (pkt/s) eg:200 pkts/s which can be transported over the wireless link. Whenever the source is generating data at a rate of 300 pkts/s to be transmitted at the time jamming to be occurring. Then the throughput rate to be less. If the source node becomes aware of this effect the allocation of traffic can be changed to 150 pkts/s on each of paths thus recovers the jamming path.

4.Estimating End-to-End Packet Success Rates

The packet success rate estimates for the links in a routing path, the source needs to estimate the effective end-to-end packet success rate to determine the optimal traffic allocation. Assuming the total time required to transport packets from each source s to the corresponding destination is negligible compared to the update relay period.

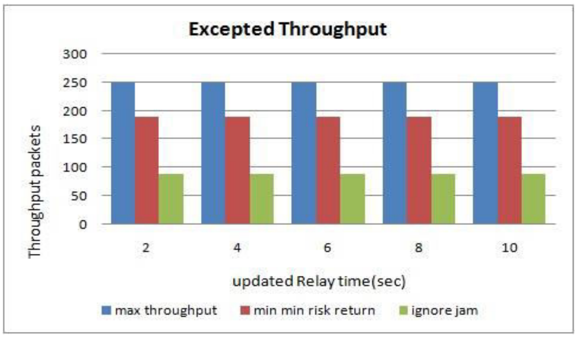
***5.* Optimal Jamming-Aware Traffic Allocation**

An optimization framework for jamming-aware traffic allocation to multiple routing paths 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.

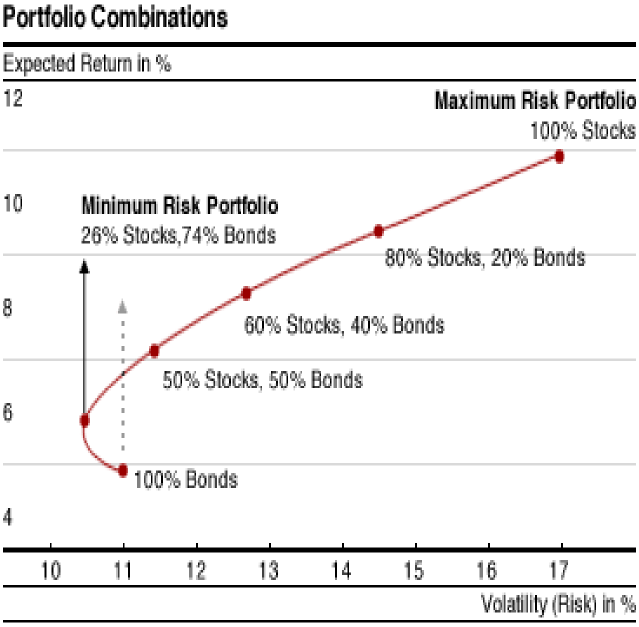
Estimate local packet success rates (LPSR)

Each node updates (LPSR), Update period T << Ts update relay period

IV. RESULT ANLYSIS



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 .We assume that all communication is unicast over the directed edges in , i.e., each packet transmitted by node is intended for a unique node with . The maximum achievable data rate, or capacity, of each unicast linkin the absence of jamming is denoted by the predetermined constant rate in units of packets per second.



In this paper, we assume that the source nodes in 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.

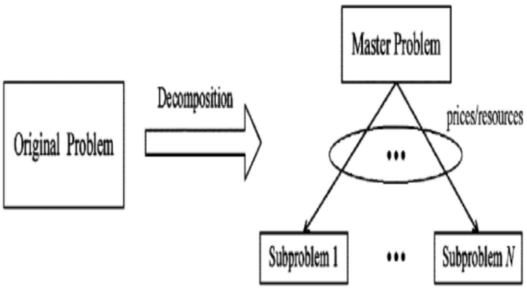


Fig: Problem Solution

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.

V. CONCLUSION

In this article, we studied the problem of traffic allocation in multiple-path routing algorithms in the presence of jammers. We have presented methods for each network node to probabilistically characterize the local impact of a dynamic jamming attack and for data sources to incorporate this information into the routing algorithm and successfuuly packet transfer by splitting data rate. We formulated multiple-path traffic allocation in multi-source networks as a lossy network flow optimization problem using an objective function based on portfolio selection theory from finance. We showed that this centralized optimization problem can be solved using a distributed algorithm based on decomposition in network utility maximization (NUM). We 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. We have thus shown that multiple path source routing algorithms can optimize the throughput performance by effectively incorporating the empirical jamming impact into the allocation of traffic to the set of paths.

REFERENCES

[1]. F. Akyildiz, X. Wang, and W. Wang, “Wireless mesh networks: A survey,” Computer Networks, vol. 47, no. 4, pp. 445–487, Mar. 2005.

[2]. E. M. Sozer, M. Stojanovic, and J. G. Proakis, “Underwater acoustic networks,” IEEE Journal of Oceanic Engineering, vol. 25, no. 1, pp. 72–83, Jan. 2000.

[3]. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. JohnWiley&Sons, Inc.,2001.

[4]. J. Bellardo and S. Savage, “802.11 denial-of-service attacks: Real vulnerabilities and practical solutions,” in Proc. USENIX Security Symposium, Washington, DC, Aug. 2003, pp. 15–28.

[5]. D. J. Thuente and M. Acharya, “Intelligent jamming in wireless networks with applications to 802.11b and other networks,” in Proc. 25th IEEE Communications Society Military Communications Conference (MILCOM’06), Washington, DC, Oct. 2006, pp. 1–7.

[6]. A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks,” IEEE 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 Communications and Mobile Computing, 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 Network, vol. 20, no. 3, pp. 41–47, May/Jun. 2006.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details

www.ijircce.com