# Dynamic Jamming Aware Routing Protocols for Routing Loads and Congestion Status

**Devendra Kumar, Mr. Atma Prakash Singh**

***Abstract*— We put forward techniques for network nodes to approximate and set apart the impact of jamming and in support of a source node to include these estimates into its traffic allotment. The main advantage of the proposed system is that 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. Mesh routers have minimal mobility and perform dedicated routing and configuration, which significantly decreases the load of mesh clients and other end nodes. And the goal of the paper is to efficiently allocate the traffic to maximize the overall throughput.**

***Index Terms*—Routing Loads, jamming, WLANs.**

## I. INTRODUCTION

Mobile environment differs from the stationary environment in many respects. Computers in stationary environments are usually very reliable and efficient during data transfer from one host to another host. A stationary environment can distribute an application's components and rely upon the use of high-bandwidth, small latency networks to provide excellent interactive application performance. The attribute of the typical stationary environment has guided the development of classified distributed computing techniques for building client-server application. These applications are usually unaware of the actual state of the environment so they assume implicit assumptions about type location and availability of resources. But mobile computers are quite fragile. A mobile computer may run out of battery power, be lost or damage or be stolen. Mobile computer also interacts with surrounding environment, which may introduce noise, interruption blocking, disconnection, privacy breach, and risk of data loss due to remote access, low bandwidth and bandwidth variability. Relative to most stationary computers, a mobile computer has fewer computational resources available, which may change dynamically. So special precautions should be taken to enhance the reliability of data stored on mobile computers. In mobile computing, hosts move frequently. When a mobile host moves to new location it informs with nearby base station for further communication. This means frequent mobility of hosts leads an issue of location management for quick communication between mobile hosts for exchange of database.

**Manuscript received April 24, 2015.**
**Devendra Kumar**, D.O.B .- 16/Feb/1988, Ph.No – 9415036180, Address - Village +Post – Dandopur , Distt. – Kushinagar ,Pin -274304 Mtech (Final Sem.) C.S. Branch
**Mr. Atma Prakash Singh**, Asstt. Proff. Azad Institute of Engineering & Technology , lucknow, Deptt. - C.S.

## II. DETECTION OF JAMMING

WLANs are built upon a shared medium that makes it easy to launch jamming attacks. These attacks can be easily accomplished by sending radio frequency signals that do not follow any MAC protocols. Detection of jamming attacks can be done in multiple ways. One of the most efficient ways is to jump channels. Because communication between two legitimate nodes is done through a specific frequency, the frequency can be changed if necessary.

While a jammer is attacking the wireless network, there are other effective ways to continue legitimate communication in the network. Engaging the jammer on the jammed channel and continuing communication in another channel was introduced by Beg, Ahsan, and Mohsin [8]. When the nodes detected the jamming in the wireless network, they jumped to another channel to continue legitimate communication. In the experiments, both 10 and 20 nodes experiments were done, and in both scenarios, after channels were jumped, the network resumes communications as normal. In both scenarios, the amount of packets dropped reduced immediately.

The research concluded that channel jumping will decrease the throughput of the network. Also, it was easier to detect jamming through intermitted channel jumping. Concluded, channel jumping was a superior method of combating network interference, rather than changing network protocols [3].

A study on a channel migration scheme to mitigate wireless jamming attacks was done by four experiments[4]. The first experiment was done without jammers in order to test the performance of network, and the second experiment tested a jamming attack in a single channel. The third experiment tested jamming attacks in multiple channels, while the last experiment of jamming attacks was varied in different channels in multiple regions. An algorithm of channel migration was applied to the network system, which stated that when jamming attacks were launched in the channel, the communication of nodes should migrate to another channel and continue.

In order to prevent from multi-channel jamming attacks, a cross-layer jamming detection method was developed [5]. Cross-layer jamming detection is a tree-based approach. A jamming detection algorithm was utilized in all legitimate nodes; when the communication process began, all the nodes had the ability to report jamming attacks in different layers, and only the reports which were generated by nodes with

jamming detection algorithm were accepted by the system in order to avoid error. Research was also done about multi-channel jamming attacks by Jiang and Xue [6]. The difference from the jamming detection algorithm was that it focused on network restoration and design of traffic rerouting.

Another way to lower the influence of jamming attacks is to set thresholds and priority to the network system [7]. OPNET Modeler was selected as the simulation tool in the research. In the experiment, three legitimate nodes communicated in the network, while three jammers launched DoS attacks. A monitor node was set to watch the thresholds in the network. Legitimate nodes were set to a priority number, while the jammers' priority number was zero. When data transmitting in the network exceeded the threshold, packets sent by lower threshold were discarded first. In this case, useless messages in the network were dropped first when network is busy, and legitimate communication was continued. Through this method, data dropped by the nodes was largely decreased, and the transmission quality of the network was increased.

## III. ROUTING

Routing is the process of finding optimal path between source and destination. Because of the fact that packet may be necessary to hop or several hops before a packet reach the target, a routing protocol is needed. Routing protocols allow routers to dynamically advertise and discover routes, decide which routes are available and which are the most efficient routes to a target. The routing protocol has two main jobs, selection of routes for various source-target pairs and the deliverance of massages to their correct target. The second function is conceptually straight forward using a verity of protocols and data structures (routing tables). In this research work we focused on selecting and finding route.

## IV. CONVENTIONAL ROUTING PROTOCOLS

If a routing protocol is required, we cannot use usual routing protocols like link state or distance vector for Ad hoc networks even though they are well tested and people recognize them. It is because they are intended for static topology, which means that they have a problem to coverage to a steady state in an Ad hoc network with a very frequently changing topology. Link state and distance vector would probably work well in an Ad hoc network with low mobility, i.e. a network where topology is not changing very often. Another trait for usual protocols is that they presume bi-directional links, e.g. the communication between two hosts works equally well in both directions. In the wireless radio situation this is not always the case.

Because many of the proposed Ad hoc protocols have a traditional routing protocol as underlying algorithm, it is essential to comprehend the basic operation for usual protocols like link state, distance vector, source routing and flooding. Distance Vector protocols decide best path on how far the destination is, while Link State protocols are proficient of using more sophisticated methods taking into thought link variables, such as delay, reliability, bandwidth and load.

Link State routing protocols offer greater flexibility and sophistication than the Distance Vector routing protocols. They diminish overall broadcast traffic and make better decisions about routing by taking characteristics such as bandwidth, delay, reliability, and load into concern, instead of relying their decisions exclusively on distance or hop count.

## V. LINK STATE

In link state routing each node maintains a view of the complete topology with a cost for each link. To keep the costs steady, each node periodically broadcasts the link costs of its outgoing links to all other nodes using flooding. As each node accepts this information, it revises its view of the network and applies a shortest path algorithm to choose the next hop for each destination.

Some link costs in a node view can be inaccurate because of extended propagation delays, partitioned networks, etc. Such inconsistent network topology views can lead to formation of routing loops. These loops are conversely short-lived, because they vanish in the time it takes a message to traverse the diameter of the network.

## VI. DISTANCE VECTOR

In distance vector each node not only monitors the expenditure of its outgoing links, but instead of broadcasting this information to all the nodes, it periodically broadcasts to each of its neighbors an approximation of the shortest distance to every other node in the network. The receiving nodes then utilize this information to recalculate the routing tables, by using a shortest path algorithm. Compared to link state, distance vector is additional computation efficient, easier to implement and necessitates much less storage space. Distance-vector routing protocols are easy and efficient in small networks, and require little, management if any. Nonetheless, they do not scale well, and have reduced convergence properties, which has led to the development of more complex but more scalable link-state routing protocols for use in large networks.

However, it is well known that distance vector can cause the formation of both short- lived and long- lived routing loops. The primary cause for this is that the nodes choose their next hops in a completely distributed manner based on information that can be staled.

## VII. SOURCE ROUTING

Source routing means that each packet must transmit the complete path information that the packet should take through the network. The routing decision is therefore made at the source. The advantage with this approach is that it is very simpley to evade routing loops but it undergoes form a minor overhead needed by each packet.

## VIII. FLOODING

Many routing protocols utilize broadcast to dispense control

information, i.e., send the control information from the source node to all other nodes. A extensively used form of broadcasting is flooding [1, 2]. The source node sends its information to its neighbors and so on, until the packet has reached all nodes in the network. A node will only relay a packet once and to guarantee this some sort of sequence number can be used. This sequence number is augmented for each new packet a node sends.

## IX. Dissimilarity between WSNs and Other Wireless Ad Hoc Networks

A wireless ad hoc network (WANET) is a temporary network that is set up between peer nodes to satisfy an immediate need. Many protocols exist for wireless ad hoc networks, but are unsuitable for WSNs due to the unique requirements of WSNs. WSNs differ from other WANETs in seven areas, namely: network size, node density, node proneness to failure, frequency of topology changes, communication paradigm employed, resource limitations of nodes and node identification. Each of these areas is discussed in the following paragraphs.

The network size of a WSN can be anything from a few nodes up to many thousands of nodes. Other WANETs on the other hand usually consist of less than a hundred nodes. A Bluetooth piconet, which can consist of up to a maximum of eight nodes, is an example of a WANET. A wireless local area network (WLAN) is another illustration of a WANET. WLAN is based on the IEEE 802.11b standard, which was developed by the Institute of Electrical and Electronic Engineers (IEEE). The size of a WLAN is limited to 32 nodes per access point.

Node density in a WSN is usually high, with a huge number of nodes in a comparatively small area, while other WANETs mostly consist of only a few nodes in close proximity of each other. This is due to the size of nodes. A WSN node can be as tiny as a one Euro coin, while nodes of other WANETs are mostly notebook computers, cellular telephones or palmtops.

A WSN might be deployed in a remote or inaccessible area, such as a jungle or a disaster area. In such circumstances the *node proneness to failure* is high due to the possibility of nodes being damaged and failing. Some nodes might also exhaust their energy resources quicker than other nodes due to being on a routing path that is utilized more than other paths. Nodes in other WANETs have rechargeable energy supplies and are not subjected to adverse environmental conditions that could damage them to the extent of not being able to function any longer.

The frequency of topology changes in a WSN is high, due to factors such as node breakdown, node additions, nodes moving and environmental interference. The network has to be able to adapt to these changes in node position and number. Topology changes can happen as frequently as every few milliseconds. In other WANETs, nodes typically demand to join the network and depart from the network after a certain period of time, which is rarely less than a couple of minutes.

The communication paradigm employed in WSNs includes a large number of broadcasts that are sent through the network. These broadcasts are utilized for network set up and maintenance, discovery of neighbours and sending of data. Other WANETs typically use point to point communications, since the source knows how to contact the target.

The resource limitations of nodes in WSNs include limited energy and bandwidth resources, compared to other WANETs. The energy resources of WSN nodes cannot be replenished, while other WANETs' nodes have rechargeable batteries. The limited data rate of up to a few kilobits per second in WSNs is small compared to data rates of between one and a few hundred megabits per second in other WANETs. The memory of WSN nodes is restricted to a few kilobytes, whereas other WANETs' nodes can have gigabytes of memory. The processors employed in WSN nodes are limited. The TUV WSSN nodes, for instance, use 4MHz processors. This is very limited, compared to the GHz processors of notebook computers.

Node identification by means of globally unique identifiers are not always possible in WSNs, due to the possibly very large number of nodes in the network and the overhead caused by having a unique identifier for each node. In other WANETs, the nodes have exclusive identifiers such as internet protocol (IP) addresses.

The WSN is a new and unique class of WANET that differs considerably from other WANETs. The unique nature of WSNs implies that protocols designed for other WANETs cannot be implemented in WSNs, so a novel protocols have to be developed.

### *Comparison of Wireless Networking Standards*

There are many different standards for wireless networks. These standards divide wireless networks into categories based on factors such as network size, data rate, transmission range and battery lifetime. Table 1 shows a comparison of three important wireless network standards.

Table 1: A comparison of wireless networking standards .

| **Market Name** | **Wi-Fi** | **Bluetooth** | **ZigBee** |
|---|---|---|---|
| **Standard** | **IEEE 802.11b** | **IEEE 802.15.1** | **IEEE 802.15.4** |

| **Type of Network** | WLAN | WPAN | WPAN |
|---|---|---|---|
| | Web, Email, Video | Cable Replacement | Monitoring andControl |
| **Application Focus** | 1MB+ | 250KB+ | 4KB - 32KB |
| **System Resources Battery Life** | 0.5 - 5 | 1 - 7 | 100 - 1,000+ |
| **(days) Network Size** | 32 | 7 | 255 / 65,000 |
| **Data rate (kbps) Transmission** | 11,000+ | 720 | 20 - 250 |
| **Range (meters)** | 1 - 100 | 1 - 10+ | 1 - 100+ Reliability, |
| | | | Power, |
| **Success Metrics** | Speed, Flexibility | Cost, Convenience | Cost |

## X. Congestion Control on The Internet

TCP provides an end-to-end, reliable, byte-oriented service to the applications. To prevent senders from overwhelming the receivers, TCP employs flow control whereas in order to avoid overwhelm- ing the network, it uses congestion control. In this section, we focus on the congestion control algorithm used by TCP.

A TCP source maintains a sliding window called congestion window or *cwnd*, which indicates its current belief about the number of packets that the network can safely handle. TCP increases *cwnd* after every new acknowledgement[1] until it detects a packet loss, upon which, TCP decreases *cwnd*, which in turn reduces the load on the network. TCP detects packets losses by two mech- anisms. First, when a packet is sent, it initializes a timer. If no acknowledgement is received within the timeout interval, the packet is assumed to be lost. Second, when out-of-order packets are received by TCP receivers, they send acknowledgements for the last in-order packet received. When sources receive three duplicate acknowledgements, it assumes that a packet was lost and retransmits a packet.

TCP uses two algorithms for dynamically changing *cwnd*, namely, *Slow-Start* and *Congestion Avoidance*. In Slow-Start, sources increase *cwnd* by one Maximum Segment Size (MSS) for each new acknowledgment received, which results in the window doubling after each window's worth of data is acknowledged. With this exponential increase, $RTT \cdot log_2 W$ seconds time is required to reach a window of size $W$. A connection enters Slow-Start when starting up or on experiencing a packet retransmission timeout, and exits Slow-Start when it detects a packet loss or when the congestion window has reached a dynamically computed threshold, *ssthresh*. More specifically, *ssthresh* is set to half of the current congestion window when packet loss was detected. TCP exits Slow-Start to enter the Congestion Avoidance phase, where it continues to probe for available bandwidth, but more cautiously than in Slow-Start.

In the Congestion Avoidance phase, TCP uses the Additive Increase and Multiplicative De- crease (AIMD) algorithm to probe for network bandwidth. With AIMD, TCP increases its window by one packet every round-trip time until it experiences a packet drop. Upon detecting a packet loss, TCP reduces its *cwnd* by half.

## XI. Conclusion

Multi-hop wireless networks (MHWN) have emerged to be a promising cost effective paradigm for the next-generation wireless technology. However, the unique characteristics of nowadays MHWN, such as distributed and dynamic network architecture, broadcast nature of wireless medium and stringent resource constraints of wireless devices, makes it extremely attractive and vulnerable to malicious attacks. So how to ensure continuous network service becomes a critical problem especially in jammed situations. Although some research has been conducted on countering jamming attacks, few works consider jamming dynamics.

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.

## Reference


[1] 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 .

[2] R. C. Shah and J. Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks," in Proceedings of the IEEE Wireless Communications and

[3] Jeung, J., Jeong, S., & Lim, J. (2011). Anti Jamming – Based Medium Access Control Using Adaptive Rapid Channel Hopping in 802.11. Graduate School of Ajou University, 70-82.

[4] Hyun, S., Ning, P., & Liu, A. Mitigating Wireless Jamming Attacks via Channel Migration. International Conference on Distributed Computing Systems Workshops, 31, 313-322.

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

[6] 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.

[7] 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.

[8] 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.