iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XII **Month of publication:** December 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

MPRP: A Jamming-Aware Multi-Path Routing Protocol For wireless Ad-Hoc Networks

G. Saranya[1] A.Arivazhagan[2]
[1, 2] *Assistant Professor Department of Computer Science Engineering* M.A.M School of Engineering, Trichy, Tamil Nadu

Abstract: ***Robust network operation and the ability to provide user and data security while under attack are desirable qualities of network protocols. However, these qualities require a fundamental understanding of network protocol vulnerabilities and characterization of the space of possible attacks. Hence, understanding attacks and their impact is a necessary prerequisite to the design of secure network protocols. Jamming of wireless networks can be realized by generating continuous noise with sufficient power in the wireless network. There are many disadvantages of this approach including high energy requirements and a high probability of packet loss. The purpose of this paper is to provide a solution to the jamming problem using multiple path routing. This multiple path routing uses Ad-hoc On Demand Multipath Distance Vector Routing (AOMDV), a novel algorithm for the operation of ad-hoc networks. Each Mobile Host operates as a specialized router and routes are obtained as needed (i.e, on-demand) with little or no reliance on periodic advertisements.***

Our new routing algorithm is quite suitable for a dynamic self starting network, as required by users wishing to utilize ad-hoc networks. AOMDV provides loop-free routes even while repairing broken links. Because the protocol does not require global periodic routing advertisements, the demand on the overall bandwidth available to the mobile nodes is substantially less than in those protocols that do necessitate such advertisements and also the overall throughput achieved in greater amount. Nevertheless we can still maintain most of the advantages of basic distance-vector routing mechanisms. We show that our algorithm scales to large populations of mobile nodes wishing to form ad-hoc networks. We also include an evaluation methodology and simulation results to verify the operation of our algorithm.

Keywords: Jamming, Multiple path routing, AOMDV, Ad-hoc network, Throughput.

I. INTRODUCTION

Jamming point-to-point transmissions in a wireless mesh network [1] or underwater acoustic network [2] 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 [3], [4] on end-to-end data communication. The simplest methods to defend a network against jamming attacks comprise physical layer solutions forcing the jammers to expend incorporate cross layer protocol information into jamming attacks [5]. Using multiple-path variants of source routing protocols such as Dynamic Source Routing (DSR) [6] or Ad-Hoc On- Demand Distance Vector(AODV) [7], for example the MPDSR protocol [8], each source node can request several routing paths to the destination node for concurrent use.

Like AODV-BR, the AOMDV uses the basic AODV route construction process. In this case, however, some extensions are made to create multiple loop-free, link-disjoint paths. The main idea in AOMDV is to compute multiple paths during route discovery. It consists of two components: (1) A route update rule to establish and maintain multiple loop-free paths at each node. (2) A distributed protocol to find link-disjoint paths. Ad hoc On-Demand Multipath Distance Vector (AOMDV) Routing is a routing protocol for Mobile Ad hoc NET works (MANETs) and other wireless ad-hoc networks. It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. In contrast, the most common routing protocols of the Internet are proactive, meaning they find routing paths independently the usage of the paths. AOMDV is, as the name indicates, a distance-vector routing protocol. AOMDV avoids the counting-to-infinity problem of other distance-vector protocols by using sequence numbers on route updates. AOMDV is capable of both unicast and multicast routing. In AOMDV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AOMDV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time. In AOMDV, when a source needs a route to a destination, it initiates a route discovery process by flooding a RREQ for destination throughout the network. RREQs should be

uniquely identified by a sequence number so that duplicates can be recognized and discarded. Upon receiving a non-duplicate RREQ, an intermediate node records previous hop and checks whether there is a valid and fresh route entry to the destination in routing table. If such is the case, the node sends back a RREP to the source; if not it rebroadcasts the RREQ. A node updates its routing information and propagates the RREP upon receiving further RREPs only if a RREP contains either a larger destination sequence number (fresher) or a shorter route found.

When a link fails, a routing error is passed back to a transmitting node, and the process repeats in AODV but in AOMDV each RREQ, respectively RREP arriving at a node potentially defines an alternate path to the source or destination. Just accepting all such copies will lead to the formation of routing loops. In order to eliminate any possibility of loops, the "advertised hop count" is introduced. The advertised hop count of a node *I* for a destination *d* represents the maximum hop count of the multiple paths for *d* available at *I*. The protocol only accepts alternate routes with hop count lower than the advertised hop count, alternate routes with higher or the same hop count are discarded. The advertised hop count mechanism establishes multiple loop-free paths at every node. These paths still need to be disjoint. For this use the following notion: When a node *S* floods a RREQ packet in the network, each RREQ arriving at node *I* via a different neighbor of *S*, or *S* itself, defines a node-disjoint path from *I* to *S*. In AOMDV this is used at the intermediate nodes. Duplicate copies of a RREQ are not immediately discarded. Each packet is examined to see if it provides a node-disjoint path to the source. For node-disjoint paths all RREQs need to arrive via different neighbors of the source. This is verified with the first hop field in the RREQ packet and the first hop list for the RREQ packets at the node. At the destination a slightly different approach is used, the paths determined there are link-disjoint, not node-disjoint. In order to do this, the destination replies up to k copies of the RREQ, regardless of the first hops. The RREQs only need to arrive via unique neighbors.

The remainder of this article is organized as follows. In Section II, we state the network model and assumptions about the jamming attack. To motivate our formulation, in Section III, we formulate the optimal multiple path traffic allocation problem using our proposed method. In Section IV, we show the simulation results. We summarize our contributions In Section V.

II. SYSTEM MODEL AND ASSUMPTIONS

The wireless network of interest can be represented by a directed graph G = (N, E). The vertex set N represents the network nodes, and an ordered pair (i, j) of nodes is in the edge set E if and only if node j can receive packets directly from node i. We assume that all communication is multicast. Each source node s in a subset S Є N generates data for a single destination node ds Є N. We assume that each source node s constructs multiple routing paths to ds using a route request process similar to those of the DSR [8] or AODV [9] protocols. We let Ps = {ps1, . . . , psLs} denote the collection of Ls loop-free routing paths for source s.

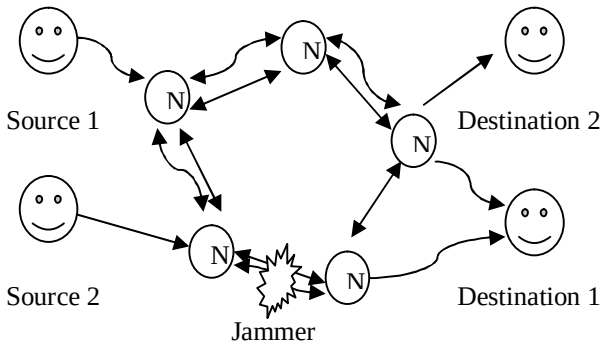


Fig. 1. An example network with sources S = {s1, s2} , destinations ds={ds1, ds2} is illustrated.

In this article, we assume that the source nodes in S 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.

III. AD-HOC ON DEMAND MULTIPATH DISTANCE VECTOR

Our basic proposal can be called pure on demand route acquisition system: nodes that do not lie on active paths neither maintain any routing information nor participate in any periodic routing table exchanges. Further, a node does not have to discover and maintain a route to another node until the two needs to communicate, unless the former node is offering its services as an intermediate forwarding station to maintain connectivity between two other nodes. When the local connectivity of the mobile node is of interest,

each mobile node can become aware of the other nodes in its neighborhood by the use of several techniques, including local (not system wide) broadcasts known as hello messages. The routing tables of the nodes within the neighborhood are organized to optimize response time to local movements and provide quick response time for requests for establishment of new routes.

A. The algorithm's primary objectives are

1) To broadcast discovery packets only when necessary
2) To distinguish between local connectivity management neighborhood detection and general topology maintenance
3) To disseminate information about changes in local connectivity to those neighboring mobile nodes that are likely to need the information.

AOMDV uses a broadcast route discovery mechanism as is also used with modifications in the Dynamic Source Routing DSR algorithm. Instead of source routing, however AOMDV relies on dynamically establishing route table entries at intermediate nodes. This difference pays off in networks with many nodes where a larger overhead is incurred by carrying source routes in each data packet. To maintain the most recent routing information between nodes, we borrow the concept of destination sequence numbers from DSDV. Unlike in DSDV however each ad-hoc node maintains a monotonically increasing sequence number counter which is used to supersede stale cached routes. The combination of these techniques yields an algorithm that uses bandwidth efficiently (by minimizing the network load for control and data traffic) is responsive to changes in topology, and ensures loop free routing.

B. Important properties of the protocol

1) Extension of AODV.
2) RREQs from different neighbors of the source are accepted at intermediate nodes.
3) Multiple link-disjoint routes are created (with modification at the destination they can be node-disjoint).
4) Maximum hop count to each destination ("advertised hop count") is used to avoid loops.
5) Multiple routes are established in single route discovery process.
6) Nodes maintain next-hop info for destinations (multiple next-hops possible).
7) No complete route(s) information known at a source.

C. Path discovery

The Path Discovery process is initiated whenever a source node needs to communicate with another node for which it has no routing information in its table. Every node maintains two separate counters: a node sequence number and a broadcast-id. The source node initiates path discovery by broadcasting a route request (RREQ) packet to its neighbors. The RREQ contains the following fields

<source_addr, source_sequence _#, broadcast_id, dest_addr, dest sequence _#, hop _cnt >

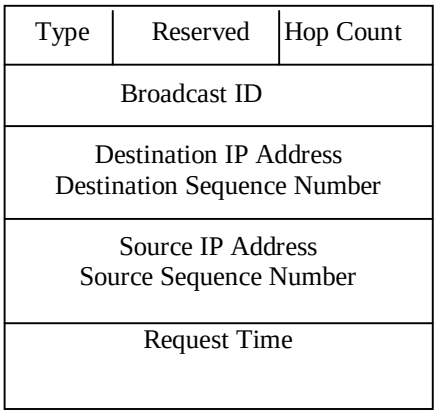


Fig: 2 Structure of an RREQ packet

The pair <source_addr, broadcast id > uniquely identifies a RREQ, broadcast_id is incremented whenever the source issues a new RREQ. Each neighbor either satisfies the RREQ by sending a route reply (RREP) back to the source, or rebroadcasts the RREQ to its own neighbors after increasing the hop cnt. Notice that a node may receive multiple copies of the same route broadcast packet from various neighbors. When an intermediate node receives a RREQ, if it has already received a RREQ with the same broadcast id and source address, it drops the redundant RREQ and does not rebroadcast it.

D. Route table Management

In addition to the source and destination sequence numbers, other useful information is also stored in the route table entries, and is called the soft-state associated with the entry. Associated with reverse path routing entries is a timer, called the route request expiration timer. The purpose of this timer is to purge reverse path routing entries from those nodes that do not lie on the path from the source to the destination. The expiration time depends upon the size of the ad-hoc network. Another important parameter associated with routing entries is the route caching timeout, or the time after which the route is considered to be invalid. In each routing table entry, the address of active neighbors through which packets for the given destination are received is also maintained. A neighbor is considered active (for that destination) if it originates or relays at least one packet for that destination within the most recent active timeout period. This information is maintained so that all active source nodes can be notified when a link along a path to the destination breaks. A route entry is considered active if it is in use by any active neighbors. The path from a source to a destination, which is followed by packets along active route entries, is called an active path. Note that, as with DSDV, all routes in the route table are tagged with destination sequence numbers, which guarantee that no routing loops can form, even under extreme conditions of out-of-order packet delivery and high node mobility. A mobile node maintains a route table entry for each destination of interest.

1) Each route table entry contains the following information:

a) Destination
b) Next Hop
c) Number of hops (metric)
d) Sequence number for the destination
e) Expiration time for the route table entry

Each time a route entry is used to transmit data from a source toward a destination, the timeout for the entry is reset to the current time plus active route timeout. If a new route is offered to a mobile node, the mobile node compares the destination sequence number of the new route to the destination sequence number for the current route. The route with the greater sequence number is chosen. If the sequence numbers are the same, then the new route is selected only if it has a smaller metric, fewer number of hops, to the destination.

E. Path maintenance

Movement of nodes not lying along an active path does not affect the routing to that path's destination. If the source node moves during an active session, it can reinitiate the route discovery procedure to establish a new route to the destination. When either the destination or some intermediate node moves, a special RREP is sent to the affected source nodes. Periodic hello messages can be used to ensure symmetric links, as well as to detect link failures. Alternatively, and with far less latency, such failures could be detected by using link-layer acknowledgments (LLACKS). A link failure is also indicated if attempts to forward a packet to the next hop fail. Once the next hop becomes unreachable, the node upstream of the break propagates an unsolicited RREP with a fresh sequence number (i.e. a sequence number that is one greater than the previously known sequence Number) and hop count of ∞ to all active upstream neighbors. Those nodes subsequently relay that message to their active neighbors and so on. This process continues until all active source nodes are notified, it terminates because AOMDV maintains only loop-free routes and there are only a finite number of nodes in the ad-hoc network. Upon receiving notification of a broken link, source nodes can restart the discovery process if they still require a route to the destination. To determine whether a route is still needed, a node may check whether the route has been used recently, as well as inspect upper level protocol control blocks to see whether connections remain open using the indicated destination. If the source node (or any other node along the previous route) decides it would like to rebuild the route to the destination, it sends out an RREQ with a destination sequence number of one greater than the previously known sequence number, to ensure that it builds a new, viable route, and that no nodes reply if they still regard the previous route as valid.

F. Local connectivity management

Nodes learn of their neighbors in one of two ways. Whenever a node receives a broadcast from a neighbor, it updates its local connectivity information to ensure that it includes this neighbor. In the event that a node has not sent any packets to all of its active downstream neighbors within hello interval, it broadcasts to its neighbors a hello message a special unsolicited RREP containing its identity and sequence number. The node's sequence number is not changed for hello message transmissions. This hello message is prevented from being rebroadcast outside the neighborhood of the node because it contains a time to live TTL value of Neighbors that receive this packet update their local connectivity information to the node. Receiving a broadcast or a hello from a new neighbor or failing to receive allowed hello loss consecutive hello messages from a node previously in the neighborhood is an

indication that the local connectivity has changed. Failing to receive hello messages from inactive neighbors does not trigger any protocol action. If hello messages are not received from the next hop along an active path, the active neighbors using that next hop are sent notification of link failure. We have determined the optimal value for allowed hello loss is two. The local connectivity management with hello messages can also be used to ensure that only nodes with bidirectional connectivity are considered to be neighbors. For this purpose each hello sent by a node lists the nodes from which it has heard. Each node checks to make sure that it uses only routes to neighbors that have heard the node's hello message. To save local bandwidth, such checking should be performed only if explicitly configured into the nodes.

IV. SIMULATIONS

We have simulated AOMDV using an event- driven simulator. The NS2 language is suited to the simulation of dynamic topologies and routing algorithms. The main objective of our simulations is to show that on-demand route establishment with AOMDV is both quick and accurate. Additional objectives include showing that AOMDV scales well to large networks, and determining the optimal value for each of the necessary parameters.

End-End Delay

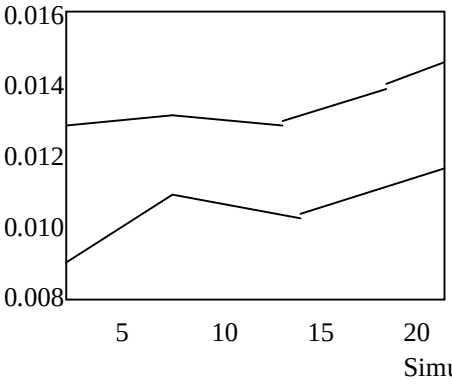


Fig 3(a) Simulation Time Vs End-End Delay

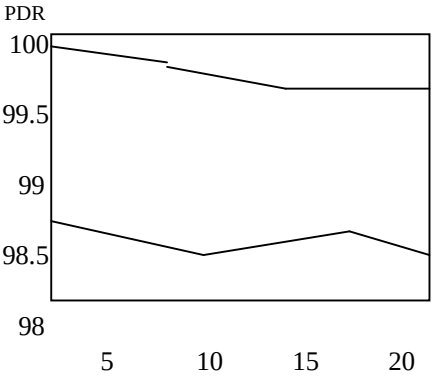
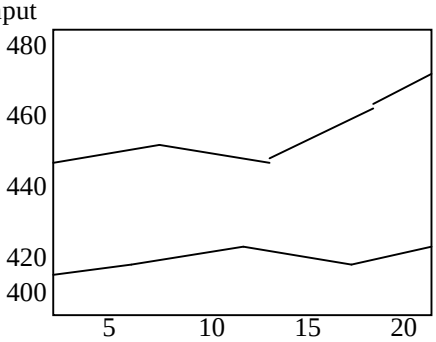


Fig 3(b) Simulation Time Vs PDR

Throughput



Simulation Time

Fig 3(c) Simulation Time Vs Throughput

Figures 3(a), 3(b), 3(c) show the comparison results of the proposed method and the previous method. In fig 3(a) end-end delay is reduced (i.e., below 0.010). In fig 3(b) PDR is achieved 100%. In fig 3(c) the amount of throughput achieved is greater.

V. CONCLUSION

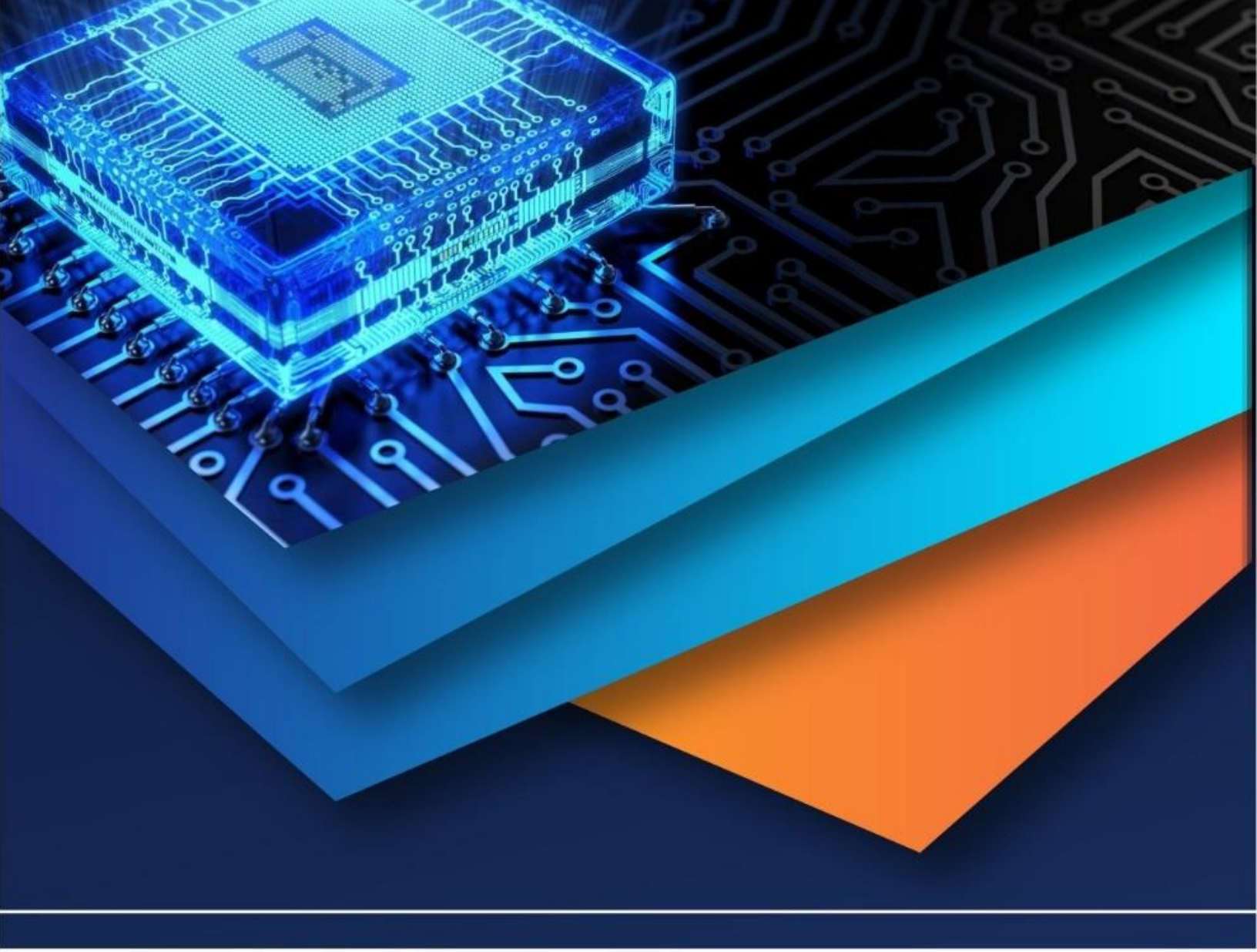
In this article, we studied the problem of traffic allocation in multiple-path routing algorithms in the presence of jammers whose effect can only be characterized statistically. In summary, we have presented a distance vector algorithm that is suitable for use with ad-hoc networks. AOMDV avoids problems with previous proposals and has the following features.

A. Nodes store only the routes that are needed
B. Need for broadcast is minimized
C. Reduces memory requirements and needles duplications
D. Quick response to link breakage in active routes
E. Loop free routes maintained by use of destination Sequence numbers
F. Scalable to large populations of nodes.

Compared to DSR and other algorithms which store continuously updated routes to all destinations in the ad-hoc network, our algorithm has longer latency for route establishment. AOMDV is an excellent choice for ad-hoc network establishment. It will be useful in applications for emergency services, conferencing, battlefield communications, and community-based networking. We look forward to further development of the protocol for quality of service.

REFERENCES

[1] Akyildiz, X. Wang, and W. Wang, “Wireless mesh networks: Asurvey,” Computer Networks, vol. 47, no. 4, pp. 445–487, Mar. 2005. [2]E. M. Sozer, M. Stojanovic, and J. G. Proakis, “Underwater acousticnetworks,” IEEE Journal of Oceanic Engineering, vol. 25, no. 1, pp. 72–83, Jan. 2000.
[2] 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
[3] A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks,”IEEE Computer, vol. 35, no. 10, pp. 54–62, Oct. 2002
[4] [5]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
[5] D. B. Johnson, D. A. Maltz, and J. Broch, DSR: The Dynamic SourceRouting Protocol for Multihop Wireless Ad Hoc Networks. Addison-Wesley, 2001, ch. 5, pp. 139–172.
[6] E. M. Royer and C. E. Perkins, “Ad hoc on-demand distance vector routing,” in Proc. 2nd IEEE Workshop on mobile Computing Systemsand Applications (WMCSA’99), New Orleans, LA, USA, Feb. 1999, pp.90–100
[7] 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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY