A Novel Jamming-aware Metric for MHWN Routing

B.Q. Kan, J.H. Fan

(Nanjing Telecommunication Technology Institute,PLA University of Science and Technology, Nanjing, China)

Abstract

In recent years, framework based on multi-hop wireless network (MHWN) mechanism has been paid more attentions. While the broadcast nature of wireless medium in MHWN 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. In this paper，we address the dynamical jamming problem in MHWN. In our proposed solutions, interference avoidance mechanisms were well concerned and a proactive multi-path routing mechanism based on novel jamming aware metric was proposed. The proposed mechanisms need extra support in the form of routing Interference Activity (IA) entries to build higher robust anti-jamming paths in MHWN, while keeping the less reroute request times. Our evaluations based on NS2 show that the proposed mechanisms can provide robust anti-jamming paths for MHWN.

Keywords multi-hop wireless network (MHWN); jamming; dynamics; multi-path routing

I. Introduction

Multi-Hop Wireless Network（MHWN）is formed to serve autonomous collection of nodes which communicate over wireless links through multi-hop fashion. Since MHWN can be rapidly deployed without the support of a fixed networking infrastructure, it has been envisioned for a wide range of application scenarios, such as mobile ad hoc networks（MANETs）, Mesh Network , Cognitive Radio Network(CRN) ,wireless sensor network.（WSN）,broadband Internet disaster relief and homeland security, etc[1].

While, the nature of using an open and shared physical medium for MHWN makes it susceptible to numerous interfering threats. Depending on the objectives and capabilities of an adversary, MHWN systems can be jammed in various ways. A simplest form of jamming is that the jammer interrupts transmitted messages to the targeted receivers by generating electromagnetic interference with the transmitting pairs' operational frequencies. So how to hold the ability to recover from attacks and maintain a continuous acceptable level of service in the design of MHWN is a crucial issue.

In recent years, some efforts of researchers address this issue, as summarized in [1], various efficient defense strategies have been developed. Among them, idiomatic methods to anti jamming attacks is the use of spread-spectrum techniques or beamforming in physical layer, forcing the adversary to jam a wider frequency band and significantly increasing the jamming power to reach the same goal[2]. Such techniques are especially effective against resource-constrained physical layer jamming adversaries, but not a good strategy against high layer denial of service (DoS) attacks. For example, intelligent attackers can launch various types of attacks in different layers of a MHWN. In [3] , the

authors showed that jammers can get multilayer protocol knowledge and incorporate it into jamming attacks, which can greatly reduce resource expenditure by attacking certain link layer, MAC layer or route layer. For example, jammer can only disrupt the "ACK" message delivery of its neighboring nodes with interference signals [1]. Therefore, more adaptive anti-jamming methods and defensive measures should be incorporated into higher-layer protocols.

However, most of previous studies only present countermeasures analysis for different type of jamming, and have not considered the real dynamics in the interference environment. Most of the works assume that the attackers adopt a fixed strategy that will not change with time. In fact, if the attackers are also equipped with cognitive technology, it is highly likely that they will adapt their attacking strategy according to the environment dynamics as well as the MHWN users' actions. So the impact on the network by jamming is probabilistic with the fact the jammers' strategies may be dynamic or the jammers themselves may be moving [2].

In order to characterize the dynamics of jamming, an intuitionistic way is to capture jammers' physical signals. Unfortunately, with the development of intelligent jamming signal, especially operating in high layer, it becomes more and more difficult for nodes in MHWN to accurately obtain the jammers' real-time physical signal. While, we should consider the fact that the characterization of the jamming impact on network is easy to collect. Therefore, in this paper, we apply a jamming impact collecting based approach, which formulates the dynamics of jamming. The basic idea of our solution is to first identify the states of victim nodes by collecting information on the impact of the jamming attack in various parts of the network, such as corresponding links packet delivery ratio (PDR) and received signal strength (RSS). Then the state of being jammed at each node was modeled as a random process. At a given measuring time, the randomness in the jammed state is due to the uncertainty in the jamming parameters, while the time-variability in the jammed state is due to the jamming dynamics and mobility. Since the effect of jamming at each node is probabilistic, the state being jammed will also be non-deterministic and, hence, must be studied using a stochastic framework. To model the stochastic state being jammed, we present a novel metric interference activity (IA), which is a statistical measure of jammed state along time. The interference activity results can be stored locally for reactive routing schemes or delivered to the neighbors for jamming avoidance process.

The rest of this paper is organized as follows. In Section II, we introduce the related works that address the anti-jamming issue. In Section III, we present a new jamming aware routing metric that characterizes the dynamic impact of jammer on network, as well as provide simulation studies of the effectiveness of our metric. In Section IV we introduce the formulation of a resilience-jamming multi-path routing based on the jamming dynamics. Then we evaluate the performance of the proposed protocol via detailed theoretical analysis in V and simulations in VI. In Section VII, we summarize our results and give directions for future work.

II. Related Works

In the recent years, some efforts of researchers developed various efficient defense strategies. In [4], Xu et al. proposed two evasion strategies against constant jammers: channel surfing and spatial retreat. And in [5], Cagalj et al proposed a reactive wormhole-based anti-jamming scheme for WSNs. In [6] , Wood et al studied routing around jammed regions of the network by detecting and mapping jammed areas in sensor networks. McCune et. al. proposed methods for detecting DoS attacks against broadcasts [7].

Tague et al [2] proposes a framework to control the channel access, using the random assignment of cryptographic keys to hide the location of the control channels. And, Li et al provided a game theoretic formulation for optimal jamming and anti-jamming strategies at the MAC layer in wireless sensor networks [8].

III. System Model

To formalize the concept of jammed state of a set of nodes, we define *Node Jammed State* and *Interference Activity* as follows. To give a unified model in a general way, let us consider an *N*-channel network first.

Definition 1. The *Node Jammed State* $\vec{\Lambda}$ denotes the jammed status of each channel in the node. $\vec{\Lambda}$ is an *N* dimensional vector comprising an entry for each channel that indicates whether the channel is being jammed or not in the state. $\vec{\Lambda} = (a_1, a_2, a_3, ..., a_N)$, and

$$a_i = \begin{cases} 1 & i\text{th channel being jammed} \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

Where a_i = 1, 0 indicates that channel *i* is being jammed or not, respectively. Note that each node jammed state is univocally identified by the set of active jammers' channels.

Since there are *N* channels in the node, there are 2^N possible states denoted by $\vec{\Lambda}_1$, $\vec{\Lambda}_2$, … , $\vec{\Lambda}_{2N}$. However, it is more meaningful to get the total number of jammed channels, that is $\Lambda = \sum_i a_i$, then we can rewrite $\vec{\Lambda}$ by $\Lambda_j = j, j = 0,1,..., N$. And The *Instantaneous Node Jammed State* at time t_0, $\Lambda(t_0)$, is the jammed state of the node at time t_0, i.e., $\Lambda(t_0) = \Lambda_j$ if the node jammed state at time t_0 is Λ_j. With *N*=1, it is simplified to a single channel network, so $\Lambda = 0$ indicates that the node is being unjammed，and $\Lambda = 1$ indicates that the node is being jammed.

Next, we define the *Interference Activity (IA)* which is the time jammed channels spend in each state per time unit.

Definition 2. *The Interference Activity* for node jammed state Λ_j, denoted by A_j, is the fraction of time during the interval [0, *L*] for which the node was in state Λ_j, i.e.,

$$A_j = \frac{1}{L}\int_0^L 1_{[\Lambda(t)=\Lambda_j]} d_t \quad (2)$$

in which, $1_{[\Lambda(t)=\Lambda_j]}$ denotes the indicator function such that $1_{[\Lambda(t)=\Lambda_j]}$=1， if the node jammed state at time t $\Lambda(t)$ is equal to Λ_j, and 0 otherwise. Clearly, the sum of A_j over all possible states adds to one, i.e. $\sum_j A_j = 1$.

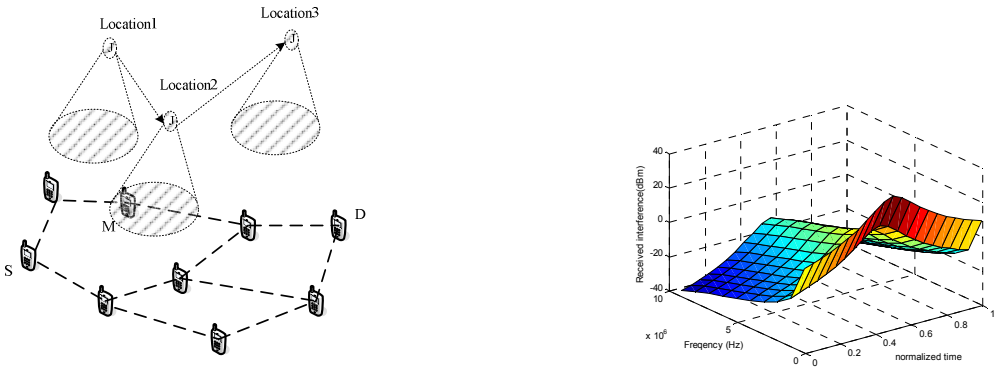
We separately denote as interference Activity set, $\vec{A}$ the distribution of time among all states that the node being jammed during the time interval [0, *L*], i.e., $\vec{A} = \{ A_j(\Lambda_j, L), \forall \Lambda_j \}$. Note that if the network is stationary and $L \to \infty$, then $\lim_{L\to\infty} A_j$ is the probability that the node at any time instant is in state Λ_j. And when *N*=1, $L \to \infty$, then A_1 is the instantaneous steady probability of launching attacks by the jammer.

To get the estimation of the *Interference Activity*, we need determine the *Node Jammed State* first. In this paper, we apply heuristics to determine whether the current node is experiencing non-transient jamming that might be called interference. So using the condition in

which the utility of the communication channel drops below a certain threshold, we may expand our definition of jamming to include any kind of denial-of-service. The idea is that below this utility threshold, we are unable to communicate effectively enough for long enough to accomplish our objectives. Factors which impact this utility metric can be repeated inability to access wireless channel, repeated collisions, excessive received signal level etc.[6], which may be obtained from the local radio hardware, MAC layer, network layer, or other available neighbors.

In Fig.1 and Fig.2, we descript how the metric IA can effectively estimate and characterize the impact of jamming for multi-channel case. Here, the *Node Jammed State* is determined by the excessive received signal level. Fig.3(a) and (b) show the real distribution of jamming and the estimation of IA, respectively, for the static single channel case.

Once obtaining the estimation of IA, we can get the jamming dynamics information for path availability. As we will see in the next section, we build dynamic multi-path routing protocols on this metric, providing method for sources to aggregate this information and characterize the available paths on the basis of minimized impact caused by jammers. In the following paper, we mainly consider the single channel case.



(a) Topology (b) Distribution of received interference signal

Fig.1 An example that illustrates a multi-channel network with a moving jammer from location 1, through location 2, to Loaction3.

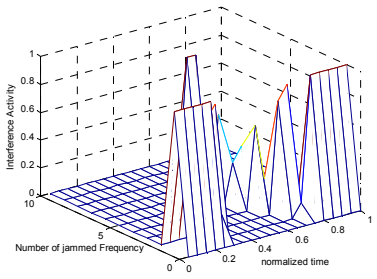
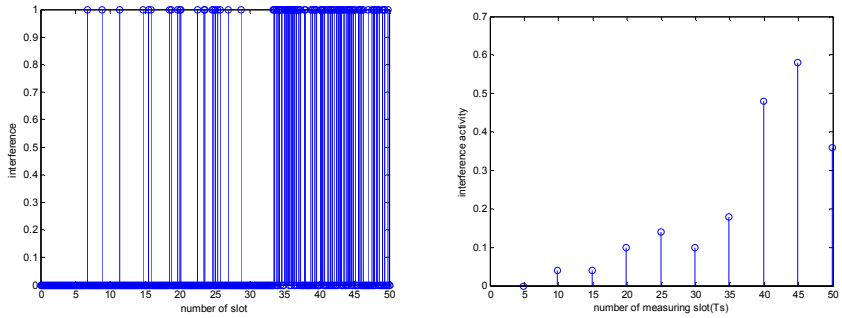


Fig.2 Estimation of A_j for multi-channel network with a moving jammer from location 1, through location 2, to Loaction3.



(a) Distribution of jamming (b) Estimation of IA

Fig.3 An example that illustrates a single-channel network with a random operation of jamming

IV Anti-jamming routing based on the novel metric

As we know, AOMDV did not need to record all of the passed nodes in the headers of control packets, which resulted in non-extra overhead into data packets, so we introduce an enhanced, interference activity aware multi-path routing protocol (IAMP) based on modified AOMDV protocol.

In order to improve multi-path routing anti-jamming performance, we use specific, timely, jamming dynamics information allowing us to work with the minimized jamming impact flow of path availability. This approach allows us both reuses of paths which become unavailable for a time and avoid simply regarding them as useless, upon jammed, and discarding them. We utilize the interference activity as a measure of jamming dynamics, and this metric is combined with hop count information in making a path selection. As in [9], the theoretical analysis has showed that the route reliability of non-disjoint paths is higher than disjoint paths when the wireless links are unstable. Therefore, in IAMP, we introduce a new multi-path discovery scheme that can find multiple loop free non-disjoint paths for relay nodes based on modified AOMDV route discovery procedure.

We describe the protocol in two components: route discovery and route maintenance. The more details are as followed.

*A. **Route Discovery Process***

The proposed routing protocol uses Route Request (RREQ) and Route Reply (RREP) messages defined in the AODV protocol for route discovery. Route Error (RERR) and Hello messages are also used for route maintenance.

In IAMP, similar to AODV and AOMDV, when a node needs to send the application packets to some destination, it first check its' routing table, if not finding effective entry, the source initiates a route discovery process by generating a route request packet (RREQ). Since the RREQ is flooded network-wide, a node may receive several copies of the same RREQ. As for the case of node S in Fig.4, it sends RREQ, and the neighboring nodes of node S will rebroadcast this RREQ packet after their first receiving that. The detail is as followed.

When a node broadcasts a RREQ message, the node in the network who first time receives a RREQ packet setups its alternate reverse paths to the node that sends out the RREQ packet. Then it copies the hop count to the original source node information and jamming dynamics information of the backward link of the previous node from the received RREQ packet to its local memory. And it adds them to the value of hop_count and IA field in the header of the received RREQ packet, rebroadcasts the RREQ message. Next time when this node receives the same RREQ packet again, it will discard the received packet. After a RREQ packet has been broadcasted in a

network, we can get a spanning tree rooted in the source node as shown in Fig.4 by drawing an arrow from each node's upstream to itself.

In order to avoid "broadcast storms" and incorporate jamming dynamics properties for choosing more reliable paths, in IAMP, we use priority-based route discovery strategy, which sets the priority by the candidates' IA metric. It assigns a high rebroadcast RREQ priority to low IA candidates. By using this mechanism, the node with lower jamming condition can have higher chance to setup the critical upstream path, hence more reliable path for source node. As an example, in Fig.4, when node 3, 4,5 receive RREQ form node 1, they will rebroadcast the first time received RREQ packet. As node 5 have lower IA value, it will have the highest priority to rebroadcast the received RREQ packet, hence node 8 will only setup the reverse path to node 5. So in the next routing discovery phase, RREP messages will be transmitted by more reliable paths.

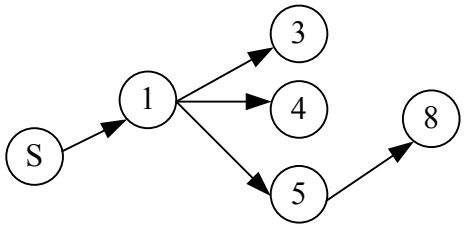


Fig.4. The spanning tree formed by the route request packets

When an intermediate node obtains a reverse path via a RREQ copy, it checks whether there are one or more valid forward paths to the destination. If so, the node generates a RREP and sends back a route reply (RREP) packet to its upstream node along the reverse path; and the node setups a forward route to the node that sends out the RREP packet after it receives the RREP packet. The RREP includes a forward path that was not used in any previous RREPs for this route discovery. The same send-back and setup-route procedures are repeated again and again, finally the source node will receive this RREP packet, and a route from the source node to the destination one is built. In this case, the intermediate node does not propagate the RREQ further. Otherwise, the node re-broadcasts the RREQ copy if it has not previously forwarded any other copy of this RREQ and this copy resulted in the formation/updation of a reverse path. These steps are the AOMDV protocol used to setup disjoint routes [10]. The flow process is illustrated in Fig.5.

So when the source node receives RREP messages, the new route is generated and updated. And when all the route discovery procedure is done, multiple routes will exist on the routing table.

In IAMP, path selection is based on IA as well as destination sequence number and advertised hop-count. The routing table structure for each path entry in IAMP is shown in Table 1.

Table 1 routing table entry structures in IAMP

Destination IP address1	Destination sequence number	Advertised hop-count	$IA_{\min} = \min_{i \in Path\_list}(IA_i)$ Path list {（next hop1，hop-count 1，IA1,potential_failure），（next hop2，hop-count2，IA2, potential_failure }	Expiration time
Destination IP address2	Destination sequence number	Advertised hop-count	$IA_{\min} = \min_{i \in Path\_list}(IA_i)$ Path list { （ next hop1,hop-count	Expiration time

…	…	…	1,IA1 ,potential_failure），（next hop2,hop-count2 ,IA2, potential_failure } …	…

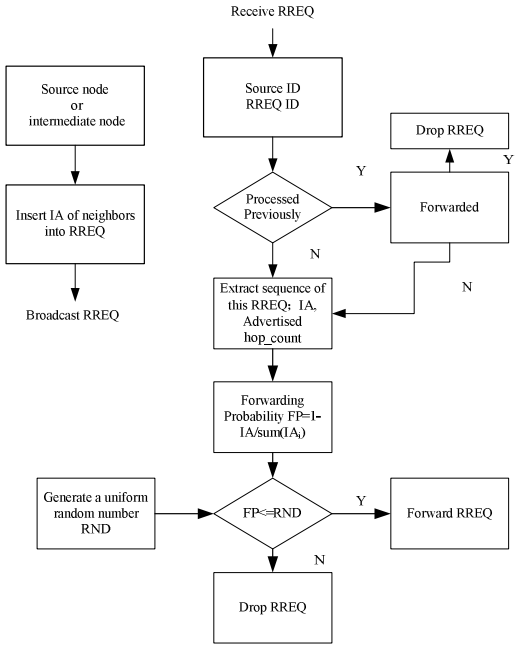


Fig.5. The flow chart for forwarding RREQ

B. Route maintenance

Route maintenance in IAMP is a simple extension to AOMDV route maintenance. Like AOMDV, IAMP also uses HELLO and RERR packets. To find efficient ways of addressing path failure , in IAMP, we use IA to preempt failures on a link on the active path.

In IAMP, both jamming dynamics sensing and neighbor detection are based on the periodic exchange of HELLO messages. When a node receives a Hello message, the node records the receiving IA. Then, it will update its route table entries and neighbor table entries of the changes in the field. While a node detects the IA is greater than a network-specific threshold, the node broadcasts a route error message for any active route coming through j for repairing the potentially link failure. Any node receiving a non-duplicate RERR checks for alternative paths to destination. By this way, when the node's IA is lower than a network-specific threshold, the potentially breaking link may be reutilized. So disconnections can be minimized, also reducing transmission latency and packet drop rate.

If an established link with a neighboring node j during time 2* HELLO _INTERVAL is broken, the node also sends RERR but without changing the potential_failure field. Any node that participates in the broken route marks the particular route as invalid and re-broadcasts the message until S or D are informed about the path breakage. According to the operation mode, an end node may restart the route request when all existing paths from S to D are broken.

V Simulation results

We compare the simulation results with AODV, AOMDV and our protocol. These experiments are carried out using NS version 2.34. The versions of AODV is supplied with NS and AOMDV has been implemented in the newly version. We summarize the main findings of the comparison at the end of this section.

A. Simulation Environments

In the following simulations, "hello" packet interval is set 1000 ms. Physical layer parameters of the NIC wireless network card is adopted with the random waypoint mobility model. Constant Bit Rate (CBR) sources are used with the IEEE 802.11 DCF MAC protocol.

To implement our jammer on an 802.11 legacy node in NS, we set the CCA threshold to a very high value (0 dBm). By this way, the device will ignore all the traffic in transit over the wireless medium. NS tool such as “threshold” has been used to find that packets always arrive at the jammer’s circuitry with power less than 0 dBm even if the distances between the jammer and the legitimate transceivers are very small. We ensure the jammer continuously transmitting packets on the medium by developing a specified MAC layer utility. With this, the jammer continuously broadcasts UDP packets. Given that the backoff functionality is by default disabled in 802.11 for broadcast traffic, our specified utility can ensure that packets are sent as fast as possible. With such transmissions the jammer does not wait for any ACK packets. To summarize, our jammer utility consists of a specific NIC configuration that sets CCA=0 and a specified utility for continuously generating and transmitting broadcast packets. In the following simulations we implement two or ten randomly distributed jamming nodes in the network respectively, each of which has a jamming range of 50m. The traffic generating rates of the jammers are randomly from 0.2 to 0.8 Mbps. There are 10 flows in the network with randomly selected sources and destinations. All the flows have the same traffic demand of 1 Mbps.

And in the simulated multihop wireless network, 100 wireless nodes are randomly deployed over a 1000x500m^2 region. Each node has a transmission range of 250m and an interference range of 350 m.

B. Performance Metrics

We use the following four metrics to compare the performance of the protocols.

1) Packet delivery ratio (PDR)

The packet delivery ratio is the ratio of the total number of received data packets by the destination to the total number of data packets sent by the source.

2) Average end-to-end delay of data packets

The average end-to-end delay is the transmission delay of data packets that are delivered successfully.

3) Throughput

It is the rate of data being received at the servers. This can be calculated as (Offered Load) × (Packet Delivery Ratio).

4) Routing overhead

The routing overhead is measured as the average number of control packets transmitted at each node during the simulation.

C. Results

The the main object of IAMP is to ensure the ability for normal nodes to operate effectively under dynamically jammed networks. To test this ability, we set up a network scenario and measure the performance as the jammers' Max-Pause time increases with 2 and 10 jammers respectably. We vary the Max-Pause time by setting 0s，10s，15s，20s，30s，60s and 100s.

In Fig.6 we show the PDR performance of the three routing protocols under two jammers scenario as the Max-Pause time of jammers is varied. Fig.7 shows the same set of experiments with ten jammers. In each set of experiments, as the Max-Pause time of jammers increases, so does the success rate for access to the radio channel. As the success rate in the network increases, the delivery of each packet requires a less number of transmissions to be delivered. Since IAMP transmits packets with less jammed path, the impact of jammers on the network performance is stable.

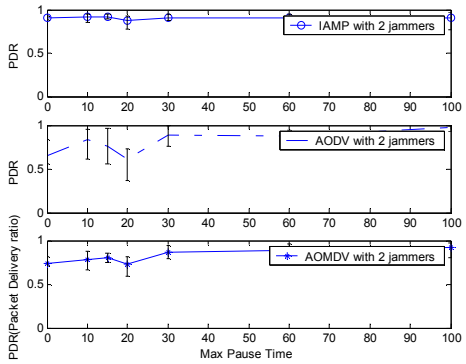


Fig.6. PDR performance with 2 jammers

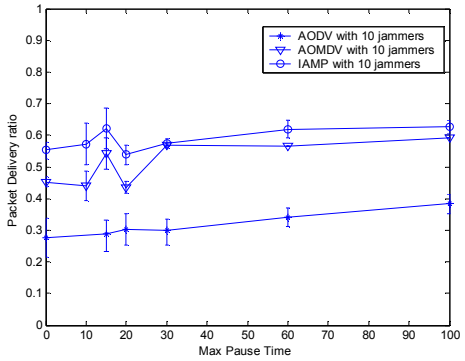


Fig.7. PDR performance with 10 jammers

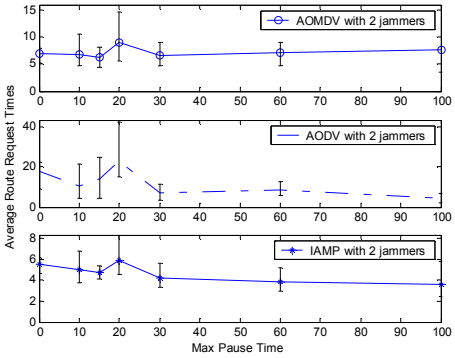


Fig.8.Average overhead with 2 jammers（100S）

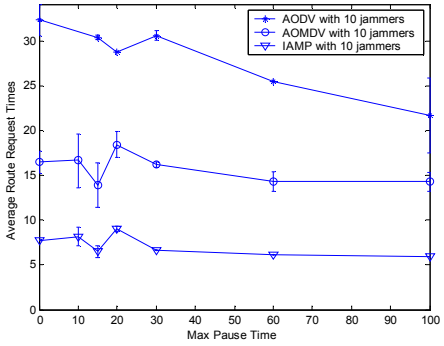


Fig.9.Average overhead with 10 jammers（100S）

Fig.8 and 10 show the routing overhead for the three routing protocols with two and ten jammers respectively. The advantage of IAMP over AODV and AOMDV is demonstrated as the Max-Pause time of jammers decreases. Whereas the performance of AODV is reduced significantly as the mobility of jammers increases, the IAMP and AOMDV protocol manages to maintain a good level of performance by finding backup paths. This decrease in performance of AODV and AOMDV with increasing number of jammers and their mobility is explained by the fact that, AODV interpret a unicast failure as a broken link, triggering route update mechanisms which require a large number of packets to be sent throughout the network, and AOMDV only finding paths without considering the network jamming dynamics which results the frequently lunching ineffective routing discovery process.

VI Conclusions

In this paper, a routing metric based on measuring jamming dynamics is proposed which utilizes interference activity, combined with hop-count, to select reliable links. Then, a jamming dynamics aware routing protocol, IAMP, is introduced. Simulation results provide detailed insights into the differences between the other protocols and show that IAMP can ensure more robust path in highly stressing environments.

References

[1] Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou. A Survey on Jamming Attacks and Countermeasures in WSNs. IEEE Communications Surveys & Tutorials, vol. 11, no. 4, pp. 42–56, 2009.

[2] Tague, P., Li M. and Poovendran. Mitigation of control channel jamming under node capture attacks. IEEE Transactions on Mobile Computing, 2009, 8(9), 1221–1234.

[3] Lazos, L., Liu, S., & Krunz, M.. Mitigating controlchannel jamming attacks in multi-channel ad hoc networks. In ACM WiSec 2009 .

[4] W. Xu, W. Trappe, Y. Zhang, “Anti-Jamming

Timing Channels for Wireless Networks," In Proc. of the 1st ACM Conference on Wireless Security (WiSec), 2008.

[5] M. Cagalj, S. Capkun, and J.-P. Hubaux, \Wormhole-based Anti-jamming Techniques in Sensor Networks," IEEE Trans. on Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007.

[6] A. D. Wood, J. A. Stankovic, and S. H. Son, JAM: A Jammed-Area Mapping Service for Sensor Networks," in Proc. of RTSS, 2003.

[7] J. M. McCune, E. Shi, A. Perrig, and M. K. Reiter. Detection of Denial of Message Attacks on Sensor Network Broadcasts. in Proc.of IEEE Symposium on Security and Privacy, 2005.

[8] M. Li, I. Koutsopoulos, and R. Poovendran, \Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks," in Proc. of INFOCOM, 2007.

[9] Y. Zhongbang, J. Junfeng and F. Pingyi,. A neighbor-table-based multipath routing in ad hoc networks. Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual , Volume: 3, pp. 1739 - 1743 ,2003.

[10] Marina, M. K. and Das, S. R., On-demand Multipath Distance Vector Routing for Ad Hoc Networks, in Proceedings of the International Conference for Network Protocols (ICNP). Nov. 2001: Riverside, CA. p. 14-23.

[11] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, “On the Performance of IEEE 802.11 under Jamming,” in Proc. of IEEE INFOCOM, 2008.

[12] Shanshan Jiang and Yuan Xue. Providing survivability against jamming attack for multi-radio multi-channel wireless mesh networks. Journal of Network and Computer Applications, 34 (2011) ,443–454.

[13] P. Tague, S. Nabar, J. A. Ritcey, and R. Poovendran.Jamming- Aware Traffic Allocation for Multiple-Path Routing Using Portfolio Selection. IEEE/ACM Transactions on Networking, 2010.

[14] Chen, Xiaoqin and Jones, Haley and Jayalath, Dhammika.Channel aware routing in MANETs with route handoff. IEEE Transactions on Mobile Computing, Volume 2010 .