Kan and Fan *EURASIP Journal on Wireless Communications and Networking* 2012, **2012**:267
http://jis.eurasipjournals.com/content/2012/1/267

EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Interference activity aware multi-path routing protocol

Bao-Qiang Kan* and Jian-Huan Fan

Abstract

With the development of wireless network, framework based on multi-hop wireless network (MHWN) mechanism is paid more attention. However, the unique characteristics of MHWN, such as distributed and dynamic network architecture, broadcast nature of wireless medium and stringent resource constraints of wireless devices, make it subject to interference from other nearby communication system, malicious jammers, and other sources of noise. So countermeasure should be taken to ensure tolerant network service for MHWN especially in jammed situations. Although some works have addressed this issue, few works consider interference dynamics. In this article, we investigate the effects of time-varying interference on MHWN. Different from previous studies, a proactive multi-path routing mechanism based on interference dynamic metric is presented. In the novel mechanism, we incorporate the routing interference activity entries and hop count to build higher robust anti-jamming paths in MHWN, with less re-route request times. Interference avoidance performance is well evaluated based on NS2. The results show that the proposed mechanisms can perform well in a wide variety of interference conditions.

Keywords: Multi-hop wireless network (MHWN), Interference dynamics, Multi-path routing

Introduction

The nature of multi-hop wireless network (MHWN) using an open and shared physical medium make it subject to numerous interfering threats. 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 works addressing this issue, as summarized in [1], various efficient defense strategies have been proposed and developed. However, few of them consider the real dynamics in the interference environment. Most of the works assume that the interference is constant with time. In fact, interference is time-varying in many cases.

An intuitionist way to characterize the dynamics of interference is to capture jammers' physical signals. Unfortunately, it is not an easy job because of the development of intelligent jamming signal, especially operating in high layer [2-8]. While, we should notice the fact that the characterization of the interference effects on network is easy to collect. Therefore, in this article, we propose a jamming impact collecting-based approach, which formulates the dynamics of jamming. The aim of our solution is first to identify the states of victim nodes by collecting information in various parts of the network, such as corresponding links packet delivery ratio (PDR) and received signal strength (RSS), then we model the state of being jammed at each node as a random process. In general, the randomness in jammed state is due to the uncertainty of jamming parameters, and the time-variability in jammed state is due to the interference dynamics. As the effect of jamming at each node is probabilistic, the state of being jammed will also be non-deterministic and, hence, must be studied using a stochastic framework. To model the stochastic state of being jammed, we present a novel metric interference activity (IA), which is a statistical measuring of jammed state along with time. The IA results can be stored locally for reactive routing schemes or delivered to the neighbors for jamming avoidance process.

The goal of this article is to find the network continuous service strategies that can minimize the performance degradation under jamming attacks. In this article, we introduce an enhanced, jamming aware version of the AOMDV routing protocol. The key aspect of this enhancement is that our protocol explicitly incorporates

* Correspondence: bqkan@163.com
PLA University of Science and Technology, Nanjing, China

the unique characteristics of wireless network including the jamming dynamics and path optimally selection. To the best of our knowledge, this is the first work that studies the jamming-resistant network restoration strategies in MHWNs using a jamming dynamics model-based approach.

The rest of this article is organized as follows. In Section. 2, we introduce the related works that address the multiple-path issue. In Section 3, we present a new 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 3, we also introduce the formulation of a resilience-jamming multipath routing based on the jamming dynamics. Then, we evaluate the performance of the proposed protocol via detailed theoretical analysis in Section 4 and simulations in Section 5. In Section 6, we summarize our results and give directions for future work.

Background and related study

Among various efficient defense strategies, the simplest method to defend a network against jamming attacks is the use of spread-spectrum techniques or beamforming in physical layer [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, as intelligent attackers can launch various types of attacks in different layers of a MHWN. In [3], the authors showed that jammers can get multi-layer 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]. Hence, more adaptive anti-jamming methods and defensive measures should be incorporated into higher layer protocols. In [3], Xu et al. proposed two evasion strategies against constant jammers: channel surfing and spatial retreat. And in [4], Cagalj et al. proposed a reactive wormhole-based anti-jamming scheme for WSNs. In [5], Wood et al. studied routing around jammed regions of the network by detecting and mapping jammed areas in sensor networks. JM McCune et al. [7] proposed methods for detecting DoS attacks against broadcasts. 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, M Li et al. [8] provided a game theoretic formulation for optimal jamming and anti-jamming strategies at the MAC layer in wireless sensor networks.

In recent years, several multiple-path variants of source routing protocols for wireless networks have been proposed [6]. For instance, dynamic source routing (DSR) [9] and temporally ordered routing algorithm (TORA) [10] have the ability to request multiple paths between the source node and the destination nodes. So in DSR protocol, the destination node can provide multiple node-disjoint paths using the information received from multiple route queries which might traverse distinct paths. SMR is an on-demand multipath routing protocol based on the DSR protocol. SMR is more efficient when new route discovery is initiated only when both the routes are broken, as it generates less control overhead. MP-ODP was proposed to discover alternate disjoint routes for the DSR protocol [11]. It was shown in the simulation done for a network with 60 mobile nodes that MP-ODP has a better delivery rate, control overhead ratio, and error ratio, over DSR. TORA attempt to builds and maintains multiple paths using Directed Acyclic Graph (DAG) rooted from the destination to guarantee loop-freedom. ad hoc on-demand distance vector multi-path (AODVM) is another multi-path routing protocol providing node-disjoint paths based on variants of AODV [12]. AOMDV routing protocol is proposed by extending AODV for constructing node-disjoint or link-disjoint multiple loop free paths using “advertised hop count.” The results show that AOMDV offers reduction in end-to-end delay more than a factor of two, as it has a particular property of flooding to achieve link disjointness. It provides 20% reduction in the routing overhead and the frequency of route discoveries but increases the number of delivered messages. The standard DYMO protocol [13] has been extended to keep multiple routes in DYMOM [14]. DYMOM keeps only node-disjoint routes. In [15], the authors propose a dual-path routing protocol, which is suitable for tactical wireless networks for reducing control message overhead for route discovery in multi-channel multi-interface environments. Channel information is used to reduce interferences and control message overhead.

As stated in [16], there are some key differences between the multi-path routing protocols and the multipath selection routing protocols. Although many works have considered the multi-path routing protocols, a few focus on the routing metrics for multi-path selection. Traditionally, designing routing protocols in wireless networks based on minimum hop count is an unwritten law. However, such routes may lead to poor throughput and delay as they include jammed or lossy links. Furthermore, the above-mentioned multi-path routing research does not focus on utilizing jamming dynamics information for path availability under jammed environments. Instead, a multi-path selection routing protocol can select better paths by explicitly taking the quality of the wireless links into account. In this article, we utilize timely jamming dynamics information as routing metric to enhance throughput and QoS. In particular, our protocol explicitly incorporates the unique characteristics of wireless network including the interference dynamics and path assignment.

Proposed schemes

Metric of interference dynamics based on determining node state

We define the novel node jammed state and IA metric as follows.. To give a unified model in a general way, an N channel network is considered firstly.

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

As there are N channels in the node, there are 2^N possible states denoted by $\rightarrow \Lambda_1, \rightarrow \Lambda_2, \ldots \rightarrow \Lambda_{2^N}$ However, it is more meaningful to get the total number of jammed channels, i.e.$^{\Lambda=}\sum_i{}^{a_i}$, then we can rewrite $\rightarrow \Lambda$ by $\Lambda_j = j, j = 0, 1, \ldots, N$. 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 node is being unjammed, and Λ=1 indicates that node is being jammed.

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

Definition 2 The *IA* for node jammed state $_{\Delta_i}$, denoted by $_{A_j}$, is the fraction of time during the interval [0, *T*] for which the node is in state Λ_j, i.e.,$A_j = \frac{1}{T}\int_0^T I_{[\Lambda(t)=\Lambda_j]}dt$, in which, $\mathrm{I}_{[\Lambda(t)=\Lambda_j]}$ denotes the indicator function such that $I_{[\Lambda(t)=\Lambda_j]} = 1$, 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 IA set, $\rightarrow A$, the distribution of time among all states that the node being jammed during the time interval [0, *T*], i.e., $\rightarrow A = \{A_j(\Lambda_j, T), \forall \Lambda_j\}$. Note that if the network is stationary and, $T \rightarrow \infty$, then $\lim_{T\rightarrow\infty} A_j$is the probability that the node at any time instant is in state Λ_j. And when $N = 1$, $T \rightarrow \infty$, then A_1 is the instantaneous steady probability of launching attacks by the jammer.

From analysis above, to get the estimation of *IA*, we need determine the *node jammed state* first. In this article, we apply heuristic approach 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 DoS. The idea is that below this utility threshold, we are unable to communicate effectively 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. [5,6], which may be obtained from the local radio hardware, MAC layer, network layer, or other available neighbors.

In Figures 1 and 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. Figure 3(a) and (b) shows 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, a dynamic multi-path routing protocol on this metric is presented, providing methods for sources to aggregate this information and choose the available paths based on impact caused by jammers. In the following article, we mainly consider the single channel case.

Multi-path routing protocol aware of IA

We utilize the IA as a metric, combined with hop count information in making a path selection. This approach allows us to both reuse of paths which become unavailable for a time and avoid by simply treating them as useless, upon interfered, and discarding them. In [17], 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 this article, 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 [18-20].

We describe the protocol in two components: route discovery and route maintenance. 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 our IA aware multi-path (IAMP) routing protocol, 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 RREQ packet. Since the RREQ is flooded network-wide, a node may receive several copies of the same RREQ

When a node broadcasts a RREQ message, the node in the network who first time receives a RREQ packet set

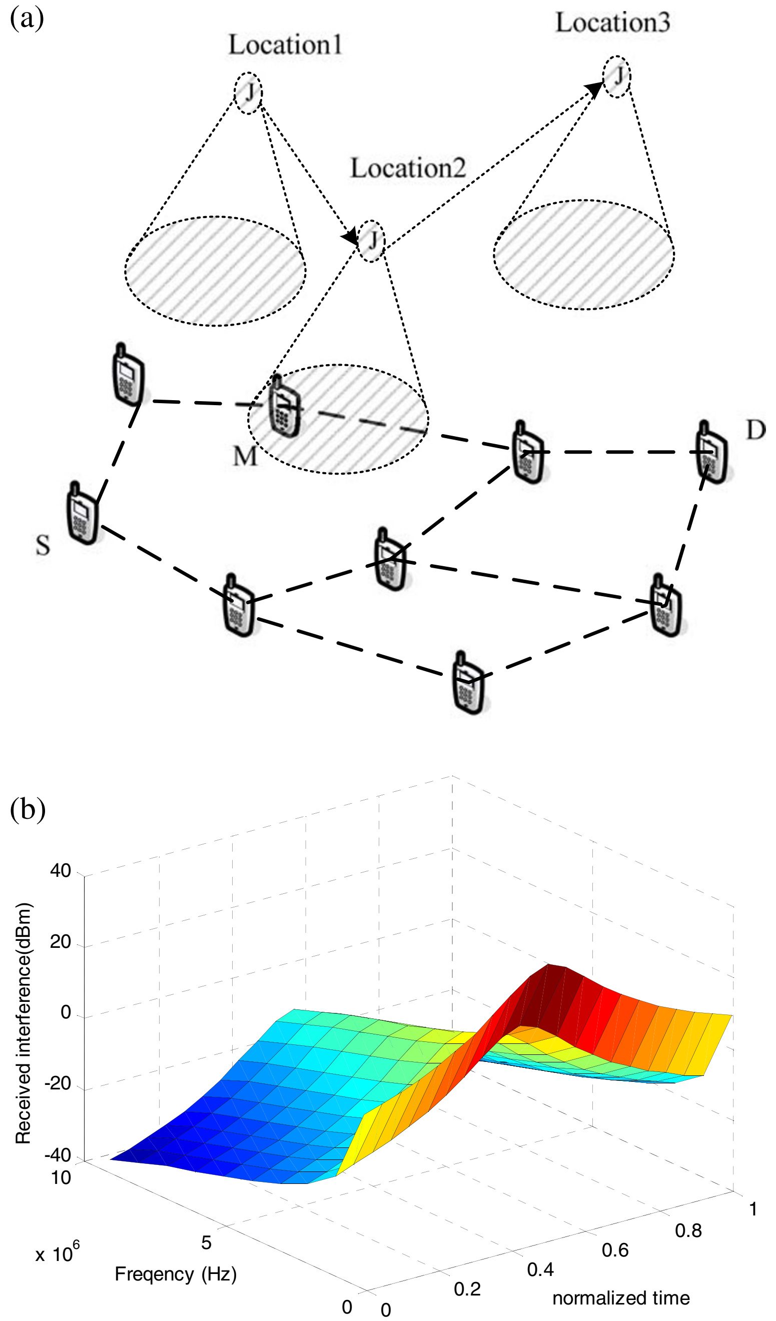

Figure 1 An example that illustrates a multi-channel network with a moving jammer from location 1, through location 2, to loaction 3. Topology, (b) distribution of received interference signal.

ups its alternate reverse paths to the node that sends out the RREQ packet. Then it copies the hop_count to the original source node 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 Figure 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

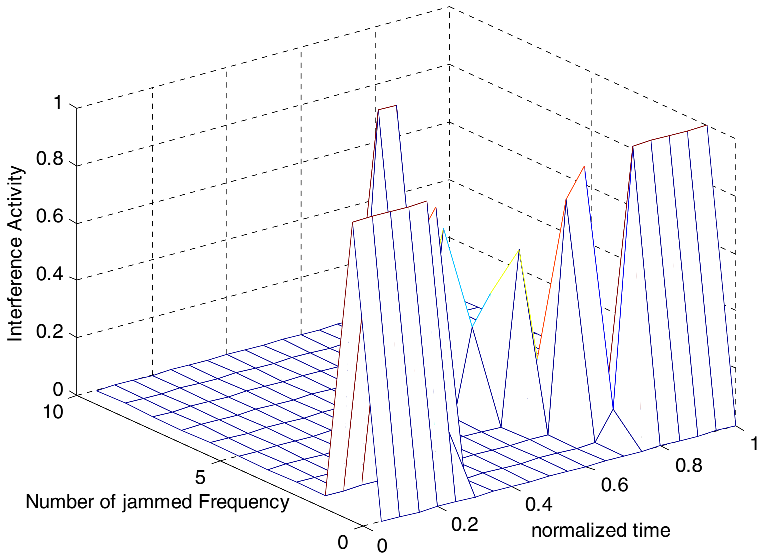

Figure 2 Estimation of A_j for multi-channel network with a moving jammer from location 1, through location 2, to loaction 3.

strategy, which sets the priority by the candidates' IA metric. It assigns a high rebroadcast RREQ priority to low IA candidates. Using this mechanism, the node with lower jamming condition can have higher chance to set up the critical upstream path, hence more reliable path for source node. The flow process is illustrated in Figure 5.

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 RREP packet to its upstream node along the reverse path; and the node set ups 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/updating of a reverse path. These steps are the AOMDV protocol used to set up disjoint routes [21].

We make some modifications here to obtain multiple non-disjoint routes information.

First, we divide nodes into two categories, the verge nodes and the backbone nodes.

In a spanning tree, as shown in Figure 4, a backbone node is defined as a node which has both the upstream and the downstream neighbors. For a verge node, it has only upstream neighbors but without any downstream one. To make nodes self-determine the category, we use the following methods. For example, node 1 in Figure 4, assuming every neighboring node of node 1 (such as nodes 2, 4, 5) has already received the same RREQ packet before it received the one sent by other nodes. So, when a node 4 first time receives a RREQ packet, it labels itself verge node, then it adds its address to the RREQ rq_last_hop field and rebroadcasts this RREQ packet. If node 4 can hear any neighboring node that rebroadcasts the same RREQ packet with increased hop_count which is broadcasted by node 4 itself, node 4 will change itself to be a backbone node; otherwise it will remain the "verge" status. In IAMP, rq_last_hop field is added in RREQ packet to implement the function.

Second, in the RREP process, we arrange nodes of different types act differently when receiving RREP packets. The relative details are explained in the following part.

A verge node will turn on its overhearing function. When a verge node *i* overhears a RREP packet sent by node *j*, node *i* set ups a forward route to node *j*, puts the hop count and IA information of node *j* and that of itself into the header of the RREP packet, and then sends back to its upstream node. To avoid the loop problem, we restrict that every verge node can only overhear and set up the forward route once. For example, in Figure 4, when the destination node D receives the RREQ packet broadcasted by node 7, node D will send back a RREP packet with its hop count and IA information to node 7. The verge node 3 overhears the RREP packet sent by node D, so node 3 set ups a forward route to node D, and then sends back a RREP packet to its upstream node 2 with its own hop count and IA information and that of node D. The verge node 4 will set up a forward route to any

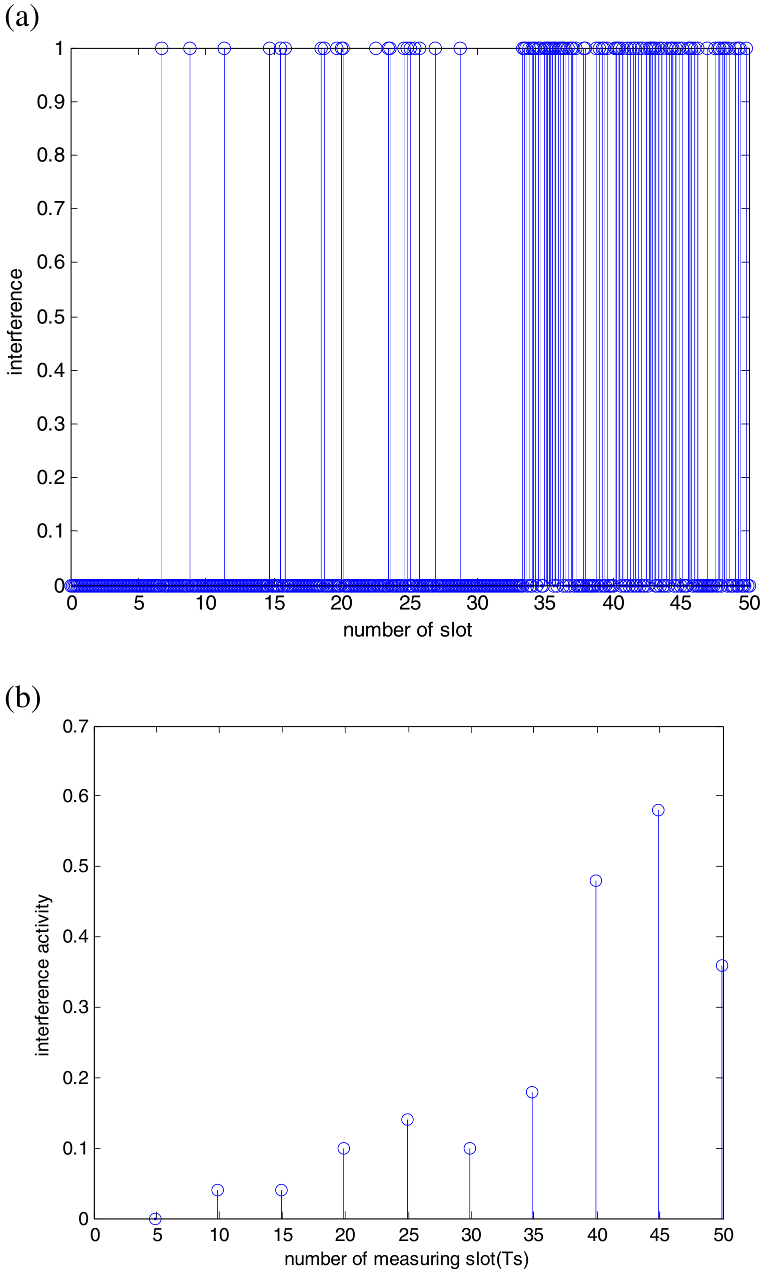

Figure 3 An example that illustrates a single-channel network with a random operation of jamming. (**a**) Distribution of jamming, (**b**) estimation of IA.

one node of 3, 6, or 7 depends on whose RREP packets can be overheard by node 4 first.

Contrarily, backbone nodes will not overhear any packet. When a backbone node receives a RREP packet for the first time, it set ups a forward route to the sender of the RREP packet, updates the hop count and IA information field in the header of RREP packet with its own values, and then sends this RREP packet back to the next hop node using its reverse path. If a backbone node *i* receives a same RREP packet again, it will check whether its own hop_count value is greater than that of the piggybacked filed in the RREP packet. If the checking result is true, the backbone node *i* set ups a forward route to the sender. However, the backbone node forwards the same RREP packet only once. As we use priority-based route discovery strategy, RREP packet will contains information of the path to destination with the least IA or with the same IA but lower hop count value.

As for the case of node 5 in Figure 4, it may receive the first RREP packet from node 6 or 7. Anyway, it will set up

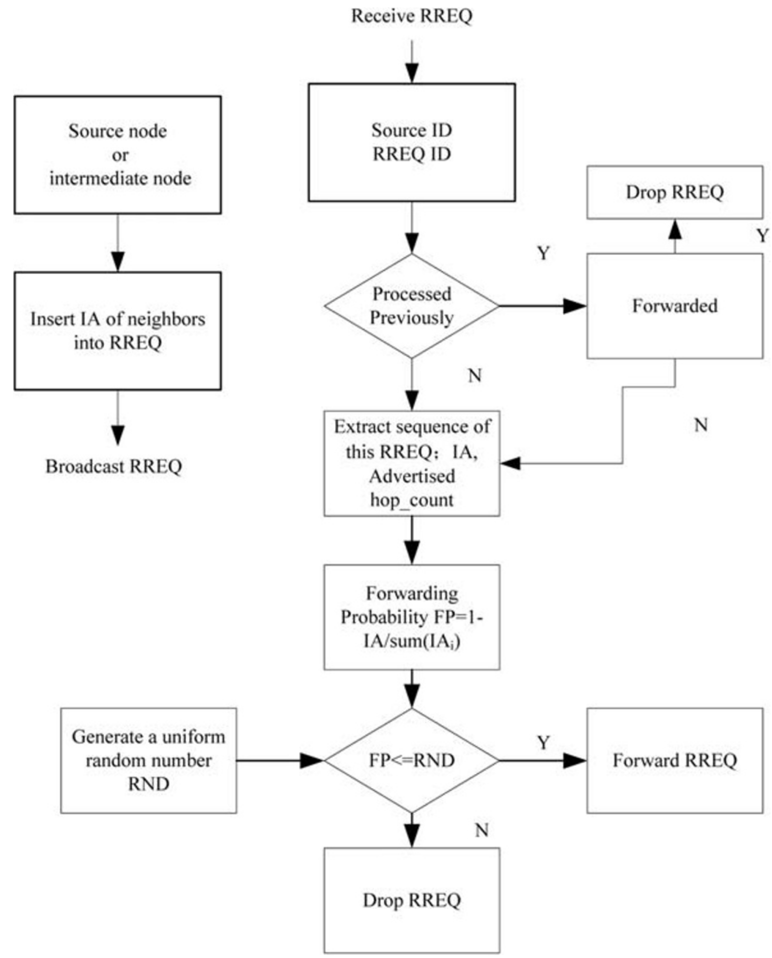

Figure 4 **Routing discovery process.**

forward routes to nodes 6 and 7, respectively, for the hop count to destination of nodes 6 and 7 are less than that of the node 5. And node 5 will forward the RREP message from the one with least IA using its reverse path.

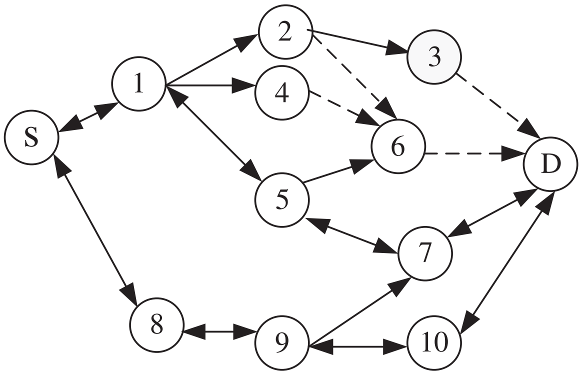

Figure 5 **The flow chart for forwarding RREQ.**

So when the source node receives RREP messages, the new route is formulated and updated. And when all the route discovery procedure is done, multiple routes will exist on the routing table. Figure 4 shows the multiple paths found by our scheme.

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.

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

Table 1 Routing table entry structures in IAMP

Destination IP address1	Destination sequence number	Advertised hop-count	$\mathrm{IA_{min}} = \min_{i \in \mathrm{Pathlist}} (\mathrm{IA}_i)$ 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	$\mathrm{IA_{min}} = \min_{i \in \mathrm{Pathlist}} (\mathrm{IA}_i)$ Path list {(nexthop1,hop-count 1,IA1, potential_failure), (nexthop2,hop-count2,IA2, potential_failure}	Expiration time
…	…	…	…	…

greater than a network-specific threshold, the node broadcasts a RERR 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. If not, as for the case of node 5 in Figure 4, it propagates the RERR from the node 7. Otherwise, if it has one or more "good" alternative paths to the destination, it marks the potentially jammed path with next_hop = 7 indicated in the RERR as dormant, setting the potential_failure field in its routing table entry for that path to Truth. The RERR is then dropped. 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 re-start the RREQ when all existing paths from S to D are broken.

Overhead analysis

In this section, we give a framework to analyze the overhead performance of IAMP. From the essential behavior of the IAMP routing protocols similar to AODV and AOMDV, we consider that the overhead of the routing protocol can be associated with two operations: route discovery and route maintenance. To give an average overhead analysis, we assume a MHWN of N nodes which are distributed on a two-dimensional plane over an area of side length $2L{*}2\mathrm{L}$. Then, the node density $\rho = N/(2L)^2$. Assuming all nodes in the network have equal transmission range r_0, the expected distance between a source-destination pair for each connection can be given by $\frac{L}{3}\left(\sqrt{2+}1n\left(1+\sqrt{2}\right)\right)$. So we can approximate the expected number of hops per connection as $L_h = \frac{L}{3r_0}\left(1n\left(1+\sqrt{2}\right)\right)$. Furthermore, we assume that each link has a link breakage rate of μ, i.e., a link has an average lifetime of $1/\mu$ seconds on average. The link breakage rate μ is determined by two factors, i.e., natural failure rate and jammed rate. Let the natural failure rate be $P_{failure}$, and the jammed rate be P_{jam}, then $\mu = 1-\left(p_{failure}\right)\left(1-p_{jam}\right)$.

Assuming that N nodes each broadcast a RREQ λ_m (i.e. the route discovery frequency) times per second, λ_m is related to link breakage as $\lambda_m = \mu L_\mathrm{h}$. As stated in [22], the expected forward degree (EFD) of a node is the average (or mean) number of neighbors of that node which forward a received RREQ. Then, we can get the amount of overheads due to the RREQs using EFD metric as

$$H_{rq} = N\lambda_m M_{rq}\left(p_s n_{avg}\sum_{i=1}^{L_h-1} p_s^{i+1}\pi \prod_{j=1}^{i} d_f[j]\right) \tag{1}$$

in which, p_s is the probability that a node will forward an RREQ message to its neighbors and the message will be successfully delivered to them, n_{avg} represent the average degree of a node, i.e., $n_{avg} = \rho\pi r_0^2$, $d_f[j]$ is the EFD of a node at j hops which is the ratio of nodes in the two rings, M_{rq} is the size of RREQ.

Different from AODV and AOMDV, in IAMP, nodes of both non-disjoint and disjoint paths forward RREP. As the verge node who overhears the REPP packet will forward it to its upstream nodes, the overhead due to RREPs can be stated as

$$H_{rp} = N\nu\lambda_m M_{rp} L_h\left(1+n_{avg}-2\right) \tag{2}$$

in which, ν is the average routes maintained by source-destination pair and M_{rp} is the size of RREP.

When a link is broken, an error packet is sent back to the source to signal the link breakage. Since each source-destination pair maintains ν routes, the RERR broadcast frequency can be given by $p_{rerr} = 1-(1-\mu)^{\nu L_h}$. Recall that L_r is the average length of the path from the broken link to the source ($L_\mathrm{r} < L_\mathrm{h}$). The probability that a node will forward an RERR

Table 2 Overhead under different link break rate

Link break rate	0	0.1000	0.2000	0.3000	0.4000	0.5000
Overhead (*10e4)						
AODV	2.8716	3.1695	3.4674	3.7653	4.0632	4.3611
AOMDV	3.0149	3.0286	3.0605	3.1285	3.2508	3.4454
IAMP	3.0908	3.1015	3.1123	3.1231	3.1346	3.1506

message to its upstream nodes is $p_{rerr_{f}wd} = \mu^{v}$, then the overheads due to error packets is

$$H_{rr} = \sum_{i=1}^{L_r-1} M_{rr} L_h v p_{rerr} \mu^{iv} \tag{3}$$

in which, M_{rr} is the size of RERR.Then, the total amount of overheads due to RREQs, RREPs, RERRs for IAMP can be expressed as $H = H_{rq} + H_{rp} + H_{rr}$.

Using the results derived above, we give the numerical analysis by choosing AODV as typical candidates for single path, and AOMDV, IAMP for multi-path routing protocols, respectively. Clearly seen from Table 2, AODV and AOMDV exhibit higher overhead than IAMP when the link break rate is high. So it is again confirmed that IAMP have the more ability to operate under network scenario with changeful environments.

Simulation results

We compare the simulation results with AODV, AOMDV, and our proposed IAMP on-demand routing 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 new version [23]. We summarize the main findings of the comparison at the end of this section.

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 <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 50 m. The traffic-generating rates of the jammers are randomly from 0.2 to 0.8 Mbps. There are ten flows in the network with randomly selected sources and destinations. All the flows have the same

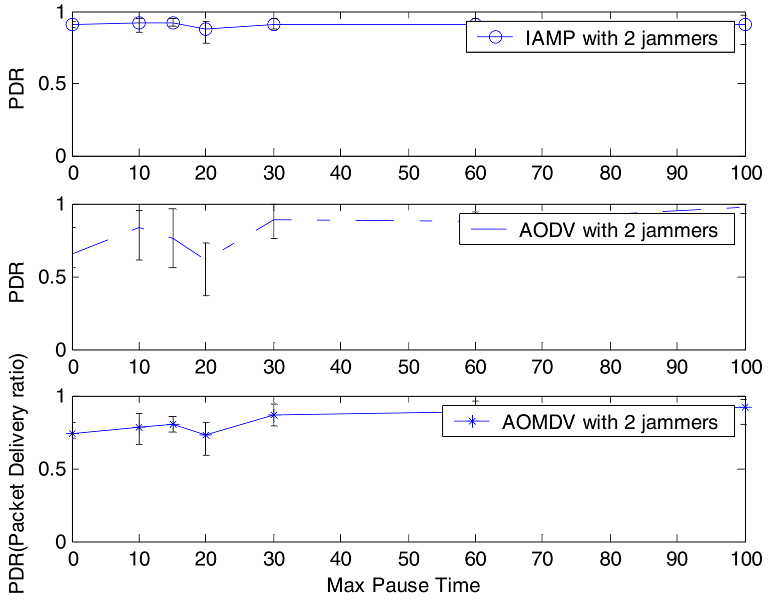

Figure 6 PDR performance with 2 jammers.

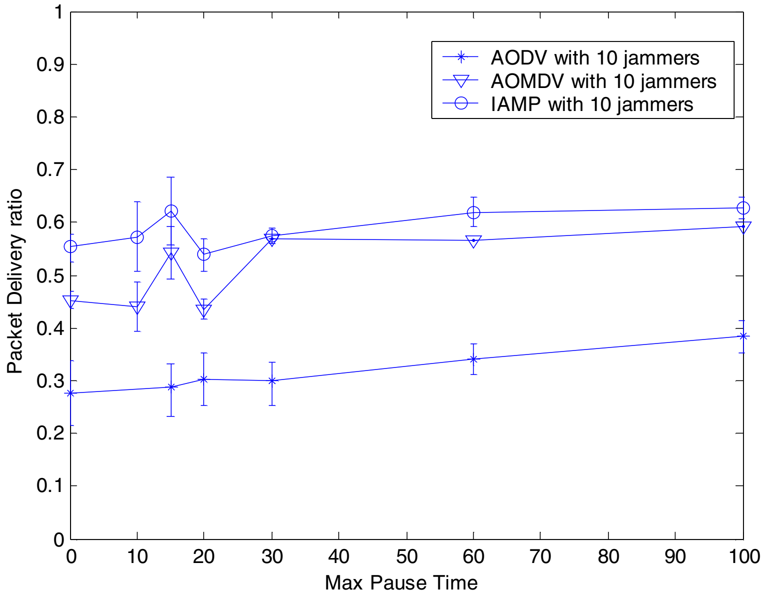

Figure 7 PDR performance with 10 jammers.

traffic demand of 1 Mbp. And in the simulated MHWN, 100 wireless nodes are randomly deployed over a 1000 × 500 m^2 region. Each node has a transmission range of 250 m and an interference range of 350 m.

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

(1) PDR: The PDR 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: The rate of data being received at the servers. This can be calculated as (offered load) × (PDR).

(4) Routing overhead: The routing overhead is measured as the average number of control packets transmitted at each node during the simulation.

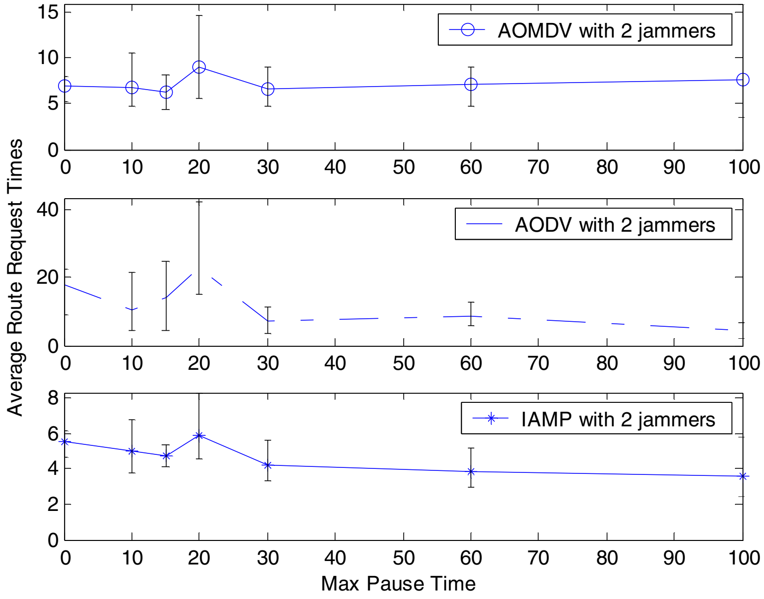

Figure 8 Average overhead with 2 jammers (100 s).

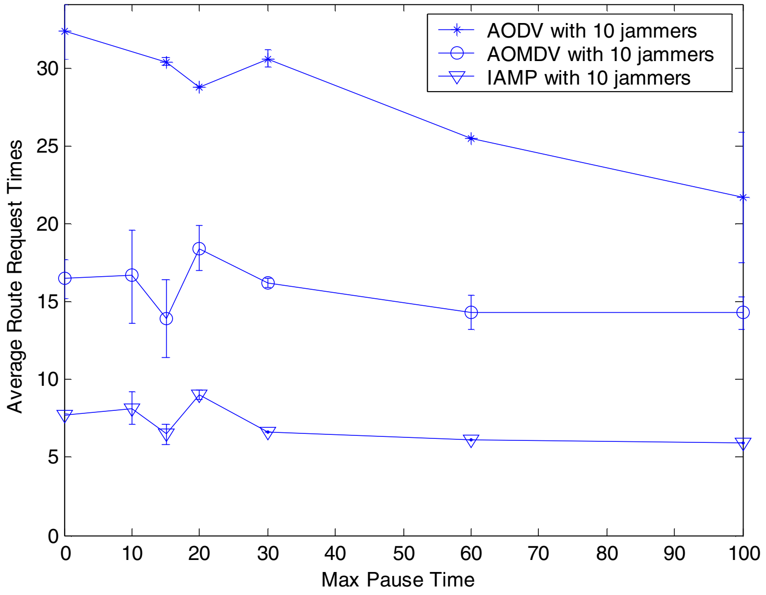

Figure 9 Average overhead with 10 jammers (100 s).

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, respectively. We vary the Max-Pause time by setting 0, 10, 15, 20, 30, 60, and 100 s.

In Figure 6, we show the PDR performance of the three routing protocols under two jammers scenario as the Max-Pause time of jammers is varied. Figure 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 accessing 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.

Figures 8 and 9 show the routing overhead for the three routing protocols with two and ten jammers,

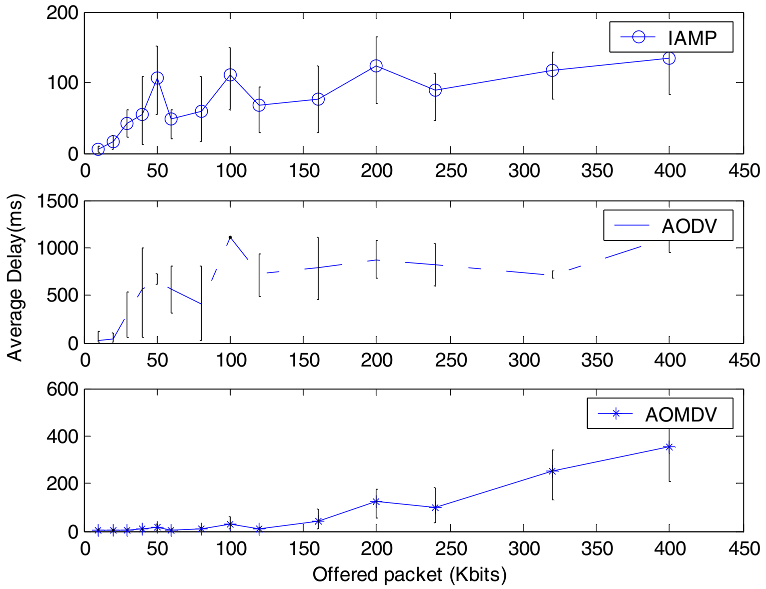

Figure 10 Average delay performance.

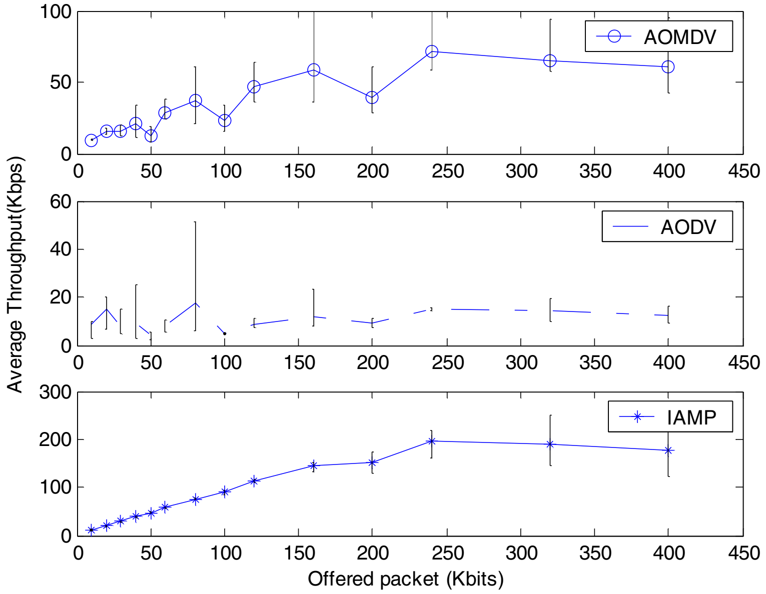

Figure 11 Average throughput performance.

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.

As the metric IA is modeled on node jamming state which is determined using the condition in which the utility of the communication channel drops below a certain threshold, IAMP should have the ability to operate effectively within congested networks. To test the performance of IAMP within congested networks, we set up a network scenario and measure the performance as the offered load increases. The network scenario used is with 100 fixed nodes, 50 mobile nodes. There are three server nodes, and the number of clients is varied. Each client sends constant-bit-rate traffic at a rate of five packets per second. The size of packets is varied to increase the congestion in the network.

In Figure 10, we show the average delay performance of the three routing protocols as the number of clients is varied. Figure 11 shows the throughput for the three routing protocols as the offered load to the network increases. As the contention in the network increases, the delivery of each packet requires a larger number of transmissions to be delivered. Since IAMP retransmits packets after they fail to unicast, this increased cost represents the increased congestion in the network.

Conclusions

In this article, we studied the problem of finding the reliable route with minimum jamming impact for a multiple-hop wireless network in the presence of jammers whose effect can only be characterized statistically. We have presented a novel routing metric IA to probabilistically characterize the local impact of a dynamic jamming attack. And a jamming dynamics aware multiple-path routing protocol, IAMP, incorporating this metric into the routing algorithm was proposed. We presented numeric and simulation results to illustrate the impact of jamming dynamics and mobility on network throughput and to demonstrate the efficacy of our algorithm. In our future works, we will take the cooperative jammers into considerations [24,25].

Competing interests

both authors declare that they have no competing interests.

Received: 6 September 2011 Accepted: 23 May 2012
Published: 22 August 2012

References

1. Mpitziopoulos A, Gavalas D, Konstantopoulos C, Pantziou G: A survey on jamming attacks and countermeasures in WSNs. IEEE Commun. *Surv Tutor* 2009, 11(4):42–56.
2. Tague P, Li M, Poovendran R: Mitigation of control channel jamming under node capture attacks. IEEE Trans. *Mobile Comput* 2009, 8(9):1221–1234.

3. Xu W, Trappe W, Zhang Y: **Anti-jamming timing channels for wireless networks**. ACM In *Proceedings of the 1st ACM Conference on Wireless Security (WiSec)*. Virginia:; 2008:203–213. ISBN vol.1.
4. Cagalj M, Capkun S, Hubaux J-P: **Wormhole-based anti-jamming techniques in sensor networks.** *IEEE Trans Mobile Comput*. 2007, **6**(1):100–114.
5. Wood AD, Stankovic JA, Son SH: **JAM: A jammed-area mapping service for sensor networks**. IEEE, In *Proceedings of RTSS*. Mexico:; 2003:286–293. ISBN vol.1.
6. Kan BQ, Fan JH, Wang JY, Lu ZY: **Jamming aware routing for MHWN with dynamic measurement.** *Comput Electr* 2012, **38**(3):510–521.
7. McCune JM, Shi E, Perrig A, Reiter MK: **Detection of denial of message attacks on sensor network broadcasts**. IEEE, In *Proceedings of IEEE Symposium on Security and Privacy*. California; 2005:64–78. ISBN vol. 1.
8. Li M, Koutsopoulos I, Poovendran R: **Optimal jamming attacks and network defense policies in wireless sensor networks**. IEEE, In *Proceedings of INFOCOM*. Alaska; 2007:1307–1315. ISBN vol. 1.
9. Johnson DB, Hu Y, Maltz DA: *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks for IPv4, Request For Comments (Proposed Standard) IEEE,*. Carnegie Mellon University, Pennsylvania; 2007. vol. 4728.
10. Park VD, Corson MS: *A highly adaptive distributed routing algorithm for mobile wireless networks*. Japan: in Proceedings of IEEE Infocom; 1997:1405–1413. ISBN vol. 3.
11. Nasipuri A, Castaneda R, Das SR: **Performance of multipath routing for on-demand protocols in mobile ad hoc networks.** *ACM/Kluwer Mobile Netw. Appl. (MONET) J* 2001, **6**(4):339–349.
12. Ye Z, Krishnamurthy SV, Tripathi SKA: **Framework for reliable routing in mobile ad hoc networks.** *in IEEE INFOCOM, San Francisco* 2003, **vol.1:**270–280.
13. Chakeres I, Perkins C: *Dynamic MANET On-demand (DYMO) Routing.Mar. 2009, IETF Draft draft-ietf-manet-dymo-17*; 2009. http://www.ietf.org/internet-drafts/ draft-ietf-manet-dymo-17.txt.
14. Koltsidas G, Pavlidou FN, Kuladinithi K, Timm-Giel A, Goerg C: *C, Investigating the performance of a multipath DYMO protocol for ad-hoc networks*. Athens, Greece: in IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC); 2007:1–5. ISBN vol. 1.
15. Choi JY, Ko Y-B, Kim Y-S: *A dual-path on-demand routing protocol for tactical wireless networks, IEEE, in ICACT'2010*. Korea:; 2010:445–450. ISBN vol. 1.
16. Ju S, Evans JB: *Intelligent multi-path selection based on parameters prediction, in ICC'2008*. China; 2008:529–534. ISBN vol. 1.
17. Zhongbang Y, Junfeng J, Pingyi F: *A neighbor-table-based multipath routing in ad hoc networks, IEEE, in Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual*. Korea; 2003:1739–1743. ISBN vol. 3.
18. Marina MK, Das SR: *On-demand multipath distance vector routing for ad hoc networks, IEEE, in Proceedings of the International Conference for Network Protocols (ICNP)*. Riverside, CA; 2001:14–23. ISBN vol.1.
19. Leung R, Liu J, Poon E, Chan ALC, Li B: **MP-DSR: a QoS-aware multi-path dynamic source routing protocol for wireless ad-hoc networks**. IEEE, In *26th Annual IEEE Conference on Local Computer Networks*. Florida, USA; 2001:132–141. ISBN vol. 1.
20. Jiang S, Xue Y: **Providing survivability against jamming attack for multi-radio multi-channel wireless mesh networks.** *J Netw Comput Appl* 2011, **34:**443–454.
21. Lazos L, Liu S, Krunz M: **Mitigating controlchannel jamming attacks in multi-channel ad hoc networks**. In *ACM WiSec*. Switzerland:; 2009:169–180. ISBN vol. 1.
22. Saleem M, Khayam S, Farooq M: **On performance modeling of ad hoc routing protocols. Springer, EURASIP.** *J. Wireless Commun Network* 2010, **2010:**1–13.
23. Chen X, Jones HM, Jayalath D: **Channel aware routing in MANETs with route handoff.** *IEEE Trans. Mobile Comput* 2011, **10**(1):108–121.
24. Tague P, Nabar S, Ritcey JA, Poovendran R: **Jamming-aware traffic allocation for multiple-path routing using portfolio selection.** *IEEE/ACM Trans. Network* 2011, **19**(1):184–194.
25. Strasser M, Danev B, Capkun S: **Detection of reactive jamming in sensor networks.** *ACM Transactions on Sensor Networks* 2010, **7**(1):Article No. 16.

doi:10.1186/1687-1499-2012-267
Cite this article as: Kan and Fan: **Interference activity aware multi-path routing protocol.** *EURASIP Journal on Wireless Communications and Networking* 2012 **2012**:267.