Thesis for the Degree of
Master of Engineering

Jamming Resilient Routing Scheme in Wireless Networks

by

Seon Yeong Park

Department of Information and Communications Engineering

The Graduate School

Pukyong National University

February 2013

Jamming Resilient Routing Scheme in Wireless Networks
(무선센서네트워크에서 재밍에 회복력 있는 라우팅 기법)

Advisor: Prof. Sung-Un Kim

by
Seon Yeong Park

A thesis submitted in partial fulfillment of the requirements
for the degree of

Master of Engineering

in Department of Information and Communications Engineering,
The Graduate School,
Pukyong National University

February 2013

박선영의 공학석사 학위논문을 인준함.

2013년 2월 22일

주 심 공학박사 박 규 칠 (인)

위 원 공학박사 류 지 열 (인)

위 원 공학박사 김 성 운 (인)

Jamming Resilient Routing Scheme in Wireless Networks

A dissertation

by

Seon Yeong Park

Approved by:

(Chairman) Kyu-Chil Park

(Member) Jee-Youl Ryu

(Member) Sung-Un Kim

February 22, 2013

CONTENTS

LIST OF FIGURES

LIST OF TABLES

무선네트워크에서 재밍에 회복력 있는 라우팅 기법

박 선 영

부경대학교 대학원 정보통신공학과

요 약

무선네트워크의 응용이 군사적 통신, 비즈니스 및 교육 등의 다양한 분야로 확대됨에 따라 무선네트워크에서 통신 신뢰성 보장에 대한 중요성이 부각되고 있다. 이러한 무선네트워크는 공유된 매체를 통해 통신하는 특성으로 인해 재밍 또는 전파 간섭에 매우 취약한 문제점을 지닌다. 재밍은 서비스 거부 공격의 한 종류로, 재머라 불리는 악의적인 공격자가 임의의 또는 의미가 없는 신호를 무선통신 채널로 전송함으로써 무선네트워크에서 통신을 효과적으로 방해하는 공격을 일컫는다.

본 논문에서는 무선네트워크의 통신 신뢰성을 위협하는 재밍에 강력하게 대처하기 위해 새로운 메시지 구조를 제시하고, 또한 이를 활용하여 계산되는 패킷 전달률(PDR: Packet Delivery Ratio)을 기반으로 재밍을 감지하고 PDR 및 경로의 홉 수를 고려하여 최적의 재밍 지역 우회 경로를 선택하는 재밍에 회복력 있는 라우팅(JRR: Jamming Resilient Routing) 기법을 제안한다.

MATLAB을 활용한 시뮬레이션을 통해 제안된 기법과 기존의 재밍 방어 기법들의 성능을 비교하였으며, 그 결과 제안된 JRR 기법이 통신 신뢰성 및 경로의 홉 수 측면에서 기존의 재밍 방어 기법들보다 우수한 성능을 나타냄을 확인하였다.

Ⅰ. Introduction

As wireless networks are receiving attention due to their ever-widening application in military communication, business, education, and even entertainments, it has become an important issue how to ensure their reliability despite local failures and various forms of attacks [1]. Wireless networks provide communication through shared media which are highly vulnerable to jamming attacks or radio interferences [2]. Jamming is a kind of Denial of Service (DoS) attacks [1][3], which can damage the reliability of wireless communication where a malicious adversary called a jammer sends random or meaningless signals in large quantities to the shared channels [3][4]. Jamming causes data transmission failures by disrupting communication among nodes [5][6]. In addition each node quickly wastes valuable power in futile attempts to re-send messages repeatedly in order to communicate or recover the failed paths [4]. Jammers can be divided into five types [1][4][7]:

- Constant jammers who keep sending random or meaningless signals to the channel disregarding the MAC protocols.
- Deceptive jammers who continually inject valid packets with valid packet headers but with useless or even empty payloads to the channel without a gap between packets.

- Random jammers alternate between jamming and sleep modes. Their actual jamming attacks often involve constant or deceptive jammings which are active for a while and turn silent for another while before an unwelcome wakeup for another round.
- Reactive jammers who stay quiet till the occurrence of an activity on the channel and then interrupt the reception of the packet. This type of jammers spends more power on sensing the channels to corrupt than the jamming per se.
- Mobile jammers are simply those who are mobile. They often sneak into critical paths according to the information they got by eavesdropping on the traffic and mount constant or deceptive jammer attacks.

There are two distinct measures against jamming attacks, detection and defense. According to the literature on jamming detection methods, they commonly utilize such measurements as the average Signal Strength (SS), the Carrier Sensing Time (CST), the Packet Delivery Ratio (PDR), and the Signal Strength Consistency (SSC) [2][4][8]. Of them the PDR is a tool of our choice which is closely related to the reliability of the path in a wireless network. On the other hand the existing solutions for defending against jamming attacks come in two modes [1][5][6]; one is the active mode in which we reroute data via an alternative path once a jammed region is located. The other one is the passive mode that helps save power by working only when an attack is present [1].

There are a number of defence schemes against jamming attacks in both active and passive methods. They avoid jamming attacks by establishing specific topologies in the network formation process [1] or simply by taking a detour around a jammed area [6]. Frequently, however, their transmission paths are unduly long [1][6] and the maximum packet delivery ratio is not guaranteed despite costly detours [5][6]. Accordingly, we need a solution to those problems in order to provide higher efficiency and reliability for the communication even when an invader attempts at jamming in the wireless network.

In this paper, we present a new approach that detects jamming conditions based on the PDR and the number of hops at the time of path selection so as to defend the network reliably from various jamming attacks. In the proposed JRR scheme, nodes exchange new messages among them periodically, and then each node detects jamming attacks depending on the PDR computed based on the statistics about those new messages and the mathematical characterization of jamming situations. Once jammed regions are detected, nodes adopt alternative transmission paths which have small hops and the grate delivery ratio so as to recover data transmission failures. Therefore, not only can this proposed scheme solve the problem of existing methods that detour paths are long, but also it enhances the packet deliver ratio of the transmission paths.

The rest of the paper is organized as follows. In Section II we take brief reviews of the efforts concerned with jamming detection and defense. In Section

III we propose a Jamming Resilient Routing (JRR) scheme under jamming attacks in detail. Then Section IV presents our simulation model and a set of test results. Finally Section V concludes this paper.

Ⅱ. Related Works

The majority of research efforts to date on jamming in the wireless network have been around detection of jamming and effective defense against it. Brief reviews of previous efforts are given here.

1. Detecting Jamming Attacks

According to the literature on jamming detection, a number of methods are distinguished depending on the measurement features employed, namely, the Signal Strength (SS), the Carrier Sensing Time (CST), the Packet Delivery Ratio (PDR), and the Signal Strength Consistency (SSC) [3][4][8]. The SS and the CST methods can detect constant and deceptive jammers but not random and reactive jammers [4]. The PDR method utilizes the packets delivery ratio which can drop sharply under a jamming attack [4][8][9]. There is also a hybrid approach which complements the PDR with an additional measurement of the SSC [4].

Table 1. Measurement for detecting jamming attacks

Measurement	Type of detectable jammers
SS	Constant and Deceptive
CST	Constant and Deceptive
PDR	Constant, Deceptive, Random, and Reactive
PDR and SSC (Hybrid approach)	Constant, Deceptive, Random, and Reactive

2. Defending Jamming Attacks

Once detected, jamming attacks can be resolved in several ways. Most conveniently, existing methods can be divided into two types, active and passive methods. Active methods can be described as being network layer-based in that they reroute packets along alternative transmission paths once jammed regions are detected. This type of methods includes the multi-dataflow topologies defense [1], the Proactive Protection (PP), the Reactive Protection (RP) [5], the Failure-Based Learning (FBL), and the Detour by Anchor Point (DAP) schemes [6].

The multi-dataflow topologies defense scheme is designed in order to cope with mobile jamming attacks [1]. In this scheme multi-dataflow topologies are set up in the network formation process. When a jamming attack is detected in one of multi-dataflow topologies, we can recover the lost part of the wireless network using one of the alternative topologies. One shortcoming, however, is that each node belongs to only one dataflow topology and thus can communicate only with the nodes belonging to the same topology.

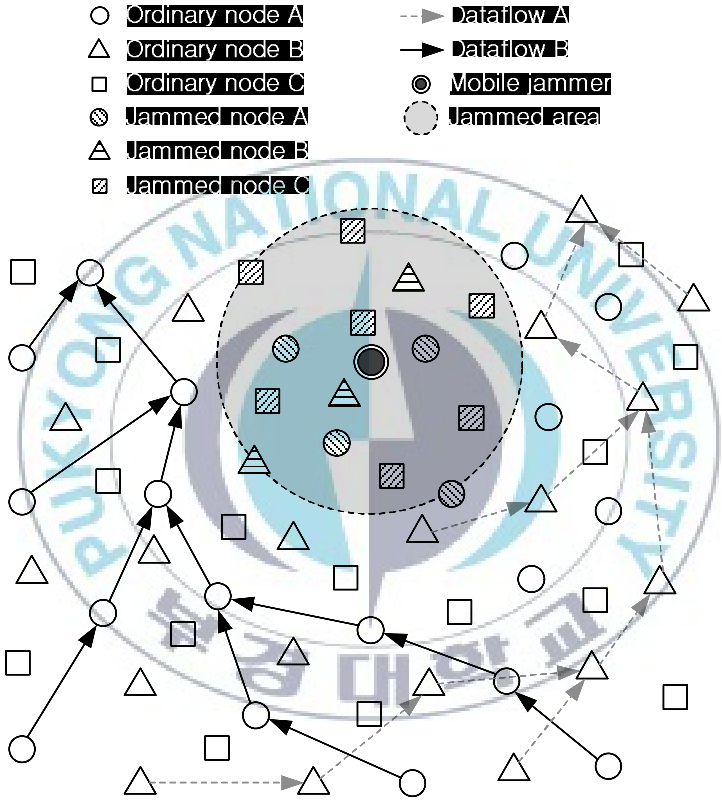


Figure 1. Multi-dataflow topologies defense scheme jammers

The PP is another scheme that applies the multipath routing and power control to prevent network disruptions caused by jamming attacks in the network [5]. In this scheme several cases of jamming were shown mitigated through an appropriate power control, but it is difficult to find the optimal power assignments and thus the performance tends downwards due to extended search time for multipath routing.

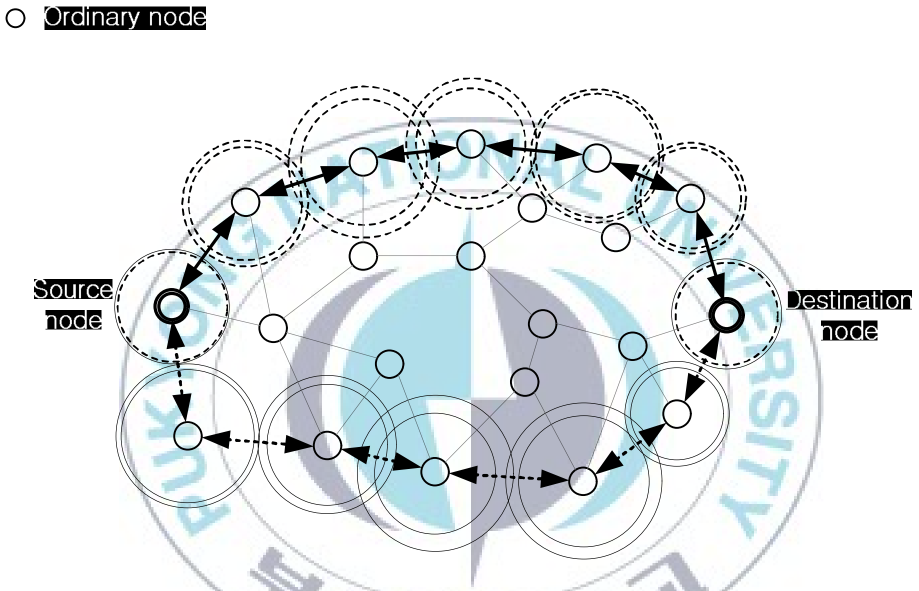


Figure 2. Multipath routing and power control of the proactive protection scheme

Unlike the PP scheme, the RP [5] and the FBL [6] schemes find new paths to send data to avoid the jammed region only when a transmission failure occurs. In these two schemes, the path selection methods are the same except that the FBL scheme sends data to a group of destination nodes rather than to a single destination node as in the PR scheme. One drawback of these schemes is the increased load to determine the detour which avoids the region affected by jamming attacks. Besides, they cannot ensure the highest reliability of the selected paths.

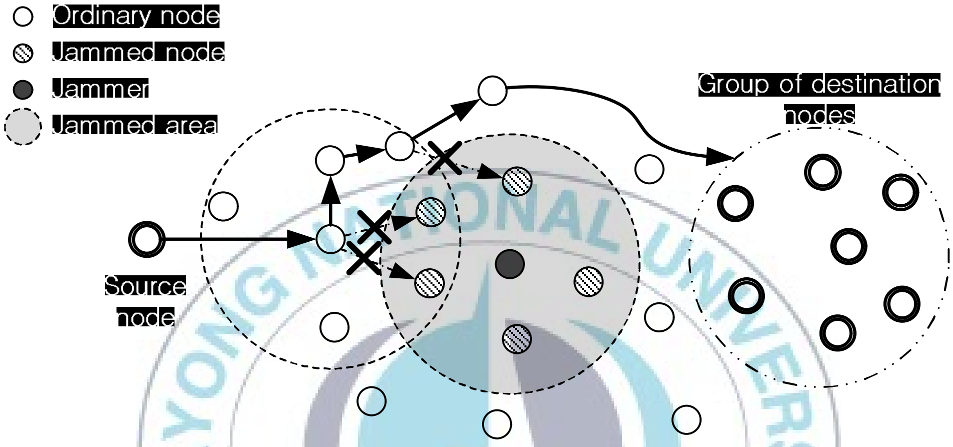


Figure 3. Failure-based learning scheme

The DAP is still another scheme that solves the jamming problem by transmitting data through a detour via an anchor point far away from the jammers [6]. It is useful when network nodes are aware of jammed areas. The price, however, is that the resulting paths become significantly longer than the original paths.

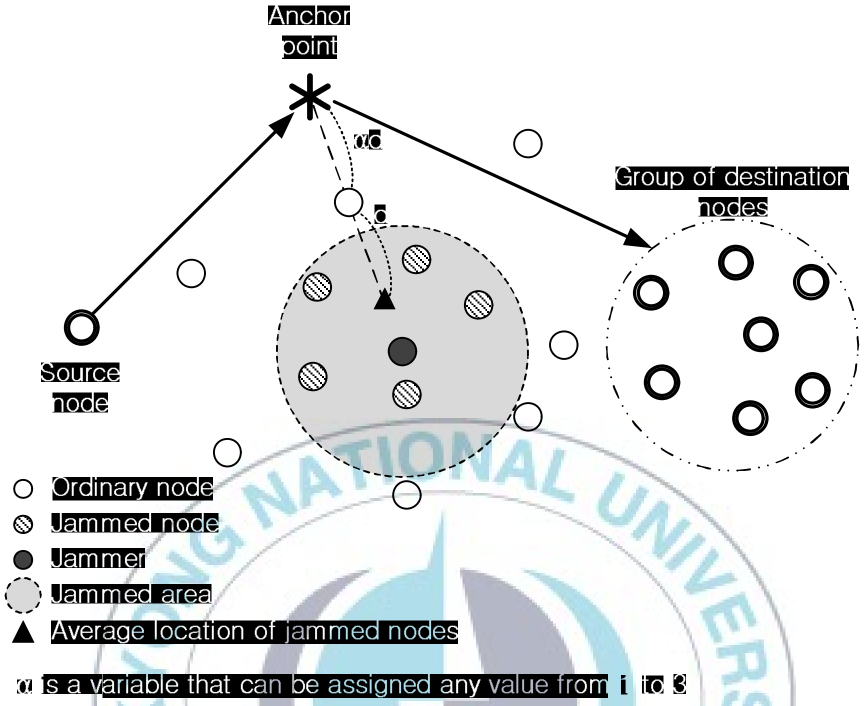

Anchor point
αd
d
Group of destination nodes
Source node
○ Ordinary node
▨ Jammed node
● Jammer
Jammed area
▲ Average location of jammed nodes
α is a variable that can be assigned any value from 1 to 3

Figure 4. Detour by anchor point scheme

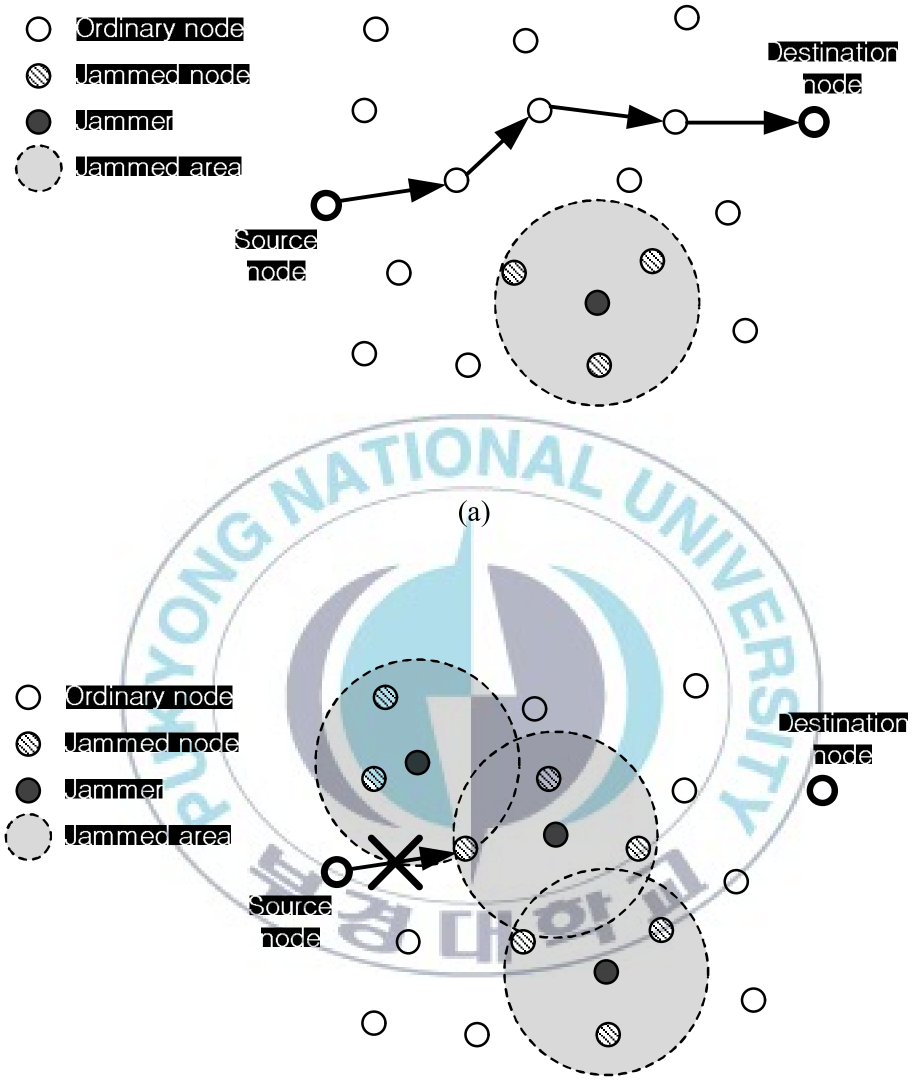
Active schemes discussed thus far tend to waste precious power. In contrast passive methods save energy by modifying the MAC layer protocol or reducing the packet transmission frequency [1][10][11]. Improving the MAC layer protocol helps decrease the chance of a jammer launching an attack. In addition reducing the packet transmission frequency can lead to reduced damage when jamming attacks come to pass [1].

Ⅲ. Jamming Resilient Routing

In this section we define a jamming model based on the PDR and then describe the proposed JRR scheme that returns an optimal path founded on the number of hops to the destination node as well as the PDR.

1. Jamming Model

A formal analysis of jamming incidents requires a mathematical characterization of jamming situations. Here we assume that non-mobile nodes are distributed uniformly in the wireless network and constant, deceptive, random or mobile jammers are scattered randomly as shown in Figure 5. In Figure 5(a) a number of nodes around the jammer are jammed or affected as they cannot communicate successfully with any other nodes. In the case of Figure 5(b) the jammed region cuts across the entire network because of simultaneous jamming attacks by several jammers between the source node and the destination node. In other words, there is no communicating between the source node and the destination node. This kind of cases, though possible, is deemed rare and will not be considered in this paper.



(a)

(b)

Figure 5. Two jamming situations (a) a localized jamming by a single isolated jammer, (b) a extensive regional jamming by multiple simultaneous jammers

If a jammer launches an attack on a wireless network, it typically affects a number of nodes around the jammer within a range of some radius, called the jamming range. The radius is determined by the Signal Strength (SS) of the jammer subject to attenuation with the distance. Due to power dissipation, the SS of a node at a distance d from the jammer drops exponentially in proportion to d as follows [12]

$$\frac{P(d)}{P(0)}=\mathrm{e}^{-2\alpha d} \tag{1}$$

where $P(0)$ is the SS at the jammer and α is the attenuation coefficient which is positive real [12].

The Packet Delivery Ratio (PDR) of a node is the ratio of the number of successfully received packets to that of total packets which the node sent. The PDR is also presumed to be a function of d. When there are no interruptive factors between nodes, the PDR would be 1 representing 100% delivery. In addition the node's power dissipates in proportion to the communication failure rate. Therefore the PDR of a node at distance d m from the jammer can be described as the difference between the ideal PDR and the communication failure rate due to the jamming attack. From Equation (1) we can derive the following relation.

$$PDR(d)=1-\mathrm{e}^{-2\alpha d} \tag{2}$$

This tells us that the PDR of a node recovers gradually beyond the jammed area immediately surrounding jammers.

2. Jamming Resilient Routing Scheme

Once the measurement model of jamming is defined, we can proceed to the details of the proposed scheme which is resilient to a variety of jamming attacks. The proposed scheme works into primary two phases, the routing table update (Phase I) and actual routing (Phase II). Figure 6 shows the flowchart of the JRR algorithm.

In the routing update phase, we renew the routing table about neighborhood nodes and their PDRs. In the message routing phase, any relevant data is sent along the optimal path that has been found based on the PDRs and the number of hops to the destination node considering the routing table. We deal with Phase I and Phase II in detail in Section 2.1 and Section 2.2, respectively. The following steps summarize the overall proposed algorithm:

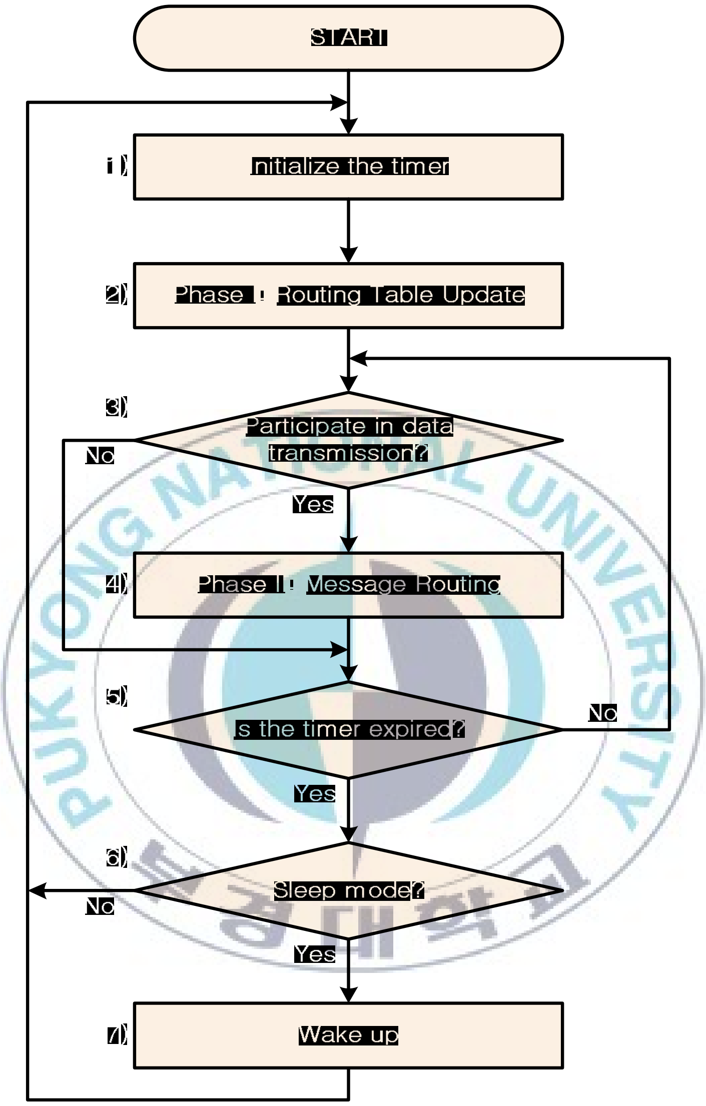


Figure 6. Flowchart of the JRR algorithm

1) Initialize the timer of the node.

2) Apply the routing table update (Phase I).

3) If the node participates in data transmission, go to Step 4), otherwise go to Step 5).

4) Apply the message routing (Phase II).

5) Check if the timer is expired. If not, go to Step 3), otherwise go to Step 6).

6) Check if the current node is sleep mode. If not, go to Step 1), otherwise go to Step 7).

7) Wake up and then go to Step 1).

Both phases, Step 2) and Step 4) in Figure 6, rely on two kinds of messages `Hello_req` and `Hello_rep` for traffic statistics in order to determine the PDRs and apply them to actual routing. Figure 7 shows the two message structure and Table 2 explains their fields.

If the field `dst` in both message types is zero, this means that the message has no particular destination node for data transmission. In this case the two fields, `trav_list` and `path`, are not used, meaning that the current node is operating in Phase I of the routing table update. Otherwise the node will be working in routing phase.

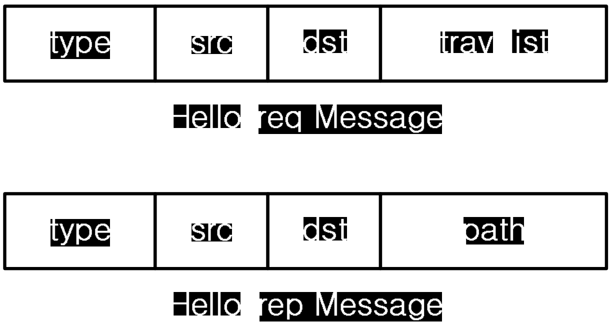


Figure 7. `Hello_req` and `Hello_rep` message formats

Table 2. Fields of `Hello_req` and `Hello_rep` messages

Field	Description
type	Message type. `Hello_req` or `Hello_rep`.
src	Source node identifier
dst	Destination node identifier
trav_list	List of identifiers of nodes thus far traversed
path	List of identifiers of nodes on the `src` to `dst` path

In the routing table update phase, each node computes the PDR of the neighborhood nodes based on the numbers of `Hello_req` messages sent out and `Hello_rep` messages received. They use these PDRs to judge for themselves whether they are jammed or not. The PDR is estimated by the ratio

$$PDR=\frac{N_{\text{Hello\_rep}}}{N_{\text{Hello\_req}}} \tag{3}$$

where $N_{\text{Hello\_req}}$ is the number of `Hello_req` massages transmitted to the neighbor node, and $N_{\text{Hello\_rep}}$ is that of `Hello_rep` received by the node.

2.1. Phase I: Routing Table Update

Successful packet routing requires information about the current network status. We evaluate it via the PDR using two kinds of 'roll call' messages, namely `Hello_req` and `Hello_rep`. In this phase each node sends out `Hello_req` messages with the `dst` field set to zero to its neighbor nodes and then waits for responses `Hello_rep` from them. The statistics about these messages are then used to update the routing table according to Equation (3). The PDR will drop sharply when jamming attacks are launched by constant, deceptive, random or mobile jammers. Therefore a simple rule is to decide on the jamming by comparing the PDR to a certain threshold as

$$PDR_{\text{avg}} < \theta \tag{4}$$

where PDR_{avg} is the average PDR computed at a node and θ is a threshold for judging about jamming.

The threshold, though critical, can only be determined empirically. According to Wang et al. [4], a threshold of 0.1677 or 16.77% was used for deciding constant, deceptive, random or reactive jamming attacks. Since a mobile jammer is also a type of constant or deceptive jammers and its PDR values are usually below the threshold, we can safely apply it to most PDR values in areas affected by any jammers, mobile or not, but, in this paper, with a slight increase to 20% for a greater reliability.

Once a node has found itself jammed, it goes into a sleep mode in order to avoid unnecessary consumption of power until the term of the last `Hello_req` expires. The sleep node cannot participate in data transmission and thus is removed from routing tables in the neighbor nodes. On the other hand, normal nodes which are not found to be jammed proceed to update their routing tables periodically and, of course, participate in data transmission in the network. Figure 8 illustrates the flowchart of the routing table update phase.

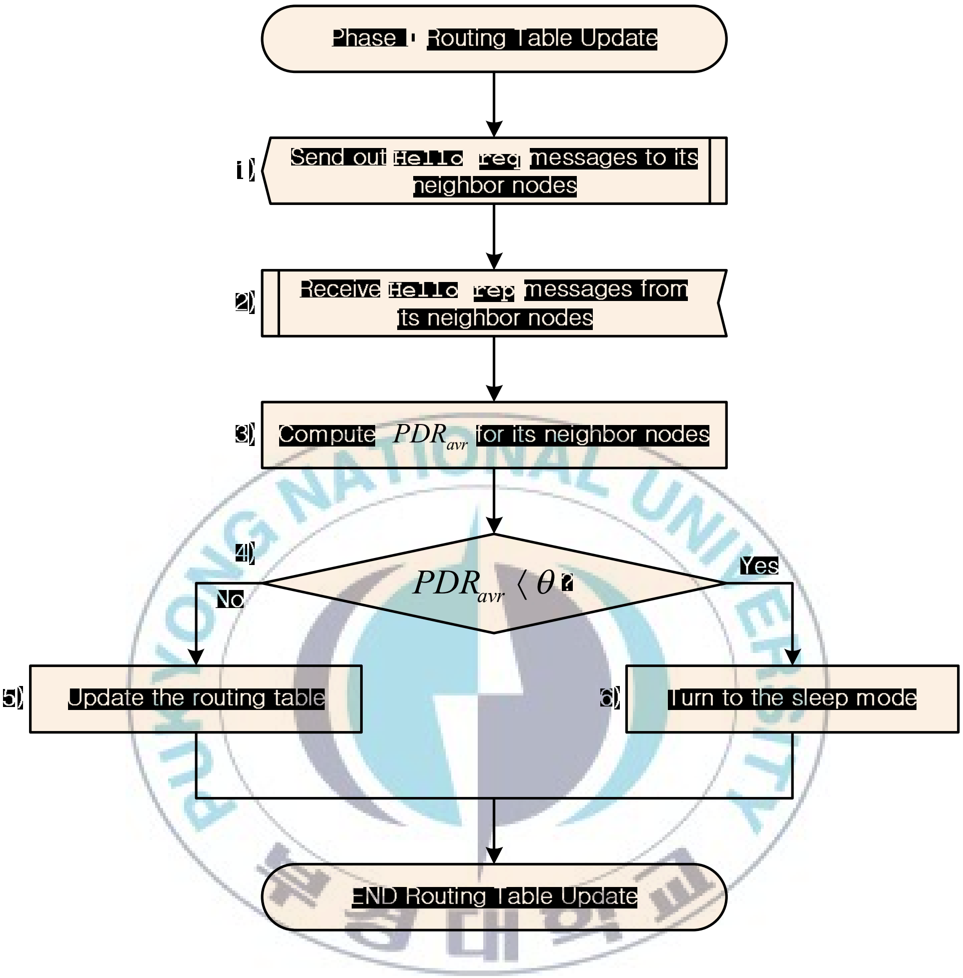

Phase I: Routing Table Update
1) Send out Hello_req messages to its neighbor nodes
2) Receive Hello_rep messages from its neighbor nodes
3) Compute PDR_{avr} for its neighbor nodes
4) $PDR_{avr} \langle \theta$?
Yes
No
5) Update the routing table
6) Turn to the sleep mode
END Routing Table Update

Figure 8. Flowchart of the routing table update phase

The routing table update phase works as follows.

1) Send out `Hello_req` messages with the `dst` field set to zero to its neighbor nodes.

2) Receive `Hello_rep` messages from its neighbor nodes.

3) Compute PDR_{avg} for all its neighbor nodes using (3).

4) Judge if it is jammed for itself using (4). If not, go to step 5), otherwise go to step 6).

5) Update the routing table for its neighbor nodes and their PDR_{avg} values.

6) Turn to the sleep mode.

2.2. Phase II: Message Routing

In the routing phase, a source node prepares `Hello_req` messages with the `dst` field set to the destination node identifier. Then these messages are sent out to its neighbor nodes. Those nodes receiving the `Hello_req` message append their own identifier in the `trav_list`, and then transmit it to another node on the way toward the destination. This process repeats until the message reaches the destination node. In response the destination node creates `Hello_rep` messages where the field path is initialized to the value of `trav_list` of the `Hello_req` massage just received, and sends it back to the previous node in the same list. All the nodes in the list will return it in the reverse order of the list. Ultimately the `Hello_rep` will reach the source.

The source node may often end up with several candidate paths $\mathrm{Q} = \{1, 2, \ldots\}$ from one or more `Hello_rep` messages returned. It will select the best path with the minimum scores as defined by

$$\min_{i \in Q} \frac{H_i}{\sum_{j=1}^{H_i} PDR_{ij}} \tag{5}$$

where H_i is the number of hops for the i-th path and PDR_{ij} is the packet delivery ratio at the link j of the i-th path. Therefore the resulting path is that of a combined measurement of the smallest hops and the greatest delivery ratio. If paths satisfying the equation (5) are more than one, the path which has the minimum number of hops will be determined among them. Figure 9 shows the flowchart of the message routing phase of the JRR.

The message routing phase is composed of the following steps.

1) The source node transmits `Hello_req` messages to its neighbor nodes.
2) Each neighbor nodes of the source node receives the `Hello_req` message.
3) That node receiving the `Hello_req` message appends its own identifier in the `trav_list` field of the `Hello_req` message.
4) Check if the current node is the destination node. If not, go to step 5), otherwise go to step 6).
5) The node transmits `Hello_req` messages to its neighbor nodes, and then goes to step 2).
6) The destination node generates `Hello_rep` messages where the `path` field is initialized to the value of `trav_list` of the `Hello_req` massage just received.
7) The node sends the `Hello_rep` message back to the previous node.

8) The previous node receives the `Hello_rep` message.

9) Check if the current node is the source node. If not, go to step 7), otherwise go to step 10).

10) Determine one or more paths using (5).

11) If selected paths are more than one, go to step 12), otherwise go to step 13).

12) Determine only one path which has the minimum number of hops among selected paths.

13) The source node transmits the data along the selected path.

14) The destination node receives the data along the selected path.

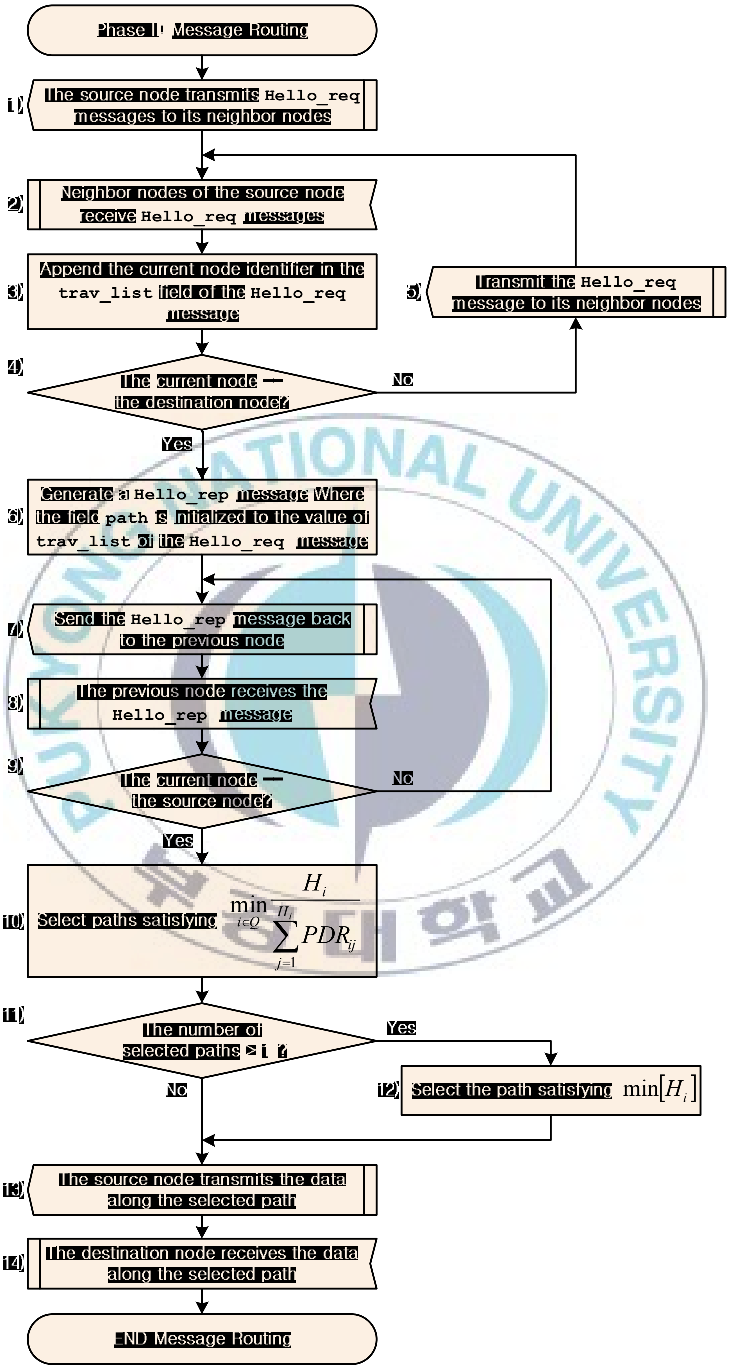

Phase II: Message Routing
1)
The source node transmits Hello_req messages to its neighbor nodes
2)
Neighbor nodes of the source node receive Hello_req messages
3)
Append the current node identifier in the trav_list field of the Hello_req message
4)
The current node = the destination node?
No
5)
Transmit the Hello_req message to its neighbor nodes
Yes
6)
Generate a Hello_rep message Where the field path is initialized to the value of trav_list of the Hello_req message
7)
Send the Hello_rep message back to the previous node
8)
The previous node receives the Hello_rep message
9)
The current node = the source node?
No
Yes
10)
Select paths satisfying $\min_{i \in Q} \frac{H_i}{\sum_{j=1}^{H_i} PDR_{ij}}$
11)
The number of selected paths > 1 ?
Yes
No
12)
Select the path satisfying $\min[H_i]$
13)
The source node transmits the data along the selected path
14)
The destination node receives the data along the selected path
END Message Routing

Figure 9. Flowchart of the message routing phase

Ⅳ. Performance Evaluation

1. Simulation Environment

A rigorous evaluation of the performance of the proposed routing scheme in a wireless network requires a field test in real environments, which is not easy for practical reasons. Instead we will create a simulation environment which lends itself to easy control of test parameters. The simulation model is designed as a field of 2000m×2000m area that is comparable to the work of Yoon et al. [6] as shown in Figure 10. Here up to 400 nodes are deployed randomly, about one per 100 m^{2}. The wireless transmission range of a normal node is 200m. For jammers, however, the range is much greater, increasing to 500m. Jammers are assumed to occur randomly across the network, too.

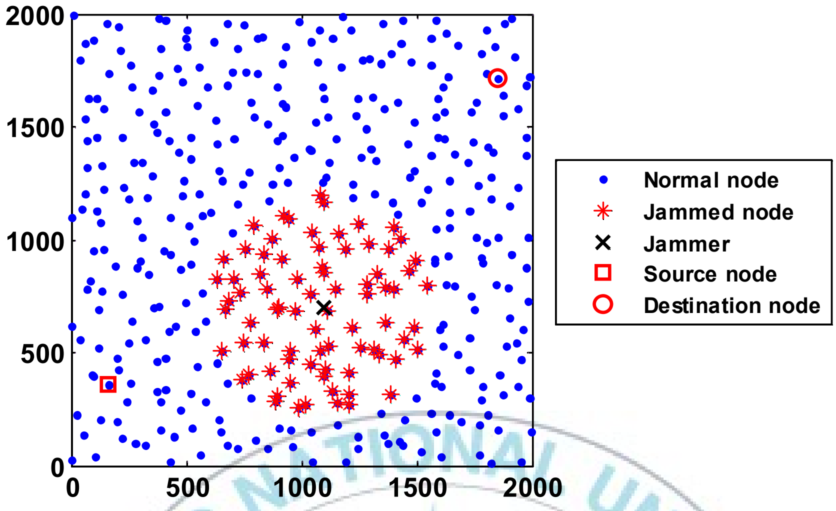


Figure 10. Deploying nodes and the jammer in the wireless network environment

Figure 11 shows the curve of the PDR as a function of the distance from a jammer as described by Equation (2). The attenuation coefficient α is set to $-ln0.8/1000 \approx 2.23 \times 10^{-4}$ corresponding to the condition that the jamming range is 500m and the PDR of jammed nodes are below 20%.

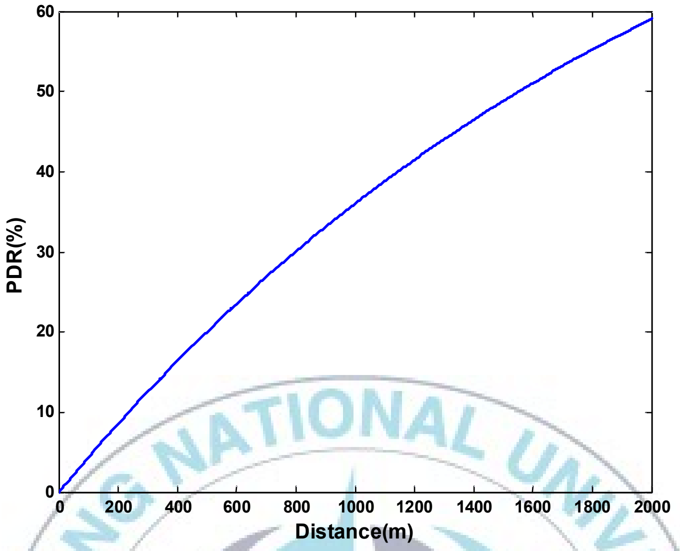


Figure 11. The relation between the distance from the jammer and PDR in the simulation environment

In the routing phase, we choose two normal nodes randomly for the source and the destination with a jammed region in-between as shown in Figure 10.

2. Simulation Results

The goal of the proposed Jamming Resilient Routing (JRR) scheme is to ensure reliable data transmission over paths which are efficient in the number of hops. The simulation environment so designed in the above allows the JRR to work in an active mode to defend against constant, deceptive, random and mobile jammers. As reviewed in Section II, the active mode includes RP, FBL and DAP schemes. Of these methods, the path selection methods of FBL and RP schemes are virtually equivalents leading us to conclude that it is sufficient to test only the RP scheme in our experiment.

In the first set of experiments, we compute the PDR and measure the number of hops when the network is under the attack by a constant, deceptive, random or mobile jammer. The results are compared with those of DAP and RP schemes in Figure 12. We carried out the simulation 100 times each with a different mobile jammer, and took their averages.

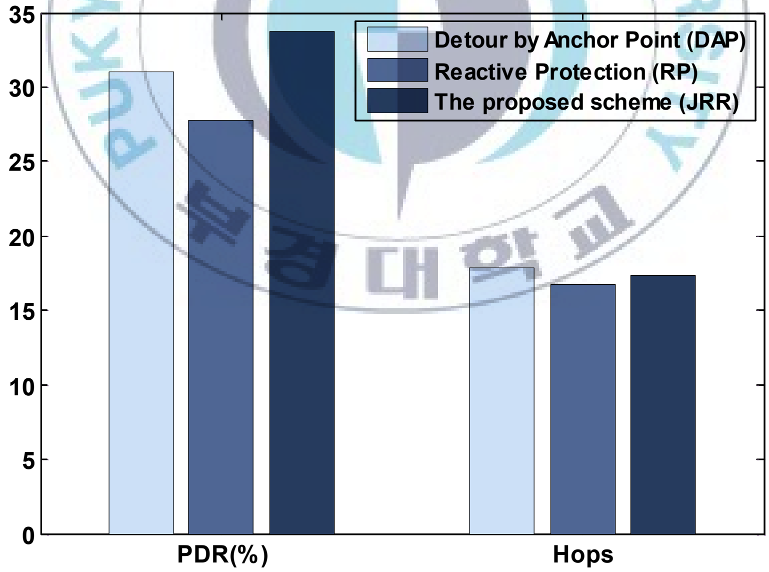


Figure 12. The PDRs and the number of hops of three schemes attacked by mobile jammers

Table 3. The complete PDRs for three schemes attacked by mobile jammers (DAP: Detour by Anchor Point, RP: Reactive Protection, JRR: proposed scheme)

Field	PDR average (%)	PDR standard deviation (%)	PDR improvement rate by JRR (%)
DAP	31.01	1.31	8.92
RP	27.75	1.08	21.72
JRR	33.78	1.18	-

Table 4. The numbers of hops for three schemes attacked by mobile jammers (DAP: Detour by Anchor Point, RP: Reactive Protection, JRR: proposed scheme)

Field	Hops average	Hops standard deviation	Hops improvement rate by JRR (%)
DAP	17.82	1.42	-2.86
RP	16.77	0.42	3.22
JRR	17.31	1.32	-

Figure 12 tells us that there are 8.92% and 21.72% performance improvements by the proposed scheme over the DAP and the RP respectively. In addition we can read that the number of hops of JRR is about 2.86% greater than RP but 3.22% less than that of the DAP.

In the RP scheme, the average number of hops is the smallest but its average PDR is significantly below ours, which can be explained by its choice of nodes with a PDR sometimes barely greater than 20%. In fact many nodes do have a low PDR approaching the threshold as has been observed in our experiment.

On the other hand the DAP scheme takes the most hops primarily due to the choice of the anchor point away from the jammer. Despite this, the DAP does not achieve the highest average PDR. This is partly due to the fact the paths from and to the anchor points are not free from the influence of nearby jammers. Specifically, The DAP scheme selects intermediate nodes of the path which satisfy the only one condition that the distance from the source node to the anchor point and that from the anchor point to the destination node should be the shortest. In other words the PDR and the distance from the jammer of each immediate node in the path are not guaranteed in this method, and these PDRs have an effect on the average PDR of the selected path. Accordingly, the DAP is unable to assure the highest average PDR of the path though it detours far away from the jammer.

By comparison, the proposed JRR scheme takes slightly more hops than one of the previous two methods under attack by a mobile jammer but records the highest PDR implying the greatest reliability for wireless networks.

In the second set of tests, we compared the PDRs averaged over complete paths from sources to destinations during attacks by constant, deceptive or random jammers.

As noted in Section II the distinction between constant and deceptive jammers is made by the nature of packets or payloads; constant jammers send simply meaningless signals while deceptive jammers send valid packets but with useless payloads. Simulation results show that they are indistinguishable from each other by PDRs.

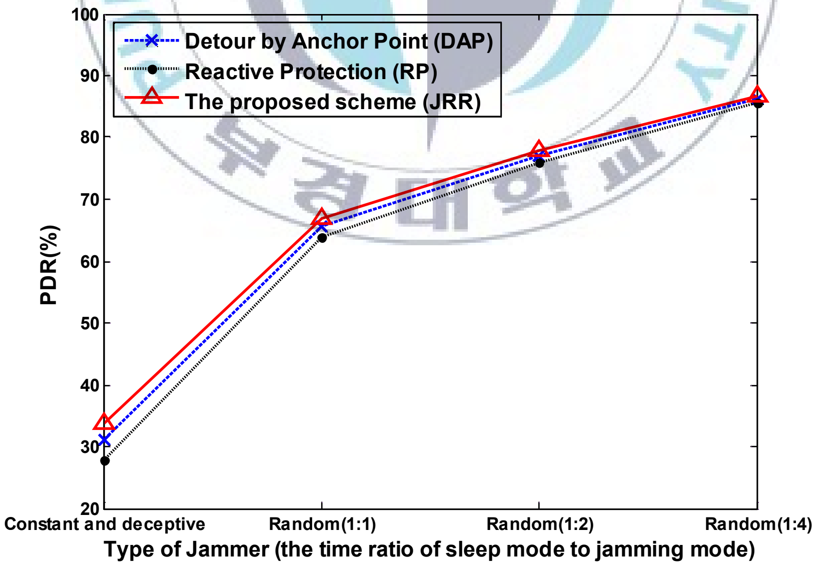


Figure 13. Comparisons of the PDRs under jamming attacks by constant, deceptive and random jammers

Table 5. The PDRs of the three schemes in attacks by constant, deceptive and random jammers. (DAP: Detour by Anchor Point, RP: Reactive Protection, JRR: proposed scheme)

Type of jammer	Field	PDR average (%)	PDR standard deviation (%)	PDR improvement rate by JRR (%)
Constant and deceptive jammer	DAP	31.01	1.31	8.92
	RP	27.75	1.08	21.72
	JRR	33.78	1.18	-
Random jammer (1:1)	DAP	65.51	0.65	2.11
	RP	63.88	0.54	4.72
	JRR	66.89	0.59	-
Random jammer (1:2)	DAP	77.00	0.44	1.20
	RP	75.92	0.36	2.65
	JRR	77.93	0.39	-
Random jammer (1:4)	DAP	86.20	0.26	0.64
	RP	85.55	0.22	1.41
	JRR	86.76	0.24	-

At the leftmost end of the chart in Figure 12 the average PDR of the JRR is measured at 33.78% which is an improvement of 8.92% and 21.72% from those of the DAP and the RP respectively. When intermittent sleeps of increasing the duration in the attacks of random jammers are introduced, we can observe an increasing trend of PDRs though with diminishing slopes as sleep increases.

The RP scheme returns routing paths using packets with additional fields containing the location information of nodes in order to establish the transmission path [5]. However the proposed method utilizes messages with fewer additional fields than those of the RP scheme. This implies that the JRR is more efficient because the energy consumption for transmission of the extra fields so as to transfer actual data, payloads in the packet, is lower [5]. In addition the JRR scheme requires a simple procedure involving Equations (3) and (5). In Yoon et al's work [6] with the DAP scheme, the message formats are not explained completely. This DAP is based on the premise that all relevant nodes know the location of the source and the destination nodes [6]. Therefore the DAP scheme needs the location and the angle information of nodes to set up a path with an anchor point, and computational procedure of it is also complicated [6]. As a result, despite computation is simple and an additional field size for transmission of actual data is reduced, the proposed JRR scheme shows a consistent advantage over other schemes.

Through two sets of experiments and analyses, we could confirm that the proposed scheme of JRR did present a superior performance in terms of the reliability of the path to the other schemes when a constant, deceptive, random or mobile jammer launches a jamming attack. It is more obvious when an attack is in progress as shown in the second set of experiments.

Ⅴ. Conclusion

Wireless networks are vulnerable to jamming or radio interference by malicious adversaries due to its characteristics of providing communication channels through a shared medium. Solutions to this problem require a robust – reliable and effective – detection and protective methods against jamming attacks of various kinds.

This paper has presented a new routing scheme that utilizes the PDR which is associated with path reliability in the detection of jamming attacks. The proposed scheme selects an optimal path based on the PDR as well as the number of hops along the path from the source node to the destination node.

In the simulation study, we measured the performance of the proposed JRR scheme and compared it with those of other methods. Consistently the proposed scheme achieved a superior performance in terms of the packet delivery ratio and shown to be competent in the number of path hops. These were particularly apparent when there was an active attack in progress.

Consequently we believe that the proposed scheme can be applied in practice to making more effective and reliable the wireless networks under frequent jamming attacks. It could be much more valuable when it comes to providing highly security-aware services in today's jam-prone wireless networks.

References

[1] Hung-Min Sun, Shih-Pu Hsu, and Chien-Ming Chen, “Mobile Jamming Attack and its Countermeasure in Wireless Sensor Networks,” Advanced Information Networking and Applications Workshops (AINAW'07), pp. 457-462, 21-23 May 2007.

[2] Hongbo Liu, Wenyuan X,Yingying Chen, and Zhenhua Liu, “Localizing Jammers in Wireless Networks,” Pervasive Computing and Communications, 2009. PerCom 2009, pp. 1-6, 9-13 Mar. 2009.

[3] Abderrahim Benslimane, Abdelouahid El Yakoubi, and Mohammed Bouhorma, “Analysis of Jamming effects on IEEE 802.11 Wireless Networks,” 2011 IEEE International Conference on Communications (ICC), pp. 1-5 , 5-9 June 2011.

[4] Le Wang and Alexander M. Wyglinski, “A Combined Approach for Distinguishing Different Types of Jamming Attacks Against Wireless Networks,” Communications, Computers and Signal Processing (PacRim), pp. 809-814 , 23-26 Aug. 2011.

[5] U. Patel, T. Biswas, and R. Dutta, “A Routing Approach to Jamming Mitigation in Wireless Multihop Networks,” Local & Metropolitan Area Networks (LANMAN), pp. 1-6, 13-14 Oct. 2011.

[6] Sun-Joong Yoon and Young-Bae Ko, “JRGP: Jamming Resilient Geocasting Protocol for Mobile Tactical Ad Hoc Networks,” Information and

Communication Technology Convergence (ICTC), pp. 437-442, 17-19 Nov. 2010.

[7] Liu Zhiping and Li Hui, “Mobile Jamming Attack in Clustering Wireless Sensor Network,” Computer Application and System Modeling (ICCASM), Vol. 9, pp. 5-8, 22-24 Oct. 2010.

[8] Ming Yu, Wei Su, J. Kosinski, and Mengchu Zhou, “A New Approach to Detect Radio Jamming Attacks in Wireless Networks,” Networking, Sensing and Control (ICNSC), pp. 721-726 , 10-12 April 2010.

[9] Ming Yu, Wei Su, J. Kosinski, and Mengchu Zhou, “Short Paper: Jamming-Resilient Multipath Routing Leveraging Availability-Based Correlation,” Proceedings of the Fourth ACM Conference on Wireless Network Security, WISEC 2011, pp. 41-46, 15-17 June 2011.

[10] Y. W. Law, P. Hartel, J. D. Hartog, and P. Havinga, “Link-layer jamming attacks on S-MAC”, Technical Paper, Univ. of Twente, NL, 2005.

[11] M. Brownfield, Y. Gupta, and N. Davis, “Wireless sensor network denial of sleep attack”, Proc. IEEE Workshop on Systems Man and Cybernetics, June 2005, pp. 356–364.

[12] Harald T. Friis, “A Note on a Simple Transmission Formula,” Proc. IRE, pp. 254-256, May 1946.

Acknowledgments

I appreciate a steady attention and precious advice of Prof. Sung-Un Kim for the completion of this dissertation with all my heart. Furthermore, I am very thankful to Prof. Gyu-Chil Park and Prof. Jee-Youl Ryu for examining this dissertation along with much good advice. I would also like to express a word of thanks to Prof. Moon-Gab Joo and Prof. Bong-Kee Sin who led me to develop. Finally, I acknowledge several professors in Dept. of Telematics Engineering, Pukyong National University for considerable instructions and encouragement until now.

Meanwhile, I thank my big seniors in the protocol-engineering laboratory, who gave much advice and help to me. I would like to acknowledge seniors: Chan-Hyo Jo and Hyun-Soo Cheon who were already graduated, and especially, Ki-Hyun Sun, Kyung-Ho Kang, Yu-Ri Lee, and Tae-Ho Shin who help to me in every respect. I thank, too.

Above all, I would like to acknowledge my parents, sister, and brother who have devoted themselves to support me even despite many difficulties, as well as my friends: Yoon-Seong Kim, Bae-Geun Song, Hyun-Jeong Kim, So-Rim Choi, Su-Jeong Kim, Da-Seul Lee, and Dong-Su Kim. I am also thankful to other acquaintances as missed on this paper.