

# An Experimental Study of the Performance Impact of Path-Based DoS Attacks in Wireless Mesh Networks

Avesh K. Agarwal · Wenye Wang

© Springer Science + Business Media, LLC 2009

**Abstract** Wireless mesh networks (WMNs) are considered as cost effective, easily deployable and capable of extending Internet connectivity. However, one of the major challenges in deploying reliable WMNs is preventing their nodes from malicious attacks, which is of particular concern as attacks can severely degrade network performance. When a DoS attack is targeted over an entire communication path, it is called a path-based DoS attack. We study the performance impact of path-based DoS attacks by considering attack intensity, medium errors, physical diversity, collusion and hop count. We setup a wireless mesh testbed and configure a set of experiments to gather realistic measurements, and assess the effects of different factors. We find that medium errors have significant impact on the performance of WMNs when a path-based DoS attack is carried out, and the impact is exacerbated by the MAC layer retransmissions. We show that due to physical diversity, a far attacker can lead to an increased performance degradation than a close-by attacker. Additionally, we demonstrate that the joint impact of two colluding attackers is not as severe as the joint result of

individual attacks. We also discuss a strategy to counter path-based DoS attacks which can potentially alleviate the impact of the attack significantly.

**Keywords** performance evaluation · wireless mesh · denial of service · implementation

## 1 Introduction

Wireless mesh networks (WMNs) have emerged as a viable option for offering ubiquitous Internet access to the users in the context of home, enterprise, and community networks [3]. Multi-hop communications in WMNs are also promising for extending their coverage to remote areas. However, the multi-hop communication nature of WMNs is prone to a wide variety of attacks, either passive (such as eavesdropping or traffic analysis) or active (such as message modification, replay or denial of service (DoS)). Specifically, DoS attacks are of major concerns due to their direct impact on network performance. For examples, authors discuss in [32] that mesh routers are very attractive targets and network entry points for DoS attacks. As WMNs already suffer from self-interference due to the existence of multiple ongoing flows, the presence of DoS attacks can further degrade their capacity [16].

The performance impact of DoS attacks can be even more severe, if the attacks are carried out on all the hops of a communication path between a sender and a receiver, instead of targeting just a few hops on the path. Assuming a path is of five hops, and the attack is carried out on all five hops first, and then on just two hops of the path. As the attack on five hops covers the entire path, the performance impact will be

---

This project is supported by National Science Foundation (NSF) under award ECS-0524519.

---

A. K. Agarwal (✉)  
3042 EBII, NC State University, 890 Oval Drive,  
Raleigh, NC 27606, USA  
e-mail: akagarwa@unity.ncsu.edu

W. Wang  
3056 EBII, NC State University, 890 Oval Drive,  
Raleigh, NC 27606, USA  
e-mail: wwang@eos.ncsu.edu

higher as compared to the attack on two hops. The DoS attacks impacting the entire communication path are defined as *path-based DoS* attacks [13]. Due to the multi-hop communication nature of WMNs, the impact of path-based DoS attacks can be very harmful leading to significant performance degradation. These path-based DoS attacks are studied in the context of sensor networks [13]. In their work, authors have proposed a one-way hash chains mechanism to prevent communication from path-based DoS attacks, without considering the performance impact. WMNs are very different from sensor networks in a way that an attacker has to attack much more powerful nodes in WMNs as compared to low processing and low memory nodes in sensor networks. As the multi-hop flows are inherent in WMNs competing for the bandwidth, the damage due to reduced bandwidth caused by the path-based DoS attacks can be drastic. Therefore, it becomes even more important to understand the path level impact of such attacks in WMNs.

In this paper, we present a comprehensive performance study of the path-based DoS attacks in WMNs. The central question addressed in this work is: what is the performance impact (in terms of packet loss and packet delay) on a multi-hop flow under a path-based DoS attack? Specifically, we discuss performance degradation with respect to varying attack intensity, characterized by attack traffic's packet size and packet rate. We also show how the path-based DoS attacks interact with factors such as physical diversity, medium errors, and hop-count. To address these questions, we conduct a measurement study based on a real-time,<sup>1</sup> because it can capture many realistic factors than analytical and simulation studies. For instances, unlike in simulation studies, it is not required to assume an approximate interference model which can skew the accuracy of the results. In the testbed, different scenarios are designed by changing wireless cards power levels (link qualities), by considering attacker's mobility (physical diversity), and by carrying out two attackers simultaneously (collusion of attackers).

The contributions of this study are the several insightful observations based on the measurement results. We demonstrate that the presence of *hidden* poor links (due to retransmission at the MAC layer) in a network is beneficial to path-based DoS attacks. It is noticed that a low intensity attack is not powerful

in general, but can also cause significant performance degradation in the presence of external interference. We observe that due to physical diversity, an attacker farther from the targeted path can be more damaging than the attacker in the close proximity of the targeted path. We also demonstrate that the impact of attack during collusion (more than one attacker) is not equivalent to the additive of individual attackers. Finally, we present discuss a simple strategy to counter path-based DoS attacks which can potentially reduce the impact of the attack significantly.

The remainder of the paper is organized as follows. We discuss existing studies in Section 2. We describe the goals of this study, attack model, testbed setup, and performance metrics in Section 3. The detailed experimental results in various scenarios are presented in Section 4. Insights obtained from the measurement results, a simple counter strategy, and a comparative study with related works are discussed in Section 5. Finally, Section 6 concludes the paper.

## 2 Related work

The relevant studies on DoS attacks in wireless networks can be broadly categorized into four parts: (1) preventive solutions [31, 32]; (2) physical jamming [9, 27]; (3) non-protocol complaint attack [5, 23]; (4) protocol complaint attack [1].

There are several works where researchers have proposed mechanisms to prevent DoS attacks in wireless multi-hop networks. For example, authors have proposed a new framework which makes WMNs resilient to attacks such as bogus-beacon flooding attack [31, 32]. Authors have discussed a new key management scheme for WMNs which ensures that illegitimate nodes are not able to get unauthorized access to the network. Similarly, another key management scheme is proposed in [4] to prevent ad hoc networks from attacks. In this work, authors have divided a network in a group of clusters, and the key management is based on each cluster in the network. A scheme which first detects malicious nodes by the collaboration of legitimate nodes, and performs elimination of such nodes by a credit strategy is discussed in [29]. However, these works have not discussed specifically that the path-based DoS attacks can be prevented in WMNs. In addition, these solutions are not implemented on any commercial wireless systems, thus it is yet unknown how these solutions are effective in preventing path-based DoS attacks. In addition to studies on preventive solutions, other works have focused on proposing detection algorithms for physical jamming.

<sup>1</sup>In our work, by real-time testbed we mean that a prototype network is deployed physically and equipped with required hardware devices and their software modules.

Generating RF noise constantly by a malicious node captures the medium entirely, and the nearby legitimate nodes can not gain access to the network [27]. Such DoS attacks are defined as physical jamming, and studied extensively in the literature, and can *kill* the connectivity of legitimate nodes [9]. Xu et al. studied four different jamming models and their effectiveness in wireless networks. Their main focus was to provide detection algorithms, although not providing any solutions to prevent them [27]. Similarly, jamming of encrypted wireless ad hoc networks at transport (TCP) and network (AODV) layers is studied in [9]. They showed that if the packet type and timing information above network layer are available, the jamming gains above 100% can be obtained. With regard to prevention measures for jamming, a scheme at physical layer using code tree has been proposed in [11]. Their scheme is able to deliver 100% packets when there are five or fewer jammers, and 90% with six to ten jammers. Switching to different channel or moving to different location away from the jammer has been discussed at [25, 26, 28]. Their results have specifically focused on showing how the jammed nodes can recover effectively by using their schemes.

In general, the interference due to RF noise is intentional, which is generated by malicious entities; but then one aspect of it is *unintentional*, which may be due to poor placement of nodes, or external sources in a network [21]. Such unintentional interference can degrade the performance *gracefully* instead of immediately killing the network access like physical jamming. Wireless multi-hop networks are highly prone to such kind of interference<sup>2</sup> and the issue has received large attention in the past [17, 24]. However, the interference issue in WMNs has been studied extensively to understand its impact on the capacity of the networks [8, 19] and many solutions have been proposed to this problem, thus we do not focus on the interference from physical layer jamming.

DoS attacks due to non-protocol compliant behavior occur when the parameters of a standard protocols are modified either to gain unlimited network access or to prevent legitimate nodes from accessing the network [5, 23]. For example, Bellardo and Savage [5] studied the impact of virtual carrier sense attacks (in which an attacker sends frames with large duration value to follow non-compliant CSMA protocol), and their observations show that such attacks can degrade the

performance severely by denying access to the nearby nodes. In addition, they study deauthentication attacks (also termed as MAC layer flooding attacks), in which an attacker generates fake disassociation or deauthentication requests to disconnect a legitimate node from the network. Raya et al. [23] present IEEE 802.11 protocol misbehavior in which an attacker modifies protocol parameters (such as NAV value) to gain high bandwidth share. Extensive research effort in the past is spent to understand, to detect, and to counteract such attacks in wireless networks [22]. Therefore, we do not focus on such attacks in our work.

On the other hand, protocol-compliant DoS attacks follow all rules of a standard protocol. For instance, the JellyFish and Black Hole DoS attacks at the networking layer fall into this category [1]. In these attacks, malicious nodes on routing paths either do not forward packets in a legitimate way or drop them either partially or entirely. Although existing solutions can detect protocol misbehavior, it is not easy to detect protocol-compliant DoS attacks as they operate according to the standardized behavior of a protocol. The impact of such attacks can be for long term, and can cause graceful damage by slowing down the system gradually. With no modification to a standard protocol, they are very easy to carry out. Therefore, we focus on protocol-compliant DoS attackers in this work, and carry out DoS attacks by flooding traffic in the networks.

Therefore, we study the performance impact of path-based DoS attacks on traffic flows in WMNs. Specifically, we focus that how the parameters of an attack traffic (such as packet size, packet rate, and number of attackers) interact with the same parameters of the normal flows. In addition, we provide a simple counter strategy that exploits the MAC level properties of wireless networks to reduce the impact of an attacker without affecting the performance of normal flows. We believe that our works can be useful for the jamming detection algorithms, and also for providing corrective measures for the efficient placement of routers in WMNs.

### 3 Goals and methodology

The goal of this study is to assess the performance of WMNs and further understand how well they work under path-based DoS attacks in realistic settings. In particular, we are interested in the results of interaction among various factors, such as attack intensity, collusion, medium errors, physical diversity. To this end, we perform a small-scale measurement study in order to achieve following objectives.

<sup>2</sup>It is a kind of MAC layer jamming due to nodes, which are either inside the carrier sense (CS) range or act as hidden terminals in wireless networks.

### 3.1 Objectives

Through this study, we answer following questions:

- 1 *How does the physical diversity affect the impact of path-based DoS attacks?* Wireless links experience varying medium conditions depending upon their locations. It is not yet discussed in the literature that how varying link conditions can alleviate or exacerbate the impact of path-based DoS attacks. It is important to know because it can be helpful to design a better placement of nodes in the network.
- 2 *Are the medium errors conducive to path-based attacks?* Medium errors are very common on wireless links. The retransmissions at the MAC layer help in reducing the impact of medium errors. However, we are interested to know about the performance impact of the path-based DoS attacks, when varying medium errors are present on the links.
- 3 *Is the collusion of attackers always helpful?* More than one attackers can collude to increase the intensity of their attack. However, it is not clear that whether the gain is always the multiple of number of attackers involved in collusions. We take an example of two attackers to find about it. The results may be helpful for detection algorithms to find out if the attack is being carried out by one or multiple attackers.
- 4 *Can there be a simple counter strategy to lessen the impact of such DoS attacks?* To address this question, we discuss a simple strategy, which exploits the MAC level properties of wireless networks for reducing the impact of such attacks without affecting the performance of normal communication.

Recently, there has been an increase in performing experimental studies [6, 15], as they are able to provide a realistic view of the network performance. Also, the results obtained with an experimental testbed can be used to understand the performance of a real network deployment. However, there are several challenges in carrying out an experimental study. One of the main challenges in our study is placing routers in locations so that an attacker router can be outside CS range of particular routers whenever needed. Due to geographic restriction in placing routers anywhere in the campus building, we pre-determine the router positions, which is typical in WMNs [3]. However, to generate dynamic network connections, we vary power levels of each router. Another challenge is that we aim to differentiate the effects of routing and attacks, e.g., packet losses due to the attack or link dynamics. This is not trivial

because we observe that paths are updated frequently, even in our quite limited-size setup with optimized link state routing (OLSR) protocol. It becomes very difficult to have consistent observations unless we can have stable paths. Therefore, we resort to static routing to achieve stable paths in order to provide conform observations.

### 3.2 Attack model

DoS attacks in wireless networks can be performed at network layer (such as JellyFish, or black hole [1]), at MAC layer (such as deauthentication/disassociation attacks [5], DIFS and NAV attacks [23], or attacks by flooding traffic in the network), and at physical layer (such as high RF noise [26]). Although, prevention measures at network and physical layers [25, 26, 28] have been extensively discussed, MAC layer attacks are not fully addressed. For example, there are solutions to prevent deauthentication or disassociation attacks [5] or DIFS and NAV attacks [23], but it is still not possible to prevent an attacker from flooding traffic in the network.

As noted above that existing solutions can not prevent an attacker from flooding traffic into a network, we discuss an attack model based on flooding traffic in the network. In this model, an attacker floods a stream of packets by broadcasting data in the network, such that the nodes in the vicinity of the attacker are not able to utilize their capacity completely. This attack model is powerful because the attacker follows all rules at the MAC layer, and does not use any protocol misbehavior. Due to this, it is very difficult to detect such an attacker, and is even unlikely to differentiate it network congestion. Also, these attacks are very easy to carry out, because any one without changing parameters in MAC protocol can perform such attacks by generating only dummy packets. Such attacks can be intentional (by external entities) and unintentional (by an internal node due to its placement). We consider both behaviors as attacks in this model and discuss other properties associated with this attack model.

In this model, the intensity of the attack is defined by the characteristics of the traffic an attacker generates. We use a CBR (constant bit rate) stream in the attack model as it is simple to generate by many open source tools (Click, <http://www.read.cs.ucla.edu/click/>). Packet size and packet rate are two parameters which are used to vary the intensity of the attack. For example, in this work, the packet size of an attack is varied from 32 bytes to 512 bytes. It is because most of the traffic streams over the Internet are with packet size in this range [18]. The packet rate of an attack is varied from

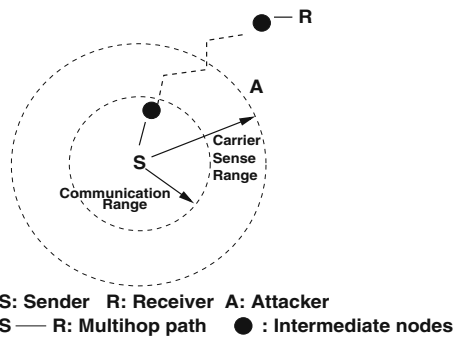


Fig. 1 Path-based DoS attack

50 to 1,000 packets per second (pps), which allows us to distinguish the impact of low intensity and high intensity attacks.

To obtain the maximal effect of an attack, the location of the attacker node is carefully chosen such that it is outside the CS range, but inside interference range of all of the routers en-route a path. Therefore, the attacker acts as a hidden terminal to the sender and can cause the significant damage to the sender’s traffic. Moreover, as it is outside the CS range of all intermediate routers and receiver node, the attacker node can further interfere with the traffic forwarded by intermediate nodes, and the traffic coming back from the receiver. Therefore, the attacker is able to cover the maximum portion of the path between the sender and receiver. Figure 1<sup>3</sup> depicts an illustration of a typical attack scenario studied in our work. In addition, we have specifically discussed attacks generated by at most two attackers to study the impact of attacks based on the number of sources involved in a particular attack.

### 3.3 Wireless mesh testbed

We setup a wireless mesh testbed as a miniature version of infrastructure wireless mesh networks deployed in real environments. The testbed is on the second and third floor in a building for which a sketch diagram is shown in Fig. 2. The testbed consists of seven mesh routers, and several mesh clients to form a wireless multi-hop mesh network. The three mesh routers (with ids R2, R5, R7) also act as access points. The clients are mobile, whereas all mesh routers are static in our testbed. All nodes (routers or clients) are using IEEE

<sup>3</sup>Communication and carrier sense ranges shown in circles are just for illustration purposes here. In real world, the coverage is almost never circular and varies a lot depending on obstacles (walls, doors), and interference sources.

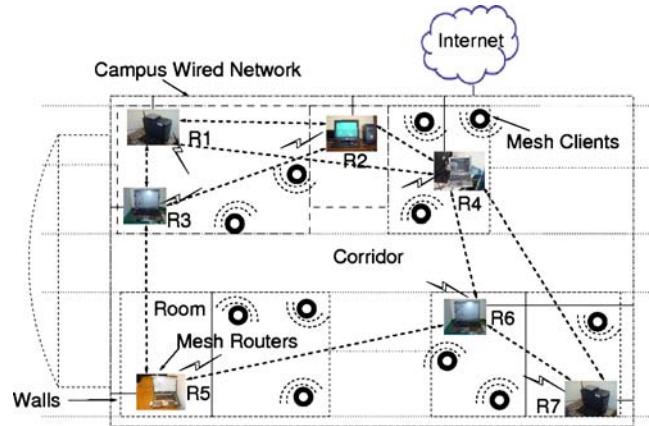


Fig. 2 Testbed setup

802.11b based wireless cards. The routers are configured in *ad hoc* mode, with a *pre-determined* channel, which is the farthest than the channels used by other networks in the vicinity of our testbed to reduce the impact of interference from those networks. The transmission rate on all nodes is set to 11 Mbps. The *ip* addresses are assigned statically to each node to eliminate the delay due to DHCP configuration. All nodes are running Ubuntu linux with 2.6 kernel. In addition, one machine is used as a controller and helps in accessing all nodes (mesh routers and clients) remotely over our campus wired network for monitoring and configuring multiple measurements during a long period time. A snapshot of the console accessing nodes remotely is presented in Fig. 3. Figure 3 shows the routing entries for a particular mesh node in the testbed.

We notice that hardware and software associated with devices span a wide variety. Therefore, our testbed represents a general network using many heterogeneous devices. In the testbed, desktops are Dell PC (Pentium IV 2.6 GHZ), and laptops have Dell (Celeron Processor 2.4 GHZ). Access points are Cisco 1200 series access points. Wireless Cards are from Lucent (Orinoco hermes based) and Netgear vendors (atheros and prism based). We use *Ethereal* as packet analyzer. *Click* is used as traffic generator for setting up various configurations.

#### 3.3.1 Data collection

We carry out experiments in nights (unless otherwise stated) to have the minimal impact by external interferences, such as traffic from wireless nodes associated with campus network, cell phones and microwaves. We repeat each experiment 20 times over a long duration (over 3-month period) to obtain a good average of measured parameters. We measure packet loss, and

```

Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.2         0.0.0.0        255.255.255.0  U     0      0      0 eth1
10.0.0.3         10.0.0.2       255.255.255.0  U     1      0      0 eth1
10.0.0.1         0.0.0.0        255.255.255.0  U     0      0      0 eth1
10.0.0.0         0.0.0.0        255.255.255.0  U     0      0      0 eth1
152.14.96.0     0.0.0.0        255.255.254.0  U     0      0      0 eth0
169.254.0.0     0.0.0.0        255.255.0.0    U     0      0      0 eth0
0.0.0.0         152.14.96.1    0.0.0.0        UG    0      0      0 eth0

```

**Fig. 3** Controller's console screenshot

delay to analyze the impact of attacks on the performance of flows in WMNs, as these metrics are used extensively to study the performance of wireless mesh networks [2, 7]. We vary packet size, packet rate of normal traffic, and attack traffic.<sup>4</sup> The attack traffic is generated by broadcasting UDP packets in the testbed, whereas the normal traffic is *Ping* traffic. In addition, we vary number of attacker nodes and number of hops between the sender and receiver.

The details of traffic flows are as follows, which are the same for all experiments, otherwise specified for each individual scenario.

**Attacker** Router *R1* is selected as the attacker node which broadcasts traffic in the network. The power levels of routers are set in such a way that it is out of the CS range of and inside interference range of the routers on different paths.

**Starting and ending routers** We randomly take a pair of client nodes for measurements, but focusing on a particular pair of router nodes indexed *R5* and *R7* as shown in Fig. 2 for discussion only. Where router *R5* is the end point or the egress router and router *R7* is the starting point or ingress router in the network, although the clients associated with routers *R7* and *R5* are the *actual* sender and receiver. We compute an average of experimental measurements by considering multiple client pairs for better accuracy.

**Routing and locations** Router *R6* is configured as the intermediate node to enable a minimum of two-hop as shown in Fig. 2. The location of each router is chosen to ensure that packet losses between a client and an access or ingress router are almost negligible; thus measuring

packet losses occurred only in the backbone (formed by routers) of a wireless mesh network.

**Traffic flows** The flow between routers *R5* and *R7* is *Ping* traffic, whereas attacker broadcasts UDP traffic. The attacker's packet rate and packet size are kept fixed at 100 pps and 200 bytes IP packet<sup>5</sup> in this scenario.

### 3.4 Performance metrics and impact factors

Previous experimental studies have considered packet loss and packet delay extensively as their performance metrics [10, 12]. It is because these metrics are very useful in revealing the performance view of a network, and have direct relationship with network throughput [20]. In addition, cumulative distribution function (CDF) has been used by researchers to under the performance trend of a particular performance metric in the existing literature [30]. Therefore, we use packet loss, delay and CDF as performance metrics, and define them as follows:

- **Packet Loss:** Specifically, we measure the percentage of packet lost out of total packets sent to indicate packet losses.
- **Packet Delay:** In our measurements, per packet end-to-end delay has tracked the impact of delay in the network.
- **CDF:** We run each experiments multiple times to obtain an accurate average. The values from multiple runs of each experiments is used to compute the CDF for packet losses or delays.

Now we discuss different factors associated with our experiments, which help us in simulating different scenarios experienced in real environments. Some of the

<sup>4</sup>In our work, normal traffic (or flow) is generated by an authorized node, whereas, the attack traffic is generated by an unauthorized and malicious node.

<sup>5</sup>Just for differentiation, the attacker's packet size is the same as IP packets, whereas the normal flow packet size is only the application payload.

factors, such as heterogeneous devices, are introduced in our setup intentionally, whereas some factors, such as interference, are unintentional. Therefore, our measurements are expected to be helpful in providing deeper insights into the measurements of wireless mesh networks.

**Interference** It is pervasive in wireless networks as signals from different sources impact each other. It is of more concern in WMNs as the traffic from different sources can affect routing leading to degradation in the quality of multi-hop paths. Although, we have tried to avoid interference in our testbed by running experiments with the minimal interference (such as at 2AM), it is not possible to avoid the interference entirely. Moreover, we also ran some of our experiments during day time to explicitly study the impact of interference and to compare them with the measurements taken over nights. However, in this work, we have presented only the average values of performance parameters measured during nights. Although, there were high packet losses during day time, but we noticed the trend of measurements being similar to measurements taken over nights.

**Physical layer channel diversity** Such diversity in wireless networks can arise due to various reasons. First, if we put wireless devices at different locations, the physical channels of devices can get affected differently by the adjacent environment, even though devices are using the same physical channel. Second, multiple devices interact in different manners at different locations to acquire the medium access leading to diversified channel conditions. Third, wireless devices can use physical channels in such a way to best utilize the wireless resources, such as bandwidth. In our testbed, devices use the same physical channel (to make communication possible as devices have single wireless interface), covering physical location and link. We study such diversities by placing attackers at different locations (with other similar properties, such as packet rate and size) to measure the variations in their impacts.

**Heterogeneous devices** In any network deployment, it is bound to have routers and client machines using different hardware and software configuration. Although, our goal is not to quantify the impact associated with different hardwares, it helps us study a more realistic environment. In order to obtain insights that are applicable to networks with heterogeneous rather than homogeneous devices, we have used machines with different hardware configurations (desktop machines, laptops machines, Cisco access points),

and wireless cards with different chipsets (atheros, prism, hermes).

## 4 Measurement results

The main focus of obtaining measurement results is to answer questions described in Section 3. The performance impact of attack intensity (invariant and variant) is presented in Subsections 4.1 and 4.2. How the physical diversity interacts with path-based DoS attacks is discussed in Subsection 4.3. We discuss the conducive nature of medium errors for path-based DoS attacks in Subsection 4.4. The performance impact of collusion in WMNs is shown in Subsection 4.5. The performance trend of the impact of attacks with respect to varying hops is discussed in Subsection 4.6.

### 4.1 Impact of invariant attack traffic

First, we study the impact of attack traffic, which is of broadcast nature, on the performance of one two-hop flow in the network as shown in Fig. 2. The parameters of attack traffic, such as packet size and packet rate, are fixed, whereas the same parameters of the normal flow are varied. We consider that the normal flow is between the routers  $R7$  and  $R5$ , where router  $R7$  is the start point and router  $R5$  is the end point in the network, although the client associated with routers  $R7$  and  $R5$  are *actual* sender and receiver. Router  $R6$  is used as the intermediate node for making it a two-hop flow. The router  $R1$  is the attacker node, which broadcasts traffic in the network. The power level of routers are set in such a way so that so that router  $R1$  is out of carrier sense range of and inside interference range of the routers on the flow, and can act as attacker for the flow. To verify this, we periodically carried out a simple experiment to find out whether router  $R1$  and each of other routers ( $R5$ ,  $R6$  and  $R7$ ) can transmit simultaneously at the maximum rate. The retry-count at routers  $R5$ ,  $R6$ , and  $R7$  is set to their minimum allowed values, which are 0, 0, 1, respectively, and the retry-count at router  $R1$  is set to default value (8). The minimum retry count is helpful in obtaining repeatable measurements, because of the less variations in transmitting the packets. The flow between routers  $R5$  and  $R7$  is Ping traffic, whereas attacker broadcasts UDP traffic. The attacker's packet rate and packet size are fixed at 500 pps and 200 bytes IP packet in this scenario. In addition, by repeating many run, we have ensured that packet losses between a client and an access point are almost negligible, so that the packet losses occur

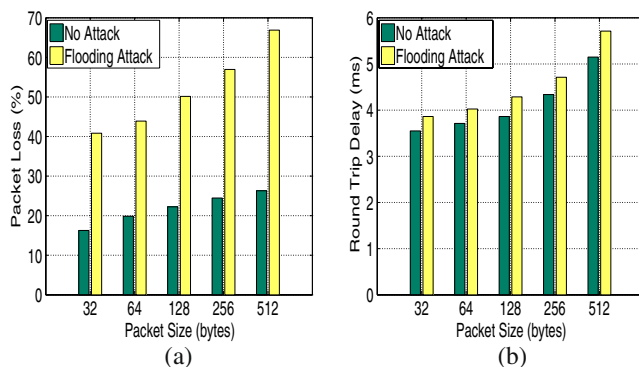
only in the backbone (formed by routers) of wireless mesh network.

#### 4.1.1 Normal traffic: packet size variations

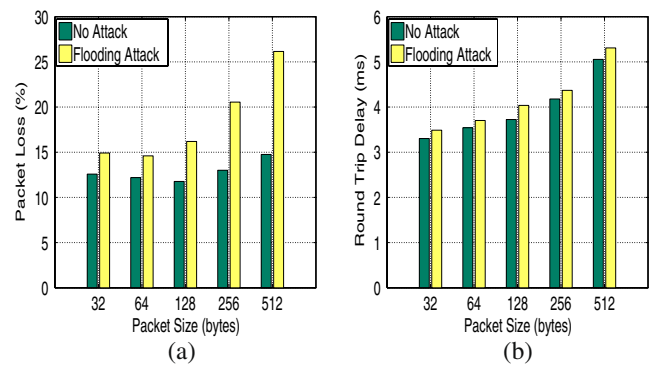
In this scenario, the packet size (ip payload) of the normal flow is varied from 32 bytes to 512 bytes, while the rate is fixed at 100 pps. The observed packet loss and round trip delay with and without attack are shown in Fig. 4. We notice that mostly packet losses under no attack are up to 25%, whereas packet losses increase up to 70% when an attack is carried out. It is obvious that an attack is more severe as the packet size of the normal flow is large. It is due to the fact that large packets spend more time in air leading to higher probability of collision with attack traffic.

By taking a closer look at Fig. 4a, we notice that packet losses are more than twice in the presence of attack. Although, it seems that the impact is more severe for large packets (packet losses almost three times) than small packets, an attack is equally effective (in terms of percentage loss) when packet size is small. In addition, the average packet losses without attack seem to be almost similar across different packet sizes, whereas packet loss in the presence of attack increases quickly with the increase in packet size. By looking at the delay in Fig. 4b, we can see that the delay with attack increases slightly as compared to the delay without attack. We believe that it is because we have almost disabled retries during experiments, which leads to increased delays.

Note that we have lowered power levels in such a way, so that the attacker is out of CS range of all routers. However, with the reduced power level, packet losses are little higher due to poor link quality of the path. Thus, we increase the power level of the routers to the maximum for better link quality. However, we placed the attacker router 1 at some other location



**Fig. 4** a, b Invariant attack: average statistics (packet sizes)



**Fig. 5** a, b Invariant attack on good links: average statistics

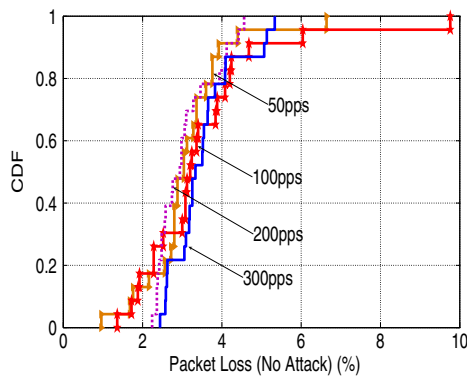
so that it was still outside the carrier sense of and inside the interference range of the other routers. The obtained results in this scenario are presented in Fig. 5.

We notice that packet losses under no attack are reduced (mostly packet losses are below 15%) as compared to the previous scenario, and are almost similar across different packet sizes. It is because of the improved link quality due to the increased power levels. Packet losses under attack are also reduced (mostly up to 35%) as compared to the previous case. It shows that an attack is not as effective as in the previous case. Figure 5a also shows that an attack is not very effective for small packets; while its impact is more severe on traffic of large packets such as 256 or 512 bytes. The increase in delay is even less effective as compared to the previous case with the similar reason cited before.

Therefore, we observe above that attacks are more effective on the path with poor link qualities. An attacker (either external or internal) can easily take advantage of this fact, and make the network disconnected, if the attacker obtains such information about the network. As it is frequent to have such poor links in WMNs that are unavoidable during path establishment, it is necessary to protect such paths as compared to the paths with very good quality links.

#### 4.1.2 Normal traffic: packet rate variations

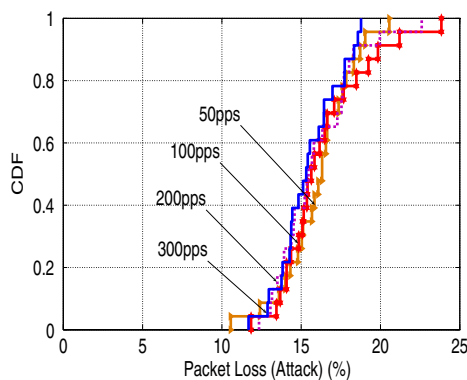
In previous case, packet rate of the normal flow is fixed at 100 pps and packet size is varied. Now, we study the impact of attacks when the packet rate is varied from 50 to 300 pps with packet size fixed at 64 bytes. The reason for choosing 64 bytes packet size is due to observations in Figs. 4 and 5 that packet losses are generally less with small packet sizes as compared to large packet sizes, assuming other factors are similar. Therefore, this scenario also helps us in studying the impact of attacks when packet losses are low in the networks. In addition,



**Fig. 6** No attack: packet loss CDF

this scenario is similar to the previous scenario as the attacker is outside the CS range of all routers on the path (*R5, R6, R7*), and link quality is good. Results are presented in Figs. 6 and 7.

We observe that packet losses under no attack in Fig. 6 are similar across different packet rates. It means that only packet size has an impact on packet losses as compared to the packet rate. Generally packet losses are below 5% across different packet rates with no attack. However, we notice that packet losses are increased almost 4 times in the presence of the attacks as shown in Fig. 7. However, the damage due to an attack across different rates remains same. It means that if the attack traffic is fixed, flows with high packet rates can be preferred due to almost similar packet losses. This observation is very important because higher packet rates lead to increased throughput in the work. In addition, it shows that as the attacker is outside the CS range of all routers, its impact can be very severe (up to 4 times). As we observed minor variations in delay as in the previous case, measurements are not presented here.



**Fig. 7** Invariant attack: packet loss CDF

## 4.2 Impact of variant attack traffic

Here, we change the packet rate and packet size of the attacker’s traffic, and keep other parameters associated with the normal flow fixed. These experiments are carried out by placing *R1* at the same place as shown in Fig. 2. Power levels of the normal flow routers are reduced to enable the attacker being outside their CS range. The packet rate and packet size of the normal flow are fixed at 100 pps and 128 bytes (IP payload), respectively.

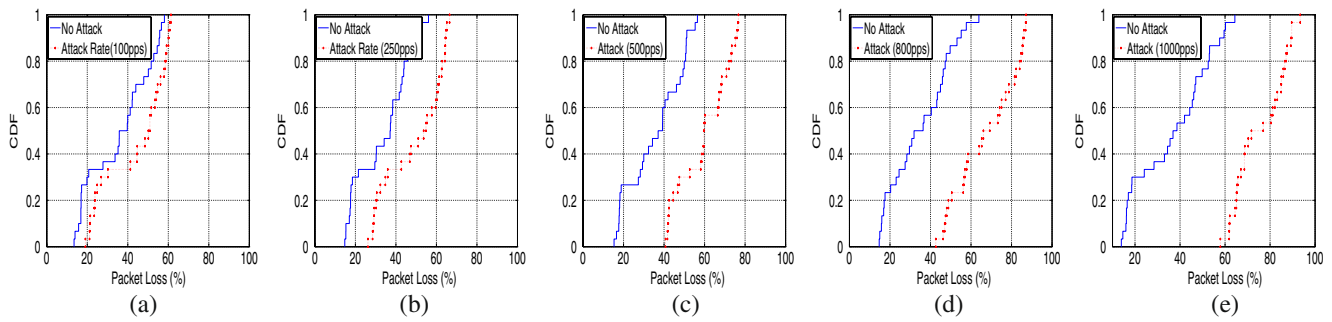
### 4.2.1 Effects of attack rates

We vary attacker’s packet rate from 100 to 1,000 pps with a fixed packet size of 200 bytes IP packet. Figure 8 shows the comparison between packet losses with and without attack for different rates. We notice that the small attack rate with 50 pps causes minor damage to the normal flow. However, the gap between curves widens as the attack rate increases. The packet losses with higher attack rates are almost close to 80%, leading to a significant damage. The average packet losses in Fig. 9a shows that they become even worse with a rate of 250 pps, which causes almost 50% more losses as compared to the losses without attack. Such statistics can be helpful in identifying external attacks (intentional) or attacks due to poor placement of nodes (unintentional). For example, packet rate beyond 250 pps may not be used on the nearby routers to prevent high packet losses. Moreover, statistics of average packet losses (and other metrics) can be stored and updated periodically in a database. If the packet losses are very high as compared to the historic values, preventive measures can be triggered to maintain good network performance.

Further, we see in Fig. 9b that the delay shows only minor increase with lower attack rates. The maximum increase in delay is about 25% with 1,000 pps attack rate. The increase in delay is only for attacks with 800 pps and higher. We consider that the increase in delay is mainly due to the waiting time at MAC layer for accessing the medium, because there is almost no retransmission delay for retry limit being 0 or 1 on the routers. Therefore, although the packet losses become significant even beyond the rate of 250 pps, the increase in delay becomes much higher for attacks with 800 or 1,000 pps.

### 4.2.2 Effects of packet size variations

Now, the attacker’s packet size is varied from 32 to 512 bytes (IP packets) and packet rate is fixed at



**Fig. 8 a–e** Variant attack: attack rate variations

500 pps, as shown in Fig. 10. We observed that average packet losses without attack are approximately 25% in Fig. 11b. However, with an attack, we notice from Fig. 11 that the packet losses are almost 100% higher even for 32 bytes packet size. The packet losses becomes almost 150% higher with large packet size. Therefore, at the rate of 500 pps, even small packet size can cause significant damage to normal flows. However, the delay exhibits a significant increase only beyond packet size of 256 bytes. Therefore, we suggest that the delay alone can not be used to identify the performance degradation due to attacks in the network, while packet loss is a good metric to detect attacks.

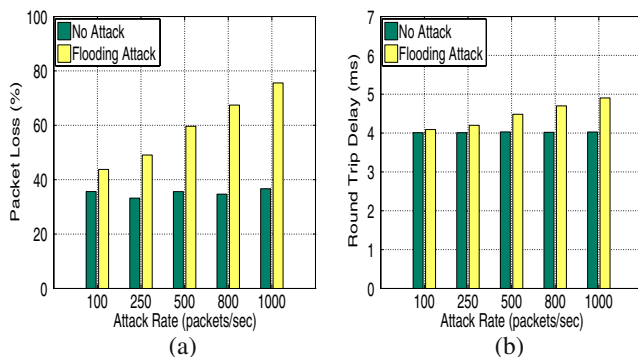
### 4.3 Physical diversity

Physical diversity is an important issue in wireless networks because of dynamic radio channels in real world. For example, when wireless devices are at different locations, the physical channel associated with devices can be affected by the adjacent environment, even though devices with same physical channel. Also, multiple devices (or users) interact with each other for capturing shared medium, leading to different channel conditions as well. In this work, we focus on the effects

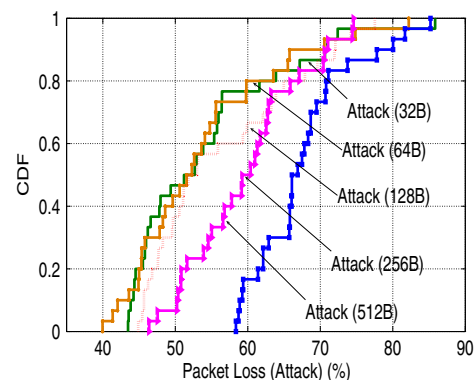
of the same channel, without considering the effects of channel assignment.

We study physical diversity by moving an attacker in different directions (by keeping other parameters constant) to measure the impact of links. We do so because, if the attacker’s position is fixed, the impact of the attack may also be fixed given that the other conditions remain similar during the execution of the attack. However, an intelligent attacker would want to move in such a manner nearby the targeted path to inflict the most severe damage. Although, it may seem obvious that if the attacker moves very close to the targeted path, the impact of attack may be higher. However, we find that it may not be always true and when the attacker moves farther from the targeted path, the impact of the attack may be higher.

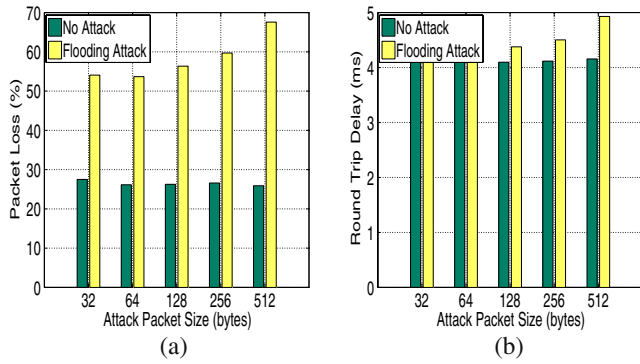
We use two experiments in this work to study the impact of physical diversity. In the first experiment, the attacker (closeby attacker in Fig. 12) moves along the targeted path, and we measure the packet losses at four different locations, where P11 and P14 are starting and end points, and P12 and P13 are any intermediate points. In the second experiment, the attacker (far attacker in Fig. 12) moves away from the path, and packet losses are measured at four locations, where P21 and



**Fig. 9 a, b** Variant attack rates: average statistics



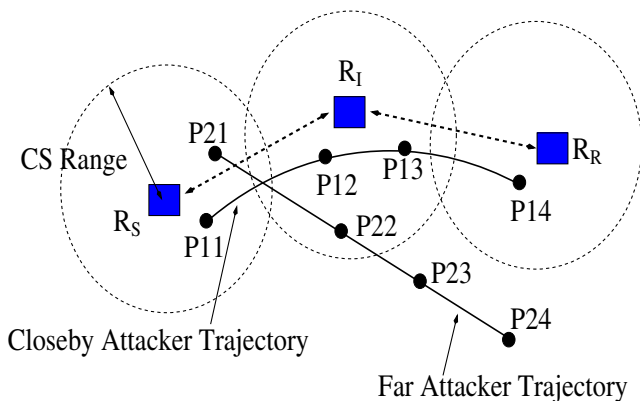
**Fig. 10** Variant attack packet size: packet loss CDF



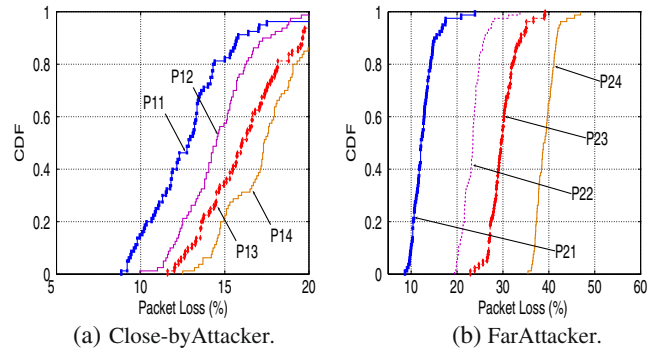
**Fig. 11** a, b Variant attack packet size: average statistics

P24 are starting and end points, and P22 and P23 are any intermediate points in Fig. 12.

The results are presented in the Fig. 13. We notice that *the packet losses are higher when the attacker moves away than the packet losses when the attacker moves closer to the targeted path*. The reason is that when the (closeby) attacker is very close to the targeted path, the attacker remains in the CS range of several nodes on the path. Therefore, the impact is not very severe except stealing some of the capacity of the path. Consequently the impact from all the four points are similar. However, when the attacker (far attacker case) moves away from the path, initially (at the first point P21) the impact is very similar to the impact when the attacker moves closely. It is because the attacker is still in the CS range of many nodes on the path, and can not act as the hidden terminal. Due to this, the impact of far attacker at point P21 is not significant. However, as the attacker moves further away, the impact becomes severe and the packet losses increase. We notice that the packet losses are the highest at point P24. It is because that the attacker is completely out of the CS range of any



**Fig. 12** Attacker's mobility



**Fig. 13** a, b Physical diversity: impact of attacker's mobility

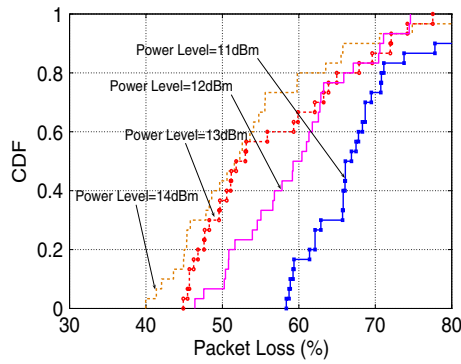
of the nodes on the path, therefore causes the highest damage. Although, the packet losses are high at P22 and P23 points too, we observed (by running a separate small experiment) that the attacker was not completely out of the CS range of all the nodes on the path. Infact, the attacker was able to sense the channel busy intermittently at these points. Due to this, the impact of attack is less compared to the impact when the attacker is at point P24.

These measurements suggest that it is not always good to create paths which are far from the attacker's position. One way is to form paths such that the attacker is outside the interference range of all the nodes so that the attacker does not act as an attacker at all. However, if it can not be possible, then one of the strategies to counter it can be establishing the required path as close as possible to the attacker. In this way, the path will lose some of its capacity (due to carrier sensing with the attacker) but packet losses will be low and the impact of the attack will be much less.

#### 4.4 Medium (radio link) errors

When the raw bits of a frame are transmitted over wireless medium from a sender to a receiver, it is very common to have one or more bits to be in error. Wireless devices employ error correcting mechanisms at the physical layer to recover from these errors. If the errors are not recovered, a negative acknowledgment (NACK) is sent to the sender (to its MAC layer) by the receiver. Once the sender receives a NACK, it retransmits the frame. There may be several causes to induce medium errors such as interference, signal quality and multipath diversity, and so on.

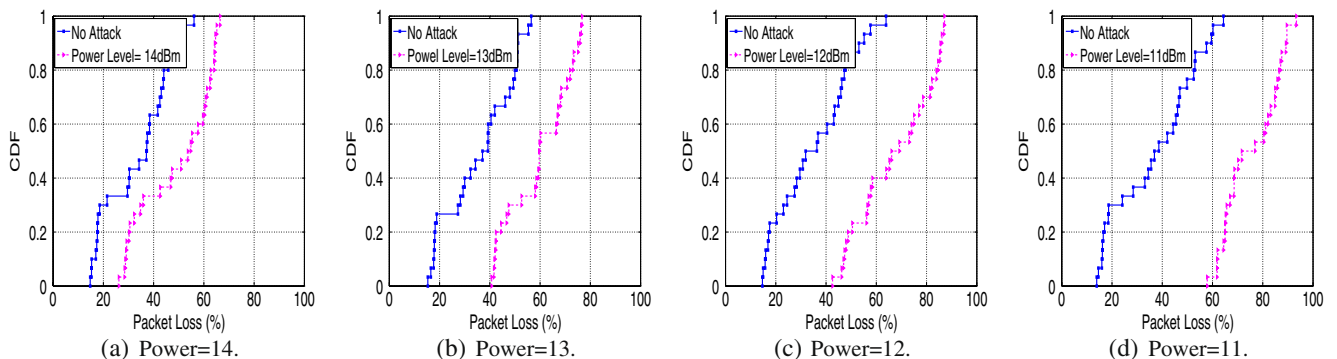
Radio link errors are one of the most critical causes impacting wireless link quality. However, as the wireless MAC layer uses retransmissions, often times the actual quality of poor links is not exposed. We call such links as *hidden poor links*. Therefore, it becomes



**Fig. 14** Packet loss CDF: no attack (retry = 0)

essential to study that how a path-based attack behaves under different radio link errors. To study this, we change power levels of the nodes in our testbed to observe different radio link errors. Specifically, we used power level values of 14, 13, 12, and 11 dbm. Initially, we set the retry count to 0 in order to obtain actual errors on the path, and there was no attack being carried out. The measurements are presented in the Fig. 14.

We notice that as the power level is reduced, there are higher packet losses experienced on the path. It shows that reduced power level leads to higher link errors, causing higher packet losses. We further carried out the same experiment again with retry count set to the highest possible value to allow retransmissions. We noticed that packet losses are almost the same, close to 20%. It is because that the retransmissions mask the impact of poor link quality induced by reduced power levels. However, we find that as soon as the same experiment is carried out again under the presence of attack, the attack takes the advantage of *hidden radio errors*, and causes higher packet losses with low power levels opposed to high power levels as shown in Fig. 15.



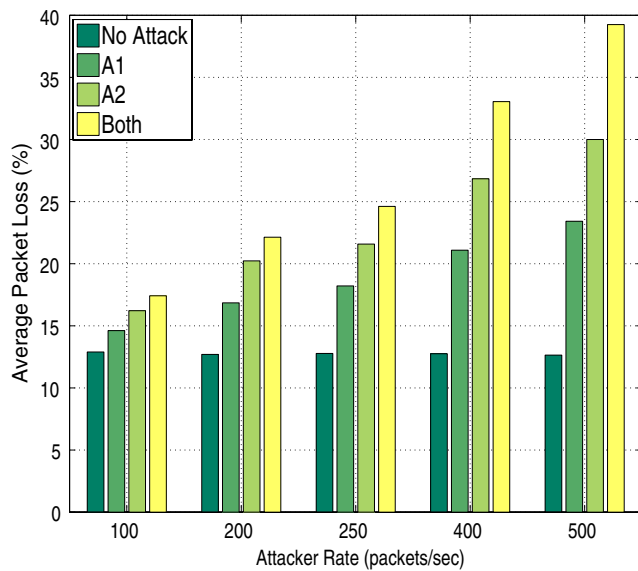
**Fig. 15** a-d Power level variations

It can be easily seen that the path experiences similar packet losses without attacks even though power levels of the links are varied (i.e., due to retransmissions). However, when the attack is carried out, different packet losses are experienced increasing monotonically as the power level is reduced from 14 to 10. It is evident from the results, that the radio errors which are masked due to retransmissions, are exposed again, and the attack is able to take its advantage. With the same intensity of the attack, the attack is able to cause severe damage to the communication on the path.

The important conclusion from the above results is that an attack is more effective on the path with *hidden* poor links. If an attack is carried out over hidden poor links, the performance degradation can be very significant compared to good quality links.

#### 4.5 Collusion: multiple attacks

Now we discuss the impact of multiple attacks on the performance in WMNs. We aim to determine if the joint impact of multiple attacks has any co-relation with the impacts of individual attackers. We specifically discuss the impact of two attacks with regard to their position, and packet rates. In this scenario, router *R3* in Fig. 2 also acts as an attacker in addition to router *R1*. Both attackers are in the communication range of each other, but outside the CS range of normal flow routers. The normal traffic is fixed at 200 pps and packet size (IP payload) is 512 bytes. The traffic from both attackers are similar, and are UDP broadcast with packet size fixed at 200 bytes (IP packets). Figure 16 shows the impact of different packet rates (shown inside brackets) individually as well as jointly at various experiments. The legend *Both* in Fig. 16 represents the scenarios when both attackers send traffic simultaneously at the corresponding rate. As the maximum achievable packet rate with 200 bytes IP packets is more than 1,000 pps by



**Fig. 16** Multiple attackers: comparison of losses

any one node, both attackers can transmit at 500 pps simultaneously.

#### 4.5.1 Effect of attacker's position

Router  $R_3$  (attacker  $A_2$ ) is closer to the normal flow path than router  $R_1$  ( $A_1$ ), which has more significant effect (up to 30%) than  $A_1$  (packet losses up to 25%). It is because that  $A_2$  can generate higher noise than  $A_1$  attacker to the concerned routers ( $R_5$ ,  $R_6$ ,  $R_7$ ), leading to high probability of meddling with the packets originating at the routers. Therefore, although both attackers  $A_1$  and  $A_2$  have similar properties (in terms of traffic parameters) and have similar relationships with the routers ( $R_5$ ,  $R_6$ ,  $R_7$ ) (in terms of carrier sense range), their impacts vary significantly due to their different positions.

#### 4.5.2 Effect of joint attacks

When the two attackers generate traffic simultaneously to degrade the performance of a targeted path, it is called a joint attack or collusion attack. We observe from Fig. 16 that the impact of the joint attack is just little more effective for lower rates such as 100 pps as compared to the impact due to individual attackers. When attack rates increase to 200 and 250, the impact of joint attack grows to 25%, but it is still not very significant as compared to the results of individual attackers, which is up to 23%. However, as the rate increases further, the joint impact is significantly higher than the impact due to individual attackers, which is

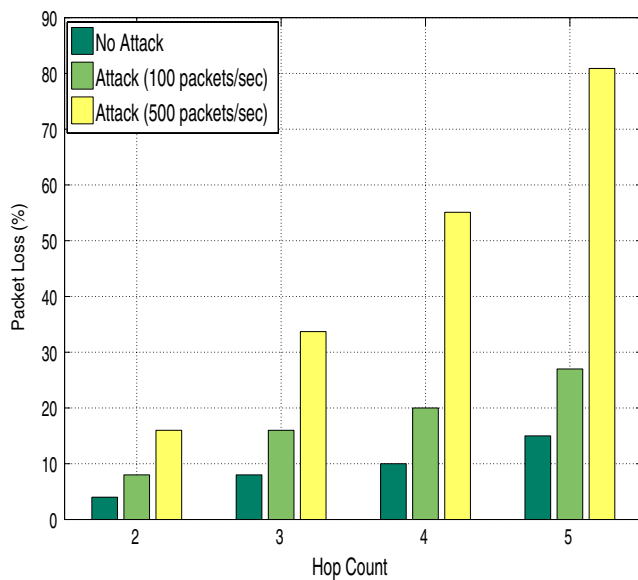
up to 30%. It is because, at higher rates, there are more attack packets over the radio medium, leading to high probability of collision with the normal flows. Therefore, packet losses due to joint attack are up to 40%.

Further, we see that the impact of joint attack is not equivalent to the additive impact of individual attacks. For example, the losses due to  $A_1$  and  $A_2$  are 18% and 22% at rate 250 pps, respectively. However, the losses due to the joint attack (both attackers transmitting at 250 each) are approximately 25%, much below than the sum of their individual losses ( $18\% + 22\% = 40\%$ ). It is true for losses at all packet rates as shown in Fig. 16.

#### 4.6 Impact of attacks on multiple hops

So far we have studied the impact of attacks on two-hop paths. However, it is very frequent to have paths with longer than two hops. Therefore, in this section, we discuss how an attack may impact paths having more than two hops. Specifically, we experimented with paths having two-, three-, four- and five-hop in our testbed. The normal flow on the path consists of 64 bytes packets and packet rate of 100 pps. We have studied two scenarios with respect to attack traffic. In the first scenario, packet rate of attack traffic is 100 pps, where the rate in the second scenario is set to 500 pps. The packets generated by the attacker in both scenarios are set to 200 bytes IP packets. Again, the normal traffic is Ping flow, whereas the attack traffic is UDP (broadcast). The attacker node is placed outside CS range of each router on the paths, but within interference range of each router. However, the power levels of the routers on the normal flow path are at the maximum such that each link quality on the path was good enough to have not very high packet losses even with five-hop paths.

Figure 17 shows the average losses obtained from the measurements. The losses under no attack are less than 20% for all paths. However, we notice that when an attack with 100 pps is carried out, packet losses for two-hop and three-hop paths do not increase very significantly, but become almost doubled for four-hop and five-hop paths, and are below 40% in all cases. When the intensity of an attack (with 500 pps) is increased, packet losses increase faster even for three-hop path, and are significantly high for four-hop and five-hop paths. This observation is consistent with our intuition that paths with more number of hops are affected much more severely as compared to paths with low hop count. Consequently, a path-based DoS attack can inflict more damage by attacking longer paths in WMNs.



**Fig. 17** Hop count: comparison of losses

## 5 Observations and a simple counter strategy

In this section, we first summarize the insights obtained from the measurement results. Then, we propose a simple counter strategy to alleviate the impact of path-based DoS attacks. We also present a comparative study with other related work to justify our observations.

### 5.1 Summary of insights

Now, we highlight the main insights from the measurements presented above.

*Remark 1* One of the main insights is that attacks are more effective on the path with poor link qualities. An attacker (either external or internal) can easily take advantage of this fact, and make the network disconnected, if the attacker obtains such information about the network. As it is frequent to have such poor links in WMNs that are unavoidable during path establishment, it is necessary to protect such paths as compared to the paths with very good quality links.

*Remark 2* If the attack traffic is fixed, flows with high packet rates can be preferred due to almost similar packet losses. This observation is very important because higher packet rates lead to increased throughput in the work. In addition, it shows that as the attacker is outside the CS range of all routers, its impact can be very severe (up to four times).

*Remark 3* We notice that the small attack rate with 50 pps causes minor damage to the normal flow. However, the gap between curves widens as the attack rate increases. The packet losses with higher attack rates are almost close to 80%, leading to a significant damage. The packet losses become even worse with a rate of 250 pps, which causes almost 50% more losses as compared to the losses without attack. For example, packet rate beyond 250 pps may not be used on the nearby routers to prevent high packet losses.

*Remark 4* The results suggest that it is not always good to create paths which are far from the attacker's position. One way is to form paths such that the attacker is outside the interference range of all the nodes so that the attacker does not act as an attacker at all. However, if it can not be possible, then one of the strategies to counter it can be establishing the required path as close as possible to the attacker. In this way, the path will lose some of its capacity (due to carrier sensing with the attacker) but packet losses will be low and the impact of the attack will be much less.

*Remark 5* Another conclusion is that an attack is more effective on the path with *hidden* poor links. If an attack is carried out over hidden poor links, the performance degradation can be very significant compared to good quality links.

*Remark 6* The impact of the joint attack is little higher for lower packet rates as compared to the impact of individual attackers. However, as the rate increases beyond 250, the joint impact is significantly higher than the impact due to individual attackers. Although two attackers can have similar properties (in terms of traffic parameters) and have similar relationships with the routers on the normal flow path (in terms of carrier sense range), their impacts vary significantly due to their different positions. We also see that the impact of joint attack is not equivalent to the additive impact of individual attacks, which is true for losses at all packet rates.

*Remark 7* Another observation consistent with our intuition is that paths with more number of hops are affected much more severely as compared to paths with low hop count. Consequently, a path-based DoS attack can inflict more damage by attacking longer paths in WMNs.

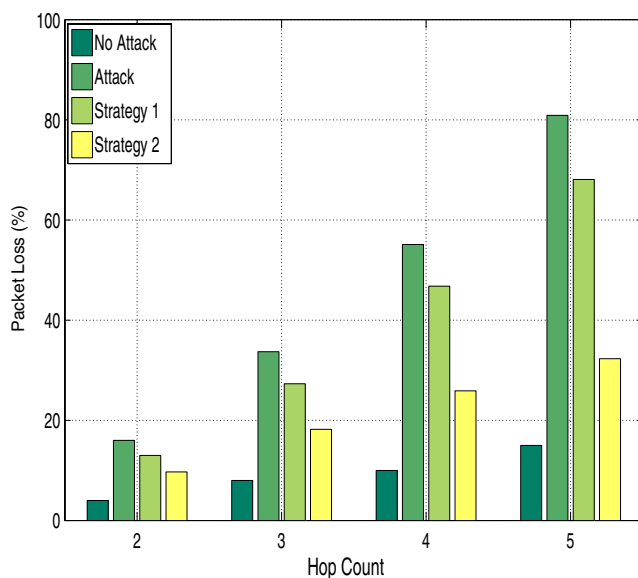
### 5.2 A simple counter strategy

We have, by far, discussed the impact of attack by changing their intensity, number of attacker, and

number of hops on the normal flows in WMNs. Now we discuss a simple strategy to lessen the impact of attacks studied above. In this strategy, a *helper node* is placed in the network in such a way that it acts as an *attacker* to the attacker node, but does not impact the normal flows. Such arrangement can easily be achieved by placing the helper node outside the interference range of routers on the normal flow path, and inside the interference range of the attacker node.

The setup and parameters associated with the attack traffic and normal traffic are similar to the previous multi-hop case. However, the attack traffic is only with 500 pps. In addition to that, a helper node is used and placed in two ways. In first case (strategy 1 in Fig. 18), the helper node is placed inside carrier sense range of the attacker node, whereas in the second case (strategy 2 in Fig. 18), the helper node is placed outside carrier sense range and within interference range of the attacker node. The traffic parameters of the helper node are similar to the attacker node. Results are presented in Fig. 18. We observe that both strategies subdue the damage caused by the attack. However, strategy 2 is much more powerful than strategy 1, as its traffic collides with the attack traffic significantly, leading to the higher reduction in packet losses for the normal flow. The second strategy lowers packet losses by more than half of the packet losses caused by the attack. Therefore, it shows that such a counter strategy can be useful in leveraging the performance of the network.

The above strategy requires knowing the precise location of the attacker, which is challenging. Although, we do not focus on finding the location of the attacker



**Fig. 18** A simple counter strategy

node in this work, we discuss a simple method to achieve that. A node is placed such that it acts as an attacker for the network, by determining the flow paths of interest and then applying the strategy on each nearby routers of the flow path. After applying the strategy on router, say  $r$ , if the performance of the flow path improves, then that router,  $r$ , should be considered as an attacker for that path. In this manner, the above strategy can be used to eliminate attackers from the network. This strategy can also be applied to the group of routers, which might act as attackers collectively for some paths in the network. Therefore, it is not necessary to use a helper node for each attacker node, as a helper node can be collectively used to attack more than one attacker node in the network.

### 5.3 Comparison with related studies

In this section, we compare our observations with the results of other works to gain better understanding.

#### 5.3.1 Comparison with experimental studies

A similar study on DoS attacks in multi-hop networks is carried out in [1]. The authors have studied the impact of JellyFish and black hole attacks on the performance of ad hoc networks. For example, authors have presented in their study that as the number of relay nodes involved in the attack increases, performance degrades faster. It is similar to our results shown in Fig. 16, where we have also shown that the collusion of attacker leads to high performance degradation. The difference is that we have also shown that the gain by collusion may not be additive of individual attackers depending upon their location.

In addition, authors have shown that the placement of the attacker nodes affects the impact of performance. It is close to our observation in Fig. 13, where we have shown that the attacker position (changed due to mobility) also affects the performance impact. Besides, authors have shown that as the number of hops increases, the performance impact is higher, similar to our observation in Fig. 17.

In the study [27], authors observed that as the distance between the attacker and legitimate nodes are increased, the impact of jamming reduces. It is similar to our observations in Fig. 16, where we also show that the attacker farther to the targeted path causes less performance degradation than the attacker closer to the targeted path. However, the difference is that the main focus of their study has been to propose novel detection algorithms, where our focus is understanding the performance impact of attacks in WMNs. Another

difference is that we have considered various scenarios, such as physical diversity, attack intensity, number of hops, and medium errors, which are not discussed in their study.

Therefore, besides some similarities, we provide some new insights too about link qualities, and impact of traffic parameters such as packet size and packet rate.

### 5.3.2 Comparison with simulation studies

Due to the complexity involved in setting up a real-time experimental testbed, a significant part of the research on multi-hop networks has been based on simulations. For example, the study of a novel system, called DOMINO, has been studied in [23]. The attack model in their work follows a non-compliant MAC protocol behavior unlike our work. Though, it may not be possible to compare our results with their results in a straight forward manner, we still discuss the similar observations. For example, they have shown that as the malicious node gets higher share of network bandwidth, the performance of the legitimate nodes decreases. It is similar to the results in Fig. 9, where we show that as the attack intensity (packet rate in this case) is increased, the performance of targeted path reduces.

A recent simulation study to prevent pollution attack in network coded WMNS is carried out in [14]. To show the impact of attack, authors have used a metric, called pollution intensity, which is the percentage of polluted packets among total packets. It is shown that as the pollution intensity increases, the throughput of the flows in WMNs degrades severely. This result is similar to our observation in Fig. 9, in which we also demonstrate the rising performance degradation with the increase in attack intensity.

Due to the differences in the attack models in this work and related studies, it is not possible to validate each and every measurements presented in this work. Nevertheless, we notice that some of our observations are similar to the results presented in other studies, and validates the accuracy of our results. We also notice that most of the existing studies have focused on detecting attacks without considering the detailed performance impact. Therefore, our results of performance impact may provide useful implications to the design of countermeasures to DoS attacks and performance evaluations.

## 6 Conclusions

We have presented a measurement-based study on the impact of path-based DoS attack in WMNs. Through

the testbed setup and traffic generation tools, we have shown how the various factors, such as attack intensity, physical diversity, link errors, collusion, and number of hops affect the impact of path-based DoS attacks on the performance of WMNs. Our results show that the attack is more effective on the path with poor links than good links. Also, a far attacker can be more dangerous than a close attacker due to physical diversity. More importantly, the hidden poor links become exposed when a path-based DoS attack is carried out because of the retransmissions at the MAC layer. Both of these factors are very conducive to the path-based DoS attacks, and lead to significant packet losses. We also observed that collusion of attackers can not yield an additive gain caused by individual attackers, and depends upon the location of the attackers. We further discussed a strategy, where a node can act as a countermeasure to an attacker, and can help subdue its damage.

## References

1. Aad I, Hubaux J-P, Knightly EW (2004) Denial of service resilience in ad hoc networks. In: Proc. of the ACM MOBICOM'04, pp 202–215
2. Aguayo D, Bicket J, Biswas S, Judd G, Morris R (2004) Link-level measurements from an 802.11b mesh network. In: Proc. of SIGCOMM'04, pp 121–132
3. Akyildiz IF, Wang X, Wang W (2005) Wireless mesh networks: a survey. *Comput Networks* 47(4):445–487
4. Bechler M, Hof H-J, Kraft D, Pählke F, Wolf L (2004) A cluster-based security architecture for ad hoc networks. In: IEEE INFOCOM'04, vol 4, pp 2393–2403
5. Bellardo J, Savage S (2003) 802.11 denial-of-service attacks: real vulnerabilities and practical solutions. In: USENIX security symposium, p 2-2
6. Bianchi G, Di Stefano A, Giaconia C, Scalia L, Terrazzino G, Tinnirello I (2007) Experimental assessment of the back-off behavior of commercial IEEE 802.11b network cards. In: Proceedings of IEEE INFOCOM'07, pp 1181–1189
7. Bicket J, Aguayo D, Biswas S, Morris R (2005) Architecture and evaluation of an unplanned 802.11b mesh network. In: Proc. of the ACM MOBICOM'05, pp 31–42
8. Bohacek S, Wang P (2007) Toward tractable computation of the capacity of multi-hop wireless networks. In: Proceedings of IEEE INFOCOM'07, pp 2099–2107
9. Brown TX, James JE, Sethi A (2006) Jamming and sensing of encrypted wireless ad hoc networks. In: ACM MobiHoc, pp 120–130
10. Toh C-K, Delwar M, Allen D (2002) Evaluating the communication performance of an ad hoc wireless network. *IEEE Trans Wirel Commun* 1(3):402–414
11. Chiang JT, Hu Y-C (2007) Cross-layer jamming detection and mitigation in wireless broadcast networks. In: ACM MobiCom, pp 346–349
12. Das SR, Perkins CE, Royer EM (2000) Performance comparison of two on-demand routing protocols for ad hoc networks. In: Proc. of the IEEE INFOCOM'00, vol 1, pp 3–12
13. Deng J, Han R, Mishra S (2005) Defending against path-based DoS attacks in wireless sensor networks. In: ACM SASN, pp 89–96

14. Dong J, Curtmola R, Nita-Rotaru C (2009) Practical defenses against pollution attacks in intra-flow network coding for wireless mesh networks. In: ACM WiSe, pp 111–122
15. Eisenman S, Campbell A (2007) E-CSMA: supporting enhanced CSMA performance in experimental sensor networks using per-neighbor transmission probability thresholds. In: Proceedings of IEEE INFOCOM'07, pp 1208–1216
16. Eriksson J, Agarwal S, Bahl P, Padhye J (2006) Feasibility study of mesh networks for all-wireless offices. In: Proceedings of ACM MOBISYS'06. Uppsala, Sweden, pp 69–82
17. Gummadi R, Wetherall D, Greenstein B, Seshan S (2007) Understanding and mitigating the impact of RF interference on 802.11 networks. ACM SIGCOMM Comput Commun Rev 37(4):385–396
18. Hu N, Li L, Mao ZM, Steenkiste P, Wang J (2005) A measurement study of internet bottlenecks. In: IEEE INFOCOM'05
19. Kashyap A, Ganguly S, Das SR (2007) A measurement-based approach to modeling link capacity in 802.11-based wireless networks. In: ACM MobiCom, pp 242–253
20. Plesse T, Adjih C, Minet P, Laouiti A, Plakoo A, Badel M, Muhlethaler P, Jacquet P, Lecomte J (2005) OLSR performance measurement in a military mobile ad-hoc network. Ad Hoc Networks 3(5):575–588
21. Hamed Mohsenian Rad A, Wong V (2007) Joint channel allocation, interface assignment and MAC design for multi-channel wireless mesh networks. In: Proceedings of IEEE INFOCOM'07, pp 1469–1477
22. Radosavac S, Moustakides G, Baras JS, Koutsopoulos I (2008) An analytic framework for modeling and detecting access layer misbehavior in wireless networks. ACM Trans Inf Syst Secur (TISSEC) 11(4):1–28
23. Raya M, Hubaux J-P, Aad I (2004) DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots. In: ACM MobiSys, pp 84–97
24. Vasan A, Ramjee R, Woo T (2005) ECHOS: enhanced capacity 802.11 hotspots. In: IEEE INFOCOM'05
25. Xu W, Trappe W, Zhang Y (2006) Channel surfing: defending wireless sensor networks from jamming and interference. In: ACM SenSys, pp 403–404
26. Xu W, Trappe W, Zhang Y (2007) Channel surfing: defending wireless sensor networks from interference. In: IPSN, pp 499–508
27. Xu W, Trappe W, Zhang Y, Wood T (2005) The feasibility of launching and detecting jamming attacks in wireless networks. In: ACM MobiHoc, pp 46–57
28. Xu W, Wood T, Trappe W, Zhang Y (2004) Channel surfing and spatial retreats: defenses against wireless denial of service. In: ACM WiSe, pp 80–89
29. Yang H, Shu J, Meng X, Lu S (2006) SCAN: self-organized network-layer security in mobile ad hoc network. IEEE J Sel Areas Commun 24(2):261–273
30. Zhai H, Fang Y (2006) Impact of routing metrics on path capacity in multirate and multihop wireless ad hoc networks. In: Proceedings of IEEE ICNP'06. Santa Barbara, CA, USA, pp 86–95
31. Zhang Y, Fang Y (2007) A secure authentication and billing architecture for wireless mesh networks. ACM Wirel Netw 13(5):663–678
32. Zhang Y, Fang Y (2006) ARSA: an attack-resilient security architecture for multihop wireless mesh networks. IEEE J Sel Areas Commun 24(10):1916–1928