



ELSEVIER

Contents lists available at ScienceDirect

## Ad Hoc Networks

journal homepage: [www.elsevier.com/locate/adhoc](http://www.elsevier.com/locate/adhoc)

## On the reliability of ad hoc routing protocols for loss-and-delay sensitive applications

Muhammad Saleem<sup>a,\*</sup>, Israr Ullah<sup>b</sup>, Syed Ali Khayam<sup>c</sup>, Muddassar Farooq<sup>b,1</sup>

<sup>a</sup> Center for Advanced Studies in Engineering Islamabad 44000, Pakistan

<sup>b</sup> Next Generation Intelligent Networks Research Center (nexGIN RC), National University of Computer and Emerging Sciences (NUCES), Islamabad 44000, Pakistan

<sup>c</sup> School of Electrical Engineering & Computer Science (SEECS) National University of Sciences & Technology (NUST) Islamabad 44000, Pakistan

### ARTICLE INFO

#### Article history:

Received 25 April 2009  
Received in revised form 6 July 2010  
Accepted 20 July 2010  
Available online xxxx

#### Keywords:

Wireless ad hoc and sensor networks  
Routing protocol  
Reliability  
Energy efficiency  
Scalability

### ABSTRACT

In this paper, we analyze the packet delivery reliability of ad hoc routing protocols for loss-and-delay sensitive applications. Since a typical flooding-based route discovery used in ad hoc routing protocols – DSR for instance – can only discover node-disjoint paths. In this context, we first show that the reliability function of such a multipath system is concave with respect to the total number of paths. Therefore, maximum steady-state reliability may be attained by routing each packet through a small set of node-disjoint paths. Subsequently, we prove that a partially-disjoint path is more reliable than a node-disjoint path. Hence, high reliability and significant energy savings may be achieved by routing a packet through fewer partially-disjoint paths. Based on these findings, we suggest modifications to flooding-based route discovery procedure to discover partially-disjoint paths. We complement our theoretical outcomes through extensive simulations. Finally, we analyze the reliability of beacon-based routing protocols and derive an upper bound on the number of hops at which a beacon should be placed to satisfy a given packet reliability constraint.

© 2010 Elsevier B.V. All rights reserved.

## 1. Introduction

Many deployment scenarios of multihop wireless networks require high transmission reliability. Transmission reliability is particularly important for mission-critical applications such as remote patient monitoring, battlefield monitoring, monitoring of disaster-struck regions, home automation, and tracking of chemical and explosive agents. These applications are loss-and-delay sensitive and therefore reliable and timely delivery of information is critical. In addition to loss-and-delay sensitivity – implying high reliability, these applications are also concerned with en-

ergy efficiency because ad hoc nodes have limited battery capacity.

In this paper, we analyze the packet delivery reliability of ad hoc routing protocols for loss-and-delay sensitive applications. In view of the above motivation, our reliability analysis is based on the following two constraints:

1. The data packets must be routed reliably to the destination node with a lower delay.
2. Energy required for reliable delivery of packets must be kept to a low value.

Retransmission of packets at the medium access control layer (MAC) is a common method used to achieve higher reliability. However, we ignore these retransmissions because they adversely affect Constraint 1.

As an alternative to retransmissions, we investigate the use of multiple simultaneous paths for delivering a data packet to its final destination by routing a copy through

\* Corresponding author. Tel.: +923215063473.

E-mail addresses: [msaleem@case.edu.pk](mailto:msaleem@case.edu.pk) (M. Saleem), [israrullahk@yahoo.com](mailto:israrullahk@yahoo.com) (I. Ullah), [ali.khayam@seecs.edu.pk](mailto:ali.khayam@seecs.edu.pk) (S.A. Khayam), [muddassar.farooq@nu.edu.pk](mailto:muddassar.farooq@nu.edu.pk) (M. Farooq).

<sup>1</sup> Tel.: +92 51 8314100.

more than one paths. In this context, we show that flooding-based ad hoc routing algorithms discover node-disjoint paths only [16]; some protocols discover a single path while others maintain multiple paths between a given (source,destination) pair. We then model the reliability of multiple node-disjoint paths and show that the reliability function is a concave function of the total number of paths. Consequently, while an initial set of paths results in an exponential increase in the reliability, addition of more paths beyond a certain threshold yields negligible improvements in the reliability. Therefore, we advocate the use of a small subset of available paths as they incur less discovery and maintenance overhead.

Routing a packet through a small set of node-disjoint paths can achieve higher packet delivery reliability and lower delay. However, it may not be an energy-efficient option. Therefore, we analyze an alternate routing mechanism in which we model and compare the reliability of partially-disjoint paths [12] with that of node-disjoint paths. We show that a partially-disjoint path is more reliable and energy-efficient than a node-disjoint path. Hence, we argue that ad hoc routing protocols should discover and maintain a small set of partially-disjoint paths rather than the conventional node-disjoint paths. Based on this outcome, we suggest modifications to a typical RREQ-based route discovery mechanism to discover partially-disjoint paths. Furthermore, to complement the reliability analysis, we compare the performance of the two variants of Dynamic Source Routing (*DSR*) protocol namely *DSR-PD* (where *PD* refers to partially-disjoint) and *DSR-FD* (where *FD* refers to fully-disjoint) through extensive simulations. The empirical results demonstrate that *DSR-PD* performs extremely well than *DSR-FD* in all assumed scenarios which is completely in agreement with the theoretical findings of this paper.

Finally, we analyze an alternate solution to enhance the packet delivery reliability by introducing high-end beacon nodes in the network [11,25]. For such beacon-based routing protocols, we derive an upper bound on the flooding distance up to which a packet may be flooded under given reliability constraints. If the number of paths between a source and a beacon node is higher, i.e. the network is dense, the packet can be flooded to a larger distance.

### 1.1. Organization of the paper

The rest of this paper is organized as follows. Section 2 briefly summarizes the previous research efforts in the area. Section 3 introduces the definitions of the terms used in the reliability analysis. A typical flooding-based route discovery and the reliability of ad hoc routing protocols with node-disjoint paths are discussed in Section 4. Comparison of partially-disjoint paths and the node-disjoint paths is explained in Section 5. Modifications to a typical flooding-based route discovery mechanism to discover partially-disjoint paths are described in Section 6. Section 7 contains the empirical evaluation of the two variants of *DSR* protocol namely *DSR-PD* and *DSR-FD*. Reliability analysis of beacon-based ad hoc routing protocols is presented in Section 8. Section 9 summarizes the key conclusions of the paper.

## 2. Related work

While hop-by-hop and end-to-end reliabilities of unicast transmissions in an ad hoc network have been investigated, reliability analysis of RREQ-based ad hoc routing protocols is largely unexplored. Gnawali et al. investigated the tradeoffs of three techniques; link layer retransmissions, blacklisting the poor quality links and the use of reliability metrics to improve the data delivery reliability in sensor networks [13]. They concluded that blacklisting of bad links or the use of reliability metrics coupled with link layer retransmissions can provide consistent high quality paths. However, they also demonstrated that blacklisting fails at low densities because it causes the network to partition.

With an argument that conventional end-to-end retransmissions are inefficient in sensor networks, Kim et al. explored alternative approaches for achieving high packet delivery reliability, e.g. link layer retransmissions, use of erasure codes, etc. [17]. They proved experimentally that link layer retransmissions, although efficient, are limited in improving reliability. On the other hand, erasure codes provided high reliability by tolerating packet losses while route fixation gracefully handled the link failures. Based on these findings, Kim et al. concluded that a right combination of these techniques can lead to substantially higher reliability.

Akan and Akyildiz [2] proposed a reliable transport protocol – event-to-sink reliable transport (ESRT) – for wireless sensor networks (WSNs). ESRT is based on the fact that a sink node is interested in the event detection only rather than individual node reports. ESRT is energy-efficient as well as capable of controlling the network congestion. Another important feature of ESRT is that the bulk of an algorithm resides on a sink node with minimum processing load on resource-constrained sensor nodes.

Bhandari and Vaidya investigated the problem of reliable broadcast in wireless networks by assuming a perfectly reliable channel and MAC layer in [5]. By considering that nodes can fail with certain probability  $p$ , they derived expressions for critical node degree for a reliable broadcast. Wan et al. proposed a transport layer solution, pump-slowly fetch-quickly (PSFQ), for WSNs which is customizable for different applications [26]. PSFQ is simple and scalable with minimum signaling overhead. An interesting characteristic of PSFQ is its ability to perform well in highly erroneous network environment. Saleem et al. has proposed a mathematical evaluation framework to model the two key metrics of ad hoc routing algorithms; routing overhead and routing optimality [22]. After validating the models through simulations, the authors also proved that the framework can easily be adapted to develop protocol specific routing overhead and route optimality models. Lee et al. analyzed the aging process of a sensor network [15]. They proved that connection probability to a sink node decreases exponentially with the hop level. In addition, the authors of [15] also showed that an increase in the node density, while keeping the radio transmission range to a fixed value, does not affect the network disconnection time.

Kumar et al. [18] combined erasure coding with a probabilistic broadcast technique to improve the reliability of WSNs for information dissemination. Chieh and Robertazzi [8] studied the effect of node density and transmission power on the broadcast percolation in multihop wireless networks. Santivanez et al. [24] performed a scalability analysis of a number of ad hoc routing algorithms. They defined a scalability factor for ad hoc routing protocols in terms of total overhead and minimum traffic load. Their analysis showed that plain flooding (PF) algorithm scales better in high mobility scenarios where as hazy sighted link state (HSLs) [23] scales with the size of the network. Zhou and Abouzeid [28] used information theory to derive lower bounds on the average size of a control packet and the memory required to store the routing information gathered by an hierarchical proactive routing protocol. They also analyzed the scalability of memory requirements and routing overhead with the network and cluster size. Heusse et al. [14] analyzed the performance anomaly of 802.11b [1]. The authors have shown that if few nodes operate at a lower bandwidth, the performance of the entire network degrades. None of the above studies investigate the reliability of RREQ-based ad hoc routing protocols which is the prime motivation of this work.

### 3. System description and definitions

#### 3.1. System description

We consider an ad hoc network in which nodes are distributed randomly on a two-dimensional plane. The resultant network is connected and all the links – or edges – are symmetric. We assume a CSMA/CA-based MAC layer protocol for contention resolution. Even in the case of no contention, we account for the possibility that a packet may get lost due to channel errors, e.g. attenuation, fading, interference, thermal noise, etc. We also assume that there is no transport layer protocol to provide additional data delivery reliability.

#### 3.2. Definitions

In this section, we provide formal definitions of the key concepts/terms used in the paper.

**Definition 1.** RREQ flooding is the process in which each node in an ad hoc network, except the destination, broadcasts the first received copy of a route request (RREQ) packet to its neighbors.

Another relevant term in this context is the flooding distance.

**Definition 2.** The total number of hops between a (source,destination) pair is the flooding distance of that path.

A shortest path, therefore, has the minimum flooding distance.

**Definition 3.** Average node degree,  $d_{avg}$ , refers to the average number of neighbors of a node.

We emphasize here that a RREQ broadcast may or may not be received by all the neighbors of the broadcasting node. To incorporate packet loss in the route discovery model, we define the following term.

**Definition 4.** Packet forwarding probability ( $p_f$ ) is the probability that a packet forwarded on a link will be delivered successfully to a next hop node.

For generality, we define packet forwarding probability as the product of two probabilities:

$$p_f = \overline{p_c} \overline{p_e}, \quad (1)$$

where  $\overline{p_c}$  is the probability that a packet forwarded on a link will not experience a collision at the MAC layer and  $\overline{p_e}$  is the probability that the packet is not lost due to channel errors. We provide expressions for computing  $\overline{p_c}$  as well as  $\overline{p_e}$  in Section 4.

**Definition 5.** Node-disjoint paths refer to the paths between a given (source,destination) pair which do not contain any overlapping node(s).

**Definition 6.** Partially-disjoint paths are the paths between a (source,destination) pair with one or more overlapping nodes.

Fig. 1 shows an example of a node-disjoint and a partially-disjoint path.

**Definition 7.** An optimal route is a route of minimum flooding distance.

**Definition 8.** An  $n$ -suboptimal route between a (source,destination) pair is a route of length  $t+n$  hops, where  $t$  is the optimal length and  $n = 1, 2, \dots$

### 4. Packet delivery reliability of ad hoc routing protocols

Flooding is the most common technique used by on-demand ad hoc routing protocols for route discovery [3,29]. Such a route discovery mechanism can discover node-disjoint paths only. We elaborate this argument with reference to the route discovery process used in several prominent ad hoc routing protocols e.g., Ad hoc On-demand Distance Vector (AODV) routing protocol [20], DSR [16], BeeSensor [30].

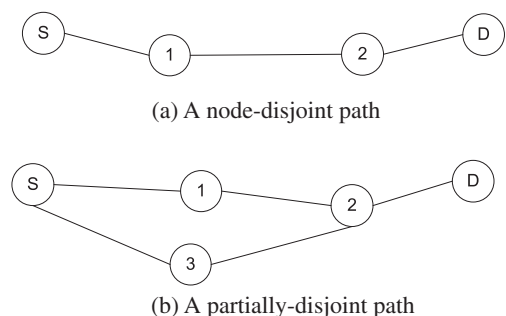


Fig. 1. Example of a node-disjoint and a partially-disjoint path.

Fig. 2 gives an illustration of this process. A source node *S* initiates the route discovery by broadcasting a route request (RREQ) message to all its neighbors. The receiving nodes broadcast the first unique copy of RREQ to their neighbors and the process continues. Nodes may receive multiple copies of RREQ as all of their neighbors are expected to broadcast at least (as well as at-most) once. However, since nodes do not forward multiple RREQs, the duplicates are discarded. Therefore, intermediate nodes maintain a single reverse link entry in their routing table/RREQ cache. When such an intermediate node receives a route reply (RREP), it forwards the RREP along the reverse link and flushes the RREQ cache entry. Consequently, future RREPs are not entertained at this node.

As an example of this behavior, consider node 3 in Fig. 2 to which node 4 forwards a RREP. Node 3 will either forward the reply to node 2 or node 5 depending upon its reverse link entry. Once node 3 forwards this reply to one of these two nodes (node 2 in this case – see Fig. 2), it becomes part of a route connecting node *S* and node *D*. Since it will discard the future RREPs, it cannot be a part of another route connecting the same (source,destination) pair. For example, if node 6 forwards a RREP to node 3, it will be discarded. Consequently, link between node 3 and node 6 will not be discovered.

This can also be verified through Fig. 3 which shows the links that are not likely to be discovered in the route discovery process. For instance, link between node *H* and *E* can only be discovered if node *E* maintains two reverse links, one leading to node *S* and the other leading to node *H*. This is possible if node *E* broadcasts two copies of RREQ received from *S* and *H* and keeps their corresponding records. This contradicts the definition of flooding. Therefore, node *E* lies on a single route only.

In the following subsections, we first develop the reliability model of such a RREQ-based ad hoc routing protocol. We then derive expressions for the probability of zero collisions  $\bar{p}_c$  and zero channel error  $\bar{p}_e$ . We conclude

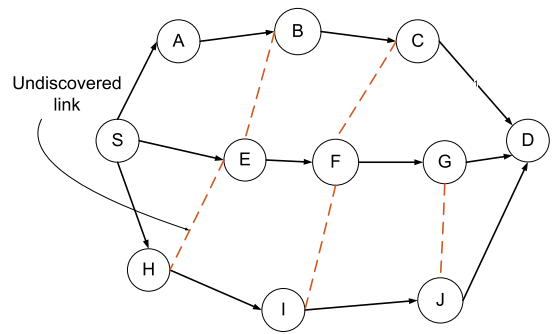


Fig. 3. Source *S* connected with destination *D* through multiple node-disjoint paths (*S-A-B-C-D*, *S-E-F-G-D* and *S-H-I-J-D*).

this section by discussing the practical significance of the proposed reliability model.

#### 4.1. Reliability model

A network is said to be *connected* if every pair of nodes is connected through at least one path. Let us assume that the minimum flooding distance between a source node *S* and a destination node *D* is *t*. A packet sent by node *S* must traverse all the *t* links before being delivered to node *D*. Therefore, the reliability  $R_s(p_f, t)$  of such a single path routing protocol is given by

$$R_s(p_f, t) = (p_f)^t. \tag{2}$$

Clearly, and as can be intuitively argued, the reliability that a packet would be delivered to node *D* decreases as *t* increases. As a result, protocols that maintain a single path between a (source,destination) pair, e.g. AODV, cannot ensure a packet delivery at large flooding distances.

A common solution to this problem is to maintain multiple node-disjoint paths between a (source,destination)

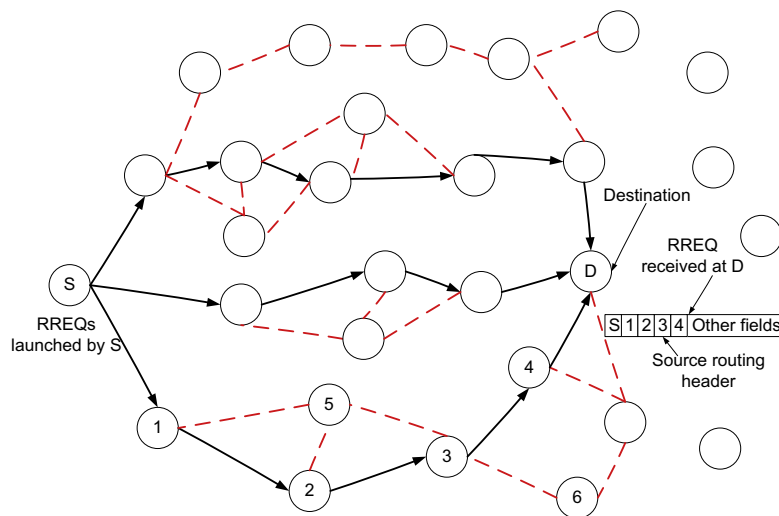


Fig. 2. An illustration of flooding-based route discovery in ad hoc networks to discover node-disjoint paths. Solid lines show the links which shall be discovered while red-and-dashed lines represents undiscovered links. A RREQ received at *D* with the source routing header (as in DSR) is also shown to further elaborate the process.

pair [7,10,16]. Such a strategy in essence trades off routing efficiency – measured in terms of the routing overhead – for higher packet delivery reliability. The packet delivery reliability of a protocol that maintains  $m$  node-disjoint paths between a (source,destination) pair is:

$$R_p(m, p_f, t) = 1 - (1 - p_f^t)^m \quad (3)$$

The above expression assumes that all the paths connecting  $S$  and  $D$  have the same minimum flooding distance  $t$ . In other words, all discovered paths are assumed to be optimal. While this assumption is unrealistic, it allows us to quantify the *best-case* reliability of a multipath ad hoc routing protocol.

Fig. 4 plots the packet delivery reliability – Eq. (3) – against an increasing number of redundant paths  $m$ . Note that an increase in the value of  $m$  does not always result in a proportional increase in the packet delivery reliability. In fact, addition of the first few paths results in an exponential increase in the reliability which then reaches a saturation point after which the curve flattens. In other words,  $R_p(m, p_f, t)$  is concave with respect to  $m$ ; see Appendix A.1 for the mathematical proof. Therefore, addition of redundant paths beyond a certain threshold will simply increase the route discovery and maintenance overhead without providing a proportional dividend in terms of packet delivery reliability. We also derive bounds on  $R_p(m, p_f, t)$  in Appendix A.2.

It can also be observed from Fig. 4 that for higher values of  $p_f$ , saturation point is achieved with significantly less number of paths. For instance, for  $p_f = 0.85$  and  $t = 8$ , the steady state is achieved at  $m = 15$ . In comparison, for  $p_f = 0.95$  and  $t = 8$ , the steady state occurs at  $m = 5$ . It leads to an important result of this model. If we are able to minimize the number of collisions and channel errors to increase  $p_f$  – Eq. (1) – we can attain a significantly higher reliability by maintaining fewer node-disjoint paths. Furthermore, the discovery and maintenance overhead will also decrease accordingly.

#### 4.2. Collision and channel error modeling

We express the packet forwarding probability  $p_f$  as the product of  $\bar{p}_c$  and  $\bar{p}_e$  – Eq. (1). Therefore, in this section, we derive expressions for these two probabilities for the sake of completeness.

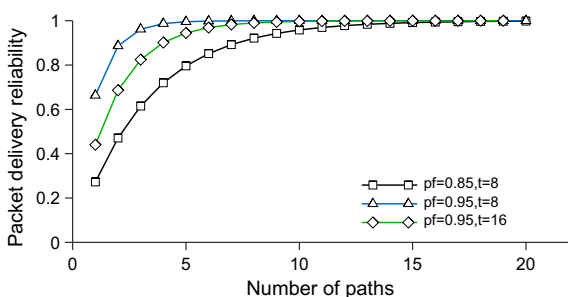


Fig. 4. Packet delivery reliability with multiple node-disjoint paths.

#### 4.2.1. Collision modeling

As mentioned in Section 3, we assume CSMA/CA MAC layer protocol in the proposed reliability model. Therefore, our collision model inherently assumes that a node never retransmits any data packet. In addition to this, we also assume that every node in the network has always a packet to send. Consequently, nodes contending for the channel access always find the channel busy in the first attempt. In such a busy network, probability of no collision  $\bar{p}_c$  is given by

$$\bar{p}_c = \left(1 - \frac{1}{CW_{min}}\right)^{d_{avg}-1}, \quad (4)$$

where  $CW_{min}$  (=31 as defined in 802.11b standard) is the minimum contention window and  $d_{avg}$  is the average degree of a node. For dense networks,  $d_{avg}$  will be high leading to lower value of  $\bar{p}_c$ .

#### 4.2.2. SNR-based channel error modeling

Log-normal shadow fading is a commonly used physical layer channel model for wireless networks. Under this scheme, the physical channel is modeled in terms of two additive components: (1) a deterministic distance-dependent attenuation component with a path-loss exponent  $\alpha$ , and (2) a SNR-based fading component defined as a normal random variable with a zero mean and variance  $\sigma^2$ . Now, the probability of a packet loss between a pair of communicating nodes on the channel – as given in [4] – is:

$$\bar{p}_e = 1 - \frac{1}{2} + \frac{1}{2} \operatorname{erf}\left(\frac{\beta_{th} - \alpha \times 10 \log(z)}{\sqrt{2}\sigma}\right), \quad (5)$$

where  $\operatorname{erf}(\cdot)$  is the standard error function,  $z$  is the distance between the two nodes and  $\beta_{th}$  is the lowest threshold attenuation which is required to deliver a packet between the nodes.

#### 4.3. Practical significance of the reliability model

A simple comparison of (2) and (3) shows that single path ad hoc routing protocols have less packet delivery reliability than multipath protocols. Ad hoc routing protocols, in general, route a packet through a single path and rely on an explicit transport protocol for reliable packet delivery. For instance, if a packet is not delivered to the final destination, it is retransmitted along another path. As we are focusing on delay-and-loss sensitive applications, reliability achieved through retransmissions is not suitable because it adds to the overall packet latency. Therefore, we use multiple node-disjoint paths in a rather unconventional manner as described in the following.

To minimize the routing delay and maximize the packet delivery reliability, we suggest that a copy of the packet must be sent through multiple node-disjoint paths. There are some sensor networks routing protocols that are based on this idea [9] [27]. As reliability function – Eq. (3) – is concave with respect to  $m$ , we do not need to route a packet along all the available paths. Rather, a subset of the paths can serve the stated objectives. The problem with this approach is that it may not be an energy-efficient alternative. Therefore, we need to reduce the total number of paths along which a packet must be sent to gain high reliability.

The results of this section lead to a critical question: *What is the minimum number of paths  $m_{min}$  that will allow us to achieve the steady-state reliability?* We address this question in the following sections.

### 5. Improving packet delivery reliability using partially-disjoint paths

We propose to improve the reliability of a path by adding node or edge level redundancy. The resulting path is partially-disjoint – the concept of partially-disjoint paths already exists in ad hoc routing literature [12][19]. A partially-disjoint path provides parallel links through which a packet can be forwarded to a next hop node. For instance, node 2 in Fig. 1b can receive a copy of packet either from node 1 or node 3. Consequently, it is more reliable than a node-disjoint path shown in Fig. 1a. The reliability of a partially-disjoint path increases as more redundant links are added.

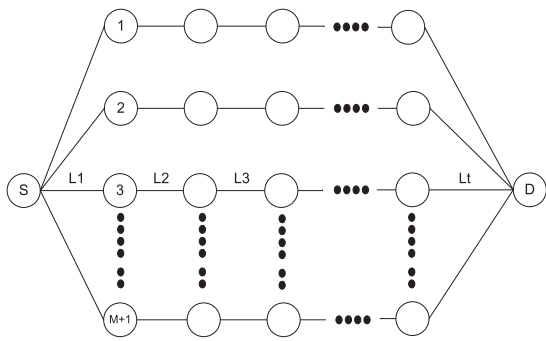
In this section, we compare the reliability of multiple node-disjoint paths with that of partially-disjoint paths and prove that the later are more reliable than the former. Consequently, the required reliability level can be achieved through fewer partially-disjoint paths.

#### 5.1. Reliability of a partially-disjoint path

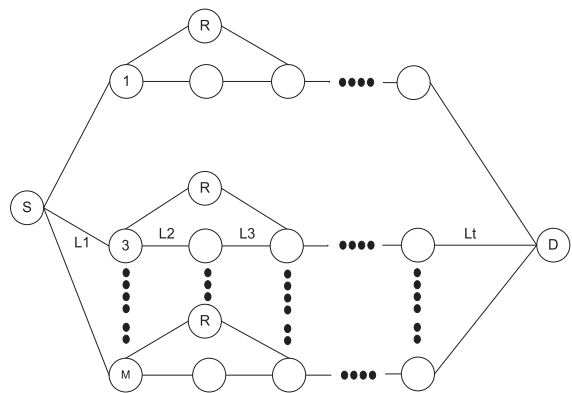
To compare the reliabilities of node-disjoint and partially-disjoint paths, we consider two cases. In the first case, a pair of nodes,  $S$  and  $D$ , is connected through  $m + 1$  node-disjoint paths each with the minimum flooding distance  $t$  – Fig. 5a. In the second case, the same pair of nodes are linked through  $m$  partially-disjoint paths – Fig. 5b. Nodes labeled  $R$  provide node/edge level redundancy. This leads us to the following lemma.

**Lemma 1.** *The reliability of  $m$  partially-disjoint paths is higher than  $m + 1$  node-disjoint paths.*

**Proof 1.** Recall that  $p_f$  is the packet forwarding probability on a link. Then, the reliability of  $m + 1$  node-disjoint paths, using (3), may be written as



(a)  $m + 1$  node-disjoint  $S \rightarrow D$  paths



(b)  $m$  partially-disjoint  $S \rightarrow D$  paths

**Fig. 5.** A pair of nodes, separated by flooding distance  $t$ , linked through a set of node-disjoint/partially-disjoint paths.

$$R_{ND}(m, p_f, t) = 1 - (1 - \epsilon)^{m+1}, \quad (6)$$

where  $\epsilon = p_f^t$ . To model the reliability of  $m$  partially-disjoint paths, we first find the reliability of a single partially-disjoint path and then combine the reliabilities of  $m$  paths using (3). Now, the reliability of a partially-disjoint path of  $t$  hops long  $r_{pd}(m, p_f, t)$  is given by

$$r_{pd}(m, p_f, t) = \beta \epsilon, \quad (7)$$

where  $\beta = t(1 - p_f) + 1$  which is always greater than 1. Now the overall reliability of  $m$  partially-disjoint paths using (3) and (7) is

$$R_{PD}(m, p_f, t) = 1 - (1 - \beta \epsilon)^m. \quad (8)$$

Comparing (6) and (8), we observe that  $\epsilon \leq \beta \epsilon$  (where  $0 \leq \epsilon, \beta \epsilon \leq 1$ ) because  $\beta > 1$ . This leads to  $(1 - \epsilon)^m \geq (1 - \beta \epsilon)^m$ . Thus we can write,

$$(1 - \epsilon)^{m+1} \geq (1 - \beta \epsilon)^m,$$

since  $(1 - \epsilon)^{m+1} = (1 - \epsilon)^m - \epsilon(1 - \epsilon)^m$  and the difference between  $(1 - \epsilon)^m$  and  $(1 - \beta \epsilon)^m$  approximately equals  $m\epsilon(\beta - 1)$  which is greater than  $\epsilon(1 - \epsilon)^m$ . Hence,

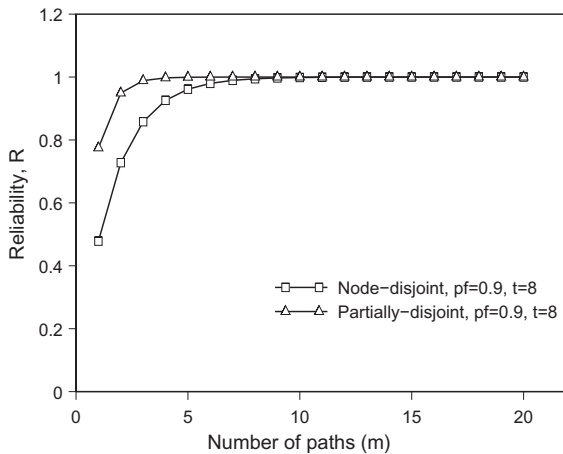
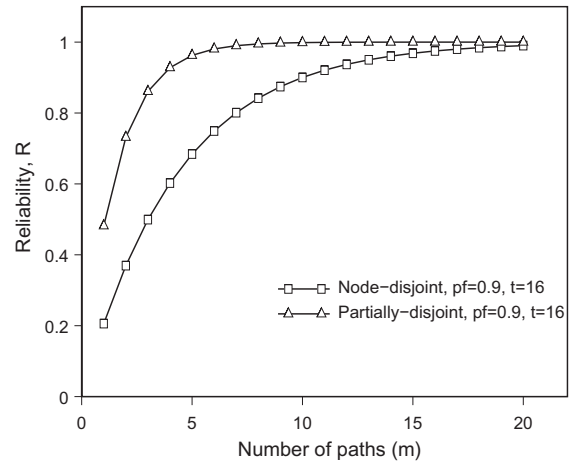
$$R_{PD}(m, p_f, t) \geq R_{ND}(m, p_f, t), \quad (9)$$

which proves the lemma.  $\square$

Lemma 1 clearly leads to the conclusion that partially-disjoint paths are more reliable thereby providing a viable alternative to node-disjoint paths. We present a detailed discussion on the practical aspects of this finding in the following subsection.

#### 5.2. Discussion

To elaborate the reliabilities achieved by a set of node-disjoint paths and partially-disjoint paths, we plot (6) and (8) for different combinations of packet forwarding probabilities  $p_f$  and flooding distance  $t$ . The results are shown in Fig. 6. The reliability curves lead to two important results. First, for the same number of paths  $m$ , reliability of partially-disjoint paths is significantly higher than that of node-disjoint paths. Consequently, reliability curve of partially-disjoint paths saturates with

(a) Reliability curves at  $p_f = 0.9, t = 8$ .(b) Reliability curves at  $p_f = 0.9, t = 16$ .**Fig. 6.** Reliability comparison of node-disjoint and partially-disjoint paths.

few number of paths. Second, Fig. 6b shows that, for longer paths, partially-disjoint paths attain higher reliability than node-disjoint paths. Therefore, partially-disjoint paths scale better with an increase in the flooding distance.

In the next phase, we compute the total number of transmissions required to deliver a packet to its final destination at a desired reliability level. Results shown in Table 1 compare the number of paths and the corresponding transmissions required for both types of paths. It is interesting to note that a single partially-disjoint path can deliver a packet with higher reliability and lower number of transmissions. For longer paths, the number of transmissions required in case of node-disjoint paths is substantially higher than that of partially-disjoint paths. For instance, for  $p_f = 0.9$  and  $t = 8$ , transmissions required to deliver a packet with reliability of 0.99 are almost 2.5 times higher than that of node-disjoint paths. Therefore, we conclude that partially-disjoint paths are more reliable, scalable and energy-efficient than node-disjoint paths. Consequently, even in case of conventional routing schemes – single path routing relying on MAC/transport layer for higher reliability – use of partially-disjoint paths can be instrumental in improving a protocol performance over a large operational landscape.

Bounds on the latency of a data packet is a critical parameter for delay sensitive applications. Therefore, in

the following subsection, we derive an upper bound on the packet latency which will conclude this section.

### 5.3. Latency bounds

Latency is commonly defined as the difference in time when a data packet is generated at a source node and when it got delivered at the destination node. We compute the packet latency in terms of contention time which represents the time for which a packet has to wait at the MAC layer in order to get the channel access. Recall that we assume CSMA/CA as a MAC layer protocol. Therefore, we proceed with the same assumption as used in the derivation of  $\bar{p}_c$  – Section 4. Since data packets are never retransmitted, contention time  $t_{cont}$  is given by

$$t_{cont} = \frac{SLOT \times \bar{p}_c \times CW_{min}}{2}, \quad (10)$$

where  $SLOT$  ( $=20 \mu s$  for 802.11b standard) is the duration of a wait slot. For a given network, all variables in (10) are constants ( $d_{avg}, CW_{min}, SLOT$ ) and hence a node experiences a constant delay to get the channel access. Now assuming a path length of  $t$  hops, one way packet latency equals  $t \times t_{cont}$  which really is the case when a route to the destination exists. However, if no route is available, a packet may have to wait till a new route is discovered. Therefore, the worst case latency of a data packet  $L_p$  equals

**Table 1**

Total transmissions required to route a packet at a desired reliability level.

Values of $p_f$ and $t$	Node-disjoint paths			Partially-disjoint paths		
	No. of paths (m)	Reliability $R_{ND}$	Transmissions ( $m \times t$ )	No. of paths (m)	Reliability $R_{PD}$	Transmissions ( $m \times (t + 2)$ )
$p_f = 0.9, t = 8$	2	0.73	16	1	0.78	10
	4	0.93	32	2	0.95	20
	8	0.995	64	4	0.997	40
$p_f = 0.9, t = 16$	2	0.37	32	1	0.48	18
	10	0.9	176	4	0.93	72
	20	0.99	320	7	0.99	126

$$L_p \leq 3 \times \left( \frac{SLOT \times \bar{p}_c \times CW_{min}}{2} \right), \quad (11)$$

Eq. (11) does not contain packet processing delay because it is a system dependent parameter. This concludes our discussion on the reliability of partially-disjoint paths.

Since flooding-based route discovery mechanism is only able to find node-disjoint paths, in the next section, we suggest modifications to this method to discover partially-disjoint paths.

## 6. Discovering partially-disjoint paths in ad hoc routing protocols

We have already discussed the basic route discovery mechanism in Section 4. Therefore, in this section, we only describe modifications to the process to realize partially-disjoint paths.

### 6.1. Modifications to route request (RREQ)

To discover partially-disjoint paths, an ad hoc routing protocol needs to keep a record of three additional parameters at intermediate nodes: (1) number of RREQs received by a node with minimum hop count  $Drreq$ , (2) *terminal node*, and (3) minimum hop count  $mhops$ . Terminal node refers to a node located at two hops from the current node. For instance, in Fig. 1b, node  $S$  is the terminal node for node 2. This information is contained within a RREQ. When an intermediate node  $i$  receives a unique RREQ from node  $j$ , identified by the  $\langle rreq\ ID, source\ node\ ID \rangle$  pair, it updates the RREQ cache as before. Additionally,  $Drreq$  (duplicate RREQs) is initialized to zero and  $mhops$  field is set to the hops carried by the RREQ after incrementing it by one. Finally, terminal node entry in RREQ cache is set to node  $j$ . After updating the cache, node  $i$  inserts node  $j$  in the RREQ (it will be a terminal node for the receiving node) and broadcasts it to its neighbors.

If node  $i$  receives a duplicate RREQ, it compares the number of hops traveled by the new RREQ with the one available in its cache. If the hops traveled by new RREQ is less than the current value, node  $i$  replaces the old cache information with the new one with  $Drreq$  field reset to 0. If both values are equal, node  $i$  only increments the  $Drreq$  field and discards the RREQ. If the number of hops traveled by the new RREQ is higher, the new RREQ is discarded without any further processing.

### 6.2. Modifications to route reply (RREP)

Let the reverse link entry maintained at an intermediate node be termed as *PrevHop*. A RREP packet, in addition to a *next hop* field, contains a *terminal node* field and an *adjacent node* fields. The terminal node normally contains 0 or valid node ID. When a node receives a RREP packet, it checks the value of  $Drreq$  field in its cache. If  $Drreq$  is greater than zero, *terminal node* field in the RREP is set to the entry maintained in cache, *adjacent node* entry is set to *PrevHop* and *next hop* is set to the broadcast address. After updating the routing table, the node broadcasts the RREP. If  $Drreq$  is zero, *next hop*, *adjacent node* and *terminal node* field are

all set to *PrevHop*. The node then unicasts the RREP to the *next hop* after updating its routing table.

When neighbors receive the broadcast RREP, they are bound to forward this RREP to the *terminal node* after updating their local routing table. *Terminal node* may receive more than one replies but it only maintains two forward links, one to the *adjacent node* and the other to a randomly selected node. Once the terminal node detects that it has discovered a redundant node on the path, it may stop further redundant node discoveries on the path by setting terminal node entry in the RREP to a negative value before forwarding it to its *PrevHop*.

Fig. 2 provides a pictorial representation of the modified route discovery process. Here node 3 receives two RREQs, from node 2 and node 5, and rebroadcasts the RREQ received earlier. Next duplicate RREQ increments the  $Drreq$  field. When node 4 forwards a reply back to node 3, it sets node 1 – assuming that node 3 forwarded the RREQ received from node 2 – as the *terminal node* and node 2 as adjacent node and broadcasts the RREP. When node 5 receives this reply, it updates its routing table and unicasts the reply to node 1 and so does node 2. We can improve this mechanism even further to add more redundancy at the node level by setting up a counter in the RREP field which may be decremented once a redundant node is discovered.

In the following section, we use this technique for the discovery of partially-disjoint paths in DSR protocol and compare its performance with a protocol that uses node-disjoint paths.

## 7. Empirical validation of the reliability models

Theoretical models are generally based on some simplifying assumptions. Therefore, it is compulsory to support the outcome of this analysis through simulation studies. We used *ns-2* simulator for this purpose. The major objective of this empirical study is to show that a protocol using partially-disjoint paths is more reliable and energy-efficient. Therefore, it is suitable for loss-and-delay sensitive applications. Ideally, one would like to analyze the impact of node-disjoint paths/partially-disjoint paths only. This in turn requires that other protocol parameters/characteristics must be identical in each case. Therefore, we opted to go for a single protocol and developed its two different variants.

We selected a prominent MANET routing protocol, DSR [16], for this purpose. Selection of DSR is mainly driven by the fact that, by default, it is a multipath routing protocol which discovers node-disjoint paths only (see Section 4). Therefore, to develop its first variant, the only major modification in the *ns-2* implementation of DSR protocol is to modify its routing functionality so that it routes a copy of packet through all discovered paths. We call it *DSR-FD* where FD stands for fully-disjoint. In the second variant, we modified the route discovery process of DSR – as described in Section 5 – so that it discovers multiple partially-disjoint paths. We then modified its routing functionality – like *DSR-FD* – such that a copy of data

packet is sent along each partially-disjoint path. We call it *DSR-PD* where PD stands for partially-disjoint.

Recall our assumption in Section 3 that underlying medium access control (MAC) layer does not provide any reliability guarantees. It is simply a best-effort MAC protocol. To simulate this functionality, we modified the code of 802.11 MAC layer available in *ns-2* simulator. We disabled RTS/CTS and Data/ACK mechanisms. Consequently, the data packets are never retransmitted at the MAC layer. In all our experiments, we assume that the nodes are deployed randomly in an area of 1500 m × 300 m. The transmission range of each node is set to 250 m while the size of each data packet is 512 bytes. The movement pattern is characterized by random waypoint mobility model in which every node moves to a random destination with a given speed. After reaching the destination, it stops there for 50 s and then moves to a next random location. We do not use TCP sources primarily because it modifies the network conditions – packet sending rate for instance – under different network conditions preventing a direct comparison of the protocols [6]. UDP provides a fair environment in which candidate protocols can be evaluated under identical network conditions. We used CBR traffic model in which sources generate packets at the prescribed rate.

Our empirical analysis is based on three evaluation metrics; packet delivery ratio, latency and average used energy. We collect the values of these metrics in four different experiments. The details of simulation parameters used in each case are listed in Table 2. Each experiment is performed for a duration of 500 s and the reported values are an average of 10 independent runs. We now provide formal definitions of the evaluation metrics – in the following subsection – before switching to the description of simulation results.

### 7.1. Definitions of the evaluation metrics

**Latency.** It is defined as the difference between the time of reception of a packet at a destination node and the time of generation of the packet at the source node. We report the average value of all packet latencies.

**Packet delivery ratio.** We define it as the ratio of the total number of packets received at all destinations to the number of packets generated at all the source nodes.

**Average used energy.** It refers to the amount of energy consumed in successful delivery of a data packet to its final destination. We report it in Joules/packet.

### 7.2. Discussion on results

#### 7.2.1. Packet delivery ratio

Packet delivery ratios of the two protocols in each of the four experiments are shown in Fig. 7. The results clearly show that *DSR-PD* performs much better than *DSR-FD* in all the assumed scenarios. Fig. 7a shows that, in case of static network, packet delivery ratio of *DSR-PD* is close to the maximum possible value. However, *DSR-FD* has significantly smaller packet delivery ratio even in the simplest scenario. As the speed goes higher, performance of both

**Table 2**  
Simulation parameters.

Experiment No.	Variable Parameter	Parameter values			
		Speed (m/s)	No. of flows	Pkt. sending rate	Network size
1	Speed	0–20	2	2	100
2	No. flows	10	2–8	2	100
3	Network size	10	2	2	50–200
4	Packet sending rate	10	2	2–8	100

the protocols degrades which is expected as the network topology changes rapidly.

Fig. 7b and d shows the performance of *DSR-PD* under high traffic loads. As the number of flows rises, the performance of *DSR-PD* degrades which primarily is due to an increase in the number collisions in the network. Recall that we do not allow retransmissions at the MAC layer which ultimately results in the packet loss. In all these experiments, the number of paths maintained by a source in *DSR-FD* – on average – is four. However, source nodes in *DSR-PD* only maintain two paths and achieve reliability through redundant edges on a path. Therefore, we can improve the reliability of *DSR-PD* by replicating more than one edges on a path. We did not demonstrate it here in order to remain consistent with our theoretical study. Another important observation is decrease in the packet delivery ratio with an increase in the network size (Fig. 7c). An increase in the network size leads to an increase in the node density, i.e. higher average node degree  $d_{avg}$ . This ultimately leads to more collisions and packet loss. It can also be inferred from (4).

#### 7.2.2. Packet latency

Latencies of both the protocols in different sets of experiments are shown in Fig. 8. The results are extremely convincing in which *DSR-PD* simply outperforms *DSR-FD* in all the cases. As the node speed rises, the latencies of both the protocols increase as well. Under high traffic loads, Fig. 8b, contention at the MAC layer increases thereby resulting in higher packet latency. A similar argument holds for the results shown in Fig. 8c.

It is however interesting to note that with an initial increase in the packet sending rate, latencies of both the protocols drop sharply and then flatten. This is rather unusual behavior and needs some explanation. With higher packet sending rate, the route breaks are detected more rapidly resulting in quick rediscovery of the fresh paths. This argument is also supported by the results shown in Fig. 7d in which packet delivery ratio does not fall sharply as the packet sending rate is increased. However, the effect is more obvious in the early stage which then decays when the packet sending rate reaches a certain threshold value.

#### 7.2.3. Average used energy

Average used energy for the two protocols is shown in Fig. 9. The trend is identical to the results shown earlier. Remember that average used energy depends upon two parameters. First, it depends upon the number of packets

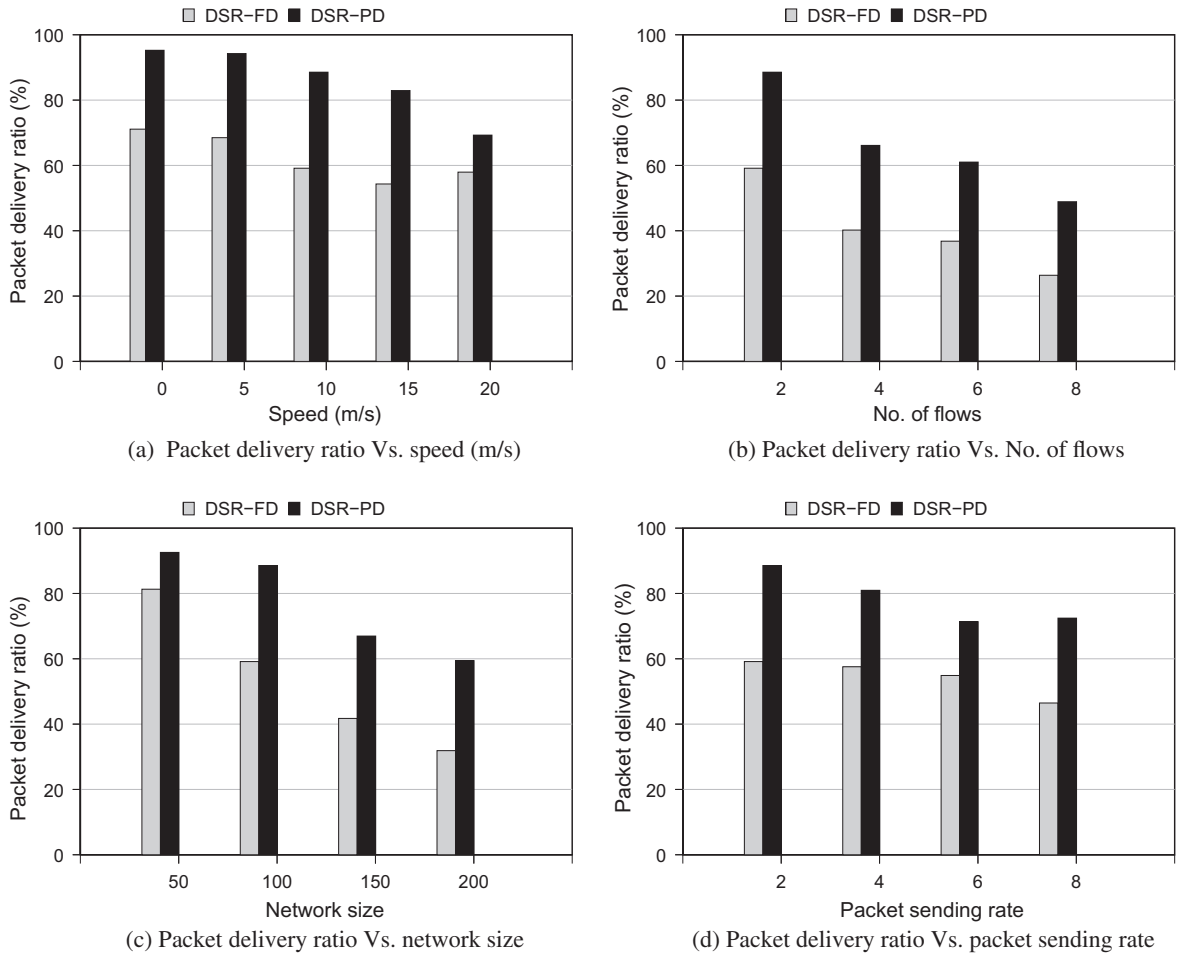


Fig. 7. Packet delivery ratios of *DSR-PD* and *DSR-FD* against speed, number of flows, network size and packet sending rate.

delivered successfully. Second, it also depends upon the total energy consumed by a protocol. As *DSR-PD* has higher packet delivery ratio in all assumed scenarios, it also results in less amount of average used energy. We also argued earlier that *DSR-FD* maintains a rather bigger set of node-disjoint paths leading to high energy consumption. In addition to this, lower packet delivery ratio of *DSR-FD* may also lead to the activation of repeated route discovery procedures. Consequently, it fails to perform well in this metric as well. We would also like to mention here that choice of a specific protocol – *DSR/AODV* – will not affect the aforementioned theoretical/empirical outcomes.

In this section and the preceding sections, we identified and evaluated mechanisms to achieve higher packet delivery reliabilities in a homogeneous ad hoc network. However, many ad hoc deployment scenarios are heterogeneous containing nodes with high energy, range and processing capabilities. For instance, vehicular ad hoc networks will be deployed with regularly-spaced info-stations. Most sensor network deployments employ beacon nodes which have higher transmission ranges and energies. In the following section, we analyze the reliability of such a beacon-based ad hoc routing.

## 8. Beacon-based flooding in large-scale ad hoc networks

Flooding is considered as one of the most reliable and robust packet delivery mechanism. However, the reliability of a flooding-based packet delivery system is

$$R_f(p_f) = p_f^h (N_{opt} + N_1 p_f + N_2 p_f^2 + \dots + N_n p_f^n), \quad (12)$$

where  $N_{opt}, N_1, N_2, \dots, N_n$  are the number of optimal paths (shortest path), 1-suboptimal paths, 2-suboptimal and  $n$ -suboptimal paths and  $h$  is the minimum flooding distance between a  $\langle$ source,destination $\rangle$  pair. As can be intuitively argued, as  $h \rightarrow \infty$ ,  $R_f(p_f) \rightarrow 0$ , irrespective of the network density.

A viable solution to this problem is to use long-haul nodes or *beacons*; see for instance [11,25] that partition a large network into small regions using beacons. The use of beacon nodes is illustrated in Fig. 10. The ad hoc network is divided into a number of small regions. Each region is equipped with a beacon node which is capable of communicating with the other distant beacon nodes using different signal strengths and frequencies. The purpose of beacons is to maintain a list of neighboring nodes and

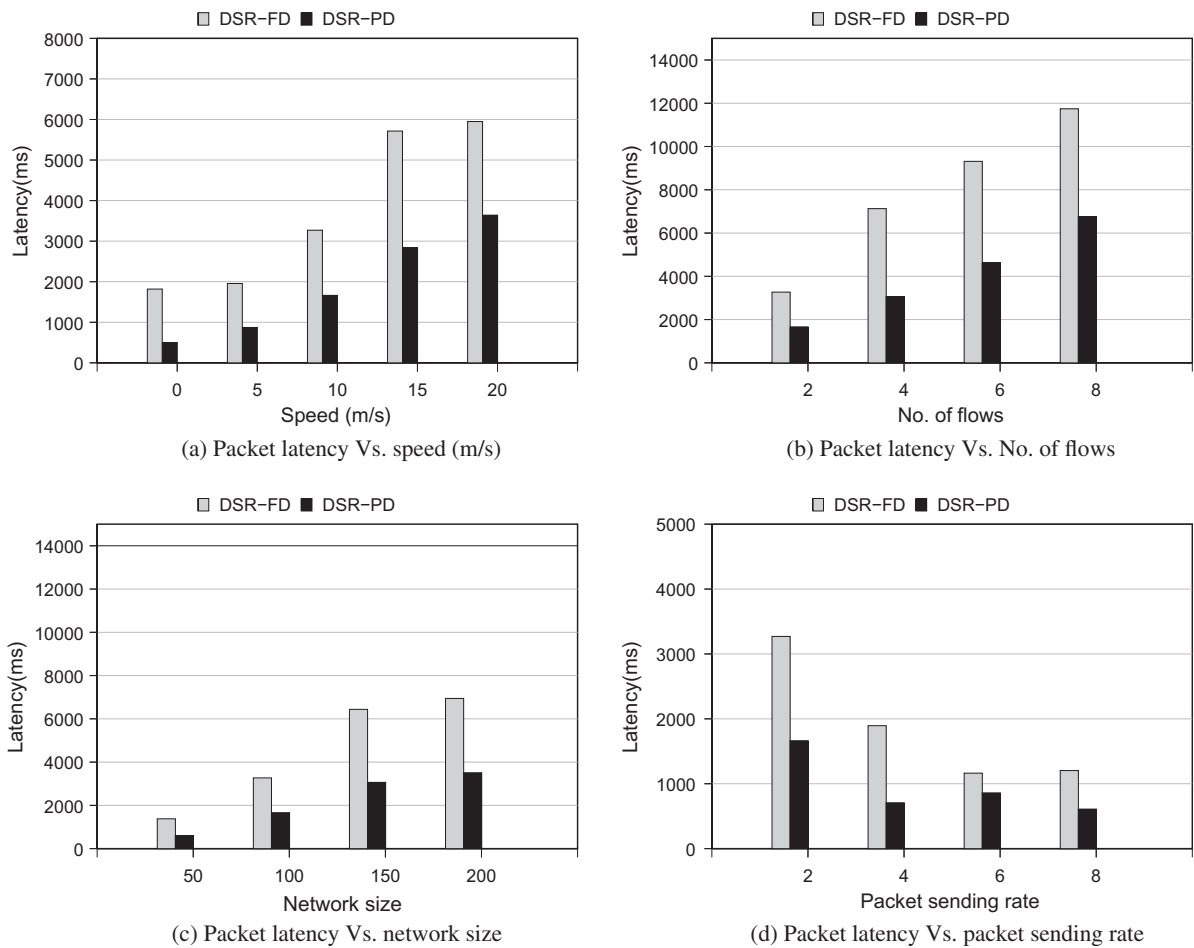


Fig. 8. Packet latencies of DSR-PD and DSR-FD against speed, number of flows, network size and packet sending rate.

exchange this information on periodic basis with other beacon nodes. The list is either maintained by passive listening of the network traffic or through sending special information messages. Normal ad hoc nodes flood a packet up to a specified flooding distance (TTL) towards a destination node  $D$ . If destination  $D$  is not within the list of the local beacon node, it unicasts the flooded packet to the beacon which has the destination in its region. The packet is finally delivered to its destination.

We now analyze the following problem: *What is the maximum flooding distance at which a beacon can be placed in order to deliver a packet under a given reliability constraint?* For this purpose, we first provide a key definition that is used in the analysis.

**Definition 9.** *Safe flooding distance* is the distance to which a packet may be flooded under a given reliability constraint.

The following lemma provides a bound on the safe flooding distance in terms of optimal paths.

**Lemma 2.** *The safe flooding distance for a given minimum reliability  $R$  in an ad hoc network is bounded by*

$$h \leq \frac{\ln\left(1 - (1 - R)^{\frac{1}{N_{opt}}}\right)}{\ln(p_f)}, \quad (13)$$

where  $N_{opt}$  is the number of optimal paths of  $h$  hops each and  $p_f$  is the packet forwarding probability.

**Proof 2.** Assuming that there are  $N_{opt}$  optimal paths of  $h$  hops between a given (source, destination) pair, the reliability of packet delivery in either direction is given by (12) as

$$R = \sum_{i=1}^{N_{opt}} p_f^h. \quad (14)$$

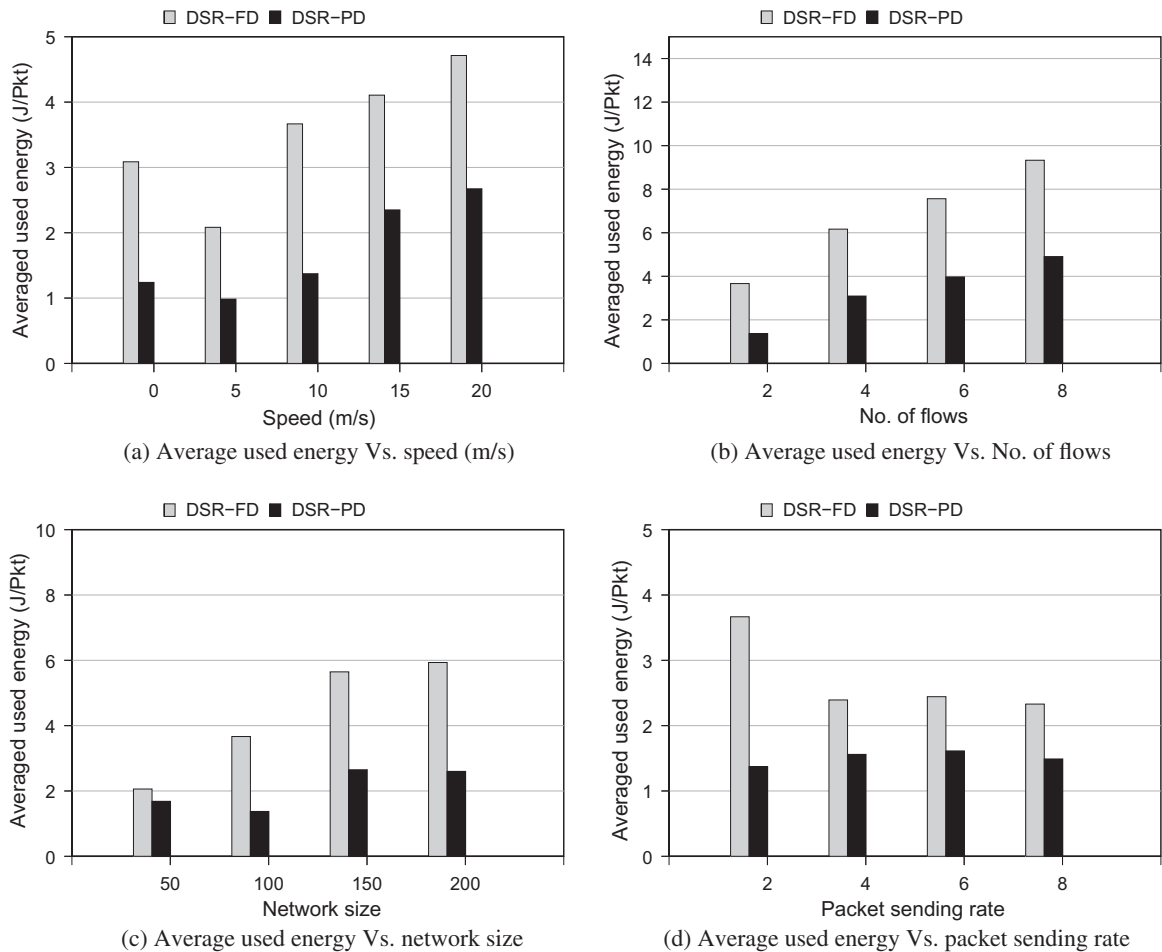
Eq. (14) provides the desired reliability level through optimal paths only. Without loss of generality, inclusion of suboptimal paths will only enhance  $R$ . Now (14) can be expressed as

$$R = 1 - \left(1 - p_f^h\right)^{N_{opt}}. \quad (15)$$

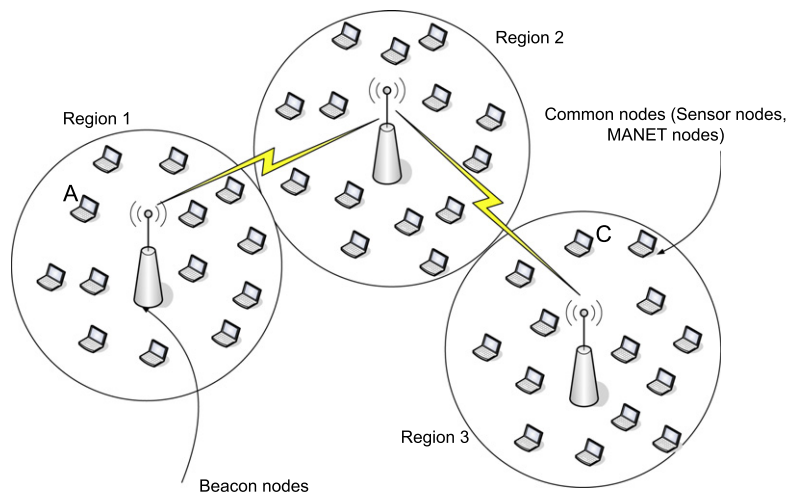
Simplifying and rearranging (15), we get

$$p_f^h = 1 - (1 - R)^{\frac{1}{N_{opt}}}.$$

Taking log on both sides and simplifying the resulting expression yields (13) which proves the lemma.  $\square$



**Fig. 9.** Average used energy of DSR-PD and DSR-FD against speed, number of flows, network size and packet sending rate.



**Fig. 10.** A hybrid network with beacon nodes.

We calculated the safe flooding distance using (13) for different values of  $R$  and optimal subsystems  $N_{opr}$  by assuming  $p_f = 0.8$ . Results are plotted in Fig. 11. All three curves have almost identical trends. If a packet need to be delivered

with higher reliability level  $R$ , it can only be delivered to a small flooding distance. Secondly, if the number of optimal paths is higher, we can deliver a packet at higher flooding distance with the same reliability level  $R$ .

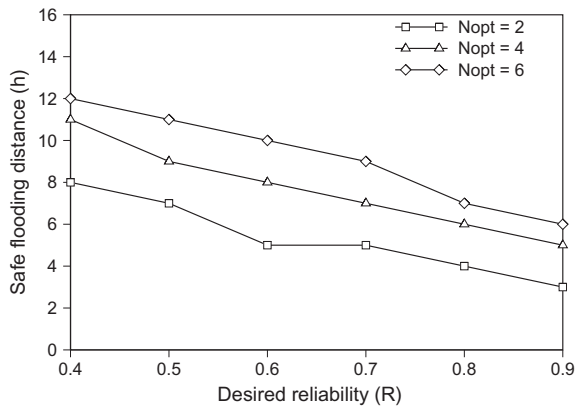


Fig. 11. Safe flooding distance at various reliabilities levels.

## 9. Conclusions

In this paper, we analyzed the impact of multiple node-disjoint paths on the reliability of a typical ad hoc routing system in the context of delay-and-loss sensitive applications. We proved that the reliability of multiple paths increases exponentially with the addition of first few paths and then saturates at a steady-state value. Therefore, we propose that it is sufficient to maintain and use a small set of redundant paths. We also conclude that partially-disjoint paths play a key role in enhancing the packet delivery reliability of an ad hoc routing/dissemination protocol. We proved that the reliability achieved through a relatively small number of partially-disjoint paths is considerably higher than the reliability provided by node-disjoint paths while incurring less energy overhead. Based on this conclusion, we proposed modifications in the route discovery process of a typical on demand ad hoc routing protocol to allow the protocol to discover partially-disjoint paths. We validated the outcomes of our theoretical analysis through simulations. Finally, we modeled the reliability of beacon-based routing protocols and derived an upper bound on the flooding distance at which a beacon node may be placed to deliver a packet under a given reliability constraint.

## Appendix A. Concavity and bounds of the reliability function of node-disjoint paths

### A.1. Concavity

To prove that the reliability function is concave with respect to  $m$  (i.e. the number of node-disjoint paths), we may rewrite (3) as

$$1 - R_p(m, p_f, t) = (1 - \epsilon)^m, \quad (\text{A.1})$$

where  $\epsilon = p_f^{t-1}$ . Taking the log of both sides and differentiating w.r.t.  $m$  yields:

$$\frac{1}{(1 - R_p(m, p_f, t))} \times -\dot{R}_p(m, p_f, t) = \ln(1 - \epsilon).$$

Replacing  $1 - R_p(m, p_f, t)$  with (A.1) and rearranging, we get

$$\dot{R}_p(m, p_f, t) = -(1 - \epsilon)^m \ln(1 - \epsilon). \quad (\text{A.2})$$

Note that  $\dot{R}_p(m, p_f, t) > 0$ . We again differentiate (A.2) w.r.t.  $m$  to obtain

$$\ddot{R}_p(m, p_f, t) = -(1 - \epsilon)^m (\ln(1 - \epsilon))^2.$$

As second derivative of the reliability function  $\dot{R}_p(m, p_f, t)$  w.r.t. to  $m$  is less than zero,  $R_p(m, p_f, t)$  is a concave function of  $m$ .

### A.2. Reliability bounds

Let  $P_1, P_2, P_3, \dots, P_m$  represent the paths between a given (source, destination) pair, each with a flooding distance  $t$ , and  $E_1, E_2, E_3, \dots, E_m$  be the events such that

$$E_i = \{\text{Path } P_i \text{ is a valid path}\}.$$

Now, we can write the reliability function  $R_p(m, p_f, t)$  in terms of the union of these events, i.e.

$$R_p(m, p_f, t) = P(\cup_i^m E_i).$$

Utilizing the formula of inclusion and exclusion bounds on the probability of union of events [21], we obtain:

$$P(\cup_i^m E_i) \leq \sum_{i=1}^m P(E_i)$$

$$P(\cup_i^m E_i) \geq \sum_i P(E_i) - \sum_{i < j} P(E_i E_j).$$

Since all  $E_i$  (where  $i = 1, 2, 3, \dots, m$ ) are independent events, the above terms can be computed as:

$$P(E_1) = P(E_2) = P(E_3) = \dots = P(E_m) = \epsilon, \quad \text{and}$$

$$P(E_1 E_2) = P(E_2 E_3) = \dots = P(E_{m-1} E_m) = \epsilon^2,$$

where  $\epsilon = p_f^{t-1}$ . Now we can write the sum of probabilities of events  $E_i$  in terms of the probability that none of the  $E_i$ 's occur. In other words,

$$\sum_{i=1}^m P(E_i) = 1 - (1 - \epsilon)^m, \quad (\text{A.3})$$

which is the upper bound on the reliability function  $R_p(m, p_f, t)$ .

Using the argument used in (A.3), we express the probability of joint events as

$$\sum_{i < j} P(E_i E_j) = 1 - (1 - \epsilon^2)^{m-1}. \quad (\text{A.4})$$

Subtracting (A.4) from (A.3), we get the lower bound on  $R_p(m, p_f, t)$  as:

$$\sum_{i=1}^m P(E_i) - \sum_{i < j} P(E_i E_j) = (1 - \epsilon^2)^{m-1} - (1 - \epsilon)^m. \quad (\text{A.5})$$

## References

- [1] Wireless LAN medium access control (MAC) and physical layer (PHY) specification, 2000.
- [2] O.B. Akan, I.F. Akyildiz, Event-to-sink reliable transport in wireless sensor networks, IEEE/ACM Transactions on Networking 13 (5) (2005) 1003–1016.
- [3] K. Akkaya, M. Younis, A survey on routing protocols for wireless sensor networks, Ad Hoc Networks 3 (2003) 325–349.
- [4] C. Bettstetter, C. Hartmann, Connectivity of wireless multihop networks in a shadow fading, ACM/Kluwer Wireless Networks Journal 11 (5) (2005).

- [5] V. Bhandari, N.H. Vaidya, Reliable broadcast in wireless networks with probabilistic failures, in: Proceedings of IEEE INFOCOM, Anchorage, Alaska, USA, May 2007, pp. 715–723.
- [6] J. Broch, D.A. Maltz, D.B. Johnson, Y.-C. Hu, J. Jetcheva, A performance comparison of multi-hop wireless ad hoc network routing protocols, in: Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom98), 1998.
- [7] G. Di Caro, F. Ducatelle, L.M. Gambardella, AntHocNet: an adaptive nature-inspired algorithm for routing in mobile ad hoc networks, European Transactions on Telecommunications (ETT), Special Issue on Self Organization in Mobile Networking 16 (5) (2005) 443–455.
- [8] Y.-C. Cheng, T.G. Robertazzi, Critical connectivity phenomena in multihop radio models, IEEE Transactions on Communications 37 (7) (1989) 770–777.
- [9] B. Deb, S. Bhatnagar, B. Nath, ReInForM: reliable information forwarding using multiple paths in sensor networks, in: Proceedings of IEEE International Conference on Local Computer Networks (LCN), Bonn/Knigswinter, Germany, October 2003.
- [10] M. Farooq, Bee-Inspired Protocol Engineering: From Nature to Networks, Natural Computing Series, Springer-Verlag, 2009, ISBN: 978-3-540-85953-6.
- [11] R. Fonseca, S. Ratnasamy, J. Zhao, C. Tien Ee, D. Culler, S. Shenker, I. Stoic, Beacon vector routing: scalable point-to-point routing in wireless sensor networks, 2005. <<http://berkeley.intel-research.net/sylvia/bvr.pdf>>.
- [12] D. Ganesan, R. Govindan, S. Shenker, D. Estrin, Highly-resilient, energy-efficient multipath routing in wireless sensor networks, Mobile Computing and Communications Review 5 (4) (2001) 11–25.
- [13] O. Gnawali, M. Yarvis, J. Heidemann, R. Govindan, Interaction of retransmission, blacklisting, and routing metrics for reliability in sensor network routing, in: Proceedings of IEEE SECON, Santa Clara, CA, USA, October 2004, pp. 34–43.
- [14] M. Heusse, F. Rousseau, G.B. Sabbatel, A. Duda, Performance anomaly of 802.11b, in: Proceedings of IEEE INFOCOM, San Francisco, USA, April 2003, pp. 836–843.
- [15] C.-C.J. Kuo, J.-J. Lee, B. Krishnamachari, Aging analysis in large-scale wireless sensor networks, Ad Hoc Networks 6 (2008) 1117–1133.
- [16] D.B. Johnson, D.A. Maltz, J. Broch, Dynamic source routing in ad hoc wireless networks, in: Tomasz Imielinski, Hank Korth (Eds.), Mobile Computing, 1996, pp. 153–181.
- [17] S. Kim, R. Fonseca, D. Culler, Reliable transfer on wireless sensor networks, in: Proceedings of IEEE SECON, Santa Clara, CA, USA, October 2004, pp. 449–459.
- [18] R. Kumar, A. Paul, U. Ramachandran, D. Kotz, On improving wireless broadcast reliability of sensor networks using erasure codes, in: Proceedings of 2nd International Conference on Mobile Ad-hoc and Sensor Networks, Hong Kong, China, December 2006, pp. 155–170.
- [19] A. Nasipuri, S. Das, On-demand multipath routing for mobile ad hoc networks, in: Proceedings of IEEE International Conference on Computer Communication and Networks (ICCCN), Boston, MA, October 1999, pp. 64–70.
- [20] C. Perkins, E. Royer, Ad-hoc on-demand distance vector routing, in: Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, USA, February 1999, pp. 90–100.
- [21] S.M. Ross, Introduction to Probability Models, Harcourt Academic Press, CA, USA, 2000.
- [22] M. Saleem, S.A. Khayam, M. Farooq, On performance modeling of ad hoc routing protocols, EURASIP Journal on Wireless Communications and Networking, vol. 2010, Article ID 373759, 13pp., 2010, doi:10.1155/2010/373759.
- [23] C. Santivanez, S. Ramanathan, I. Stavrakakis, Making link state routing scale for ad hoc networks, in: Proceedings of ACM MobiHOC, Long Beach, CA, USA, October 2001, pp. 22–32.
- [24] C.A. Santivanez, B. McDonald, I. Stavrakakis, R. Ramanathan, On the scalability of ad hoc routing protocols, in: Proceedings of IEEE INFOCOM, New York, USA, June 2002, pp. 1688–1697.
- [25] G. Sharma, R. Mazumdar, Hybrid sensor networks: a small world, in: Proceedings of ACM MobiHOC, Chicago, IL, USA, May 2005, pp. 366–377.
- [26] C.-Y. Wan, A.T. Campbell, L. Krishnamurthy, Pump-slowly, fetch-quickly (PSFQ): a reliable transport protocol for sensor networks, IEEE Journal on Selected Areas in Communications 23 (2005) 862–872.
- [27] F. Ye, G. Zhong, S. Lu, L. Zhang, Gradient broadcast: a robust data delivery protocol for large scale sensor networks, ACM/Springer's Journal on Wireless Networks 11 (3) (2005) 285–298.
- [28] N. Zhou, A.A. Abouzeid, Routing in ad hoc networks: a theoretical framework with practical implications, in: Proceedings of IEEE INFOCOM, Miami, USA, March 2005, pp. 1240–1251.
- [29] M. Saleem, G. Di Caro, M. Farooq, Swarm intelligence based routing protocol for wireless sensor networks: Survey and future directions, Information Sciences (2010), doi:10.1016/j.ins.2010.07.005.

- [30] M. Saleem, M. Farooq, Beesensor: a bee-inspired power aware routing protocol for wireless sensor networks, in: Proceedings of the 4th EvoCOMNET Workshop, LNCS, vol. 4448, 2007.



**Muhammad Saleem** received the B.E. degree in electronics from NED University of Engineering and Technology, Karachi, Pakistan, and the M.S. in computer engineering from Center for Advanced Studies in Engineering affiliated with University of Engineering and Technology, Taxila, Pakistan. He is currently pursuing his Ph.D. studies at Center for Advanced Studies in Engineering, Islamabad, Pakistan, in the area of natural computing with application to routing in wireless ad hoc and sensor networks. His other research interests include performance modeling of ad hoc routing algorithms.



**Israr Ullah** received his MCS degree from Institute of Computing and Information Technology (ICIT), Gomal University, Pakistan, in 2004. He completed his M.S. in computer science from National University of Computer and Emerging Sciences (NUCES), Islamabad, Pakistan, in 2009. Currently, he is pursuing his Ph.D. studies at NUCES Islamabad, Pakistan, in the field of grid networks dimensioning and modeling. His research interests also include design and analysis of optimization algorithms.



**Syed Ali Khayam** received his B.E. degree in Computer Systems Engineering from National University of Sciences and Technology (NUST), Pakistan, in 1999 and his M.S. and Ph.D. degrees in Electrical Engineering from Michigan State University in 2003 and 2006, respectively. In February 2007, he joined the School of Electrical Engineering & Computer Science (SEECs), National University of Sciences & Technology (NUST), Pakistan, as an assistant professor. AT NUST-SEECs, he directs the Wireless and Secure Networks (WiSNet)

Research Lab. Khayam has received research awards from Nokia Research, Korean Research Foundation and Pakistan National ICT R&D Fund. He offers consultancy for some Silicon Valley based technology companies. He also worked at Communications Enabling Technologies as a Design Engineer from October 2000 to August 2001. His research interests include analysis and modeling of statistical phenomena in computer networks, network security, cross-layer design for wireless networks, and real-time multimedia communications. He has more than 50 publications and 4 pending patents in this area.



**Muddassar Farooq** received his B.E. degree in Avionics Engineering from National University of Sciences and Technology (NUST), Pakistan, in 1996. He completed his M.S. in Computer Science and Engineering from University of New South Wales (UNSW), Australia, in 1999. He completed his D.Sc. in Informatics from Technical University of Dortmund, Germany, in 2006. In 2007, he joined the National University of Computer & Emerging Sciences (NUCES), Islamabad, Pakistan, as an associate professor. He is also the

Director of Next Generation Intelligent Networks Research Center (nexGIN RC) at NUCES. He is the author of the book “Bee-inspired Protocol Engineering: from Nature to Networks” published by Springer in 2009. He

has also has coauthored two book chapters in different books on swarm intelligence. He is on the editorial board of Springer's Journal of Swarm Intelligence. He is also the workshop chair of European Workshop on Nature-inspired Techniques for Telecommunication and Networked Systems (EvoCOMNET) held with EuroGP. He also serves on the PC of well-known EC conferences like GECCO, CEC, ANTS. He is the guest editor of a

special issue of Journal of System Architecture (JSA) on Nature-inspired algorithms and applications. His research interests include agent based routing protocols for fixed and mobile ad hoc networks (MANETs), nature inspired applied systems, natural computing and engineering and nature inspired computer and network security systems, i.e. artificial immune systems.