Interference Aware-based Ad-Hoc On Demand Distance Vector (IA-AODV) ultra wideband system routing protocol

Floriano De Rango *, Fiore Veltri, Peppino Fazio

D.E.I.S. Department, University of Calabria, P. Bucci Road, Rende 87036, Italy

A B S T R A C T

Ultra wideband (UWB) systems are communication systems based on a baseband impulsive transmission that has recently excited interest both in the commercial and academic fields. Physical layer aspects and MAC protocols have been intensively investigated in the recent years leading, in some cases, to important and definitive results. However, many questions relating to the UWB network layer are still open. The aim of this paper is to investigate the network layer of the UWB system: for this purpose a new routing protocol called Interference Aware-based Ad-Hoc On Demand Distance Vector (IA-AODV) and based on the interference concept has been proposed. In particular, two distinct metrics are explained in detail: the first one is based on the concept of global interference perceived by each node; the second one is based on the concept of link interference perceived by a node on a wireless path to a generic neighbor. Finally, a comparative analysis between our protocol and Ad-Hoc On Demand Distance Vector (AODV) protocol are carried out in order to show the soundness of our proposal.

1. Introduction

UWB system is a transmission scheme employing baseband pulses characterized by a great fractional band (>25%) [1]. Physical layer aspects and MAC protocols for UWB systems have been intensively studied in these last years leading, in some cases, to important results. Instead, many fields of research are still open with regard to the routing layer of UWB system, so in this paper we investigate some of these aspects. In UWB networks, nodes are affected by mutual reciprocal interference [2]: for this purpose a new routing protocol based on the interference concept has been proposed. This protocol employs the *Dynamic Channel Coding-MAC* (DCC-MAC) model [3,4]. Moreover, DCC-MAC employs an UWB impulse radio physical layer based on *Time-Hopping* (TH-UWB IR) as in [5,6].

The interference issue is not a trivial problem. The concept of optimum routing metric employed in classic narrowband wireless systems could not be extended to the UWB case. For example, the shortest route could not be the best route. In the choice of the optimal route from source to destination, interference has to be considered. In this work, starting from the considerations drawn in [7,8] about *Interference Based On-Demand Routing* (IBOR) protocol, the *Ad-Hoc On Demand Distance Vector* (AODV) protocol [9] has been opportunely modified in order to consider the interference perceived during the route discovery phase: we call the proposed protocol *Interference Aware-based Ad-Hoc On Demand Distance Vector* (IA-AODV). A first version of the IA-AODV has been presented in [8]. However in this paper more explanation and more mights into the simulation campaigns are given. In particular, two distinct metrics are proposed in this paper. The first one, called *Link Interference* (*LI*) metric is based on the interference affecting the links involved in the transmission (from source to destination). The second one, called *Node Interference* (*NI*) metric is based on the global interference perceived by nodes. In order to test the soundness of the proposed protocol, we used NS-2 and compared IA-AODV with the standard AODV protocol in terms of end-to-end delay, overhead and packet delivery ratio.

The paper is organized as follows: the related works are discussed in Section 2; the reference scenario is shown in Section 3; IA-AODV protocol is explained in Section 4; performance evaluation is shown in Section 5 and finally conclusions are summarized in Section 6.

2. Related works

Generally, classic ad hoc network routing protocols employ metrics such as minimum hop count [9] or geometric criterions [10–12]. Therefore, ad hoc routing algorithms must provide the optimal route adapting to the frequent and unpredictable network topology variation. Also some UWB routing algorithms make use of the high precision localization capability of UWB network [13–15], to choose the optimum route: using location information, nodes can choose to send packets to neighbors that are closer to the destinations [16]; moreover, in order to improve these mechanisms, cluster structures can be formed, and can lead to a routing algorithm described by [17].

All these approaches can be useful in those architectures that are not affected by neighbor interference, but they are not valid for the UWB networks. The traditional routing protocols used in ad hoc networks, such as the AODV [9], *Dynamic Source Routing* (DSR) [18], and others [19,20], do not take into account directly interference "between the nodes". In this way, the choice of a path, on which the packets must travel from the source to destination, may be wrong in terms of degradation of the signal: the distance between the source and destination can be minimized, but the level of interference may be too high if new metrics are not defined in the routing protocols.

Transmission interference is the most difficult problem for wireless communications. In the last few years, many new techniques have been proposed to reduce the effects of interference, defining interference-aware metrics and routing protocols. The reciprocal interference between system nodes considerably affects the path-delay and, so, the data-rate. The older interference-aware metrics tried to optimize these parameters: the DIAR [21,22] is one of the interference-aware routing protocols for IEEE 802.11 networks and it is based on the *Network Allocator Vector Count* (NAVC). The simulation results that the NAVC is not dependent on the total number of nodes in the system. The path with the lowest NAVC is a path with a lower delay and a lower interference [23,19]. With a similar approach, in [20], where the employed metric chooses the path with the lowest path delay, defined as the interval between the *Route REQuest* (RREQ) dispatch and the related *Route REPly* (RREP) reception. In [24], the chosen interference-aware metric is different: the authors make the assumption that if there is a higher number of neighbors, a higher probability of interference for a node will be observed; for this reason, through the adopted metric, the routing protocol selects a certain number of paths, verifying that the sum of the coverage values of the nodes belonging to the single path is the lowest. It must be remembered that the coverage value of a node is the number of nodes that are directly covered by it. In [7,8], the authors propose the IBOR protocol, where the employed metric considers the interference level as the parameter to make the routing decision: the optimum route minimizes the effects of interference. In [25,26] the authors propose some interesting routing metrics for a generic CMDA environment, introducing a cooperative approach by considering not only the cost associated with the current route, but also the potential interference impact of the route on the neighboring nodes. In particular, in [25], the authors presented two main routing schemes. The first one is the Time Multiplexing (T.M.), for which the scenario results in equal interference created by all nodes in the network so, without power control, the interference level is not affected by the number of flows at a node; the other one is the Simultaneous Transmission (S.T.), for which the interference created by a particular node varies with the number of relayed flows. In both cases, the introduction of constraints on Near–Far Effects (NFE) levels lead to performance enhancements: the routing algorithm minimizes the energy expenditure on an end-to-end path, subject to constraints on the interference caused by the nodes participating in a route to other nodes in their neighborhood. The proposed algorithm in [25] starts by determining a source to destination route using a minimum energy metric, based on the routing table available at the transmitting node. After a minimum energy route has been determined, the amount of interference caused by each node in a route to receiving neighboring nodes is estimated. If the interference caused to other transmissions is greater than a target T, the node is excluded from the current route and a new minimum energy route is determined for the remaining possible relaying nodes.

Starting from classic AODV protocol [9] and from IBOR protocol [7,8], two new metrics, based on the concept of global interference perceived by a node, for the *NI* metric, or on the interference perceived along the paths of a route, for the *LI* metric, have been proposed in this work. AODV is a reactive routing protocol based on distance vector algorithm. A key feature of this protocol is the use of "*sequence numbers*", which provides a method for a node to establish if a particular route is updated.

In the following are the main novelties of our protocol:

- Our protocol introduces the concept of interference in the choice of optimum route improving the system performance: in fact, in a UWB network, the minimum hop route, such as in AODV, could not be an optimum choice because it could be affected by a high amount of interference that could make the communication substantially impracticable;
- Two distinct metrics are proposed: the first one, proposed in [7,8] and called *NI*, is based on the global interference perceived by nodes involved in the communication; instead, the second one, called *LI*, is based on the interference perceived only on the links belonging to the route from source to destination;
- Links refresh, provided by standard AODV, occurs only in the presence of breakage of links and not when there is a substantial variation in interference. However, in the presence of scenarios with mobility, having the routing tables updated on the basis of important variations in the perceived interference, could lead to a better use of the minimum interference routes. For this purpose, we introduced a further refresh mechanism taking into account the interference variation.

Moreover, the proposed protocol employs the TH-UWB IR physical (PHY) layer and DCC-MAC. As better explained in the following section, DCC-MAC offers some techniques for interference evaluation and mitigation, by using the intrinsic characteristics of TH-PHY. So, for the application of our protocol, localization mechanisms, as in [13–17], are not needed: node power levels are easily computed through the already implemented PHY and MAC primitives. Finally, in our work, clustering approaches have not been implemented, due to the distributed structure of the considered network: our protocol inherits route discovery and maintenance procedures from the standard AODV, by which each node of the network can directly manage its routing table, without the need of hierarchical network organization.

3. Reference scenario

In this section, some considerations about reference physical and MAC layers are presented. In this work, we adopt as MAC layer the DCC-MAC model [3,4]. This protocol allows devices to perform multiple parallel transmissions, adapting communications on the basis of interference perceived by the same devices. To realize this, an opportune coding mechanism is used. DCC-MAC employs an UWB impulse radio physical layer based on TH-UWB IR as in [5,6]. In the *Time-Hopping* based system, the transmission time is divided in short chips of T_c duration aggregated into frames (whose duration is T_f) in order to transmit one pulse in one chip per frame. Multi-user access is provided by pseudo-random *Time-Hopping Sequences* (THS) that determine in which chip each user should transmit. Besides, due to the nonzero cross-correlation between Time-Hopping Sequences, time-asynchronicity between sources and a multipath channel environment, TH-UWB is sensitive to strong interferers. Further details on this physical layer model can be found in [5,6].

A specific analysis of UWB network optimum planning is described in [27] where DCC-MAC is also discussed. Interference at the receiver is more harmful when the impulses of a neighbor collide with those of the source. Instead of inhibiting the sources into exclusion region, DCC-MAC uses a different strategy called *interference mitigation*.

Interference mitigation allows the erasure of interfering impulses having an energy higher than the signal received from the source: this scheme cancels the samples resulting from a collision with pulses of a strong interferer and replaces them by erasures (for example skipping them in the decoding process). Compared to other schemes such as power control or exclusion mechanism, the interference mitigation does not require any coordination between nodes [3,4]: when a source must communicate, it transmits at the maximum power without considering other ingoing transmissions. In particular, the communication uses either public (receiver-based) or private THSs. The public THS of user with MAC address A, called THS (A), is the THS produced by the *pseudo-random generator* (PRG) with seed = A. The private THS of users A and B, called THS (AB) is the THS produced by the PRG with a seed equal to the number whose binary representation is the concatenation of A and B. Note that a node can always compute the THS used by a potential source. In order to take more advantage of the channel, transmission needs to be constantly adapted to the higher code rate allowing a correct decoding at the receiver. Dynamic coding is performed through a hybrid *Automatic Retransmission request* (ARQ) protocol: if channel conditions degrade and the coding fails, additional information is sent until the packet is correctly decoded; if no further information is available, the transmission fails. Another issue regards the possibility of multiple transmissions toward the same destination: the goal of the *private MAC* protocol is to ensure that several senders cannot communicate simultaneously with one destination; the *private MAC* solves this problem combining receiver-based and invitation-based selection of THSs. Moreover, the mechanisms provided by DCC-MAC, based on the management of THS, allow us to estimate the interference perceived during the reception of a packet. Further details of this protocol can be found in [3,4].

Finally, we present some considerations about the channel model employed in our simulations. As in [3,4], we used the propagation indoor model described in [28,29] where the power attenuation in decibels, due to distance, is at a given distance d is defined as follows:

$$\overline{PL(d)} = [PLo + 10\mu_\gamma \log d] + [10n_1\sigma_\gamma \log d + n_2\mu_\sigma + n_2n_3\sigma_\sigma] \qquad (1)$$

where the intercept point PLo is the path loss at d_0 = 1 m whereas μ_γ and σ_γ are, respectively, the normal distribution media and the standard deviation of the decaying path loss exponent γ. The shadowing effects, in accordance with [28,29], are modeled through a zero-mean Gaussian distribution with standard deviation σ, normally distributed and characterized by average value μ_σ and standard deviation σ_σ. n_1, n_2 and n_3 are zero-mean Gaussian variables with unit standard deviation $N\,[0,1]$. More specifically, the first term of (1) represents the median path loss, whereas the second term is the random variation around median value. Further details can be found in [28,29].

4. Interference Aware-based Ad-Hoc On Demand Distance Vector (IA-AODV)

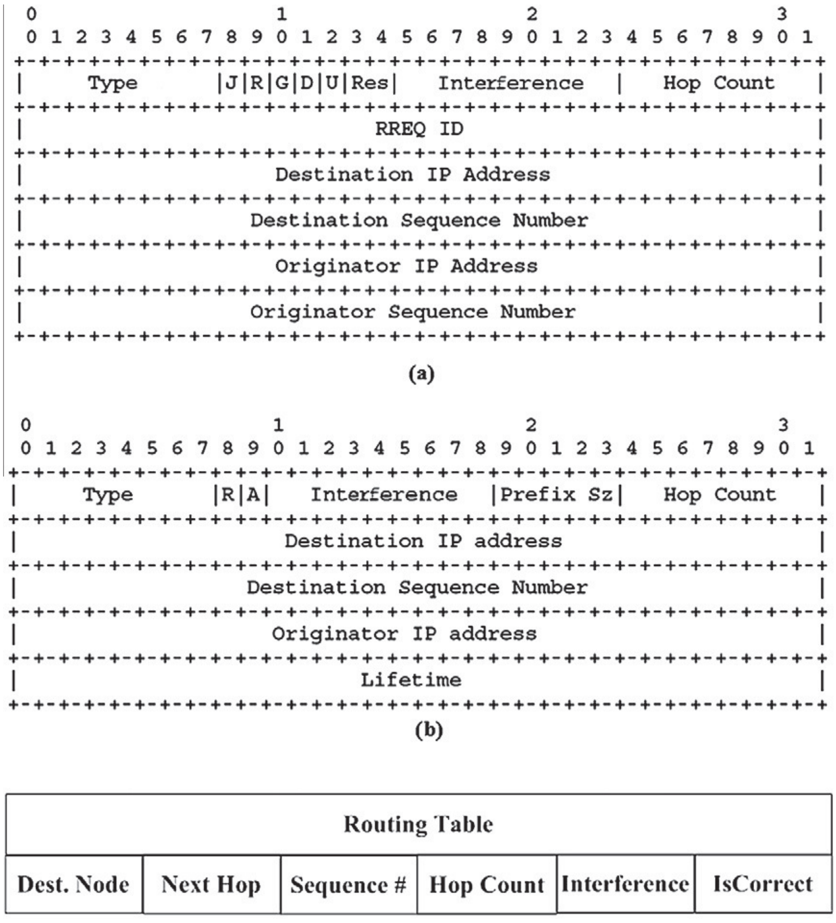
The proposed protocol inherits part of its working operation and control packets, and the IBOR protocol [7,8], from the classic AODV protocol [9].

The novelty of the proposal is in two metrics adopted to select the optimal route from source to destination and in the route maintenance procedure: the proposed metrics are not based on the minimum hop number, such as in AODV protocol, but on the global interference perceived by nodes (*NI* metric), and on the interference affecting the link involved in the transmission (*LI* metric). In order to realize these metrics, we modified some control packets: an the *Interference* field was added to the RREP and RREQ packets. The modified structures of the packets are respectively shown in Fig. 1a and b. Also the structure of the entry of the routing tables was modified: as *Interference* field, in which is stored the interference from the node to the destination, and as *IsCorrect* field, a Boolean variable indicating the validity of links (see Fig. 1c), were added. This last variable is needed because the interference on the link A–B could be different from that on the link B–A, therefore we need to know if the value stored in the entry refers to an interference perceived or transmitted by the node (this concept is better explained in the following). Other parameters needed by our protocol are presented in the next subsection.

4.1. Analytical formulation

In this subsection, the analytical formulation of our metrics is described. Before starting our analysis, some definitions must be given:

- P_{BA} is the data packet sent from node B to the node A;
- P_l is a generic data packet received in a certain observation window by a given node;
- *PI* (*Packet Interference*) is the interference contribution, expressed in Watts, generated by a packet that is interfering on the currently received packet;
- n is the number of packets that are interfering with the reception of a specific packet;
- CTC_i (*Collision Time Coefficient*) is the time fraction of the P_{BA} receiving time affected by the interference of the packet p_i;
- *WI* (*Window of Interference*) is the interval during which the interfering packet impacts on the reception of P_{BA};
- $I_{P_{\mathrm{BA}}}$ is the total perceived interference on P_{BA};
- *OW* (*Observation Window*) is a generic observation window of fixed length in which we collect the information needed to compute the interference;
- OW_k is the kth observation window;
- I_{P_l} is the total perceived interference for P_l;
- SPI_k (*Set of Packet Interference*) is the set of I_{P_l} values observed during the kth period OW_k;
- GI_k is the global interference perceived by a node during the kth observation window OW_k;
- *NSW* (*Number* of Stored OW) is the number of *OW* that must be taken into account for the metric *NI*;
- *GI* is the global node interference employed in the *NI* metric for a generic node;
- $I_{P_{\mathrm{BA}_j}}$ is the interference perceived by A at the reception of jth packet from node B;
- m is the number of packets received by a node on a specific link during the observation window *OW*;
- $\hat{ij}$ link is a generic link belonging to the route from the source to the destination in *LI* metric;
- $I_{\hat{ij}}$ is the interference perceived on the generic link $\hat{ij}$ in *LI* metric;
- *Path* (S,D) is the set of nodes belonging to the route from *Source* to *Destination*;
- *NI* is the *Node Interference*-based metric;
- *LI* is the *Link Interference*-based metric;
- I_{NI} is the interference computed by the *NI* metric;
- I_{LI} is the interference computed by the *LI* metric;
- α is a threshold influencing the occurrences of the interference information refresh;
- *SI* (*Stored Interference*) is the (global or link) interference stored by a node.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |J|R|G|D|U|Res|   Interference  |   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            RREQ ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Originator IP Address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Originator Sequence Number                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

(a)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |R|A|   Interference    |Prefix Sz|   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Destination IP address                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Originator IP address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Lifetime                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

(b)

Routing Table					
Dest. Node	Next Hop	Sequence #	Hop Count	Interference	IsCorrect

(c)

Fig. 1. (a) RREQ packet structure. (b) RREP packet structure. (c) Routing table entry.

We suppose that a generic node A is receiving a packet, denoted by P_{BA}, from node B. During the reception of this packet, node A detects an amount of interference (intended as interfering power in Watts) due to some packets transmitted by the nodes in its coverage range (and different from the node B). We indicate with *PI* the interference due to a generic packet interfering with the packet P_{BA}. This amount of interference is given by the expression:

$$PI = P_{RX} \cdot CTC \tag{2}$$

where P_{RX} is the received interfering power, and *CTC* is the *Collision Time Coefficient*, that is the time fraction needed to receive P_{BA} on which the interfering packet impacts. In particular, *CTC* is defined as [3,4]:

$$CTC = \frac{WI}{TE_{P_{\mathrm{BA}}} - TS_{P_{\mathrm{BA}}}} \tag{3}$$

where $TE_{P_{\mathrm{BA}}}$ and $TS_{P_{\mathrm{BA}}}$ are, respectively, the start and end reception time for the P_{BA} packet, while *WI*, the interval during which the interfering packet impacts on the reception P_{BA}, is given by:

$$WI = \min(TE_{P_{\mathrm{BA}}}, TE_{PI}) - \max(TS_{P_{\mathrm{BA}}}, TS_{PI}) \tag{4}$$

where TS_{PI} and TE_{PI} are, respectively, the start and end reception time for the interfering packet. If we denote with PI_i the interference, perceived for the reception of the P_{BA} packet, due to the specific interfering packet *i*, then the total perceived interference for P_{BA} can be expressed as:

$$I_{P_{\mathrm{BA}}} = \sum_{i=1}^{n} PI_i = \sum_{i=1}^{n} P_{RX_i} \cdot CTC_i \tag{5}$$

This *NI* metric can be defined by subdividing the temporal axis in *OW*. We indicate with P_l a generic packet received during a *OW*, with I_{P_l} the perceived interference relative to P_l reception computed applying the (5) and with TS_{Pl} and TE_{Pl}, respectively, the start and end reception time for the generic packet P_l. From this, we can express SPI_k as:

$$SPI_k = \{I_{P_l} | TS_{P_l} \in OW_k \wedge TE_{P_l} \in OW_k\} \tag{6}$$

The *GI* belonging to OW_k can be expressed as follows:

$$GI_k = \sum_{j}^{|SPI_k|} \frac{SPI_k(j)}{|SPI_k|} \tag{7}$$

where $SPI_k(j)$ and $|SPI_k|$ are, respectively, the *j*th element and the cardinality of the SPI_k set.

From the definition of *PI*, the *NI* metric can be derived as a parameter for evaluating the interference observed by a certain node. The global interference *GI*, employed in the *NI* metric, for a generic node is expressed as:

$$GI = \frac{\left(\sum_{l=1}^{NSW} GI_l\right)}{NSW} \tag{8}$$

where *NSW* is the number of *GI* that must be taken into account.

The *NI* metric is based on the global node interference calculated as the ratio between the sum of the interference *GI* of each node belonging to the route and the number of hops composing the route:

$$I_{NI}(S,D) = \sum_{j \in Path(S,D)} \frac{GI_j}{HopCount_{Path(S,D)}} \tag{9}$$

where *j* and *HopCount* are, respectively, the node indexes and the number of hops of the considered route. *S* and *D* is the source–destination pair. After introducing the global interference metric, now we proceed with the description of the link interference metric *LI*. Node A monitors the wireless link condition for each neighbor computing the interference perceived on every link. Regarding its neighbor B, node A will estimate the average interference perceived for the reception of each packet from B in a specific observation time window *OW*. At the end of this observation, node A computes the average interference perceived on the link as follows:

$$I_{\mathrm{BA}} = \frac{\sum_{j=1}^{m} I_{P_{BA_j}}}{m} \tag{10}$$

where $I_{P_{BA_j}}$ is the interference perceived by A at the reception of the *j*th packet from node B, while *m* is the number of packets received by node A during *OW*.

The proposed metric employs the link interference values in order to find the minimum interference route on which to forward the packets. In particular, the interference from a source *S* to a destination *D* for the *LI* metric is simply given by the expression:

$$I_{LI}(S,D) = \sum_{\hat{ij} \in Path(S,D)} I_{\hat{ij}} \tag{11}$$

where the $\hat{ij}$ link is a generic link belonging to the route from the source to the destination and $I_{\hat{ij}}$ is the interference perceived on it computed according to (10).

The source will choose the freshest route toward destination (managed with *sequence number* as in standard AODV), with the lowest interference value, computed applying the (11).

4.2. Refresh procedure

Every node will store the average interference perceived on each path, linking it to its neighbors applying (10), and the global value of interference computed applying (8). However, this information can quickly vary in the network and therefore a refresh mechanism is necessary in order to avoid the propagation and the use of false interference information. Furthermore, if the interference perceived by a node significantly increases, it is necessary to invalidate all routes using that node to reach a generic destination.

We solve this problem by introducing an interference variation control in each node. The interference values are updated only if the interference variation, with respect to the stored values, is greater than a prefixed threshold α. Analytically, this can be expressed as:

$$\begin{cases} SI_k = SI_{k-1} & \text{if } \left(\frac{I-SI_{k-1}}{SI_{k-1}}\right) \cdot 100 < \alpha \\ SI_k = I & \text{if } \left(\frac{I-SI_{k-1}}{SI_{k-1}}\right) \cdot 100 \geqslant \alpha \end{cases} \tag{12}$$

In (12), SI_{k-1} is the value stored at the end of the $(k-1)$th iteration, while *I* is the interference computed in the *k*th iteration applying, on the basis of the adopted metric, (8) or (10). The procedure for the *LI* metric is shown clearly in Fig. 2. If the updating of the value stored in *SI* is required, then the node performing the computing, informs its neighbor about interference variation (for example, referring to (12) the node *j* informs node *i* about link interference variation) using the unicast RRER mechanism of AODV protocol: this message is propagated to every node of the path toward destination *D* preceding the node discovering interference variation.

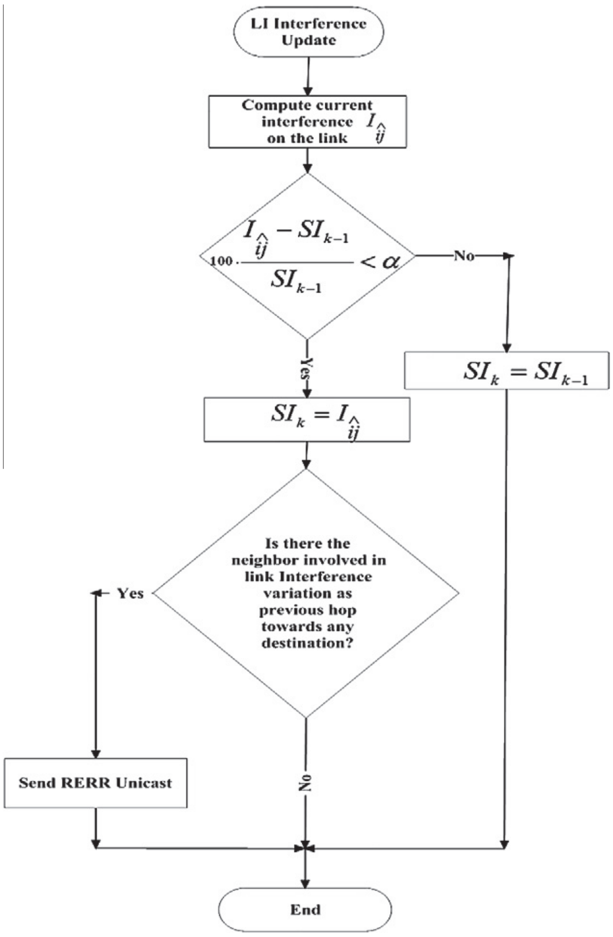

LI Interference Update
Compute current interference $I_{\hat{ij}}$ on the link
$100 \cdot \frac{I_{\hat{ij}} - SI_{k-1}}{SI_{k-1}} < \alpha$
No
Yes
$SI_k = SI_{k-1}$
$SI_k = I_{\hat{ij}}$
Is there the neighbor involved in link Interference variation as previous hop towards any destination?
Yes
No
Send RERR Unicast
End

Fig. 2. Interference control on a generic link for the *LI* metric.

4.3. Route discovery and maintenance

When a source must communicate with another node of the network, it checks in its routing table if a valid *entry* toward that destination is present. In this case, the packets are sent toward the node indicated as *next hop* in the *entry* (likewise AODV standard). An *entry* is valid if it is fresh (this is provided by standard AODV procedure) and the *IsCorrect* field is set to true. Otherwise, if an *entry* is not present or it is invalid, the sender starts the route discovery procedure: a RREQ packet, in which the *Interference* field is set to zero (other fields are set following standard AODV procedure), are sent in flooding. When a node receives a RREQ, it adds the stored value of interference (this value is stored in *SI*) to the *Interference* field; therefore, if it does not have an *entry* toward the sender, it creates a new *entry* inserting in the *Interference* field the new value stored in the RREQ and setting to false the *IsCorrect* field. This last step is needed because the interference stored in the RREQ is computed from the source toward this node and it could be different from the interference on the backward route: we must avoid that other RREQs use this wrong information about interference to reach the sender from the current node. If the *entry* is already present and its *IsCorrect* field is set to false, then the *Interference* field is updated only if the interference value stored in the RREQ is less than that one in the *entry* (*IsCorrect* field is not updated). In this way, the nodes, locally, already make a choice about the minimum interference route: if information updating interference is available, the RREP will find fresh value of interference and it will be forwarded automatically on the minimum interference route available. If the *IsCorrect* field is set to true, the *entry* is not modified in order to not mistakenly change the information referring to the correct direction toward sender. After these operations, the node must verify if it is the destination or if it has a valid route toward destination (recall that the *IsCorrect* field must be set to true). If neither condition is satisfied, the node must forward the RREQ packet with the updated *Interference* field. Otherwise, the node must generate a RREP packet toward the sender through the nodes belonging to the route crossed by the RREQ (as in classic AODV).

In particular, if the node is the destination, in the *Interference* field of the RREP the interference value *SI* stored by the node is moved; otherwise, it must insert the value stored in the *Interference* field of the routing table *entry* relative to the considered destination in the RREP. After these operations, the RREP (with the remaining fields set according to standard AODV) is forwarded to the previous hop of the route. When a generic node receives a RREP packet, it must apply the procedures described in Fig. 3. Regarding the route maintenance, the proposed protocol maintains the AODV procedures based on the route freshness, on the link breakage and on the sending of the RERR message.

In addition to these procedures, a further mechanism was introduced to take into account the significant variation in interference. For example, considering the *LI* metric, the node A computes, at each observation window, the average interference perceived on the path linking it to the node B applying (10): if this interference is significantly different with respect to the previously stored value, i.e. an updating of *SI* is required according to (12), then node A sends a particular unicast RERR to the neighbor node involved in

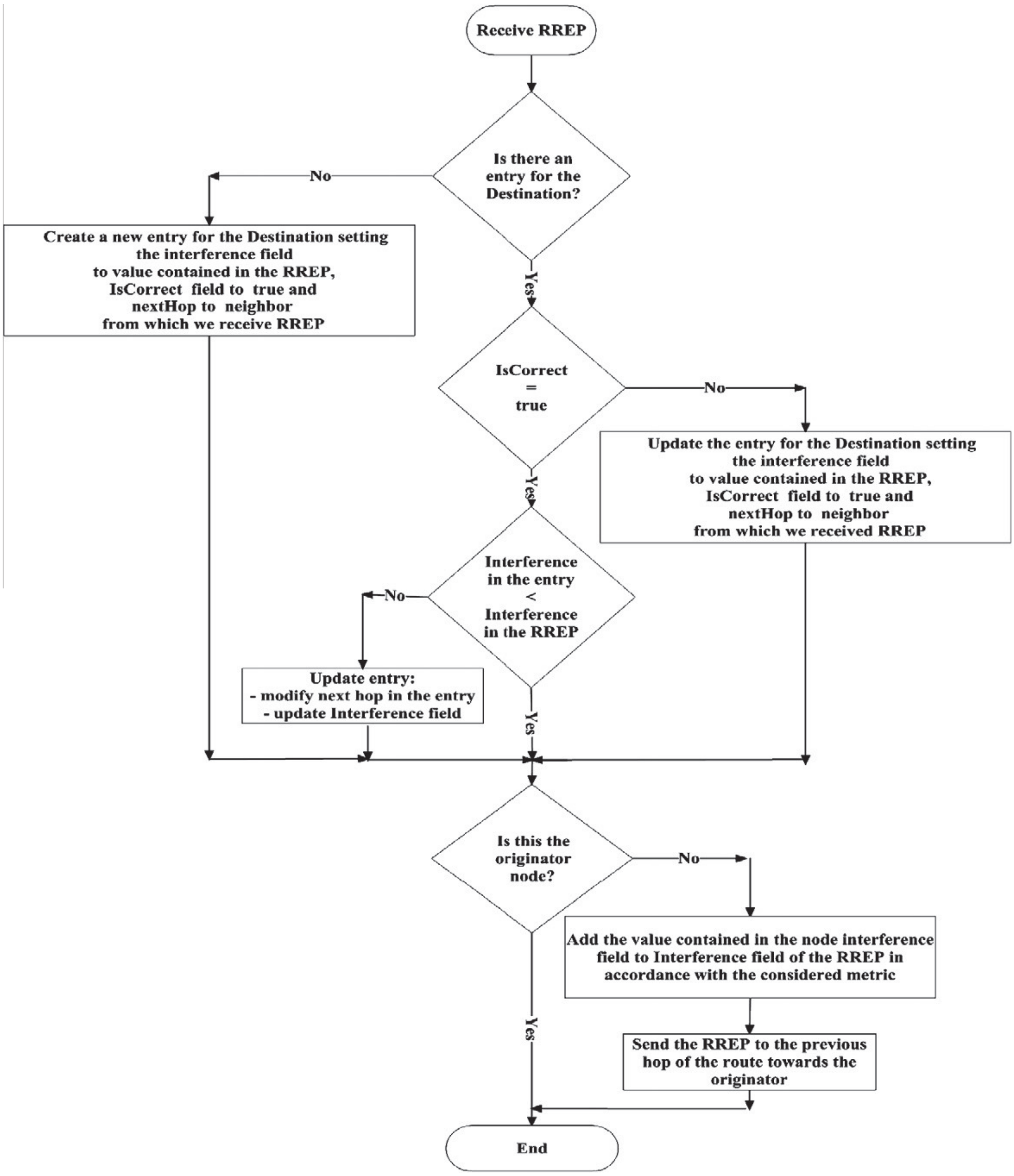

Receive RREP
Is there an entry for the Destination?
No
Create a new entry for the Destination setting the interference field to value contained in the RREP, IsCorrect field to true and nextHop to neighbor from which we receive RREP
Yes
IsCorrect = true
No
Update the entry for the Destination setting the interference field to value contained in the RREP, IsCorrect field to true and nextHop to neighbor from which we received RREP
Yes
Interference in the entry < Interference in the RREP
No
Update entry: - modify next hop in the entry - update Interference field
Yes
Is this the originator node?
No
Add the value contained in the node interference field to Interference field of the RREP in accordance with the considered metric
Send the RREP to the previous hop of the route towards the originator
Yes
End

Fig. 3. Procedures performed by a node at the reception of a RREP packet.

the link variation (in this case B). When node B receives the RERR, it drops all entries in the routing table having the node A as next hop because the interference toward the destination stored in the *Interference* field of that *entry* is no longer accurate. Then the node B informs, through the forwarding of an unicast RERR, all its precursor nodes involved in the interference variation of that route. The RERRs are forwarded backwards until all the nodes involved know the variation in the link B–A. In a similar way, in the *NI* metric, the nodes exchange information about significant interference variation. This procedure allows us to obtain the information about the interference of various links and nodes always updated in the network.

5. Performance evaluation

In the following, simulation results will be shown. In the first subsection some considerations about the α threshold, already discussed previously, will be given. Afterwards, a comparison between the proposed protocol, the standard AODV protocol and the interference aware protocols described in [25] will be presented.

In order to test our protocol, the NS-2 [30] simulator was used (for details, see [30]). In particular, we have extended the NS-2 UWB implementation available in [31].

Our protocol was tested considering the same reference scenarios: the nodes are randomly collocated on a 200 × 200 m grid, on which they move according to the *Random Waypoint* mobility model [32] with a speed variable in the range 1–4 m/s. Further simulation parameters are summarized in Table 1.

Performance evaluation has been carried out in terms of *Data Packet Delivery Ratio* (DPDR), *Average End-To-End Delay* (AED), *Normalized Routing Overhead* (NRO) and *Throughput* (THR).

5.1. Analysis of α threshold

As previously described, when a node perceives an interference variation greater than a given threshold α on a specific link, it invalidates the route involved in this variation. Furthermore, this could also mean sending RERR messages in that network portion and starting a search for a new route. Therefore, we can deduce that the choice of α is a very important issue because it can affect link refresh mechanisms: a too small α value could lead to frequent updates of the interference information that can cause a network traffic increment; on the other hand, too high α values would mean rare updates and so the information concerning interference could become obsolete. In order to find, in an experimental way, the value of α maximizing DPDR (this performance parameter is preferred to others because our main goal is to reduce interference and so the packet loss) many simulations were carried out. Simulation results show that the optimum value for α is around 5% independently of the number of nodes and maximum concurrent connections.

Table 1
Simulation parameters.

Parameter	Symbol	Value
Transmission power	*Pt*	0.280 mW
Nominal bit rate	*br*	18 Mbps
Bandwidth	*Bw*	5 GHz
Max speed	V_{MAX}	4 m/s
Packet size	P_{size}	512 Byte
Interval between packets	t_P	0.012 s
Node number	*N*	120, 140, 160,200
Max concurrent connection number	*Cmc*	4, 8, 12, 20
Observation time window	*OW*	10 s
Number of *WO* to consider for *NI* metric	*NSW*	5

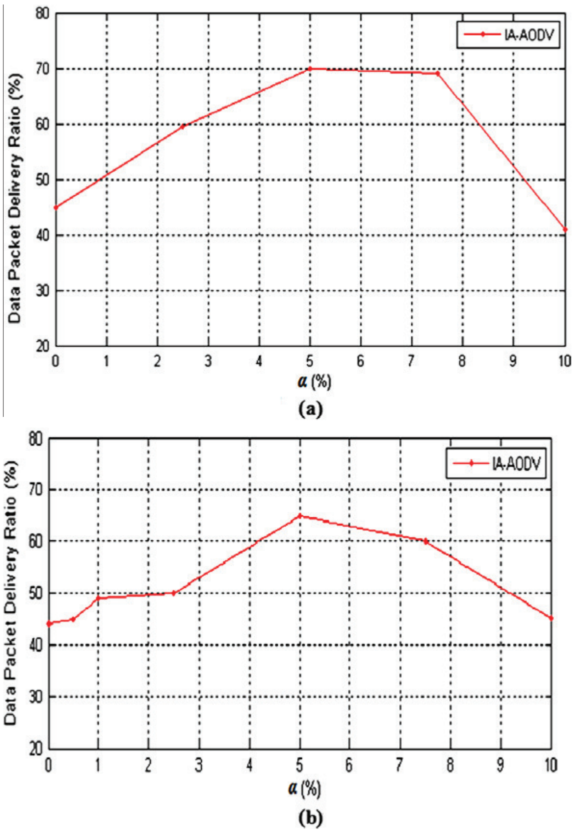


Fig. 4. (a) PDR vs. α, four maximum concurrent connections, 120 nodes. (b) PDR vs. α, eight maximum concurrent connections, 140 nodes.

In particular, in Fig. 4a, the PDR vs. α trend is shown for a scenario with four maximum concurrent connections and 120 nodes: in this case, we can see how the DPDR increases until $\alpha = 5\%$, it remains approximately constant and then it decreases for $\alpha > 8\%$. In order to verify our choice, the number of nodes and the maximum number of concurrent connections were increased respectively to 140 and 8. Even in this case the value of α, maximizing DPDR, is around 5%. Fig. 4b shows DPDR vs. α trend: we can see how, for this scenario, the advantages of the choice $\alpha = 5\%$ is even clearer. On the basis of these results, the protocol performance evaluation, shown in the following, sets the α parameter to 5%.

5.2. Simulation results analysis

Now we evaluate the performance of the proposed protocol varying the maximum number of concurrent connections and fixing the total number of nodes in the network. We consider a scenario in which 120 nodes move on a grid with a maximum speed of 4 m/s. A comparison with the performance obtained with some of the metrics proposed in [25,26] is made. We remember that for both metrics (*NI* or *LI*) the refresh mechanism is a procedure allowing to invalidates the routes, sending RRER packets, in presence of sensible interference variation in according to (12) (in this way, in the network, the information about interference will be always fresh). In absence of refresh mechanism (denoted with “no refresh”) the route can be invalidated only in presence of a link breakage similarly to the AODV standard.

Observing the DPDR (in percentage) curves depicted in Fig. 5, we immediately note how the *LI* metric with refresh mechanism shows a constant improvement with respect to AODV regardless of the number of concurrent connections. This improvement for the *LI* metric with refresh, although decreasing, remains however

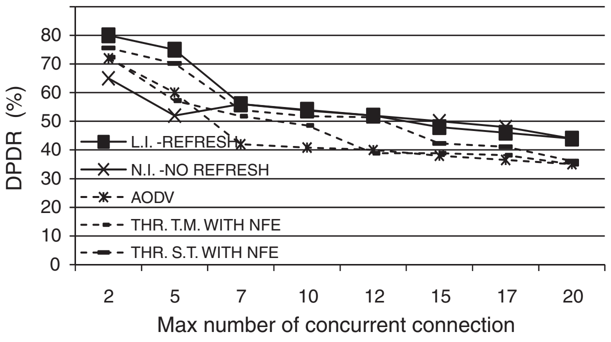


Fig. 5. DPDR vs. maximum number of concurrent connections, in presence of 120 nodes.

around 10%. On the other hand, the *NI* metric with refresh mechanism (not shown in the figure) leads to a decline in performance because the increase in the number of connections causes the increase in the total interference perceived by the nodes. Therefore, the greater amount of interference makes the links more unstable due to the increase in interference information update requests (considering the total interference perceived by a node, *NI* metric, a variation in a single link could cause an updating of all links involving the node). The *NI* metric without refresh is depicted in the figure, because it performs better than the case with refresh: its PDR is lower than the one of *LI* metric for a number of connections from 2 to 7; for higher number of connections, the performance of *LI* with refresh and *NI* without refresh are comparable. It can be seen that the proposed metrics outperform the Time Multiplexed with Near Far Effect (T.M. – with NFE) and Simultaneous Transmission with Near Far Effect (S.T. with NFE) with a threshold value of 20%. We have observed that a threshold value of 20% leads to the best performance for T.M and S.T. metrics; in addition the NFE coefficient has been considered because it enhances the performance.

Fig. 6 shows the curves relative to Average End-to-end Delay (AED) expressed in milliseconds (ms). We can see how, for the *LI* metric with refresh, the end-to-end delay is little influenced by the number of concurrent connections, at least in the presence of 120 nodes. These considerations can be partially made also for AODV and *LI* without refresh, while they cannot be made for the *NI* metric (independently of the refresh mechanism) because it shows an exponential increase in the delays. So, comparing *NI* also with the metrics proposed in [25,26] makes it unsuitable for a number of connections exceeding the value of 10. The *LI* metric (with refresh) shows best results if compared with other proposed schemes.

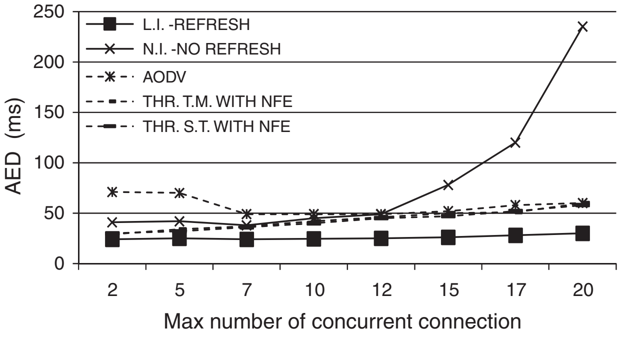


Fig. 6. AED vs. maximum number of concurrent connections, in presence of 120 nodes.

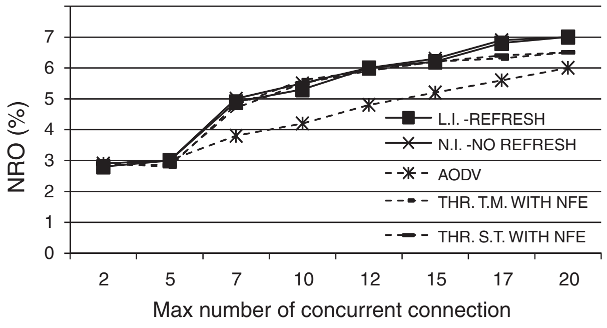


Fig. 7. NRO vs. maximum number of concurrent connections, in presence of 120 nodes.

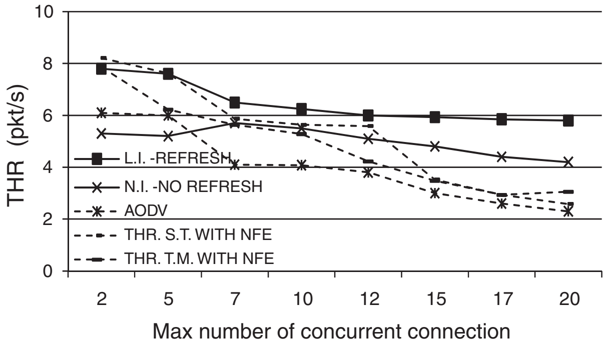


Fig. 8. THR vs. maximum number of concurrent connections, in presence of 120 nodes.

In Fig. 7, the trend of the Normalized Routing Overhead (NRO) in percentage vs. the number of concurrent connections is shown for all considered protocols and metrics. In this case, Interference Aware protocols cost slightly more in terms of NRO: IA-AODV (*NI* or *LI*), *ST* and *TM* show a NRO greater than 1–2 percentage points compared to AODV which increases with an increasing number of connections. We obtain this trend because the presence of a lower node number (120) leads to a less global interference, meaning also less link breakage and so less exchange of control messages for AODV. However, all the considered protocols show a NRO always less than 8%, offering comparable performance, so no one can be preferred in terms of introduced overhead.

Fig. 8 illustrates the obtained throughput (THR) expressed in packets/s: we can see how the *LI* (with refresh) metric outperforms the other metrics even if, in presence of a low-loaded network (<5 concurrent connections) the *ST* with NFE behaves slightly better than *LI*.

6. Conclusions

The traditional metric employed for narrowband wireless protocol, such as hop count, is not useful for architectures in which devices are very sensible to neighbor interference: this is the case of the UWB system whose nodes are affected by mutual reciprocal interference. For this purpose a new routing protocol called IA-AODV and based on the interference concept has been proposed. In particular, two metrics were proposed: the *NI* metric based on the global interference perceived by the node, and the *LI* metric based on the interference perceived only on the links involved in the communication. To take into account interference variation occurring in the network, a refresh mechanism was also introduced: in this way, we can quickly propagate this information to all nodes. Our protocol is compared with AODV and other Interference Aware (Time Multiplexed and Simultaneous Transmission) protocols in terms of DPDR, AED, NRO and THR. Simulation results show how IA-AODV performs better than the other protocols both in terms of DPDR and AED: e.g. for the DPDR, we obtain an average improvement of 10–15% with respect to AODV especially for the *LI* metric. *LI* presents also the lowest end-to-end delay, outperforming the other metrics. Generally, also the NRO trend of IA-AODV is comparable or better than other protocols. Furthermore, we note that in the presence of less dense scenarios (and so with a lesser global interference), IA-AODV has an overhead slightly higher than the AODV protocol: however this gap is on average around 1–2% and so it is negligible with respect to the improvement obtained in terms of DPDR and AED. Furthermore, we note that in the absence of the refresh mechanism our protocol performs comparably with AODV protocol because if the interference variation information is not propagated in the network, the nodes continue to transmit on corrupted links and this leads to the loss of many packets.

References

[1] A.F. Molisch, Ultra wideband propagation channels-theory, measurement, and modeling, IEEE Transaction on Vehicular Technology 54 (5) (2005).

[2] M.-G. Di Benedetto, G. Giancola, Understanding Ultra Wide Band Radio Fundamentals, Prentice Hall Pearson Education Inc, New Jersey, 2004.

[3] J.Y. Le Boudec, R. Merz, B. Radunovic, J. Widmer, A MAC protocol for UWB Very Low Power Mobile Ad-hoc Networks based on Dynamic Channel Coding with Interference Mitigation, EPFL Technical Report ID: IC/2004/02, 01-26-2004.

[4] J.Y. Le Boudec, R. Merz, B. Radunovic, J. Widmer. DCC-MAC: a decentralized mac protocol for 802.15.4a-like uwb mobile ad-hoc networks based on dynamic channel coding, in: Proceedings of Broadnets, San Jose, October 2004.

[5] B. Hu, N. Beaulieu, Accurate evaluation of multiple-access performance in th-ppm and th-bpsk uwb systems, IEEE Transactions on Communications 52 (10) (2004) 1758–1766.

[6] M.Z. Win, R.A. Scholtz, Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple-access communications, IEEE Transactions on Communications 48 (4) (2000) 679–691.

[7] F. De Rango, P. Fazio, F. Veltri, S. Marano, Interference aware routing protocols over ad hoc UWB networks, IEEE International Symposium on Wireless Communication Systems 2007 (ISWCS), Trondheim, Norway, October 16–19, 2007.

[8] F. De Rango, F. Veltri, D. Critelli, P. Fazio, S. Marano, Interference-Aware Ad-hoc on Demand Distance Vector (IA-AODV) Protocol, 2009 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS 2009), Istanbul, Turkey, July 13–16, 2009.

[9] C.E. Perkins, E.M. Belding-Royer, S. Das. Ad Hoc On Demand Distance Vector (AODV) Routing, IETF RFC 3561, 2003.

[10] F. De Rango, M. Gerla, K. Biao Zhou, S. Marano, GeO-LANMAR routing protocol: asymptotic analysis in large and dense ad hoc networks, in: 2nd Int. Conf. On Broadband Networks (Broadnet 2005), Boston, Massachusetts, USA, 3–7 October 2005.

[11] I. Stojmenovic, Position based routing in ad hoc networks, IEEE Communications Magazine 40 (7) (2002) 128–134.

networks, in: ACM/IEEE Proc. of Int. Conf. on Mobile Computing and Networking (MobiCom'00), Boston, Massachusetts, United States, 2000, pp. 243–254.

[13] S. Gezici, Z. Tian, G.B. Giannakis, H. Kobayashi, A.F. Molisch, H.V. Poor, Z. Sahinoglu, Localization via UWB Radios, IEEE Signal Processing Magazine 22 (4) (2005) 70–84.

[14] J.-Y. Lee, R.A. Scholtz, Ranging in a dense multipath environment using an UWB radio link, IEEE Transactions on Selected Areas in Communications 20 (9) (2002) 1677–1683.

[15] W.C. Chung, D.S. Ha, An accurate ultra wideband (UWB) ranging for precision asset location, in: Proc. IEEE Conference on Ultra Wideband Systems and Technologies (UWBST'03), Reston, VA, November, 2003, pp. 389–393.

[16] W. Horie, Y. Sanada, Novel Routing Schemes Based on Location Information for UWB Ad-Hoc Networks, Wiley Periodicals, Electronic and Comm. in Japan, Part 3, vol. 88, No. 2, 2005, pp. 22–30.

[17] L. De Nardis, P. Baldi, M.-G. Di Benedetto, UWB ad-hoc networks, in: Proc. of IEEE Conference on Ultra Wideband Systems and Technologies, 2002, pp. 219–224.

[18] D. Johnson, Y. Hu, D. Maltz, The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, Internet experimental RFC 4728, February 2007.

[19] E.M. Royer, C.-K. Toh, A review of current routing protocols for ad hoc mobile wireless networks, IEEE Personal Communications (2) (1999) 46–55.

[20] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, M. Degermark, Routing protocols for mobile ad-hoc networks – a comparative performance analysis, in: Proc. ACM/IEEE Mobicom, '99.

[21] L. Mal, Q. Zhang, F. An, X. Cheng, DIAR: A Dynamic Interference Aware Routing Protocol for IEEE 802.11-based Mobile Ad Hoc Networks in MSN 2005, pp. 508–517.

[22] L. Ma, Q. Zhang, Y. Xiong, W. Zhu, Interference aware metric for dense multi-hop wireless networks, in: IEEE International Conference on Communications (ICC'05), vol. 2, Issue, 16–20 May 2005, pp. 1261–1265.

[23] 802.15.4™ IEEE Standard, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std 802.15.4™-2003, October 2003.

[24] H.-Y. Wei, S. Ganguly, R. Izmailov, Z.J. Haas, Interference-aware IEEE 802.16 WiMax mesh networks, in: Proceedings of 61st IEEE Vehicular Technology Conference (VTC 2005 Spring), Stockholm, Sweden, May 29–June 1, 2005.

[25] H. Mahmood, C. Comaniciu, Interference aware cooperative routing for wireless ad hoc networks, Elsevier Ad Hoc Networks 7 (2009) 248–263.

[26] H. Comaniciu, Poor, On the Capacity of Mobile Ad Hoc Networks with Delay, 2005.

[27] B. Radunovic, J.Y. Le Boudec, Optimal power control, scheduling and routing in UWB networks, IEEE Journal on Selected Areas in Communications 22 (7) (2004) 1252–1270.

[28] S. Ghassemzadeh, R. Jana, C. Rice, W. Turin, V. Tarokh, Measurement and modeling of an ultra-wide bandwidth indoor channel, IEEE Transaction on Communication (2004) 1786–1796.

[29] F. De Rango, P. Fazio, F. Veltri, S. Marano, Time and distance dependent DS-SS UWB channel modeling: BER and PER evaluation, IEEE Vehicular Technology Conference 2006 Fall (VTC Fall 2006), Montréal, Canada, 25–28 September 2006.

[30] Available from: <http://www.isi.edu/nsnam/ns/>.

[31] R. Merz, J. Widmer, J.-Y. Le Boudec, B. Radunović, Ultra-wideband MAC and PHY layer implementation for ns-2, 2004. Available from: <http://icawww1.epfl.ch/uwb/>.

[32] C. Bettstetter, C. Wagner, The spatial node distribution of the random waypoint mobility model, in: Proceedings of German Workshop on Mobile Ad Hoc networks (WMAN), Ulm, Germany, March 2002.