Interference-Aware Ad-hoc on Demand Distance Vector (IA-AODV) Protocol

Floriano De Rango[1], Fiore Veltri[1], Domenico Critelli[2], Peppino Fazio[1], Salvatore Marano[1]
D.E.I.S. Department, University of Calabria, Italy, 87036
e-mail: [1]{derango, fveltri, pfazio, marano}@deis.unical.it; [2]dome.critelli@gmail.com

***Abstract*—Ultra-Wideband (UWB) is a promising technology for wireless personal area networks (WPANs) and Sensor networks. In particular, it is a viable candidate for short/medium-range communications. These motivations lead IEEE and scientific community to increase research on UWB technology. Many studies have been already addressed UWB physical and MAC problematic, but, at the present, many challenges are yet opened on the UWB routing level. However, traditional routing approach based on hop count or geometric criterions can be inadequate due to mutual interference affecting UWB nodes. The main goal of our work is to propose a new routing protocol, called Interference Aware-based Ad-hoc on Demand Distance Vector (IA-AODV), based on the concept of interference: the optimum route is chosen on the basis of the minimum perceived interference. Two distinct metrics are proposed: the first one based on the global interference perceived by a node (NI) and the other one based on the link interference (LI). To test the proposed protocol a ns-2 based simulator was realized. The two proposed metrics were compared with the AODV protocol in terms of packet delivery ratio, end-to-end delay and normalized overhead. Simulation results show as LI metric outperforms the others in all considered scenarios: only in few cases, LI IA-AODV presents an overhead slightly higher than AODV.**

Keywords—UWB routing; Interference Aware protocol; AODV; TH-UWB IR; DCC-MAC.

I. INTRODUCTION

Ultra-Wideband (UWB) technology is at present defined by the *Federal Communications Commission* (FCC) as any wireless transmission occupying a fractional bandwidth larger than 25% or an absolute bandwidth larger than 500MHz.. Such ultra-wide bandwidth gives to UWB system important advantages as low *Power Spectrum Density* (PSD) of the transmitted signal, that allows UWB system to coexist with narrowband radio systems operating in the same spectrum, better immunity to multipath propagation and low cost of devices [1].

At the best of our knowledge, many studies have been addressed UWB physical and MAC problems, but, at the present, many challenges are opened on the UWB routing level. Due to its physical characteristics and the mutual node interference, traditional ad-hoc network approaches, based for example on minimum hop count or geometric criterions, can be inadequate for these networks. The interference is the most undesired problem in UWB wireless network and it can cause an irretrievable degradation of communications [2]. Therefore, a routing protocol, that does not take into account directly interference "between the nodes, could lead to choose a path 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 metric are not defined in the routing protocols. For this reason a new protocol based on the concept of interference is proposed in this work. The proposed routing protocol employs as physical and MAC layers the *Dynamic Channel Coding-MAC* (DCC-MAC) model ([3],[4]). This MAC protocol allows devices to perform multiple parallel transmissions, adapting communications on the basis of interference perceived by the same devices. Furthermore, DCC-MAC employs an UWB impulse radio physical layer based on *time-hopping* (TH-UWB IR) as in ([5],[6]). Our protocol, called *Interference Aware-based Ad-hoc on Demand Distance Vector* (IA-AODV), lays its foundation in the classic *Ad-hoc On Demand Distance Vector* (AODV) protocol [7], of which inherits part of working operation and control packets, and in the *Interference Based On-Demand Routing Protocol* (IBOR) protocol [8], from which inherits the introduction of the interference concept in the selection of the optimum route. The novelty of the proposal is in the two distinct metrics adopted for the choice of the optimal route from the source to the destination: they are not based on the hop number, as the classic AODV, but on the global interference perceived by nodes (called *Node Interference*, NI, metric) and on the interference affecting the links involved in the transmission (called *Link Interference*, LI, metric). In order to verify the IA-AODV protocol goodness, a ns-2 simulator was realized and a comparison with AODV is carried out.

The paper is organized in this way: the related works are presented in Section II; reference scenario is described in Section III; IA-AODV protocol is well explained in Section IV; performance evaluation is shown in Section V and finally conclusions are summarized in Section VI.

II. RELATED WORKS

Generally, the classic ad-hoc network routing protocols employ metrics as minimum hop count [7] or geometric criterions ([9],[10],[11]). Therefore, ad-hoc routing algorithms must provide the optimum route adapting themselves, simultaneously, to the frequent and unpredictable network topology variation. Also some UWB routing algorithms make use of the high precision localization capability of UWB network ([12],[13],[14],) to chose the optimum route: using location information, nodes can choose to send packets to neighbors that are closer to the destinations [15]; moreover, in order to improve these mechanisms, cluster structure can be formed, and can lead to a routing algorithm described by [16]. 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, as the AODV [7], *Dynamic Source Routing* (DSR) [17], and others ([18],[19]), 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 metric are not defined in the routing protocols. Transmission interference is the most undesired problem for wireless communications. In the last few years, many new techniques have been proposed in order to reduce the effects of the 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 ([20],[21]) is one of the interference-aware routing protocols for IEEE 802.11 networks and it is based on the *Network Allocator Vector Count* (NAVC). Thanks to the simulation results obtained in ([20],[21]), it has been discovered that the NAVC is not sensitive to the total number of nodes in the system. If the path with the lower NAVC is chosen, then it will correspond to the one with a lower delay and a lower interference ([22],[18]). A similar approach is made in [19], 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 [23], the chosen interference-aware metric is different from the previous one: the authors make the assumption that if there is a higher number of neighbour nodes, a higher probability of interference for a node will be observed; for this reason, through the adopted metric, called blocking metric *B(k)*, 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 from it. In [8], the authors propose the IBOR protocol, in which the employed metric makes use of the interference level as the parameter to take routing decision: the optimum route is that one minimized the interference effects.

Starting from classic AODV protocol [7] and from IBOR protocol [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 LI metric, have been proposed in this work. AODV is a reactive routing protocol based on distance vector algorithm. A key feature of the this protocol are the "*sequence numbers*", which provide to node method to assess what is update a particular route.

We list in the following the most novelties introduced by our protocol:

- Our protocol introduces the concept of interference in the choice of optimum route improving in this way the general system performance: in fact, in a UWB network, the minimum hop route, as for examples in AODV, could not be an optimum choice because it could be affected by a high amount of interference that may make substantially impracticable the communication;
- Two distinct metrics are proposed: the first one, 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 on the only links belonging to the route from the source to the destination;
- Links refresh, provided by standard AODV, occur only in the presence of breakage of links and not when there is a substantial variation of interference. However, in the presence of scenarios with mobility, having the routing tables updated on the basis of important variation of the perceived interference, it 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.

III. REFERENCE SCENARIO

In this section, some considerations about reference physical and MAC layers are made. 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 are 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 about UWB network optimum planning is described in [24]. The authors drew the following conclusions: the optimum planning should not employ a power control and the sources should transmit with the maximum power; it is optimum in terms of throughput to allow the interfering sources to transmit concurrently on the condition that they are not in a well defined exclusion region around destinations and thus channel coding, and so data rate, must be adapted to the interference; on the other hand, interference into exclusion region must be contrasted.

These issues are the basis of DCC-MAC. Interference at the receiver is more harmful when the impulses of a neighbor interfering 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 to detect and erase 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). Contrarily to others schemes 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 others 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 better take advantages of channel, transmission needed to be constantly adapted to the higher code rate allowing a correct decoding at the receiver. Dynamic coding is performed through an hybrid *Automatic Retransmission request* (ARQ) protocol: if channel conditions degrade and the coding failed further information are sent until the packet is correctly decoded; if no further information are available, the transmission failed. Another issue regards the possibility of more nodes in transmission toward the same destination: the goal of the private MAC protocol is to enforce that several senders cannot communicate simultaneously with one destination: the private MAC solves this problem by a combination of 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 on the reception of a packet. Further details on this protocol can be found in ([3],[4]).

Finally, some considerations must be given on the channel model employed in our simulations. As in ([3],[4]), we used the propagation indoor model described in ([25],[26]): in particular, the power attenuation in decibel, due to distance, is at a given distance *d*:

$$\overline{PL(d)} = \left[PLo + 10\mu_\gamma \log d\right] + \left[10 n_1 \sigma_\gamma \log d + n_2 \mu_\sigma + n_2 n_3 \sigma_\sigma\right] \quad (1)$$

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 according to ([25],[26]), are modelled 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 the (1) represents the median path loss, whereas the second term is the random variation around median value. Further details are available in ([25],[26]).

IV. Interference Aware-based Ad hoc On Demand Distance Vector (IA-AODV)

The proposed protocol has as basis the classic AODV protocol, of which inherits part of working operation and control packets, and the IBOR protocol, from which we draws on the introduction of the interference concept.

The novelty of the proposal is in the two metrics adopted for the choice of the optimal route from the source to the destination and in the route maintenance: they are not based on the hop number, as the classic AODV, but on the global interference perceived by nodes, for the NI metric, and on the interference affecting the link involved in the transmission, for the LI metric. In order to realize these metrics, it has been needed to modify some control packets: in particular, the *Interference* field is added in the RREP and RREQ packets. The modified structures of the packets are respectively shown in Figure 1.a and Figure 1.b. The modification was made also at the entry of the routing tables: the field *HopCount*, the *Interference* field, in which is stored the interference from the node to the destination, and *IsCorrect* field, a boolean variable that indicates the validity or less of links, were added (see Figure 1.c). This last variable is needed because the interference on the link A-B could be different from that one on the link B-A, therefore we must be able to know if the value stored in the entry reefers to an interference perceived or transmitted by the node (this concept is better explained in the following). Others parameters needed to our protocol are given in the next subsection.

```
 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)

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

A. Analytic Formulation

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

- P_{BA} is the data packet that node B is sending to the node A;
- P_l is a generic data packet received in 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 receiving time for P_{BA} that is 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};
- $I_{P_{BA}}$ is the total perceived interference for P_{BA};
- *OW (Observation Window)* is the duration in seconds of a fix observation window in which we collect the information need to compute the interference;
- I_{P_l} is the total perceived interference for P_l;
- SPI_k (*Set of Packet Interference)* is defined as the set of I_{P_l} values observed during the *k*-th period OW_k;

- GI_k is the global interference perceived by a node during the k-th observation window OW_k;
- *NSW (Number of Stored OW)* is the number of *OW* that must be taken in account for the metric NI;
- *GI* is the global node interference employed in NI metric for a generic node;
- $I_{P_{BA_j}}$ is the interference perceived by A at the reception of *j* packet from node B;
- *m* is the number of packet 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 the 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*;
- I_{NI} is the NI metric;
- I_{LI} is the LI metric;
- α is a threshold that influences the occurrences of the interference information refresh;
- *SI* (*Stored Interference*) is the interference (global or on a link) stored by a node.

We suppose that a generic node A is receiving a packet, denoted by P_{BA}, from node B. During the reception of this packet, the 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 on the packet P_{BA}. This amount of interference is given by:

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

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

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

where TE_{PBA} and TS_{PBA} 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:

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

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:

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

We define now the NI metric. This metric can be defined by subdividing the temporal axis in *OW* in which a node receives a certain number of packets. We indicate with P_l a generic packet received during a *OW*, with I_{Pl} 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:

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

The *GI* that belongs to OW_k is:

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

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 NI metric, for a generic node is expressed as:

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

where *NSW* is the number of *GI* that must be taking 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 the route and the number of hops composing the route:

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

where *j* and *HopCount* are respectively the nodes indexes and the number of hops of the considered route. *S* and *D* is the source-destination pair.

After having introduced the global interference metric, now we proceed with the description of link interference metric LI.

The node A monitors the wireless link condition for each neighbor computing the interference perceived on every link. Regarding its neighbor B, the 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, the node A computes the average interference perceived on the link as:

$$I_{BA} = \left(\sum_{j=1}^{m} I_{P_{BA_j}} \right) \Big/ m \tag{10}$$

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

The proposed metric employs the link interference values 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:

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

where $\hat{ij}$ 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 computing in according with (10). The source will choose the most fresh route toward destination (managed with *sequence number* as in standard AODV) and with the lesser interference value, computing applying the (11).

B. Refresh Mechanism

Every node will store the average interference perceived on each path, linking it to its neighbors applying the (10), and the global value of interference computed applying the (8). However, these information can vary quickly 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 needed to invalidate all routes using that node to reach a generic destination.

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

$$\begin{cases} SI_k = SI_{k-1} & if \quad \dfrac{I - SI_{k-1}}{LI_{k-1}} < \alpha \\ \\ SI_k = I & if \quad \dfrac{I - SI_{k-1}}{SI_{k-1}} \geq \alpha \end{cases} \qquad (12)$$

In (12), SI_{k-1} is the value stored at the end of (*k-1*)-th iteration, while I is the interference computed in the *k*-th iteration applying, on the basis of the adopted metric, the (8) or the (10). The procedure for the LI metric is better shown in

Figure 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 contemplated by AODV protocol: this message is propagating to every node of the path toward destination *D* preceding the node discovering interference variation.

As shown in the following, the refresh mechanism is very important and it can significantly affect the system performance.

C. Route Discovery and Maintenance

When a source must communicate with another node of the network (called destination), 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, that is no *entry* is present or it is invalid, the originator starts the route discovery procedure: a RREQ packet, in which the *Interference* field is set to zero (others fields are set following standard AODV procedure), are sent in flooding. When a node receives a RREQ, it adds to the *Interference* field the stored value of interference (this value is stored in *SI);* therefore, if it has not an *entry* toward the originator, 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 source toward this node and it could be different from the interference on the backward route: we must avoid that others RREQs use this wrong information about interference to reach the originator 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 lesser than that one in the *entry* (*IsCorrect* field is not updated). In this way, the nodes, locally, make already a choice on the minimum interference route: if information updating about interference are made, the RREP will find fresh value and it will be forwarded automatically on the minimum interference route available until now. If the *IsCorrect* field is set to true, the *entry* is not modified in order to not wrongly change the information refereed to the correct direction toward originator.

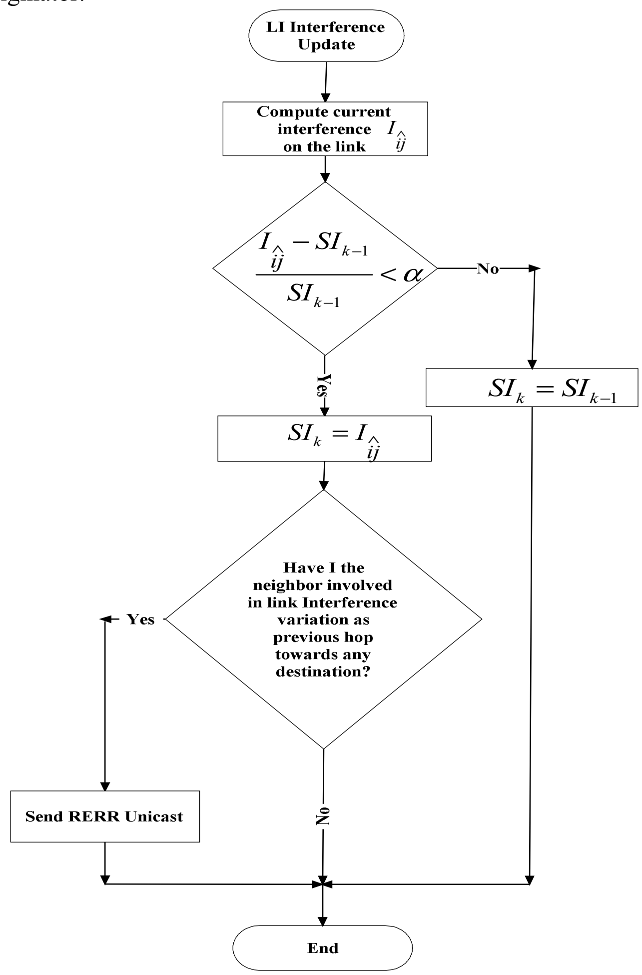

Figure 2. Interference Control on a generic link for the LI metric.

After these operations, the node must verify if it is the destination or if it has a valid route toward destination (we remember 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 originator through the nodes belonging to the route crossed by the RREQ (as in classic AODV). In particular, if the node is the destination, the interference value *SI*, stored by the node, is moved in the *Interference* field of the RREP; otherwise it must insert in the RREP the valued stored in the *Interference* field of the routing table *entry* relative to the destination at issue. After these operations, the RREP (with the remaining fields set in according to standard AODV) is forwarded to the previous hop of the route. 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 RERR message. In addition to these procedures, a further mechanism was introduced to take into account of sensible interference variation on. 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 the (10): if this interference is sensible varied respect to the previously stored value, that is in according to (12) an updating of *SI* is required, then the node A sends a particular unicast RERR to the neighbor node involved in the link variation (in this case B). When the 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 now not 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 backwards forwarded until all involved nodes know of the variation on the link B-A. In a similar way, in the NI metric, the nodes exchange information about sensible interference variation. This procedure allows us to have the information about the interference of various link and node always updated in the network.

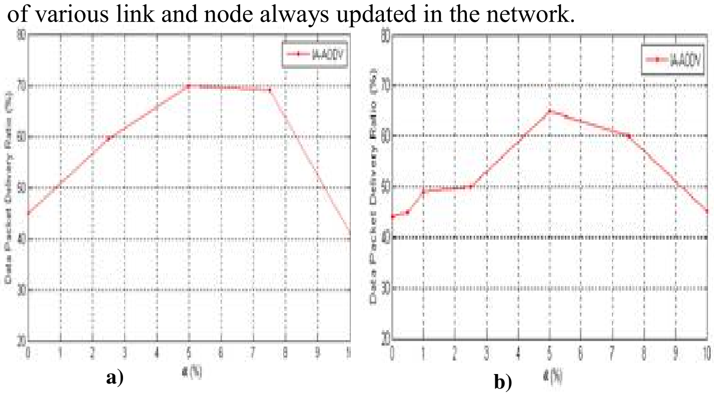

Figure 3. a) PDR vs. α, 4 maximum concurrent connections, 120 nodes. b) PDR vs. α, 8 maximum concurrent connections, 140 nodes.

Table I. 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	WO	10 *s*

V. PERFORMANCE EVALUATION

In this section, the simulation results will verify the improvements, introduced by IA-AODV, respect the AODV.

The simulator, taken into account for our tests, is *Network Simulator 2* (ns-2) and in particular, we have extended the ns-2 UWB implementation available on [27].

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

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

In the following, some consideration on the threshold α (see section 4.1) are made and then simulation results are shown.

A. Analysis of α threshold

When a node perceives an interference variation greater than a given threshold α on a generic node, it invalids the route involved in this variation. Furthermore, this could mean also to send RERR messages in that network portion and to start new route discovery. Therefore, we can deduce as the choice of parameter α is a very important issue because it can affect link refresh mechanisms: a too small α could lead to frequent updating of the interference information that can cause a network traffic increment; on the other hand, a too high α should mean rare updating and so the information concerning interference could become obsolete.

In order to find, in an experimental way, the value of α maximizing PDR (this performance parameter is preferred to others because our main goal is to reduce interference and so the packet loss) many simulations are carried out. Simulation results show that the optimum value for α is around 5% independently by node number and maximum concurrent connections. In particular, in Figure 3.a, the PDR vs. α trend is shown for a scenario with four maximum concurrent connections and 120 nodes: in this case, we can see as the PDR increases until α =5%, it remains approximately constant and then it decrease for α>8%. In order to better proof our choice, the number of nodes and the maximum number of concurrent connections were increased respectively to 140 and 8. Also in this case the value of α, maximizing PDR, is around 5%. Figure 3.b shows PDR vs. α trend: we can see as, for this scenario, the advantages to choose α=5% is even more clear.

On the basis of these results, the protocol performance evaluation, shown in the following, is made setting α parameter to 5%.

B. Simulation Results Analysis

In the first campaign, we analyze the system performance in function of node number, fixing the maximum number of concurrent connections to 12.

In Figure 4.a, the PDR is depicted: we can see as the data packet delivery ratio decreases to increase of node number. In fact, a greater number of nodes in the network means a greater device density in a specific area and so a higher interference. This causes a regular performance degrading. Furthermore, we can note as our metrics (specifically the LI metric), in absence of refresh mechanism show performance comparable with AODV protocol because, if the interference variation information are not propagated in the network, the nodes continue to transmit on corrupted links and this leads to lose many packets. If the refresh mechanism is introduced, the IA-AODV performance improves significantly; in particular, we can see as LI metric provides performance better than others: we have an improvement of 10% respect to refresh-based NI metric and 20% in comparison with AODV protocol and LI without refresh in terms of PDR. The best performance of the LI metric with refresh is even more evident from the analysis of AED in Figure 4.b. With the increase of the network node number, the average delay for NI metric with refresh and AODV protocols increase significantly, taking values very high in relation to the proposed protocol. On the other hand, LI metric without refresh shows performance comparable with refresh-based LI metric even if, in presence of dense scenario, the delays increase more quickly. In general, the increase of delay is very affected by the choice of route because the path at minimum interference reduces the number of retransmissions of lost packet owing to interference and therefore it leads to a minor processing time for each node belonging to the same route. What is said about the PDR and AED, it is confirmed by the analysis of NRO shown in Figure 4.c. In fact, the augment of the interference, due to a greater node number, leads to an increase of the NRO. However, in this case, the two protocols present comparable performance: IA-AODV shows an overhead taking values between 6%-8% on the basis of adopted metric, whereas the AODV protocol shows an overhead assuming values around 8% with a peak of 10% in presence of 200 nodes.

In the following, the performance of the proposed protocol are evaluated in function of the maximum number of concurrent connections fixing the total number of nodes in the network to 120. Also in this case, the nodes move on a grid with a maximum speed of 4 *m/s*. Observing the PDR curves depicted in Figure 4.d, we immediately note as IA-AODV with refresh mechanism shows a constant improvement respect AODV regardless of the number of connections. This improvement for the LI metric with refresh, although decreasing, remains however around 10%. However, in absence of refresh mechanism, AODV shows a PDR greater than IA-AODV due to greater interference present in the network with the increase of connections number. Figure 4.e shows the curves relative to AED. We can see as for refresh-based LI metric the end to end delay is very 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 refresh-based NI metric because it shows an exponential increase of the delays. In Figure 4.f, the trend of NRO vs. maximum number of concurrent connections is show for all considered protocols. In this case, our protocol pays slightly in terms of NRO: IA-AODV (with and without refresh mechanism) shows a NRO greater than 1-2 percentage points compared to AODV with a growing trend with increase of the connections number. We have this trend because the presence of a lower node number (that is 120) leads to a lower amount of global interference meaning also lower link breakage and so lesser exchange of control messages for AODV. However, our protocol shows a NRO always lower than 7%.

VI. CONCLUSIONS

Generally, the classic ad-hoc network routing protocols employ metrics as minimum hop count or geometric approaches. These can be useful in those architectures that are not affected by neighbor interference, but they are not valid for the UWB ad-hoc networks, in which the mutual nodes interference can cause serious problems also to the routing operations. For this purpose, in this work, a new routing protocol for UWB network, IA-AODV, based on the concept of interference, has been proposed. In particular, two metrics were proposed: the first one based on the global interference perceived by nodes, called NI metric, and the other based on the interference affecting the link involved in the transmission, called the LI metric. Furthermore, a refresh mechanism was introduced in order to more quickly propagate in the network information about interference variation. Our protocol is compared with the AODV protocol in terms of PDR, AED and NRO: for this purpose a ns-2 simulator has been implemented. Simulation results show as IA-AODV with refresh mechanism performs better than others protocol both in terms of PDR and AED: e.g. for the PDR, we obtain an average improvement of 15% respect to AODV especially for the LI metric. Generally, also NRO trend of IA-AODV is comparable (or better) to others protocols. Furthermore, we note that in absence of refresh mechanism our protocol shows performance comparable with AODV protocol because, if the interference variation information are not propagated in the network, the nodes continue to transmit on corrupted links and this leads to lose many packets.

REFERENCE

[1]. A. F. Molisch, “Ultrawideband Propagation Channels-Theory, Measurement, and Modeling”, *IEEE Transaction on Vehicular Technology*, VOL. 54, NO. 5, September 2005.

[2]. M.-G. Di Benedetto and 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 and 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, and 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 and N. Beaulieu. Accurate evaluation of multiple-access performance in th-ppm and th-bpsk uwb systems. *IEEE Transactions on Communications*, 52(10):1758–1766, October 2004.

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

[7]. Charles E. Perkins, Elizabeth M. Belding-Royer, and Samir Das. "Ad Hoc On Demand Distance Vector (AODV) Routing." IETF RFC 3561.

[8]. Floriano De Rango, Peppino Fazio, Fiore Veltri, Salvatore Marano, “Interference Aware Routing Protocols over Ad Hoc UWB Networks”, *IEEE International Symposium on Wireless Communication Systems 2007 (ISWCS)*, October 16-19 2007, Trondheim, Norway.

[9]. F. De Rango, M.Gerla, K.Biao Zhou, S.Marano, “GeO-LANMAR Routing Protocol: Asymptotic Analysis in Large and Dense Ad Hoc Networks,” *2nd Int. Conf. On Broadband Networks (Broadnet 2005)*, 3-7 Oct., Boston, Massachusetts, USA, 2005.

[10]. I. Stojmenovic, Position based routing in ad hoc networks, *IEEE Communications Magazine*, Vol. 40, No. 7, July 2002, 128-134.

[11]. B.Karp, H.T.Kung, “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks,” in ACM/IEEE *Proc. of of Int. Conf. on Mobile Computing and Networking (MobiCom’00)*, Boston, Massachusetts, United States, pp.243-254, 2000.

[12]. S. Gezici, Z. Tian, G. B. Giannakis, H. Kobayashi, A. F. Molisch, H. V. Poor and Z. Sahinoglu, “Localization via UWB Radios,” *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 70-84, July 2005.

[13]. J-Y. Lee and R. A. Scholtz, “Ranging in a dense multipath environment using an UWB radio link,” *IEEE Transactions on Selected Areas in Communications*, vol. 20, no. 9, pp. 1677-1683, Dec. 2002.

[14]. W. C. Chung and D. S. Ha, “An accurate ultra wideband (UWB) ranging for precision asset location,” *Proc. IEEE Conference on Ultra Wideband Systems and Technologies (UWBST’03)*, pp. 389-393, Reston, VA, Nov. 2003.

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

[16]. L. De Nardis, P. Baldi and M.-G. Di Benedetto, "UWB Ad-Hoc Networks," *Proc. of IEEE Conference on Ultra Wideband Systems and Technologies*, pp.219-224, 2002.

[17]. 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.

[18]. Elizabeth M. Royer, Chai-Keong Toh, "A review of current routing protocols for ad hoc mobile wireless networks", *IEEE Personal Communications,* no. 2, April 1999 pp. 46-55.

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

[20]. Liran Mal, Qian Zhang, Fengguang An, and Xiuzhen Cheng, "DIAR: A Dynamic Interference Aware Routing Protocol for IEEE 802.11-based Mobile Ad Hoc Networks" *in MSN 2005*, pp.508-517.

[21]. Liran Ma, Qian Zhang, Yongqiang Xiong, and Wenwu 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.

[22]. 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.

[23]. Hung-Yu Wei, Samrat Ganguly, Rauf Izmailov, Zygmunt 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.

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

[25]. S. Ghassemzadeh, R. Jana, C. Rice, W. Turin, and V. Tarokh, "Measurement and modeling of an ultra-wide bandwidth indoor channel," *IEEE Transaction on Commun*., pp. 1786–1796, 2004.

[26]. Floriano De Rango, Peppino Fazio, Fiore Veltri and Salvatore Marano, "Time and Distance Dependent DS-SS UWB Channel Modeling: BER and PER Evaluation", *IEEE Vehicular Technology Conference 2006 Fall (VTC Fall 2006)*, 25 – 28 September 2006, Montréal, Canada

[27]. Ruben Merz, Jörg Widmer, Jean-Yves Le Boudec, Božidar Radunović, "Ultra-wideband MAC and PHY layer implementation for ns-2", 2004. Available on http://icawww1.epfl.ch/uwb/ .

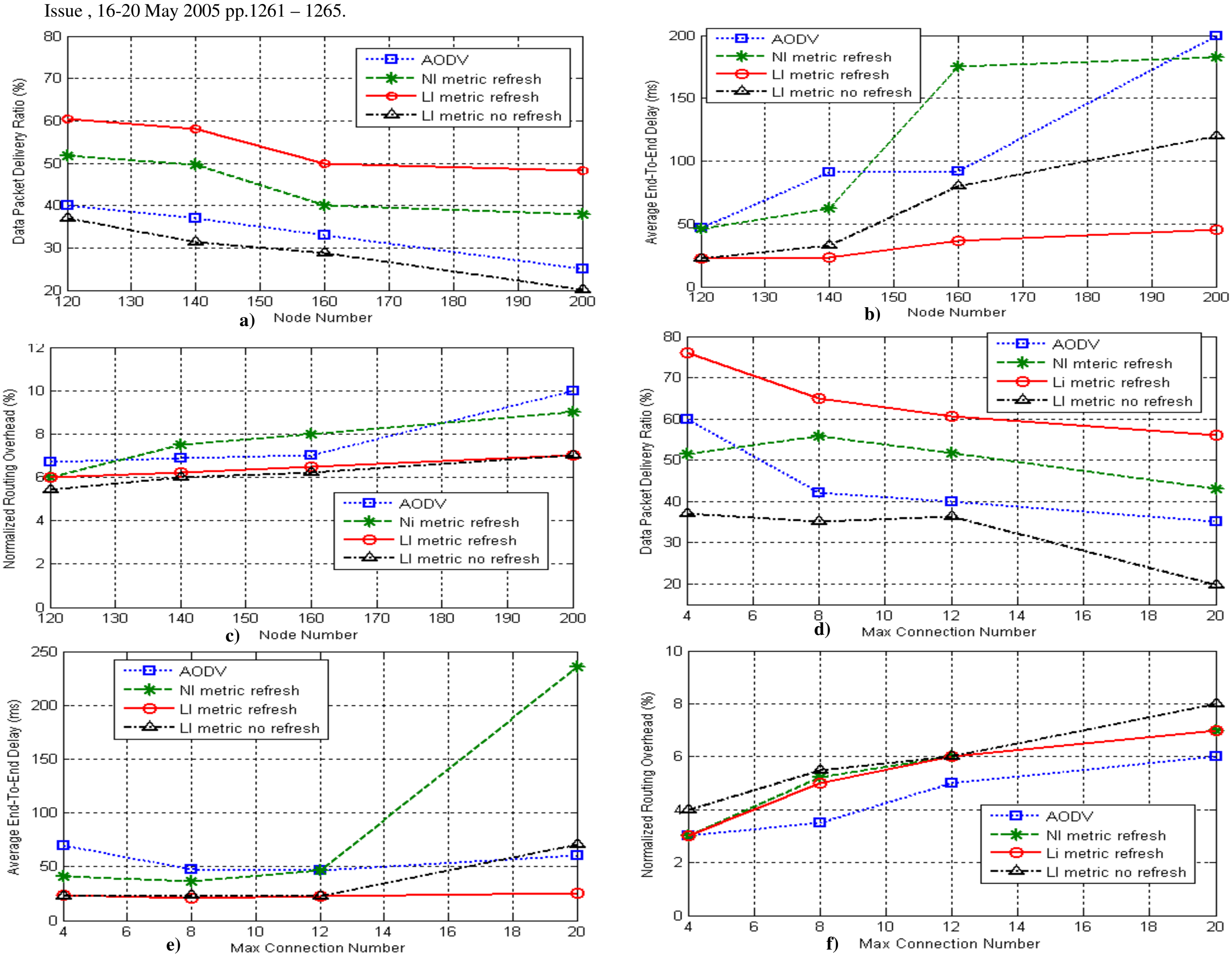

Figure 4. a) PDR vs. node number in presence of 12 maximum concurrent connections. b) AED vs. node number in presence of 12 maximum concurrent connections. c) NRO vs. node number in presence of 12 maximum concurrent connections. d) PDR vs. concurrent connection maximum number with 120 nodes. e) AED vs. concurrent connection maximum number with 120 nodes. f) NRO vs. concurrent connection maximum number with 120 nodes.