Interference Aware Routing Protocols over Ad Hoc UWB Networks

Floriano De Rango, Peppino Fazio, Fiore Veltri, Salvatore Marano

D.E.I.S. Dept., University of Calabria, ITALY e-mail: {derango, pfazio, fveltri, marano}@deis.unical.it

Abstract— UWB technology is considered as the best way to implement high speed WPAN with low costs and good commercial reliability. All the standards concerning the UWB address the problems that regard the PHY and the MAC layers of the ISO/OSI stack, while actually there is not enough work about the development of the Network layer of the UWB systems. Common routing protocols used in the Ad-Hoc Networks, like the AODV, do not take into account "inter-node" interference, for this purpose in this work new routing metrics are proposed for the implementation of interference-aware routing protocols. These new proposed metrics are finally compared with the AODV protocol in order to proof the better efficiency of our proposal.

I. Introduction

In the last few years there has been a growing interest in Ultra Wideband Technology (UWB), since it is considered as the best way to implement high speed Wireless Personal Area Networks (WPAN), with low costs and good commercial reliability [1]. These features led to the development of many projects related to UWB technology. The main contribution of the scientific community has been focused on the definition of the Physical Layer and the MAC layer, however, among the previous proposals, only the 802.15.3 and 802.15.4 [2] standards are available at the IEEE. All the above standards address the problems that regard the PHY and the MAC layers, so there is not enough work about the development of the Network layer. UWB technology needs some additional work, in order to define new metrics and new routing protocols that can increase systems performances, taking advantage of UWB technology peculiarities. Classical routing protocols used in the Ad-Hoc Wireless Networks use some metrics like the Minimum Hop-Count or some criterions based on system geometry. This kind of approach can be suitable in those architectures that are not affected by "neighbour-nodes" interferences, obtaining good performances. The same argumentation cannot be made for UWB systems. Common Routing protocols used in the Ad-Hoc Networks, like the Ad-Hoc on Demand Distance Vector (AODV) [3], Dynamic Source Routing (DSR) and so on ([4],[5]), do not take into account "inter-node" interference. In this way, the choice of a path on which the packet must travel from source to destination can be wrong in terms of signal degradation: the distance between source and destination can be minimized, but the interference level may be too high, if new metrics are not defined in the routing protocol. Owing to the above problems, it is necessary to introduce some indexes related to the interference level among the wireless system nodes in order to define some new metrics that can make the routing

protocol able to choose the proper paths, minimizing the interference over the paths or over the entire system. Therefore the goal of this work is the proposal of a new routing metrics for the implementation of interference-aware routing protocols for Wireless Ad-Hoc UWB networks; moreover we proofed that these new protocols can lead to better performances, if compared to those of the classical routing protocols. The paper is organized as follows: section II gives a brief overview of the work related to the interference aware routing; proposed algorithms are presented in section III; implementation issues are discussed in section IV; section V presents the performance evaluation and finally conclusions are summarized in the last section.

II. RELATED WORK

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 degrades the path-delay and, so, the datarate. The older interference-aware metrics tried to optimize these parameters: the DIAR ([6],[7]) 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 ([6],[7]) 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 ([2],[4]). A similar approach is made in [8], where the employed metric chooses the path with the lower path delay, defined as the interval between the Route REQuest (RREQ) dispatch and the related Route REPly (RREP) reception [1]. In [9] 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 [11] a routing protocol, called power-efficient, is proposed and in particular it is suitable for UWB networks with ranging. It uses a metric based on a cost function, that reduces the emitted power for all the system

nodes, decreasing the Multiuser Interference (MUI) level.

III. INTERFERENCE AWARE ROUTING ALGORITHMS

In this section some novel Interference Aware Routing algorithms are presented. The metrics that make of the interference level the parameter to take routing decisions are called Interference-Aware metrics. Up to now, most of the Interference-Aware protocols use the effects of interference on the system in order to estimate the interference level and to choose the paths, minimizing the interference effects [10]. This paper presents novel routing algorithms based on two kinds of interference metrics: node interference and node coverage. The reference architecture used in this work uses the PHY/MAC layers as defined in DCC-MAC [12]. It neglects the collision-avoidance mechanisms based on the exclusion zones around nodes and it introduces the Interference Mitigation mechanisms, based on the physical model proposed in [12]. The Interference Mitigation mechanism uses the *Erasure* concept, that consists in erasing the samples generated by one collision between impulses with a big interference and to replace them with one Erasure. For further details please refer to [12].

A. Interference Based On-Demand Routing Protocol (IBOR)

IBOR is an *Interference-Aware* routing protocol for ad-hoc wireless *UWB* networks, which uses a metric based on the interference perceived by system nodes. Interference can be defined in different ways.

Packet Interference (PI) is the interference contribution, expressed in Watts, generated by a packet that is interfering on the currently received packet. If a node A is receiving the packet p_0 and, at the same time, it is listening for the $p_1, ..., p_n$ packets arrivals, then each p_i packet with $i \in (1,...n)$ generates an interference contribution on the receiving node A. Each contribution is called Packet Interference (PI). For the specific case of the DCC-MAC architecture, it can occur if a receiving node A, during the reception of the data packets from the transmitting node B on the private Time Hopping Sequence THS(AB), listens on a THS near to THS(AB) the arrival of other packets (Fig. 1). In an analytical way, the Packet Interference PI_i related to the interfering packet i is:

$$PI_{i} = RP_{i} \cdot CTC_{i} \tag{1}$$

where RP_i (Received Power) is the received power of the packet p_i and CTC_i (Collision Time Coefficient) is the time fraction of the receiving time for p_0 that is affected by the interference of the packet p_i . The Collision Time Coefficient CTC_i is defined as:

$$CTC_i = IfI_i / (RE_0 - RS_0)$$
 (2)

where RE_0 and RE_i are respectively *Receiving End time* for the packet p_0 and p_i , while RS_0 and RS_i are respectively *Receiving Start time* for the packet p_0 and p_i . Instead *ifI* (*Interfering Interval*) is the time duration of the interference caused by packet p_i and it is defined as:

$$ifI_i = \min(RE_0, RE_i) - \max(RS_0, RS_i)$$
(3)

The total Packet Interference (PI) is instead given by:

$$PI = \sum_{i=1}^{n} RP_i \cdot CTC_i \tag{4}$$

The *PI* is used for defining the *Period Interference* (*ifPeriod*), that is a periodic evaluation of the interference that affects the receiving node in each observation period. Therefore, *ifPeriod* is the average of the *PI* samples, collected in a fixed observation period of *IF CAL PERIOD* seconds.

This metric can be defined by subdividing the temporal axis in a certain number of observation periods of IF_CAL_PERIOD seconds; after, the $ifList_k$ is defined as the set of PI values observed during the k-th period $IF_CAL_PERIOD_k$. Analytically, the set $ifList_k$ can be expressed as:

$$ifList_k = \{PI_{xc} \mid rxStart_c \in IF_CAL_PERIOD_k \land rxStap_c \in IF_CAL_PERIOD_k\}$$
 (5)

where rxStart and rxStop are respectively the beginning and the ending time of interfering packet p_c just listened to.

The *ifPeriod* that belongs to $IF_CAL_PERIOD_k$ is:

$$ifPeriod_k = \sum_{j}^{|ifList_k|} ifList(j) / |ifList_k|$$
 (6)

where ifList(j) is the j-th element of the $ifList_k$ set.

From the definition of *PI* the *Node Interference* (*NI*) can be derived, as a parameter for evaluating the interference observed by a certain node.

NI: it is the average of the last ifStory Period Interference values for a generic node A, where ifStory is the number of observation periods that must be taken in account.

The *Node Interference* for *A* is expressed as:

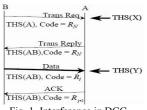
$$NI_A = \sum_{m}^{ifStory} ifPeriod_m / ifStory$$
 (7)

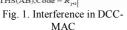
The *IBOR* protocol is based on the *Interference metric*, calculated as the ratio between the sum of the interference *NI* of each node on the path and the number of hops that compose the path:

$$Interference(s,d) = \sum_{j \in Path(s,d)} NI_j / Hop _Count_{Path(s,d)}$$
 (8)

where j and Hop_Count are the nodes indexes and the number of hops on the considered path respectively. s and d is the source-destination pair. Path(s,d) is the set of nodes belonging to the path from s to d.

The IBOR is an On-Demand protocol and it uses the classical path construction method, based on the RREO and RREP cycle. For every sent RREQ, the source node S receives the RREP as answers. Each couple (RREQ, RREP) represents a different path from the source S to the destination D. Let us now consider only RREP messages. Each RREP contains the Interference and Hop Count fields. The Interference field contains the sum of the Node Interference values of the nodes belonging to the path. The Hop Count field contains the number of hops that compose the path associated with the RREP. If i is the index associated to the RREP (that is to say associated to the paths that RREP is traversing), then S will choose the path i, associated with the $RREP_i$ with the lowest Interference_i/Hop_Count_i value. The Interference Metric expresses the average interference value on the links that belong to the path. It indicates the average interference level that packets will suffer along the path. The use of the average values, calculated as the average on the observation periods,





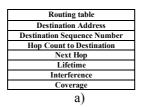
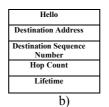


Fig. 2.a) Routing Table of the M-CIBOR protocol. b) HELLO packet





RREP
Source Address
Destination Address
Destination Sequence N°
Hop Count
Lifetime
Interference
Coverage
b)

Fig. 3.a) RREQ packet for M-CIBOR. b) The RREP packet of the M-CIBOR

allows the protocol to consider the actual interference level or the long range interference over the path.

B. Coverage Based On-Demand Routing Protocol (CBOR)

CBOR uses a metric based on the nodes coverage of the system. The *interference aware* nature of the protocol is given by the use of a metric that employs the nodes coverage definition in order to evaluate the interference of the system. The Coverage of a node is given by the number of directly covered neighbour nodes. More details about the Coverage concept can be found in [9] and [13]. The interference on a receiver node is caused by the overlapping of one or more transmissions on the signal that the node is currently receiving. Supposing that a node can listen to one or more transmissions simultaneously, the higher number of interfering signals, the higher interference that affects the receiver node. So the number of neighbour nodes directly covered can be used to estimate the interference that the receiver node observes. The neighbour nodes of a generic receiver node can assume three different states: receiving, transmitting and waiting. Only the neighbour nodes that are in the transmitting state can generate interference, so the Coverage value of a node expresses the probability of having a high interference value. Assigning to each node the same probability of being in the transmitting state, a node with a higher Coverage will have a higher probability of being subject to a higher level of interference. The definition of Coverage is well-explained as follows. The temporal axis is subdivided into a certain number of observation periods of CVG PERIOD seconds. Let cvgList_k be the set of different nodes from which the generic node A has received at least one *HELLO* message during the k-th observation CVG PERIOD_k. The Coverage of the node A is equal to the cardinality of the $cvgList_k$ set, where $CVG\ PERIOD_k$ is the last observation period just elapsed:

$$Coverage_{A} = |cvgList_{k}| \tag{9}$$

The dimension of the CVG_PERIOD is a planning parameter of primary importance. Its dimension must not be inferior to the period of the HELLO packet transmission. The Interference-Aware metric, employed by the CBOR protocol is called Coverage metric. It is defined as the sum of the Coverage value of each node belonging to the path:

$$Coverage = \sum_{j \in Path(s,d)} Coverage_j$$
 (10)

where j is the index of the nodes that belong to the path. This kind of metric takes into account not only the probability of the interference level that can affect the packets that are travelling through the considered path, but it also considers

the level of interference that affects the nodes that are directly covered by the nodes that belong to the path. A generic node T will select a path to the destination considering the packet RREQ or RREP with the lowest Coverage value.

C. Multiplication Coverage for Interference Based Ondemand Routing Protocol (M-CIBOR)

M-CIBOR mixes the characteristics of the IBOR and CBOR protocols. The purpose of the M-CIBOR protocol is to join the previous protocols characteristics, by the definition of a multiplicative metric called Inter-Cov metric. The evaluation indexes used by the M-CIBOR protocol are the Node-Interference and the Coverage, defined by (7) and (9) respectively. The Inter-Cov metric is obtained from the product of the indexes of the Interference and Coverage metrics. It is expressed as follows:

$$Inter - Cov_k = Interference_k \cdot Coverage_k \tag{11}$$

where k is the index associated with the considered path.

The path-construction mechanism is the same as the previous protocols, based on the RREQ, RREP messages. When a node receives an RREQ or RREP message, the path associated with the packet with the lowest value of Inter-Cov will be selected. This joined-metric permits to face the potential interference associated to the topology (node density) and the interference associated to the nodes activity (control and data traffic) and it addresses towards the selection of the lowest interference path.

IV. PACKET STRUCTURE MODIFICATIONS

The above protocols are AODV-like on-demand protocols [3] and they take the advantage of its mechanisms: collecting routing information and their synchronization are the tasks that are managed in the same way as the AODV. Each node stores the routing information in the Routing Table, which contains some tuples as illustrated in Fig. 2.a. The *Destination* Address, Destination Sequence Number and Hop Count To Destination fields contain the destination node address, the last sequence number received by the first node which created the path, the hop number of the path associated with the tuple. The Next-Hop field contains the address of the node that must receive the packets destined to the node specified in the Destination Address field. The path associated with the tuple can be considered valid before Lifetime units of time. The *Interference* and *Coverage* fields contain the average value of the Node Interference and the sum of the Coverage values of the nodes that belong to the path. When a node becomes aware of a path with a higher sequence number than the value

stored in the Destination Sequence Number field of the path tuple, it updates the Routing Table, by substituting the path information in the tuple. The paths, that are associated with tuples that have a *Lifetime* field that is lower or equal to the current time, are not considered as valid paths. The Lifetime value is updated every time the node specified in the Next-Hop field generates or forwards a packet to the destination of the path. System nodes are acquainted with the neighbour nodes with the RREQ, RREP mechanism or with other particular messages called HELLO packets. Each HELLO packet contains four fields: Destination Address and Destination Sequence Number that contain the address and the sequence number of the node that sends the packet; the Hop-Count field contains the number of hops that the packet has passed and the *Lifetime* field containing the time instant value before which the sender of the HELLO packet still has to be considered under radio coverage (see Fig. 2.b). Each node periodically sends a broadcast packet that contains the *HELLO* message. In this way each node can maintain a list of system nodes that are directly connected to it and the associated Lifetime value. When a node receives a HELLO message, it updates the information about the neighbour nodes, then it destroys the packet. When the Hop-Count in the HELLO message is higher or equal to 1, it must immediately discard the packet, because it cannot be considered a valid message. Periodically, the information about the local connectivity is changed and all the nodes that have an associated Lifetime field that is lower than the current time are deleted from the neighbour list. The Lifetime value associated to each neighbour node is updated every time a HELLO message is received by the considered node. The HELLO messages are used for the calculation of the Coverage value. At the end of the transmission of each data packet, the source node S verifies the presence of the destination node D inside the Destination Address field of the tuples of the own Routing Table. If the information is not present, then S activates the path discovery process, by sending a path request through a broadcast RREQ message. The structure of the RREQ packets is depicted in Fig. 3.a. When the RREO packet arrives at destination D or to an intermediate node that has knowledge of a valid path to D, a RREP packet is generated. Fig. 3.b depicts the structure of the RREP packet. In the RREP packet, the Source Address field contains the address of the node that sends the packet, the Destination Address and Destination Sequence Number contain the address of the node that has created the RREP packet and the last known sequence number for the destination node of the path. The Hop-Count value is initially set to zero. The *Lifetime* field contains the time instant before which it is possible to consider the path associated with the RREP packet as a valid path. When the RREP packet is generated, the Coverage field and the Interference field contain the Coverage and the Node Interference values of the node that generates the packet.

V. PERFORMANCE EVALUATION

In this section the simulation scenario is briefly described and simulation results that account the evaluation indexes typical of wireless ad hoc networks are presented.

A. Simulation Scenario

Our simulation tool is the famous network simulator NS-2. version 2.26. This version of NS-2 does not directly support wireless networks with UWB technology, so we used the UWB implementation, developed at Ecole Polytechnique Fédérale de Lausanne (EPFL). Performance evaluation of proposed protocols has been carried out by considering UWB physical layer and 802.15.4 MAC protocol. Performances of the proposed protocols are compared with those of the reference AODV protocol. The evaluation of the performances is carried out through the analysis of the *Packet Delivery Ratio* (PDR), the Average End-To-End Delay (AED) and the Normalized Routing Overhead (NRO). NRO is expressed as the ratio between the control packets and the data packet received at the destination. The analysis of the performances is carried out through the study of a simulative scenario, characterized by a 200m x 200m grid, on which a high number of nodes moves according to the Random Waypoint mobility model. Every node transmits with a power of approximately $0.283 \cdot 10^3$ W, that permits a transmission range of approximately 60m. Simulated time is 400s.

B. Simulation Results

Performance Analysis vs. Number of Nodes: We consider some networks with a maximum of four concurrent connections, where the nodes move with maximum speed of 4 m/s. The PDR, such as shown in Fig. 4, is monotonically decreasing because the increasing number of nodes determines a greater interference with a consequent packet delivery reduction. However CBOR, IBOR and M-CIBOR outperforms AODV through a better path selection. In Fig.5. we can see as AODV presents also a greater average end-toend delay due always to the greater interference around the selected path and to the higher number of retransmissions at MAC layer. IBOR, CBOR and M-CIBOR improve the performances also in terms of average end-to-end delay. Everything illustrated for PDR finds confirmation by NRO analysis, shown in Fig. 6. Increasing the interference leads to higher values of NRO. There is a great difference between Interference Aware protocols and AODV, when the nodes density is high. By increasing nodes density, AODV always chooses shorter paths, while the proposed protocols tend to choose paths with a length that is quite constant. In this way, the number of generated control packets increases.

2) Performance Evaluation vs. Number of Connections: Considering a network scenario in which 140 nodes that move on a grid with a maximum speed of 4 m/s. An increasing of the number of connections in the network causes an increasing of the network interference, so the PDR decreases (this trend can be observed in Fig. 7). Observing the increasing difference between the PDR of AODV and the proposed protocols when the number of connections increases, it can be seen that the proposed protocols perform better. The previous performance description is also valid for AED, shown in Fig. 8. Also in this case, better performances are obtained by M-CIBOR, IBOR and CBOR protocols. However it can be observed as IBOR and M-CIBOR perform better than CBOR

due to the metric that account for the interference associated to the node activity (traffic). On the other hand, CBOR outperforms IBOR in the first simulation campaign, because it accounts for the node density. It is possible to observe also how M-CIBOR is the best metric, because it can account at the same time of traffic and node density such as confirmed by two simulation campaigns.

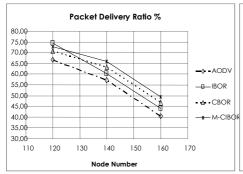
VI. CONCLUSIONS

In this work interference-aware routing protocols (*IBOR*, *CBOR* and *M-CIBOR*) for wireless Ad-Hoc UWB networks based on 802.15.4a standard have been proposed. These protocols are compared with the *AODV* protocol in terms of *PDR*, *AED* and *NRO*. In particular we have carried out two distinct simulation campaigns: the first one analyzes the previous indexes as a function of nodes number, while the second analyzes them in terms of connections number. Both campaigns proofed that all our protocols are more performing than *AODV*; in fact for high interference level (that is a higher number of nodes or connections) they present a greater *PDR* and a lower normalized routing overhead and average end-to-end delay respect to the traditional *AODV* protocol.

REFERENCES

- "Revision of Part 15 of the Commission's Rules Regarding Ultra-Wideband Transmission Systems," First note and Order, Federal Communications Commission, ET-Docket 98-153, Adopted February 14, 2002, released April 22, 2002.
- [2] 802.15.4TM 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 802.15.4TM-2003, October 2003.

- [3] Charles E. Perkins, Elizabeth M. Belding-Royer, and Samir Das. "Ad Hoc On Demand Distance Vector (AODV) Routing." IETF RFC 3561
- [4] 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
- [5] 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.
- [6] Liran Ma1, 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.
- [7] 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.
- [8] Wing Ho Yuen, Heung-no Lee, Timothy D. Andersen, "A Simple and Effective Cross Layer Networking System for Mobile Ad Hoc Networks," in EEE PIMRC 2002, Lisbon, Portugal, Sept. 2002
- [9] 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.
- [10] Hasan Mahmood, Cristina Comaniciu, "Location Assisted Routing for Near-Far Effect Mitigation in Wireless Networks," in First International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Dec.2005.
- [11] Luca De Nardis, Guerino Giancola, Maria-Gabriella Di Benedetto, "Effect of power-efficient routing in UWB wireless mobile networks". In proceedings of 12th IST Mobile and Wireless Communications Summit 2003, IST 2003, Aveiro, Portugal.
- [12] Jean-Yves Le Boudec, Ruben Merz, , Božidar Radunović, Jörg Widmer, "DCC-MAC: A decentralized MAC protocol for 802.15.4a-like UWB mobile ad-hoc networks based on dynamic channel coding". In First International Conference on Broadband Networks (BroadNets 2004), San Jose, CA, October 2004.
- [13] Martin Burkhart, Pascal von Rickenbach, Roger Wattenhofer, Aaron Zollinger, "Does Topology Control Reduce Interference?". MobiHoc'04, May 24–26, 2004, Roppongi, Japan.



Average End-To-End Delay

1,20

1,00

0,80

0,60

0,40

0,40

0,40

0,40

120

140

160

Node Number

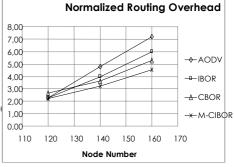
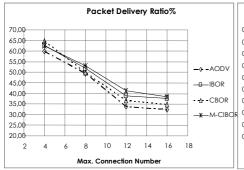
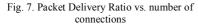


Fig. 4. Packet Delivery Ratio vs. number of nodes

Fig. 5. Average End-To-End Delay vs. number of nodes

Fig. 6. Normalized Routing Overhead vs. nodes number





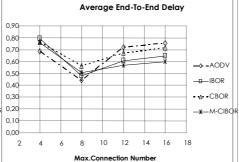


Fig. 8. Average End-To-End Delay vs. number of connections

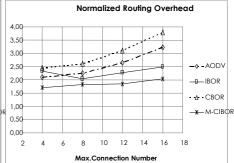


Fig. 9. Normalized Routing Overhead vs. number of connections