Project Acronym	CORMORAN (ANR 11-INFR-010)
Document Title	D3.3 – MAC/NWK Cross-layer Design for Inter-WBAN Networking (Initial Document)
Contractual Date of Delivery	M22 (31/10/2013)
Actual Date of Delivery	M30 (30/06/2014)
Editor	Télécom ParisTech
Authors	Claude Chaudet, Jihad Hamie, Anis Ouni (TPT) Jimenez Guizar Arturo Mauricio, Claire Goursaud, Jean-Marie Gorce (INSA) Nicolas Amiot, Bernard Uguen, Stéphane Avrillon, Meriem Mhedhbi (UR1)
Participants	UR1, INSA, TPT
Related Task(s)	T3
Related Sub-Task(s)	T3.3
Security	Public
Nature	Technical report
Version Number	1.0
Total Number of Pages	35

Contacts & Correspondence

Claude CHAUDET

- Address: Télécom ParisTech ; Dept. INFRES ; 23 avenue d'Italie ; CS 51237 - 75214 Paris Cedex 13
- Email: claude.chaudet@enst.fr
- Tel: (+33) (0)1 45 81 71 51

TABLE OF CONTENT

ABSTRACT

This document belongs to the subtask 3.3 of the CORMORAN project (*Inter-WBAN networking*) focuses on inter-BAN communication and interaction. Instead of letting every BAN act as a standalone network, this task examines the possibility to foster inter-BANs cooperation in order to optimize resources usage, to solve connectivity issues, or to improve the localization application accuracy with the added diversity. This deliverable focuses on the MAC and routing layers, describes protocols and algorithms that could be relevant for the CORMORAN scenarios, and proposes a few optimization tracks.

EXECUTIVE SUMMARY

This document presents ideas and base information about the collaboration between the MAC and routing layers in the CORMORAN scenarios. These two layers of the OSI model are often cited in scientific contributions as natural collaborators, as several of their tasks can be mutualized. The neighbors identification process, for instance, has an impact on the congestion that is solved by the MAC layer and on the paths diversity, which influences the routing process.

We first examine which requirements two flagship applications of CORMORAN impose on these layers. The motion capture application has stringent QoS requirements but requires no or few multihop routing, while the group navigation application is less constrained but could benefit from the variety of paths offered by the neighbor BANs. We then focalize on the network topology and its dynamics, which have a strong influence on the solutions efficiency at the MAC and routing levels. We identify the key parameters (transmission technologies, network size, network mobility pattern, traffic profiles, etc.) that are expected to make a real difference. We then list the data a BAN node is able to acquire to create its own perception of the context that surrounds it: the nodes neighborhood, the mobility model and the applicative traffic. We then look individually at the routing and the MAC problems, listing families of solutions and finish this document by evoking how the parameters measured at the various layers can be interpreted to deduce metrics that can in turn influence the different layers parameters.

1. INTRODUCTION

This document belongs to the subtask 3.3 of the CORMORAN project (*Inter-WBAN networking*) focuses on inter-BAN communication and interaction. Instead of letting every BAN act as a standalone network, this task examines the possibility to foster inter-BANs cooperation in order to optimize resources usage, to solve connectivity issues, or to improve the localization application accuracy with the added diversity. This deliverable focuses on the MAC and routing layers, with the idea that these two layers could collaborate to perform the aforementioned tasks, and could benefit from their results. We describe protocols and algorithms that could be relevant for the CORMORAN scenarios, and proposes a few optimization ideas for the following specific issues:

- Context detection and characterization (BAN network environment, applications and services, traffic, ...)
- Dynamic network layer algorithms selection based on the perception of the context
- Dynamic tuning of the network protocols to adapt the network behavior to the context

In section 2, we first examine the constraints in terms of QoS, but also on protocols operation and reactivity, that the two core scenarios of CORMORAN impose on these layers by focusing on the evolution of the network topology and on the data traffic profile. We then look at the problem of dynamic context detection in section 3. How can a node, based on its local perception, infer or evaluate how the network evolves? We then look at the degrees of freedom offered by the routing and MAC layers in section 4. Which are the parameters we could adapt, based on our perception of the context, to improve the behavior of the network? We then evoke inter-layers cooperation in section 5, looking at how the different components of the communication stack can collaborate to acquire data, evaluate the context and change their behavior accordingly. We finally conclude this document by evoking upcoming working directions.

2. INFLUENCE OF THE TARGET APPLICATIONS ON THE MAC AND ROUTING LAYERS

CORMORAN has selected two main target application scenarios called *Large-scale individual motion capture* (LSIMC) and *Coordinated group navigation* (CGN). We refer the reader to deliverable D1.1 for an extensive description of both scenarios and we will remind, in this section, the specificities of each scenario that are expected to have an influence on the inter-WBAN communication process.

2.1. APPLICATION SCENARIOS SUMMARY

The first class of scenarios, LSIMC, several devices are located on a single body. Hence, the interaction between close WBANs is not necessary, at least to perform relative on-body ranging and positioning tasks. However, in the last sub-scenario evoked in D1.1, nodes that are located on-body are supposed to be able to express their coordinates in a global system,

either by converting the local coordinate system to a global reference, or by directly localizing each node within the global infrastructure.

Therefore, off-body communication with anchor nodes located in the environment is necessary only in this very last sub-scenario, with 3 possible main situations:

- In the first case, on-body nodes are in visibility range of the different landmarks and exchange beacons with the landmarks to perform or enhance their localization process, as illustrated by Figure 2.1. This communication scheme cannot be qualified of inter-WBAN communication, as it basically consists in receiving or sending broadcast frames directly with the infrastructure.

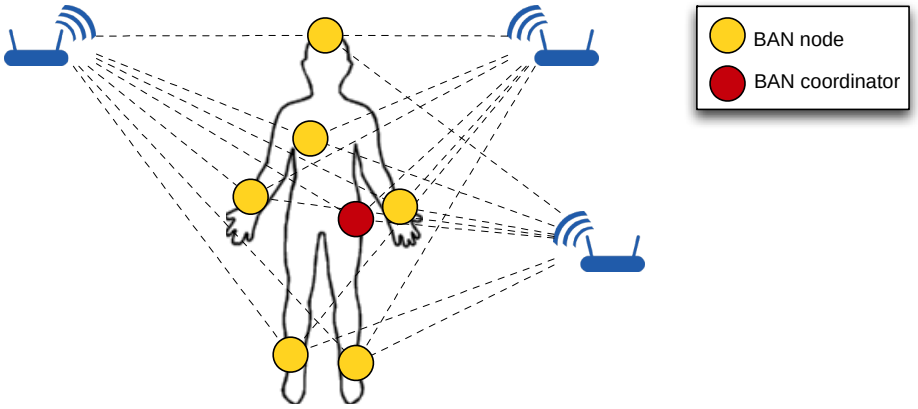

Figure 2.1: BAN scenario 1: all BAN nodes are able to communicate directly with the landmarks/access points located in the infrastructure.

- In the second case, the WBAN coordinator exchanges beacons with the infrastructure to localize itself in the global coordinate system, as illustrated by the bold lines in Figure 2.2. It then propagates this information to individual nodes that are able to convert the local coordinate system in the global one (translation and rotation operations). This scenario does not involve inter-WBAN communication either, strictly speaking.

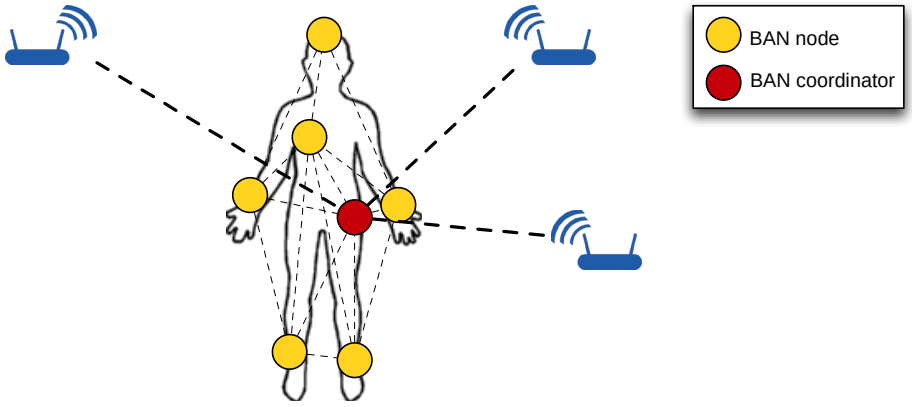

Figure 2.2: BAN scenario 2: all BAN nodes communicate through the coordinator with the landmarks/access points located in the infrastructure.

- In the last scenario, not all WBANs are necessarily in communication range of enough landmark nodes to find their position in the global coordinate system. The WBANs exchange beacons together to perform distributed localization, as illustrated by the bold lines on Figure 2.3. In this case, inter-WBAN communication occurs, at least between WBAN nodes and their immediate neighbors. Information propagation across WBANs (i.e. routing) could also be necessary, depending on the distributed global localization algorithm.

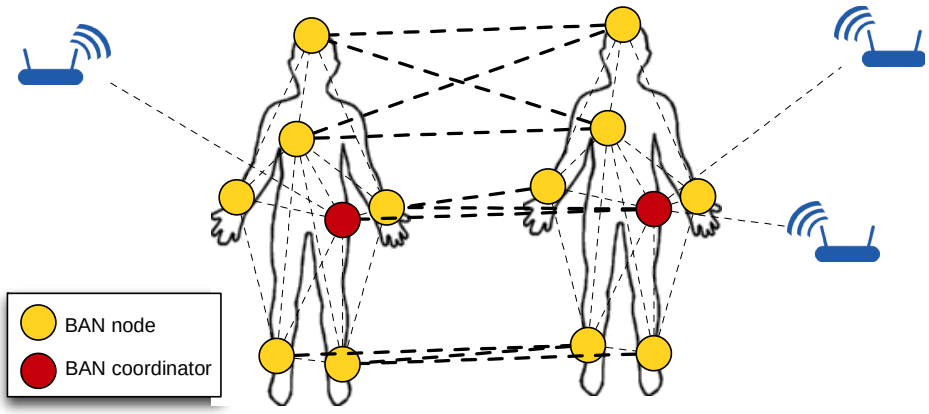

Figure 2.3: BAN scenario 3: all BAN nodes can directly communicate with other BAN nodes.

Finally, the LSIMC scenario includes the possibility to report all measurements to a server, which could be realized online (i.e. while capturing), or offline (post capture). The second situation requires the nodes to dedicate a slight amount of history to positions logging, but does not involve any WBAN to infrastructure communication. The first situation, however, requires nodes to be able to report measurements to the infrastructure, which introduces an upwards data flow from each WBAN to a gateway, possibly routed in a multihop manner.

The second class of scenarios, CGN, involves body-to-body communication, as it requires body-to-body ranging, or absolute body positioning in a group. For these operations, the

inter-WBAN communication scheme is similar to the last LSIMC sub-scenario mentioned above: on-body nodes exchange data together for positions exchange, ranging and distributed localization.

However, in this scenario, data exchange with a global network could also be required. When it comes to navigation, the nodes could need to download maps or directions from a server in the global network. Besides, each node could also need to send its position to other nodes in the group, as well as to a control center in the infrastructure (in an extended scenario). Finally, nodes could have to exchange date in a peer-to-peer manner, for instance to determine the location of the network centroid, or simply application-specific traffic.

Hence, this scenario involves three main schemes of inter-body communications:

- Local broadcasts between in-range nodes (beacons, announcements,...), as represented by the green lines on Figure 2.4.

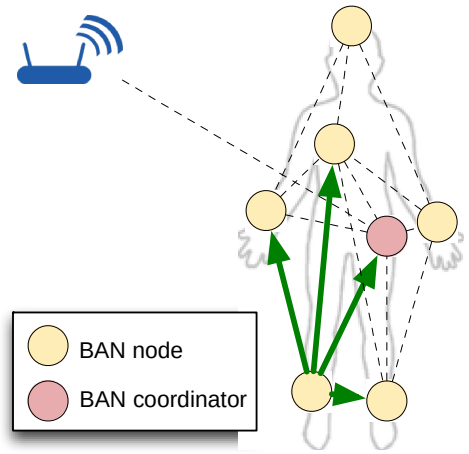

Figure 2.4: Traffic pattern 1: local broadcast (beacons, announcements,...).

- Upwards traffic towards the infrastructure through one or several gateways (tree-like network organization), routed through the WBANs, as represented by the red lines on Figure 2.5.

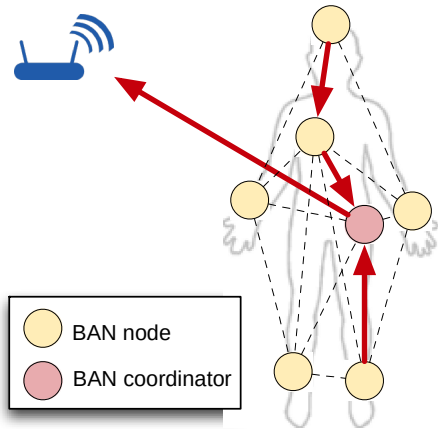

Figure 2.5: Traffic pattern 2: upwards traffic towards the infrastructure.

- Downwards traffic from the infrastructure to each WBAN, routed through the WBANs. Most of this traffic will be composed of network-wide flooding to disseminate maps and common data, as represented by the blue lines on Figure 2.6.

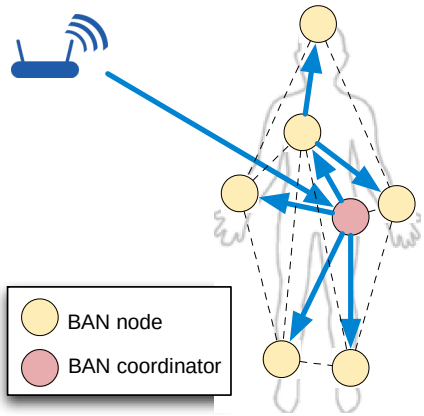

Figure 2.6: Traffic pattern 3: downwards traffic from the infrastructure (flooding or direct communication).

- Peer-to-peer exchanges between the WBANs, routed through the WBAN if needed, as represented by the orange lines on Figure 2.7. The proportion of such traffic is not expected to be very large, and depends on the exact application requirements.

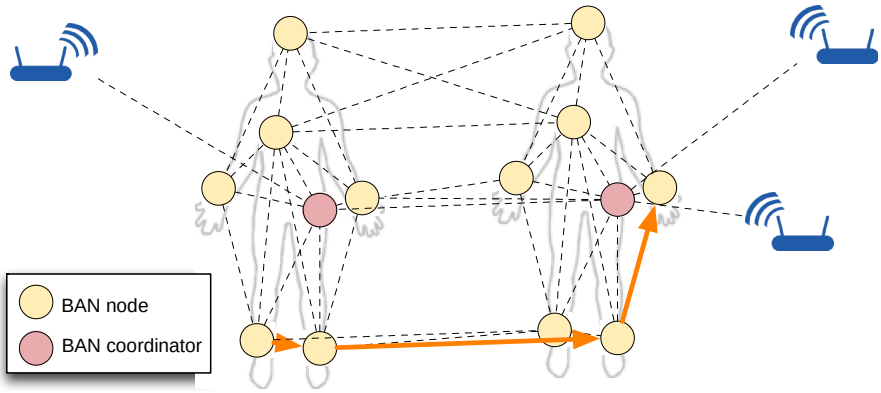

Figure 2.7: Traffic pattern 4: multihop peer-to-peer communication between WBANs.

To summarize, we can safely neglect peer-to-peer communication between the nodes at this stage, or use an off-the-shelf reactive routing protocol like LOADng [LoadNg] or a lightweight implementation of AODV [AODV] if required. Inter-WBAN communication should rather be optimized for data dissemination from the infrastructure (1-to-many), or for data collection from the WBANs to one or few gateways.

2.2. NETWORK TOPOLOGY AND DYNAMICS

Numerous protocols have been proposed for routing and MAC layers in various infrastructure-less networks (ad-hoc, sensors, ...). What can be learned from this mass of contributions is that the performance of various solutions is highly dependent on the scenario. The shape and dynamics of the topology have a strong influence on the efficiency of the various techniques and the best techniques for static networks could exhibit poor performance in dynamic network. That's why, prior to any optimization it is fundamental to sketch the network we expect. In this paragraph, we summarize the characteristics of the different transmission technologies and the consequences on the network.

To characterize and understand the network topology that we have to manipulate, let us first examine Figure 2.8, extracted from previous deliverables. This figure represents the different types of links that can co-exist in the global scenario. Orange lines represent off-body links between a WBAN and the infrastructure, lavender lines represent body-to-body links that are used either for point-to-point communication or for routing traffic, and blue lines represent on-body links.

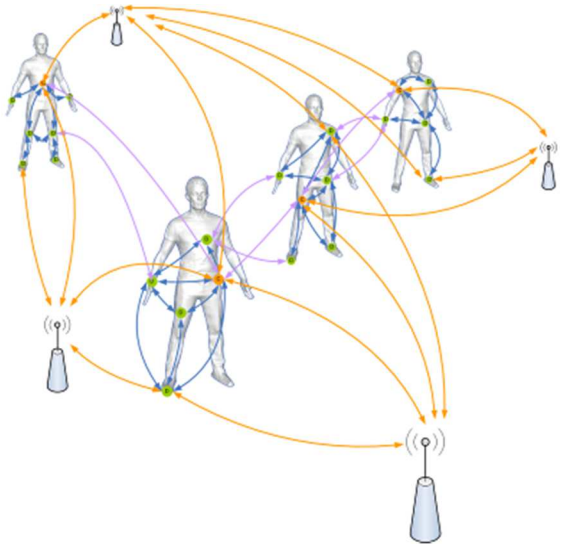

Figure 2.8: Generic deployment scenario for CORMORAN, with ultra short-range intra-WBAN links (blue), medium-range inter-WBAN links (lavender, and large-range off-body links (orange).

2.2.1 TRANSMISSION TECHNOLOGIES

The communication technologies envisioned in CORMORAN can work on two different frequency bands, which have slightly different characteristics. The maximum allowed transmission powers influence the communication range and hence define the network topology and its dynamics.

The classical narrowband technology, in the 2.4 GHz band, is utilized in most of today's wireless LANs. It has a range between 10 m and 100 m depending on the transmission power and on the modulation technique utilized. Classical ranges vary from about 10 m (Bluetooth and Zigbee) to 100 m (Wi-Fi and to some extent Zigbee). The LOS / NLOS condition influences the link quality but should not provoke too many harsh disconnections.

Impulse Radio Ultra Wide Band transmission (IR-UWB) happens between 3.1 GHz and 10.6 GHz. In France, the sub-carrier between 6 GHz and 8.5 GHz is the only one that allows an unlicensed transmission power of -41.3 dBm, in compliance with the US ECC rules without any further PIRE limitation technique.

[R13] analyzes the communication range that an realistic IEEE 802.15.4a transmitter could achieve over an IR-UWB channel with a fair packet error ratio. The article shows that using a correlation receiver improves the necessary signal over noise ratio of up to 9 dB when compared to a simple energy detection receiver. The two figures below, taken from the article, show the packet error rate in function of the communication range for different modulation and coding schemes in the case of the energy detection receiver (Figure 2.9) and in the case of the correlation receiver (Figure 2.10) in line of sight.

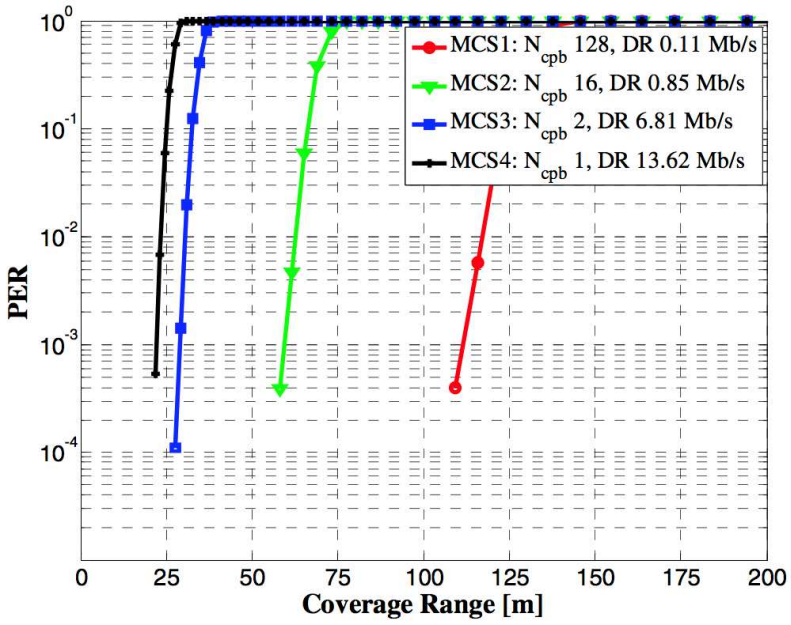

Figure 2.9: Packet error rate in function of the communication distance for an IR-UWB energy detection receiver (extracted from [R13]).

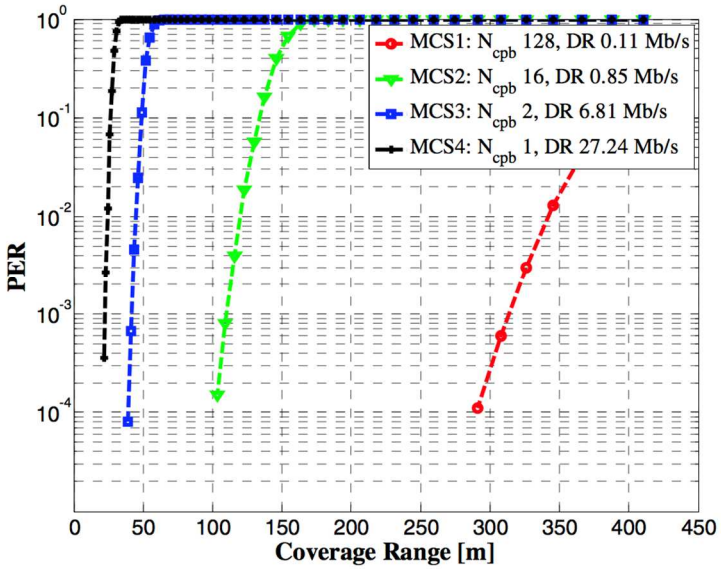

Figure 2.10: Packet error rate in function of the communication distance for an IR-UWB correlation receiver (extracted from [R13]).

No such study exists for IEEE 802.15.6 transmitters to our knowledge. However, the target of this standard specifies an expected range of 10 m. This means that both technologies could be

utilized for body-to-body communication as well as for off-body communications, under certain conditions. Indeed, the values reported above are valid when the maximum output power is utilized, which would probably not be the general situation in BANs, as energy preservation and exposure to radio waves plead for a reduction of the transmission power. Besides, the line of sight constraint might not be satisfied and the performance of wireless links using IR-UWB technologies will change quickly with the movements of the wearers.

2.2.2 NETWORK SIZE

In the initial scenarios identification, we had submitted a few devices locations to the end-users. The outcome of this survey is reported and analyzed in D1.1. Considering these results, we can expect a single BAN to be composed of 5 to 10 devices, organized in a 1-hop or 2-hops network, depending on the chosen transmission power (and hence the range). Considering the mobility patterns of a single body, the single-BAN scenario can be handled by the L2/L3 technologies that already exist.

However, the range of the wireless transmitters allows close bodies to interact and we could expect close BANs to interfere (in the worst case) or to merge. As IR-UWB is sensitive to the LOS/NLOS conditions, the network density should not increase too much with this type of technology, except for highly crowded scenarios such as public transportation or manifestation.

Nevertheless, it remains necessary to select or to design the MAC layer so that it can deal with interferences that appear between close networks when two devices that use the same schedule on the same channel get in mutual range. At the upper layers (routing), the algorithms should be adapted to benefit from the path diversity that appears in these situations, even it it may be episodic.

2.2.3 NETWORK DYNAMICS

The network dynamics, i.e. how and how often each link characteristics change, is highly dependent on the mobility model, which can be divided into two levels: a first level of mobility is defined by a single body mobility. The movement of a wearer changes the attenuation and the LOS/NLOS conditions according to the change of posture of the person. A few works have tried to characterize such mobility.

Concerning relative BANs movements inside a group, several models coming from the ad-hoc research area can be suitable. The reference point group mobility model is one of the first group mobility models that has been proposed and that is very generic. It partitions the network in groups and groups have their own mobility pattern, which lets the groups centroid move according to any of the classical random models, and nodes inside the groups then move relatively to the position of the centroid. This model does not answer the question of the degree of realism of this or that random model, but it is configurable enough to give us a good basis for evaluating propositions.

Concerning intra-BAN mobility, few attempts to derive a generic BAN mobility model have been published. The most accomplished model is MoBAN [NGB11], which introduces the concept of *posture*. A posture defines the way the different nodes move (run, walk, sit, ...) and

a Markov chain models the transitions between the different postures. If this model is generic enough to render a wide range of situations, the exact tuning of the parameters (nodes speeds, communication ranges, etc.) remain undecided and should require in-vivo experimentation. MoBAN provides an implementation for the MiXim framework of the OmNET++ simulator, which should ease parameters tuning and protocols evaluation.

2.2.4 SUMMARY

Based on the reflections of the previous sections and on the literature survey, we can list a few characteristics of the networks that CORMORAN will address. These networks can be described at three different hierarchical levels: multiple BANs will move together, forming groups that have their own group trajectory, meeting and separating according to classical mobility models. Inside a group, nodes move around a reference point (usually the centroid), and we can expect slow relative motion to mimic the behaviour of a group of persons traveling together.

Each individual in the group wears a few devices (from 5 to 10) that have multiple interfaces : IEEE 802.15.6, bluetooth LE or IEEE 802.15.4a should be utilized for on-body and body-to-body opportunistic communication, IEEE 802.15.4 or Bluetooth would be good candidates for inter-BAN communications passing through gateways such as mobile phones. BAN-to-infrastructure communication (off-body) will probably utilize Wi-Fi (IEEE 802.11), IEEE 802.15.4 or a cellular access technology, depending on the traffic. For example, off-body communications destined to enhance localization would use the shortest range communication technique available, while statistics reporting to a distant server would use opportunistically Wi-Fi links or cellular access. Table 2-1 recalls the most common characteristics of each of these links types. One of the key challenges of the joint MAC and routing layers consists in optimizing the network operation in this heterogeneous and ever-evolving scenario.

Link type	Involved nodes	Technology	Band	Data rate (announced)	Range
On-body	Unit nodes	IEEE 802.15.6	IR-UWB	≥ 487.5 kb/s	5 m
		Bluetooth-LE	Narrow (2.4GHz)	1 Mbit/s	100 m
		IEEE 802.15.4a	IR-UWB	≥ 850 kb/s	10 m
Body-to-body	Coordinators	IEEE 802.15.4a	IR-UWB	≥ 850 kb/s	10 m
		IEEE 802.15.4	Narrow (2.4GHz)	250 kb/s	75 m
Body-to-body	Unit Nodes	IEEE 802.15.6	IR-UWB	≥ 487.5 kb/s	5 m
		Bluetooth-LE	Narrow (2.4GHz)	1 Mbit/s	100 m
Off-body	Coordinators	IEEE 802.15.4a	IR-UWB	≥ 850 kb/s	10 m
		IEEE 802.15.4	Narrow (2.4GHz)	250 kb/s	75 m
		IEEE 802.11	Narrow (2.4 GHz)	54 Mb/s	100 m

Table 2-1 : Summary of the characteristics of the different link types.

2.3. APPLICATIONS AND DATA TRAFFIC PROFILES

Table 2-2, issued from previous deliverables, reports the applicative constraints that apply to the two core CORMORAN applications. Large-scale Individual Motion Capture (LSIMC) requires a fast refreshment rate (down to 10 ms), while the Coordinated Group Navigation (CGN) has more usual constraints (1 s refreshment rate). The design of the MAC and routing layer should be realized with these constraints in mind.

	Large-Scale Individual Motion Capture		Coordinated Group Navigation
	Low Precision	High Precision	
On-Body Nodes Location Precision (Relative)	$\varepsilon_{90} < 25$ cm (worst case CDF @ 90%) $\varepsilon_{50} \approx 5$ cm (median CDF @ 50%)	$\varepsilon_{90} < 5$ cm (worst case CDF @ 90%) $\varepsilon_{50} \approx 1$ cm (median CDF @ 50%)	N/A
Average Body Location Precision (Absolute)	$\varepsilon_{90} < 1$ m (worst case CDF @ 90%) $\varepsilon_{50} \approx 0.3$ m (median CDF @ 50%)		
Nodes Location Refreshment Rate	100 ms	10 ms	1s
Maximum Speed	{5, 15} km.h^{-1}		
Anchors Density	< 0.05 anchors / m²		< 0.01 anchors / m²
Nb Persons per Group	N/A		{5, 10}
Maximum Inter-Body Distances	N/A		{1, 5, 10, 50}
Nb of On-Body Nodes	{5, 10, 20}		{2, 5}
Rank of Preferred On-Body Nodes Location	**An-He-Wr-To-Hi-Lg-Ba-Sh-Kn-Bd**		**Sh-To-Ba-Hi-Wr**
Environment	{Outdoor, Indoor}		Indoor
Place for Final Location Info	{Server, User}		User
Pre-Calibration (Deployment Convention to be Respected)	{None, Precise Deployment Pattern}		{None, Rough Deployment Pattern}

Table 2-2 : Summary of application needs in both large-scale individual motion capture (Within low precision and very high precision modes) and group navigation applications.

The LSIMC application is clearly the most demanding. The required refreshment rate has an influence on the transmission delay. When the capture needs to be realized in real-time (i.e. the body position is displayed live, as data is acquired), the constraints on the transmission delay are defined by the maximum time allowed between the capture of a position and its display. This lag should be sufficient for capturing, sending, forwarding, receiving and interpreting the position data. Depending on how stringent this constraint is, captures may or may not be grouped into large frames and buffering may or may not happen at the sender or in the network. Shorter constraints lead to a high throughput, due to packet headers and per-frame overhead and they also demand a more precise scheduling at the MAC layer. Hopefully, in this scenario routing should not be necessary, and we do not expect to rely on multihop forwarding.

When the objective is a posteriori reconstruction of the movement, few constraints pertain on the transmission delay. These constraints could be imposed by the necessity to empty the nodes buffers. Besides, any lossless compression technique could be utilized to reduce the volume of information transmitted over the air. The gateway could also have a large storage capacity, like mobile phones or small GPS loggers, which would bring back the problem to

the MAC layer only, as traffic would remain inside the BAN (with possibly two-hops forwarding).

Concerning the CGN scenario, the expected traffic is more reasonable, as the delay is closer to what multihop networks can achieve in reasonable scenarios. The distance between the source and the destination of the information should remain moderate, but a 1s delay within a group is feasible, as long as the nodes remain active and the MAC and routing layers are tuned properly.

Besides the Core CORMORAN application, we could also be interested in other applications such as social networks, medical data transmission, sports-related or quantify-self applications. All these applications have similar profiles: they either collect data for local exploitation (i.e. transmission to a smartphone that displays and/or logs the data), or have very loose delay constraints. Reliability and confidentiality could be issues, but are beyond the scope of the MAC and routing layers.

2.4. SUMMARY

As we have seen in this section, the applications envisioned by CORMORAN can take multiple shapes. The traffic profile is different depending not only on the application, but also on the architecture and to the set of software bricks that can be implemented for security or compression purposes.

The shape of the network itself varies: if the nodes density is not expected to rise drastically, the in-network mobility profiles depend on human movement and are hence difficult to predict. The set of wireless technologies that will be effectively deployed depends on the choice of the user and may vary.

The MAC and routing layers are in the front line when it comes to dealing with this variability. Indeed, the MAC layers should adapt to the body mobility and to the group mobility patterns, preventing interferences to have a too strong impact and optimizing the use of resources while limiting control traffic and energy expenses. The routing layer should be adaptable enough to abstract the heterogeneity of the various MAC layers, and be able to address the particular mobility that mixes regular and irregular patterns.

We expect the routing and MAC layers to be able to adapt their behavior to the actual scenario, which means that in practice, the devices should include a few configurable implementations of each protocol type. However, the number of such protocols should be as reduced as possible. Indeed, as the protocols should work in cooperation (cross-layer design), multiplying the alternatives for routing or for medium access is costly, as adding one MAC layer, for example, requires specifying and implementing adaptations in *all* the routing protocols included. At this stage, we do not know yet whether there should be variety in the protocols families. We expect to answer these questions based on extensive simulations and on the measurement campaigns that will occur at the end of the first semester of 2014. We should however have in mind that it is more efficient to favor parameters tuning instead over protocols diversity. Once the protocols are selected and

configuration parameters are identified, the protocol stack also needs to be able to detect the context in order to select the most appropriate building blocks and to fine-tune parameters.

3. DYNAMIC CONTEXT DETECTION

In this section, we detail the elements that define the context a BAN evolves in. In other words, what are the key parameters that can evolve and which evolution models are realistic? In the second part of this section, we detail which parameters an isolated node can rely on to detect that a change of context occurred and to classify this change.

3.1. RELEVANT COMPONENTS OF THE CONTEXT OF A BAN

As mentioned in section 2, several parameters may influence the selection of the appropriate protocols and parameters for a given BAN communication layers.

3.1.1 NODES INSTANTANEOUS NEIGHBORHOOD

The first parameter that is of primary importance to the medium access control layer is simply the **network density**, or at a more detailed scale, the **composition of each node's neighborhood**. How many neighbors or contenders does each node possess? Is the density uniform across the network or are there variations from area to area? Brought at the routing level, the network density influences the path diversity, but a finer grain of description may be required to optimize the routing operation, and more specifically the stability of the routes. For example, a routing protocol may benefit from knowing which proportion of the neighbors of a node belong to the same BAN, which proportion belong to a close BAN that belongs to the same group (in the sense of group navigation) and how many episodic contacts a node has. Figure 3.1 illustrates such situation. On this figure, each color materializes one group and we can see three groups of body devices interleaving. Each device's neighborhood is composed of a mixture of devices that belong to the same BAN, to the same group or to stranger BANs.

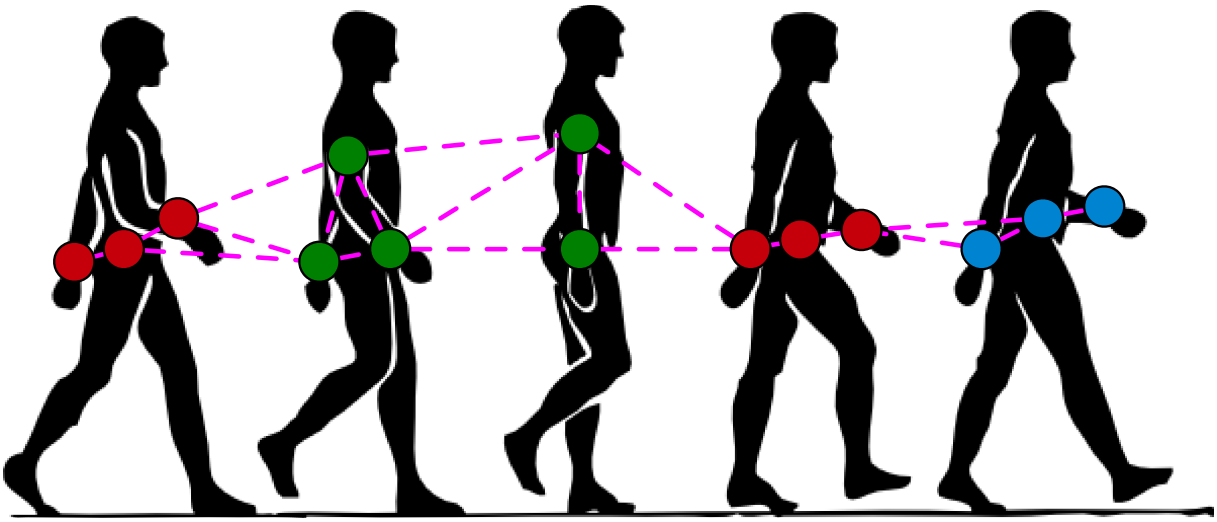

Figure 3.1: Group navigation: three groups interleaving.

3.1.2 MOBILITY MODEL

The **nodes mobility** is related to the neighborhood characterization, but introduces new parameters. As mentioned above, mobility can be decomposed in a few hierarchical levels. We may at least distinguish the mobility pattern of nodes that belong to the same BAN, the pattern of the BANs that belong to the same group and the relative mobility of the different groups. These three scales may have very different profiles and be described by very different models.

Several works, for instance, model in-BAN mobility by a composition of periodic patterns. Arms move along the torso and links appear and disappear regularly, as the wearer walks. This is obviously an approximation and no protocol should imagine that the period is strict. However, when probabilistic scheduling or routing is involved, the probabilities to see a link reappear after a certain time could be calculated based on recent history, which would yield to a correct approximation in several cases. Devices that belong to a different BAN in the same group should also be considered as reliable contacts, as the links are expected to appear, but the mobility pattern should be sensibly different.

Concerning intra-group mobility (i.e. how people move relatively to each other within a group that travels together). No really convincing intra-group model has been proposed to our knowledge, however we can easily derive a realistic intra-group mobility model by defining how the inter-contact evolve. Moving groups of people tend to keep a relatively stable pattern. People start discussions, walk together by groups of two or three, as illustrated on Figure 3.2 and sometimes change contacts. The group is usually spread across the line of movement and the density tends to vary proportionally to the inverse of the group speed: when the group slows down or stops, the group gathers and the local density increases and vice-versa.

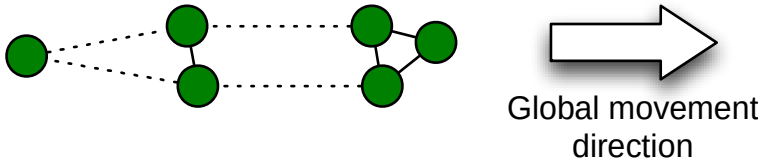

Figure 3.2: Organization of a group of people in sub-groups. The plain lines represent strong and stable links. The dotted lines represent links with a strong attenuation whose length varies with the centroid speed.

Finally, concerning the mobility of the groups themselves, several possibilities exist depending on the scenario. This level of mobility can be reduced to the definition of the movements of the centroid of each group. The purely random mobility models (random waypoint, random direction, Gauss-Markov) are convenient for experimenters, as they are described by a simple set of parameters that influence random variables, but do not necessarily reflect reality. Map-based mobility models would be more relevant: groups evolve in a constrained environment, surrounded by walls (indoor) or streets (outdoor). Several random map generation tools exist and it is possible, afterwards, to simulate mobility within a given map either by random generation of Origin-Destination matrices (similarly to what is done in the vehicles traffic simulation in cities), or by applying an evolution of the random walk model: every time a group reaches an intersection, it chooses a direction randomly, as illustrated on Figure 3.3. The movement speed is also random, within an interval, and may vary smoothly. It can be modeled by defining speed recursively, time slot by time slot, with the help of a random variable whose variance defines the maximum speed instantaneous variation: $v_{t+1} \sim \mathcal{N}(v_t, \sigma)$

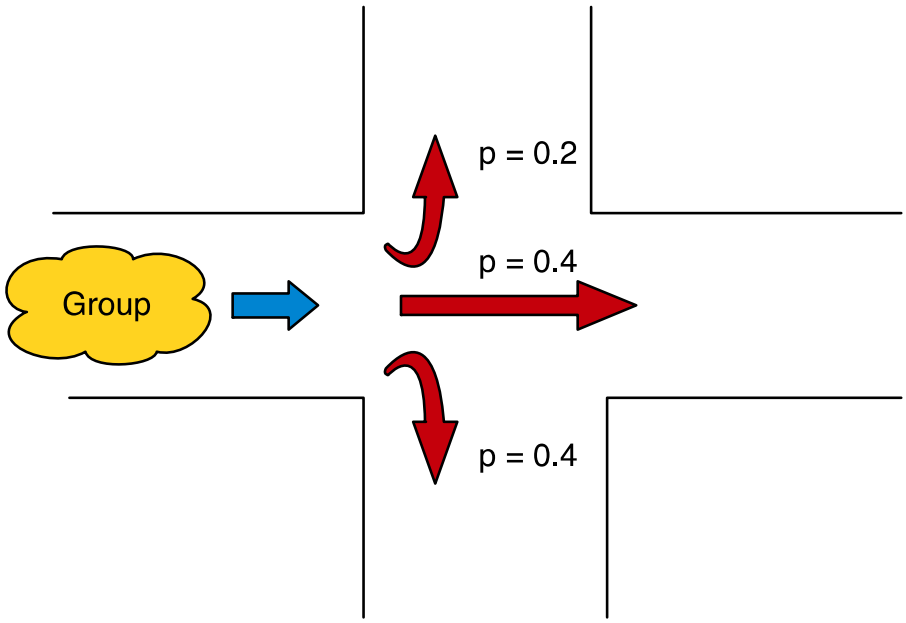

Figure 3.3: Group global random movement within a map.

3.1.3 APPLICATIVE TRAFFIC

The traffic generated by the nodes also has an influence on the L2/L3 protocols design. The traffic intensity and its origin and destination define the load that is perceived by each node in the BAN and hence influences the MAC protocol design. The origin and destination of the traffic imposes constraints on the routing protocol: it is probably not necessary to maintain routes towards every possible destination. A few stable routes could be updated with a proactive protocol, while the less frequent routes may be handled by an on-demand routing protocol.

The traffic within a BAN depends strongly on the application. Based on works in CORMORAN, we can imagine that close nodes will exchange point-to-point beacons regularly for ranging purposes (two-way or three-way handshakes). Besides, a traffic related to positions reporting will flow from individual nodes to the gateways on each BAN, which will then retransmit them to close BANs or to an archiving server. The routing protocol itself, as well as all the network-level protocols, also generates control traffic that needs to be considered.

3.2. AVAILABLE PARAMETERS TO DETECT CONTEXT

In the previous paragraph, we identified a few criteria that would, together, influence the design and tuning of the MAC and routing layers. However, these criteria are defined at a global scale, which is inaccessible to standard nodes. We examine here which information nodes have at their disposal to try and estimate these global parameters. This paragraph only contains a listing, as the exact correlation relationships need to be measured and quantified based on experimental or at least simulation studies.

A BAN node can first acquire quite easily an instantaneous vision of its neighbors. Spoofing the wireless channel(s) can provide information about active nodes in range, by looking for instance at the source MAC addresses of the frames received and successfully decoded. It however requires a constant monitoring of the wireless channel(s) and is very energy consuming. Nevertheless, several routing protocols rely on a neighbor discovery process. Nodes regularly send beacons to all their neighbors and use the received beacons to update their vision of their local vicinity. The rate of these packets emissions defines the accuracy of the neighborhood identification process.

The emission rate of these packets is usually defined by the routing protocol for its own needs. It is possible to use them for it is used for other purposes such as neighbors identification for MAC layer optimization, we could have to increase the rate. For regular movement that imply links connections and disconnections, a faster rhythm could be desirable at the beginning, and the pace can slow down once the pattern is identified. In the RPL routing protocol, for example, the interval between two control packet transmissions increases exponentially when the environment is stable.

Neighbors identification and the monitoring of neighbors appearances and disappearances can be sufficient for a node to characterize its mobility model relative to each of its neighbor. Indeed, what we are seeking here is to characterize the inter-contact pattern that is widely utilized in delay tolerant network.

Going a bit further, we can even associate to each links one or several quality factors. The most immediate metrics that fit in this category are the RSSI that characterizes the link attenuation, or the loss rate on the link, measured by monitoring, for instance, the number of retransmissions of each packet.

At the network level, the set of available parameters depends strongly on the selected routing protocol. We could monitor route change events, which either indicate nodes mobility, or change in links quality. Route usage can also be logged to focus optimization on the primary routes. Finally, network identifications, and more specifically IPv6 prefixes, can give a hint on nodes associations to groups: nodes belonging to the same BAN should have the same prefix.

4. DYNAMIC SELECTION OF NETWORKING ALGORITHMS AND PARAMETERS

4.1. ROUTING ALGORITHMS

Looking at the literature, there have been numerous proposals for routing in various multihop networks. From ad-hoc networks to vehicular networks and from delay tolerant networks to wireless sensor networks, routing has been examined under multiple scenarios and the BAN context also has been addressed by a few contributions. Section 5 of deliverable D3.1 presents a selection of routing algorithms and protocols coming essentially from the DTN and sensors worlds, which could be adapted to this context.

Indeed, in CORMORAN, routing could be an issue in only one of the two scenarios. In the motion capture scenario (LSIMC), a BAN is a two-hops star centered on a gateway and classical routing could be implemented between gateways if the application requires or benefits from multi-hop communication. However, in most situations, the gateway would either be directly connected to the infrastructure (via Wi-Fi for instance), or have access to a cellular network (LTE), or could dispose of sufficient storage space.

The CGN scenario is indeed more relevant to evolved routing, as it involves multiple devices that belong to different BANs, connected through multiple technologies. Besides, close BANs may belong to the same group or not. Each BAN device can therefore communicate directly with multiple types of peers. Table 4-1 reports the different possibilities for a node belonging to a BAN A that belongs to a group Γ_1 :

Type of node	Peer	Technology	Notes
Regular node in BAN A belonging to group Γ_1	Regular node or gateway in BAN *A*	IR-UWB	Link may have a quasi-periodical appearance and disappearance process.
	Regular node or gateway in BAN B belonging to group Γ_1	IR-UWB	Link between two BANs, requires synchronizing the schedules to avoid interferences
	Regular node or gateway in BAN C belonging to group Γ_2	IR-UWB	Low trust link. Can disappear anytime with low probability to reappear later on. Potential confidentiality issues.
Gateway in BAN A belonging to group Γ_1	Regular node in BAN *A*	IR-UWB	Link may have a quasi-periodical appearance and disappearance process.
	Regular node in BAN B belonging to group Γ_1	IR-UWB	Link between two BANs, requires synchronizing the schedules to avoid interferences
	Regular node in BAN C belonging to group Γ_2	IR-UWB	Low trust link. Can disappear anytime with low probability to reappear later on. Potential confidentiality issues.
	Gateway in BAN B belonging to group Γ_1	802.15.4 BT-LE	Ad-hoc like routing with low mobility (nodes in the same group move together). Possibility of sudden disconnection with reappearance later.
	Gateway in BAN C belonging to group Γ_2	802.15.4 BT-LE	DTN-like routing with an unknown contact time
	Infrastructure LAN	Wi-Fi 802.15.4 BT-LE	Uplink to an infrastructure can be used in an opportunistic way. Good coupling with DTN-like routing.
	Cellular access	3G LTE	Direct uplink that may have a cost (limited data plan), could be utilized with different priorities depending on the origin of the data.

Table 4-1: different types of links and relevant constraints / routing strategies.

Considering diversity of links and the lack of a one-fits-all routing solution, the best strategy would consist in implementing several routing algorithms in the nodes and dynamically selecting the best routing algorithm(s) to activate based on the context. Simple nodes that form the BAN should have limited routing capabilities. Indeed, they should, by default, organize around their BAN gateway and forward all frames towards that more powerful node. However, they should also be able to forward data using other BANs in range, to increase the network capacity in case some links are overloaded, or in case of a gateway

failure. Such loss of a gateway is indeed highly probable, especially if the gateway is a smartphone that runs multiple applications.

4.1.1 ROUTING STRATEGIES COMPARISON

In deliverable D3.1, we listed a few routing strategies that are relevant to our scenario. From a more global perspective, routing protocols for mutlihop wireless networks can generally be regrouped into 5 families whose performance depends on the scenario:

- **Proactive protocols** (ad-hoc) are the closest to classical Internet-like routing protocols. All nodes exchange control packets to acquire a local or global vision of the network topology and to find the best routes towards every destination. Routes are available immediately and the protocol always generates control traffic, which is not optimal in stable networks. However, in highly dynamic networks the required update frequency generates a very high control traffic load, which make these types of protocols more suited to moderate mobility networks in which all nodes can be the destination of data packets.
- **Reactive routing protocols** (ad-hoc) build routes on-demand, when the application wishes to send data, by flooding a probe into the network. The data packets are delayed until the route is established, which introduces an initial latency. In case of high mobility nodes, these protocols must include a route reparation mechanism in order to limit the control traffic volume. These protocols are particularly well suited when the network is moderately mobile and when the connections between couples of nodes are infrequent. Ideally, a route should remain stable during the communication and nodes would move sensibly between two connections between a couple of nodes.
- **Message-passing approaches** (DTN) is relevant in sparse mobile networks. When the network is often partitioned, nodes may exploit their mobility to transmit or duplicate data when they come in range of a new node. The whole difficulty consists in deciding which node(s) should be entrusted with the packets without knowing their future movements. Protocols range from basic flooding (give a copy of the data to every node we meet and that did not receive it yet), to purely probabilistic strategies (transmit to a new node according to a probability that depends on encounters history). These protocols are the only solution in sparse mobile networks but need to be tuned properly to reach a good delivery rate.
- **Tree or DAG-based routing protocols** (sensors) are destined to networks composed of many sources and few destinations, like sensor networks in which numerous sensors report to a few collection points. As the traffic profile is destination-oriented, the nodes routing tables can be composed on a single entry towards the (closest, best, ...) collection point, or of a few alternatives, suing mechanisms similar to the spanning tree construction. In this latter case, the algorithm builds a directed acyclic graph instead of a tree. In both cases, the construction process is simple and similar: the destination floods regularly the network with a beacon that is received multiple times by every node. Nodes compare announced paths and are able to choose the best one(s). These protocols are particularly relevant when there is only a few

destinations in the network, as they limit the number of nodes allowed to emit control packets. Besides, the nodes are aware of the whole topology, if collisions are avoided, and can select the best path(s) and acquire a vision of their neighborhood simultaneously. However, as the control packets are flooded throughout the network, their emission rate should be tuned according to the maximum mobility that needs to be detected.

- **Geographic protocols** (ad-hoc) do not rely on routing tables updates but only on the nodes physical coordinates. Packets are sent towards a geographic position and the nodes forward the packet to bring it closer to the destination. Several techniques exist to address "holes" or dead-ends, but the main issue consists in synchronizing the local coordinates systems together and identifying the geographic coordinates of the destination. However, if the nodes are all aware of their geographic coordinates (which is feasible considering the applications targeted by CORMORAN) and if the destinations have fixed and well known coordinates, this strategy may be the most adapted to high mobility. Indeed, nodes do not need to exchange routing-specific control packets but only need to take a decision based on their status when they forward or receive a frame.

This fast comparison of the most classical routing strategy confirms that there is no one-fits-all solution and that routing should be adapted based on the context. Nevertheless, nothing forbids to mix multiple protocols together, except the nodes capacity in terms of CPU (to run multiple algorithms), space (to store the code and the routing tables). Indeed, the purpose of routing is to make sure the packet gets closer to the destination at every step, and that the number of hops traveled is as small as possible. Each node should therefore be free to select its own routing protocol, as long as the metrics are coherent and as a proportion of its neighbors are able to participate in the routing process.

In the remaining of this project, we intend on studying this type of strategy and the criteria that should influence the selection of a routing algorithm. Each node should select its own routing protocols based on its neighbors and on its perception of the network mobility. All nodes that implement multiple routing protocols shall make the interface by announcing routes on all protocols.

4.1.2 DEGREES OF FREEDOM

In the previous section, we identified the routing protocols as a first degree of freedom for the nodes. A node may dynamically choose to participate in one or several routing algorithms based on its perception (mobility, density, traffic, ...) and on its capabilities (load, bandwidth, ...). There are however other parameters that a node may tune to find the good compromise between routing accuracy and its cost.

Most routing protocols rely on a regular emission of status updates such as Hello messages that announce a node's presence and sometimes its neighbors. A few protocols already noticed that the frequency of these updates could be adapted. The interval between two successive updates should increase when the topology is stable and decrease when changes

are noticed. This principle is at the basis of the trickle timer used in RPL. The interval between two routing updates (in a general meaning) therefore should constitute a second degree of freedom.

Specific protocols can also be tuned dynamically. For instance, DTN-like routing protocols often rely on a probability of handing a packet to a newly encountered neighbor and on a probability to create a new copy of the packet. These are also parameters that can be adapted dynamically to the context of the network. In parallel with simulations that we will realize to study the multi-protocols interaction, we will list parameters of individual routing protocols.

4.1.3 COMBINING ROUTING ALGORITHMS

As evoked above, we intend on combining multiple routing protocols. The combination in itself is essentially a question of defining a coherent set of metrics, implementation and space available on devices. The network formed this way can be thought of as a collection of disconnected sub-networks that are interconnected together by gateways. Each node will play with global as well as per-protocol parameters and will exchange data with its neighbors to optimize the network operation.

However, it is possible to update further this process by combining routing packets. Several routing protocols, for example, require identifying each node's neighbors and using Hello control packets to this extent. These can be mutualized and can also serve as a basis for acquiring data on inter-contact times that are necessary for DTN-like protocols. There are several such optimization possible which will be identified and evaluated. In particular, mutualizing control packets may lead to some issues, as the loss of a single packet can impact several protocols.

In terms of implementation, this mutualization should be as transparent as possible. That's why, today we have in mind to build an intermediate layer that catches and aggregates routing protocols control packets into a generic format on the emitter's side and that reconstructs routing packets on the receiver's side.

4.2. MEDIUM ACCESS CONTROL

4.2.1 MEDIUM ACCESS CONTROL PROTOCOL COMPARISON

Deliverable D3.1 contains a survey of a few medium access control protocols that could be relevant in the CORMORAN scenarios. IEEE 802.15.6 and IEEE 802.15.4a employ a mixture of CSMA-based random access and TDMA-like scheduled access. These standards work with superframes whose boundaries are announced by the network coordinator through beacon frames. These beacon frames define, for the next transmission period, the scheduling within a single BAN.

Generally, scheduled access like TDMA are very efficient for small-sized networks (1 or 2 hops diameter) that are relatively static and when the traffic pattern is predictable. If these conditions are not met, deciding of a scheduling can be tedious and random protocols are preferred, even though nothing forbids using a pre-defined scheduling.

Other strategies such as preamble sampling are not fully relevant in our context, as they take reveal their full potential in presence of long duty cycles, when the clock drift effects become significant. Considering our applicative constraints, time synchronization can be maintained through data exchanges and the MAC layer will probably use mostly scheduled access.

4.2.2 DEGREES OF FREEDOM

At the medium access layer, the amount of parameters we can adapt to improve the behavior of the network depends on the protocol family:

- In random access protocols, the channel access procedure usually depends on a random parameter (probability to transmit or random backoff), which can be influenced depending on the link type, on its quality or on the LOS/NLOS conditions. This type of parameter defines how careful or aggressive the nodes are and it should be tuned, according to the literature, to minimize the collision probability that depends on the number of contending devices and on the traffic intensity.
- In scheduled access (TDMA), it is possible to change the slots allocation to the transmitting devices, including the number of slots per superframe that are allocated to a single link.

When both accesses coexist, like in the IEEE 802.15.x protocols, a beacon is generally sent by the coordinator to materialize the beginning of a new scheduled access period. This beacon contains the whole schedule, as well as the duration of a random access period that will follow the scheduled access rounds. In this type of scenario, besides each protocol family parameters, we can define dynamically the duration of the superframe (i.e. the interval between two beacons emissions) and the relative duration of the scheduled access and random access.

4.3. ADDRESSING

Defining an addressing scheme for CORMORAN application is pretty straightforward, yet it needs to be implemented. Addressing can easily be based on IPv6, thanks to the 6LowPAN extensions that provide header compression. 6LowPAN is normally limited to the link-local scope, however drafts have been submitted to the IETF for compressing headers that use a global, routable, prefix. This header compression mechanism brings back the source and destination address to 2 bytes each, based on the 16-bits IEEE 802.15.4 address. The 6LowPAN IETF draft [6LowPAN] defines the compression methods applicable that we can reuse in the CORMORAN context.

5. INTER-LAYERS COOPERATION

The communication process involves three main components: the MAC layer, the routing protocol(s) and the application. Each of these processes is able to measure a few quality indicators that can be utilized to infer the network status and the individual layers parameters can be tuned based on this perceived network status. This process introduces a retroaction that needs to be characterized and controlled.

Figure 5.1 represents the quality indicators (in blue) that can be provided by each of the components (in red).

The MAC layer at the receiver's side can assess of the link quality through classical measures like the received signal strength indicator or the link quality indicator. At the emitter's side, this layer can report the loss rate (how many frames were dropped, regardless of the reason) and the link delay (how much time does it take to access the wireless channel). Besides, the MAC layer is able to identify a few active neighbor nodes by examining the source MAC addresses of the overheard frames, even when these frames are not forwarded to the upper layers.

The routing protocol(s) also have their vision of each node's neighbors, usually based on control packets such as hello messages. This vision can be shared or coupled with the MAC layer to improve or optimize neighbors identification. Then, routing statistics such as the frequency of route repair events indicate the stability of the route and could help assess the dynamics of the network. Route usage, when correlated with the traffic coming from the application, gives insight on the expected medium load.

At the application level, the localization process in itself can provide to the lower layers information on each node's position, or on the BAN centroid's position. Finally, an application can report whether the perceived QoS corresponds to its expectations or not.

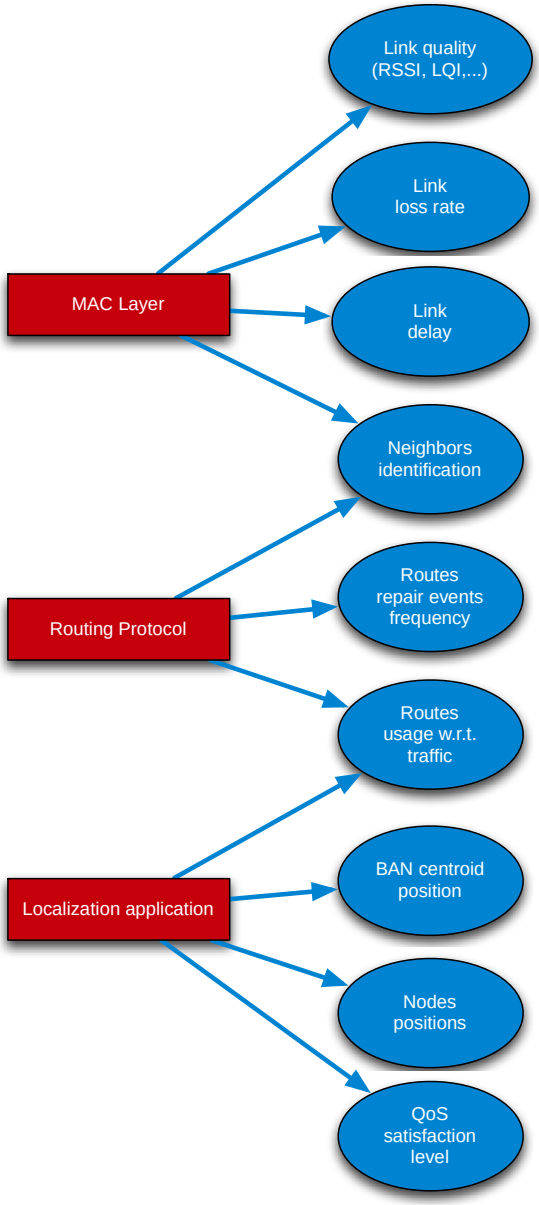

Figure 5.1: Functional components and associated communication quality indicators

Once the quality indicators have been acquired from various layers, they can be utilized, individually or conjointly, to deduce second-level context elements, as represented on Figure 5.2.

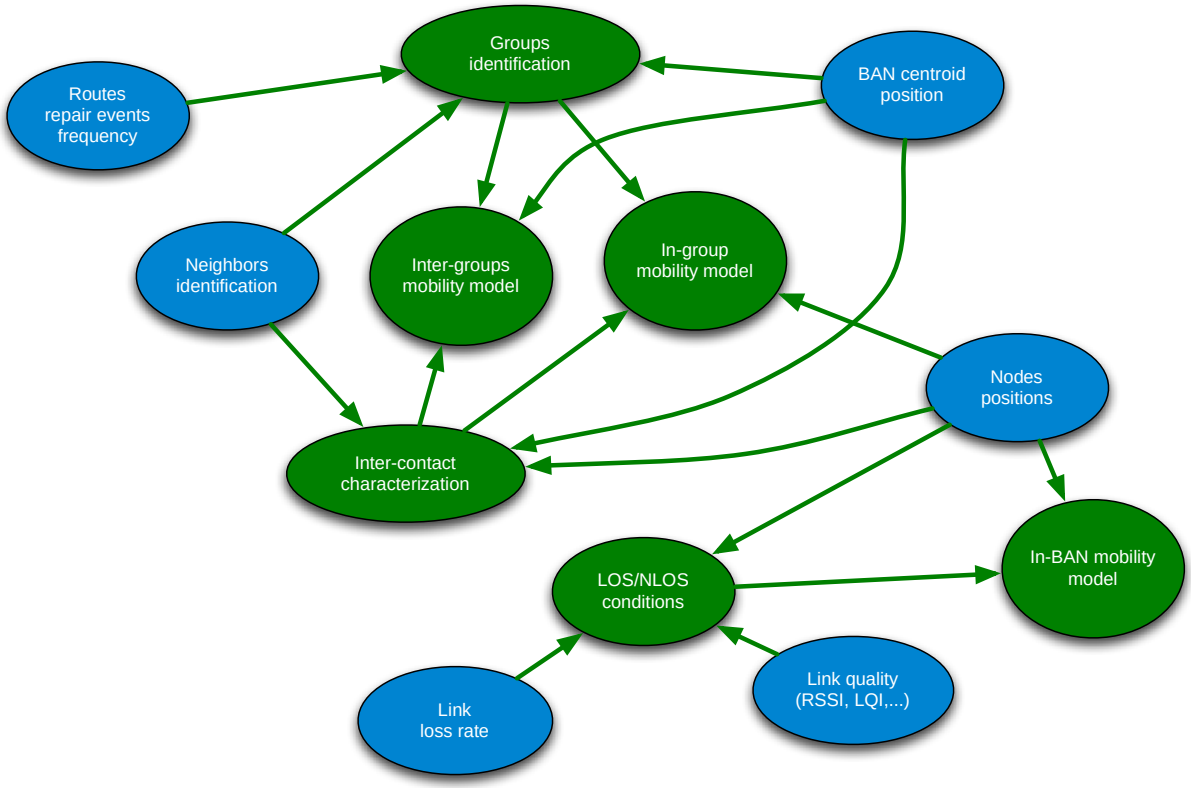

Figure 5.2: second level context identification indicators and their relationships with communication quality metrics

Most context identification elements that we can identify are related to the relative mobility of the nodes. We expect to have three levels of mobility: inside a single BAN, where the mobility models may experience some periodical or pseudo-periodical behavior; between BANs that belong to the same group (i.e. how people traveling together move around each other), and between groups (when two groups meet, merge and separate). These mobility models can be deduced from the positions of the individual nodes and of a BAN's centroid (or gateway), as well as from other metrics such as the characterization of the nodes inter-contact patterns that can be deduced from routing or MAC-level neighbors identification. Mobility inside a single BAN can also be characterized with the knowledge of the LOS/NLOS condition that is related to the link quality and to the loss rate. In addition, we may want to automate the identification of the nodes that belong to the same BAN or group, which can be based on BAN centroid positions as well as on higher layers events such as the frequency of route updates necessary to keep a communication between two nodes.

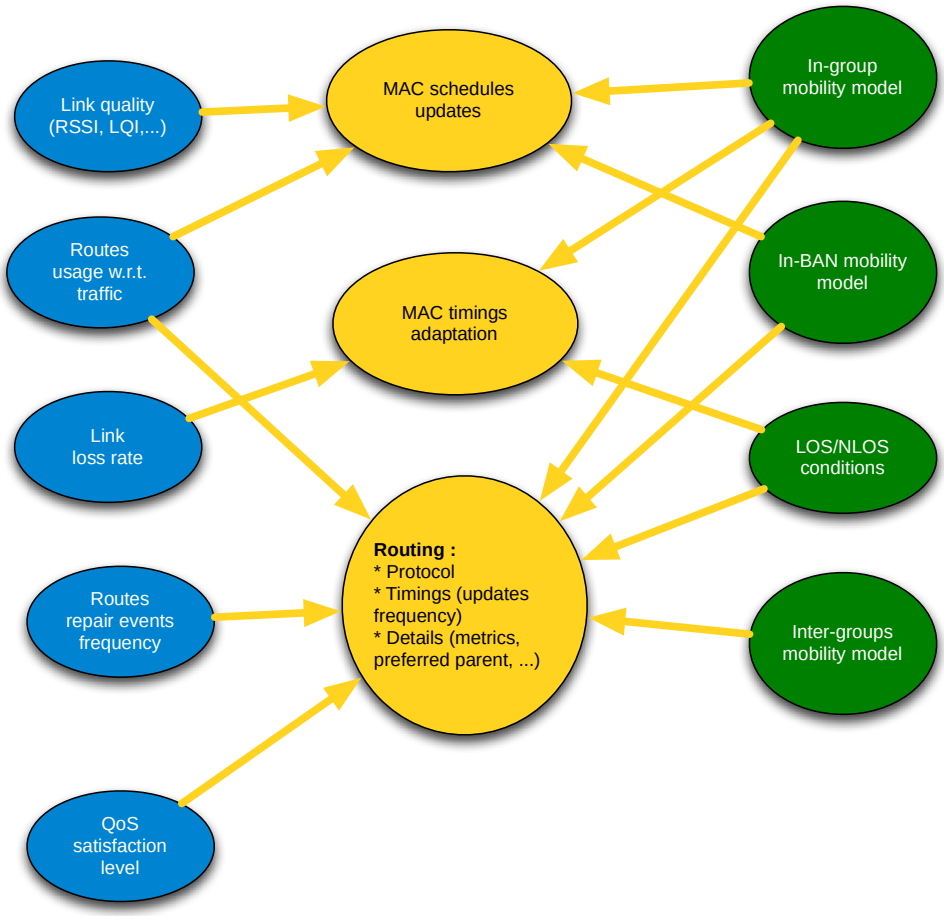

Figure 5.3: influence of the context on the routing and MAC layers parameters

Finally, the set of communication quality indicators and context parameters can then be utilized to tune the MAC and routing layers parameters, as represented on Figure 5.3. MAC schedules (TDMA for instance) may need to be updated regularly combining the characteristics of the mobility model (regularity e.g.), of the link quality, and on the traffic pattern. The MAC timings (e.g. backoff interval, duty cycles when applicable, etc.) should use similar inputs, but also data about the LOS/NLOS conditions. At the routing layer, we may select the routing protocol that is implemented, its timings (the frequency of updates, e.g.), and to influence its internal behavior (e.g. the routing metric, or the algorithm that selects the next hop towards a destination), based on the mobility model, on routing stability and on a feedback from the application.

The relationships depicted in this paragraph only represent an excerpt of what can really be implemented. The set of core level metrics could increase or decrease based on the hardware capabilities (is it possible to acquire this or this parameters, what is the confidence level / accuracy, etc.). Same observation holds for the MAC parameters tuning, which may or may not be possible depending on the implementation. That's why this set of metrics will constitute our first objective and can be modified in the rest of the project.

6. CONCLUSIONS AND PERSPECTIVES

In this document, we examined the routing and medium access layers of the body area networks under the light of the CORMORAN target applications. We identified a few directions for joint optimization and collaboration of these two layers, including the application in the process as a "client" of these layers (defining QoS requirements) and as a provider (positioning information). We believe that the CORMORAN context is precise enough to allow a fine optimization of the communication process.

We will now have to analyse the experimental results obtained during the June 2014 measurement campaign to assess of the accuracy of the measurements and the possibility to deduce, for instance, link qualities from RSSIs, or the perception the nodes have on their mobility. This will give us an indication of the quality of the different indicators and on the usage they may have.

In parallel, we will use state of the art models to feed the CORMORAN joint simulator. We intend on implementing gross versions of the classical routing protocols under WSNET (RPL [RPL], DYMO [DYMO], ...) and use the channel modelled by PyLayers to evaluate these protocols and the joint optimizations we discussed in this document in a realistic BAN context.

7. REFERENCES

[NGB11] Majid Nabi, Marc Geilen, Twan Basten, "MoBAN: A Configurable Mobility Model for Wireless Body Area Networks " - 4th International Conference on Simulation Tools and Techniques, SIMUTools 2011, march 2011

[R13] Rafael Reinhold, "Coverage Range Analysis of IEEE 802.15.4a IR-UWB for Reliable Data Transmission in Wireless Sensor Networks" - 2013 IEEE International Workshop on Measurements and Networking (M&N), October 2013

[6LowPAN] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams in Low Power and Lossy Networks (6LoWPAN)", Internet Draft draft-ietf-6lowpan-hc-15, IETF, February 2011

[LoadNg] T. Clausen et al., "The Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation (LOADng)", Internet Draft draft-clausen-lln-loadng-10, IETF, October 2013

[AODV] C. Perkins, E. Belding-Royer and S. Das, " Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, IETF, July 2003

[RPL] T. Winter et al., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, IETF, March 2012

[DYMO] C. Perkins, S. Ratliff and J. Dowdell, "Dynamic MANET On-demand (AODVv2) Routing", Internet Draft draft-ietf-manet-dymo-26, IETF, February 2013