EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Scalable multi-hop routing in wireless networks

David Palma[*] and Marilia Curado

Abstract

Infrastructure-less wireless multi-hop networks have long been proposed for natural disaster and warfare scenarios. However, the current demand of such networks has been towards social networking, gaming and ultimately, ubiquitous computing. In fact, the increasing number of users that own wireless capable devices is taking these networks to an entirely different scale. Existing routing protocols do not scale and do not consider the context wherein services operate. By presenting an alternative routing scheme that appropriately handles mobility of users among different contexts, large-scale clustered wireless networks are designed, using an efficient gateway selection with load-balancing capabilities. This approach uses a virtual hierarchy of clusters to explore the contextual-proximity of nodes, while reducing the total overhead of routing traffic even when compared with other cluster-based approaches. Moreover, it is capable of predicting gateway link disconnections, increasing the total amount of delivered data. The obtained results reveal that this routing scheme outperforms existing routing protocols regardless of the mobility pattern being used, being consistently lighter in overhead and delivering up to 50% more data traffic. These results motivate a new era of large-scale wireless multi-hop networks suitable for hand-held devices exchanging data amongst themselves.

Keywords: Scalable routing, Cluster gateway protocol, Wireless, Ad-hoc networks, Mobility

1 Introduction

Recent technological advances have promoted a massive dissemination of wireless capable devices with greater processing power, higher memory and autonomy, increasing the connectivity of users to different services and applications. As a result, in a near future each person is expected to be surrounded by hundreds or even thousands of these devices [1], motivating the development of networks capable of connecting them whilst supporting the applications' requirements, taking into account that a considerable amount of physical resources from the available infrastructures will be necessary. Moreover, in certain occasions such as conferences, music concerts or football games, the increased number of people in the same site may render such networks impractical. The ad-hoc creation of wireless multi-hop networks to handle this new communication demand may be a solution. However, the management of a large scale infrastructure-less network is still a challenge.

Another typical characteristic of the spreading wireless gadgets is their portability, creating new challenges related with mobility. This aspect is crucial for users who expect seamless connectivity regardless of where they are. However, different trajectories may reduce connectivity coverage, resulting in the disruption of paths established by routing protocols.

Wireless multi-hop networks have increasingly stood out for being available anywhere, without requiring any existing infra-structures and also for being self-organized, self-administrated and self-maintained. For this purpose, several existing works on this topic—such as the optimized link-state routing protocol (OLSR) [2] which provides an optimization for the typical link-state routing, and the Dynamic MANET On-demand (AODVv2, previously known as DYMO) routing [3] which, on its hand, offers an on-demand routing approach—have already been proposed. However maintaining routing performance for large scale networks is still an issue for both proactive and reactive routing protocols. Taking this problem into account, different works propose schemes involving techniques such as: dynamic addressing, keeping network nodes organized in a well defined topology

*Correspondence: palma@dei.uc.pt
Centre for Informatics and Systems, University of Coimbra (CISUC), Coimbra, Portugal

as proposed by the dynamic address routing for scalable ad-hoc and mesh networks (DART) [4]; geographic partitioning, to easily create stable clusters as presented by Hamma et al. [5]; and typical clustering solutions as defined by Canourgues et al. [6].

While some approaches aim at scalable routing using different approaches, they lack a thorough evaluation of the impact of different mobility models. In fact, regarding this aspect, most routing solutions disregard the dynamics of different mobility models, focusing only on one mobility pattern. Nevertheless, in order to appropriately evaluate the efficiency of an ad-hoc network and the performance of routing protocols, these aspects have to be taken into account. Moreover, other works that study the impact of mobility fail to provide an extensive evaluation with existing mobility models [7].

A different perspective on wireless multi-hop routing has been provided with the definition of delay-tolerant networks (DTN). In these networks routing protocols are designed to deliver traffic that is not delay sensitive, despite the sparse intermittently connected properties of such network. Conventional routing in wireless multi-hop networks is not suitable for highly dynamic scenarios as it needs to establish an end-to-end path before starting the routing of data packets, which may not be possible at a given moment.

Even though most wireless networks are in fact intermittently connected due to interferences in the wireless medium, the mobility of nodes has also an important role in this aspect. Typical DTN solutions such as PRoPHET [8] are capable of operating with delay tolerant traffic when wireless connections are not reliable, but fails to perform well with completely unknown node mobility. Other approaches focus on more stable parameters such as social interactions between nodes. For instance, the friendship-based routing (FBR) protocol [9] or the social aware networking (SANE) scheme [10] take into account social interactions, both physical and virtual, in order to take a packet forward decision. Nonetheless, these schemes fail to determine a possible path to deliver their packets in real time being therefore not comparable with the presented routing solution. Moreover, scalability issues are again not taken into consideration, rendering these approaches useless in highly populated scenarios where a large amount of data traffic may depend on one node alone.

Motivated by the lack of a routing scheme where large clusters of wireless nodes may exist, this article presents a new routing approach that takes into account the increased interaction between users within a same context, regardless of the used mobility pattern, using a well defined network hierarchy of real and virtual clusters. Previous studies show that content is exchanged between millions of individuals resorting to phone interactions or on-line services. In this sense, clusters of users can be identified in friendship circles, or on common interest groups where clusters within clusters exist [11]. Therefore, and due to the registered growth of wireless capable portable devices, this study aims at defining a scalable routing scheme, resilient to mobility phenomena capable of taking advantage of existing clusters.

Since interactions between members of the same cluster are likely to take place, the cluster gateway protocol (CGP) is defined taking this aspect into account. The protocol resorts to aggregated views of the network, establishing a hierarchy between existing clusters and virtual ones, camouflaging the negative impacts of node mobility between them. As a result, each node will solely keep detailed information about its own cluster and will maintain aggregated information about the network according to a pre-defined cluster hierarchy.

In the used hierarchy, inter-cluster communication is guaranteed by border nodes, Gateways, which are responsible for forwarding packets. However, since several Gateway nodes may exist in one cluster, it is important to select the most suitable one. This is achieved by using a new Gateway Selection Metric which estimates the Link Quality of a Gateway using Kernel Based Regression Methods and the interval time between received routing messages.

The CGP stands out for exploring locality within a cluster while still being able to deliver packets in distant areas of the network. The provided routing scheme has some resemblances with both conventional and DTN routing as it establishes an end-to-end path when routing inside a cluster but it also uses a store-and-forward approach when routing between different clusters, without previously determining the entire path. In addition to this, since clustered networks are used in the existing hierarchy, the used Gateway selection scheme, in conjunction with a kernel-based link quality estimator, will also allow load balancing of traffic in the network.

As previously mentioned, the effect of mobility on the performance of a routing approach is an important aspect to take into consideration. Therefore, a thorough evaluation of the proposed scheme is provided, using six distinct mobility models and a static scenario, allowing a deeper understanding of how mobility is handled by CGP and how the cluster changes of nodes are processed, comparing the impact different patterns in the routing performance.

In Section 2, an overview of existing techniques used for scalable routing in wireless multi-hop networks is presented, followed by the description and specification of the CGP approach, presenting the overall concept in Section 3. As the name indicates, CGP relies on Gateway nodes for an efficient forwarding of packets between clusters, which in their turn rely on an efficient link quality metric defined in Section 4. Regarding the evaluation of the presented routing scheme, an assessment methodology is defined in Section 5, presenting six distinct mobility models applied to 541 wireless nodes in a total area of 2.25 km^2. The obtained results are presented in Section 6, comparing them with a clustered and unclustered version of the OLSR protocol. Finally, in Section 7, the final thoughts on this study are presented.

2 Related study

In order to achieve scalable routing many different protocols have been proposed using distinct techniques. One typical solution for scalable routing is known as clustering, where nodes are grouped into clusters, limiting the amount of shared information amongst them. Routing in these clustered networks is typically characterized by the definition of specific hierarchies by routing protocols, aiming at keeping themselves more scalable.

The "Cluster-based OLSR extensions to reduce control overhead in mobile ad hoc networks", **C-OLSR protocol** [12], proposes an extension to OLSR by introducing a cluster organized network. While this study does not define a clear hierarchy between nodes and clusters, the authors propose a scheme where the existing clusters are considered as nodes themselves, using the multipoint relays (MPR) concept, which was introduced by the OLSR protocol, and apply it to clusters. This scheme results in a flat clustered routing approach even though it bears resemblance to hierarchical routing because of the existing MPR clusters.

In the C-OLSR protocol the definition of cluster *HELLO* and topology control messages (*C-HELLO* and *C-TC*), allows the maintenance of paths among the existing clusters while reducing the required amount of routing information, as only MPR Clusters generate C-TC messages.

Even though the approach presented by these authors uses the OLSR protocol for intra-cluster routing, the use of the aforementioned *C-HELLO* and *C-TC* extensions to support a clustered network, may have a negative impact, as the propagation of these new messages across clusters is required. Moreover, the introduced mechanisms may suffer from mobility phenomena, requiring an additional overhead of updating the entire network structure. Regarding this aspect, the CGP protocol does not exchange additional messages keeping routing more scalable while handling mobility more efficiently by using hierarchically aggregated views of the network.

In contrast with typical flat routing protocols, hierarchical protocols usually exchange their routing information in different ways, according to a cluster or node hierarchy level. The usage of hierarchies in conjunction with proactive routing approaches is found in the form of a hierarchy of clusters, as an organized tree of addresses, or even as trees of paths forming a topology.

An example of hierarchical proactive routing protocol presented in "Source-tree routing in wireless networks protocols", **STAR** [13], is a link-state protocol which has on average less overhead than on-demand routing protocols. Its bandwidth efficiency is accomplished by restraining the dissemination of link-state information only to the routers in the data path towards the desired destinations. STAR also creates paths that may not be optimal while avoiding loops, such that the total available bandwidth is increased. Moreover STAR has specific mechanisms to know when update messages must be transmitted to detect new or unreachable destinations, and loops.

Despite being able to scale, as each node only maintains a partial topology graph of the network, the STAR may suffer from large memory and processing overheads in scenarios where constant mobility may report different source trees, and routing paths are too long due to the network size. To handle this aspect of increased memory and processing overhead, the CGP makes use of virtual clusters which aggregate real clusters, reducing the amount of information required for routing.

In another existing study, entitled "Multimedia support in mobile wireless networks" **MMWN** [14], the authors propose an architecture consisting of two main elements, corresponding to different node types, which can either be switches or endpoints. Both of these can be mobile, however only switches can route packets and only endpoints can be sources of or destinations for packets. This protocol also keeps a cluster hierarchy as a location management scheme, capable of obtaining the address of an endpoint. This information is kept as a dynamic distributed database, such that in each node there is a location manager node.

The proposed hierarchy allows the necessary amount of routing messages to be reduced, such that only location managers are required to update their information and only then perform the location finding process. However, this aspect is also negative on the overall performance of the protocol, as routing is strongly related with the hierarchy of the network, making the routing process complex and vulnerable to disruptions when location managers change. The CGP protocol is more efficient in this aspect as it is completely decentralized, using interchangeable gateway nodes for packet forwarding between clusters.

Another proactive hierarchical routing protocol is the "Cluster-head gateway switch routing" protocol, **CGSR** [15], where nodes are also grouped into clusters. This protocol relies on a cluster-head node to keep routing information about its cluster, and all other nodes only need to know the routing path until their own cluster-head. Additionally, all the inter-cluster routing is also processed by the cluster-head which connects to remaining clusters' cluster-head nodes.

Even though the proposed cluster hierarchy may reduce the amount of flooding for dissemination of routing information, as only the cluster-heads are responsible for this task, the process of maintaining these clusters involves additional overheads, in particular the election of an appropriate cluster-head node. Moreover, this special node will always represent a bottleneck on each cluster, overloading it and possibly leading to a faster energy depletion, and consequent cluster-head re-election. The CGP approach has also a reduced amount of required routing information but does not required a centralized entity, being more resilient to node mobility.

Inspired on a previous study on a dynamic addressing paradigm, the "Dynamic address routing for scalable ad-hoc and mesh networks" **DART** [4], is proposed as a proactive hierarchical approach that efficiently manages the organization of nodes into zones for large scale networks. Address allocation and lookup are the main drawbacks of this proposal. However, the published study presents schemes to tackle these problems, showing how addresses can be allocated taking into account node positioning, building a tree with l levels – where l is the number of bits used in the routing address. A clear distinction is made between routing address and the identity of a node (a unique identification tag) as the routing address is dynamic and changes with node movement, contrasting with the node identifier which is always the same.

The three most important functionalities in DART are: first, the address allocation responsible for maintaining one routing address per network interface according to the movement and current position of a node; second, the routing which determines how to deliver packets from source to destination and, third, the node lookup which consists of a distributed lookup table in charge of mapping identifiers to network addresses.

The DART proposal reveals to be an efficient solution for routing in large scale ad-hoc networks. However, for small networks the Dynamic Address Heuristic has a strong overhead impact and in general it is difficult to implement, as the distributed lookup table is hard to manage. Since the CGP scheme can be implemented on top of any link-state routing protocol, using it for intra-cluster routing, small networks are no challenge and its implementation is straightforward.

The usage of Hierarchical Reactive Protocols is modest when compared with proactive or hybrid routing approaches. This is most likely due to the fact that most well defined hierarchies require constant updates in order to be efficiently kept. However, this goes against the concept behind Reactive Routing, which only exchanges routing information when required. Nevertheless, some Hierarchical Reactive protocols do exist and, as an example, the "Cluster based routing protocol", **CBRP** [16], proposes a variation of the "Min-Id" [17] for cluster formation, restraining the typical flooding required by proactive protocols within each cluster. By relying on flooding between cluster-heads in different clusters, adjacent clusters can be known and therefore reducing routing overhead.

As a 2-level hierarchy, this protocol can be scalable to a certain extent, however, the typical cluster formation and cluster-head election computational cost still exists. Even though node mobility does not necessarily lead to inaccurate routing table calculations, as it would happen with a proactive approach, the inherent route retrieval propagation delay may lead to temporary loops. In a highly dynamic network where several flows may exist, the CGP protocol is more efficient as it is able to immediately initiate the packet-forwarding process, not requiring an expensive flooding for each flow.

The "Hierarchical AODV routing protocol", **Hi-AODV** [18] is a hierarchical version of the well known AODV routing protocol, using a tree based on cluster-heads, for the creation of the concept of virtual nodes, which correspond to a typical cluster. The cluster-head is the only node responsible for handling control packets and managing the routing table of its own internal cluster. Having a tree composed of clusters seen as a virtual node, allows Hi-AODV to reduce the number of control packets and avoid additional routing traffic.

In addition to the already mentioned challenges and overheads related to the maintenance of clusters and their cluster-heads, it is clear that, even though routing overheads can be reduced, the cluster-head will always have to be part of any routing path, leading to non-optimal paths, and additional interferences in the vicinities of cluster-heads. The CGP approach is focused on choosing the most stable routing paths, not being restrained by any cluster-heads.

Quite a few hybrid routing protocols for ad-hoc networks can be found in the literature, still, despite the fact that many rely on clusters or well defined zones, not many implement a hierarchical routing scheme. The following protocols propose a hybrid routing scheme capable of retrieving inter-cluster information in a reactive approach, avoiding the necessity of restraining routing information in cluster-heads to reduce the overall overhead. However, on a downside, inter-cluster communication may be subject to route retrieval delay if no previous path has been maintained in cache.

The "Zone-based hierarchical link-state" routing protocol, **ZHLS** [19], is characterized by dividing the network into non-overlapping zones where two different routing paradigms are used: proactive routing within the zones and reactive between different zones. This proposal alleviates single points of failure and bottlenecks by not being dependent on cluster-head nodes and, at the same time, by maintaining a scalable hierarchy based topology.

One important assumption, and a possible limitation from this protocol is that each node knows its own position (for instance by using GPS) and consequently its zone

ID which is directly mapped to the node position. With this approach packets are forwarded by specifying in their header the zone ID and node ID of their destination.

The division of the network into a number of zones depends on factors such as node mobility, network density, transmission power and propagation characteristics. The geographic awareness is much more important in this partitioning process, as it facilitates it when compared to radio propagation partitioning.

In addition to the limitation of requiring some positioning system, the ZHLS protocol requires that all nodes exchange inter-zone flooding information when only Gateway nodes need this routing information for calculating the shortest path between different zones. Moreover, the ZHLS is susceptible to a route retrieval delay when establishing inter-zone paths, as reactive routing is used for this purpose.

In ZHLS, each node contains an intrazone and interzone routing table to manage routing between nodes from a same zone and from different zones respectively. The update of these tables is performed by sending two types of LSP: node LSP and zone LSP for intrazone and interzone, in that order.

A proposal to enhance the routing made by ZHLS is presented by Hamma et al. [20], where a gateway flooding scheme (**ZHLSGF**) is defined to reduce routing overhead and routing tables' size. This modification is closely related with the nodes that act as a border between different zones, since they are responsible for calculating the shortest path between other Gateway nodes. By sending only interzone discovery packets between each other, unnecessary packet forwarding is avoided to other nodes within the zone. Despite this optimization, the delay on path retrieval between different clusters still exists, being the CGP more efficient in this aspect, while also avoiding the overhead of the on-demand routing messages.

Another hierarchical hybrid routing protocol, the "Distributed dynamic routing" algorithm for mobile ad-hoc networks **DDR** [21], is a tree based routing protocol which consists of six different stages. In these stages an election of the preferred neighbor is made, followed by the forest construction, which creates a suitable structure for the wireless network, allowing an improved resource utilization. Afterwards intra and inter tree clustering is performed, followed by zone naming and partitioning. Zones are responsible for maintaining the protocol scalable and reducing the delay.

While DDR creates and maintains a dynamic logical structure of the wireless network, the "Hybrid ad hoc routing protocol", **HARP** [22] finds and maintains routing paths. The HARP protocol aims at discovering the most suitable end-to-end path from a source to a destination by using a proactive intra-zone routing approach and a reactive inter-zone scheme, by performing an on demand path discovery and by maintaining it while necessary.

Even though the DDR algorithm does not require any sort of cluster-head for cluster maintenance, the possibility of some nodes being chosen as preferred neighbors by other nodes may lead to the creation of bottlenecks, as they would be required to transmit an increased amount of both routing and data packets. It is important that the choice of preferred neighbors is balanced in order not to compromise the overall performance of the protocol. Moreover maintaining the entire logical structure of the network could be heavy, depending on how dynamic nodes may be. The CGP handles the dynamism of nodes by using aggregated view of the network and avoids bottlenecks with the used link quality metric for gateway selection.

Hierarchical routing is expected to improve resilience to mobility [23]. However, to the extent of our knowledge, there is only one hierarchical routing protocol that aggregates cluster information with different granularity, named Deferred aggregated routing for scalable adhoc networks, **DASH** [24], which implements a Deferred Routing approach [25]. Even thought this routing concept is more effective in supporting node mobility, it does not avoid bottlenecks in the choice of the used Gateways for inter-cluster communication, leading to a higher overhead in the network and losses. Moreover, it lacks a proper evaluation that considers demanding node mobility, with nodes constantly changing between different clusters. The least disruptive approach regarding communication overhead is provided by Hybrid Hierarchical protocols which use Reactive Routing for inter-cluster paths, however they suffer from a typical delay in on-demand solutions when retrieving paths. The CGP is an purely proactive routing protocol that aims at tackling the identified issues in scalable multi-hop routing, being resilient to node mobility.

3 Cluster gateway protocol

The paramount importance of Scalable Routing in Wireless Multi-hop Networks has been stressed out by many recent works in the area of mobile ad-hoc networks (MANETs). In fact, in a near future, users are expected to be surrounded by thousands of wireless capable devices [1], connecting people to their everyday objects, jobs, and hobbies.

In this section, the CGP paradigm is presented, defining a method for scalable proactive routing in Clustered MANETs and the necessary procedures to be added to an existing link-state routing protocol such as OLSR, allowing it to support this scheme.

3.1 Concept and definition

Previous studies addressing the topic of scalable multihop routing have relied on the usage of straightforward clustered network organizations. By using a clustering protocol, these approaches are able to restrain the propagation of routing messages throughout the entire network and reduce the impact of node mobility within clusters. However, a major drawback of these solutions is related with inter-cluster routing overhead and poor support of node mobility between different clusters. Moreover, some existing solutions also rely on super-nodes or cluster-heads, to guarantee the dissemination of routing information, creating bottlenecks and putting these nodes under additional stress.

The CGP approach consists in efficiently handling routing in clustered networks by defining a network hierarchy, without the use of cluster-heads. In addition to this, the CGP protocol does not exchange any additional routing messages, including only the required cluster and routing maintenance information in already existing messages.

The network organization used by CGP resembles to the cartographic division of continents, countries and cities, assigning identifiers with different granularities to each region. As an example, when traveling through different countries or when sending a letter, people only consider their destination in a broader view, setting their goal to it. For instance, when someone writes a letter, they specify the name and address of their correspondent, however the postman only takes into account a broader view of the destination, such as the destination country. Then, upon reaching the desired goal (e.g., a country), will then the destination perception be updated into a city, municipality, street and so on until ultimately the building or person in question is discovered. In CGP the same principle is found: routes are established according to their reliability and available Gateways, using different granularity levels, rather than on the total hop count from source to destination, discovering the path as packets get forward through different clusters.

Similar approaches such as the "Fisheye" and "Hazy sighted link state" routing protocols [26,27], improve their scalability by using mechanisms that allow imprecise or slightly out-of-date routing information regarding distant nodes, on a node basis. Even though these schemes reduce the amount of routing information, they do not support clustered networks nor do they do avoid disruption from strong mobility.

One key advantage of using the CGP is that, by keeping its optimized network hierarchy, it is able to limit not only the effects of intra-cluster mobility but also the effects of inter-cluster mobility. Moreover, it does not require additional routing messages for inter-cluster routing, being adaptable to any available link-state routing protocol. A preliminary version of this study, entitled deferred routing [25], has been proposed with a similar hierarchy but which does not take into account node mobility across different clusters. Not only does the CGP protocol handle mobility, but it also makes use of an optimized Gateway metric selection which is able to load-balance the existing traffic among the existing Gateway nodes, avoiding bottlenecks. Moreover, the thorough evaluation provided with this study also shows that the store-and-forward technique of CGP, in conjunction with self-healing routes are also relevant contributions for efficient traffic delivery in large-scale multi-hop networks.

3.2 Defining a cluster hierarchy to different clusters

In order to define a proper routing hierarchy to be used by CGP, groups of nodes are defined, similarly to Autonomous Systems in BGP but applied to wireless networks [28], which represent their clusters as presented in Figure 1. When considering mobile ad-hoc networks, this organization can be achieved by using a clustering algorithm such as the generalized max-min clustering algorithm [29], being the management of the clusters and their identification managed by the CGP routing scheme. In order to do so, each routing message used by the CGP protocol includes a cluster identification (CID) kept by each node. Due to mobility, whenever a node changes its cluster, the CGP routing scheme will update the CID of that node and perform the required adjustments regarding the existing routing tables.

An important part of the view determination of each CID is the assignment of CIDs to each cluster and the construction of the required hierarchy which occurs while the clustering algorithm defines new clusters. The binary hierarchy is used not only for performance purposes, but also to accommodate the creation and deletion of clusters. Whenever a new cluster is added, or when an existing one grows enough and divides itself, two new CIDs are created. The existing Cluster Identifier of the dividing cluster, or of the cluster to where the new one is attached, is kept unchanged becoming a Virtual Cluster. The remaining two CIDs are calculated using the old CID: $\text{New\_CID}_{\text{left}} = \text{Old\_CID} \times 2 + 1; \text{New\_CID}_{\text{right}} = \text{Old\_CID} \times 2 + 2$. This simple but efficient numbering of clusters allows the determination of the hierarchical level of each CID directly and it also allows to determine which clusters are contained within each virtual cluster.

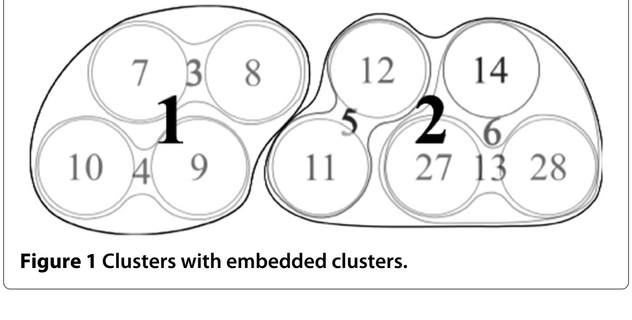

Figure 1 Clusters with embedded clusters.

The hierarchy employed by the CGP is based on a binary tree structure, motivated by the bisection that occurs in growing clusters and also by the base-2 logarithmic complexity of balanced binary-search-trees, illustrated by Figure 2, being also simple to compute the respective CID of each cluster. This organization defines different level clusters paired with virtual identifications for each cluster of nodes which correspond to different granularity levels of knowledge. In this example, the higher level clusters, with the CID number 1 and 2, can correspond to two different neighborhoods. The remaining CIDs represent buildings or common areas within the neighborhood (CIDs 3, 4, 5, and 6). Finally the leaf clusters of the hierarchy correspond to actual clusters of nodes, where users share similar interests and closely interact (in this hierarchy: CIDs 7, 8, 9, 10, 11, 12, 14, 27, and 28).

The CID information for each node is included in the header of the sent routing messages. The CGP protocol is an entirely proactive routing protocol, periodically exchanging its routing messages with the CID of the cluster to which the nodes belong. Moreover, since routing messages are not forwarded across different clusters, a list of IP addresses and their corresponding CIDs is also included in some routing messages. The details about the routing procedures are explained in further detail in the 3.2 section.

The hierarchy defined by the CGP also establishes a relation between the virtual clusters and the real clusters which represent the most detailed level of knowledge about an existing cluster (represented by the leaf clusters). While other hierarchies simply take into account existing clusters, the virtual aggregation of clusters allows the CGP scheme to be more resilient to mobility phenomena, reducing the undesirable effects of micro and macro mobility, thus maintaining routing more scalable. In particular, since people movement is not expected to be entirely random, this organization will reduce the number of registered cluster changes.

One key aspect of the presented hierarchy is related with the different perception that nodes have of the entire network and all the existing clusters. In fact, the nodes' membership to each cluster provides them a different network perspective according to their hierarchical position. Figure 3a depicts the network organization as it is perceived by clusters 7 and 8, following the hierarchy previously presented. As sibling clusters, 7 and 8 recognize each other but acknowledge only two other clusters: 4 and 2. As previously explained, clusters 4 and 2 are the result of an aggregated view of the network, being themselves virtual clusters. In a real scenario, clusters 7 and 8 could be for instance two groups of people within a building, whereas CID 4 would correspond to a next door edification, being cluster 2 another infrastructur nearby.

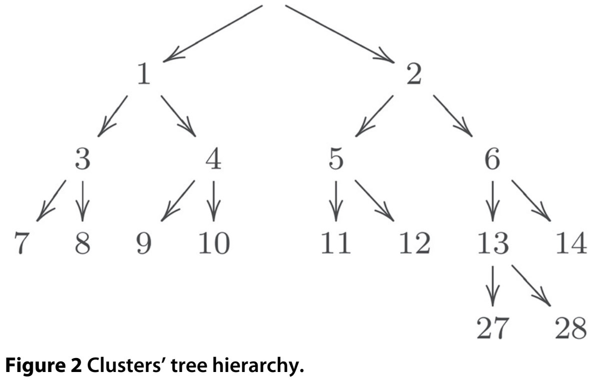

Figure 2 Clusters' tree hierarchy.

The aggregation is performed according to the hierarchical relationship between clusters, such that hierarchically closer clusters are less aggregated and further away clusters are progressively more aggregated. A similar aggregation level is obtained for clusters 9 and 10, as illustrated by Figure 3b. By using broader parameters that bring clusters together, these different granularity perspectives allow the desired organization for the forwarding of packets through selected Gateways. Moreover, as presented later in this study, the gateway selection will take into account the reliability of each gateway link, avoiding congestion on existing links. In this example, the given hierarchy reveals that clusters 9 and 10 are more likely to interact with clusters 7 and 8 (aggregated into CID 3) rather than with any other node in the remaining clusters.

Another noteworthy example of this aggregation scheme is presented in Figure 4a, which represents the view of clusters 27 and 28. These two clusters have an additional hierarchical level, which may have resulted from a more detailed cluster division due to an increasing

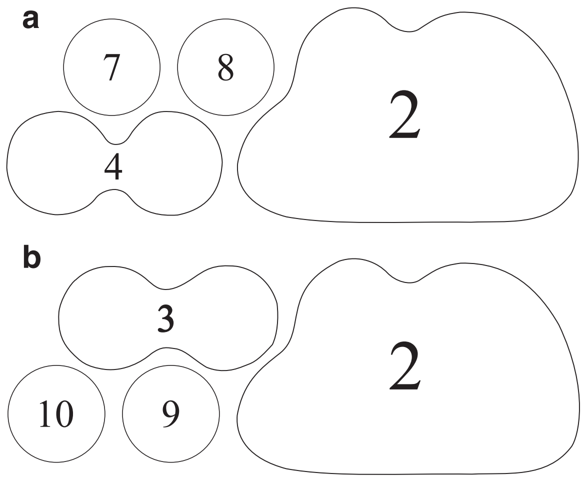

Figure 3 Additional network views. (**a**) Network view for clusters 7 and 8. (**b**) Network view for clusters 9 and 10.

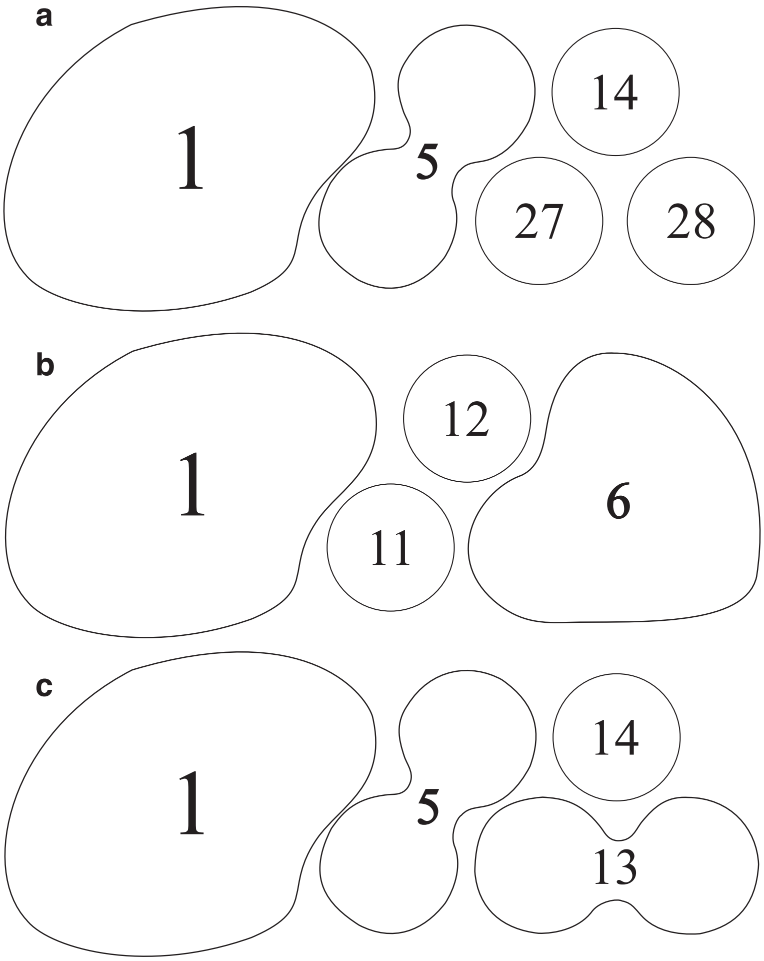

Figure 4 Additional network views. (**a**) Network view for clusters 27 and 28. (**b**) Network view for clusters 11 and 12. (**c**) Network view for cluster 14.

number of nodes or separation of interests, resulting in an additional cluster in their view. Moreover, in this particular example, even though cluster 14 is the actual cluster, if one or more divisions were to occur, no changes would be noticed by clusters 27 and 28. The remaining views for clusters 11 and 12, as well as for cluster 14 are presented in Figures 4b,c, respectively.

In addition to the already mentioned aspects of the CGP Hierarchy, the most relevant characteristic is how it is able to cope with mobility phenomena and with changes in the clustered network. By using different network perspectives to each cluster, the addition or deletion of clusters, as well as the changes in nodes' cluster association, will only have an impact to hierarchical nearby clusters in which the changes occur.

Route establishment

Despite having a robust hierarchy, a key aspect of the CGP is enabling the routing between the virtual and real clusters, ensuring scalable routing between source and destination nodes. Similarly to other routing protocols, the path establishment within clusters is performed by a link state routing protocol, such as the OLSR protocol. However, additional procedures have to be guaranteed so that packets are correctly forwarded between different clusters, as no additional protocol is used.

The CGP approach does not require additional routing messages and limits its overhead by inserting Gateway Information in the messages of the OSLR routing protocol. Moreover, the presented routing approach maintains a mapping of each node's cluster association, propagating this information in existing routing messages only when changes occur.

The creation of Gateway Information occurs only when a node in the vicinities of a neighbor cluster receives routing messages from other clusters. While routing messages from foreign clusters are typically discarded, the CGP uses these foreign messages to overhear the network topology information as perceived by other clusters. A foreign message is received when a routing message with different CID is received. This process, which extracts foreign information for use inside the GW's own cluster, is described in Procedure 1.

After processing this information, border nodes, or Gateways, learn their own network perspective as well as the reliability of themselves as Gateways, and announce it to every node within their clusters. This aspect results from the link quality of the Gateway node, determined by using Kernel Estimators, presented later in this study. An additional feature of the used Gateway nodes, is the store-and-forward capability. This allows Gateways to temporary store data packets when for some reason a broken link is detected, or when a cluster changes. By using this mechanism, less packets are lost and the healing process of previous routes is automatically triggered.

When defining a routing path, a source node's main concern is to identify where the destination node can be found, the node's perspective to what concerns their own CID is presented in Procedure 2. Assuming that the destination node is within the same cluster as the source node, the shortest path is already known according to the routing table defined by the link-state protocol. However, when a destination is found in a different cluster, the next task of the source node is to find the most suitable Gateway node. By analyzing the provided information by each Gateway node in each cluster, the source node will choose the path with less cluster-hops, forwarding packets to it.

As previously presented, nodes within a cluster only perceive the network's clusters to a certain extent. This network perspective allows a very straightforward routing decision which aims at reducing routing complexity, maintaining scalability. However, as nodes choose the shortest path taking into account cluster-hops, the total number of hops may be penalized against routing stability. Also, the Gateway selection also thrives to choose the Gateway with the best link-quality, avoiding nodes under congestion or with unreliable links due to mobility or

Procedure 1 Message received algorithm

```
procedure PROCESS_ROUTING_MESSAGE($message$)
    ...
    $src_{addr} \leftarrow message.src_{ip}$
    $cluster_{id} \leftarrow message.cluster_{id}$
    $Ip\_Cluster\_Mapping\_Create(src_{addr}, cluster_{id})$

                                        ▷ Get IP-Mapping information (performed by all nodes)
    for each $mapping_{entry}$in $message.ip\_mappings_{shared}$ do
        $Ip\_Cluster\_Mapping\_Create(mapping_{entry})$
    end for

    if $cluster_{id} \neq own\_cluster_{id}$ then                          ▷ This Node is a Gateway
        $Gw\_Connectivity\_Create(cluster_{id})$
        for each $cluster_{entry}$in $message.cluster_{connectivity}$ do
                                        ▷ Overhear information by foreign clusters
            for each $gw_{entry}$in $cluster_{entry}.gateways$ do
                $Gw\_Connectivity\_Create(src_{addr}, cluster_{entry}, gw_{entry})$
            end for
        end for
                                        ▷ Messages from different clusters must not be further processed
        return                          ▷ Consequently, end the procedure

    else                                ▷ Message received from the same cluster
        for each $cluster_{entry}$in $message.cluster_{connectivity}$ do
                                        ▷ Determine if new GWs exist in own cluster
            for each $gw_{entry}$in $cluster_{entry}.gateways$ do
                $Cluster\_Connectivity\_Create(gw_{entry}, cluster_{entry})$
            end for
        end for
    end if
    ...                                 ▷ Link-state Routing Procedures
end procedure
```

Procedure 2 View determination algorithm

```
procedure DETERMINE_VIEW($CID_{own}, CID_{foreign}$)
    $level_{own} \leftarrow$ GET_LEVEL($CID_{own}$)
    $level_{foreign} \leftarrow$ GET_LEVEL($CID_{foreign}$)
    if $level_{foreign} > level_{own}$ then                                ▷ Needs to be Raised
        $CID_{foreign} \leftarrow$ JOIN_VIEW($CID_{foreign}, level_{foreign} - level_{own}$)
    else
        if $level_{foreign} < level_{own}$ then
            $CID_{own} \leftarrow$ JOIN_VIEW($CID_{own}, level_{own} - level_{foreign}$)
        end if
    end if
    if $CID_{own}$ mod $2 = 0$ then                           ▷ To check if the CIDs are "brothers"
        $even \leftarrow -1$
    else
        $even \leftarrow 1$
    end if
    while $CID_{own} + even \neq CID_{foreign}$ and $CID_{own} \neq CID_{foreign}$ do
                                         ▷ Perform a join until both CIDs are at the same level
        $CID_{foreign} \leftarrow$ JOIN_VIEW($CID_{foreign}, 1$)
        $CID_{own} \leftarrow$ JOIN_VIEW($CID_{foreign}, 1$)
        if $CID_{own}$ mod $2 = 0$ then
            $even \leftarrow -1$
        else
            $even \leftarrow 1$
        end if
    end while
    return $CID_{own}$
end procedure

procedure JOIN_VIEW($CID, n_{level}$)
    $CID_{new} \leftarrow \left\lceil \left[ CID - (2^{n_{level}+1} - 2) \right] / 2^{n_{level}} \right\rceil$
    return $CID_{new}$
end procedure

procedure GET_LEVEL($CID$)
    $Level \leftarrow \left\lfloor log_2(CID + 1) \right\rfloor$
    return $Level$
end procedure
```

interference, allowing load-balancing between the existing resources.

Even though the total number of hops achieved by CGP may not be the smallest possible, as packets travel through clusters, their proximity to the destination cluster unveils a more precise network view and thus shortest paths are more likely to be established. In addition to this, mobility phenomena which might render previously calculated paths impractical, are transparent throughout the packet forwarding amongst different clusters. This straightforward approach allows the CGP to automatically repair routing paths such that an outdated routing decision does not result in a packet drop. Hence, with this self-healing characteristic, whenever a packet is incorrectly forwarded, the following nodes will certainly be able to re-forward it into the correct path.

3.3 CGP routing examples

While having a wireless network organized according to the expected node interactions will allow routing protocols to perform more efficiently, less common interactions between different clusters must also be handled. For instance, referring back to the network hierarchy presented in Figure 2, the worst case scenario would occur with packets being sent from a source node S within cluster 7 to a destination node D in cluster 28. Even though this social interaction is not expected to be common, it might occur and the packet forwarding by CGP will be described next. The presented Gateway and path choices are merely illustrative and, despite aiming at minimizing the number of cluster hops, different paths may exist and will be chosen according to the current load in each link.

The forwarding process begins with identification of the destination's node (D), and the cluster to which it belongs. The source node (S), is responsible for this task and verifies that the most suitable Gateway is G_1 which has a distance of 2 Cluster Hops. The routing from S to G_1 is performed within the cluster by checking the intra-cluster routing tables. At this point, all the nodes handling packets from this flow know only that node D has a CID of 2 (according to their hierarchical perspective). This is illustrated by Figure 5.

After having received an incoming flow from Cluster 7, node N_1 processes it similarly to node S, verifying that G_2 is able to reach the desired destination with a single Cluster Hop. Once the packets are received by N_2, the hierarchical perspective is changed and the forwarding path is narrowed. As illustrated by Figure 6, node N_2 has a more precise knowledge about the destination's cluster and forwards the traffic to G_6. As soon as packets arrive to cluster 27, node N_6 already knows the exact cluster to which the packets must be forwarded as it is a sibling cluster. The final forwarding steps are depicted in Figure 7.

In the previous example, the destination node D is expected to remain static in cluster 28. However, if this node moved itself to a nearby cluster, only small parts of the forwarding procedure would have to be changed. This transparent way of dealing with mobility results from the usage of virtual clusters which enables a progressive or deferred routing discovery. For instance, assuming that the destination node moves to cluster 27, all the previous steps would be kept unchanged until node N_6 is reached, using the default intra-cluster routing tables to route the packets to node D. Moreover, if any packets are sent to the destination node during the update of routing tables, no problem will be raised as nodes will automatically re-direct the packets back to the new destination's cluster.

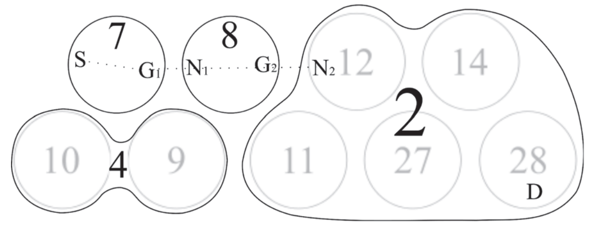

Figure 5 Forwarding illustration.

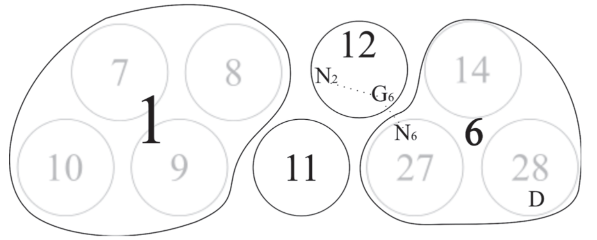

Figure 6 Updated hierarchical perspective.

The previously mentioned steps remain the same since no change is detected by the nodes in other clusters. As far as it is perceived by nodes not in clusters 27 or 28, the destination node D has always been either in cluster 2, cluster 6, or cluster 13, depending on the hierarchical position of the observing clusters.

In the described packet forwarding scheme, the Gateway nodes always have to identify the current destination's (D) Cluster. This is required since a Gateway node may be a Gateway to several clusters at the same time and it needs to choose the appropriate one. Another important aspect of packet forwarding is the choice of the most suitable Gateways. This parameter results directly from the reliability of the link between the nodes in neighbor clusters and the Gateway, as presented in the following section.

4 Gateway selection in the CGP

In CGP the appropriate choice of a Gateway node is crucial for correct forwarding of packets throughout the network. Therefore, an important part of this study is the definition of a link quality metric, achieved by using local polynomial Kernel Estimators. This metric will allow the selection of most suitable existing Gateways, being able to re-route in real-time packets to more reliable Gateways. This estimation tool is obtained from analyzing the time interval between the reception of periodical routing messages, while deriving an accurate model for that purpose, as suggested in a previous study [30] which evaluated the performance of this technique. By extending this model in order to take into account routing decisions, load-balancing properties will also be given to the protocol, avoiding links under congestion.

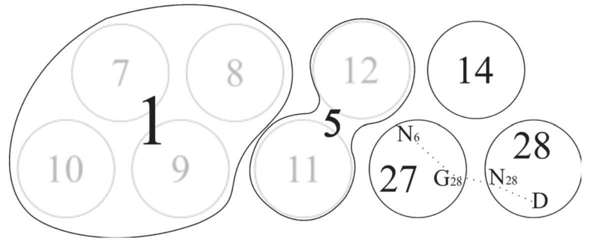

Figure 7 Final forwarding steps.

4.1 Kernel estimators

Kernel estimators are applied by Kushki et al. [31] for positioning purposes in Wireless Local Area Networks, by creating “fingerprints” using the received signal strength (RSS). The results presented show that Kernel Regression is an efficient solution for such scenarios, thus motivating further usage of Kernel methods in wireless modeling. Considering link quality, Kernel methods will allow, by using existing routing or signalling messages, the determination of a link quality model estimator. The purpose is to analyze the interval between these periodically received messages, and, based upon them, estimate the quality of the used wireless link. These periodic messages can be obtained for instance from the routing protocol or from Layer-2 messages, such as beacons.

In particular, focusing on the OLSR protocol, it periodically sends *HELLO* messages with an interval of $2 \pm d, d \in X \sim U(0, 0.5)$ seconds, being d an added delay following a uniform distribution between 0 and 0.5 s. These messages are sent so that new links and lost links are regularly detected. The random factor is added in order to try to avoid nodes from sending routing packets at the same time, which would cause several collisions in the wireless medium. The expected average interval between *HELLO* messages in a perfect connection would be exactly $E(X = \widehat{\Delta t}) = 2s$. However, since packet collisions and interferences exist, errors may occur resulting in lost packets. Thus, throughout this study, the Quality of a Link will depend on the number of lost packets between two received *HELLO* messages, such that a link without packet losses has perfect link quality. The link quality is defined by Equation (1).

$$\text{Link Quality}_{\Delta t} = \frac{1}{1 + \text{packets lost}} \tag{1}$$

The time interval between a packet being sent and received depends not only on propagation characteristics, but also on the number of required packets sent until one is properly received, as depicted in Figure 8. Figure 8a represents a link quality of 100% for Δt_1, Δt_2 and Δt_3, while in Figure 8b, Δt_1 has a link quality of 100% and in Δt_2 the link quality is only of 50%. These errors are more prone to occur when a poor link quality is registered. Therefore, by measuring the interval between consecutive *HELLO* messages, an estimation of the link quality can be retrieved using Kernel regression estimation.

As previously mentioned, the estimators used in this study are from the class of kernel-type regression which allows the estimation of a least-squared weighted regression function $\hat{m}(x; p, h)$, that “locally” fits a pth degree polynomial, for a given data set (x, y) [32], where h is the smoothing or bandwidth parameter. Kernel methods and, in particular, kernel regression methods are also called *memory-based methods* because they require keeping or storing the entire training set to estimate or compute future data points. In fact, these methods fit a model separately at each data point x_i. Only data points close to x_i are used to fit the above mentioned model. This fitting process is such that the resulting estimated function is smooth in $\Re$.

Other regression functions related with Kernel regression are the K-nearest neighbor (KNN) classification, state vector machines (SVM), Neuro-fuzzy models and radial basis functions (RBF), which may not be so robust. For instance, on the classification RSS based fingerprints, Kushki et al. [31] do not consider the KNN approach as it presents a poor performance when training vectors that are nonconvex and multimodal. Also, previously used SVMs and RBFs have shown no resilience in scenarios with highly dynamic wireless settings, where MANETs should be included.

In this study, the Gaussian Kernel [32] will be used for the estimation of link quality results and a smoothing parameter h, usually referred to as bandwidth, will be chosen using averaged squared error (*ASE*) in order to prevent under or over fitted estimations and guarantee the quality of the estimation. The *ASE* is a discrete approximation of the Integrated Squared Error (*ISE*), which has been shown by Marron et al. [33] to lead asymptotically to the same level of smoothing as the *ISE* and mean integrated squared error (*MISE*). Therefore, without significant loss of performance and knowing that it is the easiest to calculate and handle [34], the *ASE* is clearly an appropriate bandwidth selector.

4.2 Link quality estimation metric

Having defined the required theoretical aspects of the proposed Link Quality Estimator Model, it is necessary to calculate and integrate the link quality estimation as a metric in the CGP.

The *R* statistical language [35] was used together with the “locpol” package [36] in order to perform the required bandwidth computations and regression fitting, using as input *HELLO* message’s traces obtained from the OPNET Modeler Wireless Simulator [37], between two nodes placed at different distances and by collecting the link quality information.

Using the structure maintained by each active link, the time interval between each *HELLO* message is kept, as well as the previously calculated link quality defined by $\widehat{m}_{t-1}$. The defined metric that takes into account not only the current link quality, but also the stored past link quality history, weighing both in order to provide the best possible results. In Equation (2) the link quality metric (LQM) is defined, where w_{current} and w_{past} represent the

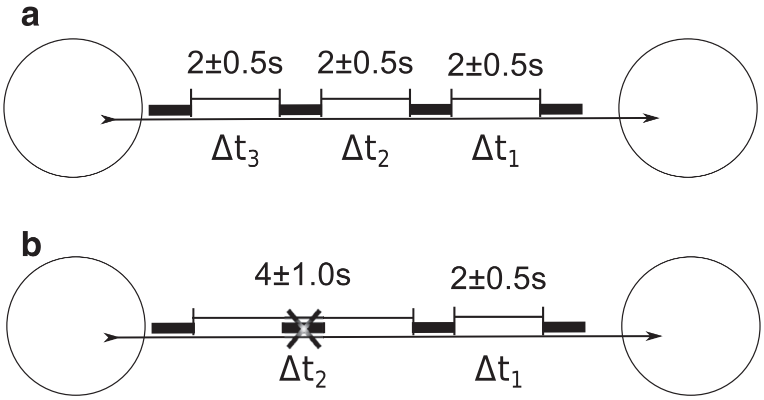

Figure 8 Periodic routing message exchange. (**a**) No lost packets. (**b**) Packet loss.

weight for the current and past link quality respectively, with the following restriction $w_{\text{current}} + w_{\text{past}} = 1.0$.

$$\text{LQM}(x) = w_{\text{current}} \times \widehat{m}(x; 1, h) + w_{\text{past}} \times \widehat{m}_{t-1} \qquad (2)$$

Since this metric analyzes the link quality between two nodes in real-time, an efficient Gateway selection can be achieved. Whenever a Gateway node is under a significant amount of traffic load, its link quality will decrease and thus an alternative Gateway, if existing, will be selected. Another external influence that can be predicted by this metric are link disconnections due to mobility since, a departing link will progressively lose its quality, leading to the selection of another Gateway node. By using this metric with a well defined cluster hierarchy and low routing overhead, the CGP is be able to efficiently forward its packets throughout the network until the final destination is reached.

5 Performance evaluation

Having presented the CGP concept and its main features towards scalable routing, it is important to evaluate its performance against other routing protocols. Moreover, being a protocol which aims at reducing the impact of mobility, the analysis of different Mobility Patterns becomes inevitable while reasoning about routing specific parameters.

5.1 Objectives

In order to provide a thorough evaluation of the CGP behavior in large scale networks, an assessment of its performance against different routing approaches must be considered such as proactive and reactive routing schemes. Moreover the following metrics will be considered in the provided evaluation:

- Traffic delivery performance:
  - Losses.
  - End-to-end delay.
- Routing performance:
  - Path length.
  - Routing stability.
  - Control traffic overhead.

Taking these different aspects into consideration, this performance assessment must involve the evaluation of a large scale network, measuring the stability and overhead of this concept, as well as its overall traffic delivery performance. Moreover, in order to allow a more exhaustive evaluation it is important to determine the protocol's ability to handle mobility phenomena, introducing dynamic scenarios with different mobility models.

Regarding this last aspect, even though many mobility models have been proposed in previous works, each one of them has unique characteristics, not replacing other existing models. Therefore, in this evaluation, several mobility patterns will be taken into consideration. In order to do so, the BonnMotion tool [38] has been used to generate different node trajectories later employed in conjunction with the OPNET Modeler Wireless Simulator [37]. These trajectories were created assuming a plausible speed for a person walking [39], between 0.5 and 1.5 m/s and a pause time of 60 s, when applicable. The mobility generation disregarded the first 3600 s, solely using the next 900 s of path randomization, avoiding the initial warm-up from the random number generations thus achieving a more stable scenario. Moreover, the area of motion was of 1500 by 1500 m, for a total number of 541 nodes. Higher speeds were not considered as the sense of clusters would be faded away and the realm of vehicular ad-hoc networks would be entered. Also, even though new mobility models already present similarities with human mobility, the used mobility patterns were chosen for the sake of comparison with existing works on this subject. Moreover, being the CGP protocol designed to explore spatial locality, it would benefit from non-random mobility models, rendering this comparison unfair.

The mobility of nodes occurs not only within but also between clusters, issuing both micro and macro mobility phenomena that must be handled by the routing protocol. The presented results reflect these routing challenges and identify the advantages of deferred routing.

For illustration purposes, after being imported to the simulator, the resulting trajectories were then converted to image files and are depicted in Figure 9 representing the Gauss-Markov (Figure 9a), Manhattan (Figure 9b), Nomadic community (Figure 9c), Random direction (Figure 9d), Random waypoint (Figure 9e) and Random street (Figure 9f) Mobility Models. These different mobility models are entirely random but each one has its own specificities. By using them the intent is to demonstrate that the Cluster Gateway paradigm is suitable in the most diverse scenarios.

5.2 Simulation conditions

In order to evaluate the performance of the presented routing paradigm (CGP in the presented figures), six scenarios incorporating different mobility models and an additional one with static nodes have been used. All these scenarios have the same area and number of nodes, using the trajectories defined by the BonnMotion tool, as previously defined.

Since the nodes move freely across the entire scenario, their cluster association has to be changed. These cluster changes are handled by the CGP protocol which considers a total of 9 clusters, divided across the scenario, updating the nodes CID when they move to a different cluster. As a result of nodes not being constrained to specific clusters, different node densities per cluster exist throughout the simulation time, while nodes follow their trajectories. These different densities impact negatively the CGP protocol since clusters are expected to be equally balanced throughout the simulation, however the CGP will still present a good performance.

Another important aspect that motivates and influences wireless multi-hop networks is the establishment of data flows between nodes. In the defined scenarios, 24 traffic flows with different destinations were generated in each run. From these flows, 50% were randomly chosen throughout the network, while the remaining traffic destinations were set to nodes within the cluster of the source node. By using this approach, both social interactions within clusters and outside will be assessed, providing a complete evaluation of the protocol's performance.

Each flow was defined with constant bit rate of 8 packets of 4 kbit per second (using UDP), being this type of traffic flows representative of typical interactive gaming, simple file transfers or information exchange [40], which are all

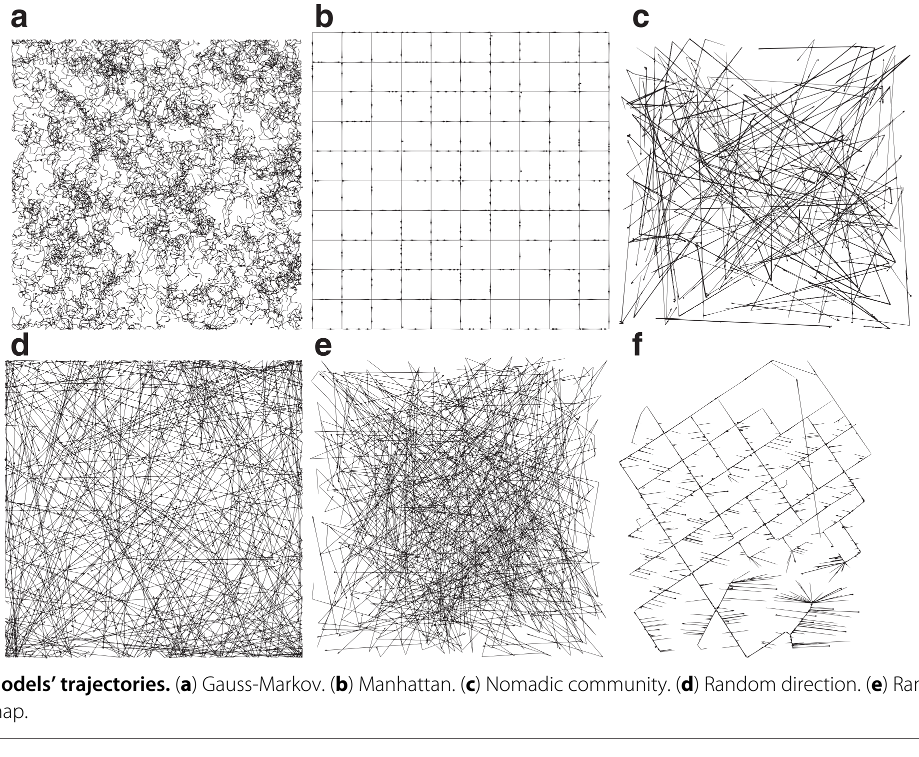

Figure 9 Mobile models' trajectories. (**a**) Gauss-Markov. (**b**) Manhattan. (**c**) Nomadic community. (**d**) Random direction. (**e**) Random waypoint. (**f**) Random street map.

well suited applications for mobile ad-hoc networks. The start time of each flow is randomly determined following a uniform distribution between 50 and 250 s of simulation time, being concluded by the end of the simulation.

For comparison purposes, all the presented scenarios have been used to evaluate the CGP, OLSR, C-OLSR, and AODV protocols. These protocols comprise respectively the different approaches available for proactive protocols, employing hierarchical clustered routing, flat un-clustered routing and flat clustered routing, taking also into account the different approaches taken by the reactive AODV protocol. By analyzing the four approaches it is easier to understand which one is more suitable for large scale networks, highlighting the main advantages and disadvantages. Moreover, by using the well known OLSR protocol, which is a standard proactive protocol from the IETF MANET working group, the CGP protocol can be validated as a functional protocol for MANETs.

6 Results

The previously described scenarios were simulated with a total of 30 runs per scenario, always using different seed values and the linear-congruential Random Number Generator Algorithm, for a total simulated time of 15 min (900 s). The considered wireless nodes follow the IEEE 802.11g standard [41] at 2.4 Ghz, and have a maximum range of 100 meters (Transmit Power of $3.7e^{-4}W$) which corresponds to the maximum obtainable range of common wireless cards [42,43]. However, due to the accurate radio model implemented by default in the OPNET simulator, asymmetric links or even unidirectional links may occur, as well as channel errors and multi-path interferences, respectively. Moreover, the CCIR propagation model was used, configured to represent small to medium city with a building coverage of 15.8 percent, as it is considered one of the best propagation models [44]. All other simulation parameters not mentioned here use their values set by default in the OPNET modeler wireless suite simulator, version 16.0.A PL1.

Regarding the store-and-forward properties of the CGP Gateways, a 4 s limit was the maximum store time defined, while re-establishing a path, before discarding packets. Even though a higher store time could be used, delay tolerant networks are out of the scope and in this study a higher delay time will mean that no route exists at a given moment from source to destination. In addition to these parameters, a Gaussian kernel was used for the link quality metric, estimating the quality of Gateways by analyzing the interval between received *HELLO* messages.

Taking into account the defined objectives of this evaluation and their statistical validity, all the presented results have a 95% confidence interval obtained from the central limit theorem which states that, regardless of a random variable's actual distribution, as the number of samples (i.e., runs) grows large, the random variable has a distribution that approaches that of a normal random variable of mean m, corresponding to the same mean as the random variable itself.

6.1 Average percentage of losses

The traffic delivery percentage obtained by a routing protocol is a good indicator of its performance when defining routing paths. Figure 10 illustrates the percentage of losses registered by the routing protocols in all the defined scenarios. In these scenarios, the CGP stands out by dint of having almost less than half of the losses than the remaining protocols. Conversely, the C-OLSR protocol registers the worst performance, having always more lost packets than the OLSR and AODV protocols. This is mainly due to the usage of C-MPRs which are not efficient in scenarios with mobility.

Regarding the Static scenario, the OLSR and C-OLSR protocols unexpectedly show worse delivery performance than in the mobile scenarios. This is a consequence of their inability to scale, as in the Static scenario more paths exist, whereas in the Manhattan scenario, for example nodes are separated by the arrangement of the streets. However, the CGP scheme is oblivious to the nodes' placement and has a similar performance in all the scenarios. This is extremely important as the social interactions between users may several times lead to static scenarios, for instance in concerts and sport events.

When comparing the standard proactive and reactive protocols, OLSR and AODV, the on-demand approach has slightly less losses in a majority of the presented scenarios. However, there is still a large number of losses since the AODV protocol is more suitable for sparse networks and does scale appropriately.

Even though the total percentage of losses is significant to all of the protocols, they are all real-time protocols and some routing paths may never exist between source and destination nodes. This is a characteristic of the used networks which do not guarantee traffic delivery at anytime, in particular since UDP is used. However, when analyzing the obtained results, the CGP always performs better than its competitors.

6.2 Average path length

Minimizing the path length is one typical target of routing protocols, with the purpose of reducing the network load and optimizing packet delivery. However, due to network dynamics, which is strongly influenced by node mobility, such routing approach may reduce the protocols' traffic delivery. Regarding the number of hops in a perfect scenario, the maximum path length should be 22, considering the maximum range of 100 m with the

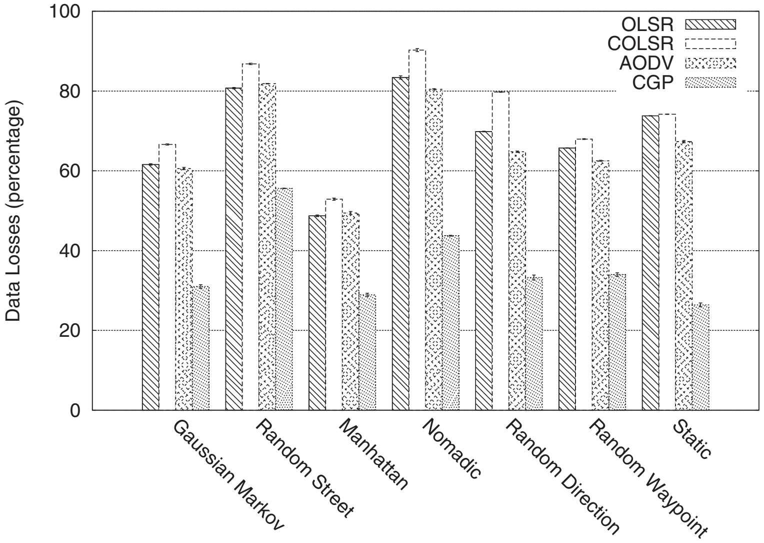

Figure 10 Average number of losses.

source and destination nodes the furthest away possible $\left(n_{\text{hops}} = \frac{\max_{\text{distance}}}{\max_{\text{range}}} = \frac{\sqrt{2}\times 1500}{100}\right)$.

In most of the scenarios, the CGP scheme is able to achieve a better path length than the remaining proactive protocols while maintaining lower losses, as depicted by Figure 11. Nevertheless, for the Manhattan, Random waypoint and Static mobility models, the CGP has a slightly higher path length. This is a consequence of the scenarios' specificities and of increased traffic performance of the CGP as it reaches more demanding destination nodes. Thus, the trade-off between path length and traffic efficiency, in order to achieve an increased traffic performance, should be regarded as an important feature from CGP.

Considering the proactive approach taken by the AODV protocol, shorter paths are provided in half of the scenarios. This reveals that proactive protocols are not as efficient, even in static scenarios. However, the CGP protocol is always capable to deliver more packets than the AODV protocol.

As a result of the randomly chosen destinations and of the wireless medium interactions, the confidence interval registered for the path length is higher than for other parameters. Nevertheless, this interval is consistent and

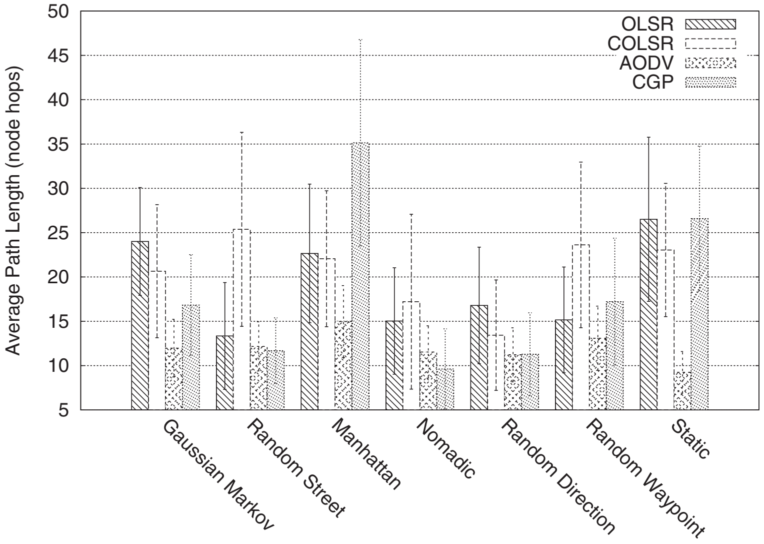

Figure 11 Average path length.

similar for all the analyzed routing protocols, validating the outcome of the parameter.

6.3 Average end-to-end delay

In Figure 12, the average end-to-end delay is presented for all the analyzed mobility models. Being the static scenario the only exception, in the remaining scenarios the CGP protocol presents a higher delay when compared against OLSR and C-OLSR. This aspect may not be desirable for certain types of traffic such as voice which are not well suited for ad-hoc networks. The explanation for the higher delay registered by the CGP is a consequence of the additional traffic delivery achieved, as an increased load of traffic is forwarded instead of being dropped.

In fact, while the end-to-end delay is typically a result of a higher path length, as shown before this is not the case. Specifically, when analyzing the Manhattan scenario, where the highest hop count of the all mobile scenarios is registered for CGP, it has at the same time the lowest delay of the all mobile scenarios. This confirms that the approach taken by CGP, which registers less losses by sometimes using longer but more stable paths, is efficient and does not introduce delay by itself. The higher delay times are not registered in the Manhattan model has the nodes follow well defined trajectories, being the additional delay overhead in the other mobile scenarios due only to repairing of broken paths, allowing the increased performance in traffic delivery registered by CGP.

Regarding the self-restoring property of the CGP, it may occur in demanding situations, where due to the mobility phenomena, instead of dropping packets while routing tables change. Thus, as previously concluded, a higher total delay average is expectable. Moreover, when bottlenecks are avoided due to load-balancing, the re-routing process may also introduce a slight delay. However, as the CGP scheme is able to reach more challenging destinations than its competitors, the additional delay overhead is justifiable, being still suitable for many different applications.

Moreover, when comparing with the on-demand AODV protocol, the CGP protocol has a significantly better performance registering up to four times less delay. The delay from the AODV protocol is accounted in part from the route discovery process but results mostly from a poor choice of paths.

6.4 Routing stability

When considering the scalability of a routing protocol, the stability of its routing tables is a key aspect on how it performs. Even though reactive protocols do not periodically update a routing table, the update of a proactive protocol's routing table may be a costly procedure in terms of both processing power and required energy, possibly leading to the creation and dissemination of additional routing messages, depleting the batteries of mobile devices faster than desirable.

Regarding this aspect, the OLSR protocol is clearly less scalable than the C-OLSR and CGP protocols which register a significantly smaller number of topology changes, as shown in Figure 13. In particular, the OLSR protocol has a worse performance for a static scenario. Such behavior is a result of the wireless medium interactions of the nodes which are strongly connected in this scenario. In fact, in the mobile scenarios, where connectivity is more often scarcer, there is a clear reduction of the number of

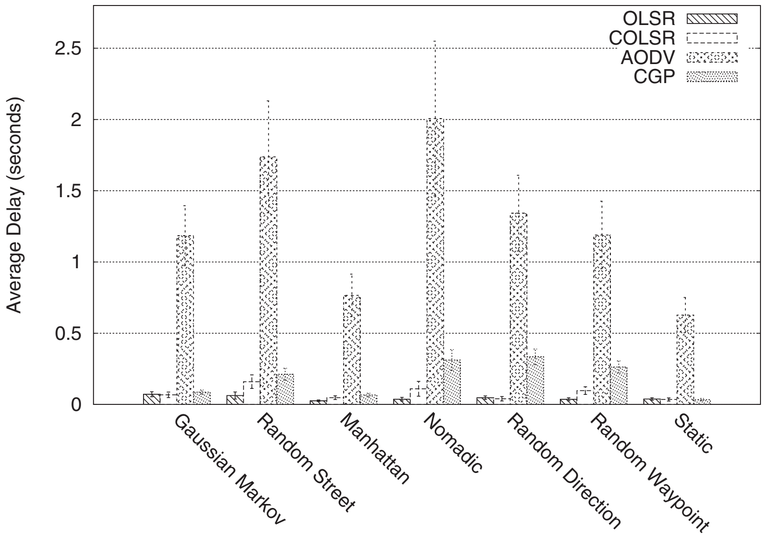

Figure 12 Average end-to-end delay.

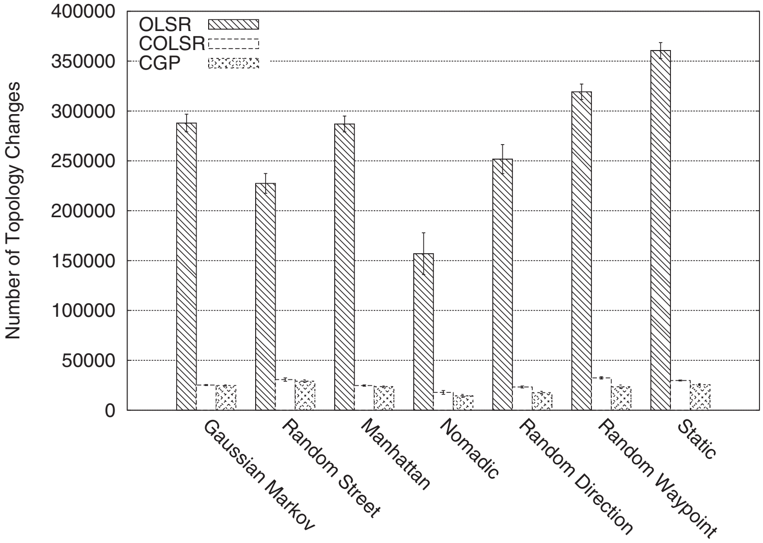

Figure 13 Average number of topology changes.

topology changes, suggesting once more that the OLSR protocol does not scale appropriately.

Regarding the C-OSLR protocol which is a clustered version of the OLSR protocol, it achieves a greater stability when compared with the standard OLSR. The number of topology changes registered by this protocol is only slightly higher than the ones obtained from the CGP. However, the overall performance of the C-OLSR protocol regarding traffic delivery suggests that its ability to timely register important topology changes is not appropriate, resulting in wrong or outdated routing paths. On the other hand, the CGP awareness of the network is entirely different, detecting only the required amount of topology changes thus being more stable, leading to an increased traffic delivery performance, lower routing overhead and better energy efficiency.

6.5 Control traffic overhead

The routing traffic overhead introduced in the network is demonstrative of a protocols' own scalability, indicating how much information it needs to exchange in order to maintain its functionality. In Figure 14, the number of sent routing control data corroborates once again the scalable properties of the CGP approach. In contrast, the OLSR protocol tends to generate a higher routing load, being only better than the C-OLSR protocol for the Random Street and Nomadic mobility models. Concerning the latter, the OLSR protocol registers a significant decrease of sent routing traffic. However, it achieves the highest number of losses when compared to the remaining mobility models, indicating its failure in establishing routing paths. This shows that even though the number of nodes in a network directly impacts the scalability and overall performance of a protocol, the mobility model must not be disregarded as it also plays an important role in these aspects.

Regarding the overhead of the AODV protocol, it strongly depends on the number of initiated flows which trigger a flooding process for route retrieval. Even though on-demand protocols are expected to generate less overhead than proactive approaches, the CGP sends less routing information than the AODV protocol.

In addition to the sent routing traffic, the amount of received control traffic should also be considered since some of the routing information may be received by several nodes at the same time. The results presented by Figure 15 confirm the tendency previously observed, where OLSR is more resource demanding than the other protocols and where the CGP scheme is the lightest. In fact, for the Nomadic scenario, where the C-OLSR protocol sends more routing information, it is possible to see that this information is only received by a reduced number of nodes when comparing with the OLSR protocol, which has a higher amount of received traffic.

Regarding this aspect, the AODV protocol provides the most efficient approach as it only requires route requests to be forward through the network until the destination node is reached. Nonetheless, the Expanded Ring Search problem, resulting from the flooding mechanisms used by AODV, has been known for generating a high overhead in challenging scenarios [45], while the CGP maintains a stable behavior.

6.6 Summary

Regarding the traffic delivery and routing performance of the evaluated protocols, the CGP achieved an overall

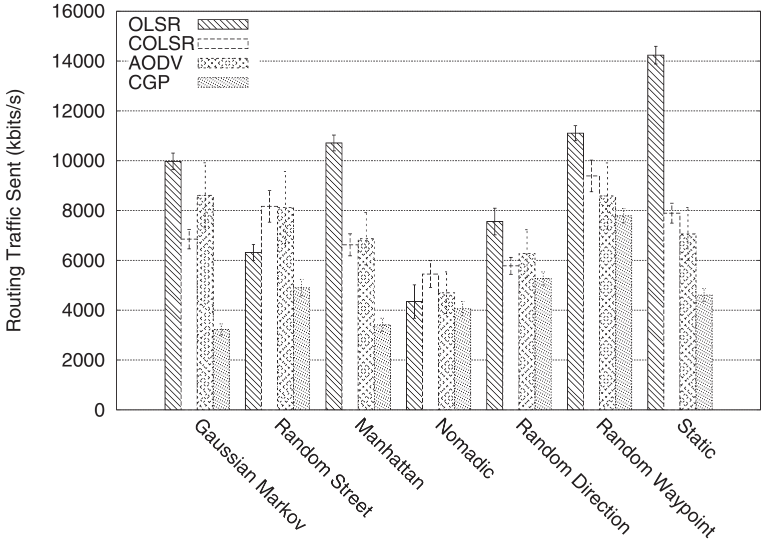

Figure 14 Average routing traffic sent.

better performance than the remaining protocols. Its self-repairing behavior and load-balancing properties for an efficient Gateway choice revealed that instead of dropping packets in changing routes, storing them temporarily and re-forwarding these packets to new appropriate routes enables a much more robust routing protocol. Moreover, the CGP also revealed that its cluster-based hierarchy and network perspective is able to maintain higher routing stability, being less resource demanding and consequently more energy efficient.

The presented results revealed that both the OLSR and C-OLSR protocols are highly influenced by the used mobility patterns. In the performed simulations, the Gauss-Markov and Random waypoint models, despite being different, present a good distribution of nodes where some areas are more dense than others. However, between these two mobility models, even though no significant changes are registered for the CGP, the performance of the OLSR and C-OLSR protocols changes considerably regarding routing overhead and path length. Moreover, the provided results also considered a reactive routing protocol, the AODV protocol, which revealed that it suffers from an increased end-to-end delay when compared to proactive versions

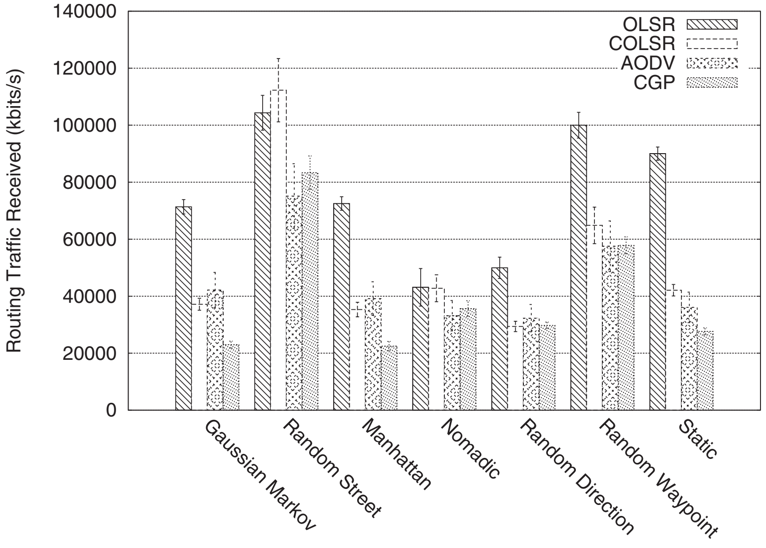

Figure 15 Average routing traffic received.

and also that it registers more losses than the CGP protocol.

In the Manhattan model, nodes are geometrically separated, avoiding a large concentration of nodes and leading to less routing path alternatives. This aspect allows the OLSR protocol to perform better than in other scenarios, but still with a large amount of losses. Due to the group mobility defined by the Nomadic mobility reference, the C-OLSR and OLSR protocols are able to generate less control overhead but the number of losses increases. The impact of mobility is also noticed in the Random Direction model where nodes only change direction when they reach the scenario boundaries, and in the Random Street Map model which, similarly to the Manhattan model, is based on the organization of the streets in a city.

This impact taken by mobility is less noticeable when analyzing the CGP which has a more stable performance than the other protocols. Its organization, Gateway selection metric with load-balancing and store-and-forward techniques allow an optimized routing performance, in both static and mobile scenarios, scaling appropriately, contrary to other routing protocols.

7 Conclusion

The increasing number and portability of wireless capable devices led to the creation of new applications and has brought new challenges for networking in wireless ad-hoc networks. In this study a new routing scheme, motivated by the existing issues in ad-hoc network and inspired by the relationships between adjacent clusters, is presented. The CGP can be defined as an "imprecise" routing scheme with self-healing routes that handles aggregated views of a clustered ad-hoc network, organized in an hierarchy. It does not exchange inter-cluster routing messages, relying on the routing information overheard by Gateway nodes, forwarding data packets between clusters. The protocol also makes use of a kernel-based link quality estimator which allows the choice of the most suitable Gateways, providing load-balancing and disconnection prediction in each cluster. These properties allow it to be a scalable routing protocol with constant communication complexity, being implementable with any link-state routing protocol.

Its efficiency is demonstrated against two different routing approaches by performing an exhaustive simulation assessment in several scenarios with different mobility patterns. The obtained results reveal that the CGP routing scheme is successful in improving traffic performance delivery while reducing the required amount of routing traffic, regardless of the mobility pattern. In particular, regarding different mobility patterns, it has been shown that while the CGP is consistently efficient, the clustered version of the OLSR protocol suffers from disruptions in some scenarios, having a higher overhead than the un-clustered version.

Competing interests

The authors declare that they have no competing interests.

Acknowledgements
The authors were grateful to the anonymous referees for their valuable comments which greatly helped in improving the article. This study was supported by the Portuguese National Foundation for Science and Technology (FCT) through a PhD Scholarship (SFRH/BD/43790/2008) and by the National Project MORFEU (PTDC/EEA-CRO/108348/2008), as well as the FCT UBIQUIMESH project (PTDC/EEATEL/105472/2008). The authors would like to thank the OPNET University Program for the licenses provided for the OPNET Modeler Wireless Suite®.

Received: 8 May 2012 Accepted: 7 February 2013
Published: 25 March 2013

References

1. A Cimmino, P Donadio, Overall requirements for global information multimedia communication village 10th strategic workshop. Wirel. Pers. Commun. **49**(3), 311–319 (2009). doi:10.1007/s11277-009-9686-3
2. T Clausen, P Jacquet, Optimized link state routing protocol (olsr). RFC 3626, Internet Engineering Task Force (2003). [http://www.ietf.org/rfc/rfc3626.txt]
3. Chakeres, C Perkins, Dynamic manet on-demand (aodvv2) routing. Internet-draft, Internet Engineering Task Force (2012). [http://www.ietf.org/id/draft-ietf-manet-dymo-22.txt]
4. J Eriksson, M Faloutsos, SV Krishnamurthy, Dart: dynamic address routing for scalable ad hoc and mesh networks. IEEE/ACM Trans. Network. **15**, 119–132 (2007). doi:10.1109/TNET.2006.890092
5. T Hamma, T Katoh, BB Bista, T Takata, in *DEXA'06: Proceedings of the 17th International Conference on Database and Expert Systems Applications*. An efficient zhls routing protocol for mobile ad hoc networks (IEEE Computer Society Washington, DC, 2006), pp. 66–70, doi:http://dx.doi.org/10.1109/DEXA.2006.24
6. L Canourgues, J Lephay, L Soyer, AL Beylot, in *IFIP Annual Mediterranean Ad Hoc Networking Conference (MED-HOC-NET), Palma de Mallorca, 23/06/2008-27/06/2008 IFIP*, vol. 265. A Scalable adaptation of the OLSR protocol for large clustered mobile ad hoc networks (Springer, 2008), pp. 97–108. [http://www.springerlink.com]
7. P Prasad, P Agrawal, K Sivalingam, in *6th IEEE Consumer Communications and Networking Conference (CCNC)*. Effects of mobility in hierarchical mobile ad hoc networks, (2009), pp. 1–5, doi:10.1109/CCNC.2009.4784895
8. A Lindgren, A Doria, E Davies, S Grasic, Probabilistic routing protocol for intermittently connected networks (prophet). Draft IRTF, Internet Engineering Task Force (2011). [http://tools.ietf.org/id/draft-irtf-dtnrg-prophet-09.txt]
9. E Bulut, B Szymanski, in *GLOBECOM 2010, 2010 IEEE Global Telecommunications Conference*. Friendship based routing in delay tolerant mobile social networks, (2010), pp. 1–5, doi:10.1109/GLOCOM.2010.5683082
10. A Mei, G Morabito, P Santi, J Stefa, in *INFOCOM, 2011 Proceedings IEEE*. Social-aware stateless forwarding in pocket switched networks, (2011), pp. 251–255, doi:10.1109/INFCOM.2011.5935076
11. F Santo, Community detection in graphs. Phys. Reports. **486**(3–5), 75–174 (2010). doi:10.1016/j.physrep.2009.11.002. [http://www.sciencedirect.com/science/article/pii/S0370157309002841]
12. FJ Ros, PM Ruiz, in *Proceedings of the 2007 international conference on Wireless communications and mobile computing, IWCMC'07*. Cluster-based olsr extensions to reduce control overhead in mobile ad hoc networks (ACM New York, 2007), pp. 202–207. [http://doi.acm.org/10.1145/1280940.1280985]
13. J Garcia-Luna-Aceves, M Spohn, in *Proceedings. Seventh International Conference on Network Protocols*, vol. 7. Source-tree routing in wireless networks (Toronto, 1999), pp. 273–282
14. K Kasera, R Ramanathan, in *IEEE 6th International Conference on Universal Personal Communications Record, 1997. Conference Record*, vol. 1. A location management protocol for hierarchically organized multihop mobile wireless networks, (1997), pp. 158–162, doi:10.1109/ICUPC.1997.625502

15. C Ching-Chuan, W Hsiao-Kuang, L Winston, G Mario, in *Proceedings of IEEE SICON*, vol. 5. Routing in clustered multihop mobile wireless networks with fading channel (Singapore, 1997), pp. 197–211
16. M Jiang, YT Jinyang Li, Cluster based routing protocol (CBRP). Internet-draft, Internet Engineering Task Force (1999). tools.ietf.org/html/draft-ietf-manet-cbrp-spec-01
17. G Zhu, X Jiang, C Wu, Z He, in *2010 Proceedings of the 5th International Conference on Ubiquitous Information Technologies and Applications (CUTE)*. A cluster head selection algorithms in wireless network based on maximal weighted independent set, (2010), pp. 1–6, doi:10.1109/ICUT.2010.5678667
18. T Ohta, *et al*, A class of hierarchical routing protocols based on autonomous clustering for large mobile ad hoc networks. IEICE Trans. Commun. **87**(9), 2500–2510 (2004)
19. M Joa-Ng, IT Lu, A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks. IEEE J. Sel. Areas Commun. **17**, 1415–1425 (1999)
20. T Hamma, T Katoh, B Bista, T Takata, in *17th International Conference on Database and Expert Systems Applications, DEXA'06*. An efficient zhls routing protocol for mobile ad hoc networks, (2006), pp. 66–70, doi:10.1109/DEXA.2006.24
21. N Nikaein, H Labiod, C Bonnet, in *2000 First Annual Workshop on Mobile and Ad Hoc Networking and Computing, 2000. MobiHOC*. Ddr-distributed dynamic routing algorithm for mobile ad hoc networks, (2000), pp. 19–27, doi:10.1109/MOBHOC.2000.869209
22. N Nikaein, C Bonnet, N Nikaein, in *proceedings of IST 2001: International Symposium on Telecommunications*, vol. 1. Harp—hybrid ad-hoc routing protocol (Tehran Iran, 2001)
23. M Zhang, PHJ Chong, in *WCNC'09: Proceedings of the 2009 IEEE conference on Wireless Communications & Networking Conference*. Performance comparison of flat and cluster-based hierarchical ad hoc routing with entity and group mobility (IEEE Press Piscataway, 2009), pp. 2450–2455
24. D Palma, M Curado, in *Wireless Days (WD), 2010 IFIP*. Dash, deferred aggregated routing for scalable ad-hoc networks, (2010), pp. 1–6, doi:10.1109/WD.2010.5657744
25. D Palma, M Curado, Onto scalable ad-hoc networks: deferred routing. Comput. Commun. **35**(13), 1574–1589 (2012). doi:10.1016/j.comcom.2012.04.026. [http://www.sciencedirect.com/science/article/pii/S014036641200151X]
26. G Pei, M Gerla, TW Chen, in *2000 IEEE International Conference on Communications*, vol. 1. Fisheye state routing: a routing scheme for ad hoc wireless networks, (2000), doi:10.1109/ICC.2000.853066
27. G Koltsidas, G Dimitriadis, FN Pavlidou, On the performance of the hsls routing protocol for mobile ad hoc networks. Wirel. Pers. Commun. **35**, 241–253 (2005). doi:10.1007/s11277-005-3491-4
28. B Zhou, Z Cao, M Gerla, in *Sixth International Conference on Wireless On-Demand Network Systems and Services (WONS)*. Cluster-based inter-domain routing (cidr) protocol for manets, (2009), pp. 19–26, doi:10.1109/WONS.2009.4801843
29. AD De Clauzade De Mazieux, M Marot, M Becker, in *Proceedings of the 6th international IFIP-TC6 conference on Ad Hoc and sensor networks, wireless networks, next generation internet, NETWORKING'07*. Correction, generalisation and validation of the "max-min d-cluster formation heuristic" (Springer-Verlag Berlin, 2007), pp. 1149–1152. [http://portal.acm.org/citation.cfm?id=1772322.1772448]
30. D Palma, H Araujo, M Curado, Link quality estimation in wireless multi-hop networks using kernel based methods. Comput. Netw. **56**(16), 3629–3638 (2012). doi:10.1016/j.comnet.2012.07.012. [http://www.sciencedirect.com/science/article/pii/S1389128612002691]
31. A Kushki, KN Plataniotis, AN Venetsanopoulos, Kernel-based positioning in wireless local area networks. IEEE Trans. Mob. Comput. **6**(6), 689–705 (2007). doi:10.1109/TMC.2007.1017
32. M Wand, M Jones, 1st edn. (Chapman and Hall/CRC, London, 1994)
33. JS Marron, W Hardle, Random approximations to some measures of accuracy in nonparametric curve estimation. J. Multivariate Anal. **20**(1), 91–113 (1986). doi:10.1016/0047-259X(86)90021-7
34. W Hardle, M Muller, S Sperlich, A Welatz, *Nonparametric and Semiparametric Models*. (Springer, Berlin, 2004)
35. R Development Core Team, R: a Language and Environment for Statistical Computing. (R Foundation for Statistical Computing, Vienna, Austria, 2010). [http://www.R-project.org/.ISBN3-900051-07-0]
36. JLO Cabrera, locpol: Kernel local polynomial regression (2009). [http://CRAN.R-project.org/package=locpol], R package version 0.4-0
37. Opnet simulator version 16.0. [http://www.opnet.com/]
38. N Aschenbruck, R Ernst, E Gerhards-Padilla, M Schwamborn, in *Proceedings of the 3rd International ICST Conference on Simulation Tools and Techniques, SIMUTools'10*, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). Bonnmotion: a mobility scenario generation and analysis tool (ICST Brussels, Belgium, 2010), pp. 51:1–51:10. http://dx.doi.org/10.4108/ICST.SIMUTOOLS2010.8684
39. 3GPP: Spatial channel model for multiple input multiple output (mimo) simulations. technical specification group radio access network. Tech. Rep. 7, 3rd Generation Partnership Project (2008)
40. ITU-T: Performance and quality of service requirements for international mobile telecommunications-2000 (imt-2000) access networks (2003)
41. S Ortiz, IEEE 802.11n: the road ahead. Computer. **42**(7), 13–15 (2009). doi:10.1109/MC.2009.224
42. G Anastasi, E Borgia, M Conti, E Gregori, in *IEEE International Conference Pervasive Computing and Communications*. Wi-fi in ad hoc mode: a measurement study, (2004), p. 145, doi:ieeecomputersociety.org/10.1109/PERCOM.2004.1276853
43. B Xing, K Seada, N Venkatasubramanian, in *INFOCOM IEEE Workshops 2009*. An experimental study on wi-fi ad-hoc mode for mobile device-to-device video delivery, (2009), pp. 1–6, doi:10.1109/INFCOMW.2009.5072111
44. W Myers, Richardson: comparison of propagation models. Technical Report 0, IEEE P802.16 Broadband Wireless Access Working Group (1999). [http://ieee802.org/16/tg2_orig/contrib/80216cc-99_13.pdf]
45. N Javaid, A Bibi, K Dridi, ZA Khan, SH Bouk, in *25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE)*. Modeling and evaluating enhancements in expanding ring search algorithm for wireless reactive protocols, (2012), pp. 1–4, doi:10.1109/CCECE.2012.6334851

doi:10.1186/1687-1499-2013-86
Cite this article as: Palma and Curado: Scalable multi-hop routing in wireless networks. *EURASIP Journal on Wireless Communications and Networking* 2013 **2013**:86.