Topology Management for Public Safety Networks

Daniel Câmara
EURECOM
2229, route des Crêtes, BP 193 06904
Sophia-Antipolis, France
daniel.camara@eurecom.fr

Christian Bonnet
EURECOM
2229, route des Crêtes, BP 193 06904
Sophia-Antipolis, France
christian.bonnet@eurecom.fr

ABSTRACT

Topology management for public safety networks (PSNs) presents some particularities which make it a challenging problem. First, the main concerns for PSNs is rapid deployment and survivability. Second, the network requirements for different disaster scenarios may differ completely. This work describes a flexible distributed algorithm to perform network admission control and topology management for public safety wireless networks using as target architecture the network proposed by the CHORIST project [5]. The proposed algorithm is able, not only to dynamically adapt to different network requirements, but also to create homogeneous clusters, where the number of mobile routers attached to each cluster is roughly the same. The technique successfully creates and maintains the desired topology relying only on a simple and customized cost function.

Categories and Subject Descriptors: C C.2.1. Network Architecture and Design: Network communications, Network topology

General Terms: Algorithms, Design, Management

Keywords: cluster heads; mesh networks; connection cost; public safety networks

1. INTRODUCTION

The deployment and the management of nodes for wireless mesh networks (WiMesh) are challenging problems and they become even more interesting when we consider them in the context of public safety networks (PSNs) environment. Not only is this kind of network, by nature, life-critical but they also have strict requirements. Moreover, these requirements may vary significantly for different disaster sites [1]. For example, the number of nodes, people served, mobility pattern and deployment environment for a forest fire fight differs from the ones for an earthquake relief effort. Well defined and maintained network structure is a fundamental step to enable the creation of efficient higher layer algorithms [2]. In this sense topology control becomes a fundamental step to enhance scalability and capacity for large-scale wireless ad hoc networks [3].

The main concerns in the establishment of public safety networks are rapid deployment and survivability [4]. PSNs must be reliable and endure even when deployed through rough environments. The network organization is a key factor to ensure endurance. In general, for small environments, the deployment of plain mesh networks is the easiest and fastest way to set a network in the field. However, this kind of structure is hardly scalable and appropriate for use on large scale and reliable environments. Structured networks, on the other hand, are more scalable, but the price to pay for this is the creation and maintenance of the structure.

This work focuses on the deployment of the access backbone proposed by the CHORIST project [5]. The backbone is responsible for providing access to end users in the field. Figure 1 presents an example of the defined structure. The main components of the network are: Cluster Heads (CHs), Mesh Routers (MRs) and Relay Nodes (RNs) and Isolated Nodes (INs). Cluster Heads are the nodes responsible for managing the radio resources for their clusters. Mesh Routers are nodes attached to CHs and that obey the CHs scheduling in order to communicate with other nodes. A node is called Isolated Node if it is not yet attached to the network, e.g. new nodes or the ones that, for some reason, lost their connection to their CHs. In the target topology neither two CHs nor two RNs can be directly connected.

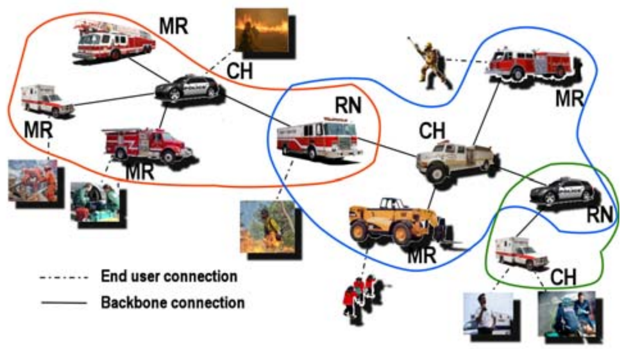

Figure 1 – CHORIST topology example

The next section presents some background concepts and some of the references used in the development of this work. Section 3 defines the problem. Section 4 introduces the proposal and discusses its main characteristics. Section 5 presents the comparative results and Section 6 shows the work conclusions and directions for future research.

2. RELATED WORKS

Midkiff and Bostian [6] present a two layer network deployment method to organize PSNs. Their network consists of a hub, and possible many purpose specific routers, to provide access to nodes in the field. In some sense our work provides the same kind of topology, since we are interested in the backbone creation to provide access for the end nodes, e.g. firefighters in the field. However, Midkiff and Bostian work has two characteristics that we want to avoid. First, the hub represents a single point of failure. If something happens to it, all the communication would be down, even between nodes inside the field. It is important for public safety networks to be as resilient as possible. The second issue we want to avoid, if possible, is long range communications and the fact that all transmissions pass through the hub. One of the objectives of this work is to avoid, as much as possible, single points of failure, while ensuring the availability of local communications. Narrowing communications to the areas they are

```
1.  Node Arrives (IN)
2.  IN sends a connection request through broadcast
3.  Waits for the responses
4.  If received any Connection response
5.      Weight the costs
6.      Sends a connection confirmation to the node with the lower cost
7.      If connected node = = CH
8.          Becomes a MR
9.      Else if connected node = = MR or to a RN
10.         Becomes a CH
11.     End if
12. Else
13.     If number of trials less than 3
14.         Return to 2
15.     Else
16.         Becomes a CH
17.         Sends a connection Update
18.     End if
19. End if
20. Wait for messages
21. If receives a Connection Request
22.     Responds with a Connection Response informing all its
    connections
23. Else if receives a Connection Confirmation
24.     Registers the connection
25.     Reevaluate state (may become a RN)
26. Else if  receives a Connection Response
27.     If interesting
28.         Sends a Connection Confirmation
29.         Registers Connection
30.         Reevaluate state (may become a RN)
31.     Else
32.         Sends a Connection Cancel
33.     End if
34. Else if  receives a Connection Update
35.     Registers the Update
36.     From time to time Evaluate Updates to find not Connected
                CHs
37. Else if  receives a Connection Cancel
38.     Removes the connection
39.     Reevaluates actual state (may become a MR or a IN)
40. End if
41. Return to 20
42. From time to time broadcasts a Connection Update
```

Algorithm 1 – Proposal high level algorithm

really needed, we save resources for other transmissions that really need to cross the network.

Bao and Lee introduce in [4] a rapid deployment method to create a wireless ad hoc backbone for public safety networks. Our work has some similarities with their proposal in the sense that we also use node connections and link quality to decide the role of the nodes, however, in our work we define dynamically the roles, using the instantaneous nodes position. We do not have any mechanism to request nodes to move to enable a better interconnection. It is true that, in some cases, this may lead to non optimal scenarios. However, we believe it is not realistic to ask a firefighter, while in the middle of a rescue operation, to move the truck to improve the network connectivity. For large scale disasters, the main focus of this work, the number of public safety teams working in a given region should give the network more than enough options to create alternative routes in the region. In this way, even if the scenario is not the optimal one, we do not consider the relocation of public safety vehicles.

The CHORIST network [5] requires the nodes to dynamically receive their roles minimizing, as much as possible, the number of communication and roles changes. We consider that nodes could arrive and attach to de network dynamically during the whole network life time. The focus of this work is the backbone structure that provides access to the end user nodes. A firefighter, for example, could connect his PDA to any of the backbone nodes and this node would work as an access point.

The desired network structure can be described as a graph and, in this case, our target network topology could be reduced to solve a Weakly Connected Independent Dominating Set (WCIDS) problem [7]. Unfortunately the dominating set and connected dominating set problems have been shown to be NP-Complete [8][9]. The minimum dominating set would also be desirable since we want to decrease the signaling messages exchanged among CH nodes. However, for our purposes it is even more important shaping the network according to the specific deployment needs than creating the minimum WCIDS.

One of the most well known heuristics for solving the connected dominating set problem is the centralized approach proposed by Guha and Khuller [10]. Even though there are approaches to solve the problem in a distributed way [11], our topology is not exactly the same one and the distributed approach can not be used directly in this case. To evaluate the proposed method we implemented a centralized and modified version of Guha and Khuller. However, we must keep in mind that for our purposes, the topology is dynamic, nodes may attach and detach from the network at any time which makes the problem even more challenging.

3. PROPOSAL

The algorithm proposed here has three main objectives. First, maintain a stable, or at least as stable as possible, network respecting the described architecture. The target application for this project public safety networks, so the topology and mechanisms to guarantee connectivity should be stable, trustworthy and rapidly deployable. The second objective is to create homogeneous clusters. Clusters should not only have roughly the same size but it is also important to be able to control and fine tuning the network shape and cluster sizes. Cluster heads must be able to optimally handle the communication among nodes inside their clusters and exchange key information with neighbor nodes rapidly and efficiently. The optimal values for number of clusters and elements by cluster vary from disaster scenario to disaster scenario. Finally, the third objective, is to keep the number of CHs and RNs as low as possible, while keeping the clusters in a reasonable size. Having the minimum number clusters, not only decreases the number of RNs but it also decreases the number, and size, of control messages in the final network.

The basic mechanism of the proposed algorithm is as follows, whenever an IN arrives, it broadcasts a connection request to the nodes nearby. This request is answered by all MR/RN/CH in the region. The neighbor nodes answer with their status, number of connections and link status. This information is then used to define a connection cost to each one of the neighbor nodes. The information on the answer packets and the cost function determine to which node the IN will attach. To accomplish all the previously defined objectives, this proposal implements a cost policy for the nodes wiling to attach to the network. Depending on the nodes that answer the message, and the connection cost of each one of these answers, the node may become a MR, or a CH. A more complete description of the proposed algorithm is depicted in Algorithm 1. The roles are designed to be stable, thus to increase the network stability a node gives up being a CH or a RN only if it moves and loses all its connections, or if, when a new CH/RN, it becomes in conflict with other, CH/RN in the region.

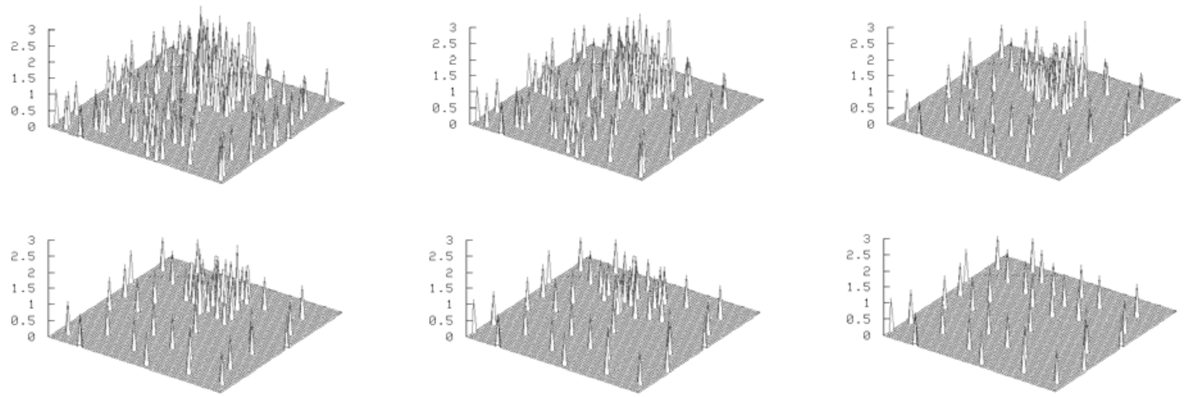

Figure 2 – Number of cluster heads spread through the network according to the different evaluated configurations, for a 40% concentration scenario

The cost function, that controls the protocol behavior, can be as simple or as complex as one needs it. For these experiments we chose only to focus on the number of nodes. However, other factors could be taken into account, e.g. perceived quality of signal, number of blocked nodes and mobility pattern. The important point is to perceive that the cost calculation is a flexible way to control the network connections and the topology behavior. Fine-tuning the defined cost function one can, for example, decrease the number of connections of each CH and increase, or decrease, the size of the clusters. This flexibility is an interesting asset since different disaster sites could have different network sizes and the network operation can be shaped as desired.

EVALUATIONS

The evaluations were made using the Sinalgo simulator [12] in a 2000x2000 square meters area. We vary the number of nodes and the communication range of the nodes. All experiments were conducted using Linux Fedora Core release 6 in an Intel Xeon 1.86GHz machine with 16GB of RAM. All graphs are presented with a confidence interval of 99% and each point is the result of the mean of 34 runs with different network configurations. The nodes arrive randomly and are placed uniformly over the observed area. For the centralized implementation all nodes positions are known in advance and the algorithm creates, in an offline manner, the complete network graph and find the best possible roles for the nodes in the final network configuration. The results of the offline implementation are the best possible configuration for the minimum WCIDS, and hardly achievable by distributed algorithms, where nodes have only local information and new nodes arrive at different moments through the network life time. Even though not applicable in the real world, the offline implementation shows how far our results are from the theoretical minimal CH optimal solution.

The communication range is 250 meters for all the nodes. To evaluate the different behaviors of the cost formula we defined six different network configurations and nodes costs. The cost to attach to a given node may translate many issues, but as we target the number of nodes, if we want, for example, to shape the network with less CHs we need to decrease the cost to attach to a CH and increase the attachment costs for other kind of nodes. The configuration values chosen need to take into account, for this case, the average expected density of the network. For, each different real deployment the values must to be adapted accordingly. The configurations used for this set of experiments are:

- *Configuration 1*: favors the creation of clusters, as much as possible, i.e. nodes should become CH. It has high cost to connect to a cluster and low cost for connecting to other nodes. The connection cost values are CH=20, MR=5, RN=1.
- *Configurations 2 to 5*: are variations over the standard configuration, small costs for attaching to CHs and little bigger one for RNs and MRs. We want to evaluate if small variations of costs may affect the algorithm behavior. The used values are : *Configuration 2* CH=0, MR=2, RN=1, *Configuration 3* CH=0, MR=5, RN=3, Configuration 4 CH=0, MR=7, RN=5 and *Configuration 5* CH=0, MR=20, RN=5.
- *Configuration 6*: is the one that tries to shape the network as close as possible to the minimum WCIDS, the target configuration of the implemented offline approach. The connection costs applied for this case are CH=0, MR=50, RN=45

The configuration 1 and 6 are diametrically opposite in the sense that the first one aims to stimulate the creation of CHs while the second one aims to prevent it.

To simulate different disaster scenarios we varied the concentration of the network. We randomly chose a point in the defined area and evaluate different nodes densities in a 300m distance from this point. The observed concentrations were 10%, 20%, 30% 40% 50% 60% 80%.

Figure 2 shows a typical example of how the CHs distribution is affected by the cost function. The graphs show that the cost functions clearly influence the final shape of the network. The first configuration, which prioritizes the clusters creation, has the number of CH nodes close to the network distribution itself. On the other hand, the configuration 6, presents a CH distribution close to the one found by the offline approach, which finds the minimum WCIDS. In fact, Configuration 6 ignores the nodes concentration and spreads the CHs more evenly over the evaluated area.

Figure 3 presents the Configuration 2 cluster sizes and the cluster distribution, for the different evaluated distributions. We can observe that for Configuration 2, as it was intended, the cost function increases the number of CHs in the more crowded areas at the same time that keeps the size of the clusters under control.

The graph of Figure 4 shows the number of CHs for different size networks, it shows that the network behaves as expected for the different configurations. The small changes in the cost values indeed enable a fine grain control of the network shape. We can also notice that the number of CHs created by the Configuration 6 is really close to the ones found by the minimum WCIDS one; the values for both are basically in the same interval of confidence. However, different of what happens in the offline implementation our approach works in a distributed way using only local information, with the CHs being assigned dynamically.

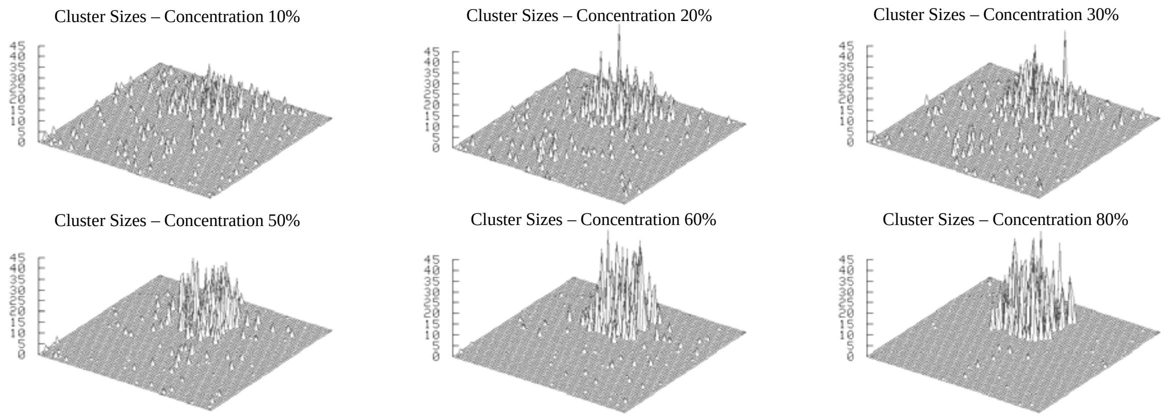

Figure 3 – Cluster sizes for configuration 2 varying the nodes concentration

Another interesting characteristic we can notice from the graph of Figure 4 is the slope of the curves, for the first Configuration, where the cost to attach to a CH is abusive, the slope is more accentuated. Nodes have a bigger tendency to become CHs. When the cost to attach to a CH decreases, the slop of the curves is less preeminent and is given by the increase in the cost of the attachment to MRs and RNs. As expected, the number of CHs decreases driven by the lower cost to attach to an existent CH. The supply and demand laws take care of load balancing the nodes and control the volume of each kind of node in the network.

The graph in Figure 5 shows the number of clusters a relay usually connects. Comparing the graphs of Figure 4 and Figure 5 we see that the number of RN connections has a direct relation with the number of CHs in the network. The bigger the number of clusters the higher is the load for the available RNs. When we decrease the number of clusters we also decrease the need for RNs. For the WCIDS offline implementation this value is around two, i.e. on average a RN connects two clusters.

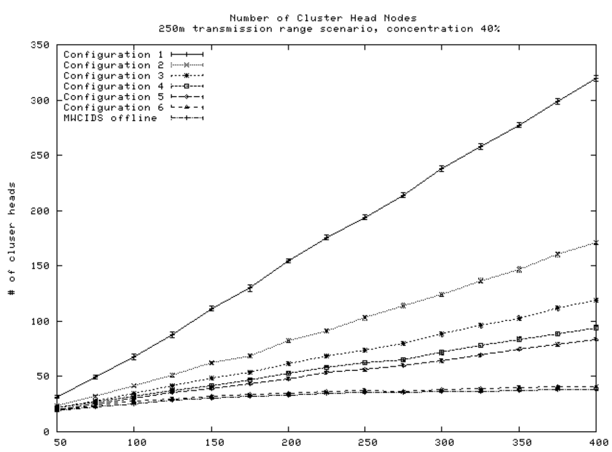

Figure 4 – Number of Cluster Head nodes

For all tested configurations our proposal increases the number of relay nodes over the minimum value, given by the offline implementation. The reasons for this are first, the technique does not have a global view to decide the best global RN. Second, as we create more clusters it is only natural we have more RNs to interconnect them. However, the most important factor that increases the number of RNs is the fact that CHs chose the RNs in a selfish manner. They choose as their RNs the nodes best suited in their point of view, not in the network one. In this way, it is possible to have, for example, two different nodes acting as RN between the same two CHs, one in each way, just because each CH chose the best node to act as its RN in a selfish manner. In this case instead of having just one RN acting as a gateway between two CHs, as it is the case for the offline approach, our approach may lead to the use of two RN, one for each CH.

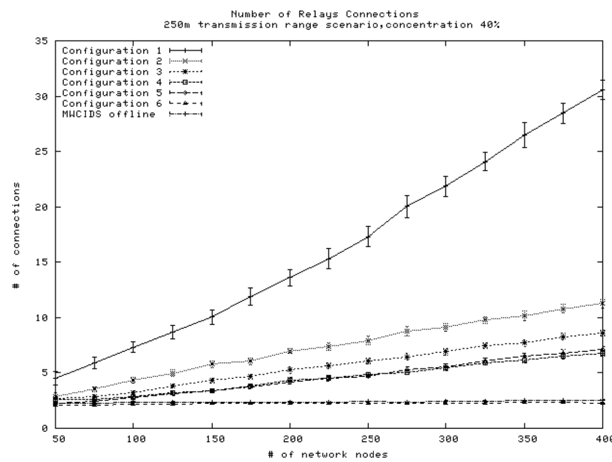

Figure 5 – Average number of clusters connected by a RN

However, the increase in the number of RNs has some advantages; first the cost function could always take into account the channel reliability and, in this case, two RNs would increase even more the network stability. Another point to observe is that path sizes are smaller when we increase the number of RNs. Increasing the number of RNs, also increases the diversity in the paths, enabling the occurrence of smaller routes between nodes.

The graph of Figure 6 shows the average size of clusters for the configuration 2 network for different network sizes and concentrations. The network concentration effectively affects the size of the clusters. However, the standard deviation for the cluster sizes, in all evaluated configurations, is typically around 0.15. This means that, even though the concentration changes, the sizes of the clusters are well balanced. Within the same scenario, the number of nodes per cluster does not present any significant variation, as we first intended.

4. CONCLUSIONS AND FUTURE WORKS

This paper presents a technique to perform network admission control and topology management for public safety networks. The addressed topology is a hierarchical one proposed by the CHORIST project [5]. The problem can be reduced to the Weakly Connected Independent

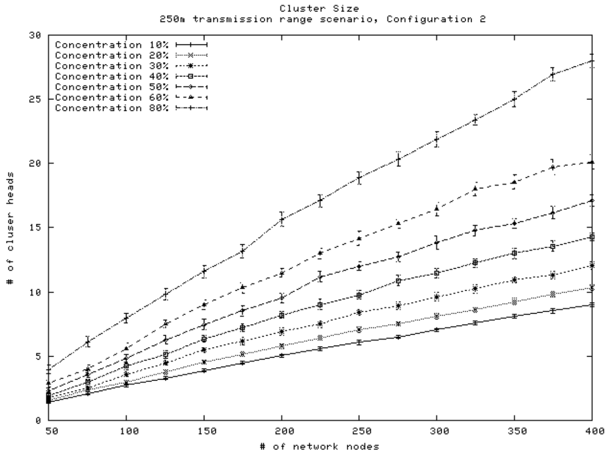

Figure 6 – Average cluster size for different concentrations of configuration 2

Dominating Set problem. For evaluating purposes a centralized version of the Guha and Khuller algorithm, to solve the minimum WCIDS problem, was implemented.

The results show that even handling only local information and without the complete final network configuration, the proposed method manages to successfully organize the nodes in the desired topology with the intended final network behavior. The technique is able to guarantee the correct clustering formation and role attribution to the nodes.

The results also show that the proposed method is quite flexible and permits, in a simple and efficient way, to shape the network topology. For example, just controlling a vector of cost functions one is able to reach, in a distributed way, results close to the one presented by the offline minimum WCIDS implementation. The simple network behavior control permits a more flexible deployment for public safety backbones in different sites. The cluster sizes are also well behaved and homogeneous, the technique manages to perform a load balance among clusters in a dynamic and simple way.

REFERENCES

[1] Ying Huang, Wenbo He, Klara Nahrstedt, Whay C. Lee, Incident Scene Mobility Analysis, IEEE Conference on Technologies for Homeland Security: Enhancing Critical Infrastructure Dependability, Waltham, MA, May 2008

[2] R.Rajaraman, Topology control and routing in adhoc networks: a survey, SIGACT News, vol. 33, pp. 60-73, Jan.2002

[3] Paolo Santi, Topology Control in Wireless Ad Hoc and Sensor Networks, WILEY, July 2005

[4] J. Q. Bao and W. C. Lee, Rapid deployment of wireless ad hoc backbone networks for public safety incident management, in Proc. IEEE Globecom, Nov., 2007

[5] http://www.chorist.eu/, last visited Apr. 2009

[6] S. F. Midkiff and C. W. Bostian. Rapidly-deployable broadband wireless networks for disaster and emergency response. In Proc. First IEEE Workshop on Disaster Recover Networks, June 2002

[7] Teresa W. Haynes, S. T. Hedetniemi, Peter J. Slater, Fundamentals of Domination in Graphs, CRC; 1 ed., Jan, 1998

[8] M. Garey and D. Johnson, Computers and Intractability: A Guide to the Theory of NP-Complet., Freeman, New York, 1979

[9] V. Chvatal, A greedy heuristic for the set-covering problem,Math of Operation Research, vol. 4, no. 3, 1979

[10] Sudipto Guha and Samir Khuller, Approximation Algorithms for Connected Dominating Sets, Algorithmica, volume 20, 1998

[11] R. Gandhi and S. Parthasarathy, Distributed algorithms for connected domination in wireless networks. J. Parallel Distrib. Comput., Jul. 2007

[12] http://dcg.ethz.ch/projects/sinalgo/, last visited Apr. 2009