Chapter 9
Growing Fully Distributed Robust Topologies in a Sensor Network

Andrea Gasparri, Sandro Meloni, and Stefano Panzieri

Abstract. Wireless Sensor Networks (WSN) are at the forefront of emerging technologies due to the recent advances in Micro-Electro-Mechanical Systems (MEMS) technology. WSN are considered to be unattended systems with applications ranging from environmental sensing, structural monitoring, and industrial process control to emergency response and mobile target tracking.The distributed nature and the limited hardware capabilities of WSN challenge the development of effective applications. The strength of a sensor network, which turns out to be also its weakness, is the capability to perform inter-node processing while sharing data across the network. However, the limited reliability of a node, due to the low-cost nature of the hardware components, drastically constrains this aspect. For this reason, the availability of a mechanism to build distributed robust connectivity topologies, where robustness is meant against random failures of nodes and intentional attacks of nodes, is crucial. The complex network theory along with the percolation theory provides a suitable framework to achieve that. Indeed, topologies such as multi-modal and scale free ones, show interesting properties which might be embedded into a sensor network to significantly increase its robustness. In this work, a mechanisms to build robust topologies in a distributed fashion is proposed, its effectiveness is analytically investigated and results are validated through simulations.

Andrea Gasparri
University of "Roma Tre", Via della Vasca Navale 79
e-mail: gasparri@dia.uniroma3.it

Sandro Meloni
University of "Roma Tre", Via della Vasca Navale 79
e-mail: sandro@dia.uniroma3.it

Stefano Panzieri
University of "Roma Tre", Via della Vasca Navale 79
e-mail: panzieri@uniroma3.it

9.1 Introduction

A sensor network consists of a collection of nodes deployed in an environment that cooperate to perform a task. Each node, which is equipped with a radio transceiver, a micro-controller and a set of sensors, shares data to reach the common objective. Sensor networks provide a framework in which, exploiting the collaborative processing capabilities, several problems can be faced and solved in a new way. However, it comes along with several challenges such as limited processing, storage and communication capabilities as well as limited energy supply and bandwidth. Performing a partial computation locally on each node, and exploiting inter-node cooperation, is the ideal way to use sensor networks. Unfortunately, this *modus-operandi* is highly constrained by the reduced hardware capabilities as well as by the limited energy resources that makes communication extremely unreliable as well as expensive in terms of node life-time. As a consequence, the availability of a mechanism to build distributed robust connectivity topologies, where robustness is meant against random node failures and intentional node attacks, is crucial.

Sensor networks can be of interest to different areas of application, ranging from environmental monitoring [5, 38], civil infrastructures [13, 25], medical care [31, 28] to home and office applications [32, 15]. In each field, the deployment of a sensor network has provided interesting advantages. For instance, in the context of environmental monitor the introduction of a sensor network made it possible to keep environments intrinsically threatening for human beings [38] under surveillance, or in the context of medical care it made it possible to remotely monitor the health condition of patients by continuously extracting clinical relevant information [28].

Regardless to the specific application, for a sensor network in oder to properly operate, information must be shared across the network allowing for data dissemination and data aggregation. Indeed, a big effort has been done by the research community to develop efficient topology discovery and control algorithms able to achieve that. Strictly speaking, the topology discovery aims to infer the topological structure of the network for management purpose, while the topology control aims to maintain some desired network properties in order to improve the performance of networking services such as routing. In particular, regarding the topology control problem, the majority of works available in literature address this problem in terms of per-node transmission power in oder to increase the life-time of the sensor network [4, 24, 2]. Some contributions focus their attention on the fault-tollerance aspects in terms of network deployment or power assignment [21, 12, 35].

In this work, a novel topology control algorithm is proposed. The main idea is to design a robust connectivity topology by exploiting the complex network along with the percolation theory. Indeed, complex networks such as the scale-free networks show interesting properties which might be embedded into a sensor network to significantly increase its robustness. These properties can be further refined by exploiting the percolation theory which turns out to be a very suitable framework for analysis purposes. In detail, a mechanisms to build an arbitrary topology over a geographical environment is proposed. In addition, a robust distribution against random

failures and intentional attacks has been exploited, its effectiveness is analytically investigated according to [34] and results are validated through simulations.

It must be mentioned that the use of the percolation theory is not new to this field. Indeed, it was already applied to analyze the connectivity of ad-hoc networks in [11, 10] and, to develop topology control algorithms for wireless sensor network that are large-scale and lack a centralised authority in [29]. The main novelty introduced by this work is that the main results of percolation theory applied to the complex networks have been extended to provide a better tolerance to random failures of sensor network nodes. This idea to use the percolation theory not as an evaluation tool but instead to build a topology with specific properties is new, up to the knowledge of the authors, to the field of sensor networks.

The rest of the chapter is organized as follows. In Section 9.2 a summary of the state of the art is presented. In Section 9.3 an overview of the theoretical background is provided. In Section 9.4 the proposed algorithm is described. In Section 9.5 a numerical analysis to corroborate the analytical results is given. Finally, in Section 9.6 conclusions are drawn and future work is discussed.

9.2 Related Work

In the last years, a great effort has been devoted by the research community to the design of energy-efficient and fault-tolerant algorithms for sensor networks, e.g., routing algorithms [8, 23, 22]. This objective is very challenging in particular due to the dynamic nature of the sensor networks. For this reason, the topology control has become a very attractive field of research. An interesting survey of this family of algorithms is given in [30]. According to it, a possible classification of topology control techniques can be drawn either in regard of constrains on the power-range assignment or with respect to topological properties of the connectivity graph. As far as the power-assignment is concerned, a distinction can be made between between homogeneous techniques [17, 27] and non-homogenous techniques [14, 20]. In the first case nodes are assumed to have the same transmitting range while in the second case nodes are allowed to have a different transmitting range. Moreover, non-homogeneous approaches can be classified into location-based [19, 20], direction based [4, 16] and neighbor based [39, 14]. For instance, location based techniques use information regarding the location of a node, while direction based techniques exploit the relative distance between nodes and finally neighbor based techniques use only information regarding the ID of a node, neither location nor distance information is available. Alternatively, topology control techniques can be classified with respect to the topological properties of the connectivity graph resulting from their applications. In particular, a significant amount of works presented in literature are concerned with building and maintaining a connected network topology which allows data to be shared across the network. In particular, some authors have considered the problem of building k-connected network topologies with the aim of improving the fault-tolerance [1, 18, 12, 35]. Some other authors instead

have focused on topology control schemas where nodes alternate between active and sleeping time while maintaining connectivity of the whole network [9, 40].

9.3 Theoretical Background

9.3.1 Complex Network

The discovery of small-world and scale-free properties of many natural and artificial complex networks has originated a big interest in investigating the fundamental organizing principles of various complex networks. In the context of network theory, a complex network is a network (graph) with non-trivial topological features, i.e., features that do not occur in simple networks such as lattices or random graphs. Indeed, a remarkable number of systems in nature present non-trivial topological features which can be properly modeled by exploiting the complex network theory. Airlines routing maps for instance are neither random graphs or regular lattices. Nodes of this network are airports connected by direct flights among them. In particular, there are a few hubs on the airline routing map representing the major cities from which flights depart to almost all other airports. Instead, the majority of airports are tiny, appearing as nodes with one or a few links connecting them to one or several hubs. The same argument can be adopted to describe the Internet as well. In fact, also in this case, there are a few hubs constituting the backbone of the network, while the majority of nodes are connected to it by a limited number of links. Another interesting example is given by how diseases are transmitted through social networks. In fact, the way in which a disease rapidly spreads can be hardly motivated by describing the social network as a random graph or a lattice. In the same way, the protein-to-protein interaction networks (PINs) at the base of any biological process show non-trivial topological features which cannot be embedded into random graphs or lattices.

In the last decades several quantities have been investigated to characterize the properties of a complex network. Thus far, three concepts, i.e., the characteristic path length, the clustering coefficient, and the degree distribution, turned out to play a crucial role in the recent study and development of complex networks theory. The characteristic path length $\langle d \rangle$ of the network is the mean distance between two nodes, averaged over all pairs of nodes, where the distance between two nodes is defined as the number of the edge along the shortest path connecting them. The cluster coefficient $\langle c \rangle$ of the network is the average of $\langle c_i \rangle$ over all nodes i, where the coefficient $\langle c_i \rangle$ of node i is the average fraction of pairs of neighbors of the node i that are also neighbors of each other. The degree distribution of the network is the distribution function $P(k)$ describing the probability that a randomly selected node has exactly degree k, that is the number of links a node owns.

Indeed, the original attempt of Watts and Strogatz in their work on small-world networks [37] was to construct a network model with small average path length as a random graph and relatively large clustering coefficient as a regular lattice, which evolved to become a new network model as it stands today. On the other hand,

the discovery of scale-free networks was based on the observation that the degree distributions of many real networks have a power-law form, albeit power- law distributions have been investigated for a long time in physics for many other systems and processes. For a comprehensive overview of the basic concepts and significant results concerning the complex network theory the reader is referred to [36].

9.3.2 Percolation Theory

The percolation theory provides a suitable framework to analytically investigate the robustness of a network, i.e., the ability of a network to properly operate even when a fraction of its components is damaged [3].

Strictly speaking, the percolation theory is a general mathematical theory of connectivity and transport in geometrical complex system. Percolation is of particular interest to physicists as it can be considered the simplest model of a disordered system capable of experiencing a phase transition. A remarkable aspect of percolation is that many results can be often encapsulated in a small number of simple algebraic relationships. For a comprehensive introduction to the percolation theory the reader is referred to [33].

A standard percolation process can be, in general, of two types: site or bond. Site percolation on a given graph means that the vertices are empty with a given probability f (or occupied with a probability $p = 1 - f$), while bond percolation refers to the existence or not of an edge between two arbitrarily chosen nodes. Once the random deletion (or placement) of nodes or edges is done, several quantities allow the characterization of the network properties. In particular, it is possible to look at the existence and size of the giant component as a function of f, and at the average size and fluctuation in the size of finite components. In this way, it can be defined a critical probability f_c below which the network percolates, i.e., it has a giant component, and a set of critical exponents characterizing the phase transition. The exact value of such a threshold f_c depends on which kind of grid (graph) is considered and its dimension. Percolation theory gives an analytical framework for the study of failures or attacks on a network in general. During the last decades some exacts results have been proposed for special types of graphs such as one and two-dimensional lattices, Cayley trees and a general criterion for study networks robustness. In 1998 Molloy and Reed [26] defined a criterion for the appearance of the giant component in a graph with generic degree distribution $P(k)$ only analyzing its first $\langle k \rangle$ and second moment $\langle k^2 \rangle$. The Molloy and Reed criterion has been used by Cohen et al.[7][6] to give a general form for the percolation threshold f_c both for random failures and intentional attacks

The study of random failures for a sensor network can be exactly mapped into an inverse percolation problem. More precisely, given an adjacency graph A_o describing the connectivity topology of a sensor network, the inverse percolation problem consists of finding the critical fraction f_c of the links of A_o for which the giant component disappears. Obliviously, such a breakdown of the connectivity topology

drastically influences the capability of a sensor network to share data across and properly operate.

9.4 The Proposed Algorithm

In this work, a way of reproducing an arbitrary degree distribution $P(k)$ on a geographical space where nodes are characterized by limited visibility is proposed. The underlying idea is that well-known techniques in the field of complex networks robustness can be suitably applied to a geographical environment. In particular, a degree distribution with properties of robustness against both faults and attacks is sought . Indeed, the multi-modal distribution proposed by [34] provides these properties. As a result, a robust topology for a sensor network can be designed.

The following scenario is considered:

- Nodes are uniformly distributed in a closed 2-Dimensional plane of side L and area $A = L^2$.
- Nodes have a limited radius of interaction r defined as a fraction of L,

Now, given a sensor network consisting of N nodes, the number of neighbors (degree) of a generic node i is $\langle k_i \rangle = \rho \pi r^2$, where $\rho = N/L^2$ is the density of nodes deployment.

According to the given scenario the proposed algorithm works as follow: i) N nodes are distributed uniformly on a square of side L ii) as each node i starts operating, it extracts a integer k from a selected distribution iii) then i tries to make k connections with the nodes in its visibility radius r, iv) to assure the full connectivity of all the nodes an additional connectivity maintenance step is introduced. Note that, a node might not be able to establish the desired number of connections, due to the limited radius of visibility r with respect to the density of deployment ρ. Nonetheless, a good approximation of the distribution can always be reached for reasonable values of ρ and r. Indeed, this is the case for a realistic sensor network scenario.

Regarding the connectivity maintenance step, the idea is to exploit a consensus algorithm by which nodes share their ID within their visibility neighborhood, i.e., nodes within its range of visibility. From an algorithmic perspective, each node broadcasts its ID to its neighbors, if a node receives a lower ID it starts sharing the received lower number. Periodically, each node check IDs within visibility neighborhood. If one of these nodes k holds a lower ID, then node i creates a new connection to k and starts sharing k's ID. This step permits to obtain a connected network only adding few links to the original distribution, and if executed periodically to readapt network topology to failures and damages. Note that, even though the connectivity maintenance step is required, from a practical standpoint this can be avoided by performing a proper choice of ρ and r.

Regarding the distributed nature of the algorithm, it is worthwhile to mention that a few parameters concerning the degree distribution $P(k)$ are required for the algorithm in order to properly operate. Moreover, as these parameters are fixed, they can be easily hardcoded into each node.

At this point, being a technique for constructing an arbitrary distribution over a geographical space available, the analytical evaluation of the best form for the $P(k)$ is faced.

9.4.1 Optimal Degree Distribution for Random Failures and Attacks

As previously mentioned, a degree distribution which provides interesting properties of robustness has been proposed in [34]. In this work, the authors show that a network which maximizes the value of the threshold f_T, defined as $f_T = f_r + f_a$ with f_r the percolation threshold for random node removal and f_a the threshold for targeting node removal, can be obtained by exploiting the following functional form:

$$P(k) = \sum_{i=1}^{m} r_i \delta(k - k_i) = \sum_{i=1}^{m} r_1 a^{-(i-1)} \delta(k - k_i) \tag{9.1}$$

where $k_i = k_1 b^{-(i-1)}$ with k_1 min degree of the network and $\delta(x)$ Dirac delta function. In detail, the model is characterized by three different quantities: a that represents the fraction of nodes having different degrees (with $a > 1$), b that controls the values of the degrees, and k_1 that is the smallest degree in the network. The two remaining parameters r_1 and r_m can be obtained from the following normalization condition:

$$\sum_{i=1}^{m} r_i = r_1 \sum_{i=1}^{m} a^{-(i-1)} = 1 \tag{9.2}$$

as follows:

$$r_1 = \frac{1 - a^{-1}}{1 - a^{-m}} \quad \text{or} \quad r_m = \frac{a - 1}{a^m - 1} \tag{9.3}$$

and

$$\frac{a - 1}{a^m - 1} = \frac{q}{N} \tag{9.4}$$

$$r_m = \frac{q}{N} = N^{\alpha - 1} \text{ with } 0 < \alpha < 0.25 \tag{9.5}$$

with q the number of nodes with the highest degree k_m. In addition, the authors evidence an inter-dependency among all the parameters of Eq. 9.1 which leads to a model that is only a function of N and m, i.e, the number of nodes and the number of distinct modes in the distribution respectively. They also demonstrate that the mean degree $\langle k \rangle$ is:

$$\langle k \rangle = \sum_{i=1}^{m} k_i r_i = k_1 r_1 \sum_{i=1}^{m} (ab)^{-(i-1)} \tag{9.6}$$

leading to the following general form of the parameters a and b:

$$ab \sim N^{(1/2 - \alpha)/(m-1)} \tag{9.7}$$

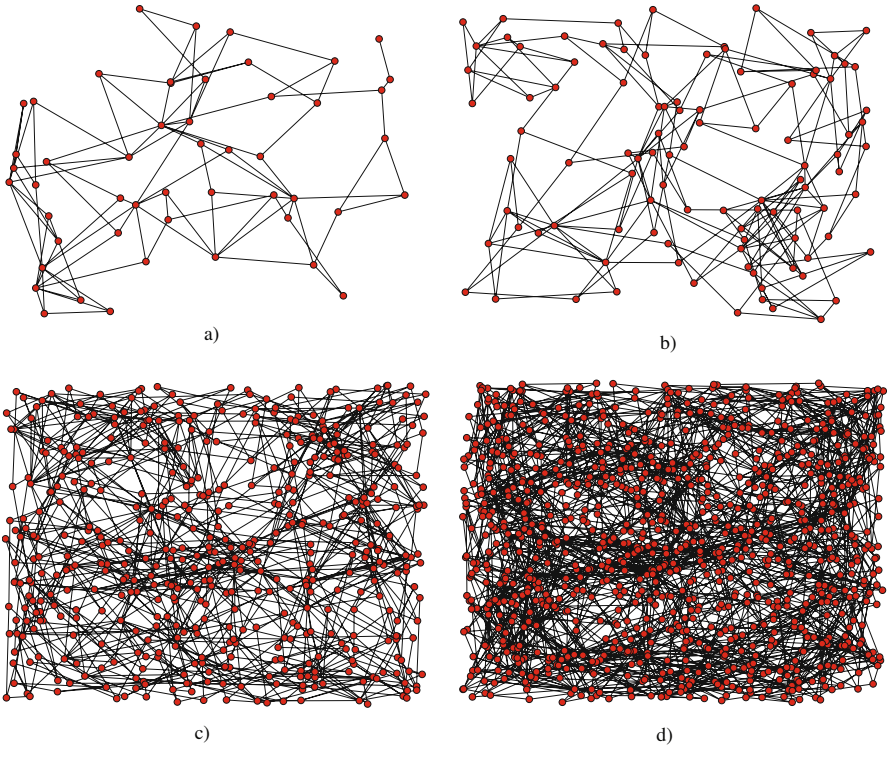

Fig. 9.1 Four examples of network produced by the proposed algorithm with different number of nodes N, a) $N = 50$, b) $N = 100$, c) $N = 500$ and d) $N = 1000$, with $m = 3$, $k_1 = 3$ and $\alpha = 0$.

from which:

$$a \sim N^{(1-\alpha)/(m-1)} \tag{9.8}$$

and

$$b \sim N^{1/2(m-1)} \tag{9.9}$$

At this point, for a given number of nodes N, the two parameters a and b depend only on m and α. This leads to a two parameters model, for which it is possible to compute the optimal value of the percolation threshold f_T^{opt} by assuming $\alpha = 0$ and $m = 2$, where $f_T^{opt} = f_a^{opt} + f_r^{opt}$ is defined as the sum of the two percolation thresholds for nodes attacks and random failures respectively. Note that, as the f_T^{opt} is a linear combination of two factors, a slightly different behavior, i.e., higher robustness to random node failures or higher robustness to intentional node attacks, can be obtained with a proper choice of the two parameters α and m.

An example of network topology created with the proposed algorithm when exploiting the multi-modal distribution described so far is given in Fig. 9.1. It can be noticed that the obtained topologies are characterized by a high number of triangles which guarantee robustness. At the same time, the degree of the most connected

nodes is kept sufficiently low which allows to both mitigate the impact of intentional attacks and limit the effect of random failures.

9.5 Numerical Analysis

The proposed algorithm have been thoroughly investigated through simulations. Two aspects of interest have been investigated: the robustness to random node failures and the robustness to node attacks. The first aims to evaluate the capability of the sensor network to properly operate even when suddenly some nodes stop working, while the second investigates the resistance of the network when in presence of organized attack aiming to destabilize the normal operating conditions.

The following indexes of quality have been considered: i) the number of components ii) the size of the giant component iii) the percentage of network disconnected. The first index gives an information about the overall connectivity of the network, the second one gives an idea about the remaining operability, while the last one gives an information about the number of nodes still functioning.

Moreover, a comparison against a null-model has been performed. Such a null-model is built starting from the network produced by the proposed algorithm by keeping the same constraints on the number of nodes, the visibility radius r but introducing a randomized version of the link connections leading to a Poisson degree distribution. As a result, a random network topology is achieved.

Several network configurations have been analyzed. In the following only results regarding a network composed by 2500 nodes deployed in an geographical space with density $\rho = 0.5$ are shown.

Fig. 9.2-a) shows the degree distribution $P(k)$ obtained for the proposed model with the parameter $m = 3$. It can be noticed the presence of three peaks, respectively for $k = 3, 22, 33$, representing the three modes of the distribution. The two remaining spare peaks can be explained by the limited visibility r of nodes. Indeed, these two peaks would tend to the closest ones on the line if the radius r were sufficiently large. Note that for $m \to \infty$ the distribution $P(k)$ tends to a scale-free distribution [34]. On the other hand, Fig. 9.2-b) describes the degree distribution $P(k)$ obtained for the null-model, which is, as expected, a Poisson distribution.

Table 14.1 gives a synoptical overview of the conducted analysis. In particular, it can be noticed that when considering two networks with a comparable number of nodes and links the proposed model turns out to be more robust. This can be explained by the higher value of the clustering coefficient $\langle c \rangle$ leading to an higher number of triangles in the network that are known to be the most robust structure against random failures. Moreover, another interesting aspect can be pointed out: both the characteristic path length $\langle d \rangle$ and diameter d_{max} are lower for the proposed model. Indeed, this is a good property for a sensor network as it implies a lower consumption to spread data over the network.

Fig. 9.3 shows the number of connected components (CC) for both the proposed model (circles) and the null-model (squares) when varying the fraction of removed links. In detail, Fig. 9.3-a) represents the behavior of the models against random

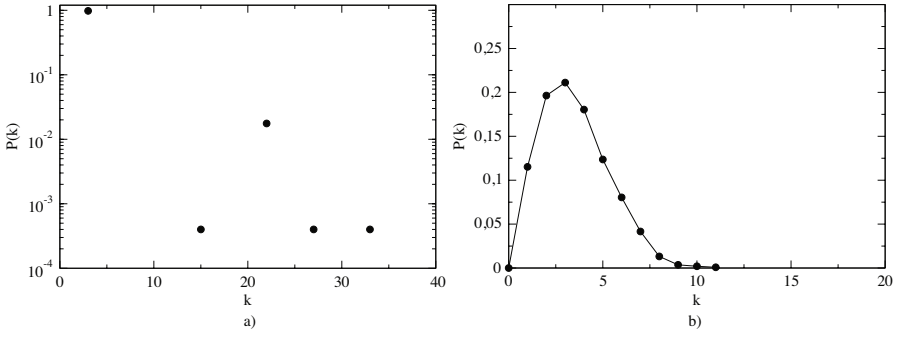

Fig. 9.2 Degree distribution of the proposed model a), and of the null-model b). Parameters setting: $N = 2500, m = 3, k_1 = 3, \alpha = 0$.

Table 9.1 Principal topological features of the proposed model and the null-model. In detail, N is the number of nodes in the network, E the numerb of links, $\langle k \rangle$ the mean degree, k_{max} the highest degree, $\langle d \rangle$ the characteristic path length, d_{max} network diameter and $\langle c \rangle$ the mean clustering coefficient.

Model	N	E	$\langle k \rangle$	k_{max}	$\langle d \rangle$	d_{max}	$\langle c \rangle$
Proposed Model	2500	4201	3.36	33	5.99	13	0.004766
Null Model	2500	4277	3.42	11	7.24	15	0.001279

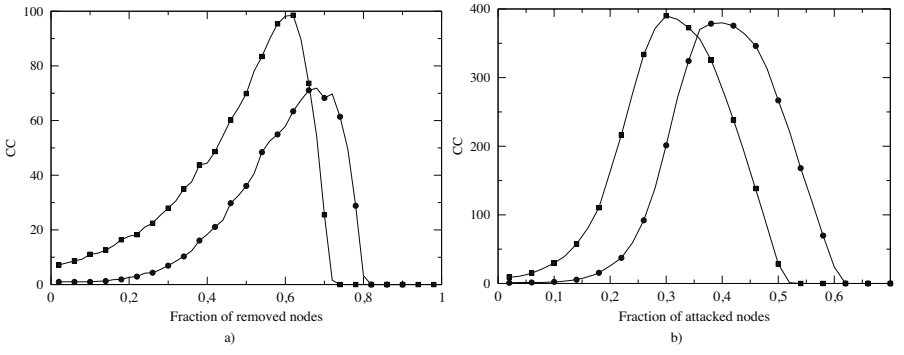

Fig. 9.3 Number of connected components (CC) vs. fraction of removed nodes for the proposed model (circles) and the null-model (squares) in case of random node failures a) and intentional node attacks b). Parameters setting: $N = 2500, m = 3, k_1 = 3, \alpha = 0$.

node failures, while Fig. 9.3-b) depicts the same behavior against intentional attacks. In both cases, the proposed model outperforms the null-model, i.e., the network starts to break down after a higher fraction of node (approx. 20%). Note that, isolated nodes are not counted as components.

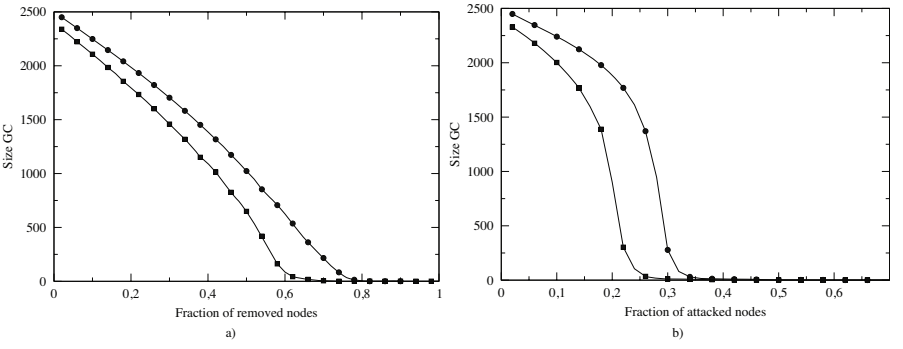

Fig. 9.4 Size of the giant component (Size GC) vs. fraction of removed nodes for the proposed model (circles) and the null-model (squares) in case of random node failures a) and intentional node attacks b). Parameters setting: $N = 2500, m = 3, k_1 = 3, \alpha = 0$.

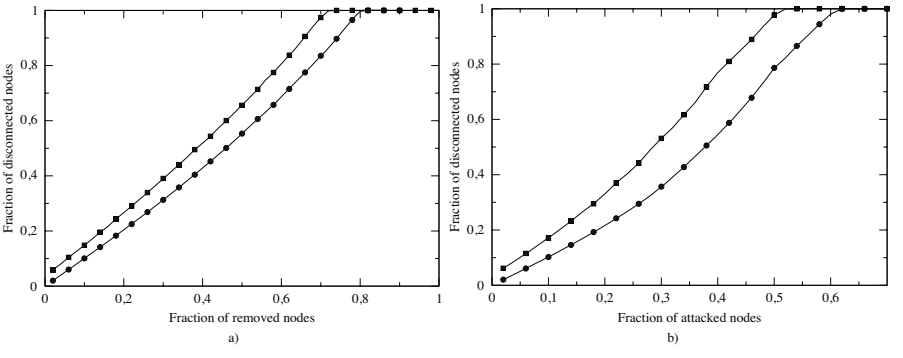

Fig. 9.5 Fraction of disconnected nodes vs. fraction of removed nodes for the proposed model (circles) and the null-model (squares) in case of random node failures a) and intentional node attacks b). Parameters setting: $N = 2500, m = 3, k_1 = 3, \alpha = 0$.

Fig. 9.4 shows the size of the giant component for both the proposed model (circles) and the null-model (squares) when varying the fraction of removed links. Also in this case, the proposed model outperforms the null-model. In particular, the size of the biggest component decreases almost linearly with the fraction of removed nodes in the case of random nodes removal.

Finally, Fig. 9.5 shows the fraction of disconnected nodes for both the model (circles) and the null-model (squares) when varying the fraction of removed links. As before, the performance of the proposed model is significantly better than the null-model.

An additional analysis of the behavior of proposed technique has been successively carried out. In particular the following aspects have been investigated: the rate of growth of the number of links with the respect to the number of nodes, the fraction of isolated nodes resulting from the removal of a fraction of nodes and the

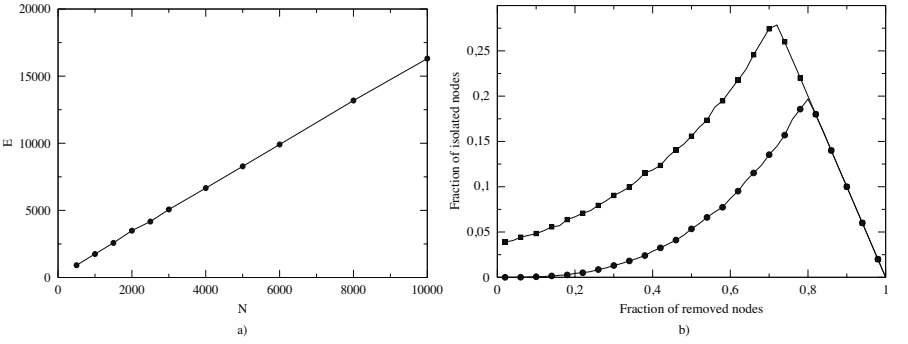

Fig. 9.6 a) Growth rate of the number of links vs. the number of nodes. b) Fraction of isolated nodes resulting from the removal of a fraction of nodes in case of random node failures.

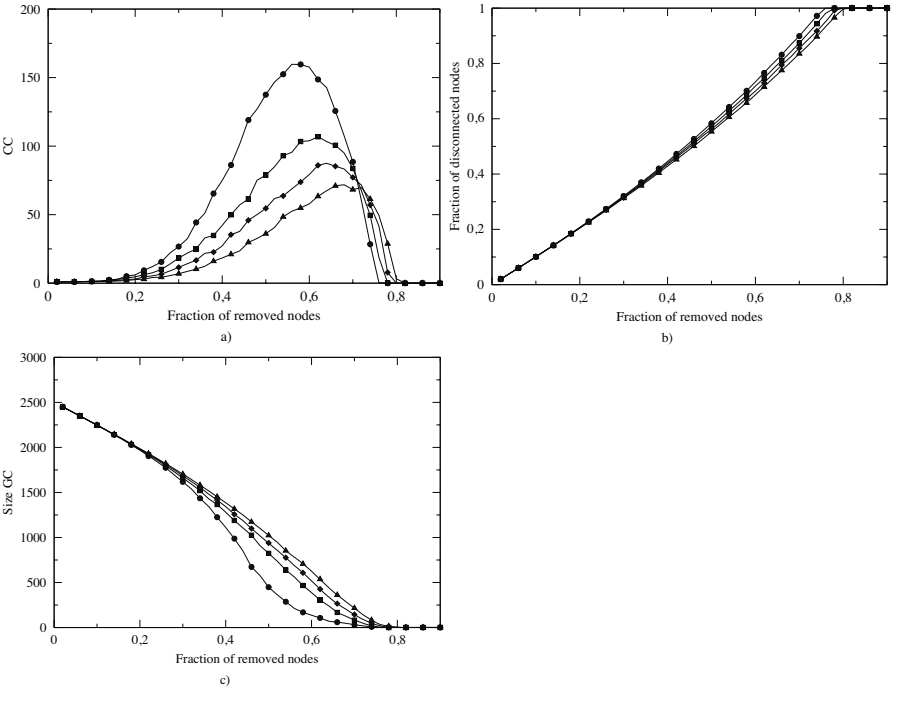

Fig. 9.7 a) Number of connected components, b) Size of the giant component and c) Fraction of isolated nodes vs fraction of removed nodes in the proposed model with different values of m. $m = 3$ (circles), $m = 5$ (squares), $m = 7$ (diamonds), $m = 10$ (triangles). Parameters setting: $N = 2500$, $k_1 = 3$, $\alpha = 0$.

variation of the tree indexes previously introduced, i.e., the number of components, the size of the giant component and the percentage of network disconnected, when varying the value of the parameter m.

Fig. 9.6-a) shows the rate of growth of the number of links with respect to the number of nodes. it can be easily noticed that the number of links increases linearly with the number of nodes. This is indeed a good property of the algorithm as the higher is the number of links the higher is the power consumption of the network leading to a good scalability. Fig. 9.6-b) illustrates the fraction of isolated nodes resulting as a consequence of the removal of a fraction of nodes. This is another interesting property of the algorithm. In fact, it points out that only a negligible percentage of nodes are affected by the removal of other nodes. In other words, by removing a node the connectivity of its neighbors is not significantly influenced.

Figs. 9.7 shows how the tree indexes change when varying the value of the parameter m. Note that, this result is referred to the proposed model against random node failures. According to the theoretical results, the higher is the value of the parameter m the better is the performance against random failures as the scale-free characterization of the degree distribution becomes more and more notable. Indeed, this is in agreement with the results obtained in [34] as the percolation threshold is not influenced by the variation of the parameter m, but at the same time other characteristics, such as the number of connected components, are positively influenced in the case of random node failures.

9.6 Conclusions

In this work, a novel topology control algorithm has been proposed. The idea is to take advantage of the complex networks along with the percolation theory to design robust topologies. Indeed, the availability of a connectivity topology algorithm able to properly operate even when in presence of random failures of nodes drastically increases the robustness as well as the operability of a sensor network.

In detail, an algorithm to build an arbitrary topology over a geographical environment is proposed. In addition, a robust degree distribution against random failures and intentional attacks has been exploited [34]. The properties of the resulting model have been analytically characterized by exploiting the percolation theory and the related results have been corroborated by numerical simulations. In particular, three different indexes of quality have been investigated, namely the number of connected components, the size of the giant component and the fraction of disconnected nodes in the network. Moreover, a comparison against a randomized version of the network (null-model) has been performed. According to these results, the proposed topology control technique has turned out to be very effective as it always outperforms the null-model in terms of connectivity maintenance against both random node failures and intentional node attacks.

To conclude, the proposed algorithm is very simple, distributed and easy to implement on-board each node. It requires a limited number of messages in order to build the topology and the number of links scales linearly with the size of the network. Moreover, even though the algorithm has been implemented only in a 2-dimensional plane, there is no additional cost to extend it to a n-dimensional space, as the topology construction relies only on the Euclidian distance.

Several challenges still remain for future work. An extension where a node independently sets its radius of visibility r might be investigated in order to reduce the energy consumption. In addition, a dynamical network rewiring process able to reconnect the network anytime two or more components arise might be considered. Finally, an enhanced scenario where mobility is taken into account for some nodes might be of interest.

References

1. Bettstetter, C.: On the minimum node degree and connectivity of a wireless multihop network. In: MobiHoc 2002: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, pp. 80–91. ACM Press, New York (2002)
2. Blough, D.M., Leoncini, M., Resta, G., Santi, P.: The k-neighbors approach to interference bounded and symmetric topology control in ad hoc networks. IEEE Trans. Mob. Comput. 5(9), 1267–1282 (2006)
3. Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., Hwang, D.-U.: Complex networks: Structure and dynamics. Physics Reports 424(4-5), 175–308 (2006)
4. Borbash, S.A., Jennings, E.H.: Distributed topology control algorithm for multihop wireless networks. In: Proc. 2002 World Congress on Computational Intelligence (WCCI 2002), pp. 355–360 (2002)
5. Cerpa, A., Elson, J., Hamilton, M., Zhao, J., Estrin, D., Girod, L.: Habitat monitoring: application driver for wireless communications technology. In: SIGCOMM LA 2001: Workshop on Data communication in Latin America and the Caribbean, pp. 20–41. ACM Press, New York (2001)
6. Cohen, R., ben Avraham, D., Havlin, S.: Percolation critical exponents in scale-free networks. Phys. Rev. E 66(3), 036113 (2002)
7. Cohen, R., Erez, K., ben Avraham, D., Havlin, S.: Resilience of the internet to random breakdowns. Phys. Rev. Lett. 85(21), 4626–4628 (2000)
8. Datta, M.-A.: A fault-tolerant protocol for energy-efficient permutation routing in wireless networks. IEEE Trans. Comput. 54(11), 1409–1421 (2005)
9. Deb, B., Nath, B.: On the node-scheduling approach to topology control in ad hoc networks. In: MobiHoc 2005: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, pp. 14–26. ACM Press, New York (2005)
10. Dousse, O., Thiran, P., Hasler, M.: Connectivity in ad-hoc and hybrid networks. In: Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2002, pp. 1079–1088 (2002)
11. Gupta, P., Kumar, P.R.: Critical power for asymptotic connectivity. In: Proceedings of the 37th IEEE Conference on Decision & Control, pp. 1106–1110 (1998)
12. Hajiaghayi, M.T., Immorlica, N., Mirrokni, V.S.: Power optimization in fault-tolerant topology control algorithms for wireless multi-hop networks. IEEE/ACM Trans. Netw. 15(6), 1345–1358 (2007)
13. Kim, S., Pakzad, S., Culler, D., Demmel, J., Fenves, G., Glaser, S., Turon, M.: Health monitoring of civil infrastructures using wireless sensor networks. In: IPSN 2007: Proceedings of the 6th international conference on Information processing in sensor networks, pp. 254–263. ACM Press, New York (2007)
14. Leoncini, M., Resta, G., Santi, P.: The k-neighbors approach to interference bounded and symmetric topology control in ad hoc networks. IEEE Transactions on Mobile Computing 5(9), 1267–1282 (2006); Senior Member-Douglas M. Blough

15. Lesser, V., Atighetchi, M., Benyo, B., Horling, B., Raja, A., Vincent, R., Wagner, T., Ping, X., Zhang, S.X.Q.: The intelligent home testbed. In: Proceedings of the Autonomy Control Software Workshop (Autonomous Agent Workshop) (January 1999)
16. Li, L., Halpern, J.Y., Bahl, P., Wang, Y.-M., Wattenhofer, R.: A cone-based distributed topology-control algorithm for wireless multi-hop networks. IEEE/ACM Trans. Netw. 13(1), 147–159 (2005)
17. Li, N., Hou, J.C., Sha, L.: Design and analysis of an mst-based topology control algorithm. In: Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, vol. 3, pp. 1702–1712 (2003)
18. Li, N., Hou, J.C.: Flss: a fault-tolerant topology control algorithm for wireless networks. In: MobiCom 2004: Proceedings of the 10th annual international conference on Mobile computing and networking, pp. 275–286. ACM Press, New York (2004)
19. Li, N., Hou, J.C.: Localized topology control algorithms for heterogeneous wireless networks. IEEE/ACM Trans. Netw. 13(6), 1313–1324 (2005)
20. Li, X.-Y., Song, W.-Z., Wang, Y.: Localized topology control for heterogeneous wireless sensor networks. ACM Trans. Sen. Netw. 2(1), 129–153 (2006)
21. Li, X.-Y., Wan, P.-J., Wang, Y., Yi, C.-W.: Fault tolerant deployment and topology control in wireless networks. In: MobiHoc 2003: Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing, pp. 117–128. ACM Press, New York (2003)
22. Liang, C., Huang, X., Deng, J.: A fault tolerant and energy efficient routing protocol for urban sensor networks. In: InfoScale 2007: Proceedings of the 2nd international conference on Scalable information systems, ICST, Brussels, Belgium, Belgium, pp. 1–8. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) (2007)
23. Liang, Q., Wang, L., Ren, Q.: Fault and tolerant and energy efficient cross-layer design for wireless sensor networks. Int. J. Sen. Netw. 2(3/4), 248–257 (2007)
24. Liu, J., Li, B.: Distributed topology control in wireless sensor networks with asymmetric links. In: Global Telecommunications Conference, 2003. GLOBECOM 2003, vol. 3, pp. 1257–1262 (2003)
25. Mehta, V., El Zarki, M.: A bluetooth based sensor network for civil infrastructure health monitoring. Wirel. Netw. 10(4), 401–412 (2004)
26. Molloy, M., Reed, B.: The size of the giant component of a random graph with a given degree sequence. Combin. Probab. Comput. 7, 295–305 (1998)
27. Nayebi, A., Sarbazi-Azad, H.: Lifetime analysis of the logical topology constructed by homogeneous topology control in wireless mobile networks. In: International Conference on Parallel and Distributed Systems, vol. 2(5), pp. 1–8 (2007)
28. Patel, S., Lorincz, K., Hughes, R., Huggins, N., Growdon, J.H., Welsh, M., Bonato, P.: Analysis of feature space for monitoring persons with parkinson's disease with application to a wireless wearable sensor system. In: Proceedings of the 29th IEEE EMBS Annual International Conference, Lyon, France (August 2007)
29. Raghavan, U.N., Kumara, S.R.T.: Decentralised topology control algorithms for connectivity of distributed wireless sensor networks. Int. J. Sen. Netw. 2(3/4), 201–210 (2007)
30. Santi, P.: Topology control in wireless ad hoc and sensor networks. ACM Comput. Surv. 37(2), 164–194 (2005)
31. Shnayder, V., Chen, B.r., Lorincz, K., Thaddeus, R.F., Jones, F., Welsh, M.: Sensor networks for medical care. In: SenSys 2005: Proceedings of the 3rd international conference on Embedded networked sensor systems, p. 314. ACM Press, New York (2005)
32. Srivastava, M.B., Muntz, R.R., Potkonjak, M.: Smart kindergarten: sensor-based wireless networks for smart developmental problem-solving enviroments. In: Mobile Computing and Networking, pp. 132–138 (2001)

33. Stauffer, D., Aharony, A.: Introduction to percolation theory. CRC Press, Boca Raton (1998)
34. Tanizawa, T., Paul, G., Havlin, S., Stanley, H.E.: Optimization of the robustness of multimodal networks. Phys. Rev. E 74(1), 016125 (2006)
35. Thallner, B., Moser, H., Schmid, U.: Topology control for fault-tolerant communication in wireless ad hoc networks. In: Wireless Networks (2008)
36. Wang, X.F., Chen, G.: Complex networks: small-world, scale-free and beyond. Circuits and Systems Magazine, IEEE 3(1), 6–20 (2003)
37. Watts, D.J., Strogatz, S.H.: Collective dynamics of 'small-world' networks. Nature 393(6684), 440–442 (1998)
38. Werner-Allen, G., Lorincz, K., Welsh, M., Marcillo, O., Johnson, J., Ruiz, M., Lees, J.: Deploying a wireless sensor network on an active volcano. IEEE Internet Computing 10(2), 18–25 (2006)
39. Xue, F., Kumar, P.R.: The number of neighbors needed for connectivity of wireless networks. Wirel. Netw. 10(2), 169–181 (2004)
40. Yuanyuan, Z., Medidi, M.: Sleep-based topology control for wakeup scheduling in wireless sensor networks. In: 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON 2007, June 2007, pp. 304–313 (2007)