Ad Hoc Networks 24 (2015) 186–199

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Bridge protection algorithms – A technique for fault-tolerance in sensor networks

Saad Ahmad Khan, Ladislau Bölöni *, Damla Turgut

Department of Electrical Engineering & Computer Sciences, University of Central Florida, 4000 University Blvd, Orlando, FL 32816, USA

ARTICLE INFO

Article history:
Received 13 February 2014
Received in revised form 8 July 2014
Accepted 28 August 2014
Available online 4 September 2014

Keywords:
Sensor network
Fault tolerance
Bridge protection

ABSTRACT

Sensor networks operating in the field might be subject to *catastrophic events* which destroy a large number of nodes in the geographic area. Often, the aftermath of such an event is the creation of a *network of bridged fragments* where connectivity is maintained by one or several bridge nodes. These networks are vulnerable, because the bridge nodes will soon exhaust their energy resources leading to the fragmentation of the network. This paper describes a *bridge protection algorithm* (BPA), a combination of techniques which, in response to a catastrophic event, change the behavior of a set of topologically important nodes in the network. These techniques protect the bridge node by letting some nodes take over some of the responsibilities of the sink. At the same time, they relieve some other overwhelmed nodes and prevent the apparition of additional bridge nodes. To achieve this, the algorithm sacrifices the length of some routes in order to distribute routes away from critical areas. In a variation on the BPA algorithm, we show that if geographic information about the nodes is available, replacing shortest path routing with a routing model which follows the edges of the relational neighborhood graph will lead to further improvements in the expected connected lifetime of the network.

1. Introduction

The nodes of a sensor network must be deployed in such a way that both the sensing and the communication requirements of the overall network are met. Sensor nodes can go off-line for a variety of reasons: running out of energy, environmental events (*e.g.* forest fire, landslides) as well as the activity of opposing forces (*e.g.* intruders disabling or compromising the sensor nodes which they detected through visual observation or radio-location). In such scenarios, naturally, the sensing quality suffers, as the off-line nodes do not contribute their sensing to the overall picture. The sensing quality loss is proportional with the number of off-line nodes.

The worst case scenario, however, happens when the loss of a single node can lead to the fragmentation of the network into disjoint subsets of nodes. This way, the loss of a single node can lead to a catastrophic loss of functionality, because even from areas where the sensors are intact, data cannot reach the sink. A well-engineered network will never fragment due to the energy consumption during the normal course of operation as the differences in the energy consumption can be taken into account during design time.

If, however, a natural or man-made catastrophic event destroys a large subset of the nodes, the remaining network can emerge with a heavily unbalanced topology which could not have been predicted at deployment time. Let us consider a situation where the connectivity still exists, but the network graph is split into several

* Corresponding author. Tel.: +1 407 823 2320; fax: +1 407 823 5835.
E-mail addresses: skhan@eecs.ucf.edu (S.A. Khan), lboloni@eecs.ucf.edu (L. Bölöni), turgut@eecs.ucf.edu (D. Turgut).

http://dx.doi.org/10.1016/j.adhoc.2014.08.016
1570-8705/

fragments, linked by *bridge nodes*. We define the bridge node as a node whose removal disconnects the network.[1] In contrast to nodes which have been engineered to handle a high load, bridge nodes are general purpose nodes which ended up in the bridge position due to unpredictable external circumstances. They do not have higher energy resources or longer transmission range, and yet they need to transport the complete traffic of the fragment on the opposite side from the sink.

In this paper we describe a series of techniques called bridge protection algorithms (BPAs). An early version of this technique has been presented in [1]. BPAs form a coherent response of the network to a catastrophic event which created a network topology of bridged fragments. The BPA changes the behavior of the bridge nodes and their neighbors in such a way as to lower the energy consumption of the bridge and to prevent future failures in the area which could create new bridge nodes.

The reminder of the paper is organized as follows. Section 2 describes the scenario we are considering, the performance metrics and the ways in which we can model catastrophic events. Section 3 describes the basic principles behind bridge protection algorithms, including the classification of specific nodes in the local area of a bridge node. Section 4 proposes a technique where geographical information about the nodes can be used to improve the efficiency of the BPA algorithm, by replacing shortest path routing with a routing in the network defined by the relational neighborhood graph. Section 5 describes the results of a simulation study comparing the performance of the BPA variants with the baseline response of a sensor network to a catastrophic event. Related work is discussed in Section 6. We conclude in Section 7.

2. Scenario: catastrophic events in an intruder tracking sensor network

2.1. The sensing task and the physical network

The scenario we are considering is that of an intruder detection system protecting an *area of interest* such as the surroundings of a high value military installation. In such a scenario the "smartdust" model where disposable nodes are deployed randomly (*e.g.* thrown out from airplanes) is not appropriate. Instead, the area is protected by a *permanently deployed wireless sensor network*, where sensor nodes costing hundreds or thousands of dollars each are deployed in carefully chosen locations. The nodes need to be in position for many years, requiring regular battery changes, with nodes expected to have larger energy consumption (for instance by being closer to the sink) being given batteries of larger capacity. In such a permanent sensor network, under normal conditions, we do not have the extreme energy limitations of the "smartdust" type of nodes. This, however, changes in the case of a catastrophic event when the bridge node needs to take on traffic many times larger than what it was designed for.

The ideal arrangement of nodes would be a rectangular or hexagonal regular grid. The density of the grid depends on the sensing and transmission range of the nodes. The sensing range determines how well the interest area will be covered by the sensors. We would prefer that every location to be covered, even by multiple nodes: but this is a *soft* preference: an intruder detection system can operate with partial coverage. The transmission range dependency, however, is hard: if a node cannot communicate with its neighbors, the system will not be operational. One reasonable compromise is to determine the grid size such that the node is within transmission range of all neighboring nodes, including along the diagonal, but it is not in the transmission range of nodes two hops away. In an ideal connection, this would imply that each node would have eight neighbors. Common sense engineering considerations dictate that arrangement to be chosen such that the transmission range of the nodes to be somewhat higher than the required minimum to maintain connectivity.

In practice, however, environmental conditions (*e.g.* the obstacles and camouflage opportunities in the environment) make the achievement of a perfect grid unfeasible. The customer would prefer to position the node to a location at some distance from the exact grid position, if this location offers advantages. In the resulting "grid with noise" arrangement of the nodes, some nodes might not reach all the near neighbors, but they might possibly reach one hop away neighbors. The main flow of information on the network is directed from the sensor nodes to the sink. The nodes detect intruders in their sensor range and send their observations with a hop-by-hop approach to the *sink node*, which has the ability to directly transmit the data to the customer.

Let us now discuss the nature of the routing algorithm used in a permanently deployed sensor network. In an intruder tracking system the overriding design requirement is that the information about intruders is transmitted as quickly as possible to the sink. This requires that the routing algorithm must converge to the shortest path in the number of hops. Note that this does not determine a unique routing algorithm – many routing algorithms used in wireless networks converge to this or closely related metrics. These include distributed techniques using variations of Bellman Ford (DSDV, OLSR and Babel), gradient based techniques such as directed diffusion, as well as centralized techniques where the neighborhood information is flooded until it reaches the sink, which calculates all the routes and transmits them back to the nodes. On-demand routing protocols such as AODV also choose shortest path, although on-demand routing does not offer advantages in a permanent sensor network. Different routing algorithms differentiate themselves in the way they handle changes in the network topology triggered by node failures or mobile nodes, as well as by the routing overhead, the cost of the signaling necessary to establish and modify the routes. However, for a sensor network with nodes deployed for years in the same position there is little to differentiate between proactive routing algorithms: the calculated routes will be the same and the cost of overhead will be

[1] Our usage of the term "bridge" differs slightly from the standard usage in graph theory. In graph theory a "bridge" is defined as an *edge* whose removal fragments the graph, while a node whose removal disconnects the graph is called a "cut-node".