A Self-Stabilizing Directed Diffusion Protocol for Sensor Networks

Doina Bein
School of Computer Science
University of Nevada, Las Vegas
siona@cs.unlv.edu

Ajoy K. Datta
School of Computer Science
University of Nevada, Las Vegas
datta@cs.unlv.edu

Abstract

We design a self-stabilizing communication protocol in a sensor network, based on the directed diffusion method [1]. A request for data from an initiator node is broadcast in the network, and the positive answers from the sensors are forwarded back to the initiator (following a Shortest-Path-Tree (SPT) construction rooted at the initiator.) The sensor nodes, starting from an arbitrary state and following our protocol, establish reliable communication in the network in a finite number of steps. Any number of initiators and any number of different requests at a time per initiator are allowed, but we limit the number of entries in the interest cache as the memory of a sensor node is limited.

1. Introduction

There are types of networks where the nodes are not identified by ID, but by the data they carried or by the their task they have to perform in the network. A sensor network is an example of such network. Sensing, data processing, and information communication are the basis of sensor networks ([2], [3]). For a large number of sensor nodes, they may not have any global identification (unique ID) because of the amount of overhead; in some cases, they may carry a global positioning system (GPS). Their positions are not predetermined, i.e. the network can start in an arbitrary topology. A sensor node is equipped with a processor, but has limited memory. As a result, it can carry out simple tasks and perform simple computations. The sensor nodes can communicate with each other unhindered within small distances, wireless, using radio, infrared, or optical media. Usually deployed for specific tasks (surveillance, reconnaissance, disaster relief operations, medical assistance, etc), they can reach a hostile environment, inaccessible terrain.

Both the sensors and the sensor network infrastructure are prone to failures, insufficient power supply, high error rate, disconnection, and little or no network support. Despite these, a sensor network should ensure a certain level of reliability, and a sensor node should ensure certain level of correctness and accuracy for the data collected and processed locally by the node. A sensor network should be able of self-organizing, and starting from an arbitrary state, to be able in real-time to achieve a correct information routing.

In this paper, we deal with the communication reliability of the network, and we present a self-stabilizing communication protocol. We do not address the reliability of the sensor node or the correctness of the data collected through the sensing unit.

The goal of this paper is to design a self-organizing sensor network, using a particular case of fault tolerance, called self-stabilization. Being self-stabilizing guarantees that the system will converge to the intended behavior in finite time, regardless of the system starting state (initial state of the sensor nodes and the initial messages on the links). Upon any request for data from a so-called *initiator*, in case the data is detected by some nodes, the possible answers are sent back to the initiator, on shortest paths (following a SPT construction rooted at the initiator). Then the initiator can send it to a higher level network (e.g. Internet, satellite, etc.) or application level. The system can also cope with topology changes as well.

1.1 Related Work

We use the directed diffusion protocol for disseminating and retrieving data through dynamically changing sensor networks. In directed diffusion, the nodes are not addressed by their IP addresses but by the data they generate. In order to be able to distinguish between neighbors, nodes have local unique IDs. Examples of such identifiers are 802.11 MAC addresses ([7]) and Bluetooth cluster addresses ([8]).

Many protocols and algorithms have been proposed for traditional wireless ad-hoc networks ([4, 5]), but they do not take into consideration frequent topology changes, sensors failures, and possible non-existent global IDs. A distributed self-configuring and self-healing algorithm for multi-hop wireless networks modeled as a honeycomb grid is proposed in [6].

The most general technique of designing a system to tolerate arbitrary transient faults is self-stabilization ([9]). A *self-stabilizing* system is guaranteed to converge to the intended behavior in finite time, regardless of the initial state of the nodes and the initial messages on the links ([10, 11]). In a distributed self-stabilizing directed diffusion protocol, with only local information and no initialization code, reliable communication is built in the network: requests for data are broadcast, analyzed, and when sensed, the answers are sent back through the shortest path toward the initiator, meanwhile taking care of topology changes as well.

In the directed diffusion protocol [1], a request for data from an initiator is broadcast in the network, and the positive answers from the sensors are forwarded back to the requester using a shortest path. For any node, an initiator is identified by a *gradient* field, which specifies the neighboring node through which the request has been received. An addition to the protocol in [1], we allow any number of initiators and any number of requests per initiator, but we restrict the number of entries in the interest cache to be at most K, as the memory in a sensor unit is limited. Another difference from [1] is that we save space and bandwidth by requiring only one gradient per entry, while in [1] there is a gradient for each neighbor (with multiple gradients for the same initiator, alternative paths may be considered, so duplicate data may be sent back to the initiator.)

If the gradient points to a broken link or non-existent neighbor, then considering only one gradient per entry has a disadvantage versus multiple gradients, when alternative paths exist. But this disadvantage is partially overcome by the fact that the initiator will re-broadcast its interest periodically. So in case the gradient points wrongfully, a new path will be found at least once the interest is re-broadcast by the initiator, if not earlier. The data collected and/or stored locally up to the moment may be lost only in case of a data entry rewriting. In that case, new data is collected and delivered back to the initiator.

Specific for sensor networks is the huge number of changes that can occur in the topology in a relative small interval of time. The self-stabilizing algorithms for SPT construction existent in the literature require a permanent communication using between neighboring nodes, that can drain out in short time the power of a sensor node. Our algorithm does not.

References

[1] Chalermek Intanagonwiwat, Ramesh Govindan, and Deborah Estrin. Directed diffusion: a scalable and robust communication paradigm for sensor networks. *Proceedings of the 6th annual international conference on Mobile computing and networking, Boston, Massachusetts, United States*, pages 56 – 67, 2000.

[2] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramanian, and Erdal Cayirci. A survey on sensor networks. *IEEE Communications Magazine August 2002*.

[3] G. Hoblos, M. Staroswiecki, and A. Aitouche. Optimal design of fault tolerant sensor networks. *IEEE International Conference Cont. Apps. Anchorage, AK*, pages 467–472, 2000.

[4] Piyush Gupta and P. R. Kumar. A system and traffic dependent adaptive routing algorithm for ad hoc networks. *Proceedings of the 36th IEEE Conference on Decision and Control*, pages 2375–2380, 1997.

[5] B. Dahill, B. N. Levine, E. Royer, and C. Shields. A secure routing protocol for ad-hoc networks. *Electrical Engineering and Computer Science, University of Michigan, Tech. Rep. UM-CS-2001-037, August 2001*.

[6] H. Zhang and A. Arora. GS^3: Scalable self-configuration and self-healing in wireless networks. In *21st ACM Symposium on Principles of Distributed Computing*, July 2002.

[7] IEEE Computer Society LAN MAN Standards Committee. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *Technical Report 802.11-1997, Institute of Electrical and Electronics Engineers New York, NY*, 1997.

[8] The Bluetooth Special Interest Group. Bluetooth v1.0b specification. *http://www.bluetooth.com*, 1999.

[9] E. W. Dijkstra. Self stabilizing systems in spite of distributed control. *Communications of the ACM*, 17:643–644, 1974.

[10] A. Arora and M. G. Gouda. Closure and convergence: a foundation of fault-tolerant computing. *IEEE Transactions on Software Engineering*, 19:1015–1027, 1993.

[11] M. G. Gouda. *Elements of network protocol design*. John Wiley & Sons, Inc., 1998.

[12] A. Bui, AK Datta, F Petit, and V Villain. Space optimal snap-stabilizing PIF in tree networks. *Proceedings of the Fourth Workshop on Self-Stabilizing Systems*, pages 78–85, 1999.

[13] A Cournier, AK Datta, F Petit, and V Villain. Snap-stabilizing PIF algorithm in arbitrary networks. In *IEEE 22nd International Conference on Distributed Computing Systems (ICDCS 02)*, pages 199–206. IEEE Computer Society Press, 2002.