A Benchmarking Algorithm for Maximum Bottleneck Node Trust Score-based Data Gathering Trees in Wireless Sensor Networks

Natarajan Meghanathan, Jackson State University, Flowood, MS, USA

ABSTRACT

The author proposes a benchmarking algorithm to determine maximum bottleneck node trust score-based data gathering trees (MaxBNT-DG trees) for wireless sensor networks (WSNs) wherein the bottleneck node trust score of a path (minimum trust score for any node on the path, including those of the end nodes) from any node to the root node of the DG tree is the maximum. He compares the performance of the MaxBNT-DG trees with that of the maximum bottleneck link weight-based data gathering trees (MaxBLT-DG trees) for which the bottleneck link trust score (minimum trust score for constituent links) of a path from any node to the root node is the maximum. The author observes the MaxBNT-DG trees to incur a smaller tree diameter, a larger percentage of nodes as leaf nodes and a larger trust score per intermediate node; whereas, the MaxBLT-DG trees incur a lower aggregation delay, indicating a trust-aggregation delay tradeoff in WSNs. The MaxBNT-DG algorithm is also generic and can be extended to any other node criterion like residual energy, wake-up frequency, etc.

Keywords: Aggregation Delay, Benchmarking Algorithm, Data Gathering Tree, Maximum Bottleneck Link Weight, Maximum Bottleneck Node Weight, Simulations, Trust Score, Wireless Sensor Networks

1. INTRODUCTION

A Wireless Sensor Network (WSN) is a network of autonomous sensor nodes that can typically sense/measure one or more environmental parameters of interest such as pressure, temperature, humidity, etc and forward the sensed data to a control center called the sink. The sensor nodes are battery charged and operate at a limited transmission range to conserve energy as well as to reduce interference occurring due to simultaneous transmissions across the shared wireless medium. It would consume a significant amount of energy in the network if each of the sensor nodes attempt to directly transmit their data to the sink, leading to premature node failures.

DOI: 10.4018/IJITN.2015070102
Hence, sensor nodes typically forward their data along a specialized communication topology, like cluster (Heinzelman et. al., 2000), grid (Meghanathan, 2010a; Luo et. al., 2005), chain (Lindsey et. al., 2002), tree (Meghanathan, 2012), connected dominating set (Meghanathan, 2010b), etc and data (from the various nodes) gets aggregated as it propagates through this topology. Several articles have been published (e.g., Meghanathan, 2012) comparing the performance of these different communication topologies for data gathering. Most of the work available in the literature focus on determining communication topologies that minimize the energy consumption at the sensor nodes and prolong the network lifetime (typically, defined as the time the network gets disconnected due to the failure of one or more nodes that run out of energy). In this paper, we focus on data gathering trees (DG trees). Lindsey et. al (2001), Dietrich & Dressler (2009) and Meghanathan (2012) have observed DG trees to be the most energy-efficient among these topologies. The links of the DG trees typically span over a shorter distance and the number of links involved in the transmission and reception of data are to the bare minimum, but still span across all the nodes.

In data gathering applications, the accuracy of the data being aggregated is of significant importance. Wireless links are prone to corruption due to channel interference, deterioration of the signal with distance, security attacks and etc. As a result, a message transmitted may not be received as it was sent from the sender side. A rooted data gathering tree comprises of intermediate nodes and leaf nodes at various levels (distance from the root node). If an intermediate node has one or more incident links in the DG tree that are prone to corruption, then the aggregated data received and processed by the intermediate node and transmitted further upstream towards the root node is likely to be corrupted. Hence, it is imperative that we construct DG trees in which the intermediate nodes are more reliable and let the relatively less reliable nodes to serve as leaf nodes. Most of the focus in the literature is on using appropriate measures (e.g., Zhan et. al., 2011; Xiang et. al., 2012; Uma Rani & Soma Sundaram, 2014) to evaluate the reliability of a link or the node and use these to decide whether or not to forward data received on a link or from a node.

We define the trust score for a link as the probability that data transmitted on the link is received without any corruption. We define the trust score for a node as the sum of the trust scores of the links incident on it. We define the bottleneck node trust score for a path as the minimum of the trust scores of the constituent nodes of the path (including those of the end nodes). Similarly, we define the bottleneck link trust score for a path as the minimum of the trust scores of the constituent links of the path. Our contribution in this paper is as follows: We propose a benchmarking algorithm to determine maximum bottleneck node trust score-based data gathering tree (MaxBNT-DG tree) for wireless sensor networks such that the bottleneck node trust score of the path from any node to the root node of the DG tree is the maximum. We prove the theoretical correctness of the algorithm as well as evaluate its effectiveness through extensive simulations.

Simulation results vindicate our hypothesis that the average trust score per intermediate node in a MaxBNT-DG tree is larger than the average trust score per leaf node (thus, more reliable nodes are likely to serve as intermediate nodes of the MaxBNT-DG tree). We also compare the performance of the MaxBNT-DG trees with that of the maximum bottleneck link trust score-based data gathering trees (MaxBLT-DG trees) for which the bottleneck link trust score (minimum trust score of the constituent links) of the path from any node to the root node of the DG tree is the maximum. We observe the MaxBNT-DG trees to incur a smaller diameter (i.e., tree height; preferable for real-time reporting of data from an individual node to the root node), a larger value for the average trust score per intermediate node (preferable for reliable data gathering) and a larger percentage of nodes as leaf nodes (preferable for maximum network lifetime; Meghanathan, 2010c). On the other hand, we observe the MaxBLT-DG trees to incur a
Cyclostationary Spectrum Sensing in Cognitive Radios at Low SNR Regimes
www.igi-global.com/chapter/cyclostationary-spectrum-sensing-in-cognitive-radios-at-low-snr-regimes/123563?camid=4v1a

Cross-Layer Framework for Power Conservation in Wireless Ad Hoc Networks: A Case Study
www.igi-global.com/chapter/cross-layer-framework-power-conservation/65672?camid=4v1a

The Internet's Impact on the Law and Economics Of the US's Motion Picture Industry
www.igi-global.com/chapter/internet-impact-law-economics-motion/20462?camid=4v1a