Journal of Network and Computer Applications 57 (2015) 85–101

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Fault resilience in sensor networks: Distributed node-disjoint multi-path multi-sink forwarding

Suchetana Chakraborty[a], Sandip Chakraborty[b,*], Sukumar Nandi[c], Sushanta Karmakar[c]

[a] Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani Hyderabad Campus, Hyderabad, Andhra Pradesh 500 078, India
[b] Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, Kharagpur, West Bengal 721322, India
[c] Department of Computer Science and Engineering, Indian Institute of Technology Guwahati, Guwahati, Assam 781039, India

ARTICLE INFO

Article history:
Received 3 February 2015
Received in revised form
1 July 2015
Accepted 22 July 2015
Available online 1 August 2015

Keywords:
Data gathering
Mission critical sensor network
Reliability
Redundancy

ABSTRACT

Sensor network deployed for the critical infrastructure monitoring requires high degree of reliability in sensory data gathering, in spite of arbitrary node or sink failures. This paper proposes a robust data gathering scheme specially designed to provide guaranteed delivery of the sensory data for applications on the critical infrastructure monitoring. Redundancy in a sensor network, in terms of both the number of deployed sensors and the amount of duplicate data delivery, is explored to design an effective protocol that ensures the reliable data delivery while assuring the timeliness, connectivity and the sensing coverage. A set of active sensors is selected from all the sensors deployed, based on the network connectivity and the sensing coverage criteria that participates in the data forwarding process. Rest of the sensors go to the sleep state, and act as a replacement on the failure of an active sensor. The proposed protocol aims to find out multiple node-disjoint paths to multiple sinks, so that the loss of connectivity in one path due to node failure does not disrupt application services. The effectiveness of the proposed scheme has been analyzed using simulation results, and compared with other protocols proposed in the literature for reliable data delivery.

1. Introduction

Critical Infrastructure (CI) like power generation and distribution centers, nuclear power plants, water supply plants, hospitals, banks, bridges, international border areas and transportation systems are the indispensable assets for the socio-economical foundation of any country. The increasing threats of catastrophe or invasion on the security of the CI demand a robust and stable monitoring system to be developed. Wireless sensor network has emerged to contribute to the imperative protection of the large-scale CI by providing flexible, cost-effective and automated solutions to achieve smooth services (Roman et al., 2007). A large number of low-cost micro-electronic sensors are deployed along the boundary of any target CI to sense different physical parameters like temperature, pressure, speed and light according to various application requirements. The deployed sensors assure the k-barrier coverage such that the movement of any object across the CI boundary is detected by at least k sensors, and the corresponding alert can be raised for taking necessary actions. The sensors form an interconnected information system such that the sensory data is forwarded to the base station or gateway through a set of intermediate sinks for statistical analysis.

Tree based data gathering (Hariharan and Shroff, 2011; Younis et al., 2014) is widely used in sensor networks because of its efficiency in the data collection with minimum contention and forwarding delay. Sensor nodes form a tree rooted at the sink, where the data is aggregated at the intermediate nodes based on the application requirement, before being forwarded to the parent. The store and forward policy is used for ensuring the reliability in the tree based data forwarding (Naderi and Mazinani, 2012), where every data packet is stored in the interface buffer, and then retransmitted in the case of transmission failure (due to either node failure or intermediate packet loss). This method is inefficient for applications that cannot tolerate the repairing and retransmission delay. Data forwarding through multiple node-disjoint paths (Radi et al., 2012; Xu et al., 2012; Felemban et al., 2006; Challal et al., 2011) is an alternative option for the delay-bounded applications to assure the reliability in spite of node or link failure. Finding multiple node-disjoint paths towards a single sink is difficult due to the inherent randomness in sensor deployment. However, multiple node-disjoint paths towards different sinks are easier to compute, because the paths are sparsely located in different directions. Further, multiple paths towards different

[*] Corresponding author.
E-mail addresses: suchetana@iitg.ernet.in (S. Chakraborty), sandipc@cse.iitkgp.ernet.in (S. Chakraborty), sukumar@iitg.ernet.in (S. Nandi), sushantak@iitg.ernet.in (S. Karmakar).

http://dx.doi.org/10.1016/j.jnca.2015.07.014
1084-8045/© 2015 Elsevier Ltd. All rights reserved.

sinks provide the support for reliability during potential sink failure. With this approach, reliable data delivery is guaranteed in spite of a node or sink failure, without any repairing or retransmission delay (which is more than twice the forwarding time because of multiple message transmission for path repairing).

Considering potential vulnerability towards the protection of the CI and the failure prone nature of sensor nodes, the inherent design challenge is to ensure the reliable delivery of the sensory data to the base station even in presence of arbitrary node failure. Sensor nodes may fail due to power outage, technical fault or tampering. Although sinks are considered to be more resource advantageous compared to sensors, they may also fail as a result of tampering. Therefore, the overall network lifetime, in terms of the connectivity and the sensing coverage, is reduced in absence of the data gathering tree maintenance from a series of node failures. On failure of a set of nodes, reconstruction of data gathering trees starting from the scratch is not a good option, as it incurs large overhead. Also, the failure of one or multiple sensors or sinks may create sensing and/or communication holes into the network, introducing threats for potential attacks and disrupting application services. Even if the data is forwarded through multiple paths towards multiple sinks, the re-establishment of the affected path due to a node failure is necessary. Sensor deployment with high redundancy can extend the network lifetime by supporting node failures, as the failed node is replaced by a suitable redundant node, such that the required network connectivity and the sensing coverage are maintained throughout. The redundancy based tree maintenance scheme is efficient, as it offers an improved network lifetime with uninterrupted application services at a nominal cost of local path repairing.

This paper proposes a framework and working principles of the reliable data gathering protocol, *RelBAS* ("Reliable Data Gathering from Border Area Sensors" as introduced in Chakraborty et al., 2013) for the critical infrastructure monitoring. The primary design objective of *RelBAS* demands the reliable delivery of the sensory data to the base station in spite of node or sink failures, such that every potential intrusion can be detected without any delay in reporting. *RelBAS* uses a multi-sink data gathering approach that is different from the conventional multicast. Multiple data gathering trees rooted at each of the multiple sinks are constructed, such that from every sensor node, there exist multiple node-disjoint paths to multiple sinks. The proposed protocol selects active set of sensors that participate in data sensing and forwarding activities, such that the *k*-barrier coverage is maintained along the boundary of the target CI. During the tree construction at every sensor node, for a particular sink, the best forwarding path is selected among all possible options based on the hop-count distance to the sink and the node's residual energy. This offers minimum delay in data forwarding while ensuring the energy efficiency. *RelBAS* deals with single node failure by designing a local tree-repairing scheme through a suitable redundant node selection for replacing the failed node, while maintaining the connectivity and the sensing coverage. It also supports the identification of an affected zone due to multiple node failures. The properties of the proposed protocol is analyzed as well as the performance is compared with other existing protocols proposed in the literature.

The rest of the paper is organized as follows. Section 2 gives a brief discussion on existing works in the literature related to this work. The system model and network architecture along with an overview of the proposed *RelBAS* protocol are provided in Section 3. The description of the *RelBAS* protocol has been presented in three phases. The initialization phase includes the scheme of active node selection maintaining the *k*-barrier coverage, as provided in Section 4. Section 5 describes the second phase of *RelBAS*, that focuses on the data gathering tree construction rooted at multiple sinks. Next section discusses the last phase of *RelBAS* for handling a single node failure and identifying an affected zone due to the failure of multiple nodes in close vicinity. A theoretical analysis to show the effect of *sink-connectivity* over the reliability has been provided in Section 7. The performance of *RelBAS* has been compared with existing schemes in the literature, those support reliability in data forwarding, by analysis of the simulation results, as presented in Section 8. Finally, Section 9 concludes the paper.

2. Related works

Wireless sensor network has emerged to contribute to the imperative protection of the large-scale CI by providing flexible, cost-effective and automated solutions to achieve smooth services (Roman et al., 2007). Most of the existing works in the literature, that have addressed the design challenges of CI monitoring system, such as (Kim et al., 2007) and the references therein, have focused mainly on the hardware aspects of sensor nodes. The characteristics and design goals of efficient data gathering protocols for sensor network are well-studied in the literature, such as (Kalpakis, 2010; Choi et al., 2012; Huang et al., 2012; Zungeru et al., 2012; Younis et al., 2014) and the references therein. These protocols mainly aim at finding the forwarding paths with minimum number of sensors involved, along with the possibility of in-network data aggregation. This reduces the average energy dissipation in the network, which results in an improved network lifetime. These protocols assure neither the reliability in data gathering, nor the sensing coverage and the network connectivity criteria during the node failures. A set of notable works in the literature (Kamal et al., 2013; Campobello et al., 2012; Troya and Vallecillo, 2012; Aksu et al., 2012; Lee et al., 2015; Bhuiyan et al., 2015; Bagci et al., 2015) have focused on the problem of reliable data delivery through the classical single path forwarding technique. There are three basic approaches to provide the reliability over the traditional single path forwarding. The first approach is to derive the statistical correlation among the sensory data to aggregate them, so that the network load is reduced. A reduction in network load can also reduce the data losses due to the network contention and congestion. The second approach is to forward data through the most reliable links. The third approach is to use the packet retransmission policy to improve the reliability. All these schemes are not efficient as the maximum reliability bound depends on the path loss rate. Further, the timeliness in data delivery is important for such applications, and therefore, the retransmission based approaches are not suitable too. A robust gradient based data delivery protocol, as proposed in Ye et al. (2005) uses the concept of traditional single-sink data forwarding mechanism. The protocol builds and maintains a cost field for providing each sensor the direction to which the sensing data needs to be forwarded by propagating advertisement packets in the network. The authors have shown that the protocol can deliver data with high degree of reliability in spite of multiple node failures that are not within close proximity. Due to the localization of node failures based on energy exhaustion the affected path is unable to provide the required reliability to the delivery of sensory data to the base station.

In Yang et al. (2010), Liaskovitis and Schurgers (2010), Moro and Monti (2012), Cărbunar et al. (2006), Challal et al. (2011), Deru et al. (2014), Costa et al. (2014) and the references therein, the authors have explored the advantages of redundancy, both in terms of the deployed redundant sensors and the redundant data delivery to satisfy the reliability and the sensing coverage. In Ganesan et al. (2001), the authors have proposed to use multi-path data delivery in sensor network to improve the reliability in data