Chapter 28
An Optimal Routing Algorithm for Internet of Things Enabling Technologies

Amol V. Dhumane
Pune University, India

Rajesh S. Prasad
NBN Sinhgad School of Engineering, India

Jayashree R. Prasad
Sinhgad College of Engineering, India

ABSTRACT

In Internet of things and its relevant technologies the routing of data plays one of the major roles. In this paper, a routing algorithm is presented for the networks consisting of smart objects, so that the Internet of Things and its enabling technologies can provide high reliability while the transmitting the data. The proposed technique executes in two stages. In first stage, the sensor nodes are clustered and an optimal cluster head is selected by using k-means clustering algorithm. The clustering is performed based on energy of sensor nodes. Then the energy cost of the cluster head and the trust level of the sensor nodes are determined. At second stage, an optimal path will be selected by using the Genetic Algorithm (GA). The genetic algorithm is based on the energy cost at cluster head, trust level at sensor nodes and path length. The resultant optimal path provides high reliability, better speed and more lifetimes.

INTRODUCTION

Kavin Ashton in 2009 proposed the term “Internet of Things”. According to him “The Internet of Things has the potential to change the world, just as the Internet did. May be even more so”. Future Internet aims to incorporate heterogeneous communication technologies, both wired and wireless, so as to contribute considerably to declare the idea of Internet of Things (IoT) (Kortuem, Kawsar, Fitton et al., 2010). Albeit there are numerous approaches to depict an Internet of Thing, which can characterize it as a worldwide

DOI: 10.4018/978-1-5225-9866-4.ch028

network of uniquely addressable interconnected objects, based on standard communication protocols. The low cost of sensor technology has eased the proliferation of Wireless Sensor Networks (WSNs) in numerous applicative scenarios such as home and office automation, environmental monitoring, agriculture, healthcare, and smart buildings. Internet of things networks are described by high heterogeneity because they are consistent with distinctive proprietary and non-proprietary solutions. Interoperability among heterogeneous sensing systems and abstraction between low layers (i.e. hardware) and high layers (i.e. user applications) are thus very vital difficulties (Zorzi, Gluhak, Lange et al., 2010).

Sensor networks based on closed or proprietary systems are integration islands with constrained communication to the outside world. There generally is the need to utilize gateways with application particular knowledge to export WSN data to other devices connected to the Internet. In addition, there is no direct communication between different standards unless complex application-specific conversions are implemented in gateways or proxies. The current trend is to utilize the Internet Protocol (IP) to attain native connectivity between wireless sensor network and the Internet (Vasseur and Dunkels, 2010). Along these lines, smart objects (e.g., tiny sensors or actuators with a network interface) are interconnected in order to make an IoT, based mainly on open standards and where every device has its own IP address. The IoT will permit gathering any helpful information about the physical world using the smart objects for utilizing it in various applications during the objects' life cycle. The web enablement of these smart objects will conveys more flexibility and customization possibilities for the Future Internet. For instance, following the trend of Web mashups (Zang, Rosson and Nasser, 2008), end users can create applications mixing real-world devices such as home appliances with virtual services on the Web. This sort of utilizations is frequently alluded to as physical mashups (Kovatsch, Weiss and Guinard, 2010).

The prominent enabling technologies of IoT such as WSN provide capabilities that are valuable for continuous remote monitoring, as research into military and environmental systems attest (Younis et al, 2002; Wood et al, 2008). One aspect of sensor networks that complicates the design of a secure routing protocol is in-network aggregation (Karlof and Wagner, 2003). Transmission of video and imaging data requires both energy and QoS aware routing in order to ensure efficient usage of the sensors and effective access to the gathered measurements (Akkaya and Younis, 2003). A method for estimating unknown node positions in a sensor network based exclusively on connectivity-induced constraints is described. Known peer-to-peer communication in the network is modeled as a set of geometric constraints on the node positions. The global solution of a feasibility problem for these constraints yields estimates for the unknown positions of the nodes in the network (Doherty, Pister & El Ghaoui, 2001). Routing protocols have two modes: greedy mode (when the forwarding node is able to advance the message toward the destination) and recovery mode (applied until return to greedy mode is possible) (Stojmenovic, 2002).

Recent advances in wireless sensor networks have led to many new protocols specifically designed for sensor networks where energy awareness is an essential consideration. Most of the attention, however, has been given to the routing protocols since they might differ depending on the application and network architecture (Akkaya and Younis, 2005). Micro sensor networks can contain hundreds or thousands of sensing nodes. It is desirable to make these nodes as cheap and energy-efficient as possible and rely on their large numbers to obtain high quality results (Heinzelman, Chandrakasan and Balakrishnan, 2000). In contrast with IP-based communication networks based on global addresses and routing metrics of hop counts, sensor nodes normally lack global addresses (Chen, Kwon and Choi, 2005). The major challenge in designing wireless sensor network is the support of the functional, such as data latency, and the non-functional, such as data integrity, requirements while coping with the computation, energy and communication constraints (Younis and Akkaya, 2008).