



Proactive Source Routing (PSR) In Shortcut Tree For Wireless Networks

S. Shabnam¹, T.Mohanraj²

III M.E., Dept of CSE, Karpagam University, Coimbatore, India¹

Assistant Professor, Dept of CSE, Karpagam University, Coimbatore, India²

ABSTRACT: The main idea of the shortcut tree routing is to calculate remaining hops from an arbitrary source to the destination using the hierarchical addressing scheme in ZigBee, and each source or intermediate node forwards a packet to the neighbor node with the smallest remaining hops in its neighbor table. The shortcut tree routing is fully distributed and compatible with ZigBee standard in that it only utilizes addressing scheme and neighbor table without any changes of the specification. The shortcut tree routing (STR) protocol provides the near optimal routing path as well as maintains the advantages of the ZigBee tree routing such as low memory consumption. There is a chance for high delay and low delivery ratio. In this paper, we propose a lightweight proactive source routing (PSR) protocol that can maintain more network topology information than distance vector (DV) routing to facilitate source routing. It increases the delivery ratio and reduce the delay. Tests using computer simulation in Network Simulator 2 (ns-2) indicate that the delay in PSR is only a fraction of the delay of STR protocols, and PSR yields better data transportation performance than the STR protocol.

KEYWORDS: Zigbee, WSN, PSR

I. INTRODUCTION

The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. A wireless sensor network (WSN) is increasingly being envisioned for collecting data, such as physical or environmental properties, from a geographical region of interest. WSNs are composed of a large number of low cost sensor nodes, which are powered by portable power sources, e.g. batteries.

In many surveillance applications of WSNs, tracking a mobile target (e.g., a human being or a vehicle) is one of the main objectives. Unlike detection that studies discrete detection events a target tracking system is often required to ensure continuous monitoring, i.e., there always exist nodes that can detect the target along its trajectory (e.g., with low detection delay or high coverage level). Since nodes often run on batteries that are generally difficult to be recharged once deployed, energy efficiency is a critical feature of WSNs for the purpose of extending the network lifetime. However, if energy efficiency is enhanced, the quality of service (QoS) of target tracking is highly likely to be negatively influenced. For example, forcing nodes to sleep may result in missing the passing target and lowering the tracking coverage. Therefore, energy efficient target tracking should improve the trade off between energy efficiency



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

and tracking performance e.g., by improving energy efficiency at the expense of a relatively small loss on tracking performance.

As a compensation for tracking performance loss caused by duty cycling and sleep scheduling, proactive wake-up has been studied for awakening nodes proactively to prepare for the approaching target. However, most existing efforts about proactive wake-up simply awaken all the neighbor nodes in the area, where the target is expected to arrive, without any differentiation. In fact, it is sometimes unnecessary to awaken all the neighbor nodes. To sleep-schedule nodes precisely, so as to reduce the energy consumption for proactive wake-up. For example, if nodes know the exact route of a target, it will be sufficient to awaken those nodes that cover the route during the time when the target is expected to traverse their sensing areas.

II. RELATED WORK

In [1] author presented applications in the areas of home automation, building automation, and utility meter reading represent the bulk of the deployed wireless sensor network devices. The current deployments are largely wireless adaptations of existing applications. The initial impetus for the use of wireless technology was access to retrofit markets and lower installation costs compared to traditional wired systems. Increasingly, commercial users of wireless sensor networks are taking advantage of the technology to provide services and features that were impossible or cost prohibitive in the past. Predictive maintenance of HVAC and lighting systems and advanced energy management through utility meters are good examples of this trend. [2] The ubiquitous home network has gained widespread attentions due to its seamless integration into everyday life. This innovative system transparently unifies various home appliances, smart sensors and energy technologies. The smart energy market requires two types of ZigBee networks for device control and energy management. Authors present the design of a multi-sensing, heating and air conditioning system and actuation application the home users: a sensor network-based smart light control system for smart home and energy control production. Authors designs smart home device descriptions and standard practices for demand response and load management “Smart Energy” applications needed in a smart energy based residential or light commercial environment. In [3] authors develop practical ZigBee deployment guideline under the interference of WLAN. We identify the “Safe Distance” and “Safe Offset Frequency” using a comprehensive approach including theoretical analysis, software simulation, and empirical measurement. In addition, they proposed a frequency agility-based interference avoidance algorithm.

The proposed algorithm can detect interference and adaptively switch nodes to “safe” channel to dynamically avoid WLAN interference with small latency and small energy consumption. The proposed scheme is implemented with a Meshnetics ZigBit Development Kit and its performance is empirically evaluated in terms of the packet error rate (PER) using a ZigBee and Wi-Fi coexistence test bed. It is shown that the empirical results agree with the analytical results. In [4] Authors present a reliable transmission protocol based on any cast routing for wireless patient monitoring. The scheme automatically selects the closest data receiver in an any fast group as a destination to reduce the transmission latency as well as the control overhead. The new protocol also shortens the latency of path recovery by initiating route recovery from the intermediate routers of the original path. On the basis of a reliable transmission scheme, they implement a ZigBee device for fall monitoring, which integrates fall detection, indoor positioning, and ECG monitoring. When the triaxial accelerometer of the device detects a fall, the current position of the patient is transmitted to an emergency center through a ZigBee network. [5] highlight the problem that the recent spatial correlation models of sensor nodes’ data are not appropriate for measuring the correlation in a complex environment. In addition, the representative data are inaccurate when compared with real data. Thus, we propose the data density correlation degree, which is necessary to resolve this problem. The proposed correlation degree is a spatial correlation measurement that measures the correlation between a sensor node’s data and its neighboring sensor nodes’ data. Based on this correlation degree, a data density correlation degree (DDCD) clustering method is presented in detail so that the representative data have a low distortion on their correlated data in a WSN. Moreover, the shape of clusters obtained by DDCD clustering method can be ad Smart grid is an intelligent power generation, distribution and control system. ZigBee, as a wireless mesh networking scheme low in cost, power, data rate, and complexity, is ideal for smart grid applications, e.g., real-time system monitoring, load control, and building automation. Unfortunately, almost all ZigBee channels overlap with wireless local area network(WLAN) channels, resulting in severe performance degradation due to interference.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

III. PROPOSED TECHNIQUES

A. Description of the Proposed Techniques:

DESIGN OF PROACTIVE SOURCE ROUTING

Essentially, PSR provides every node with a breadth-first spanning tree (BFST) of the entire network rooted at itself. To do that, nodes periodically broadcast the tree structure to their best knowledge in each iteration. Based on the information collected from neighbors during the most recent iteration, a node can expand and refresh its knowledge about the network topology by constructing a deeper and more recent BFST. This knowledge will be distributed to its neighbors in the next round of operation. On the other hand, when a neighbor is deemed lost, a procedure is triggered to remove its relevant information from the topology repository maintained by the detecting node. Intuitively, PSR has about the same communication overhead as DV-based protocols. We go an extra mile to reduce the communication overhead incurred by PSR's routing agents. Details about this overhead reduction will be discussed in Section III-C. Before describing the details of PSR, we will first review some graph-theoretic terms used here. Let us model the network as undirected graph $G = (V, E)$, where V is the set of nodes (or vertices) in the network, and E is the set of wireless links (or edges). Two nodes u and v are connected by edge $e = (u, v) \in E$ if they are close to each other and can directly communicate with given reliability. Given node v , we use $N(v)$ to denote its open neighborhood, i.e., $\{u \in V \mid (u, v) \in E\}$. Similarly, we use $N[v]$ to denote its closed neighborhood, i.e., $N(v) \cup \{v\}$ (see [14] for other graph-theoretic notions).

A. Route Update

Due to its proactive nature, the update operation of PSR is iterative and distributed among all nodes in the network. At the beginning, node v is only aware of the existence of itself; therefore, there is only a single node in its BFST, which is root node v . By exchanging the BFSTs with the neighbors, it is able to construct a BFST within $N[v]$, i.e., the star graph centered at v , which is denoted S_v .

$$G_v = S_v \cup (T_u - v).$$

B. Neighborhood Trimming

The periodically broadcast routing messages in PSR also double as "hello" messages for a node to identify which other contribution to the network connectivity should be removed; this process is called neighbor trimming. Consider node v . The neighbor trimming procedure is triggered at v about neighbor u either by the following cases:

- 1) No routing update or data packet has been received from this neighbor for a given period of time.
- 2) A data transmission to node u has failed, as reported by the link layer.

C. Streamlined Differential Update

In addition to dubbing route updates as hello messages in PSR, we interleave the "full dump" routing messages, as stated previously, with "differential updates." The basic idea is to send the full update messages less frequently than shorter messages containing the difference between the current and previous knowledge of a node's routing module. Both the benefit of this approach and balancing between these two types of messages have been extensively studied in earlier proactive routing protocols. In this paper, we further streamline the routing update in two new avenues. First, we use a compact tree representation in full-dump and differential update messages to halve the size of these messages. Second, every node attempts to maintain an updated BFST as the network changes so that the differential update messages are even shorter.

IV. SIMULATION RESULTS

The simulation analysis for PSR is implemented using Network Simulator NS2. The simulation is done for Delivery ratio, Final delay whose results are shown in Figure 1 & 2 respectively.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

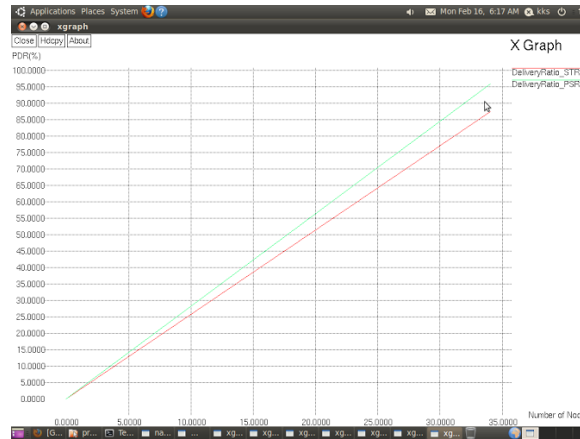


Figure 1 : Delivery ratio

The above figure shows that the delivery ratio of PSR is better than STR

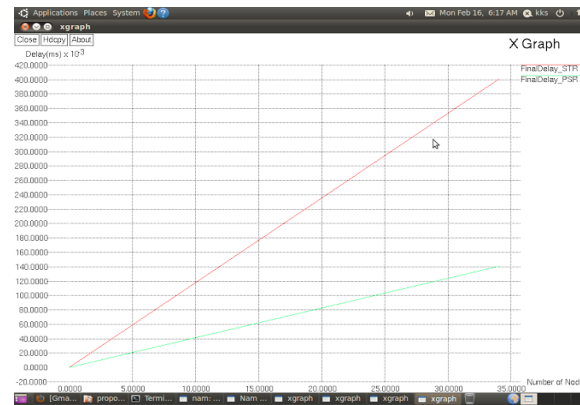


Figure 2 : Final delay

The above figure shows that the final delay of PSR is lower than STR

V. CONCLUSION AND FUTURE WORK

PSR protocol should provide more topology information than DVs and STR But It has significantly reduces the delay and increases the delivery ratio than other routing protocols. Plan to do enhancement of PSR. This paper has been motivated by the need to support opportunistic data forwarding in MANETs. To generalize the milestone work of ExOR for it to function in such networks, we needed a PSR protocol. Such a protocol should provide more topology information than DVs but must have significantly smaller overhead than LS routing protocols; even the MPR technique in OLSR would not suffice. Thus, we put forward a tree-based routing protocol, i.e., PSR, which is inspired by the PFA and the WRP. First, it uses only one type of message, i.e., the periodic route update, both to exchange routing information and as hello beacon messages. Second, rather than packaging a set of discrete tree edges in the routing messages, we package a converted binary tree to reduce the size of the payload by about a half. Third, we interleave full-dump messages with differential updates so that, in relatively stable networks, the differential updates are much shorter than the full-dump messages. To further reduce the size of the differential updates, when a node maintains its routing tree as the network changes, it tries to minimize alteration of the tree. As a result, the routing delay of PSR is only a fraction or less compared with DSDV, OLSR, and DSR, as evidenced by our experiments. Yet, it still has similar or better performance in transporting TCP and UDP data flows in mobile networks of different velocity rates and densities.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

REFERENCES

1. J. Liu et al., "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network," Int'l J. Information Security, vol. 9, no. 4, pp. 287-296, 2010.
2. Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006
3. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660- 670, Oct. 2002.
4. A. Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," IEEE Trans. Parallel & Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.
5. J. Sun et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel & Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.
6. S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," Proc. Advances in Cryptology (CRYPTO), pp. 263-275, 1990.
7. A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/ 15, pp. 2826-2841, 2007.
8. Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Mohsen Guizani, Fellow, Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 3, MARCH 2014
9. Eugene Y. Vasserman, Nicholas Hopper, " Vampire Attacks: Draining Life from Wireless Sensor Networks", IEEE transactions on mobile computing, VOL. 12, NO. 2, February 2013.
10. Farzana T, Mrs. Aswathy Babu A light weight PLGP based method for mitigating vampire attacks in Wireless Sensor Networks Volume 03 Issue 07 July,