Volume : 2 | Issue : 1 | January 2013 ISSN - 2250-1991

Research Paper Computer Science

A Study of Optical Routing Protocols for Wireless Sensor Networks

* Mr. Vishal Rajput ** Mr Digvijay Virpura
*** Dr. Nilesh K. Modi

* Assistant Professor, Narmada College of Computer Application, MCA Department, Bharuch, India

** Assistant Professor, N.V Patel College College of pure & Applied Sciences, M.Sc.IT Department, Anand, India

*** Professor& Head, SVICS, MCA Department, Kadi, India

ABSTRACT

Wireless sensors nodes are made up of small electronic devices which are capable of sensing, computing and transmitting data from harsh physical environments like a surveillance field. These sensor nodes majorly depend on batteries for energy, which get depleted at a faster rate because of the computation and communication operations they have to perform. Communication protocols can be designed to make efficient utilization of energy resources of a sensor node and to obtain real time functionality.Recent advances in wireless sensor networks have led to many new protocols specifically designed for sensor net- works 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. This paper surveys recent routing protocols for sensor networks and presents a classification for the various approaches pursued. The three main categories explored in this paper are data-centric, hierarchical and location-based. Each routing protocol is de-scribed and discussed under the appropriate category. Moreover, protocols using contemporary methodologies such as network flow and quality of service modeling are also discussed. The paper concludes with open research issues.

Keywords: Sensor networks; Energy-aware routing; Routing protocols; Classification of protocols

1. Introduction

Advances in wireless communication made it possible to develop wireless sensor networks (WSN) consisting of small devices, which collect information by cooperating with each other. These small sensing devices are called nodes and consist of CPU (for data processing), memory (for data storage), battery (for energy) and transceiver (for receiving and sending signals or data from one node to another). The size of each sensor node varies with applications. For example, in some military or surveillance applications it might be microscopically small. Its cost depends on its parameters like memory size, processing speed and battery.

Today, wireless sensor networks are widely used in the commercial and industrial areas such as for e.g. environmental monitoring, habitat monitoring, healthcare, process monitoring and surveillance. For example, in a military area, we can use wireless sensor networks to monitor an activity. If an event is triggered, these sensor nodes sense it and send the information to the base station (called sink) by communicating with other nodes.

Recent advances in optical networking expose that large-scale optical network supporting heterogeneous traffic may soon become economical as the underlying backbone in wide area networks, in which optical routers playing a key role. One big challenge in designing future large-scale optical systems is packet scheduling for the core optical router. The optical router is a delay system with packets waiting at its access queues. A scheduler is necessary to allocate resources so that delay and anxiety sensitive real-time traffic can be served with higher priority than the non-delay sensitive traffic. The system capacity should also be efficiently utilized. This is achieved by a prioritized non-blocking scalable scheduling algorithm developed in this paper. The proposed algorithm is based on a heuristic approximation of a Linear Integer Programming model. The performance evaluations in a multi-service high capacity core optical router show that the heuristic solution is close to the optimal solution most of the time, yet it is much easier to implement. In this study, therefore we are proposing optical routing algorithm for wireless adhoc networks.

2. Wireless Ad-hoc Networks Issues

2.1 Routing Protocol in Ad-hoc Networks

Wireless Ad-hoc Networks operates without a fixed infrastructure. Multi-hop, mobility, large network size combined with device heterogeneity and bandwidth and battery power limitations, all these factors make the design of routing protocols a major challenge. Lots of researchers did tremendous work on the Wireless Ad-hoc Routing Protocols.Two main kinds of Routing Protocols are existed today: one is called table-driven protocols (including distance vector and link state), another is on-demand protocols.

In table driven routing protocols, the protocols consistent and up-to-date routing information to all nodes is maintained at each node whereas in on-demand routing the routes are created only when desired by the source host. While for the on demand Routing protocols, “on demand” means that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources.If we look up the key words “Wireless Ad hoc Networks Routing Protocols” in Google, we could find tons of millions of all kinds of routing protocols, as LAR(Location-Aided Routing), DSDV (Destination- Sequenced Distance-Vector Routing), AODV (Ad-hoc On-Demand Distance Vector Routing), and DSR (Dynamic Source Routing Protocol)…… However, after survey various types of routing strategies proposed for wireless ad-hoc networks, we find the truth is all these routing protocols are all have inherent drawbacks and cannot be considered as good routing protocols for Wireless ad hoc Networks. Just like Windows operating systems need patch at all the time, the Wireless Ad hoc networks routing protocol are all needs patches too.

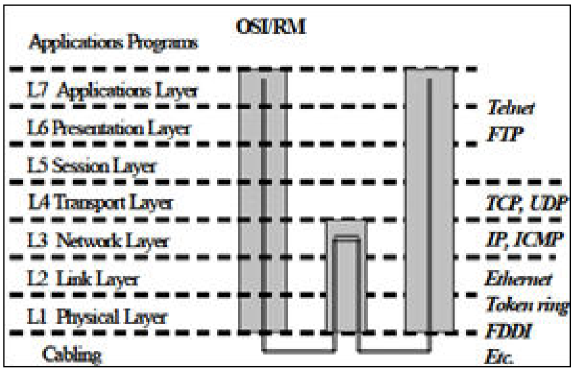
The main problems about the routing protocols are as Following:

- First of all, consider the rapid passing pattern. We define the rapid passing pattern to be one node passing through the whole network very quickly. Such a rapid passing node will generate the following affects to the whole network. First, the topology of the network changed rapidly, which will lead to the lost of packets. Second, we have to modify every node's routing table that within the communication distance of the rapid-passing node, that will greatly improve the consumption of the bandwidth and the overhead of the networks. Third, obviously there will be tremendous delay of the data sending to the rapid-moving node.
- Transmission between two hosts over a wireless network does not necessarily work equally well in both directions. Thus, some routes determined by some routing protocols may not work in some environments.
- Many routing protocols may create redundant routes,which will greatly increase the routing updates as well as increase the whole networks overhead.
- Periodically sending routing tables will waste network bandwidth. When the topology changes slowly, sending routing messages will greatly waste the bandwidth of Wireless Ad-hoc Networks. This will add additional burdens to the limited bandwidth of the Ad-hoc Networks.
- Periodically sending routing tables also waste the battery power. Energy consumption is also a critical factor which prevents Wireless Ad-hoc Networks to be a non-flowed architecture.

We all understand that a stable network routing protocols is essential for any kinds of networks. However, for the Wireless ad hoc Networks, we could not find a stable routing protocol even after we have done research on it more than 10 years. Needless to say that it is the Wireless Ad hoc Networks itself is flawed.

2.2 Open Systems Interconnection Reference Model (OSI/RM).

The International Standards Organization (ISO) OSI/RM architecture specifies the relation between messages transmitted in a communication network and applications programs run by the users. The development of this open standard has encouraged the adoption by different developers of standardized compatible systems interfaces. The figure shows the seven layers of OSI/RM. Each layer is self-contained, so that it can be modified without unduly affecting other layers. The Transport Layer provides error detection and correction. Routing and flow control are performed in the Network Layer. The Physical Layer represents the actual hardware communication link interconnections. The Applications Layer represents programs run by users.



Routing. Since a distributed network has multiple nodes and services many messages, and each node is a shared resource, many decisions must be made. There may be multiple paths from the source to the destination. Therefore, message routing is an important topic. The main performance measures affected by the routing scheme are throughput (quantity of service) and average packet delay (quality of service). Routing schemes should also avoid both deadlock and livelock (see below).

Fixed routing schemes often use Routing Tables that dictate the next node to be routed to, given the current message location and the destination node. Routing tables can be very large for large networks, and cannot take into account real-time effects such as failed links, nodes with backed up queues, or congested links.

Adaptive routing schemes depend on the current network status and can take into account various performance measures, including cost of transmission over a given link, congestion of a given link, reliability of a path, and time of transmission. They can also account for link or node failures.

Routing algorithms can be based on various network analysis and graph theoretic concepts in Computer Science (e.g. A-star tree search), or in Operations Research [Bronson 1997] including shortest-route, maximal flow, and minimum-span problems. Routing is closely associated with dynamic programming and the optimal control problem in feedback control theory [Lewis and Syrmos 1995]. Shortest Path routing schemes find the shortest path from a given node to the destination node. If the cost, instead of the link length, is associated with each link, these algorithms can also compute minimum cost routes. These algorithms can be centralized (find the shortest path from a given node to all other nodes) or decentralized (find the shortest path from all nodes to a given node). There are certain well-defined algorithms for shortest path routing, including the efficient Dijkstra algorithm [Kumar 2001], which has polynomial complexity. The Bellman-Ford algorithm finds the path with the least number of hops [Kumar 2001]. Routing schemes based on competitive game theoretic notions have also been developed [Altman et al. 2002].

Deadlock and Livelock. Large-scale communication networks contain cycles (circular paths) of nodes. Moreover, each node is a shared resource that can handle multiple messages flowing along different paths. Therefore, communication nets are susceptible to deadlock, wherein all nodes in a specific cycle have full buffers and are waiting for each other. Then, no node can transmit because no node can get free buffer space, so all transmission in that cycle comes to a halt. Livelock, on the other hand, is the condition wherein a message is continually transmitted around the network and never reaches its destination. Livelock is a deficiency of some routing schemes that route the message to alternate links when the desired links are congested, without taking into account that the message should be routed closer to its final destination. Many routing schemes are available for routing with deadlock and livelock avoidance [e.g. Duato 1996].

Flow Control. In queuing networks, each node has an associated queue or buffer that can stack messages. In such networks, flow control and resource assignment are important. The objectives of flow control are to protect the network from problems related to overload and speed mismatches, and to maintain QoS, efficiency, fairness, and freedom from deadlock. If a given node A has high priority, its messages might be preferentially routed in every case, so that competing nodes are choked off as the traffic of A increases. Fair routing schemes avoid this. There are several techniques for flow control: In buffer management, certain portions of the buffer space are assigned for certain purposes. In choke packet schemes, any node sensing congestion sends choke packets to other nodes telling them to reduce their transmissions. Isarithmic schemes have a fixed number of 'permits' for the network. A message can be sent only if a permit is available. In window or kanban schemes, the receiver grants 'credits' to the sender only if it has free buffer space. Upon receiving a credit, the sender can transmit a message. In Transmission

2.3 Routing Challenges and Design Issues in WSNs

Limited energy supply, limited computing power, and limited bandwidth of the wireless links connecting sensor nodes. One of the main design goals of WSN is to carry out data communication while trying to prolong the lifetime of the network and prevent connectivity degradation by employing aggressive energy management techniques. In order to design an efficient routing protocol, several challenging factors should be addressed meticulously. The following factors are discussed below:

Node deployment: Node deployment in WSN is application dependent and affects the performance of the routing protocol. The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths; but in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner. Hence, random deployment raises several issues as coverage, optimal clustering etc. which need to be addressed.

Energy consumption without losing accuracy: sensor nodes can use up their limited supply of energy performing computations and transmitting information in a wireless environment. As such, energy conserving forms of communication and computation are essential. Sensor node lifetime shows a strong dependence on the battery lifetime. In a multihop WSN, each node plays a dual role as data sender and data router. The malfunctioning of some sensor nodes due to power failure can cause significant topological changes and might require rerouting of packets and reorganization of the network.

Node/Link Heterogeneity: Some applications of sensor networks might require a diverse mixture of sensor nodes with different types and capabilities to be deployed. Data from different sensors, can be generated at different rates, network can follow different data reporting models and can be subjected to different quality of service constraints. Such a heterogeneous environment makes routing more complex.

Fault Tolerance: Some sensor nodes may fail or be blocked due to lack of power, physical damage, or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. If many nodes fail, MAC and routing protocols must accommodate formation of new links and routes to the data collection base stations. This may require actively adjusting transmit powers and signaling rates on the existing links to reduce energy consumption, or rerouting packets through regions of the network where more energy is available. Therefore, multiple levels of redundancy may be needed in a fault-tolerant sensor network.

Scalability: The number of sensor nodes deployed in the sensing area may be in the order of hundreds or thousands, or more. Any routing scheme must be able to work with this huge number of sensor nodes. In addition, sensor network routing protocols should be scalable enough to respond to events in the environment. Until an event occurs, most of the sensors can remain in the sleep state, with data from the few remaining sensors providing a coarse quality.

Network Dynamics: Most of the network architectures assume that sensor nodes are stationary. How-ever, mobility of both BS's and sensor nodes is sometimes necessary in many applications. Routing messages from or to moving nodes is more challenging since route stability becomes an important issue, besides energy, bandwidth etc. Moreover, the sensed phenomenon can be either dynamic or static depending on the application, e.g., it is dynamic in a target detection/tracking application, while it is static in forest monitoring for early fire prevention. Monitoring static events allows the network to work in a reactive mode, simply generating traffic when reporting. Dynamic events in most applications require periodic reporting and consequently generate significant traffic to be routed to the BS.

Transmission Media: In a multi-hop sensor network, communicating nodes are linked by a wireless medium. The traditional problems associated with a wireless channel (e.g., fading, high error rate) may also affect the operation of the sensor network. As the transmission energy varies directly with the square of distance therefore a multi-hop network is suitable for conserving energy. But a multi-hop network raises several issues regarding topology management and media access control. One approach of MAC design for sensor networks is to use CSMA-CA based protocols of IEEE 802.15.4 that conserve more energy compared to contention based protocols like CSMA (e.g. IEEE 802.11). So, Zigbee which is based upon IEEE 802.15.4 LWPAN technology is introduced to meet the challenges.

Connectivity: The connectivity of WSN depends on the radio coverage. If there continuously exists a multi-hop connection between any two nodes, the network is connected. The connectivity is intermittent if WSN is partitioned occasionally, and sporadic if the nodes are only occasionally in the communication range of other nodes.

Quality of Service: In some applications, data should be delivered within a certain period of time from the moment it is sensed; otherwise the data will be useless. Therefore bounded latency for data delivery is another condition for time-constrained applications. However, in many applications, conservation of energy, which is directly related to network lifetime, is considered relatively more important than the quality of data sent. As the energy gets depleted, the network may be required to reduce the quality of the results in order to reduce the energy dissipation in the nodes and hence lengthen the total network lifetime. Hence, energy-aware routing protocols are required to capture this requirement.

3. Classification of Routing Protocols in WSNs

A routing protocol is considered adaptive if certain system parameters can be controlled in order to adapt to the current network conditions and available energy levels. Furthermore, these protocols can be classified into multipath-based, query-based, negotiation-based, QoS-based, or routing techniques depending on the protocol operation. In addition to the above, routing protocols can be classified into three categories, namely, proactive, reactive, and hybrid protocols depending on how the source sends a route to the destination. In proactive protocols, all routes are computed before they are really needed, while in reactive protocols, routes are computed on demand. Hybrid protocols use a combination of these two ideas. When sensor nodes are static, it is preferable to have table driven routing protocols rather than using reactive protocols. A significant amount of energy is used in route discovery and setup of reactive protocols.

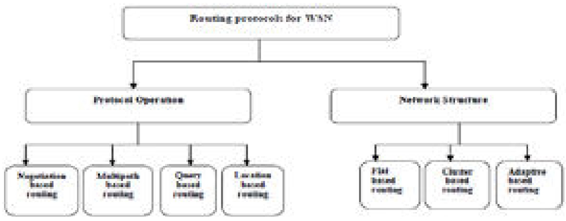


Fig: Taxonomy of routing protocols for WSN

Negotiation based routing: These protocols use high-level data descriptors called ―meta-data‖ in order to eliminate redundant data transmission through negotiations. The necessary decisions are based on available resources and local interactions.

Multipath based routing: These protocols offer fault tolerance by having at least one alternate path (from source to sink) and thus, increasing energy consumption and traffic generation. These paths are kept alive by sending periodic messages.

Flat based routing: In these protocols, all nodes have assigned equal roles in the network. The well known protocols considered in flat based routing are: Sequential Assignment Routing (SAR), .Directed Diffusion, Energy Aware Routing (EAR) etc.

Hierarchical based routing: It is also known as cluster-based routing. In these protocols, the nodes can play different roles in the network and normally the protocol includes the creation of clusters. Additionally, designations of tasks for the sensor nodes with different characteristics are also performed.

Adaptive based routing: In these protocols, the system parameters are controlled to be adapted to the actual network conditions by means of acquired information of the network and negotiation between nodes (e.g. the available energy on the node or QoS of the path). Adaptive based routing is based on the family of protocols called Sensor Protocols for Information via Negotiation (SPIN) which is described in Negotiation based routing.

Location-based Routing: In location-based routing, all the sensor nodes are addressed by using their locations. Depending upon the strength of the incoming signals, it is possible to calculate the nearest neighboring node's distance. Due to obstacles in the network often the signal strength becomes weaker and nodes find it difficulty in finding the nearest neighbor nodes, SMECN performs well in such situations also by creating a sparse graph of the network nodes before transmitting to the next node. All the nodes in the network exchange this data in order to know about neighboring nodes. This is useful for communicating and transferring information. As energy is the major factor of concern in routing protocols, location-based schemes demand that nodes should change their state from active to sleep mode when there is no activity. The more nodes in sleep mode, the more energy is saved. There are many location-based schemes of which GAF (Geographic Adaptive Fidelity) and GEAR (Geographic and Energy aware Routing) are two examples.

Query-based: In Query-based routing propagates the use of queries issued by the base station. The base station sends queries requesting for certain information from the nodes in the network. A node, which is responsible for sensing and collecting data, reads these queries and if there is a match with the data requested in the query it starts sending the data to the requested node or the base station (here). This process is known as Directed Diffusion where the base station sends interest messages on to the network. These interest messages, which move in the network, create a path while passing through all the sensor nodes. Any sensor node, which has the data suitable to the interest message, sends collected data along with the interest message towards the base station. Thus, less energy is consumed and data aggregation is performed on a route.

Negotiation-based: These protocols use high-level descriptors coded in high level so as to eliminate the redundant data transmissions. Flooding is used to disseminate data, due to the fact that flooding data are overlapped and collisions occur during transmissions. Nodes receive duplicate copies of data during transmission. The same data content is sent or exchanged again and again between the same set of nodes, and a lot of energy is utilized during this process. Negotiation protocols like SPIN are used to suppress duplicate information and prevent redundant data from being sent to the next neighboring nodes or towards the base station by performing several negotiation messages on the real data that has to be transmitted

Conclusions

Routing in sensor networks is a new area of research, with a limited, but rapidly growing set of research results. In this paper, we presented a comprehensive survey of routing techniques in wireless sensor networks which have been presented in the literature. They have the common objective of trying to extend the lifetime of the sensor network, while not compromising data delivery.

Overall, the routing techniques are classified based on the network structure into three categories: flat, hierarchical, and location based routing protocols. Furthermore, these protocols are classified into multipath-based, query-based, negotiation-based, or QoS-based routing techniques depending on the protocol operation. We also highlight the design tradeoffs between energy and communication overhead savings in some of the routing paradigm, as well as the advantages and disadvantages of each routing technique. Although many of these routing techniques look promising, there are still many challenges that need to be solved in the sensor networks. We highlighted those challenges and pinpointed future research directions in this regard.

REFERENCES

[1] IEEE Std 802.11 – 1999: Wireless Medium Access | Control (MAC) and Physical Layer (PHY) specifications, Inst. Elec. Electron. Eng., New York, USA, 1999.ISBN 0-7381-1658-0 | [2] IPN Progress Report, August 15, 2002, Analysis of | Energy Consumption for Ad Hoc Wireless Sensor Networks Using a Bit-Meter-Per-Joule Metric, J.L.Gao | [3] A Distributed Light-Weight Authentication Model | for Ad-hoc Networks | [4] M. Satyanarayanan. Fundamental challenges in | mobile computing. submitted paper. | [5] M. Haardt W. Mohr R. Becher, M. Dillinger. Broadband wireless access and futurecommunication networks. Proceedings of the IEEE, 89(1), 2001. | [6] S.Chessa, P.Santi, "Comparison Based System-Level Fault Diagnosis in Ad-Hoc Networks", Proc. IEEE 20th Symp. on Reliable Distributed Systems (SRDS), New Orleans, pp. 257-266, October 2001 | [7] Erik Skow, Jiejun Kong, Thomas Phan, Fred Cheng, | Richard Guy, Rajive Bagrodia, Mario Gerla, and Songwu Lu, "A Security Architecture for Application Session Handoff" | [8] Lidong Zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks" | [9] David B. Johnson, "Routing in Ad Hoc Networks of | Mobile Hosts", Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, December 1994. | [10] Ljubica Blazevic, Levente Buttyan, Srdan Capkun, | Silvia Giordano, Jean-Pierre, Hubaux and Jean-Yves Le Boudec, "Self-Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes" | [11] J. A. Freebersyser and B. Leinerr, "A DoD perspective on mobile ad hoc networks," in Ad Hoc Networking, C. E. Perkin, Ed. Addison-Wesley, 2001, pp. 29–51. |