Performance analysis of routing strategies for wireless sensor networks

Análisis del funcionamiento de estrategias de enrutamiento para redes de sensores inalámbricos

Raúl Aquino-Santos*, Luis A. Villaseñor-González, Víctor Rangel Licea, Omar Álvarez Cárdenas, Arthur Edwards Block

1Facultad de Telemática, Universidad de Colima, Av. Universidad 333, C. P. 28040, Colima, México
2CICESE Research Centre, Carr. Tijuana-Ensenada, km 113, Ensenada, B. C. México
3Departamento de Telecomunicaciones, Universidad Nacional Autónoma de México (UNAM), C. P. 04510, México, D. F

(Recibido el 11 de mayo de 2009. Aceptado el 23 de septiembre de 2009)

Abstract

This paper presents a performance analysis of source, shortest path, hierarchical and geographical routing strategies, which are the three most commonly implemented strategies employed by wireless ad-hoc and sensor networks. Source routing was selected because it does not require costly topology maintenance, while shortest path routing was chosen because of its simple discovery routing approach and hierarchical and geographical routing was elected because it uses location information via Global Positioning System (GPS). Many current applications require precise knowledge of physical positioning information, particularly in the areas of health, military, agriculture, robotics, and environmental and structural monitoring. Additionally, the shortest path routing technique was chosen because it is employed in several data-centric wireless sensor network algorithms such as Direct Diffusion, Rumor Routing, Gradient-Based Routing and the ZigBee standard. The performance of these three routing strategies is evaluated by providing simulation results based on latency, End to End Delay (EED), packet delivery ratio, routing overhead, overhead and routing load. Source routing only improves shortest path and hierarchical and geographical routing in terms of latency, hierarchical and geographical routing performs the worst because it must send hello packets in order to acquire and transmit location

* Autor de correspondencia: teléfono: + 52 + 3 + 126 10 75, correo electrónico: aquinor@ucol.mx (R. Santos)
information. However, despite these significant disadvantages, hierarchical and geographical routing remains the routing option most often used in health, military, agriculture, robotic, and environmental and structural monitoring.

----- Keywords: Wireless sensor networks, multi-hop networks, unicast routing, hierarchical and flat routing mechanisms for wireless sensor networks

Resumen
Este trabajo presenta el análisis de funcionamiento de estrategias de enrutamiento de fuente, de la trayectoria más corta, jerárquica y geográfica, las cuales son tres de las estrategias más comúnmente implementadas para redes ad hoc y de sensores. Enrutamiento de fuente se seleccionó debido a que no requiere un mantenimiento topológico costoso, mientras el enrutamiento de la trayectoria más corta fue elegido por su simplicidad en el descubrimiento de la ruta y la estrategia de enrutamiento jerárquica y geográfica fue seleccionada debido a que utiliza información de un sistema de posicionamiento global (GPS). Muchas aplicaciones actuales requieren el conocimiento preciso de la posición física, particularmente en las áreas de salud, militar, agricultura, robótica y monitoreo estructural y ambiental. Adicionalmente, la técnica de enrutamiento de trayectoria más corta fue seleccionada por que se emplea en algoritmos de redes de sensores inalámbricos centrados en datos, tales como: Difusión Directa, Enrutamiento por Rumor, Enrutamiento basado en Gradientes y el Estándar ZigBEE. El funcionamiento de estas tres estrategias de enrutamiento se evalúa a través de simulaciones y en términos de latencia, retardo punto a punto, tasa de entrega de paquetes, sobre procesamiento de enrutamiento, sobre procesamiento general y la carga de enrutamiento.

----- Palabras clave: Redes de sensores inalámbricos, redes multi-saltos, enrutamiento unicast. mecanismos de enrutamiento para redes de sensores inalámbricos

Introduction
Recent advances in micro-electro-mechanical systems (MEMS) technology have made the deployment of wireless sensor nodes a reality [1, 2], in part, because they are small, inexpensive and energy efficient. Each node of a sensor network consists of three basic subsystems: a sensor subsystem to monitor local environmental parameters, a processing subsystem to give computation support to the node, and a communication subsystem to provide wireless communications to exchange information with neighboring nodes. Because each individual sensor node can only cover a relatively limited area, it needs to be connected with other nodes in a coordinated fashion to form a sensor network (SN), which can provide large amounts of detailed information about a given geographic area. Consequently, a wireless sensor network (WSN) can be described as a collection of intercommunicated wireless sensor nodes which coordinate to perform a specific action. Unlike traditional wireless networks, WSNs depend on dense deployment and coordination to synchronously carry out their task. Wireless sensor nodes measure conditions in the environment surrounding them and then transform these measurements into signals that can be processed to reveal specific information...
about phenomena located within a coverage area around these sensor nodes.

Examples of WSN applications include environmental monitoring—which involves monitoring air, soil and water, condition-based maintenance, habitat monitoring (determining the plant and animal species population and behavior), seismic detection, military surveillance, inventory tracking, smart spaces, etc. [3, 4]. Despite their many diverse applications, WSNs pose a number of unique technical challenges due to the following factors: fault tolerance (robustness), scalability, production costs, operating environment, sensor network topology, hardware constraint, transmission media and power consumption.

To date, the ZigBee Alliance is developing a communication standard for WSNs to support low-cost, low-power consumption, two-way wireless communications. Solutions adopting the ZigBee standard will be embedded in consumer electronics, home and building automation, industrial controls, PC peripherals, medical sensor applications, toys and games [5].

Many researchers are currently engaged in developing strategies to meet these many diverse requirements. This paper focuses on a performance analysis of three basic strategies which are commonly used in routing protocols in wireless ad-hoc and sensor networks. The remainder of the paper is organized as follows: First, a brief overview of wireless sensor network technology is presented. Then, various routing protocols that deal with state-of-the-art routing techniques for wireless sensor networks are described. Next, details about the ZigBee architecture the scenario simulated are introduced. Finally, a summary of our work and future research is presented.

**Wireless sensor network technology**

Sensors are devices that produce a measurable response to changes in specific physical conditions like temperature and pressure. Basically, each sensor node is comprised of a sensing, processing, transmission and power unit [6, 7]. The processing unit is responsible for collecting and processing signals transmitted from sensors and forwarding them to the network. The transmission unit provides the signal transfer medium from sensors to the exterior world or computer network. It also has a communication mechanism to establish and maintain the WSN, which is usually ad-hoc. The power supply unit consists of a battery and a dc-dc converter that powers the node (Figure 1).

![Figure 1 Sensor node components](image)

Sensor networks are generally deployed into an unplanned infrastructure where there is no a priori knowledge of their specific location. The resulting problem of estimating the spatial coordinates of the node is referred to as location. Most of the proposed localization techniques today depend on recursive trilateration/multilateration techniques [8]. Routing in WSNs is one of the most challenging tasks due to the inherent characteristics that distinguish these networks from other wireless networks such as mobile ad-hoc or cellular networks. First, due to the relatively large number of sensor nodes, it is not possible to build a global addressing scheme. Thus, traditional IP-based protocols are not recommended for WSN use. Furthermore, sensor nodes that are deployed in an ad-hoc manner need to be self-organizing as the ad-hoc deployment of these nodes requires the system to establish connections and cope with the resultant nodal distribution, particularly because the operation of sensor networks is largely unattended. In WSNs, obtaining data is sometimes more important than knowing the specific Id of the originating node. Because the data collected by many sensors in WSNs is typically based on a common phenomenon, there is a high probability that this data has some degree of redundancy. Data redundancy needs to be exploited by the routing
protocol to optimize energy and bandwidth utilization.

State of the art of routing techniques for wireless sensor networks

Routing protocols for wireless sensor networks can be classified as data-centric, hierarchical or location-based (Figure 2). In these three categories, source, shortest path, and hierarchical and geographical routing have been employed to develop all of the routing algorithms. In addition, source, shortest path, and hierarchical and geographical routing have been employed in wireless ad-hoc networks (e.g. Dynamic Source Routing (DSR) [9], Ad-hoc On-Demand Distance Vector (AODV) [10], and Location Routing Algorithm with Cluster-Based Flooding (LORA-CBF) [11]).

Flooding and Gossiping

Sensor protocols for information via negotiation (SPIN) address the deficiencies of classic flooding by providing negotiation and resource adaptation [13]. However, the SPIN data advertisement mechanism cannot, by itself, guarantee data delivery [14]. SPIN employs a shortest path strategy based on three types of messages:

- ADV – new data advertisement. When a SPIN node has data to share, it can advertise this fact by transmitting an ADV message containing meta-data.
- REQ – request for data. A SPIN node sends an REQ message when it wishes to receive some actual data.
- DATA – data message. DATA messages contain actual sensor data with a meta-data header.

Unlike traditional networks, a sensor node does not necessarily require an identity (e.g. an address). Instead, applications focus on the different data generated by the sensors. Because data is identified by its attributes, applications request data matching certain attribute values. One of the most popular algorithms for data-centric protocols is direct diffusion and it bases its routing strategy on shortest path [15]. A sensor network based on direct diffusion exhibits the following properties: each sensor node names data that it generates with one or more attributes, other nodes may express interests based on these attributes, and network nodes propagate interests. Interests establish gradients that direct the diffusion of data. In its simple form, a gradient is a scalar quantity. Negative gradients inhibit the distribution of data.
along a particular path and positive gradients encourage the transmission of data along the path.

The Energy-Aware Routing protocol is a destination-initiated reactive protocol that increases the network lifetime using only one path at all times, it seems very similar to source routing [16]. Rumor routing [17] is a variation of direct diffusion that is mainly intended for applications where geographic routing is not feasible. Gradient-based routing is another variant of direct diffusion [18]. The key idea of gradient-based routing is to memorize the number of hops when the interest is diffused throughout the network. Constraint Anisotropic Diffusion Routing (CADR) is a general form of direct diffusion [19] and lastly, Active Query Forwarding in Sensor Networks (ACQUIRE) [20] views the network as a distributed database, where complex queries can be further divided into several sub queries.

**Hierarchical protocols**

Hierarchical protocols are based on clusters because clusters can contribute to more scalable behavior as the number of nodes increases, provide improved robustness, and facilitate more efficient resource utilization for many distributed sensor coordination tasks.

Low-Energy Adaptive Clustering Hierarchy (LEACH) is a cluster-based protocol that minimizes energy dissipation in sensor networks by randomly selecting sensor nodes as cluster-heads [21]. Power-Efficient Gathering in Sensor Information System (PEGASIS) [22] is a near optimal chain-based protocol. The basic idea of the protocol is to extend network lifetime by allowing nodes to communicate exclusively with their closest neighbors, employing a turn-taking strategy to communicate with the Base Station (BS). Threshold-sensitive Energy Efficient protocol (TEEN) [23] and Adaptive Periodic TEEN (APTEEN) [24] have also been proposed for time-critical applications. In TEEN, sensor nodes continuously sense the medium, but data transmission is done less frequently. APTEEN, on the other hand, is a hybrid protocol that changes the periodicity or threshold values used in the TEEN protocol, according to user needs and the application type.

**Location-based protocols**

Location-based protocols make use of position information to relay data to the desired regions instead of the entire network. Before a packet can be sent, the position of the destination must first be determined. Typically, a location service is responsible for this task. Existing location services can be classified according to how many nodes host the service. This can be either a specific node or all of the network nodes. Furthermore, each location server may maintain the position of a specific node or all the nodes in the network.

In position-based routing, the forwarding decision by a node is primarily based on the position of a packet’s destination and the position of the node’s immediate one-hop neighbor. The position of the destination is contained in the header of the packet. If a node has a more accurate position of the destination, it may choose to update the position in the packet before forwarding it. The position of neighbors is typically learned through a one-hop broadcast beacon. These beacons are sent periodically by all nodes and contain the position of the sending node.

We can distinguish three main packet-forwarding strategies for position-based routing: greedy forwarding, restricted directional flooding, and hierarchical approaches. For the first two, a node forwards a given packet to one (greedy forwarding) or more (restricted directional flooding) one-hop neighbors that are located closer to the destination than the forwarding node itself. The selection of the neighbor in the greedy case depends on the optimization criteria of the algorithm. The third forwarding strategy is to form a hierarchy in order to scale to a large number of mobile nodes.

by utilizing low-power geographic positioning system (GPS). The main idea of MECN is to find the sub-network with the smallest number of nodes that requires the least transmission power between any two particular nodes (shortest path). The Small Minimum Energy Communication Network (SMECN) [26] is an extension of MECN. The major drawback with MECN is that it assumes every node can transmit to every other node, which is not always possible. One advantage of SMECN is that it considers obstacles between pairs of nodes. Geographic Adaptive Fidelity (GAF) [27] is an energy-aware location-based routing algorithm primarily designed for ad-hoc networks that can also be applied to sensor networks. GAF conserves energy by turning off unnecessary nodes in the network without affecting the level of routing fidelity. Finally, Geographic and Energy Aware Routing [28] uses energy-awareness and geographically informed neighbor selection heuristics to route a packet toward the destination region.

Zigbee architecture

The IEEE 802.15.4-2003 standard defines the lower two layers: the physical (PHY) layer and the medium access control (MAC) sub-layer. The ZigBee alliance builds on this foundation by providing the network (NWK) layer and the framework for the application layer, which includes the application support sub-layer (APS), the ZigBee device objects (ZDO) and the manufacturer-defined application objects.

IEEE 802.15.4-2003 has two PHY layers that operate in two separate frequency ranges: 868/915 MHz and 2.4 GHz. On the other hand, the MAC sub-layer controls access to the radio channel using a CSMA-CA mechanism. Its responsibilities may also include transmitting beacon frames, synchronizing transmissions and providing a reliable transmission mechanism.

The responsibilities of the ZigBee NWK layer includes mechanisms used to join and exit a network, in order to apply security to frames and to route frames to their intended destinations based on shortest path strategy. In addition, the discovery and maintenance of routes between devices transfer to the NWK layer. Also, the discovery of one-hop neighbors and the storing of pertinent neighbor information are done at the NWK layer. The NWK layer of a ZigBee coordinator is responsible for starting a new network, when appropriate, and assigning addresses to newly associated devices.

The responsibilities of the APS sub-layer include maintaining tables for binding, which is the ability to match two devices together based by their services and their needs, and forwarding messages between bound devices. The responsibilities of the ZDO include defining the role of the device within the network, initiating and/or responding to binding requests and establishing a secure relationship between network devices. The ZDO is also responsible for discovering devices on the network and determining which application services they provide.

Simulated scenario

The routing protocols described make use of one, or a combination, of the following mechanisms: source routing, shortest path routing or hierarchical and geographical routing strategies. The performance analysis of these basic strategies is evaluated using simulation derived for the following performance metrics:

Route discovery time (Latency): is the time the sink must wait before actually receiving the first data packet.

Average end-to-end delay of data packets: includes all possible delays caused by queuing, retransmission delays at the MAC and propagation and transfer times.

Packet delivery ratio: is the ratio of the number of data packets delivered to the destination and the number of data packets sent by the sender. Data packets may be dropped en route for several reasons: e.g. the next hop link is broken when the data packet is ready to be transmitted or one or more collisions have occurred.
**Routing load:** is measured in terms of routing packets transmitted per data packets transmitted. The latter includes only the data packets finally delivered at the destination and not the ones that are dropped. The transmission at each hop is counted once for both routing and data packets. This provides an idea of network bandwidth consumed by routing packets with respect to “useful” data packets.

**Routing overhead** is the total number of routing packets transmitted during the simulation. For packets sent over multiple hops, each packet transmission (hop) counts as one transmission.

**Overhead (packets)** is the total number of routing packets generated divided by the sum of total number of data packets transmitted and the total number of routing packets.

In source routing, each packet, in its header, carries the complete, ordered list of nodes through which the packet must pass. The key advantage of source routing is that intermediate nodes do not need to maintain up-to-date routing information in order to route the packets they forward, since the packets themselves already contain all the routing information. This fact, coupled with the on-demand nature of the protocol, eliminates the need for the periodic route advertisement and neighbor detection packets present in other protocols such as the Energy Aware Routing.

In the shortest path strategy, when a node S needs a route to destination D, it broadcasts a route request message to its neighbors, including the last known sequence number for that destination. The route request is flooded in a controlled manner through the network until it reaches a node that has a route to the destination. Each node that forwards the route request creates a reverse route for itself back to node S. Examples are SPIN, Direct Diffusion, MECN, and the ZigBee standard.

When the route request reaches a node with a route to D, that node generates a route reply containing the number of hops necessary to reach D and the sequence number for D most recently seen by the node generating the reply. Importantly, each node that forwards this reply back toward the originator of the route request (node S) creates a forward route to D. The state created in each node remembers only the next hop and not the entire route, as would be done in source routing.

Hierarchical and geographical strategy improves the traditional routing strategies based on non-positional routing by making use of location information provided by GPS as it minimizes flooding of its Location Request (LREQ) packets. Flooding, therefore, is directive for traffic control by using only the selected nodes, called gateway nodes, to diffuse LREQ messages. The purpose of gateway nodes is to minimize the flooding of broadcast messages in the network by reducing duplicate retransmissions in the same region.

Member nodes are converted into gateways when they receive messages from more than one cluster-head. All the members of the cluster read and process the packet, but do not retransmit the broadcast message. This technique significantly reduces the number of retransmissions in a flooding or broadcast procedure in dense networks. Therefore, only the gateway nodes retransmit packets between clusters (hierarchical organization). Moreover, gateways only retransmit a packet from one gateway to another in order to minimize unnecessary retransmissions, and only if the gateway belongs to a different cluster-head. To avoid synchronization of neighbor transmissions, as observed in [29, 30, 31], we have delayed each packet transmission randomly.

Apart from normal hello messages, hierarchical and geographical strategy does not generate additional control traffic in response to link failures and additions. Thus, it is suitable for networks with high rates of topological change. As the protocol keeps only the location information of the [source, destination] pairs in the network, the protocol is particularly suitable for large and dense networks. Hierarchical and geographical strategy is designed to work in a completely distributed manner and does not
depend on any central entity. Additionally, it does not require a reliable transmission for its control messages. Each node sends its control messages periodically, and can therefore sustain some packet losses. This is, of course, important in radio networks like the one being considered here, where deep fades are possible. Hierarchical and geographical strategy does not operate in a source routing manner. Instead, it performs hop-by-hop routing as each node uses its most recent location information of its neighbor nodes to route a packet. Hence, when a node is moving, its position is registered in a routing table so that the movements can be predicted to correctly route the packets to the next hop towards the destination.

Methodology

We decided to evaluate source, shortest path and Hierarchical and geographical routing strategies since they represent the foundation of all of the above mentioned routing protocols. The simulation results were derived assuming a physical layer operating in the 2.4 GHz band. Consequently, we employed the IEEE 802.11 propagation model described in [32] to determine the theoretical coverage transmission and compare it with several experiments

\[ d_{802.11} = \text{anti log} \left[ \frac{L_{802.11} - 7.6 + 20\log_{10}(h_t)(h_r)}{40} \right] \]

Where:

- \( L_{802.11} \) is the path loss
- \( h_t \) and \( h_r \) are the heights of the transmitting and receiving antennas.

Results from the above equation reflect a transmission range of 144 m, with values of 94 dB for the path loss and 1 m, respectively, for the sending and receiving antennas. The values reported on the data sheet from Crossbow [2] indicate a transmission range of between 75 to 100 m. However, during tests we obtained a transmission range of only 75 m, which is what we used for simulation purposes.

The simulator for evaluating the three routing strategies for our wireless sensor network was implemented in OPNET 11.5, and the simulation models a network of 225 MICAz sensor nodes [2]. This configuration represents a typical scenario where nodes are exactly placed (Figure 3) within an area of 1.5 km². We used a 2405-2480 MHz frequency range and a 250 kbps data rate for our simulation, with a MICAz sensor node separation of 75 m. This scenario represents a typical wireless sensor network with one sink node acting as a gateway to communicate the WSN with a separate network (Internet). In our scenario one sensor node communicates with the sink, and the sensor node sends a packet every second (constant bit rate).

Figure 3 Scenario of 225 wireless sensor nodes

Simulation results

Figure 4 shows the latency between the sink and the source in milliseconds. Source and shortest path routing strategies show a similar behavior, hierarchical and geographical routing shows the poorest behavior due to the transmission of position information via hello packets.
Performance analysis of routing strategies for wireless sensor networks

Hierarchical and Geographical
Source Routing

Figure 4 Latency (Seconds)

Figure 5 shows the End-to-End Delay (EED) between the sink and the source in milliseconds. The Hierarchical and geographical routing strategy performs the worst because it transmits position information via hello packets. Frequent transmission of hello packets produces more collision with data packets.

Figure 5 End-to-End Delay (Milliseconds)

The three routing mechanisms show a similar behavior in terms of percentage of delivery ratio because of their static nature as illustrated in figure 6. Figure 7 shows the overhead between the sink and the source. The shortest path technique also has the best performance, with source routing and hierarchical and geographical mechanism performing in a similar fashion. Figure 8 shows the Routing Overhead between the sink and the source. Routing overhead is the total number of routing packets transmitted during the simulation. Again, the shortest path routing strategy performs the best and the hierarchical and geographical strategy the worst. Figure 9 shows the Routing Load between the sink and the source. This metric provides an idea of how much network bandwidth is consumed by routing packets in relation to the useful data packets actually received. Once again, the shortest path routing strategy performs the best, and the hierarchical and geographical mechanism the worst.

Figure 6 Percentage of delivery ratio (packets)

Figure 7 Overhead (packets)

Figure 8 Routing Overhead (packets)
Hierarchical and Geographical Shortest Path Source Routing

Figure 9 Routing Load (packets)

Conclusions and future work

This paper evaluated three routing strategies widely used in routing protocols for wireless sensor networks. Results show that source routing only improves shortest path and hierarchical and geographical routing in terms of latency. The main disadvantage of source routing is that it lacks a number of hop metrics, which can frequently result in longer path selection. Shortest path behaves well in terms of EED, routing overhead, overhead and routing load. Hierarchical and geographical routing performs the worst because it must send hello packets in order to acquire and transmit location information. This consideration makes hierarchical and geographical routing in wireless sensor networks more weighty because it transmits hello packets more frequently, requiring greater bandwidth and energy resources. However, despite these significant disadvantages, hierarchical and geographical routing remains the routing option most often used in health, military, agriculture, robotic, environmental and structural monitoring. An important area of future research is to optimize hierarchical and geographical routing algorithm to facilitate its use in large geographical areas requiring dense sensor distribution.

References


