Служебна бележка

Настоящата служебна бележка се издава в уверение на това, че докладите:

“ELECTRIC PARAMETERS OF DIELECTRIC MATERIALS MEASUREMENT USING ELVIS” с автори Georgi Nikolov и Boyanka Nikolova и

“NETWORK LAYER IN WIRELESS SENSOR NETWORKS” с автори Milen Todorov, Boyanka Nikolova и Georgi Nikolov,

са приети и изнесени на X международна конференция “Предизвикателствата пред висшето образование през 21 век”, проведена от 5 до 8 Юни 2012 г. в град Созопол и ще бъдат включени в сборника с доклади.

София Председател на CHER’21 ……………………………

14.06. 2012 / доц. д-р инж. Ташо Ташев /

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ • СОФИЯ •

NETWORK LAYER IN WIRELESS SENSOR NETWORKS

Milen Todorov[1], Boyanka Nikolova[1], Georgi Nikolov[2]
[1] Technical University of Sofia, Faculty of Telecommunications, 8 Kliment Ohridski,
1000 Sofia, Bulgaria, E-mail: todorov@ecad.tu-sofia.bg, bnikol@tu-sofia.bg
[2] Technical University of Sofia, Faculty of Electronics and Technologies, 8 Kliment Ohridski,
1000 Sofia, Bulgaria, E-mail: gnikolov@tu-sofia.bg

Abstract*:* The network layer is responsible for establishing and maintaining end-to-end connections in the network. This typically requires a network that is fully connected whereby every node in the network can communicate with every other node, although these connections may entail multihop routing through intermediate nodes. The main functions of the network layer in an ad hoc wireless network are neighbor discovery, routing, and dynamic resource allocation. The important differences in the routing used by sensor networks is in-network processing as data aggregating and filtering redundant information. Classifying and designing of routing protocols for Wireless Sensor Networks are challenging due to the some inherent characteristics such as energy efficiency and awareness, connection maintenance, minimum resource usage limitation, low latency etc. In present paper focus is on issues on which Wireless Sensor Networks routing protocols has been categorized or classified and challenges which must be considered while selecting an algorithm for routing purpose.

Key words: flow control, IEEE 802.15.4, metrics, neighbor discovery, resource allocation, routing protocols, topology control, wireless sensor network, ZigBee

1. Introduction

Data collected by sensor nodes in a Wireless Sensor Network (WSN) is typically propagated toward a base station (gateway) that links the WSN with other networks where the data can be visualized, analyzed, and acted upon. In large networks sensor nodes generate own information and serve as relays or forwarding nodes for other sensor nodes. Routing – the process of selecting or establishing the path through which message will be relayed to its destination is a responsibility of the network layer of the communication protocol stack. When the nodes of a WSN are deployed in a deterministic manner, communication between them and the gateway can occur using predetermined routes. By contrast when the nodes are deployed in a randomized manner, the resulting topologies are nonuniform and unpredictable.

Current problems at the network layer can be classified into three categories: topology control, routing, and coordination. A well-organized network topology can not only prolong the lifetime of a network, but also enhance data communications. Quality of Service (QoS) routing as well as multicast, broadcast, and geocast, the primary goal is to fulfill a given communication task successfully between nodes in the network. Wireless sensor actuator networks require coordination not only among sensors or actuators, but also between them.

In WSN the design of a routing protocol is challenging due to the unique characteristics of the network as resource scarcity and unreliability of the wireless medium. The limited processing, storage, bandwidth, and energy capacities require routing solutions that are lightweight, while the frequent dynamic changes in a WSN require routing solutions that are adaptive and flexible [8].

2. Classification of routing protocols in WSNs

Sensor nodes may be scattered densely in an area to observe a phenomenon. As a result, they may be a very close to each other. In such scenario, multihop communication may be a good choice for sensor networks. As compared to long distance wireless communication, multihop communication may be an effective way to overcome some of the signal propagation and degradation effects. In addition, the sensor nodes consume much less energy when transmitting a message because the distances between sensor nodes are shorter [5].

Table 1 presents three different classifications based on the network structure or organization, the route discovery process, and the protocol operation. Flat-based routing protocols consider all nodes of equal functionality as opposite to hierarchical-based protocols. Location-based protocols rely on the location information from nodes to make routing decisions. Routing protocols are responsible for identifying or discovering routes from a source or sender to the intended receiver. This route discovery process can also be used to distinguish between different types of routing protocols. Reactive protocols discover routes on-demand, when a source wants to send data to a receiver and does not already have a route established. While reactive route discovery incurs delays before actual data transmission can occur, proactive routing protocols establish routes before they are actually needed. This category of protocols is known as table-driven, because local forwarding decisions are based on the contents of a routing table that contains a list of destinations and costs associated with each next hop option. It is possible to establish routes that may never be needed. Further, the time interval between route discovery and actual use of the route can be very large, leading to outdated routes and the cost of establishing a routing table can be significant. Hybrid routing protocols exhibit characteristics of both reactive and proactive protocols. Routing protocols also differ in their operation. Negotiation-based protocols aim to reduce redundant data transmissions by relying on the exchange of negotiation messages between neighboring sensor nodes before data transfers. Multipath-based protocols use multiple routes simultaneously to achieve higher performance or fault tolerance. Query-based routing protocols are receiver-initiated. Sensor nodes send data in response to queries issued by the destination node. QoS-based routing protocols satisfy a certain QoS metric. Routing protocols also differ in the way they support in-network data processing. Coherent-based protocols perform only a minimum amount of processing before sensor data is sent to receivers and data aggregators.

Routing is considered node-centric when sensor data is explicitly sent to one or more receivers. Data-centric routing is used when nodes are not explicitly addressed, but receivers are implicitly described by certain attributes [8].

Table 1. Categories of routing protocols

Routing Protocol	**Network Organization**	Flat-Based
		Hierarchical-Based
		Location-Based
	Route Discovery	Reactive
		Proactive
		Hybrid
	Protocol Operation	Negotiation-Based
		Multi-Path-based
		Query-Based
		QoS-Based
		Coherent-Based

3. Commonly Used Metrics

In the path selection process of a routing protocol, route metrics are used to choose the best route. Most of metrics are used for building and maintaining the routing topologies, others for making forwarding decisions whereas some are also applied to constraint-based routing [9].

The most common metric used in routing protocols is minimum hop, that is, the routing protocol attempts to find the path from the sender to destination that requires the smallest number of relay nodes (hops). In this metric every link has the same cost. The routing protocol selects the path that minimizes the total cost of data propagation from source to destination which will result in low end-to-end delays and low resource consumptions. Since the minimum-hop approach does not consider the actual resource availability on each node, the resulting route is probably nonoptimal in terms of delay, energy, and congestion avoidance.

The most crucial aspect of routing in WSNs is energy efficiency, but there is not one unique energy metric. There are various different interpretations if energy efficiency: minimum energy consumed per packet, maximum time to network partition, minimum variance in node power levels, maximum (average) energy capacity and maximum minimum energy capacity. Figure 1 shows comparison of routing choices depending of used metric. The number on each link indicates the cost of propagating the packet over this link. The numbers in parentheses indicate the nodes' remaining energy capacity. The goal of minimum energy consumed per packet metric is to minimize the total amount of energy expended for the propagation of a single packet from the source to the destination. The total energy is the sum of the energy consumed by each node along a route for receiving and transmitting the packet. The challenge of maximum time to network partition metric is to reduce the energy consumption on nodes whose removal (node D) will cause a network to partition. All nodes within the network are considered equally important in minimum variance in node power levels. This could maximize the lifetime of the entire network. A routing protocol that uses maximum (average) energy capacity would choose routes that have the largest total energy capacity from source to destination. A variation of this metric is average energy capacity, which avoids choosing unnecessarily long routes in order to maximize the total energy capacity. Maximum minimum energy capacity metric protects low-capacity nodes from premature expiration, instead of maximizing the energy capacities of the entire path [8].

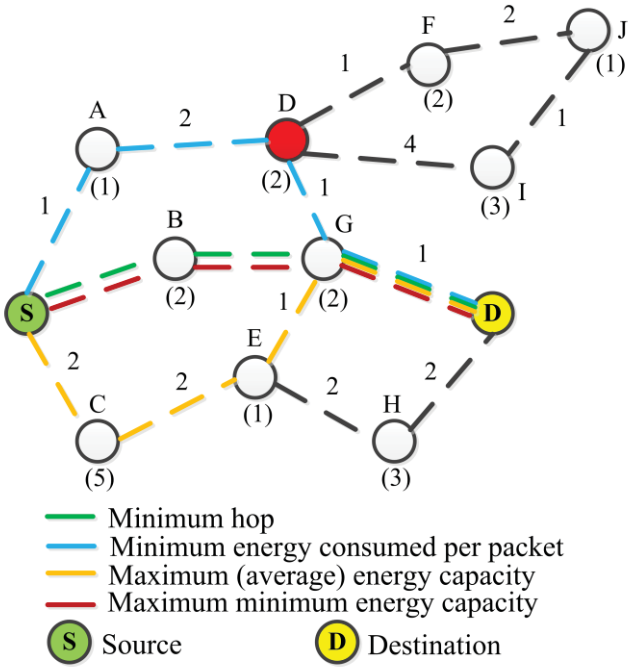
F
2
J
(1)
1
(2)
A
2
D
4
1
(1)
(2)
1
I
(3)
1
B
G
1
S
(2)
1
(2)
D
E
2
2
2
2
C
H
(1)
(5)
(3)
Minimum hop
Minimum energy consumed per packet
Maximum (average) energy capacity
Maximum minimum energy capacity
S Source
D Destination

Fig. 1 Comparison of routing choices using different metrics.

Metrics with QoS refer to defined measures of performance in networks including end-to-end latency (or delay), throughput and jitter (variation in latency) and packet loss (or error rate).

With robustness metric the sensor nodes can use routes that are stable and reliable for long periods of time. For this purpose nodes can measure or estimate the link quality to each of their neighbors and then select a next hop neighbor that increases the probability of a successful transmission.

4. Neighbor Discovery and Topology Control

Neighbor discovery is one of the first steps in the initialization of a network with randomly distributed nodes. For the individual node, this is the process of determining the number and identity of network nodes with which direct communication can be established given some maximum power level and minimum link performance requirements (in terms of data rate and associated Bit Error Rate). The higher the allowed transmit power, the greater the number of nodes in a given neighborhood. Neighbor discovery begins with a probe of a neighboring nodes using some initial transmit power. If this power is not sufficient to establish a connection with $N \geq 1$ neighbors then transmit power is increased and probing repeated. The parameter N is set based on network requirements for minimal connectivity, while P_{max} is the power limitations of each node and the network design [1]. Topology control is the process of coordinating nodes' decisions regarding their transmitting ranges, in order to generate a network with the desired properties (e.g. connectivity) while reducing node energy consumption and/or increasing network capacity [6].

5. Resource Allocation and Flow Control

When the routing optimization is based on minimum congestion or delay, routing becomes interwined with flow control, which sits at the transport layer. If the routing algorithm sends too much data over a given link, that link becomes congested, so that the routing algorithm must change to a different route to avoid this link. The delay associated with a given link is a function of the link data rate or capacity: the higher the capacity, the more data can flow over the link with minimal delay. The classic metric for delay on a link from node *i* to node *j*, neglecting processing and propagation delay, is

$$D_{ij} = \frac{f_{ij}}{C_{ij} - f_{ij}}, \tag{1}$$

where f_{ij} is the traffic flow assigned to the link and C_{ij} is its capacity [1].

6. Sensor Networking Examples

Recent advances in computing hardware and software are responsible for the emergence of sensor networks capable of observing the environment, processing the data and making decisions based on the observations. Such a network can be used to monitor the environment, detect, classify and locate specific events, and track targets over a specific region. Examples of such systems are in surveillance, monitoring of pollution, traffic, agriculture or civil infrastructures. The deployment of sensor networks varies with the application considered. It can be predetermined when the environment is sufficiently known and under control, in which case the sensors can be strategically hand placed. In some other applications when the environment is unknown or hostile, the deployment cannot be a priori determined, for example if the sensors are air-dropped from an aircraft of deployed by other means, generally resulting in a random placement. In order to detect a target moving in the region, sensors make local observations of the environment and collaborate to produce a global decision that reflects the status of the region covered. This collaboration requires local processing of the observations, communication between different nodes, and information fusion [3].

Home automation is one of the major application areas for sensor wireless networking. A security system can consist of several sensors, including motion detectors, glass-break sensors, and security cameras. It is possible to transfer images wirelessly with acceptable quality in security systems.

ZigBee is a standard that defines a set of communication protocols for lo-data-rate short-range wireless networking. In consumer electronics, ZigBee can be used in wireless remote controls, game controllers, a wireless mouse for a personal computer, and may other applications. IEEE 802.15.4 is a proper replacement for infrared technology in remote controls because of the low cost and long battery life of ZigBee-based wireless communication.

At the industrial level, ZigBee mesh networking can help in areas such as energy management, light control, process control, and asset management.

One of the applications of IEEE 802.15.4 in the healthcare industry is monitoring a patient's vital information remotely. The patient wears a ZigBee device that interfaces with a sensor that gathers information. This information is transmitted to a ZigBee gateway. A ZigBee gateway provides the interface between a ZigBee network and other networks, such as an Internet Protocol (IP) network [7].

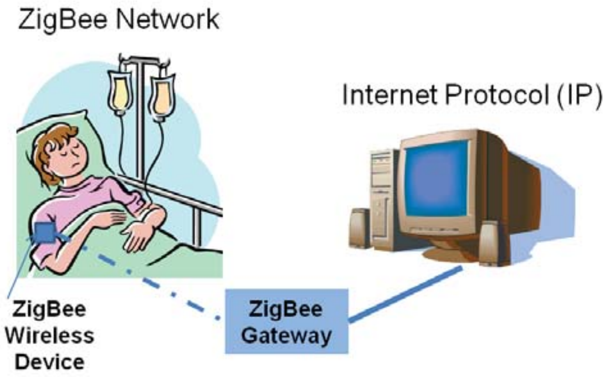

Fig. 2 In-home patient monitoring using ZigBee Wireless Networking

Military missions require sensors and other intelligence gathering mechanisms that can be placed close to their intended targets. The potential threat to these mechanisms is therefore quite high, so it follows that the technology used must be highly redundant and requires as little human intervention as possible. An apparent solution to these constraints lies in large arrays of passive electromagnetic, optical, chemical, and biological sensors. These can be used to identify and track targets, and can also serve as a first line of detection for various types of attacks. Such networks can also support the movement of unmanned, robotic vehicles.

Sensor arrays could be rapidly deployed at the site of the accident and used to track heat, natural gas and toxic substances. Acoustic sensors could be used to detect and locate trapped survivors. The collapse of bridges, walkways, and balconies could be predicted in advance using stress and motion sensors built into the structures from the outset. By inserting a large number of low-cost low-power sensors directly into the concrete before it is poured, material fatigue could be detected and tracked. The sensors may be averted through the use of ultra-small energy-harvesting radios [1].

Wireless magnetic sensor nodes can provide information about speed and direction of traffic, quantity of vehicles per time on a stretch of pavement or just reliable presence or absence of a class of vehicles. They usually use the disturbance of the magnetic field of the earth in order to determine the presence or absence of a vehicle. Most commonly used sensors are Anisotropic Magneto-Resistive (AMR) sensors. Fig. 3 shows graphical example of the lines of flux from the earth between the magnetic poles and the bending they receive as they penetrate a typical vehicle with ferrous metals.

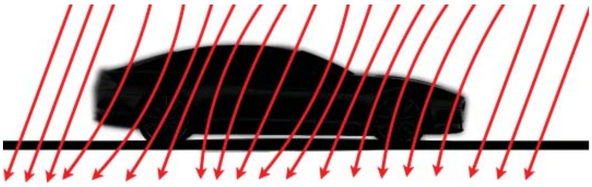

Fig. 3 Earth’s magnetic field through a vehicle

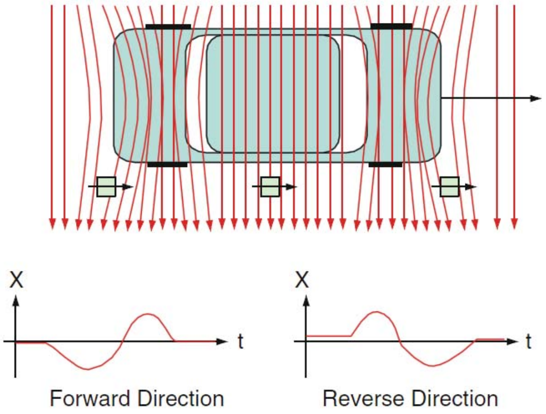

Fig. 4 Vehicle detection signature

As vehicle come near the sensor, there is a shift from the earth’s magnetic field levels. The natural earth’s magnetic field would bias the sensors with a slight negative voltage output, increasing flux concentration would further lower the voltage and decreasing concentration would raise the voltage, Fig. 4 [4].

7. Conclusion

This paper introduces the main categories of routing protocols and data dissemination strategies and describes the main functions of the network layer. The paper provides a brief overview of commonly used routing metrics. Also is presented comprehensive list of wireless sensor networking examples.

Acknowledgement

This investigation has been carried out in the framework of the research project № 122ПД0041-07.

References:

[1] A. Goldsmith, *Wireless communications*, Cambridge University Press, 2005.

[2] A. Nayak, I. Stojmenovic, Eds., *Wireless sensor and actuator networks*, John Wiley & Sons, Inc., 2010.

[3] C. Raghavendra, K. Sivalingam, T. Znati, Eds., *Wireless sensor networks*, Kluwer Academic Publishers, 2004.

[4] L. Gavrilovska *et al.*, Eds. *Application and multidisciplinary aspects of wireless sensor networks*, Springer, 2011.

[5] M. Ilyas, I. Mahgoub, Eds., *Handbook of sensor networks: compact wireless and wired sensing systems*, CRC Press LLC, 2005.

[6] P. Santi, *Topology control in wireless ad hoc and sensor networks*, John Wiley & Sons Ltd, 2005.

[7] S. Farahani, *ZigBee wireless networks and transceivers*, Newnes, 2008.

[8] W. Dargie, C. Poellabauer. *Fundamentals of wireless sensor networks*, John Wiley & Sons Ltd., 2010.

[9] Z. Shelby, C. Bormann, *6LoWPAN: the wireless embedded Internet*, John Wiley & Sons Ltd, 2009.