INFORMATION ROUTING IN WIRELESS SENSOR NETWORKS

Popa Ionut-Alin, *PhD Student University of Petrosani*
Pop Emil *PhD Prof. Eng. at University of Petrosani University of Petrosani*

ABSTRACT: *Choosing energy-efficient communication uni-destination and major arrival destination in a wireless sensor network is a crucial task optimization and evolution of her appeals to many different disciplines of knowledge. Both the design and evaluation of their car algorithms are challenging task requiring a lot of care in selecting appropriate assumptions and principles but worth solving algorithms due to the extension of the life span of the system.*

KEYWORDS*: algorithms, routing, wireless networks, routing protocols, metrics, flooding.*

1. INTRODUCTION

Routing consists of the transmission of information over a network from a source to a destination. Along the path travelled, is met at least an intermediate node. Routing is often contrasted with the function of bridge that apparently achieves the same thing. The main difference between the two is that "bridging" (switching) takes place within the level 2 (Data link layer) of the OSI reference model, while routing takes place at level 3 (network layer). This difference lies in the use of different information for routing and bridging information, necessary in the process of forwarding packets from source to destination, so these 2 functions to fulfil roles in different ways.

A router has 2 or more communications interfaces (Figure 1), or IP subnets connected to lines of type point-to-point. However, there is at least one physical interface. Submitting a OSI-IP requires in general as a router to choose the interface and the address of the next router (next-hop) or (in the case of the last router on the path), the destination host. This choice, (also called "relaying") is based on a database that is located on a router containing routes. This database is called the routing table. It is also referred as the "router" is derived from the way it builds this database contains routes (routes); routing protocols and configuration are interfacing under a process called routing.

Security of data transfers is given in Internet protocols and transport level i.e. Transmission Control Protocol (TCP), which provides relay between source and destination, the segmentation and the control connection. Services that do not rely on transport-level connection are provided by the User Datagram Protocol (UDP).

A routing protocol components are:

Data structures -some routing protocols using tables and/or data base for its operations. This information is kept in RAM.

The Algorithm - an algorithm is a finite list of steps used in accomplishing a task. Routing protocols using routing algorithms in order to facilitate routing information and to determine the most optimal way.

Mail routing protocols -routing protocols use different kinds of messages to discover neighboring routers to update routing information, as well as other tasks to learn and maintain accurate information about your network.

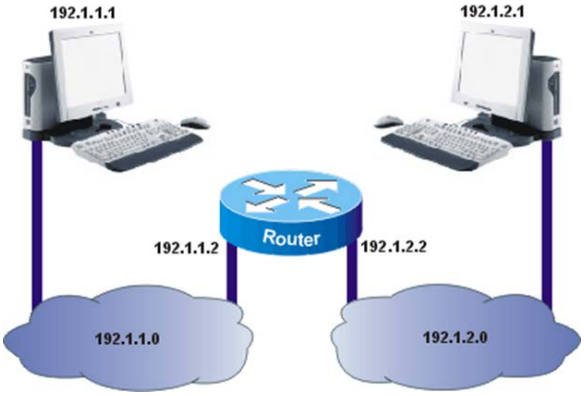

Fig. 1 interconnect with the stations through a router

On the basis of the Protocol of distance vector-based algorithm is. The algorithm is used to calculate the best route and then send this information to the neighbors. An algorithm is a procedure for accomplishing a particular task, starting from a given initial state and ends in a defined end-state. Various routing protocols uses algorithms to install various routes in the routing table, send updates to the neighbors, and to make decisions for the determination of the optimal path.

The algorithm used for routing defines the following processes:

- The mechanism for sending and receiving routing information.
- The mechanism for calculating the best path in paths and installing routing table.
- The mechanism of detection and reactionary to changes in topology.

An autonomous system (AS) is a network consisting of a collection of subnets (with attached hosts) interconnected by a set of routers. It's preferable that subnets and routers to be under the control of a single organization that carries out the operation and administration of the. In an autonomous system routers can use one or more internal routing protocols, and sometimes several sets of metrics. It is expected that an autonomic system must have a coherent internal routing plan. An autonomous system is identified with an autonomous system number.

There are two major types types of routing: static routing and dynamic routing. Static routing describes a system that routes into a data network based on fixed routes. Dynamic routing dynamically builds routing tables, based on the information carried by protocols, network permitted they act almost automatically to avoid errors and bottlenecks in the network. Thanks to its properties, dynamic routing dominates the Internet.

Dynamically routed in a network can grow faster and is able to adapt to changes in the network topology to precisely this growth or errors in one or more components of the network. Dynamic routing also has disadvantages, such as increasing the accomplished. Routing protocols use different metrics to evaluate what is the optimum way to transport a package. A metric ton is a measure, such as bandwidth. For the determination of the road, routing algorithms, initializes and manages routing tables, the information about the routes. The information in these routing tables contain the following destinations and associations "hop" that must be covered in order to reach that destination. When a router receives a packet will try to associate the packet's destination address with an address of a next hop for that destination path, if it fails will likely destroy the package. The figure below describes a scenario of the next hop.

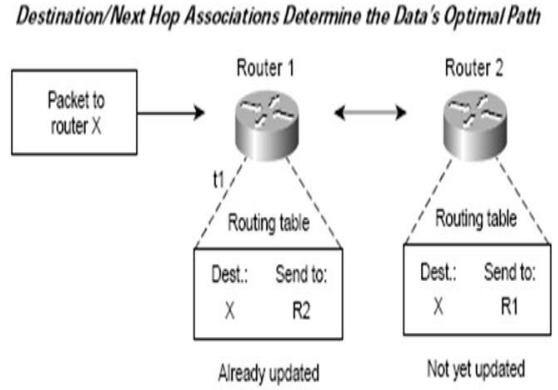

Fig. 2 the next hop Determination

Metrics.

The metric is the number of intermediate nodes ("hop-ups") through which they browse a packet from a source node to a destination node.

Routing algorithms for determining metrics using the various optimal route.

Types of metrics

- Length of road (length path). It is the most widely used metric. It is usually the sum of the cost of the road.
- Safety (reliability). Error rate, how fast to restore the fallen (B.E.R.)
- Delay (delay). How long to get a packet from a source to a destination. Depends on the bandwidth, congestion, physical distance travelled.
- Band width (bandwidth). How much traffic can bear a link.
- Loading (load). Refers to the degree to which a network resource is used, for example a router.
- Communication cost (communication cost). It is especially important that companies can use own lines (low cost) versus using other lines (perhaps a higher cost).

Routing protocols:

The best known are: routing protocols:

- Routing Information Protocol (RIP);
- Interior Gateway Routing Protocol (IGRP);
- Enhanced Interior Gateway Routing Protocol (IGRP Enhanced);
- Open Shortest Path First (OSPF);
- Intermediate System to Intermediate System (IS-IS);
- Border Gateway Protocol (BGP);
- Exterior Gateway Protocol (EGP);
- Simple Multicast Routing Protocol (SMRP);
- Novell RIP/Service Advertisement Protocol (SAP).

2. GOSSIP TRANSMISSION AND RELAYING THE UNI-DESTINATION BASED ON AGENT

Whenever a source node cannot send packets directly (without intermediaries) to destination node and must rely on the help of the intermediate nodes to retransmit these packages in his name, is called a network multi-jump.

In such a network intermediary node must decide which nearby node will forward the package received so that he can get with a given probability at destination.

The simplest way is to flood the network, that is to send the message that all neighbors. As long as the source and the destination nodes are in the same group of interconnected components of the network package will certainly get to the destination. To avoid endless circulation (in the loop) to a node will retransmit packets only packets that we received for the first time, these containing a period and expiration to avoid spread of aimless of the package (where there are no roads to the major arrival destination node horses.

An alternative to relaying the package to all neighbors is the one through which the packet is retransmitted by a single knob arbitrarily chosen, witch will forward the "gossip" (to choose a single recipient) makes the package to cross at random in the hope that the network will eventually reach their destination.

Flooding it is a technique which can be used also for routing in sensor networks. This technique consists in the fact that each node that receives data packets or administrative packages make a broadcast with them until a maximum number of bumpy is achieved for that package or until the package destination is right rule node. Flooding is a technique of reactive and does not require costly maintenance of topology or complex

algorithms for finding routes. Various mechanisms have been created which limit the multiplication of packages through the process of flooding of the outputs:

Limiting the road network. Source inserted into the package label information metering, which represents the maximum number of hops (nodes traversed) that can be performed within the network. This outline will be decrement at each transit packet suffered a node on the route to the destination. When the meter becomes invalid, the package is destroyed.

Ideally, the counter is initialized with the length of the road between source and destination (expressed in number of jumps known and possibly with the help of teach in lathe algorithm). If the source does not know how big this is long, then the meter can be initiated for worst-case: distance most of the network.

To prevent critical situations is necessary to keep an obvious has received packets, to be able to remove the copies.

Verification of identity of packages received. Every sequentially numbered source packages that you enter in the network. In addition, each node can build lists for each source, containing numbers already received packages. If a package is included on such a list, then it will be destroyed.

Because the lists don't grow indefinitely, each of them must be associated with a counter k. States that Count all packets with a number sequentially under k have already been received, so the full list of them is no longer necessary.

Selective Flooding. Transit Node cannot send a package on any line of the output, but only those who "lead" in the direction of some good package. The method can be applied only in the case of networks with a regular structure; a package arrived from the West is geared towards East of the network.

Random Routing. Direction about the transit node randomly selects a single output (using different trails; higher is very robust algorithm).

Flooding is not a practical method for any application. For the military it networks provide an increased guarantee of maintaining communications, if we think that in conflict situations at any moment the optimal routes may be "destroyed" and exactly when maintaining links is particularly important. Flooding also is recommended for applications distributed database, where it is necessary to update all data sometimes competing. Perhaps the most important use of flooding algorithm is to provide a measure of comparison with other algorithms: flooding at the path most choose short of several parallel ways.

Gossiping is a derivation of flooding in which nodes are not broadcast but also send the message to one of my neighbors chose randomly. So once the sensor node receives a message he selects at random one of its neighbors and sends the message. Although this protocol eliminates the problem of implosion, every node is just a copy of the message is needed more time to spread the message through the network flooded . Another consideration is the possibilities database as an agent "running" through the network looking for destination. In the simplest form, the result is completely random and is obtainable by relaying to a random neighbor arbitrarily. Therefore agents are transferred to uni-destination to their next jump. To shorten the time in which they reach destination through parallelism, the source can inject the most agents in the network. Probabilistic properties of random paths have been studied extensively. It was found that without some additional measures a total random little efficient to be useful in WSN.

Protocols for information in sensor networks based on negotiation (SPIN)

A family of protocols called adaptive SPIN are designed to meet the flooding through classic deficiencies negotiation and adjustment of resources. This family of protocols is based on two ideas:

- sensor nodes works more efficiently and conserve energy by sending data that describe the vertex data sensors instead of sending all the information.
- the sensors must monitor changes in terms of energy resources.

SPIN has three types of messages: ADV, REQ and DATA. Before you forward the message DATE sensor makes a broadcast with a message containing a descriptor ADV called meta-data (message DATA description). If a neighbor is interested in the data, sends a message of type REQ (request for information) and is sent the message DATE. Below this node neighbor makes a broadcast message Adv. resulting in each node in the network who is interested will have a copy of the data. Note that the SPIN is based on addressing data-centric network nodes that do a broadcast with a commercial data and waits to send a request for data.

So SPIN help efficient distribution of information in a network of sensors with constraints in terms of energy. Nodes running the SPIN attribute name data using high level descriptors are called meta descriptors. To use negotiation to eliminate redundant transmission of data through the network. In addition, nodes that use SPIN take decisions both in terms of communication systems and depending on available resources. We have in this family 4 specific protocols: SPIN-SPIN and PP-EC optimized for networks point to point and SPIN-BC and SPIN-RL-type networks optimized for broadcast.

Routing algorithms with sequential assignment (SAR)

SAR is a set of algorithms with which operations are carried out by the Organization and management in sensor networks. SMACS is a protocol for self-organization allowing a group of sensors to discover neighbors and to establish regular sessions of transmission/reception without requiring a central administration unit. SAR algorithms create many trees where the root of each tree is a node located just a hop away from the sink. Every tree grows from the sink to the sensor network nodes with avoiding small energy resources. At the end of these procedures most nodes belong to several trees. This allows a sensor node to choose a tree to send information to the sink.

LEACH (Low energy Adaptive Clustering Hierarchy)

LEACH is a protocol based on clusters of nodes that minimizes the energy dispersed networks of sensors.

The role of this algorithm is to randomly select group leaders so that the energy dissipation during communication with the base is common to all nodes in the network sensor. The mode of operation of LEACH is divided into two phases:

Setup phase: In this phase each sensor node chooses a random number between 0 and 1. If this number is less than a threshold T sensor is considered a leader of the group. After group leaders are selected, they notify the other sensor nodes as they are the new leaders of the group.Once the sensor nodes receive the announcement, they determine the group to which they belong on the basis of received signal power ad. The sensors node then informs the group leader will be chosen as a member of the Group and the group leader assigns them a slot in which nodes can send information to leaders of the group. This approach is a TDMA.

Action phase: In this phase the sensor nodes may begin to detect and transmit information to leaders of the group. They gathered information from nodes of their group before sending them to the base. After a certain period of time spent in this phase the network enter in the setup phase and into another round of selection of leaders of the group.

Direct diffusion

Direct diffusion refers to a paradigm of dissemination and coordination based on addressing data-centric data collected for distribution to the user. User queries or tasks are inserted as descriptive interest messages through a sink node. For example, Type = animal with four legs; interval = 40 ms, duration = 20s. The distance between the sink and the destination through broadcast. While browsing the network is create gradients in order to keep information about the source and destination nodes. When the query has reached its destination and the information is available it is sent on the same way by using the information in the sink node gradients.

This method is predetermined electrical nodes and consume time by selecting new ways to send end-user query.

Rumor routing

The main idea of the rumor-based routing is to use agents to create pathways to every event that occurs. Agencies are actually posts with life time that passes through the network. Later queries can follow these paths generated by agents.

Each node in the network maintains a list of its neighbors and an events table with routing information to all known events. When the network goes into operation next list is created through a broadcast, and by listening to the broadcast of other nodes. If the events are needed only a certain time or event table size is limited, you can add labels for events that are added to your tables.

AFS (Adaptive Forwarding Schemes)

AFS is a method of making a scheme of service differentiation. For this purpose it will present a model of service differentiation for networks of sensors. Source knows the degree of importance of each packet you send what you can easily translate into predefined priority levels. This establishes the PHB (priority level) for each packet. Other sensors will pick up the package and will decide the type of service they will provide a package depending on the level or priority. This type of model is highly scalable because regardless of the number of sensors, a node has to do with only one package at a time.

You will define three approaches to provide the guarantee that the package has arrived at the destination:

- Confirmation
- Redundancy packages will be sent multiple copies of packages
- FEC (forward error correcting): error correction codes.

The approach based on redundancy packages is done, as well as in the figure below, in the following ways:

- Multipath forwarding: use the advantage as wireless environment is broadcast, all neighboring nodes can listen to the environment. So although it is a single next hop based on the algorithm used, multiple nodes may forward the package.
- Multipacket forwarding: a single node forwards the package. Redundancy is the fact that the package is sent multiple times.
- Hybrid transmission: it is a combination of the first two methods e. It fixes a minimum number of horses that have sent the package, and if a node has this minimum forward package more than once on the same path for compensation.

GAF (Geographic Adaptive Fidelity)

- This protocol is based on the idea of creating a virtual grid based on location information.
- Performance similar to a routing protocol in ad hoc networks are common but with a plus in terms of conserving energy.
- A protocol is dependent on the application and require improvements in terms of the estimated time of activity nodes.
- It is applicable to both mobile networks and stationary, but the performances are better in the stationary.

Mode of operation:

- a node is active for Your time;
- with this time is made a broadcast to the other nodes in the grid;
- idle time of a node is adjusted depending on Your;
- during the discovery of the network each node makes a broadcast with a discovery message periodically at intervals of time Td.

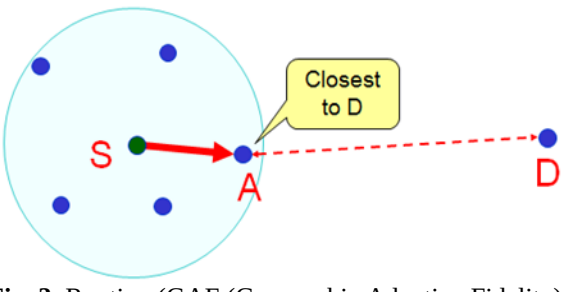

Fig. 3. Routing (GAF (Geographic Adaptive Fidelity)

3. DISTRIBUTION AND TRANSMISSION MULTI-DESTINATION. GEOGRAPHIC ROUTING. ROUTING AND ROUTING PROTOCOLS IN AD HOC NETWORKS

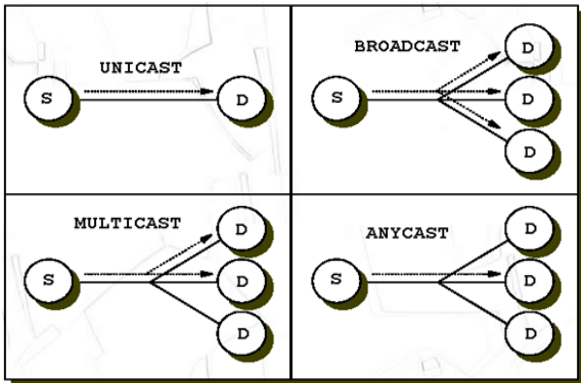

Fig. 4. Broadcast Routing. Multicast Routing. Anycast Routing. **Broadcast**

In some applications the host nodes need to send messages to multiple or all other host nodes. Simultaneous sending of a package to all destinations is called broadcast (broadcast) it several ways for its realization were proposed.

A broadcast method which has no special requirements for the subnetwork is the source to send a package to each distinct destination. The method is not only time consuming bandwidth, but it requires the source to have a complete list of all destinations. It might be that in practice it is the only method used, but it is less the desired method.

Multicast

Sending a message to such a group is called multicasting, and associated routing algorithm is called routing multicast (multicast routing). In this section, we will describe a way to realize the management of multi-cast.

Multicast routing requires the management of the group. There must be ways to create and destroy groups and to allow processes to get into groups or to leave. How to complete these functions it is not routing algorithm. Important for routing algorithm is that when a process to attach to a group he must inform the host about it. It is important that routers to know which groups you belong to the associated host computers. The host computers must be joined to the router to announce any changes in the composition of the groups, either the router must query the host computers on a regular basis. In both cases, the groups find router belong to the host computers. Informs its neighbours routers, such as information propagates through the subnetwork.

In order to achieve routing multicast, each router computes tree cover that covers all other routers on the network.

When a process sends a packet to a multicast group, the router examines its first shaft coating eliminating all lines that do not lead to host computers, which are members of the group.

There are several possible ways of cutback tree coverage. The easiest may be used if they constraint-based routing uses URIs and status of each router knows the entire topology the subnet, appurtenance including host computers to groups, the shaft can be clipped starting at the end of each horse, going towards the root and eliminating routers that do not belong to that group.

When using routing, distance vectors, can be applied to another strategy of the cutback of the tree. The algorithm used is sending on the reverse. Anyway, whenever a router without a host computer in a specific workgroup and without any connection to the other routers receives a multicast message for that group he will respond with a message plums (cutback), announcing the sender not to send more messages for that multicast group. When a router that does not have the host computer no member of any group receives such messages on all its lines, he can also respond with a PRUNE message.

A potential disadvantage of this algorithm is that it acts in case of extensive networks to be ineffective. Suppose that a network has groups, each with an average number of members. For each group, you should memorize m trees covering a total of cutting m trees. If there are many large groups, then, to save all the trees, you need a memory space considerably.

In order to transmit multicast is needed so the infrastructure layer 3 multicast, as well as support from the application level.

Nowadays the most known multicast routing protocols are: Protocol Independent Multicast Dense Mode (PIM-DM), Protocol Independent Multicast Sparse Mode (PIM-SM) Multicast OSPF (MOSPF), Distance Vector Multicast Routing Protocol (DVMRP). PIM-SM between them and PIM-DM lead comfortably in the top of the popularity, being neither DVMRP and MOSPF even fully supported on Cisco routers.

Ad hoc networks are dynamic, mobile networks that do not require a fixed architecture or configuration processes. Implementation of such networks represent a particular direction in moving new generations of communication. How an interest for such networks grows by the day, needed and a performance increase. Ad hoc network performance is determined mainly by the way in which routing protocols are communication. It requires dynamic routing protocols, fast, to cope with frequent topology changes successfully.

Types of ad hoc Networks

Ad hoc networks can be classified into many types depending on the applications in which they are used:

- Mobile ad hoc networking (MANET — Mobile Ad-hoc NETworks).
- Wireless mesh network (WMN-Wireless Mesh NETworks).
- Wireless sensor networks (WSN-Wireless Sensor NETworks).
- Mobile ad-hoc networks (MANET).

A mobile ad hoc network (MANET) is a decentralized network of mobile devices moving independently in any direction, therefore they will

change frequently the connections with other devices on the network. Mobile ad-hoc networks can be implemented with various wireless technologies such as 802.11/WiFi standard, cellular or satellite transmission. The main challenge in building a MANET is equipping each device so that you maintain at all times the information necessary to route traffic appropriately.

Ad hoc networks (MANET) mobile fall into three categories:

- Vehicular ad hoc Networks (VANET): are used for communication between vehicles and equipments installed at the side of the road.
- Vehicular ad hoc networks, intelligent (InVANET): I'm a kind of artificial intelligence, which helps vehicles to behave intelligently during vehicle-vehicle collisions, crashes, etc.
- Ad-hoc mobile Networks based on the Internet (iMANET): this type of network connects mobile devices within the MANET and the Internet unite.

Wireless mesh network (WMN)

A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology (mesh). A mesh network is reliable and offers redundancy. When a node can no longer work, the remaining nodes can still communicate with each other, either directly or through intermediate nodes.

In ad hoc networks, there are no fixed base stations, DCF module being used. The operating principle of the DCF method consists in listening environment to see if another station will emit. The station must ensure that the environment is free for a certain duration before the issue. If the medium is free during this time, the source can begin issuing the data otherwise the transmission is deferred for a period of time chosen at random, after which the station will retry to transmit in. However, if at least two stations broadcast simultaneously, a collision may occur which unfortunately cannot be detected by the sending station. For this situation to use a "prompt" (ACK-: update) with the purpose of informing the issuing station that has been successfully received the frame. The sending station sends a short message first RTS (Request To Send) containing the destination and the duration of the transmission. If the destination is free, allows the source to send a short message by issuing the CTS (Clear To Send) that indicates the source that can start to emit the data without the risk of a collision.

The characteristics of ad hoc networks are as follows:

- Mobility: the location of the network in areas where there is no fixed infrastructure. We can have random individual mobility, mobility group, movement along the pre-planned routes etc.
- Boundary type: network is a network in which a data packet sent from source through a number of intermediary nodes to reach the destination.
- Self-organization: the ad hoc network must determine independently its own configuration parameters such as: addressing, routing, identification, position control of power etc.
- -Energy conservation: most ad hoc nodes (for example, laptops, PDAs, sensors etc.) have a limited food and not having the ability to generate their own energy (e.g., solar panels). An efficient protocol for energy conservation (e.g. resource discovery, routing, etc.) is essential for the longevity of the mission.
- -Scalability: in some applications a ad hoc network can reach several thousand nodes, this feature proved to be quite problematic. For a wireless network scalability is simple to manipulate using a hierarchical structure.
- -Security: wireless Networks are somewhat less secure than wired ones, due to easier access to the network of authorized persons within the coverage areas of access points. There is implicit in the implementation of different barriers in wireless networks which form the so-called basic security to wireless networks, which prevent the access of foreigners to unintentionally network in range of an access point.
- -Internet connection: ad hoc Networks can be configured so that it can communicate with external networks that have connection to the Internet, such as wireless local area networks, through transitional devices. An example of such a piece is the router.

In ad-hoc networks, routing protocols can be divided into three categories: proactive routing protocols, routing protocols, and reactive hybrid routing protocols:

- Proactive Routing Protocols offer good performance in quick find the route and are based on the routing table. The advantage of this type of protocol routed is that, after the establishment of the routes, they will always be available and have the disadvantage of network overload due to traffic control.
- Reactive routing protocols are set out in the application, they do not regularly update its routing table and does not have a permanent routing table. The main disadvantage of using a reactive protocol is to flood the network with messages sent by the equipment that they have no possibility to communicate with the equipment requested.

Proactive routing protocols

Proactive routing protocols are also called the "table-driven" i.e. each node can build single routing table through the exchange of information between nodes on the network. This is achieved by the exchange of messages to update on a regular basis between nodes to maintain the routing table of each updated node. Then, when it initiates a transmission source node shall consult its own routing table where the routing information is no longer required to seek information about the destination, thus avoiding the delays caused by such processes.

There are two major types of routing protocols used in the Internet: based on distance vectors (e.g. RIP, EIGRP) or based on the State of the link (e.g., OSPF), both being proactive protocols. However, these protocols are not suitable for ad-hoc mobile networks that have limited resources due to high spending money and low convergence. Routing algorithm based on vector distance, also called Bellman-Ford, used as criteria for selecting the optimal route between nodes

(metric). The metric is the number of intermediate nodes ("hop-ups") through which they browse a packet from a source node to a destination node. The nodes of a network passed on a regular basis, this routing table for each node with which they are directly connected. These nodes are updated their own routing tables if necessary, after which in turn will send them their own routing tables other nodes on the network directly connected. This makes that the metric information to propagate throughout the network, so that, in the end, each node should have information on all the nodes in the entire network. Routing protocols based on distance vectors are somewhat limited in the ability of choosing the best routes. Their main advantage lies in its simplicity and their long-standing use. In recent years, many efforts have been made to adapt the Bellman-Ford algorithm in ad hoc networks, a common solution in ad hoc networks being DSDV Protocol (Destination-Sequenced Distance-Vector).

Routing algorithm "with Dynamic Distance Vector Orderly" or DSDV (Dynamic Destination Sequenced Distance Vector) was one of the oldest protocols developed by C. Perkins and P. Bhagwat for ad-hoc networks. The main objective of designing of DSDV was to develop a protocol that preserves the simplicity of RIP routing protocol based on the idea of distributed Bellman-Ford who was introduce some improvements.

DSDV Protocol is based on a transfer of control messages between routers (or nodes) in the network. In this type of messages can be found all over the routing table on each node holds. Control traffic is sent using either a layer 2 MAC address or a layer 3 address (IP). The algorithms based on the status of select optimal route based on dynamic use of the method of the shortest route (Shortest Path First). Each node shall maintain a "map" describing the current topology of the network. This map is updated regularly by testing the possibility to access different parts of the network and by exchanging information with other routers. Determine the best routes (shortest path) can be made on the basis of different metrics that indicate the true cost of sending a datagram on a particular route. The algorithms based on connection state are much stronger than those based on distance vectors. They dynamically adjust when topology changes occur in the network and also allow selecting routes based on the metrics more real than the number of hop, but are more complicated to install and use multiple resources for processing than those based on distance vectors

Proactive routing protocols combine principles of algorithms based on distance vectors and algorithms based on the State of ties, trying an adaptation in the framework of ad-hoc networks.

Reactive routing protocols

Routing protocols are called reactive and on-demand routing protocols ("on demand"), the routing process must discover a path whenever a packet from a source and must reach a destination. Here the nodes do not have a pre-defined routing table built (or other information about other nodes in the network) on the basis of which they can make decisions of knowledge.

In a reactive network discovery process of routes happens more often, Exchange messages with hop hop is made, the source of the flooding the network with messages for the route, but this process requires a low-traffic control in comparison with proactive routing. When the communication between the source and destination node node ends, the route is deleted from the routing table of the participating devices. Therefore, a reactive routing is considered to be more scalable than a proactive one. In addition, when a node tries to send a message using a type of reactive routing it must wait for the discovery of the path where you will be sent the information to end, therefore overall delaying will increase.

Hybrid protocols

Hybrid protocols combines the features of proactive and reactive, with the primary purpose of using the advantages of these two kinds of protocols. This type of network is divided into areas which are proactive and protocols used in exterior nonreactive protocols. Among the best known hybrid protocols may be listed ZRP (ZoneRouting Protocol) and ZHLS (Zone based Hierarhical Link State routing).

AODV Routing protocols

AODV Routing Protocol ("Ad Hoc Ondemand Distance Vector") or "Distance Vector routing request" was designed to improve the performance of DSDV routing protocol and to reduce the number of broadcast messages and latent in the transmission, problems common to routing protocols based on distance vectors. Routing Protocol of AODV routing protocol is a reactive, therefore the routes are determined only when needed, for example routing process must find a path whenever a packet from a source and must reach a destination. In order to detect and monitor the neighboring nodes of routing protocol of AODV requires more techniques, one of the most used being the exchange of messages with a “hello”. If the messages are "hello", each active node will periodically broadcast by all his neighbors a message of type “hello”. If a node no longer receives a message of type “hello” from its peer, then it means that the connection failed. The routing table of the neighboring node is being organized to optimize response time when topology changes and provide a very quick response applications for establishing new routes.

Routing Protocol TORA-Temporally Ordered Routing Algorithm

Temporally Ordered routing algorithm or the TORAH was intended primarily to minimize the effect of change of topology that are common in ad hoc networks. The algorithm adapts to the mobility of these environments by storing multiple horses to the same destination, which makes many of the topology changes to have a minor impact on 600,000.

A concept that underlies the design of his is that control messages generally involves a small number of nodes. Saving horses from a pair (source, destination) time, not carried out in permanent manner. Paths are created and stored according to need, as is the case for all protocols from this category. Optimization of secondary importance roads, long paths can be used in

order to avoid the development of a new process of discovery of new routes.

The TORAH makes no guarantees that the route does not present loops (temporary loops might however shape), and generally provide more routes for a source-destination pair. This protocol provides the routing mechanism only, and depends on the IMEP (Internet MANET Encapsulation Protocol) for other functions. The TORAH can be separated into three main functions: creating paths, maintain links, and delete links. Creating routes is based on assigning directions links, whether in a network (or network closure), building a directed graph (DAG) with the destination root directory.

The TORAH assigns a grade to each node in the network. All messages within the network runs from a junction with the higher rank to a node with the lower rank. The routes are discovered packages of type using Query or Update. When a node without links below require a link to the destination, it will broadcast a Query packet. QRY package will move over the network until it reaches a node that has a route to the destination, or even at your destination. That node will broadcast a package Update that contains the node. Any node receiving this package will set the level at a higher value than the node package. The node will then broadcast your own package UPD. The procedure will lead to the creation of a number of direct source-destination.

DSR routing protocol

The DSR (Dynamic source routing) is based on the use of the source routing. In this technique the source determines the sequence of nodes through which data packets will be sent. Before sending the package data to another node, the transmitter broadcasts a RREQ packet (Request Route). If the operation of route discovery is successful, the broadcaster will get a RREP (Response Route) which contains a sequence of nodes through which one can reach the destination. RREQ packet contains a record of the routes, which will be accumulated in the sequence of vertices visited during propagation of the query in the grid. The use of the source routing allows sending of data packets without transit nodes to need to keep the information updated.

Asymmetric Routing.

There are many cases where the assumption of symmetry relations between neighboring nodes may not be valid. In such networks presents an advantage and AODV is an extension of the package that includes the list of Hello known neighbours of that node. If a node receives a message Hello, but that does not contain the IP address, then realizes that with this knot is 1-way and you don't have to send any packet the node in question. Asymmetric routing poses serious problems in translating an IP address into a MAC address (so 2). Because the ARP (Address Resolution Protocol), the Protocol establishes correspondences between IP addresses and MAC addresses, presupposes the existence of a bidirectional, reliable connectivity through and in the case of asymmetric resolution of 600,000 addresses must be laid down after the special algorithms. However, it is important to establish asymmetric routes and AODV seeks to be configured to provide this functionality.

In order to promote ties by disabling the asymmetrical and symmetrical, a strategy is required for notification. Each node that receives the RREP sent a package and then a RREP-ACK (acknowledgement of receipt of the package) back to the node that sent the package initially. If a node receives the RREP, then know that the link is bidirectional because the RREP in response to demand for the route, and the confirmation package RREP-ACK, bidirectional to the next node is guaranteed.

4. CONCLUSIONS

Can be drawn such conclusions about the algorithms and data-routing techniques in wireless sensor networks:

- The studies are focused in particular on the vast majority of cases, in particular networks of organized clusters
- Most of the algorithms consider protocols that carry them, and lower-level MAC protocols do not a penalty and that the real time.
- Validation techniques and algorithms is done using simulators ignoring strong real situations.
- In many cases it is considered that the network is fixed and mobile nodes are not accurately known position of the nodes. These assumptions significantly reduce the degree of applicability of sensor networks.
- The studies are focused largely on reducing energy consumption, the nodes of a network of wireless sensors are battery powered.
- Shall not be granted in many cases greater importance to situations with strict time requirements. These situations can be encountered in significant networks of sensors, with the role of monitoring and control of the environment in which they are located, an application with clear real time requirements.
- The few studies related to real time communication-oriented are real-time statistics and less on guaranteed communication.

5. REFERENCES

[1] K. Holger, A. Willig "Protocols and Architectures for Wireless Sensor Networks". JohnWiley & Sons, 2012.

[2] Nirupama Bulusu, Sanjay Jha "Wireless Sensor Networks", ArtechHouse 2005.

[3] Capkun, M. Hansen, and J.-P. Hubaux. "GPS-free positioning in mobile ad-hoc networks". In proc. HICSS, 34th volume of 9, page 9008, 2001.

[4] J. Kay, J. Frolik "Analysis and QoS Control for Wireless Sensor Networks", IEEE 2004.

[5] Mohamed Younis, Akkaya Kemal "Energy and QoS aware Routing in Wireless Sensor Networks".

[6] Mohamed Eltoweissy, Wadaa Ashraf, Akkaya Kemal, Mohamed Younis, "On QoS handling Traffic in Wireless Sensor Networks", Proceedings of the 37th Hawaii International Conference on System Sciences, 2004.