Monitoring a Grid of Sensors by Performance Metrics for Internet of Things Applications

Carolina Del-Valle-Soto, Jafet Rodriguez

Universidad Panamericana, Facultad de Ingenieria,
Jalisco, Mexico.
Email: cvalle@up.edu.mx, arodrig@up.edu.mx

Carlos Mex-Perera

ITAM,
Ciudad de Mexico, Mexico
Email: jorge.mex@itam.mx

***Abstract*—A sensor network is composed of nodes which collaborate in a common task. These nodes have certain sensory capabilities and wireless communication that allow forming ad-hoc networks, i.e., no pre-established physical structure or central administration is necessary. Therefore, one of the main problems with ad-hoc systems is that there is no existing infrastructure, so the routes change dynamically. This is due to fading, interference, disconnection of nodes, obstacles, node movements, and so on. We expose an analysis of the Multi-Parent Hierarchical (MPH) routing protocol for wireless sensor networks, which has low overhead, reduced latency and low energy consumption. Network performance simulations of the MPH routing protocol are carried out and compared with two popular protocols, Ad-hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR) and the well-known algorithm Zigbee Tree Routing (ZTR). The combination of a hierarchical topology with self-configuration and maintenance mechanisms of the MPH protocol makes nodes optimize network processes, reduce delays, take short routes to the destination and decrease network overhead. All this is reflected in the successful delivery of information.**

Keywords–Wireless Sensor Networks; Energy Consumption; Performance Metrics; Routing Protocol; Internet of Things.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are based on low-cost devices (nodes) that are able to get information from their environment, process it locally, and communicate via wireless links to a central coordinator node. Additionally, the coordinator node might also send control commands to the nodes [1]. WSNs may not rely on a predetermined structure and require the capacity of self-organization in order to deal with communications impairments, mobility and node failures. Moreover, it is important to study the scalability and adaptation methods of the network in the face of topology changes and packet transmission failures in the wireless medium.

In this work, scenarios of wireless sensor networks are proposed under different configurations of topology arrays. The aim is to contrast the performance of the sensor network under three widely known protocols in the literature: AODV [2], DSR [3] and MPH [4]. The latter was designed and implemented by the same authors of this work in the reference cited in [4]. In this study, AODV, DSR, ZTR [5] and MPH are compared based on various efficiency metrics and how they optimize routing protocols through energy. There are several schemes to find the best routes in the shortest possible time. In terms of hierarchy algorithms, such as ZTR, it has a simple and fast routing, which reduces overload in the network, is reliable and has a distributed addressing scheme that does not require nodes to have routing tables. Results from our work show that for the single sink scenario, the MPH protocol has an energy saving of 35% against AODV and DSR protocols and 8% compared with ZTR. MPH has 27% less overhead compared with AODV and DSR. Moreover, MPH presents a 10% increase in packet delivery compared with AODV, DSR and ZTR.

We describe the organization of the rest of the paper. Section 2 introduces the related work on the wireless sensor network problem to an IoT approach. Section 3 proposes the analysis of performance metrics. Section 4 describes and explains the analysis of performance metrics under a grid topology. Furthermore, Section 5 presents the results. Section 6 has the study of sensors as base of Internet of Things. Finally, conclusions are given in Section 7.

II. RELATED WORK

Due to technological advancements, the Internet is being used to share data among different small, resource-constrained devices connected in number of billions to constitute the Internet of Things (IoT). A large amount of data from these devices imposes overhead on the IoT network. Hence, it is required to provide solutions for various network related problems in IoT including routing, energy conservation, congestion, heterogeneity, scalability, reliability, quality of service (QoS) and security to optimally make use of the available network.

One of the most efficient topologies in information delivery is the hierarchical topology [6]. The hierarchy levels allow packet forwarding with the least number of hops, which causes fewer errors in delivery and lower delays in the transmission of a packet from source to destination. Hierarchical protocols have scalability and robustness characteristics, providing energy savings in the network and distributing energy costs among network sensors. A great advantage of such protocols is that they carry information generally to one node, thus the communication with the coordinator or root node is simpler and more efficient [7]. Tree Routing is a classic form of routing that is restricted to parent-child links. This scheme eliminates the need for searching and updating paths and the overhead associated with the establishment of those paths. However, when the networks are large and the nodes can connect and disconnect from the network due to link changing conditions, it is helpful for the Tree Routing scheme to be able to change slightly, offering more flexibility in assigning IP

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-622-4

addresses to the network in order to become self-organized because it is performed using fewer links. In addition, the hierarchical protocols have simple routing algorithms that guarantee efficient delivery of information and increase the lifetime of the network.

A reliable routing protocol in WSNs is essential due to the versatility of these networks. In [8], the authors analyze metrics such as end-to-end path reliability and number of hops. Their work analyzes different routing algorithms based on link reliability models for each type of node. In [9], a routing protocol that guarantees the route with the shortest path while maintaining Quality of Service is designed. The route optimization is related to the ideal relay node position and metrics such as mean end-to-end delay and packet rate under random scenarios are considered [10]. The influence of packet retransmissions in communication and its effects on energy efficiency in the network are analyzed. Some of the most adaptable protocols for this type of networks are AODV and DSR, which are aimed at reducing cost and energy consumption and improving reliability. These protocols allow multi-hopping among the actively involved nodes that want to establish and maintain routes in a network [11]. On the other hand, ZTR, a widely referenced algorithm, has low overhead and is simple with regard to the memory capacity of the nodes since they do not have routing tables, which eliminates path searching and updating. Nevertheless, it has some drawbacks in terms of flexibility and adaptation, especially when it is deployed in wide network environments [5].

III. PERFORMANCE METRICS

Metrics of the network layer are very important because they show the performance and usefulness of a routing protocol. Each routing protocol is designed for specific applications and certain scenarios. These metrics indicate how the use of bandwidth is affected by the overhead of the routing protocol in use. In addition, the availability of effective routes and the ability of the network for self-configuration show the capacity of the protocol to recover from topology changes. Recovery times have an impact on the latency in the network and even though the networks conform with different technologies, it is highly important to understand and evaluate the performance metrics as shown in [12].

A. Optimization of Routes

An important feature in a sensor network is when nodes lose established routes due to mobility or changes in the topology. It is necessary to have a protocol that can find optimal routes and can adapt to network changes. Applications of sensor networks were used by such and such authors to conduct a study about Energy Optimal Routing algorithm in [13] for mining and tunneling approaches, which is very significant in energy savings in sensors due to their long time period in harsh environments unsuitable for constant human access. This algorithm builds routes based on transmission distance and search optimization. Moreover, it employs energy balancing strategy. In [14] Nezhad et al. proposed a Destination Controlled Anonymous Routing Protocol for Sensornets routing protocol for high traffic sensor networks. In this work, the authors propose a collector node capable of having a global view of the whole network topology representing a higher level of hierarchy than the other nodes. In [15], Nasser et al. proposed the Secure and Energy-Efficient multi-path Routing protocol that combines multi-path technique for communication among nodes, as well as safety techniques with respect to malicious attacks to a destination. This protocol is proposed for an environment of static nodes. It stores information in the node routing tables with the routes to a collector node as a final destination. This contributes to a new proposal for the establishment and maintenance of routes.

B. Routing Protocols in WSNs

In communication networks, there are routing protocols classified into two groups: proactive routing protocols and reactive routing protocols. When nodes are under a reactive protocol, they ask for a route only when it is needed. This involves high latency for the first packet and some independence among routes. The AODV routing protocol is based on routing efficiency of wireless ad-hoc networks with a huge number of nodes and it uses a route discovery mechanism in broadcast mode. It is considered as a reactive protocol: the routes are created only when they are needed, on demand. AODV can transmit in unicast or multicast mode. It uses the bandwidth efficiently and responds to the network changes in a very quick mode, preventing network loops [2]. In fact, AODV maintains time-based states in the routing tables of each node. An entry in the routing table expires if it has not been used recently. The timer function is designed to avoid the use of links which the node does not have an updated status from a long time ago. Some advantages of AODV include more reliability and less cost in bandwidth. However, there are some disadvantages, as follows: more complexity and computing, more cost in memory, and this protocol was designed to work in a network where there are no malicious nodes. In conclusion, it is not a secure protocol.

The DSR protocol is a reactive protocol. It routes from source node including a header in the packets. It indicates what nodes will be crossed to arrive at a destination because the origin node is responsible for calculating the complete path to the destination node. This process is called *Source Routing*. Each node in the network has a cache memory which stores all of the obtained routes throughout discovery processes, this could be from the source node or learned from the network. If there is no current route to a specific destination, the node begins a *Route Discovery*. The route table or route cache is constantly monitored to detect broken or invalid routes, in order to repair them, when the network topology has changed. This process is called *Route Maintenance*. DSR protocol presents some advantages; for instance, a node can obtain multiple paths to a specific destination by only requesting for a route. Also, it allows the network to be entirely self-configuring without a particular architecture or topology. Additionally, it is a good election in scenarios where the number of mobile nodes is limited. Furthermore, the protocol adapts itself quickly to routing changes when a node is frequently moving, and finally, this protocol decreases the overhead in the network.

ZTR is a simple protocol which establishes parent-child links and the nodes always carry information to their parent. It has a tree topology and is easy to implement. ZigBee requires that there is at least one full-function device with a more robust nature to act as a network coordinator, but the final nodes can have reduced function in order to reduce costs. The parent node is the one which has given the child access to the

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-622-4

network, so parent-child links are created, but each child can only have one parent. Some of the advantages of ZTR are that in the algorithm implemented in the network layer, there is a balance between cost per unit, battery expense, complexity of implementation to achieve a proper cost-performance relation to the application.

MPH creates a hierarchical network logical topology where the hierarchy of the nodes is given by its location level, which is proactive. It works like a hierarchical tree: nodes establish parent and child links that constitute the possible routes. Node hierarchies are used to establish links between parents and children based on the coverage radius that depends on the transmission power. As a result, a node can share both the children and the parents with another node belonging to the same hierarchical level, which allows more links, but does not generate unnecessary routes, and continues to express speed thanks to the hierarchical topology. This protocol takes advantage of the controlled maintenance of routes of the proactive nature, but combines the agility that allows to have more than one route for a node. This makes it more versatile and adaptable to different topologies.

IV. Analysis of Performance Metrics under a Grid Topology

WSNs consist of a number of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. They are multi-functional, low-cost and low-power networks, and rely on communications among nodes or from sensor nodes to one or more sink nodes. Sink nodes, sometimes called coordinator nodes or root nodes, may be more robust and have larger processing capacity than the other nodes. Sensor networks can be widely used in various environments, sometimes hostile. Some of the many applications of WSNs are in the medical field, agriculture, monitoring and detection, automation and data mining.

The most notable issues regarding WSNs are the difficulty in transmitting information in a wireless environment as well as the energy costs implied. When the signal suffers from physical obstacles, channel occupancy, interference and general fading with other devices, it promotes the use of high energy consuming mechanisms to send and receive packets successfully. These networks have limited resources because of the cost and size of the devices. The sensors are small in order to be adaptable to all kinds of environments and able to be installed in various conditions, locations, and infrastructures. This also causes the batteries to be small and short-lived; thus creating the need to save energy in all processes of the network.

We take into account performance metrics that directly or indirectly influence the energy consumption of a network. The delay may be an indication that packets are not directed on the optimal path, which shows an increase in the number of hops to reach the final destination. When routes are not optimal this brings more energy consumption. When the number of retransmissions is high this may be a consequence of the large number of collisions that are in the channel, and nodes can be strained to bring the information to its destination. The connections and disconnections of nodes make the network topology change constantly. This is why the implemented routing protocol must be able to respond quickly and efficiently to these failures. The availability of routes is a parameter showing the capacity of the routing protocol to maintain current valid routes due to the fact that nodes are constantly asking for routes, increasing the overhead.

V. Results

In this section, we compare the performance of the MPH protocol with that of commonly used protocols in sensor networks, such as AODV, DSR and the well-known algorithm, ZTR. We consider the following important metrics that are indicative of network performance and they are tested under the topology described in Figure 1.

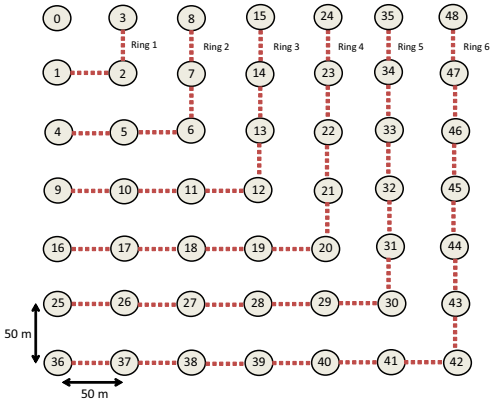

Figure 1. Network topology.

Table I describes the parameters of the simulations.

TABLE I. SIMULATION AND REAL NETWORK PARAMETERS. CARRIER SENSE MULTIPLE ACCESS WITH COLLISION AVOIDANCE (CSMA/CA) [16].

Parameter	Value
Physical Layer Parameters	
Sensitivity threshold receiver	−94 dBm
Transmission power	4.5 dBm
MAC Layer Parameters	
Maximum retransmission number	3
Maximum retry number	5
Maximum number of tries to reach a node from the collector	9
Packet error rate	1%
Average frame length	22 bytes
Maximum number of backoffs	4
MAC protocol	IEEE 802.15.4
MAC layer	CSMA/CA
Network Layer Parameters	
Number of nodes	49
Maximum data rate	250 kbps
Scenario	Static nodes

1) Delay: The time a packet takes to reach its destination is variable due to several factors, for instance: the transmission speed, the packet size and the delay of the packet in each hop in the route. Collisions and packet retransmissions also increase the end-to-end delay. The delay is related to the network complexity. The MPH protocol, through the election of a hierarchical topology, produces a reduction of the delays in the information delivery process.

It is important to consider the delay involved in reorganizing the network due to changes in connectivity, for example, due to new nodes or nodes that switch off or are faulty. Table II shows relevant delays obtained in the simulations of the

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-622-4

MPH protocol compared with AODV, DSR, and ZTR. The first row shows the time required to complete the process of table maintenance performed by a neighbor node. With this process, each node builds its neighbor table. The second row describes the time it takes a packet to travel from the farthest node to the coordinator (these are the nodes of the last ring shown in Figure 1). In the third row, we obtained the time it takes a packet from the nearest ring in Figure 1 (one hop) to get to its destination, for each of the protocols. In the fourth, fifth, sixth, seventh and eighth rows, we randomly turned off 10%, 20%, 30%, 40% and 50% of the network nodes, respectively. We observed how long it takes a packet to reach the coordinator node from the farthest node in the topology. In the ninth row, we define the recovery time for the worst case (50% nodes turned off). This metric takes into account the self-configuring time of the network due to the dynamics of the wireless scenario, such as node disconnections. This is where we see the ability of each routing protocol to overcome topology changes and reorganize the network.

2) Energy consumption: The energy model implemented for the three protocols studied is presented in Table III. When MPH is used, nodes store neighbor tables, and routing is done via the optimal route. Therefore, this protocol provides large energy savings thanks to multi-parent routes. This can be seen in Figure 2a, where we observe that AODV and DSR use more total energy than MPH because they require more routing overhead, which causes more collisions and retransmissions. ZTR does not carry out a discovery mechanism but it has less available links and does not guarantee that those are the shortest routes, so, sometimes it needs more hops.

3) Overhead: Reactive protocols such as AODV and DSR have low overhead because routes are discovered only when they are needed. However, MPH and ZTR use fewer control packets, thus nodes have low processing and simple management of neighbor tables. Therefore, MPH maintains neighbor tables with fewer control packets. ZTR does not need to maintain any table. This behavior can be seen in Figure 2b.

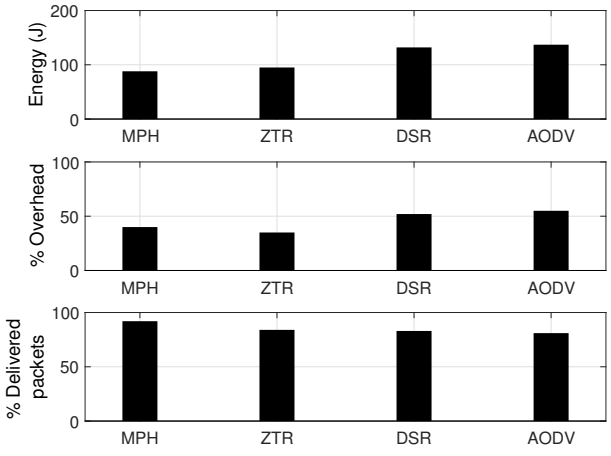

Figure 2. (a) Total energy, (b) Overhead, (c) Packet delivery ratio.

4) Packet delivery ratio: We took a radius of 10 m and analyzed the percentage of delivered packets for AODV, DSR, ZTR and MPH. The value that this metric takes is a consequence of the ability of a routing protocol to reorganize the network. Besides, if the number of hops the packets pass through is smaller, there will be fewer errors in the information delivery. Results are depicted in Figure 2c.

VI. Sensors as base of Internet of Things

Internet of Things (IoT) [17]] allows the possibility of digital interaction among objects, through the Internet, without the intervention of human beings. Thanks to wireless systems, it is possible to integrate a chip of a few millimeters in any object in the home, work or city to process and transmit information from it constantly. One of the biggest challenges of IoT is to have real-time data that are visible to extract valuable information. The goal is to have accurate information to make better decisions by discovering which data is essential through intelligent filtering. In addition, it allows understanding the signals within the data. Thus, organizations can extract and analyze data through the connected IoT ecosystem [18].

Internet of Things is precisely one of the leading areas where sensors have a fundamental role since they are the instruments capable of gathering weather, traffic, electricity, gas and water data and combine it with real-time images to understand how a neighborhood behaves. In other words, the sensors are aware of all the digital pulses in each activity in a city.

1) Availability of routes: Reliable or valid routes are the routes that are active and can be used by nodes to send packets. These routes may expire (according to the routing protocol) or may disappear from the tables due to disconnections of neighbor nodes. The most reliable routes will ensure more reliable delivery of information.

We turned off a certain percentage of network nodes to observe nodes disconnections. In this way, we could see how some routes become invalid and how nodes respond to reconfigure valid routes in the network, depending on the protocol. The percentage of reliable routes is presented in Figure 3.

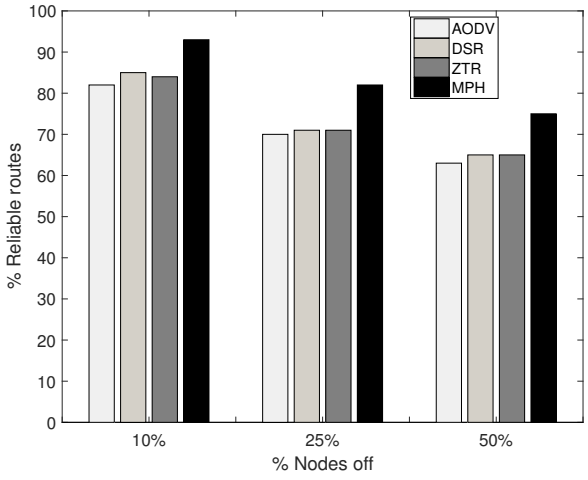

Figure 3. % Nodes off vs % Reliable routes.

Due to the persistence mechanism in MPH, that is a parameter that makes a soft output from the neighbor tables,

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-622-4

TABLE II. DELAY.

PARAMETER	AODV	DSR	ZTR	MPH
Neighbor discovery process for an average of 8 neighbors.	32.672 ms	31.592 ms	16.243 ms	29.924 ms
Average time it takes a traffic packet to reach its destination without shutdown nodes in the network (ring farthest to destination).	152.671 ms	142.411 ms	63.141 ms	62.393 ms
Average time it takes a traffic packet to reach its destination without shutdown nodes in the network (ring closest to destination).	11.937 ms	10.493 ms	10.723 ms	10.399 ms
Average time it takes a traffic packet to reach its destination with 10% shutdown nodes in the network (ring farthest to destination).	95.415 ms	93.245 ms	92.113 ms	85.836 ms
Average time it takes a traffic packet to reach its destination with 20% shutdown nodes in the network (ring farthest to destination).	97.428 ms	95.678 ms	92.436 ms	86.336 ms
Average time it takes a traffic packet to reach its destination with 30% shutdown nodes in the network (ring farthest to destination).	98.768 ms	98.258 ms	94.226 ms	88.126 ms
Average time it takes a traffic packet to reach its destination with 40% shutdown nodes in the network (ring farthest to destination).	100.258 ms	99.356 ms	96.116 ms	89.963 ms
Average time it takes a traffic packet to reach its destination with 50% shutdown nodes in the network (ring farthest to destination).	105.247 ms	104.385 ms	100.122 ms	92.836 ms
Recovery of topology with 50% shutdown nodes (the worst case).	34 sec	33 sec	21 sec	20 sec

TABLE III. ENERGY MODEL.

	Voltage (mV)	Current (mA)	Time (ms)
Start-up mode	120	12	0.2
MCU running on 32-MHz clock	75	7.5	1.7
CSMA/CA algorithm	270	27	1.068
Switch from RX to TX	140	14	0.2
Switch from TX to RX	250	25	0.2
Radio in RX mode (processing and waiting)	250	25	4.1915
Radio in TX mode	320	32	0.58
Shut down mode	75	7.5	2.5

TABLE IV. % VALID ROUTES.

TIME	% Valid Routes			
	AODV	DSR	ZTR	MPH
10	70	70	90	98
20	82	83	89	97
30	90	91	89	98
40	97	98	90	98
50	90	90	89	97
60	81	82	91	97
70	85	87	90	98
80	90	92	90	98
90	97	97	89	97
100	92	93	91	98

these become safer as well as more reliable, compared with AODV, DSR, and ZTR. This is so because in AODV routes have timers that expire after a certain period. On the other hand, DSR is aware that a route is obsolete only when it receives a route error message. ZTR does not have tables, so each time it needs to form the whole topology.

In Table IV, we took a sampling period of 100 seconds. We made tests every 10 seconds in which we compute the average number of valid routes available in case the node has to send a traffic packet right at this moment. In the AODV and DSR cases, occasionally some routes have just expired or some node in the route has been disconnected: these cases will result in invalid routes. In the ZTR case, sometimes, there is no route available to send the packet. On the other hand, when the MPH protocol is implemented, almost all the time the neighbor tables have valid routes ready to be used.

With regard to diversity of routes and hop count, we present Table V. The MPH protocol gets routes with a minimum

TABLE V. AVERAGE VALID ROUTES AND HOPS PER NODE.

TIME	AODV		DSR		ZTR		MPH	
	Routes	Hops	Routes	Hops	Routes	Hops	Routes	Hops
10	4.7	5	4.7	5	1	4.1	2.2	4.1
20	5.6	5	5.6	5	1	4.1	2.1	4.1
30	6.0	5	6.2	5	1	4.2	2.2	4.2
40	6.6	5	6.7	5	1	4.2	2.2	4.1
50	6.0	6	6.1	6	1	4.1	2.1	4.2
60	5.5	6	5.7	6	1	4.2	2.1	4.1
70	5.9	6	5.9	6	1	4.2	2.1	4.2
80	6.1	5	6.2	5	1	4.2	2.2	4.1
90	6.5	5	6.6	5	1	4.1	2.1	4.1
100	6.2	5	6.2	5	1	4.2	2.1	4.2

number of hops but it has fewer routes. The advantage of MPH compared to the AODV and DSR protocols is that MPH does not require routing tables, the decision of a node to route a packet to the coordinator is very simple because a node chooses the most widely used route. In contrast, we see that AODV and DSR have more routes to the coordinator, but they do not always guarantee the shortest route. It is true that the node chooses the shortest route from its routing table but it may be that this route is not the shortest to the destination. This effect is due to the packet loss probability. Regarding ZTR, the route to the destination is unique because it does not have the multi-parent concept. This means that, if there is any disconnection of a node (or nodes), the probability of packet loss is higher, which is a big disadvantage. In this table, the number that shows the hops is an average number of the nodes every 10 seconds.

A. *Retransmissions and retries*

Figure 4 displays the average node retransmissions and the average CSMA/CA retries for the four studied protocols. Here, we remark that for the four protocols, initially, there are many retransmissions and CSMA/CA retries. This is so because, when the nodes connect to the network they begin by sending broadcast packets to discover neighbors, so there is a greater number of packets in the network: overhead and traffic packets produce more collisions. Note that in the retransmissions, during the first 10 seconds the four protocols increase their average amount of retransmissions(the line has the highest

peak of the graph). This is because of the amount of packets flowing in the network during the time of formation of the topology. The CSMA retries also show this peak because as the channel is constantly busy, CSMA retries increase. However, regarding retransmissions, it is important to mention that this first peak has an average value of 2.7 for AODV and DSR, 2.6 for ZTR and 2.5 for MPH. Concerning also the first peak, the CSMA retries metric has an average value of 3.6 for AODV, 3.5 for DSR and ZTR and, 3.3 for MPH.

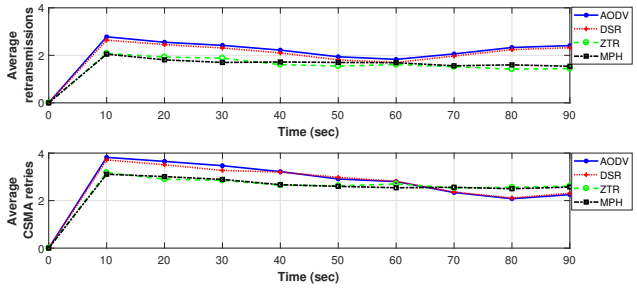

Figure 4. Time (sec) vs Average retransmissions and CSMA/CA retries.

VII. Conclusion

IoT enables physical devices or sensors to measure, perform a defined task, use the cloud for storage and to actuate the alert system automatically in case of an emergency situation with the aid of Internet as its underlying technology. Thus, IoT transforms these traditional devices to work in a smart way by using various deriving technologies such as pervasive computing, embedded devices, various communication standards and technologies.

In MPH, the coordinator node can be aware of approximately the whole topology due to the source routing mechanism. In AODV and DSR, the routes from the coordinator to some node are calculated the same way as the other routes. So, MPH has the advantage that the coordinator node can access any node to send information, statistics or measurements requests. In comparison with AODV and DSR, the coordinator has to discover the route to a specific node if it does not have it, which is not desirable. Also, MPH protocol has fewer control packets, therefore less overhead, resulting in fewer collisions, so there will be fewer packet retransmissions compared with AODV and DSR. Moreover, this is reflected in the energy saving metric. The ZTR algorithm does not present route diversity which enhances the probability of losing packets when there are disconnections of nodes.

The results for MPH protocol are encouraging because this protocol has good performance in terms of processing, fast and efficient information delivery and energy conservation. Protocols such as AODV and DSR are very efficient in terms of backup routes and connectivity from any node to any node in the network. ZTR is a simple and low energy cost algorithm, but it is not very reliable in adverse network conditions or failure on the links. The combination of a hierarchical topology with self-configuration and maintenance mechanisms of the MPH protocol makes the nodes optimize network processes, reduce delays, take short routes to the destination and decrease network overhead. All this is reflected in the successful delivery of information. As future work, this analysis of the performance of a sensor network should be complemented by low-power protocols on the Internet of things, such as 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks).

Acknowledgement

The author Carlos Mex-Perera has been supported by Asociación Mexicana de Cultura A.C.

References

[1] M. Aykut Yigitel, Ozlem Durmaz Incel, and Cem Ersoy, “QoS-aware MAC protocols for wireless sensor networks: A survey,” Computer Networks, vol. 55, no. 8, 2011, pp. 1982 – 2004.

[2] C. E. Perkins and E. M. Royer, “Ad-hoc on-demand distance vector routing,” in Proceedings - WMCSA’99: 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999, pp. 90–100.

[3] D. A. Maltz, J. Broch, J. Jetcheva, and D. B. Johnson, “Effects of on-demand behavior in routing protocols for multihop wireless ad hoc networks,” IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, 1999, pp. 1439–1453.

[4] C. Del-Valle Soto, C. Mex Perera, A. Orozco Lugo, G. M. Galvan Tejada, O. Olmedo, and M. Lara, “An efficient Multi-Parent Hierarchical routing protocol for WSNs,” in Wireless Telecommunications Symposium, 2014.

[5] Z. Alliance, “ZigBee specification (document 053474r17),” vol. 21, 01 2008.

[6] J. Macker, “Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations,” 1999.

[7] C. Sergiou, V. Vassiliou, and A. Paphitis, “Hierarchical Tree Alternative Path (HTAP) algorithm for congestion control in wireless sensor networks,” Ad Hoc Networks, vol. 11, no. 1, 2013, pp. 257–272.

[8] A. E. Zonouz, L. Xing, V. M. Vokkarane, and Y. L. Sun, “Reliability-oriented single-path routing protocols in wireless sensor networks,” IEEE Sensors Journal, vol. 14, no. 11, 2014, pp. 4059–4068.

[9] A. Bhattacharya and A. Kumar, “A shortest path tree based algorithm for relay placement in a wireless sensor network and its performance analysis,” Computer Networks, vol. 71, 2014, pp. 48–62.

[10] A. Kabila and A. Murugan, “Efficient Energy Performance of the Wireless Sensor Networks and Cross Layer Optimization,” Asian Journal of Applied Science and Technology (AJAST), vol. 1, no. 3, 2017, pp. 55–58.

[11] J. Rahman, M. A. M. Hasan, and M. K. B. Islam, “Comparative analysis the performance of AODV, DSDV and DSR routing protocols in wireless sensor network,” in 2012 7th International Conference on Electrical and Computer Engineering, ICECE 2012, 2012, pp. 283–286.

[12] S. Fauzia and K. Fatima, Performance evaluation of AODV routing protocol for free space optical mobile Ad-Hoc networks, ser. Advances in Intelligent Systems and Computing, 2018, vol. 683.

[13] H. Jiang, J. Qian, Y. Sun, and G. Zhang, “Energy optimal routing for long chain-type wireless sensor networks in underground mines,” Mining Science and Technology, vol. 21, no. 1, 2011, pp. 17–21.

[14] A. A. Nezhad, A. Miri, and D. Makrakis, “Location privacy and anonymity preserving routing for wireless sensor networks,” Computer Networks, vol. 52, no. 18, 2008, pp. 3433–3452.

[15] N. Nasser and Y. Chen, “SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks,” Computer Communications, vol. 30, no. 11-12, 2007, pp. 2401–2412.

[16] I. Computer Society, IEEE. Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs). IEEE Standard 802.15.4-2006 (Revision of IEEE Standard 802.15.4-2003)., 2006, [retrieved: January, 2018].

[17] M. Sakamoto and T. Nakajima, “Some experiences with developing intelligent Internet-of-Things,” in IEEE 2nd International Smart Cities Conference: Improving the Citizens Quality of Life, ISC2 2016 - Proceedings, 2016.

[18] S. Kurt, H. U. Yildiz, M. Yigit, B. Tavli, and V. C. Gungor, “Packet size optimization in wireless sensor networks for smart grid applications,” IEEE Transactions on Industrial Electronics, vol. 64, no. 3, 2017, pp. 2392–2401.

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-622-4