Energy Efficient Fault Tolerant Routing Mechanism for Wireless Sensor Network

Ahmed Roumane[1], Bouabdellah Kechar[2] & Belkacem Kouninef[1]

[1] National Institute of Telecommunications and ICT (INT-TIC), Oran, Algeria

[2] Oran University, Oran, Algeria

Correspondence: Ahmed Roumane, National Institute of Telecommunications and ICT (INT-TIC), Oran, Algeria. Tel: 213-550-524-514. E-mail: ironlyon@hotmail.fr

Received: March 12, 2012 Accepted: April 5, 2012 Online Published: June 1, 2012

doi:10.5539/cis.v5n4p68 URL: http://dx.doi.org/10.5539/cis.v5n4p68

Abstract

Wireless sensor networks are self-organizing systems with resource-constraints that are often deployed in inhospitable and inaccessible environments in order to gather data about some phenomenon in the outside world. For most sensor network applications, point-to-point reliability is not the main objective (Paradis & Qi, 2007); Instead, reliable delivery of the interesting event to the server has to be guaranteed (may be with a certain probability). The communication in such networks is unpredictable and failure-prone, even more so than in regular wireless ad hoc networks. Hence, it is vital to provide fault tolerant techniques for distributed applications in sensor network. Several approaches have been proposed in many recent studies to address the fault tolerance issue in application, transport and/or routing layers. In this paper, we propose a slight modification of the conventional routing (destination, next hop) by introducing the second hop information in the route construction phase in order to use it in case of node/link failure (skip only the failed link). Furthermore, the implementation of this proposed routing technique stabilizes the throughput, reduces the average jitter, provides low control overhead and decreases the energy consumption of the network. As a result, the reliability, availability, energy-efficiency and maintainability of the network are achieved.

Keywords: wireless sensor networks, fault management, AODV, fault tolerance, link failure, ad hoc routing, OFLS

1. Introduction

WSN are a modern emerging technology that rises from the advancement in many technological fields including: micro-sensing, processing, integrated circuits, and wireless communication as well as cost reduction of processing and memory elements. WSN are now used in a different application domain such as tele-medicine, space exploration, avionics (Note 1), structural sensing, environmental monitoring, and command and control. The wireless multi-hop communication characteristic, enable sensor nodes to build a reactive systems which is able to monitor and react to physical events/phenomena. In addition to the constraints of resource limitation, sensor networks are also failure-prone (Paradis & Qi, 2007).

Different reasons can create failures in wireless sensor networks. First, sensor nodes are delicate, and they can get failures after the depletion of their batteries or the destruction of their bodies by an external event. Furthermore, nodes may communicate an incorrect capture because of the influence of the environment on their sensing components. Second, as the case of wireless ad hoc networks, links are failure-prone, causing dynamic changes and network partitions in network topology. Links can get (permanent or temporal) failure if it is blocked by an external object or environmental condition. The corruption of packets may occur because the wireless communication has an erroneous nature. In addition, nodes can be taken out of the communication range, when they are carried or embedded by mobile objects. Third, congestion may induce an extensive packet loss, this can occur when a large number of nodes simultaneously transit to the state of active transmission, in response to a sensed-event (Paradis & Qi, 2007).

Furthermore, the communication in sensor networks has a multi-hop nature, which worse each of the above fault scenarios. In the most of time, data takes a bunch of hops to be delivered from a node to the sink; therefore, a single failure of node or link may isolate greater region of the sensor network.

Therefore, fault tolerance is as critical as other performance metrics such as energy efficiency, latency and accuracy in supporting distributed sensor applications.

Fault tolerance is the ability of a system to deliver a desired level of functionality in the presence of faults (Che, Al-Khateeb, & Anwar, 2010). Since the sensor nodes are prone to failure, fault tolerance should be seriously considered in the sensor network applications.

In this paper, we propose a novel approach that enhances the routing mechanism for tolerating random link failures with reducing the network energy consumption and decreasing significantly the network overhead during the route maintenance phase.

The rest of the paper is organized as follows: in the next section we will discuss the related work. In Sections 3 we describe the OFLS algorithm and its implementation in AODV, then we will show an example to illustrate the operation of our algorithm, In Section 4, we present our performance evaluation results. Finally, we make some concluding remarks in Section 5.

2. Related Work

Because of data delivery in sensor networks is inherently faulty and unpredictable; fault tolerance has been one of the most important topics in WSNs which lead to an extensive work on this field.

In (Che, Al-Khateeb, & Anwar, 2010) the authors enhance the AODV routing protocol to apply a backup route for each node along the routing path, then in case of failure, the backup route is used to forward data immediately, when the detecting node requests a new backup. Hyunyoung Lee et al. (Hyunyoung, Klappenecker, Kyungsook & Lan, 2005) have proposed a novel approach based on the graph theory (De Berg, Van Kreveld, Overmars, & Schwarzkopf, 1997; Bollobas, 1986), this method implement a hierarchical variable length addressing scheme in which a special nodes "relay" initiate the address allocation process by sending a message that contain their own addresses ($a_{rel}a_{node}$), the receiving nodes put the received address as a prefix of their own (a_{rel}), hen forward the message and so on, in this way each address represent a route, and thus no routing protocol is needed, in case of failure of node N, the nodes which have the address of N as prefix request another address from their neighbors. Author in (Belghachi & Feham, 2009) has modified the routing process of AODV by introducing the number of neighbors and the delay of each as a metric to select the route that can be easily repaired.

In both (Asim, Mokhtar, & Merabti, 2010) and (Guangyan, Yanchun, Jing, & Jinli, 2011), the problem is treated in hierarchical scheme where the central node has an essential role, the authors propose that this critical node select another as a secondary that can replace the primary in case of failure.

However, these proposed approaches are whether consuming energy to adopt the redundant paths, or are limited to tolerating unpredictable node faults other than out-of-power faults.

3. OFLS Algorithm

The Only Failed Link Skipped summarizes what our algorithm stand for, and to achieve this goal, we propose the following three steps:

→ Redefinition of the route from (destination via next hop) to (destination via next hop via second hop).

→ Exchange the second hop information during the route construction phase.

→ In case of random node or link failures, we recommend constructing a route from the detecting node to its second hop toward the destination, and thus maintaining the broken route.

In the following subsection, we present the operation details of our proposed algorithm implemented in AODV routing protocol. Furthermore, our modifications to AODV for applying our technique are also introduced.

3.1 AODV-OFLS Overview

Our enhancement of AODV (AODV-OFLS) protocol enables fault-Tolerant, self-starting, multihop routing between participating nodes wishing to establish and maintain a fault-tolerant wireless sensor network. AODV-OFLS allows nodes to enhance their vision of the network, by introducing the second hop in the routing information which is used to maintain the failed path, to respond to link breakages in a timely manner. The operation of AODV-OFLS is loop-free and able to avoid the Bellman-Ford "counting to infinity" problem by exploiting the destination sequence number.

As in (Perkins, Royer, & Das, 2003) AODV-OFLS uses a destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program.

The destination sequence number can also indicate the freshness of route information. Given the choice between two routes towards a destination, a requesting node is required to select the one with the greatest sequence number indicating most fresh route.

The number of hops along a path is also used as a metric for a path selection. If multiple RREPs with same destination sequence number are received by the source, the route with the shortest hop count is chosen (Perkins, Royer, & Das, 2003).

Route Requests (RREQs) and Route Replies (RREPs) are the same message types as defined by AODV (Perkins, Royer, & Das, 2003). However, for AODV-OFLS, we add the second hop field in both types of messages.

In AODV-OFLS we have preferred to update the neighbor's table in the reception of the control messages, instead of enabling the HELLO messages.

The touting and the neighbor tables are extended to contain the second hop field.

Additionally, AODV-OFLS operation reduces the control messages dissemination range in the maintenance phase by introducing a new type of message (Route Maintain) that contain the information necessary to guide the message toward the destination.

When a path to the destination (sink node) is needed, the node (source node) runs a "Route Discovery" process to find a path to the destination. It broadcasts a RREQ and waits for a RREP from the destination itself or from an intermediate node which has a "fresh enough" route to the destination. A "fresh enough" route is a valid route entry for a destination whose associated sequence number is at least as great as that contained in a RREQ, each node receiving the RREQ update the second hop field and exploit this information by saving it as a second hop neighbor in the extended neighbor table, and so extend its vision about the network. During the period of unicasting the RREP back to the source node, each node receiving the RREP update and exploit the second hop information as it does with RREQ.

We note that in case of receiving a RREQ, the update of the neighbor table is performed before checking the broadcast id of the RREQ, i.e. before discarding the message which contains the same request that is received earlier. This allows AODV-OFLS to exploit the received broadcast before discard it.

During data packet delivery period, when the route gets failed, the node run a route recovery process by broadcasting a (Route Maintain) RM message to its one hop neighbors, this message contain the addresses of the broken neighbor, and the second hop toward the destination, as well as the distances (hops count) from the detecting node to both the destination and the source. Each node which received this message check its extended neighbor table, to see if the broken node or the second hop are matched in the table, if so, it forward the message, else the message will be discarded. And so this message will be disseminated in a small region of the network, additionally the Route Maintain message is unicasted in four cases: in the first two cases, the RM message is unicasted directly to the second hop or the destination if it is their "one hop neighbor"; in the second two cases the RM message is unicasted the neighbor of the second hop or the destination if it is their "second hop neighbor".

When a direct unicast message toward the second hop, is not possible because of ink failure, this intermediate node will deal with the situation by replacing the second hop field of the RM message by the address of the destination, and increase the TTL the value to the distance to the destination. In this case when a node receives this message, it checks the distance to the destination and the distance to the source (fields in RM message), then it forward the RM message only if it is in the side of the destination, this allows AODV-OFLS to reduce significantly the network overhead, which decrease congestion an energy consumption of the network. As a result, it increases more reliability and availability compared to the original AODV routing protocol.

3.2 AODV-OFLS in Operation

For properly understand the operation of AODV-OFLS let us consider the example shown in Figure 1 which consist of 20 wireless sensor nodes deployed in a cellular physical topology where all the one hop links have the same length (the same delay).

In this scenario the node 0 "source" tries to communicate with node 15 "destination", so it runs the route discovery process by broadcasting a RREQ (brown quarter circle in Figure 1) to its neighbors (nodes 1 and 4), when they receive this message, each of them update its neighbor table by adding the address of the sending node (0) as a one hop neighbor, and the address of the second hop as a second hop neighbor if it does not represent a one hop neighbor, then it writes the address of the sending node (0) in the second hop field in RREQ message and broadcast the message (blue circle in Figure 1) to its neighbors (0, 1, 5, 9, 8) which run the same procedure performed by node 9 which proceed as follow: first it updates its neighbor table (put 4 as one hop neighbor and 0 as second hop neighbor), then it creates a reverse route toward the source with the second hop equal to 0, finally it puts the address of 4 as second hop in the RREQ message and broadcast it (green circle in Figure 1) to its neighbors. Note that this procedure is performed by all the nodes in the network and thus each node gets a route to the source; when the RREQ reach the destination or an intermediate node which has a fresh enough route (a valid route entry for a destination whose associated sequence number is at least as great as that contained in a RREQ). We consider that a RREP message is unicasted from the destination (15) toward the source (0), transiting by this series of nodes (11, 10, 9, 4), this message contain the second hop field which will be updated the same manner as it was done with RREQ.

Finally the node 0 can use nodes (11, 10, 9, 4) as a route to send data to the node 15, when each node in this path know its second hop in both the forwarding and the reverse routes.

Consider that a failure has been occurred to node10 which is used as next hop of node 9 in the route used to deliver data, when the node 9 detect this failure, it runs a route recovery process, so it broadcast a (Route Maintain) RM message within this information (broken neighbor= 10, second hop = 11, requested destination = 15, distance to the source = 2), which will be helpful to guide the broadcasted message toward the second hop or destination and thereby reducing the network overhead as well as energy cost.

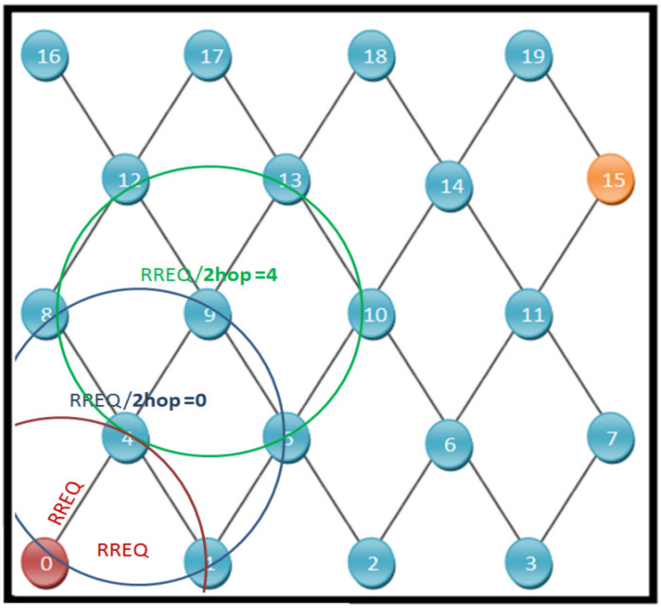

Figure 1. Route discovery

The broadcasted RM (green circle in Figure 2) “by node 9“ is received by all its neighbors, but it is forwarded by a node only if it has a neighborhood relationship with either the second hop or the broken hop, in our case the nodes (4, 8, 12) discard the message when node (5 and 13) forward it (brown and blue circles in Figure 2), this messages will be received by all their neighbors, and similarly only node 6 and 14 forward the RM message, and because they have both a neighborhood with node 11 “the requested second hop” they unicast the RM message. Finally the node 11 sends RREP to the node 9, which create the maintained route shown in Figure 3.

There is two special cases which can perturb the operation of OFLS:

The first one is when both the first and the second hop gets a failures, in this case, when the neighbor of the second hop tries to unicast the RM message to the second hop it detect a link failure, so it deal with this situation autonomously by replacing the address of the requested second hop by the address of the destination and set the TTL to the number of hops toward the destination and broadcast the message.

The second case is when the detecting node tries to send the RM message but none of its neighbor has a neighborhood with the broken neighbor or the second hop, so the detecting node rebroadcast the message with a special indication “flag” and a TTL equal to the number of hops toward the destination.

The RM message of both cases (with flag set), will be forwarded by all the receiving nodes that have a distance to the source greater or equal to that of the detecting node, thus the RM message will be propagated in the direction of the destination, and thereby reducing once again the network overhead and the energy cost.

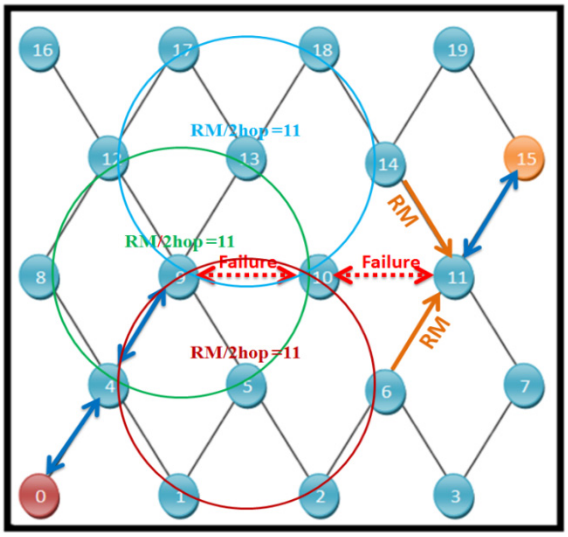

Figure 2. Failure in the created route

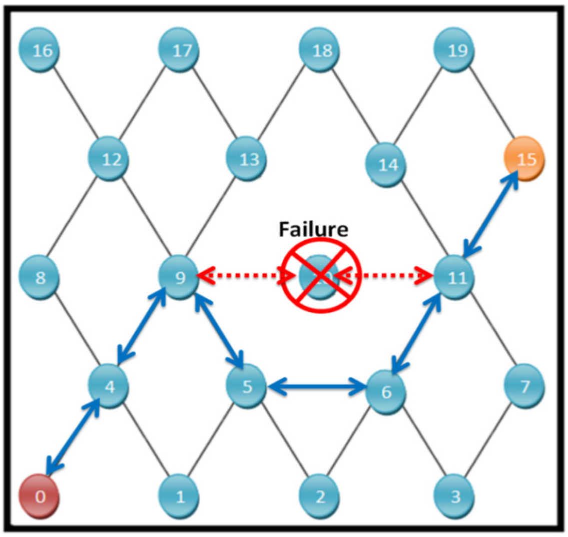

Figure 3. Route recovered by OFLS mechanism

4. Simulation Experiments

We have used the Network Simulator NS 2.33 (Fall, 2011) to evaluate the AODV-OFLS routing protocol, and compare its performance with the original AODV.

4.1 Simulation Environment

To evaluate the performance improvements made by AODV-OFLS, we compare the simulation results of AODV protocol with and without applying our OFLS scheme.

In the simulation model, there are 100 wireless sensor nodes deployed in a cellular topology. We prefer this topology because it is the only way to have the same characteristics (same delay) of all the links in the network, and thus avoid any problem due to the fast reception slow transmission which can be a cause to drop packet, thereby comparing fairly our approach with the original AODV. Table 1 summarizes the simulation parameters.

Table 1. Simulation parameters

Parameter	**Value**
N° of nodes	100
Simulation time	100 s
Coverage area	4000 x 4000
Variations in the environment and noise	not considered
Initial energy available in each node	5 Joules
Network type	Homogeneous
MAC Protocol	IEEE 802.11
Routing Algorithm	AODV
Propagation Model	Two Ray ground
Node distribution	Cellular
Transmission power	0.7 W
Reception power	0.6 W
Node receiving buffers capacity	5 packets
Node mobility	Sationary

The simulation consist of two nodes sources generating a 512 Bytes UDP data packets streaming at 40 Kb/s, and two destinations. The paths are separated, and the failures are simulated only in one of them (e.g. the first one). Our motivation to use this scenario is to study how the fault tolerant mechanism affects the performance of the whole network (i.e. other communicating nodes).

4.2 The Effect of Number of Main Path Failure for the Energy Consumed and the Number of Control Overhead

Figure 4 shows the percentage of the average energy consumed by the network against the number of main path failed in the simulation.

Unlike the fault tolerant mechanism used in the original AODV (Local repair), the OFLS mechanism consume less energy to tolerate faults, it is pretty undistinguished from the energy consumed by the network during its normal operation.

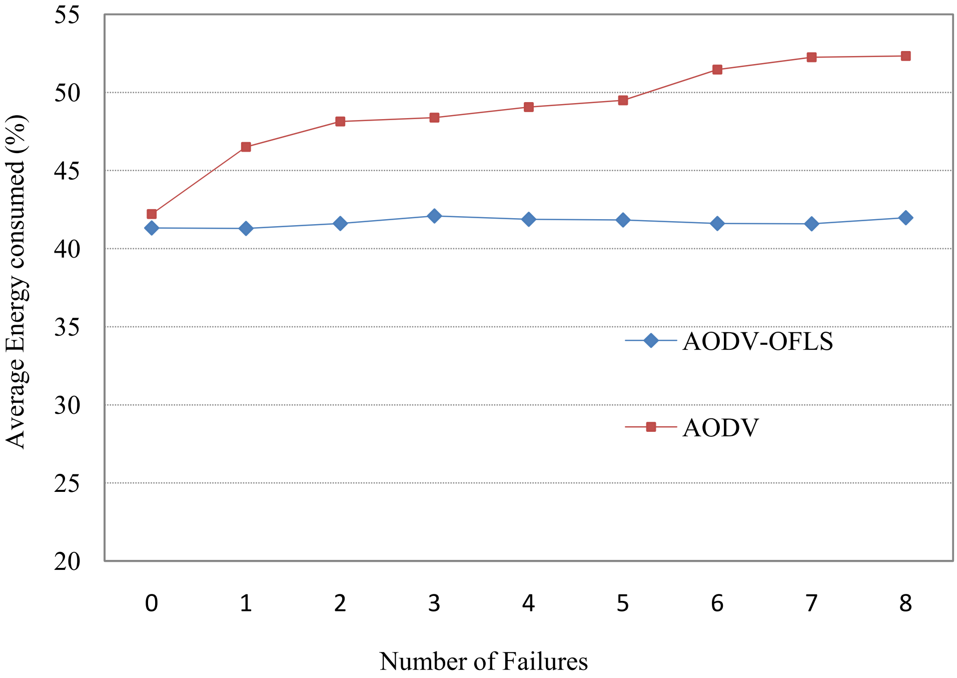

Figure 4. Average energy consumed by the whole network

Figure 5 shows the number control packet received by al nodes in the network with increased number of main path failure.

In our simulation, the control packets include all AODV packets RREQ, RREP, RERR and RM packets. The control overhead means a number of control packets received by all the nodes in the network during simulation time.

Comparing to AODV, AODV-OFLS reduce significantly the number of control packet during the fault recovery process, because of the use of the second hop information in the routing operation which enable AODV-OFLS to guide the broadcasted messages toward the destination and thus avoiding the unnecessary broadcasting of the control packets.

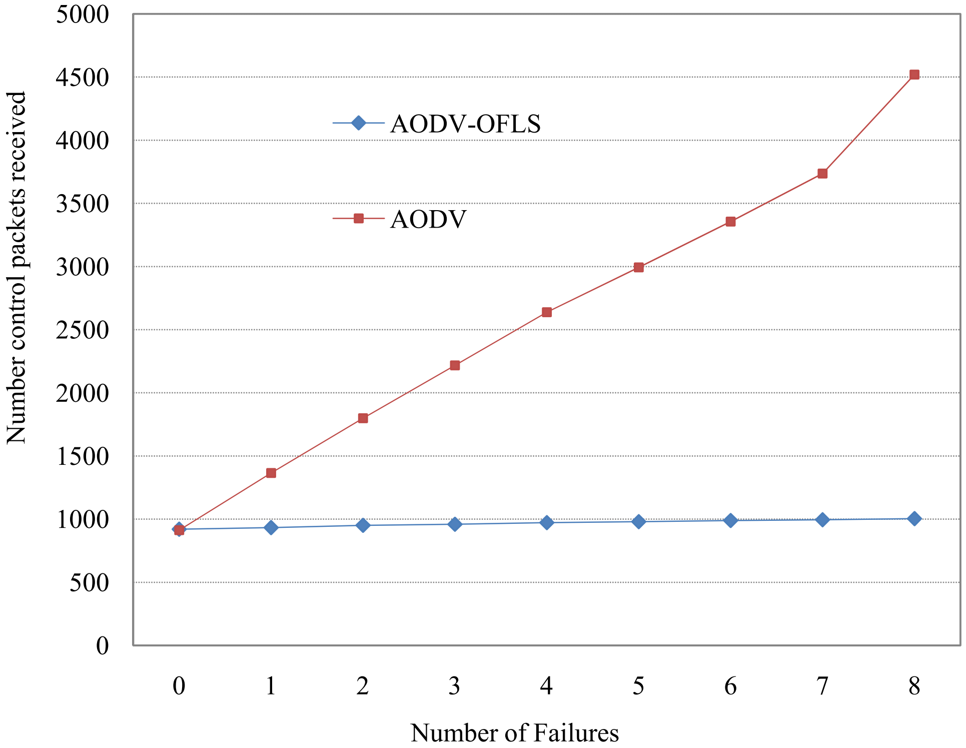

Figure 5. Control overhead with increased number of main path failure

4.3 The Effect of Number of Main Path Failure for the Throughput and the End to End Delay

Figure 6 shows the result of the destination node's throughput against the number of main path failed in the simulation.

When the throughput is dramatically decreasing with the increasing of link failures in the case of AODV, the implementation of OFLS mechanism in AODV shows that the throughput is slightly affected by link failures (Figure 6), because OFLS decrease the number of broadcasted messages which avoid congestion and thus the RREP messages can reaches the requesting node with a minimum number of retransmission and so the OFLS mechanism greatly improves the throughput and the network end to end delay (Figure 7).

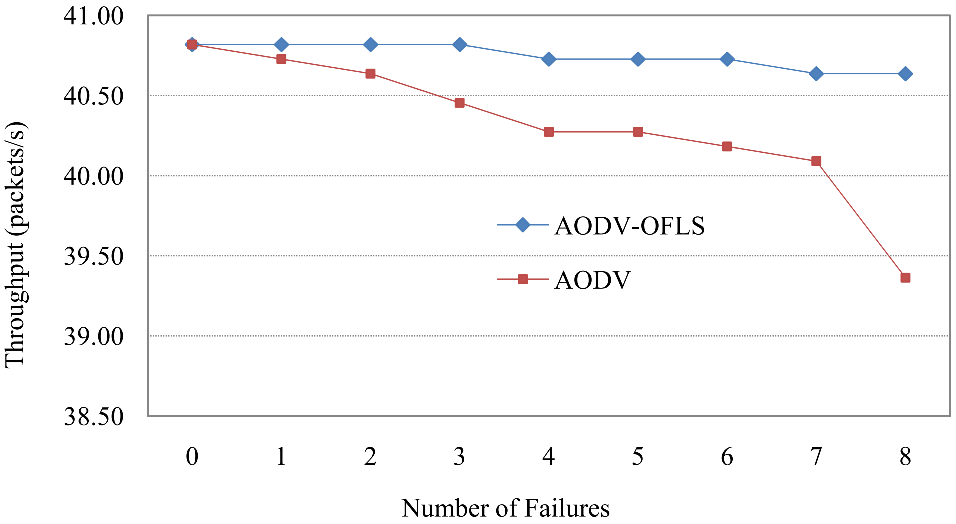

Figure 6. Throughput with increased number of main path failure

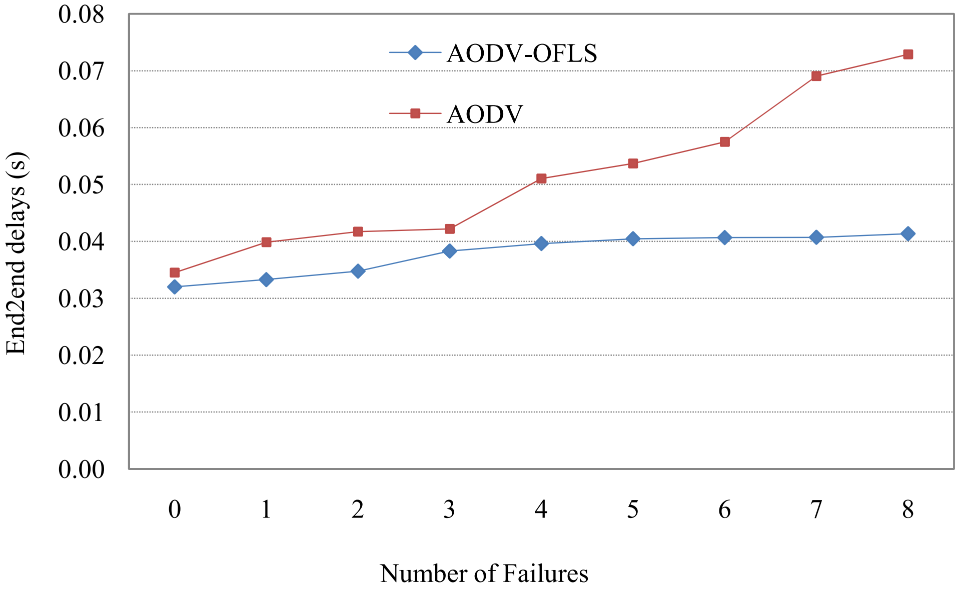

Figure 7. End to end delay with increased number of main path failure

4.4 Average Jitter Measurements

For our simulation, jitter is used as a measure of the variability over time of the data packet latency across a network. Most of applications for WSNs are real-time applications, typically, involving some kinds of monitoring, tracking, or detecting such as weather monitoring, object tracking, fire detection etc. The average jitter is an important QoS factor in an assessment of network, especially, in a realtime application. A system with low jitter provides good QoS.

Figure 8 shows the results of average jitter against the increased number of main path failure. As expected, from the graph, with increased number of main path failure, it is observed that AODV-OFLS provides lower and more stable average jitter.

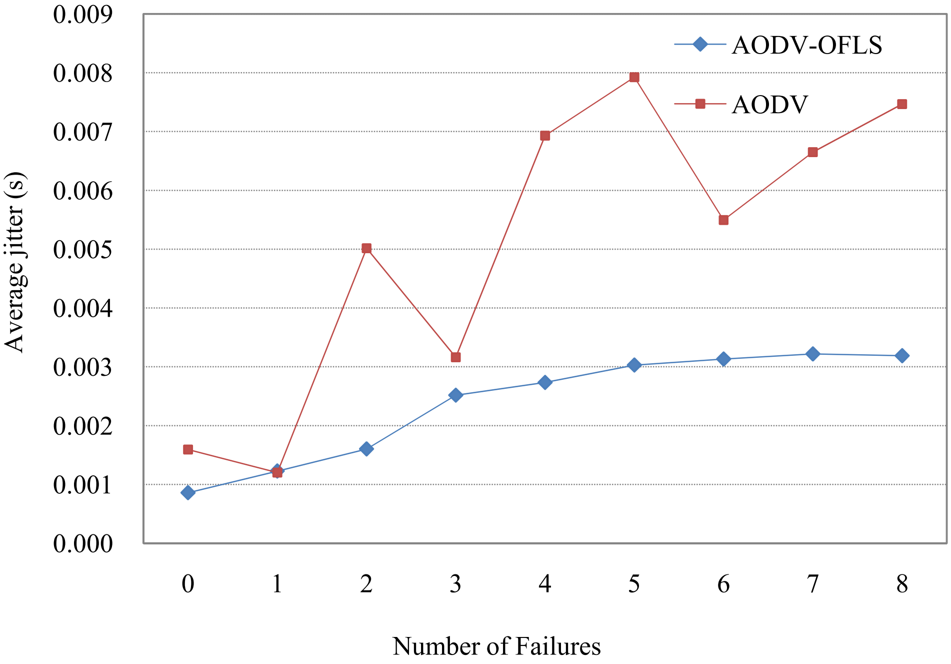

Figure 8. Average jitter with increased number of main path failure

5. Clusions and Future Work

In this paper, we propose a new fault tolerant mechanism to handle random link/node failure in wireless ad hoc sensor network, our technique introduce the address of the second hop in the routing information to enhance the node vision of the network and enable a fast self maintenance of the route for each node that detect a failure, by computing/requesting a new route using the second hop address. The implementation of our approach to AODV exhibits a great performance improvement.

The simulation result shows that our approach enhances the capabilities of the routing protocol with improving the throughput and reducing both the end to end delay and the jitter, thus the QoS is ameliorated.

The simulation results show also that our approach reduces significantly the network control overhead which is considered as one of the majors problems of wireless ad hoc network. The energy consumption is also reduced and thereby the proposed algorithm is suitable for wireless sensor networks.

Although the proposed mechanism doesn't incorporate any technique for node movement handling, the reacting nature of our method allows it to recover from faults caused by a certain scenario of node movement.

For future work, we try to enhance our scheme to support extreme conditions especially when a great number of nodes move in the network.

References

Asim, M., Mokhtar, H., & Merabti, M. (2010). A self-managing fault management mechanism for wireless sensor networks. *International Journal of Wireless & Mobile Networks (IJWMN), 2*, 184-197. http://dx.doi.org/10.5121/ijwmn.2010.2415

Belghachi, M., & Feham, M. (2009). *Conception d'une nouvelle approche pour le routage dans un réseau de capteurs sans fil.* Avignon, France: MajecSTIC.

Bollobas, B. (1986). *Extremal Graph Theory with Emphasis on Probabilistic Methods.* Providence, Rhode Island: American Mathematical Society.

Che-Aron, Z., Al-Khateeb, M. W. F., & Anwar, F. (2010). An Enhancement of Fault-Tolerant Routing Protocol for Wireless Sensor Network. *International Conference on Computer and Communication Engineering (ICCCE 2010), 11-13 May.* Kuala Lumpur, Malaysia. http://dx.doi.org/10.1109/ICCCE.2010.5556790

De Berg, M., Van Kreveld, M., Overmars, M., & Schwarzkopf, O. (1997). *Computational Geometry.* Verlag, Germany: Springer.

Demirbas, M. (2004). Scalable Design of Fault-Tolerance for Wireless Sensor Networks.

Guangyan, H., Yanchun, Z., Jing, H., & Jinli, C. (2011). Fault Tolerance in Data Gathering Wireless Sensor Networks. *The Computer Journal, 54*(6).

Hyunyoung, L., Klappenecker, A., Kyungsook L., & Lan, L. (2005). Energy Efficient Data Management forWireless Sensor Networks with Data Sink Failure. *In Proceedings of the Workshop on Resource Provisioning and Management in Sensor Networks (RPMSN 2005), in conjunction with The 2nd IEEE International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2005)* .

Kevin Fall, K. V. (2011). *The ns Manual.* (Ed.). UC Berkeley, LBL, USC/ISI, and Xerox PARC.

Paradis, L., & Qi, H. (2007). A Survey of Fault Management in Wireless Sensor Networks. *Journal of Network and Systems Management.*

Perkins, C. E., Royer, E. M., & Das, S. R. (2003). *Ad hoc on demand distance vector (aodv) routing*. (Nokia Research Center, University of California Santa Barbara, University of Cincinnati) Retrieved Novermber 22, 2011, from http://www.ietf.org/rfc/rfc3561.txt

Notes

Note 1. Development and production of control systems for airplanes.