Network Layer Benchmarking: Investigation of AODV Dependability

Maroua Belkneni[1](✉), M. Taha Bennani[2,3], Samir Ben Ahmed[2,3], and Ali Kalakech[4]

[1] LISI Laboratory, INSAT, University of Carthage, Tunis, Tunisia
belknenimaroua@gmail.com
[2] University of Tunis El Manar, Tunis, Tunisia
[3] University of Carthage, Tunis, Tunisia
taha.bennani@enit.rnu.tn, samir.benahmed@fst.rnu.tn
[4] Lebanese University, Beirut, Lebanon
akalakech@ul.edu.lb

Abstract. In wireless sensor networks (WSN), the sensor nodes have a limited transmission range and storage capabilities as well as their energy resources are also limited. Routing protocols for WSN are responsible for maintaining the routes in the network and have to ensure reliable multi-hop communication under these conditions. This paper defines the essential components of the network layer benchmark, which are: the target, the measures and the execution profile. This work investigates the behavior of the Ad Hoc On-Demand Distance Vector (AODV) routing protocol in situations of link failure. The test bed implementation and the dependability measures are carried out through the NS-3 simulator.

1 Introduction

Wireless Sensor Networks (WSNs) represent a concrete solution for building next-generation critical monitoring systems with reduced development, deployment, and maintenance costs [3]. WSNs applications are used to perform many critical tasks. Properties that such applications must have include availability, reliability, security and etc. The notion of dependability captures these concerns within a single conceptual framework, making it possible to approach the different requirements of a critical system in a unified way. The unique characteristics of WSNs applications make dependability satisfaction in these applications more and more significant [8].

The structure of the paper is as follows. In Sect. 2, we show the related work. In Sect. 3, we describe the benchmark target. Next, in Sect. 4, is held the execution profile. Section 5 defines the faultload specification. Section 6 describes measurements and simulation results. Finally, Sect. 7 concludes the paper.

2 Related Work

Various routing protocols have been compared, in the literature, using different aspects, namely the evaluation of performance or dependability. In the first case,

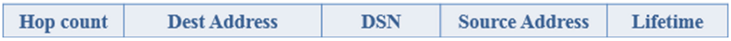
T. Czachórski et al. (Eds.): ISCIS 2016, CCIS 659, pp. 225–232, 2016.
DOI: 10.1007/978-3-319-47217-1_24

a set of measures is usually used to compare different solutions. Authors in [7] describe a number of quantitative parameters that can be used to evaluate the performance of Mobile Ad hoc Networking (i.e. MANET) routing protocols. In contrast the dependability measures define many properties like: time-to-failure and time-to-recovery [4]. Other measures may define the network and the sensing reliability. To perform such analysis we can use approaches like: simulation, emulation and real-world experiments [9]. We aim to define a fault injection based evaluator that handle errors and analyze the sensor networks reliability [1].

3 Benchmark Target

The network layer provides various types of communications. Which are not only messages delivering and the network layers yielded notification, but, also the paths discovery and its maintenance. Therefore, these two services are mandatory to build the workload that assesses the network layer dependability. We have used AODV [5] as the reference protocol to simulate these two services using NS3 [6].

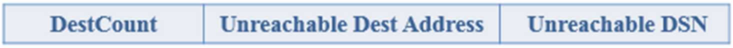
Route Calculation: AODV broadcasts a Route Request (RREQ) to all its neighbors. Then it propagates the RREQ through the network, unless, it reaches either the destination or the node holding the newest route to the destination. The destination node sends back a RREP response to the source to prove the validity of the route [2]. Route Reply (RREP) message is unicast back and it contains hop_count, dest_ip address, dest_seqno, src_ip address and lifetime as shown in Fig. 1.



Hop count	Dest Address	DSN	Source Address	Lifetime

Fig. 1. RREP packet format

Route Maintenance: AODV sends these broadcasted "`hello`" messages (a special RREP) which are simple protocols used by the neighbors to refresh their valid routes set. If one node no longer receives the hello messages from a particular node, it deletes all the routes that use the unreachable link, and that form the set of the valid routes. It also notifies the affected set of nodes by sending to them a link failure notification (a special RREP see Fig. 2).



DestCount	Unreachable Dest Address	Unreachable DSN

Fig. 2. RERR packet format

The forwardup() operation of processes, a protocol data unit (PDU) messages and delivers it to the upper layers, whereas the Receive() operation provides the requests response. These two activities define services offered by the LLC Layer.

4 Execution Profile

The execution profile activates the target system with either a realistic or a synthetic workload. Unlike performance benchmarking, which includes only the workload, the dependability assessment also needs the definition of the faultload. In this section, we describe the structure and the behavior of the workload.

4.1 Workload Structure

To apply our approach to a real structure, we chose to monitor the stability of a bridge. Figure 3 introduces the topology of the nodes which is a 3D one. In our experiments, we vary the number of nodes within the range of 10 to 50 (see Table 1). The more we define nodes, the more is dependable the structure. With ten nodes, the structure has one redundant path between the source node and the sink. Then, even though one node had failed, the emitter node would have transmitted a packet to the sink. When the structure has more nodes, it will tolerate more than one node failure.

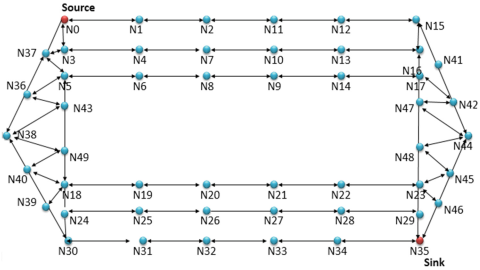


Fig. 3. Scheme of the considered bridge and resulting topology

Table 1. Simulation parameters

Network Simulator	NS3
Channel type	Channel/Wireless channel
MAC type	Mac/802.11
Routing Protocol	AODV
Simulation Time	100 s
Number of Nodes	10, 20, 30, 40, 50
Data payload	512 bytes
Initial energy	10J

4.2 Workload Behavior

As the assessed services is the route establishment and its maintenance by the network protocol, our workload consists on the sending of a packet from a source to the sink node. The Table 1 below summarises the simulations' parameters.

5 Faultload Specification

It would be awkward to identify the origin of the failure using multiple modifications, therefore, to avoid the correlation drawback, our benchmark assesses the WSN behavior using a single fault injection. As the source node triggers the communication, the route construction and its maintenance, we will inject faults within the packets received by this node and therefore the change in field of its routing table. Since the source node receives the RREP packets in the route identification phase and RERR in the maintenance one, we will inject into its different fields, described in the Table 2 below.

Table 2. The variable declaration

Fixed variable (fault injection)	
F_model	Fault model (injection into the RREQ, RREP or RRER)
F_type:	Fault node or non existing node
Dest:	The destination IPV4 Address
Cptd_Dest:	The corrupted destination IPV4 Address
SRC:	The source IPV4 Address
Cptd_SRC:	The corrupted source IPV4 Address
HC:	The hop count
Cptd_HC:	The corrupted hop count
LF:	The life time
Cptd_LF:	The corrupted Life time
DSN:	The destination sequence number
Cptd_DSN:	The corrupted destination sequence number
UNDest:	Unreachable Dest Address
UNDSN:	Unreachable DSN
Control function	
SetDst():	Set destination address
SetDstSeqno():	Set destination sequence number
SetHopCount():	Set hop count
SetOrigin():	Set source address

The table above introduces two set of elements: Fixed variables and control functions which are mandatory to specify the faultload. Fixed variables are the elementary parameters of the fault, they identify the packet's fields and their relative corrupted values. Also, the fault model specifies the faulty packet which could be the RREP or RERR packet and the fault type initializes the node's address using a random value belonging to the network or an imaginary one. All these values have to stay constant during one the simulation. The functions, belonging to the "Control functions", change the fields of control packets.

The CTL (Computation Tree Logic) formulae written below specify the fault-load used to assess the dependability of the routing layer. The expression (1) and (5) specifies respectively, a fault injection within the RREP and RERR packet. The fault type can take a false value of an another node within our architecture or a value of a non existing one. When we inject in the RREP packet, the fault may cover four fields: HC(3), DST(3), SRC(4) or DSN(4). In the RERR injection, the fault may alter these following fields: UNDST, UNDSN(7). In this section, we present the fault injection specification in the AODV protocol. The fault injection will be modeled in the primitive Forwardup () at the entrance of the network layer.

RREP Injection:

$$\begin{aligned}
Fault\_model &= RREP \wedge \qquad (1)\\
(Fault\_type &= fault \vee non\_existing) \wedge \qquad (2)\\
(DST &= Cptd\_DST \vee HC = Cptd\_HC \vee \qquad (3)\\
SRC &= Cptd\_SRC \vee DSN = Cptd\_DSN \vee LF = Cptd\_LF) \qquad (4)
\end{aligned}$$

RERR Injection:

$$\begin{aligned}
(Fault\_model &= RERR \wedge \qquad (5)\\
(Fault\_type &= fault \vee non\_existing) \wedge \qquad (6)\\
(UNDST &= Cptd\_DST \vee UNDSN = Cptd\_DSN)) \qquad (7)
\end{aligned}$$

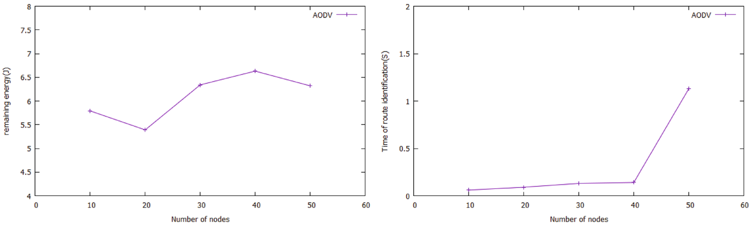
6 Measurements and Simulation Results

We need measurements to determine the dependability of the WSN:

- Remaining energy: Is the average of remaining energy of all nodes.
- Time of route recovery: It is the time taken by a protocol to find another path to the destination.
- Time of route identification: It is the time taken by a protocol to find a route to the destination.

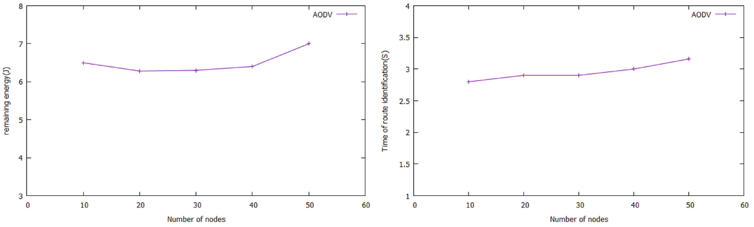
6.1 Route Calculation

In the following sections, we will present the results and analyze them. The after simulation results are viewed in the form of line graphs. The study of AODV is



(a) Remaining Energy (b) Identification time

Fig. 4. Fault free simulation



(a) Remaining Energy (b) Identification time

Fig. 5. Fault injection simulation of AODV

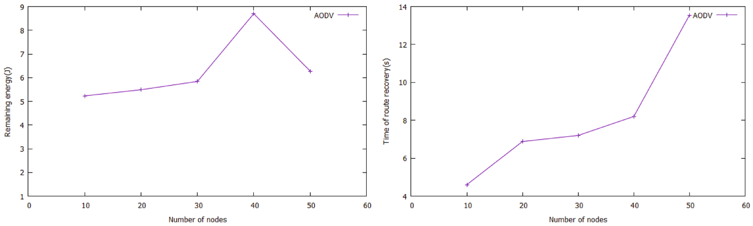
based on the varying of the workload and the faultload. This study is done on parameters remaining energy and time of route identification. The Fig. 4a shows the AODV power consumption compared to the number of nodes. In the Fig. 4b, we note that AODV is very fast to find the route especially when the number of nodes decreases.

The AODV protocol is robust to the hopcount and the lifetime fields injection. It find the route and keep the same performances as if we did not interfere.

AODV is not robust to the source address fields injection. When we inject in a node that belongs to the route and despite that there is an another one, the protocol don't find the path. With the Dest and the DSN fields injection, the protocol sends another RREQ which increases the route identification time and the remaining energy as shown in Fig. 5.

6.2 Route Maintenance

To evaluate the route maintenance we produce the failure of an intermediate node. Figure 6 shows the remaining energy and the recovery time without fault injection. To study the behavior of the AODV protocol during the route maintenance, we injected the fault after provoking the failure of the intermediate node. The fault model and the injection model used are defined in the section four. AODV protocol is robust with respect to the both filds to the Unreachable Dest Address and Unreachable DSN. Nevertheless the RERR packet rate increases which saves energy during the simulation.



(a) Remaining Energy

(b) Recovery time

Fig. 6. Fault free simulation

7 Conclusion

We studied the AODV dependability, considering the remaining energy, the time of route recovery and the time of route identification. After the benchmarking campaigns, we noticed that the AODV protocol is robust with respect to eight filds introduced in the section three except the source address in the packet RREP.

References

1. Sailhan, F., Delot, T., Pathak, A., Puech, A., Roy, M.: Dependable Sensor Networks, Atelier sur la GEstion des Donnes dans les Systmes d'Information Pervasifs (GEDSIP) au sein de la confrence INFormatique des ORganisations et Systmes d'Information et de Dcision (INFORSID), pp. 1–15, May 2010
2. Kumari, S., Maakar, S., Kumar, S., Rathy, R.K.: Traffic pattern based performance comparison of AODV, DSDV and OLSR MANET routing protocols using freeway mobility model. Int. J. Comput. Sci. Inf. Technol. **2**, 1606–1611 (2011)
3. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Comput. Netw. **38**(4), 393–422 (2002)
4. Chipara, O., Lu, C., Bailey, T.C., Roman, G.-C., Networks, reliable clinical monitoring using wireless sensor: experiences in a step-down Hospital unit. In: Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems, vol. 14, pp. 155–168 (2010)

5. Perkins, C.E., Royer, E.M.: Ad-hoc on demand distance vector routing. In: Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp. 90–100 (1999)
6. The NS-3 Network Simulator. http://www.nsnam.org
7. Corson, S., Macker, J.: Routing protocol performance issues and evaluation considerations. RFC2501, IETF Network Working Group, January 1999
8. Taherkordi, A., Taleghan, M.A., Sharifi, M.: Dependability considerations in wireless sensor networks applications. J. Netw. **1**(6) (2006)
9. Kulla, E., Ikeda, M., Barolli, L., Xhafa, F., Younas, M., Takizawa, M.: Investigation of AODV throughput considering RREQ, RREP and RERR packets. In: Advanced Information Networking and Applications (AINA), pp. 169–174 (2013)