Network Layer Dependability Benchmarking: Route Identification

Maroua Belkneni
University of Tunis El Manar
Tunis, Tunisia
Email: belknenimaroua@gmail.com

M.Taha Bennani
and Samir Ben Ahmed
University of Tunis El Manar,University of Carthage
Tunis, Tunisia
Email: Taha.Bennani@enit.rnu.tn
Email: Samir.benahmed@fst.rnu.tn

Ali Kalakech
Lebanese University
Beirut, Lebanon
Email: akalakech@ul.edu.lb

***Abstract*—The use of wireless sensor networks (WSN) is widespread; it covers, particularly, environmental and critical systems monitoring. Since the structure of the WSN has various layers including the application, the routing, the transfer, the Media Access Control(MAC) and the Radio Frequency(RF) Media, its dependability evaluation can be challenging. This paper defines the essential components of the network layers' benchmark, which are: the target, the execution profile, and the robustness measure. The dependability assessment is addressed in our benchmark by focusing on three standard protocols: Ad-Hoc on Demand Distance Vector Protocol (AODV), Optimized Link State Routing Protocol (OLSR) and Destination Sequence Distance Vector Routing Protocol (DSDV). The NS-3 simulator was used for the test bed. After the evaluation campaigns, we noticed that the DSDV and AODV protocols have an equivalent robustness. OLSR is the least robust but it is a fail-safe protocol.**

Keywords–Dependability; WSN; route discovery; assessment.

I. INTRODUCTION

A sensor node is made up of a processing unit, memory, RF transceiver, power source, and boards various sensors and actuators [2]. A large number of sensor nodes gathered in a wireless sensor network communicate in an ad hoc fashion and transmit measurements to the end user to monitor, track or detect the region in which they are deployed. Threats such as natural catastrophes, criminal or terrorist attacks have targeted Critical infrastructures (CI). Therefore, the use of WSN [8] based solutions could be a real shield to protect CIs. The deployment of such a solution helps avoid failures and possible loss of human life.

The goal of dependability benchmarking is to provide generic ways to characterize the behavior of components and computer systems in the presence of faults, which allows the quantification of reliability measures [5]. To perform such analysis, a widely accepted technique in the literature is the fault injection. It represents the observation of the system behavior in response to deliberately introduced faults. Thus, meeting the challenging task of developing dependable sensor networks requires not only the fault-tolerant sensing and actuating capabilities but also the evaluation and validation of their dependability attributes. We use a fault injection-based evaluator that deliberately accelerates the occurrence of faults to evaluate the quality of error handling mechanisms and, more generally, to analyze the dependability of the sensor network [1]. The remainder of this paper is organized as follows: Section 2 surveys some of the most relevant research works on dependability benchmarking for WSN. In Section 3, we describe the benchmark target. Next, in Section 4, the execution profile is held. Section 5 defines the faultload specification. Section 6 describes measurements and simulation results. Finally, Section 7 concludes the paper and presents directions for future studies.

II. RELATED WORKS

Some works propose a survey on adopted techniques of reporting the aspects and characteristics of some research studies. Here, we analyze the current state of the art of the WSN dependability assessment approaches in order to identify the most performant and to discuss the ongoing challenges.
A recent bibliography has categorized the approaches evaluating the WSN dependability attributes into three classes: experimental, simulative, and analytical [9]. For example, authors in [14] introduce an algorithm identifying faulty sensors which misbehave through calibration error, random noise error, and complete malfunctioning. In [15], authors present an analytical approach using an adapted probabilistic graph to model the network behavior. They associate an operational probability to each node, achieved using a data analysis field on the real sensors. The authors claim that components wear out, power failures and in some cases, natural catastrophes may lead to failures. They proved that evaluating the reliability of an arbitrary WSN is a non-deterministic polynomial-time hard problem for random networks. In [6], Heinzelman et al. provide an analytical model used to forecast the power consumption and thus the lifetime of the network. In [7], Mini et al. present a network state model to forecast the network residual energy. This work can have two different objectives, namely the evaluation of performance or dependability. In the first case, a set of measures is usually used to compare different solutions. Corson et al. [16] describe a number of quantitative parameters that can be used to evaluate the performance of MANET routing protocols, such as, packet delivery ratio, routing overhead, normalized routing overhead, Average End-to-End Delay (second), Packet Loss and Throughput (packet / second). In [17], Rahman et al. present the following measures: Remaining Battery Power, Power Consumed and MAC Load Dropped Packets. In contrast the dependability measures, rather we use the following measures: Network reliability, Sensing reliability, time-to-failure, timeto-recovery [12]. We can also use Node Uptime and Mean Time To Failure (MTTF), which were defined as reward variables in the Mobius tool [18]. In [13], Koushanfar et al. define a taxonomy for the faults of WSNs. Inconsistent measurement provided by a sensor, offset bias, death of a sensor, and idle reading are four different kinds of faults. Network reliability, sensing reliability, time-to-failure, and time-to-recovery are the key components of the

 ISBN: 978-1-61208-505-0

dependability measurements used by Chipara et al. [12].
To perform such analysis, a widely accepted technique in the literature is the fault injection. It consists in the observation of the system behavior as a response to deliberately introduced defects. Thus, meeting the challenging task of developing reliable sensor networks requires not only the fault-tolerant sensing and actuating capabilities but also the definition of the evaluation process to validate the dependability attributes. Our goal is to set the foundations of a fault injection-based evaluator that handles errors and analyzes the reliability of the sensor network [1].

III. BENCHMARK TARGET

The network layer provides two services, namely, route identification and route maintenance. This paper addresses the dependability assessment of the first service. The MANET routing protocols maintain the routes of the MANET and do not require any infrastructure to connect with other nodes in the network. Ad hoc routing protocols can broadly be classified into proactive, reactive and hybrid protocols. Proactive protocols, also known as table-driven protocols (i.e., DSDV, OLSR, Fisheye State Routing (FSR)), maintain routes between nodes in the network at all times, including the situation when the routes are not currently being used. Reactive protocols, also known as on-demand protocols (i.e., AODV, DSR, Temporally Ordered Routing Algorithm (TORA)), involve discovering routes to other nodes only when they are needed. A route discovery process is invoked when a node wishes to communicate with another for which it has no route table entry. There exists another class of protocols, such as zone routing protocols (ZRP), which employs a combination of proactive and reactive methods [19]. Even though similar studies have been carried out previously [10][11], this paper provides a comparative succinct view of DSDV, OLSR and AODV protocols. Hence, the OLSR builds up a route by maintaining a routing table at every node of the network. The topology information, which is exchanged using Topology Control (TC) packets builds the routing table. OLSR uses the HELLO messages to find its one-hop neighbors and its two-hop neighbors through their responses. The sender can, as a result, select its MultiPoint Relays (MPR) based on the one-hop node that identifies the best routes to the two-hop nodes. In DSDV, each node maintains an entry to the table containing the address' identifier of the destination, the shortest known distance metric to that destination measured in terms of hops, and the address identifier of the node that is the first hop on the shortest path to the target [4]. In reactive routing, 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 an RREP response to the source to prove the validity of the route [3].
The "`send()`" operation responsible for sending the packet, a protocol data unit (PDU) messages and delivers it to the lower layers, whereas the "`Receive()`" operation provides the requests response. These two activities define services offered by the Transport Layer. All studied network protocols, AODV, OLSR, and DSDV, have the same provided service. Nevertheless, several differences exist and belong not only to the handled message's structure but also to the mechanisms used to establish, deliver and retrieve the exchanged communications.

IV. 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.

A. Workload structure

To apply our approach to a real structure, we chose to monitor the stability of a bridge. Figure 1 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 nodes we define, the more 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.

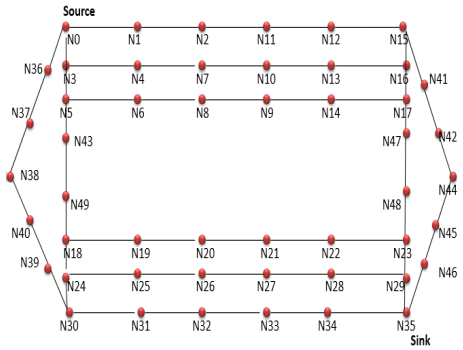

Figure 1: Scheme of the considered bridge and resulting topology

B. Workload behavior

As the assessed service is the route establishment by the network protocols, our workload consists of the sending of a packet from a source to the sink node. Table I below summarizes the simulation parameters.
Our study is carried within the NS-3 simulator, and Table I depicts the simulations' parameters implementing our experiments. We use the wireless channel and Mac802.11 to send the information throughout the nodes of the wireless sensors network. Before sending 512 bytes of useful data information, network protocol builds up the route between the sender node and the sink. We target, in our experiments, three different and

TABLE I: SIMULATION PARAMETERS

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

 ISBN: 978-1-61208-505-0

representative network protocols: AODV, OLSR, and DSDV. Different scenarios may raise various observations within a variable time duration; then each simulation lasts 100 seconds. To avoid running out of energy, we initialize our network with 10 joules.

V. FAULTLOAD SPECIFICATION

It would be troublesome 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 and the route construction, we will inject faults within the packets it creates. Nevertheless, we have designed three different origins of flaws: the source, the gateway, and the destination. Even though the failures' root is not the emitters' node, we will inject various faults, described in Table II below, within the parameters of the primitive "send" belonging to the interface of the network layer.

The Table II introduces three set of elements: Fixed variables, state 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, which are the saddr, daddr, etc. and their relative corrupted values, that are the Crpd_saddr, Crpd_daddr, etc. Also, the fault model specifies the faulty node which could be the source, intermediate or destination node 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 simulation. The state variables identify the behavior of the simulation evolution using three different variables: Total number of control packets (NCP_Total), the number of packets (NP) and the injection ratio (Rate). The three functions, belonging to the "Control functions", change the source, gateway or destination addresses.

TABLE II: THE VARIABLE DECLARATION

Fixed variables (fault injection)	
F_Model	Fault model (injection into the source, the intermediate or the destination node)
F_Type:	Fault node or non existing node.
saddr:	The source IPV4 address.
Crpd_saddr:	The corrupted source address.
daddr:	The destination IPV4 Address.
Crpd_daddr:	The corrupted destination address.
sport:	The source port number.
Crpd_sport:	The corrupted source port number.
dport:	The destination port number.
Crpd_dport:	The corrupted destination port number.
RS:	The source IPV4 route address.
Crpd_RS:	The corrupted source route address.
RD:	The destination IPV4 route address.
Crpd_RD:	The corrupted destination route address.
RG:	The gateway IPV4 route address.
Crpd_RG:	The corrupted gateway route address.
State variables	
NP	The number of control packets.
Rate	The rate of injection.
NCP_Total	The total number of control packet.
Control functions	
SetDestination(Ipv4Address dest)	Set destination address.
SetGateway(Ipv4Address gw)	Set gateway address.
SetSource(Ipv4Address src)	Set source address.

The Computation Tree Logic (CTL) formulae written below specify the faultload used to assess the dependability of the routing layer.

The expressions (1), (6) and (10) specify the fault model respectively, a fault injection within the source, gateway and destination node. The fault type can take a false value of another node within our architecture or a value of a non existing one. When we inject in the source node, the fault may cover three fields: Saddr(3), sport(3) or route (source)(4). The expression (8) indicates that the fault targets the route (gateway). In the destination injection, the fault may alter these following fields: Daddr(12), dport(12) or route (destination)(13). Fault injection is realized by an injection rate which is the ratio of modified packets over the total number of control packets sent as shown in the expressions (5), (9) and (14).

Source injection:

$$(F\_Model = source \wedge \quad (1)$$
$$(F\_Type = fault \vee non\_existing) \wedge \quad (2)$$
$$(saddr = Crpd\_saddr \vee sport = Crpd\_sport \vee \quad (3)$$
$$RS = SetSource(Crpd\_RS))) \quad (4)$$
$$\models \Box \quad (NP \leqslant rate * NCP\_Total) \quad (5)$$

Gateway injection:

$$(F\_Model = gateway \wedge \quad (6)$$
$$(F\_Type = fault \vee non\_existing) \wedge \quad (7)$$
$$(RG = SetGateway(Crpd\_RG))) \quad (8)$$
$$\models \Box \quad (NP \leqslant rate * NCP\_Total) \quad (9)$$

Destination injection:

$$(F\_Model = destination \wedge \quad (10)$$
$$(F\_Type = fault \vee non\_existing) \wedge \quad (11)$$
$$(daddr = Crpd\_daddr \vee dport = Crpd\_dport \vee \quad (12)$$
$$RD = SetDestination(Crpd\_RD))) \quad (13)$$
$$\models \Box \quad (NP \leqslant rate * NCP\_Total) \quad (14)$$

VI. MEASUREMENTS AND SIMULATION RESULTS

In addition to the performance measures as the remaining energy and the route identification time, we define the robustness :

- Remaining energy: Is the average of remaining energy of all nodes.
- Time of route identification: It is the time taken by a protocol to find a route to the destination.
- Robustness: the limit injection rate beyond which the protocol does not discover the route.

We will present the results and analyze them. The obtained simulation results are viewed in the form of line graphs. The study of AODV, OLSR and DSDV is based on the varying of the workload and the faultload.

 ISBN: 978-1-61208-505-0

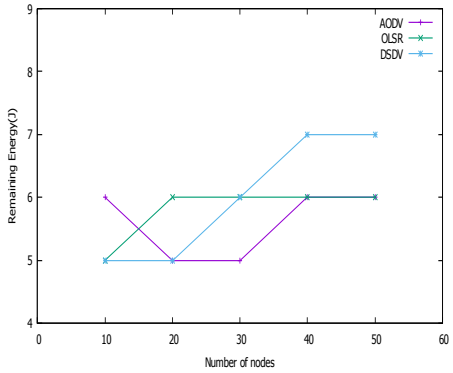

Figure 2: Fault free simulation: Remaining Energy

Figure 2 shows that DSDV consumed less energy than AODV and OLSR, especially when the number of nodes increases because the area size increases and consequently the nodes send more control packets to determine the route which preserves energy. The flow of AODV and OLSR are very close to each other, but AODV used the highest amounts of energy with 20 and 30 nodes.

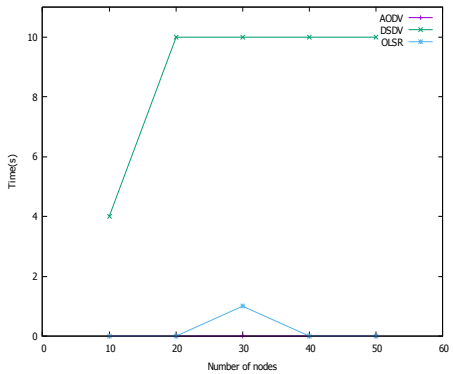

Figure 3: Fault free simulation: Identification time

In Figure 3, we note that AODV is the fastest protocol to find the route and OLSR the slowest one. DSDV has to continuously update the whole routing table periodically and when needed, which leads to a slight delay in delivery compared to AODV.

The three protocols are robust to the saddr and daddr fields injection, i.e., they identify the route. Moreover, the perfermances remain unchanged.

OLSR is not robust to the sport and route(source) fields injection. That is to say, it does not identify the route and it does not consume energy. However, AODV and DSDV are robust to the injection and, in addition, they keep the same performance as the fault free scenario.

DSDV is robust by contribution to the injection into the dport fields without changing perfermance. However AODV cannot find the route, but it preserves the energy consumption. OLSR shows a robustness rate equal to 97%. As shown in Figs. 4 and 5, the remaining energy and the time of route identification with OLSR, increases proportionally with the injection rate. However, the energy consumption decreases because the control packet does't require an increased energy consumption.

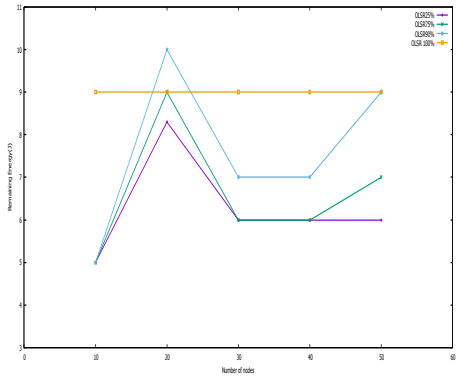

Figure 4: OLSR measures: Remaining Energy

As shown in Figure 4, the 25% injection curve is the lowest and the 90% curve is the highest one because the protocol sends more control packets. On the other hand the 100% injection curve is constant because OLSR does not identify the route and it does not consume energy.

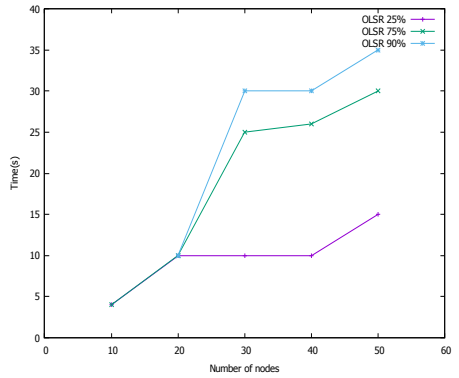

Figure 5: OLSR measures: Identification time

Figure 5 shows that OLSR takes more time to identify the route when the injection rate increases.

AODV is robust to the injection in route(destination) field. OLSR does not realize the service and does not consume energy. The DSDV behavior is based on the fault injection rates and the node number. However, with 10 nodes it crashes with 75% injection. 80% with 20 nodes, 90% with 30, and 95% with 40 and 50 nodes, as shown in Figure 6.

 ISBN: 978-1-61208-505-0

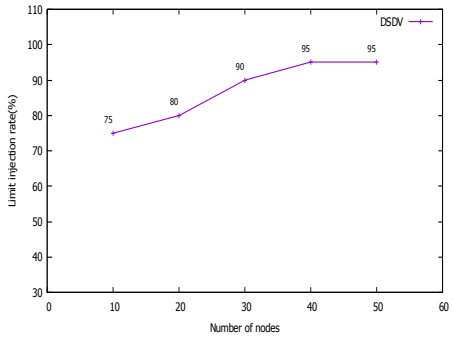

Figure 6: DSDV robustess

The three protocols are not robust to the route(Gateway) injection. Nevertheless, the fault injection leads to a total decrease in energy consumption with AODV and DSDV. It explains that all packets are either a control or a routing (RTR) packet. In fact, we notice the OLSR does not consume energy because it stops quickly. The limit injection rate of DSDV is 95% and of OLSR is lower than 10%.

Figure 7 shows a summary description of protocols robustness.

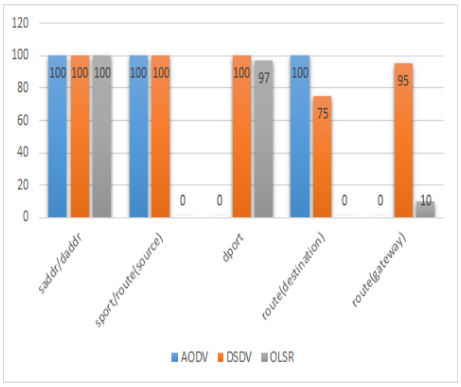

Figure 7: Protocols robustness

VII. Conclusion

The absence of an appropriate system for WSN dependability forces developers to conduct exhausting testing campaigns. Independent verification of each network layer reliability is not sufficient to guarantee the dependability of WSN, but rather makes a comparison between two or three layers. To tackle this problem, we have presented a network layer dependability benchmarking. We started by introducing the dimensions of the benchmark such as the target system, workload, faultload and measurements. We defined the robustness measure that represents the injection rate beyond what the service is no longer provided. After the evaluation campaigns, we noticed that the DSDV and AODV protocols have an equivalent robustness. The first one fails with the route(gateway) and route(destination) fields injection. The second is sensitive to the route(gateway) and dport injections field. OLSR is the least robust but it is a fail-safe protocol. However at the injection, the route is not discovered, but the energy is preserved. Our future work will include a new fault profile and a consideration of sensor nodes mobility with a real world case and the second service dependability (route maintenance).

References

[1] F. Sailhan, T. Delot, A. Pathak, A. Puech, and M. Roy, *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 dInformation et de Dcision (INFORSID), May 2010, pp. 1-15.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, *Wireless Sensor Network: A Survey*, IEEE Communications Magazine, Vol. 40, No. 8, 2002, pp. 102-114.

[3] S. Kumari, S. Maakar , S. Kumar and R. K. Rathy, *Traffic pattern based performance comparison of aodv, dsdv and olsr manet routing protocols using freeway mobility model*, International Journal of Computer Science and Information Technologies, 2011, pp. 1606-1611.

[4] E. Spaho, M. Ikeda, L. Barolli, F. Xhafa, M. Younas and M. Takizawa, *Performance of olsr and dsdv protocols in a vanet scenario: Evaluation using cavenet and ns3*, 2012 Seventh International Conference, 2012, pp. 108-113.

[5] K. Kanoun and Y. Crouzet, *Dependabiliy Benchmark for Operating Systems*, International Journal of Performability Engineering, July 2006, pp. 275-287.

[6] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, *Energy efficient routing protocol for wireless microsensor networks*. "In Proc. of Hawaii International Conference on System Sciences", HICSS00, 2000, pp. 1-2.

[7] A. Mini, B. Nath, and A. Loureiro, *A probabilistic approach to predict the energy consumption in wireless sensor networks*. "4thWorkshop de Comunicao sem Fio e Computao Mvel", So Paulo, Brazil, 2002.

[8] L. Buttyan, D. Gessner, A. Hessler, and Peter. Langendoerfer, *Application of wireless sensor networks in critical infrastructure protection: challenges and design options [Security and Privacy in Emerging Wireless Networks]*, "IEEE Wireless Communications is designed for individuals working in the communications and networking communities", Vol. 17, No. 5, 2010, pp.44-49.

[9] M. Cinque, D. Cotroneo, C. Di Martinio, and S. Russo, *Modeling and Assessing the Dependability of Wireless Sensor Networks*, Reliable Distributed Systems, SRDS 2007. "26th IEEE International Symposium on", 2007, pp. 33-44.

[10] G. Z. Santoso and M. Kang, *Performance analysis of AODV, DSDV and OLSR in a VANETs safety application scenario*, Advanced Communication Technology (ICACT), 2012 14th International Conference on 2012, pp. 57-60.

[11] R. Kaur and C. Sharma, *Review paper on performance analysis of AODV, DSDV, OLSR on the basis of packet delivery*, IOSR Journal of Computer Engineering (IOSR-JCE), Issue 1 (May. - Jun. 2013), pp. 51-55.

[12] O. Chipara, C. Lu, T.C. Bailey, and G.-C. Roman, *Reliable Clinical Monitoring Using Wireless Sensor Networks: Experiences in a Step-down Hospital Unit*, "Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems", Vol.14, 2010, pp. 155-168.

[13] F. Koushanfar, M. Potkonjak, and A. Sangiovanni-Vincentelli. *Online fault detection of sensor measurements*. "Proceedings second IEEE international conference on sensors (Sensors 03)", Vol.2, 2003, pp. 974979.

[14] J. Chen, S. Kher and A. Somani. *Distributed fault detection of wireless sensor networks*. "DIWANS 06: Proc. of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks", 2006, pp. 6572.

[15] HMF AboElFotoh, SS. Iyengar, and K. Chakrabarty. *Computing reliability and message delay for Cooperative wireless distributed sensor networks subject to random failures*. "Reliability, IEEE Transactions on", 2005, pp. 145155.

[16] S. Corson and J. Macker, *Routing Protocol Performance Issues and Evaluation considerations*, RFC2501, IETF Network Working Group, January 1999.

 ISBN: 978-1-61208-505-0

[17] A. Rahman, S. Islam, and A. Talevski, *Performance Measurement of various Routing Protocol in Ad-Hoc Network* , "IMECS", Vol. 1, March 2009, pp. 321-323.

[18] W. H. Sanders and L. M. Malhis. Dependability evaluation using composed SAN-based reward models. "Journal of Parallel and Distributed Computing 15",1992, pp. 238254.

[19] A. Kumar, M. Q. Rafiq, and K. Bansal, *Performance Evaluation of Energy Consumption in MANET*, "International Journal of Computer Applications (0975 8887)", Vol. 42, No.2, March 2012.

 ISBN: 978-1-61208-505-0