2011 3rd International Conference on Advanced Management Science
IPEDR vol.19 (2011) © (2011) IACSIT Press, Singapore

Survivability Evaluation in Wireless Sensor Network

Vahid Mavaji [1], Bahareh Abbasi [2]

Department Of Computer Engineering, Sharif University of Technology, Tehran, Iran
[1] mavaji@alum.sharif.edu
[2] b_abbasi@alum.sharif.edu

Abstract. Wireless Sensor Network (WSN) has the potential to gather information and send it to a base station. These networks are unattended and have the ability to work in military and civil applications. Wireless sensor nodes are combining the wireless communication infrastructure with the sensing technology. Instead of transmitting the perceived data to the control center through wired links, ad hoc communication methods are utilized, and data packets are transmitted using multi-hop connections. The survivability performance of WSN networks is an important issue. Network survivability is defined as the ability of a network to maintain or restore an acceptable level of performance in the event of deterministic or random failures. We perceive that packet loss, packet delay and network lifetime are integral components of WSN survivability. Therefore, we propose a composite model for survivability performance evaluation of WSN that consists of these parameters. Simulation results are used to validate the proposed model. The simulation results agree very well with the model.

Keywords: Wireless Sensor Network, Network lifetime, Survivability.

1. Introduction

Information gathering is a fast growing and challenging field in today's world of computing. Sensors provide a cheap and easy solution to these applications especially in the inhospitable and low-maintenance areas where conventional approaches prove to be very costly. Sensors are tiny devices that are capable of gathering physical information like heat, light or motion of an object or environment. Sensors are deployed in an ad-hoc manner in the area of interest to monitor events and gather data about the environment. Networking of these unattended sensors is expected to have significant impact on the efficiency of many military and civil applications, such as combat field surveillance, security and disaster management.

Sensors in such systems are typically disposable and expected to last until their energy drains. The self-organization feature of sensors makes it feasible to deploy them randomly over the region being observed. Without needing a previous exploration, sensors might be installed to the environment in a random way, like dropping them from an aircraft. In this manner, a large number of sensor nodes are spread over the environment without having a prior knowledge of where each sensor is being placed individually. Therefore, energy is a very scarce resource for such sensor systems and has to be managed wisely in order to extend the life of the sensors for the duration of a particular mission. How long the system can survive, and how much quality of service it can offer in presence of failure are major concerns in high performance dependable communication and information systems.

Because of the critical and important applications of wireless sensor network, it is necessary to know how long the network can fulfill its missions and the survivability performance of the networks is an important issue. Network survivability is defined as the ability of a network to maintain or restore an acceptable level of performance in the event of deterministic or random failures [9]. Sensor nodes have a short transmission range due to their limited radio capabilities. Therefore, the data must be relayed using intermediate nodes towards the sink. In addition, it may be more advantageous to use a multi-hop path to the

sink node consisting of shorter links rather than using a single long connection. There are some questions like: how long the network perform tasks? How can the network deal with the nodes failure? And what is the effect of loss and delay to overall network performance. These questions can be answered using the proposed WSN survivability model in this paper.

The main focus of this work is to propose a composite model to evaluate wireless sensor network survivability in the presence of different failures scenarios. We consider link failure, node failure and power failure and evaluate the network survivability in the presence of these failure scenarios. In our proposed model, we consider the effect of packet loss, packet delay and network lifetime on the survivability of the network. Simulation results are used to validate the proposed model. The results from simulation agree very well with the model.

The model can be used during the design stages of a network to ensure that the network is capable of handling the user traffic in the presence of certain failures.

In the next section, we explain different failure scenarios in WSN. In section 3, we present our proposed composite survivability performance evaluation model. Description of the simulation environment and analysis of the experimental results can be found in section 5. Finally section 6 concludes the paper and discusses our future research plan.

2. Failure scenarios in WSN

Information system survivability is defined as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents [2]. Network survivability is defined as the ability of a network to maintain or restore an acceptable level of performance in the event of deterministic or random failures [9]. Survivability is a property of a system, subsystem, equipment, process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbances. A survivable sensor network must deliver its data in a timely manner in the presence of failures. If there is a node or link failure, data will be routed using alternative routes to minimize data loss.

Consider a simple wireless sensor network shown in Fig. 1, which consists of two cells, cell A and cell B. We use A1 and A2 to represent the mobile terminals in cell A but not in cell B, B1 and B2 to represent the mobile terminals in cell B but not in cell A, and we use C1, C2 and C3 to represent the mobile terminals that are in the intersection area of cells A and B. It is worthwhile to point out that the notion of a cell is used in the sense that the mobile terminals in each cell are able to communicate with each other, while mobiles in different cells cannot directly communicate with each other due to either transmission range limits or physical obstacles between the cells. In this case, C1, C2 and C3 may act as routers for A1. There are different failure scenarios that should be considered in the model: Node, link and power failures. [5]:

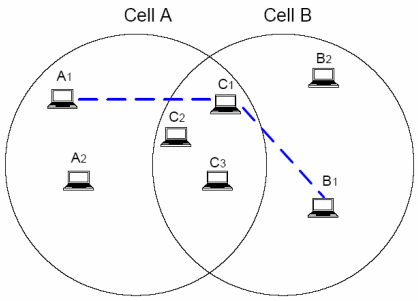

Fig. 1: A simple sensor network with two cells

- Node failures: The failures in an end-to-end connection may be caused by the unavailability of the routers, due to the mobility of terminals in the intersection region of the cells A and B. In Fig. 1, if mobile station C1 moves out of the intersection region, a router failure occurs on the path between A1 and B1. When this happens, the routing task between these two terminals may be switched to another mobile in the intersection region (C2 or C3 in our case). When no router is available, the connection between A1 and B1 fails**.**

- Power failures: Power failures are caused by the limited battery life in mobile stations. A router may be incapable of performing the routing task either due to insufficient power, or due to its desire to reserve energy for later use. In such cases, the terminals in A and B will need to switch to another router.
- Link failures: Link failures are introduced by either obstacle between nodes, known as the slow fading effect, or by excessive noise in the wireless link. Under the occurrence of a link failure, the communication between terminals in cells A and B may either be routed through another node, or interrupted for a while until the link recovers, depending on the nature of the failure and the service requirement of the communication task.

From the failure domain viewpoint, failures can be classified as value failures, where the value of the delivered service does not comply with the specification, and timing failures, where the timing of the service delivery does not comply with the specification [6, 8]. For the ad hoc network, a failure in the communication link may lead to both packet losses, which is value failure, and excessive end-to-end delay, which is a timing failure.

3. Network Survivability Evaluation Model

As discussed in section 2, three failure scenarios should be considered in wireless sensor networks. As a result of these failures, we could have packet loss and packet delay in the network. We want to measure the impact of these parameters on the overall network performance and survivability. We define two parameters for loss. Packet Loss Due To Failure (PLDF) and Packet Loss Due To Delay (PLDD). We define the total loss in the network as the summation of these two losses:

$$Total\ Loss = LDF+LDD \tag{1}$$

As the failure rate in the network increases, the loss and the network delay will increase and the network survivability will decrease.

In addition to the two loss parameters that are important in wireless networks, the network lifetime is also a vital parameter in sensor network. Network Lifetime is a function of both remaining energy and failure rate in the networks. The network lifetime is defined as the time when the first node dies or runs out of energy [3]. Network lifetime can be defined as a function of energy and network failure rate; the energy is also very dependent on nodes and the remained energy of individual batteries. We show the relationship between network lifetime with network energy and network failure rate as follows:

$$Network\ Lifetime=f\ (Energy,\ Network\ failure\ rate) \tag{2}$$

Therefore, we can increase the nodes and network lifetime by increasing the network remaining energy or decreasing the energy consumption in the network and network failure impacts. An efficient and energy aware routing algorithm can improve the energy consumption of the network [2].

In our proposed WSN survivability model, we consider network lifetime (NL), network delay (ND) and packet drop probability as a composite parameter. Using the above definitions, we find the sensor network survivability as follows:

$$S(t) = f(NL, ND, PDP)\ and$$
$$S(t)\ \alpha\ NL, S(t)\ \alpha\ \frac{1}{ND}, S(t)\ \alpha\ \frac{1}{PDP}. \tag{3}$$

Network survivability is a function of time and has direct proportion with network lifetime and reverse proportion with network delay and packet drop probability. If we represent the total percent of network loss in the network as L, which is a fraction between zero and one, and the averaged value of packets' delay over time as D, then survivability of the network is:

$S=(1-L)\times\frac{NetworkLifetime}{Nominal\,networkLifetime}$ (4) We define β as: $\beta=(1-L)$

And α as: $\alpha=\frac{Network\ \ Lifetime}{No\text{M}inal\ \ Network\ \ Lifetime}$ (5)

We call α as network lifetime index. Nominal network lifetime is determined with no limitation on nodes failure and it means that when calculating the NNL we suppose that all nodes are ok and no failure has occurred. Network lifetime is a practical lifetime that is influenced by nodes failure and losses in turn. That

can cause some nodes become failed and loss in network will increase. Now we can summarize the survivability formula as:

$$S = \beta * \alpha$$

It is easy to understand that network lifetime is smaller than nominal network lifetime and α is smaller than 1. We supposed earlier that L is also a number between zero and one and the inverse of D is also a number smaller that one. Therefore the multiplication of α and β is a number between zero and one i.e. $0 < S < 1$. So with calculating this parameter in any given sensor network, we can find the survivability of the network. We use simulations to validate our proposed model and the results agree very well with the model.

4. Simulations

Our simulations go step by step with simulating the effect of nodes failures and network delay on network lifetime and then on the survivability of network. For this purpose we used WSNsim.2 [6] which is an object oriented event driven simulator specially designed for wireless sensor network simulations.

We compare network survivability of two routing protocols using simulation; both are used in wireless sensor network infrastructure. Connected Dominating Set is designed in [7] and MHCIBT a virtual infrastructure for wireless sensor network with multi hop clustering and balanced traffic [2].

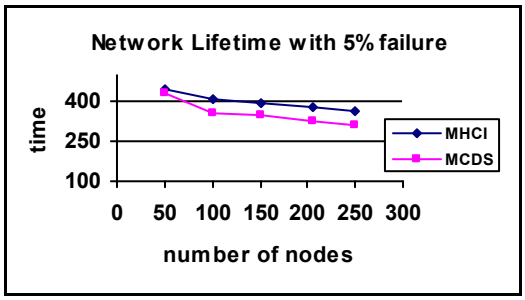

Fig. 2: Impact of node failure on network lifetime

As shown in Fig. 2 as the number of dead node increases, the network lifetime decreases.

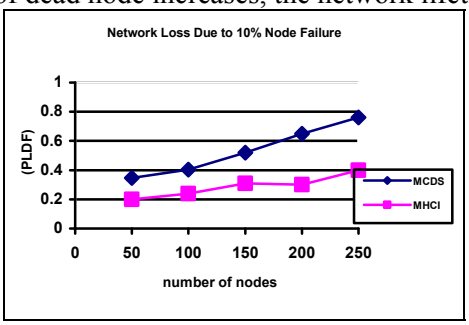

Fig .3: Effect of node failure rate on packet loss

As the failure rate increases in the network, a large number of nodes stop working and several routes are no more available for routing from source to destination. As a result, longer routes are selected and network loss increases.

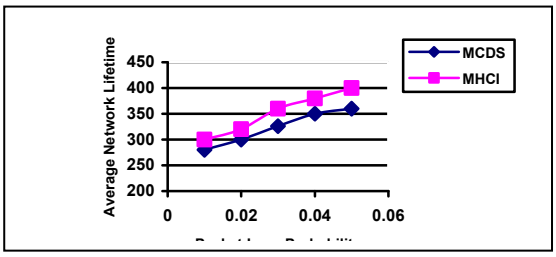

Fig. 4: Packet loss rate or packet drop probability impact on average network lifetime

Increasing packet loss in the network will cause lower rate of data that traverse across the network. Therefore, small numbers of nodes are working and overall network lifetime increases. However this doesn't yield good effect on survivability, because survivability of the network decreases when data loss increases.

We can conclude that we must separate losses-due-to-failure and losses-due-to-low-lifetime as is shown in Fig. 4.

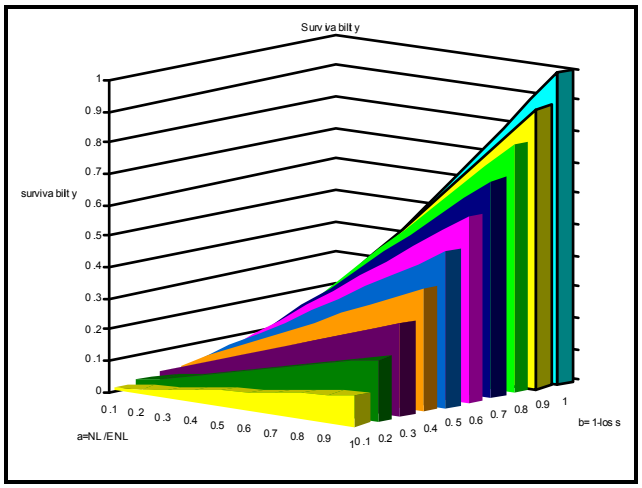

Fig. 5: Network survivability formula simulations with network lifetime index and network total loss.

As shown in Fig. 5, network survivability is increased with increasing network lifetime index and decreased when the network loss increases.

5. Conclusion and future works

In Wireless Sensor Networks, the lifetime, packet loss and packet delay are important factors that should be considered in a composite manner. We proposed a model to evaluate the system survivability performance of WSN.

6. References

[1] I. Akyldiz, W. Su, Y. Sankarasubramaniam, and E. Cayiroici. A survey on Sensor Network. *IEEE Communications Magazine*. 2002, **40**(8): 102-114.

[2] R. Azarderakhsh, A.H. Jahangir. A virtaual Infrastructure for Wireless Sensor Network. *Proc. of 13th ICEE2005 Conference on Iranian Electrical Engineering*. 2005.

[3] K. Arisha, M. Youssef, M. Younis. Energy-Aware TDMA-Based MAC for Sensor Networks. *IEEE Workshop on Integrated Management of Power Aware Communications, Computing and Networking* (IMPACCT 2002). 2002.

[4] M. Keshtgary, A. Al-Zahrani, P. Jayasumana and A.H. Jahangir. Network Survivability Performance Evaluation with Applications in WDM Networks with Wavelength Conversion. *Proc. of 29th IEEE Conffrtnrce on local computer networks.* tampaFl, 2004, pp. 344-355.

[5] Keshtgary, M. and A. H. Jahangir. Survivable Network Systems: An overview. *Fourth IEEE Information Survivability Workshops (ISW 2001/2002)*. Vancouver, Canada. 2002

[6] M. Younis, M. Youssef, K. Arisha. Energy-Aware Routing in Cluster-Based Sensor Networks. *Proc. of 10th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems* (MASCOTS2002). 2002.

[7] J. Wu and H. Li. On calculating connected dominating sets for efficient routing ad hoc wireless networks. *Proc. of* DialM'99. 1999, pp. 7–14.

[8] W. Du, et al. A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge. *Proc. of IEEE INFOCOM*. 2004.

[9] Shi, J. and Foneska, J. P. Traffic-Based Survivability Analysisof Telecommunications Networks. *Proc. of IEEE Globecom'* 95. 1995, pp. 936-940.