Common Cause Failure Analysis for Wireless Sensor Networks

Ivanovitch Silva, Luiz Alfonso Guedes, Paulo Portugal, Francisco Vasques

Common Cause Failure Analysis for Wireless Sensor Networks

Ivanovitch Silva and Luiz Affonso Guedes
Federal University of Rio Grande do Norte, Natal, Brazil
{ivan,affonso}@dca.ufrn.br

Paulo Portugal and Francisco Vasques
University of Porto, Porto, Portugal
{pportugal,vasques}@fe.up.pt

***Abstract*—Simultaneous failures of multiple devices make the dominant contribution to the unreliability of wireless sensor networks. They can hamper communications over long periods of time and consequently disturb, or even disable, the management algorithms of the network. In this preliminary work, we consider two types of common cause failures: hardware, and the temporary disruption of links. We propose an evaluation methodology based on the fault tree formalism for analyzing the reliability and availability of any wireless sensor network when common cause failures are considered.**

***Index Terms*—Common cause failure, fault tree, reliability, availability, wireless sensor network.**

I. Introduction

In wireless sensor networks (WSN), the failure of a single device might not be critical to the applications due to its intrinsic redundancy. However, when simultaneous failures occur with multiple devices, the consequences are likely to be disastrous, particulary for critical applications (patient surveillance, industrial environments, safety monitoring) [1]. This type of failure is known as common cause failure (CCF).

It is very important to measure the impact of CCF as soon as possible, ideally in the early phases of planning and designing the network. When done properly, such an early evaluation can anticipate decisions regarding the topology, criticality of the devices, the levels of redundancy, and network robustness. A tentative effort to evaluate a WSN considering CCF was performed in [2], but the technique was focused on a single cluster. By introducing the concept of coverage-oriented reliability, the same authors extended the previous work in [2] to support a more flexible way to configure failure conditions [3]. However, it is not possible to create two or more coverage subsets for the same cluster. In [4], the effects of CCF on a WSN were also evaluated. The authors proposed a progressive scheme based on binary decision diagrams for evaluating any WSN topology. However, the model supports neither generic network failure conditions nor an importance analysis of the devices.

The main focus here is to investigate the influence of common cause failures on a WSN. It becomes clear from the above discussion that previous research has only provided a partial solution for this problem. We proposed a methodology based on the fault tree formalism in [5] to evaluate the reliability and availability of a WSN, supporting the definition of flexible network failure conditions. Here, we extend this methodology to support CCF for both hardware and links.

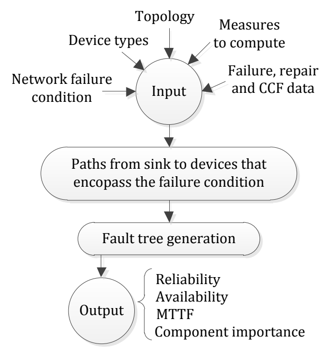


Fig. 1. Overview of the methodology for common cause failure analysis.

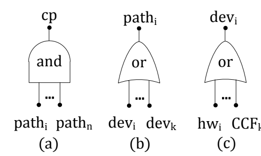


Fig. 2. Device failure condition.

II. Evaluation Methodology Incorporating Common Cause Failures

An overview of the methodology adopted in this preliminary work is given in Fig. 1. The process starts by providing information about the network topology, device types, device failure and repair processes, CCF data, and network failure condition. The latter expresses the conditions that may lead to a network (system) failure, and is defined by a logical expression that combines the failure status of the devices. The next step is to find all the paths between the sink and devices that encompass the failure condition. This is necessary for attaining flexible failure conditions and for supporting self-healing routing protocols. In the following step, a fault tree is generated using all the previous data. Finally, the metrics of interest (reliability, availability, MTTF, and importance measures) are computed.

A. Assumptions

The main assumptions of this methodology are summarized as follows:

- **Faults:** only permanent faults are considered. The links, due their wireless nature, are more affected by transient faults (millisecond scale). However, temporary barriers or bad weather conditions can obstruct a link for long hours. This case is also considered as a permanent fault. Failure occurrences are characterized by a *failure distribution*, by means of a CDF (cumulative distribution function). Any type of CDF can be used to describe their occurrence.

- **CCF:** the model support two types of CCF: hardware and link. The former is caused by shocks or other actions that damage the device hardware, whereas the latter is caused by temporary interruptions of a link (occurrence $\gg$ milliseconds). Depending on the scenario, the CCF can be fatal or non-fatal to the network.
- **Network failure condition:** the network failure condition (NFC) defines which combination of devices may lead to a network failure and its equivalent to the TOP event of fault tree. The methodology used in this letter supports any combination that can be expressed using boolean operators (i.e., AND, OR, K-*out-of*-N).

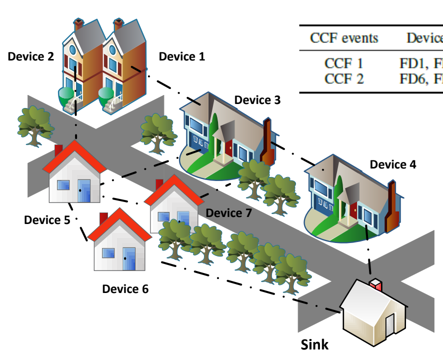
B. Device Failure Condition

After defining the NFC, it is necessary to define the conditions that may lead to the failure of a device. According to Fig. 2a, a device is considered faulty if all the paths between it and the sink fail (event cp – conectivity problem). On the other hand, as described in Fig. 2b, a path fails if at least one device along that path fails. Finally, a device also can fail if its hardware fails (event hw) or if at least one CCF occurs (Fig. 2c).

Note that it is necessary to exert some effort to find all combinations that may lead to a connectivity failure. In order to attain this, it is necessary to search all paths between the sink and devices that belong to the NFC. The paths are found by performing a depth-first search (DFS) in an adjacency matrix that represents the network. All the paths generated are then stored in a data structure based on a fault tree.

III. Preliminary Results

In this section, we evaluate the common cause failures for wireless sensor networks. The main target of the analysis is to highlight the influence of common cause failures upon network reliability. We assume a wireless sensor network mesh topology typical for condominium monitoring applications to validate the idea (Fig. 3). In this scenario, we consider that the network fails if at least three devices fail.



CCF events	Devices	MTTF
CCF 1	FD1, FD2	90 days
CCF 2	FD6, FD7	15 days

Fig. 3. Topology adopted in the evaluation process.

Regarding the failure properties, we assume that device failures occur at a constant rate. In order to simplify the procedure here, we assume that all devices have the same failure rate ($\lambda \approx 1E-5$).

The evaluation measures the influence of CCF on the network reliability. The results are described in Fig. 4. Despite the events CCF 1 and CCF 2 having different configurations, when both events occur the influence on network reliability is similar. This behavior results from the difference in criticality of devices 1, 2, and 7. Note that the network reliability decreases quickly when the events CCF 1 and CC2 are designed together. This scenario can even be pessimistic, but when compared to with the scenario without CCF, we observe that no consideration of CCF for network reliability is a very unrealistic assumption.

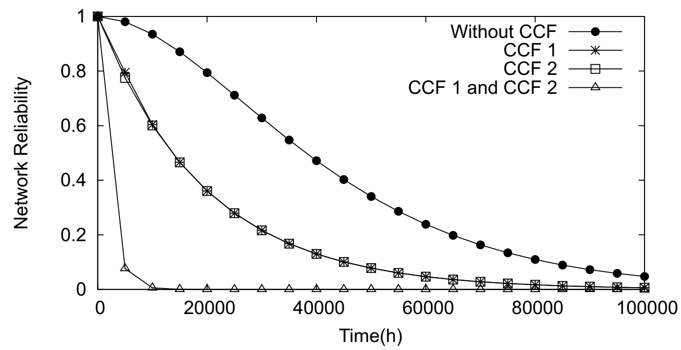


Fig. 4. Network reliability analysis considering common cause failure.

IV. Discussion and Future Work

In this preliminary work, we proposed an evaluation model for wireless sensor networks considering common cause failures. The proposal is based on the fault tree formalism and it considers hardware and link failures. A mesh topology was used for its validation (network reliability). It is also possible to analyze the network availability, and the criticality of the devices. The result showed the importance of considering CCFs during the design of a network, mainly when multiples CCF can occur. This analysis can be used to design any wireless sensor network. In future research, we plan to extend this methodology to analyze the redundancy, coverage factor, and hierarchical models.

References

[1] R. Dilmaghani, H. Bobarshad, M. Ghavami, S. Choobkar, and C. Wolfe, "Wireless sensor networks for monitoring physiological signals of multiple patients," *Biomedical Circuits and Systems, IEEE Transactions on*, vol. 5, no. 4, pp. 347–356, 2011.

[2] A. Shrestha, L. Xing, and H. Liu, "Infrastructure communication reliability of wireless sensor networks," in *Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on*, 2006, pp. 250 –257.

[3] A. Shrestha, H. Liu, and L. Xing, "Modeling and evaluating the reliability of wireless sensor networks," in *Reliability and Maintainability Symposium, 2007. RAMS '07. Annual*, jan. 2007, pp. 186 –191.

[4] L. Xing, H. Liu, and A. Shrestha, "Infrastructure communication reliability of wireless sensor networks considering common-cause failures," *International Journal of Performability Engineering*, vol. 8, no. 2, pp. 141–150, 2012.

[5] I. Silva, L. A. Guedes, P. Portugal, and F. Vasques, "Reliability and availability evaluation of wireless sensor networks for industrial applications," *Sensors*, vol. 12, no. 1, pp. 806–838, 2012. [Online]. Available: http://www.mdpi.com/1424-8220/12/1/806/