Fault Tree Analysis to Measure WSN Connectivity Reliability

Mohd Zaki B. Shahabuddin¹, Izwan Nurli B. Mat Bistaman¹ and Nor Izham B. Subri¹

¹Kolej Universiti Islam Perlis (KUIPs), 02000 Kangar, Perlis, Malaysia
mzaki@kuips.edu.my

Abstract. Wireless Sensor Network (WSN) is developed with limited capabilities to operate at low cost, using low power, and has non-exist physical topology infrastructure. Somehow, WSN must be connectively reliable to transmit the events data between communicating nodes. In this paper, we propose a method to measure WSN reliability by using the Fault Tree Analysis to identify the specific desired event that contributes to WSN connectivity failure. The computation of Boolean algebra to derive the minimal cut set of network graph discovers the components that are prone to failure. The components need to be resolved to reduce the probability of failure in WSN connectivity. The proposed Fault Tree Analysis and its related Boolean algebra computation verifies the reliability of WSN connectivity is improved by the means of network redundancy design.

1. Introduction
A wireless sensor network (WSN) can be defined as a network of devices called nodes that can sense the situations and extract the required information from the observed surroundings. The data is then forwarded via wireless multi-hops relaying to the base-station or sink for further analysis, and it can be connected to other networks through a device called a gateway [1].

The feature of WSN is as of ad-hoc network where it share the following characteristics: (1) There is no physical dedicate infrastructure topology, most of nodes connectivity are wireless and the connection mediums are by means of optical or radio signal, (2) All of the nodes are required to participate in routing protocol and must consider a suitable algorithm to run on limited computational capability, and (3) There are relay of data traffic from nodes towards the gateway [2].

Most of WSN solutions are built upon the IEEE 802.15.4 standard, a working group to offer a fundamental lower network layers (physical and media access control layers) of wireless communication. The standard emphasizes on low-cost, non-exist physical topology infrastructure, and operated by limited resources of devices.

2. Motivation of Work
There are number of WSN implementations in multiple areas such as military, rescue and recovery, environment monitoring, building automation, and so forth. These WSN applications may require different reliability level of event sensing and detection, but in common, they depend on devices that may not be highly robust.

Devices that make up WSN might have limitations in power and processing capabilities, and there are prone to error. WSN nodes which are wirelessly connected also vulnerable to environmental
forces. Correlated losses due to obstacles, asymmetric links, dislocation, and interferences make WSN quality connectivity are challenging. These factors needs to be reflexed during the implementation of reliable WSN, where the priority to ensure data travel from sensors to the gateway are acceptable by required application. Further improving WSN reliability, there is also a requisite to estimate the failure chances of each individual device, and filtered them out to ensure data are sensed and reliably transported with tolerable error [3].

3. Instruments to Measure WSN Reliability
Reliability is the important performance measurement for network system, and the network needs to be at high level of reliability to achieve its operating objectives. A network system is described as a collection of devices or components that working together. Similarly, WSN is a system composed of interconnected nodes as its elementary devices that form a network system. A WSN will operate successfully if all nodes operate successfully, or it may also operate at a minimal subset of some failure nodes.

Reliability can be defined as a measurement of individual device is successful according to specific requirements during a certain period of time [4]. Each device either has states of failure or success. When the set of successful devices and the set of failed devices are specified, it is possible to determine the status of the system reliability performance.

3.1. Graph Model
The Graph model is a tool to be used to abstract the WSN components and its links, and further used to define WSN reliability. The graph model can be used in any topology illustrating nodes (Vertices) and links (Edges) as depicted in figure 1.

Assume Node A is a source node, Node E as a sink and B, C and D are intermediate nodes. The arrow vertices represent the wireless connectivity set up between nodes. The system is considered successful when a node E able to receive data transmitted by a node A. Such example from figure 1, a failure of this WSN could happen if the link 6 is being removed. The reliability of this WSN is notated as probability of if there exist one or more successful paths from Node A to Node E.

**Formulation of reliability of node state condition**
The failure condition of WSN happened when there is a single component or combination of components that lead to overall failure [5]. This condition will cause the path of travelling data is not available. The condition to present individual node state can be written as binary indicator:

\[ x = 0 \rightarrow \text{failure} \]
\[ x = 1 \rightarrow \text{success} \]
From binary indicator of success or failure of each node, a compact description of all components are now combined, and this is called as a status vector, \(X\):

\[X = (x_1, x_2, \ldots, x_n)\]

Such example from Figure 1, we assumed all odd-numbered links are down, and all even-numbered links are up, then network status vector would be, \(X = (0, 1, 0, 1, 0, 1)\).

Status vector describing the dependence of overall network state elements will determine a network structure function, \(\Theta(X)\). Correspondingly, the network structure function \(\Theta(X)\) becomes a binary variable of following network states:

\[\Theta(X) = 1 \rightarrow \text{structure function corresponding to overall network is UP}\]

\[\Theta(X) = 0 \rightarrow \text{structure function corresponding to overall network is DOWN}\]

3.2. Minimal Path and Minimal Cut

Minimal Path is a set of links that comprise the shortest path of data to travel from the source to destination. It is the set of Edges which when traversed, will cover the least amount of distance between intermediate nodes [6]. Such in figure 1, \{1,4,6\}, \{2,5,6\} are the minimal paths, and \{1,3,5,6\} still makes the path, even though it is not a minimal path.

Minimal Cut Set is a set of components comprise the links that once being removed, then the whole connection will be in failure [6]. These links identified as Minimal Cuts serves the weakest points in the network, identified to understand the structural vulnerability of a system. Such example from figure 1, \{6\}, \{1,2\}, \{1,5\}, \{2,3,4\} and \{4,5\} are example minimal cut sets where any failure occurs to these links combination, it will cause the whole network to fail, hence not in reliable state.

3.3. Fault Tree Analysis

Fault tree is among the popular techniques used in reliability and risk analysis studies. It uses deductive logic techniques started from top events to derive the potential events that may cause the whole system to failure [7].

The causes at the lowest level are called basic events and in WSN perspective, it would be a device or node failure. Fault tree analysis is a deterministic model, means when the top event is known, automatically the status of basic and intermediate events also known.

The outcome of Fault tree analysis is represented in Boolean format. This means all events from the top to the lowest are assumed to have only two states condition: 1 – success or 0 – failure, this representing the same characteristic of WSN state condition. Table 1 shows the common basic symbols used in fault tree analysis.

| Gate symbol | Gate name | Description |
|-------------|-----------|-------------|
| ![AND gate](image) | AND gate | For the top event to occur, all the bottom events must occur (number of inputs ≥ 2) |
| ![OR gate](image) | OR gate | For the top event to occur, either one of bottom event must occur (number of inputs ≥ 2) |
Fault tree analysis can be used to provide information about possible combinations of events that result in the top event. Such a combination of top event here might be considered as a cut set for whole system to fail.

Let we evaluate a single sensor node. The events that may cause this device to fail are assumed as $E_1$, $E_2$ and $E_3$. Any failure of the event will cause the node to fail. We use the AND gate to represent if one of the event is failed, then that single node will also fail. This is illustrated in figure 2.

![Figure 2](image-url)

**Figure 2.** Simple fault tree representing events of failure of single device

For devices with redundancy, assumed when a primary device is failed the spare one will take over the connectivity. This can be presented using an OR gate to present the relationship of both devices. Both devices events are due to be the same of a single device. This can be presented in figure 3.
3.4. Boolean Algebra and Minimal Cut Set

From each node fault tree, all diagrams are then combined to present the structure of overall network. All the basic and intermediate events and combination of failure lead to the top event of WSN. To solve the fault tree computation, the probabilities of failure events are assigned from the lowest level event in each branch of the tree. Then, the intermediate event occurrence and the top level event occurrence will be determined using Boolean algebra and minimal cut set methods.

The following example is the steps of deriving Boolean algebra and minimal cut set for fault tree diagram (Figure 3).

1. Replace AND gates with the product of their basic events input.
   \[ E_7 = E_1.E_2.E_3 \]
   \[ E_8 = E_4.E_5.E_6 \]

2. Replace OR gates with the sum of their inputs
   \[ \text{Top Event} = E_7 + E \]
   \[ = E_1.E_2.E_3 + E_4.E_5.E_6 \]

3. From 2, we interpret that failure will occur if either combination \( E_1.E_2.E_3 \) or \( E_4.E_5.E_6 \) occurs during WSN lifetime. These occurrences of events are known as the minimal cut set of the systems.

4. Proof of Concept
   Assumption is made where WSN has been set up as the typical cluster topology presented in figure 4.
There are 3 cluster heads (CH) of full function device (FFD) type that serves as intermediate nodes to transmit the data from Sensor1 to the Sink. The paths extracted show that the data might take to travel, and the following figure 5 is a graph model showing possible paths available.

The possible paths taken are \{A,B,C,E\} and \{A,B,D,C,E\}. We may construct the fault tree of the graph as depicted in figure 6:
A Boolean algebra equation is then used to derive the network minimal cut set from the tree’s top event:

\[
Top \ event \ = \ (A.B.C + A.B.D.C).E \\
\ = \ A.B.C.E + A.B.C.E.D \\
\ = \ A.B.C.E(1 + D) \\
\ = \ A.B.C.E \\
\]  

(1)

The equation (1) gives the set of network minimal cut set. This means top event for WSN to fail whenever the failure happen at either node A, B, C and E. These nodes have critical impacts and must always function for the network to achieve it connectivity reliability. Then, we able to compute the reliability of system with respect to minimal cut set in (1). To measure the reliability of WSN, we make the following assumptions on individual device probability of success in the network as follow:

- Node A is a resource limited RFD has probability of 70% successful connectivity.
- Node B, C, and D are FFDs with higher resources, have higher probability of 90% successful connectivity.
- Node E, is a base station, assume to have 99.9% of successful connectivity.

By observation a minimal cut set is in a series structure. Hence the calculation of reliability can be directly performed by substituting the successful probability value of WSN components:

\[
\text{Reliability}, R = P (\Phi(X)) = A.B.C.E \\
\ = \ 0.7 * 0.9 * 0.9 * 0.999 \\
\ = \ 0.566
\]

Hence, the reliability of WSN to operate correctly is at 56.6% for the current graph (figure 5). The WSN totally relies on single communication back-bone established by node A, B, C and E. Any failures occur to these components, would bring the network to fail.

To ensure the WSN to resiliently operate, we propose a derived WSN with additional of new node. Figure 7 shows a new topology of WSN model, with implementation of new node to create alternative communication in the event of failure at A, B, C and E components. This WSN now equipped with
new node, N and another sensor, A2 to provide the alternative communication for data to travel from sensors to the sinks.

**Figure 7.** Derivation of new WSN graph model

The presentation of WSN graph in figure 7 is then composed into a Fault Tree as in figure 8.

**Figure 8.** Fault tree diagram

Derivation of minimal cut set of Fault tree in figure 8 is as follow:

*Top Event*

- \((A1BC + A1BD)E + (A1NC + A1ND)E + (A2BC + A2BD)E + (A2NC + A2ND)E\)
- \(A1BCE + A1BDE + A1NCE + A1NDE + A2BCE + A2BDE + A2NCE + A2NDE\)
- \(A1BCE + A2BCE + A1BDE + A2BDE + A1NCE + A2NCE + A1NDE + A2NDE\)
- \(BCE(A1 + A2) + BDE(A1 + A2) + NCE(A1 + A2) + NDE(A1 + A2)\)
- \((A1 + A2)(BCE + BDE + NCE + NDE)\)
- \((A1 + A2)(BC + BD + NC + ND)E\)
- \((A1 + A2)(B + N)(C + D)E \Rightarrow Minimal\ cut\ set\)

Then, WSN reliability shall be calculated as per previous assumptions:
• Node A1 and A2 are RFDs has probability of 70% successful connectivity.
• Node B, C, D and N are FFDs have higher probability of 90% successful connectivity.
• Node E, is a base station, assume to have 99.9% of successful connectivity.

\[ R = P(Y|X) \]
\[ = (A1 + A2)(B + N)(C + D)E \]
\[ = (1 - (1 - 0.7)(1 - 0.7)) (1 - (1 - 0.9)(1 - 0.9))(1 - (1 - 0.9)(1 - 0.9)) (0.999) \]
\[ = (1 - 0.3 * 0.3)(1 - 0.1 * 0.1)(1 - 0.1 * 0.1)(0.999) \]
\[ = 0.8909 \]

The reliability of this WSN to operate correctly is increased to 89.1%.

To conclude, WSN reliability is enhanced with new present of device (node N and existing node A2) deployed to create alternative path to existing communication back-bone. Hence, we get a higher reliability for this new WSN topology compared to previous one.

5. References
[1] Shahabuddin M Z, Hasbullah H and Aziz I 2016 Proc. 3rd Int. Conf. on Computer and Information Sciences (ICCOINS) IEEE pp 259-263.
[2] Pantazis N A, Nikolidakis S A and Vergados D D 2013 Communications Surveys & Tutorials IEEE 15(2) pp 551-591.
[3] Methley S 2009 Essentials of wireless mesh networking (New York: Cambridge University Press)
[4] Venkatesan L, Shanmugavel S and Subramaniam C 2013 Wireless Sensor Network, vol 5(03)
[5] Verdone R, Dardari D, Mazzini G and Conti A 2008 Wireless Sensor and Actuator Networks: Technologies, Analysis and Design (Oxford: Academic Press).
[6] Silva I, Guedes L A, Portugal P and Vasques F 2010 Sensors vol 12 pp 806-838
[7] Ericson C A and Li C 1999 System Safety Conference (Florida) pp 1-9.
[8] Bein B, Jolly B Kumar B and Latifi S 2005 Int. Journal of Information Technology vol 11(2) pp 1-8.
[9] Mahmood M A and Seah W K 2011 Proc. 7th Int. Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP) IEEE pp 377-382.
[10] Kheirreddine M and Abdellatif R 2018 Int. Journal of Technology Diffusion (IJTD) vol 9(4) pp 1-18.