Modeling and Analysis of Multi-type Failures in Wireless Body Area Networks with Semi-Markov Model

Song Wang, *Student Member, IEEE,* and Jong-Tae Park, *Senior Member, IEEE*

***Abstract*—Network reliability is very important in wireless body area network since the vital human life might be jeopardized, unless managed properly. In this article, a new modeling and analysis of node behaviors in wireless body area networks is presented for increasing reliability in the presence of multi-type failures, while saving energy. First, the nodes are classified into types with regard to their capabilities on relaying and sensing. Then, the node behaviors in the presence of failures such as energy exhaustion and/or malicious attacks have been modeled using a novel semi-Markov process. Finally, simulation has been done to evaluate the performance.**

***Index Terms*—WBAN, semi-Markov chain, multi-type failures.**

I. Introduction

Recently, a wireless body area network (WBAN) has been actively researched for monitoring the vital sign of human body. IEEE 802.15.6 TG is currently developing the standard for WBAN. A WBAN is expected to play very significant role for ubiquitous healthcare service. Components of a WBAN consist of multiple sensors, possibly actuators for pumping correct dose of medicine, relay node, and gateway or sink node for forwarding information from sensors into outside networks. All these components are equipped with wireless radio interfaces, and can be configured in star or multi-hop tree due to the power constraints [1].

Since the WBAN is used for monitoring and transmitting vital sign, measuring and increasing the reliability of WBAN is very important research issue. The reliability of WBAN is the ability of the network keeping connected even while suffering from failures and malicious attacks. Malicious users may try to get the patient information such as vital sign and patient ID, using security attacks such as wormholes and spoofing. Failures may be caused by power exhaustion as well as these malicious security attacks. Since medical BAN applications have substantial financial, privacy and human safety implications [2], WBAN nodes should be protected from aforementioned failures and malicious attacks.

In this letter, we present a new model and analysis of node behaviors for reliability analysis of a WBAN, by extending the work in [3]. First, the nodes of WBAN are classified into types in accordance with their capabilities on relaying and sensing. Then, the node behaviors have been modeled using a semi-Markov process. Finally, simulation has been done to evaluate the performance. The proposed model is helpful in analyzing the reliability of WBANs in the presence of failures such as energy exhaustion and/or malicious attacks. The proposed model is also useful for saving energy in the WBAN.

The remainder of this letter is organized as follows. In Section 2, nodes are classified by their functions, and a model of node with multi-type failure is presented. In Section 3, a semi-Markov model is given to model the multi-type failures of the nodes. In Section 4, simulation is proposed. Finally the conclusion is given in Section 5

Manuscript received May 2th, 2009.

The authors are with School of Electrical Engineering and Computer Science, Kyungpook National University, Daegu, Korea (email: jtpark@ee.knu.ac.kr)

This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency) (NIPA-2008-(109008040002-0001000100100))

II. Classification of Nodes With Capabilities on Relaying and Sensing in WBAN

A WBAN is a special type of a wireless sensor networks (WSN) with its own requirement. The monitoring of medical data requires an increased demand for reliability [2]. The sensor which is implemented on the body requires higher energy efficiency. In a typical protocol for multi-hop wireless body area networks, such as LDP [1] and EEMAP [4], sensor nodes are divided into two types: sensor nodes without relaying function, denoted by NO, and sensor nodes with relaying function, denoted by NR.

For sensor nodes without relaying function, node behaviors are modeled as follows. Cooperative nodes, denoted by NO_C, are the nodes that can get the vital information of the human body and send it to the next node. Failed nodes, denoted by NO_F, are the nodes which cannot get the information or cannot transmit it to the next node. Malicious nodes, denoted by NO_M, are the nodes that attack other nodes.

For sensor nodes with relaying function, node behaviors are modeled as follows. Cooperative nodes, denoted by NR_C, are the nodes which can both get the vital information and transmit it to the next node and relay to other nodes. Failed nodes, denoted by NR_F, are the nodes which can neither get the information nor route for other nodes for energy exhaustion or attacks. Stingy nodes, denoted by NR_S, are the nodes which can obtain their information and transmit it to the next node, but cannot route other nodes' information because it may have to save energy for itself or it lacks of power. Semi-active nodes, denoted by NR_A, are the nodes which do not have much power and do not diffuse data for other nodes except the urgent data. Relay nodes, denoted by NR_R, are the nodes which can relay to other nodes but cannot sense the vital information. This classification is mainly based on the functions of nodes in wireless body area network.

III. Modeling of Node Behaviors using Semi-Markov Process Model for Reliability Management

When a node at WBAN misbehaves due to failure and malicious attacks, a node model is much more complicated. By taking into account misbehaving nodes based on their operations in the WBAN, a state space **S** of the node status for nodes NO is defined as **S**={C(cooperative), F(failed), M(malicious)} and for nodes NR, **S**={C(cooperative), F(failed), R(relay), S(stingy), A(semi-active)}.

The node state change may occur at any instant of time due to the power exhaustion and/or security attacks, and the next state is dependent on how long the node resides in the current state, but not on any previous state. Furthermore, the intervals between transitions may have arbitrary distributions, so that continuous-time semi-Markov process is used to model the node behaviors.

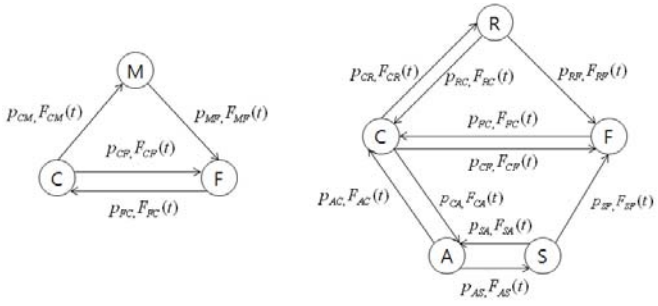
The semi-Markov process $\{F(t)\}$ of node state transition can be defined by

$$F(t) = X_n, \quad \forall t_n \le t < \forall t_{n+1} \tag{1}$$

where X_n denotes the nth state visited, and $\{X_n\}$ is called the embedded Markov chain of the process $\{F(t)\}$ [5]. *F(t)* is the state of process at its most recent transition. The transition probability from state i to state j is defined as follows:

$$\begin{aligned} p_{ij} &= \lim_{t\to\infty} \Pr(X_{n+1} = j, t_{n+1} - t_n \le t \mid X_n = i) \\ &= \Pr(X_{n+1} = j \mid X_n = i), \end{aligned} \tag{2}$$

Then a matrix $\overline{\mathbf{P}} = (p_{ij})$ is the transition probability matrix of $\{X_n\}$. The construction of $\overline{\mathbf{P}}$ can be determined by the observation of empirical results. The state transition diagram of the semi-Markov node model is shown in Fig. 1, which is determined by characteristics of node behaviors.



(a) *(b)*

Fig. 1. The semi-Markov model for nodes without relay function (a) and with relay function (b)

Characteristics of node behavior of WBAN are provided below:

- A cooperative node may become failed node or malicious node due to various reasons. For nodes with relaying function, the nodes may become relay nodes or semi-active nodes for sensor error and/or power saving.
- A failed node may become a cooperative node if this node is recovered or rebooted.
- A stingy node can be changed to a semi-active node by means of power recharge. And a stingy node can become a failed node due to power exhaustion, but it can not become a relay node directly.
- A malicious node can only become a failed node.
- A relay node can be converted to a cooperative node for reconfiguration. It can also become a failed node.

By considering the node behavior above, the transition probability matrix of $\{X_n\}$ of WBAN is given below:

For nodes NO:

$$\overline{\mathbf{P}} = \begin{pmatrix} p_{CC} & p_{CM} & p_{CF} \\ p_{MC} & p_{MM} & p_{MF} \\ p_{FC} & p_{FM} & p_{FF} \end{pmatrix} = \begin{pmatrix} 0 & p_{CM} & p_{CF} \\ 0 & 0 & p_{MF} \\ p_{FC} & 0 & 0 \end{pmatrix} \tag{3}$$

For node NR:

$$\overline{\mathbf{P}} = \begin{pmatrix} p_{CC} & p_{CS} & p_{CR} & p_{CA} & p_{CF} \\ p_{SC} & p_{SS} & p_{SR} & p_{SA} & p_{SF} \\ p_{RC} & p_{RS} & p_{RR} & p_{RA} & p_{RF} \\ p_{AC} & p_{AS} & p_{AR} & p_{AA} & p_{AF} \\ p_{FC} & p_{FS} & p_{FR} & p_{FA} & p_{FF} \end{pmatrix} = \begin{pmatrix} 0 & 0 & p_{CR} & p_{CA} & p_{CF} \\ 0 & 0 & 0 & p_{SA} & p_{SF} \\ p_{RC} & 0 & 0 & 0 & p_{RF} \\ p_{AC} & p_{AS} & 0 & 0 & 0 \\ p_{FC} & 0 & 0 & 0 & 0 \end{pmatrix} \tag{4}$$

The "0" in the matrix means that it is not possible to make transition between the two states. $\{F(t)\}$ is also associated with the time distributions between two successive transitions. Let T_{ij} denote the time spent in state i given the next state j. Then $F_{ij}(t)$ is a commonly used notation for cumulative distribution function (CDF) of T_{ij}, defined by :

$$\begin{aligned} F_{ij}(t) &= \Pr(T_{ij} \le t) \\ &= \Pr(t_{n+1} - t_n \le t \mid X_n = i, X_{n+1} = j) \end{aligned} \tag{5}$$

where $i, j \in \mathbf{S}$.

By knowing the transition probabilities p_{ij} and transition time distributions $F_{ij}(t)$, which are defined above, the probability that a node is in a certain state i can be obtained as in [5]:

$$p_i = \lim_{t\to\infty} P(F(t) = i \mid F(0) = j) = \frac{\pi_i \eta_i}{\sum_{k\in S} \pi_k \eta_k} \tag{6}$$

Here, π_i is the stationary probability of state i of X_n and η_i is the expected holding time in state i.

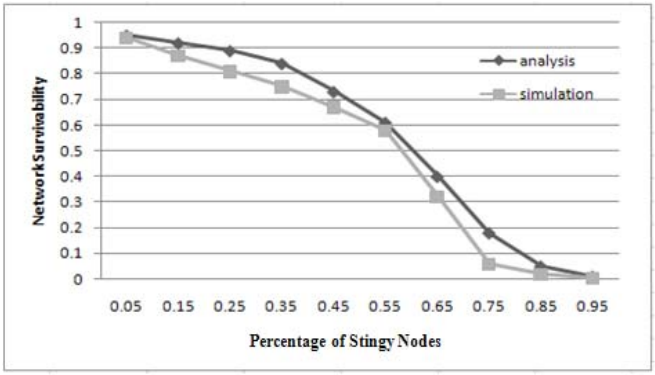
IV. Simulation and Analysis

In this work, NS2-v2.33 is used to perform the simulation. The simulation environment is shown in Table 1. Constant Bit Rate (CBR) is chosen for traffic and the traffic is ranged from 10kbps to 200kbps. As there is no MAC standard about WBAN, IEEE802.15.4 is used for the simulation environment. The results are averaged over multiple simulation rounds conducted with various random seeds.

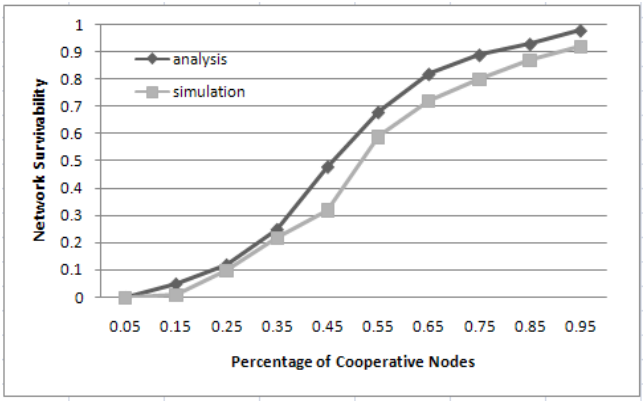
In simulation, we experiment how the matrixes affect the network reliability. In this article, the reliability of the WBAN is measured in terms of network survivability. The network

survivability is defined how many percentage of the nodes can work in the WBAN. To calculate the survivability, the received packets from the sensor node to the sink node are accounted. In other words, survivability of the networks is the percentage of the nodes which can communicate with the sink node.

In Fig. 2 (a), the curves indicate that the survivability decreases as the more stingy nodes are present. Nevertheless, the survivability does not change significantly when there is only a small amount of stingy nodes.



(a) The effect of stingy nodes on network survivability



(b) The effect of cooperative nodes on network survivability

Fig. 2. The effect of stingy and cooperative nodes on network survivability

Fig. 2 (b) shows the effect of cooperative nodes on network survivability. The network survivability is very low when the number of cooperative nodes is very low. But when the number of cooperative nodes reaches to some threshold, the survivability of the network increased sharply.

To further investigate the impacts of the misbehaving nodes on network performance, we evaluate the normalized goodput which is the ratio between the data received by destinations and the data sent by sources. Fig. 3 shows that the normalized goodput in the network decreases sharply as there are more misbehaving nodes. This impact is particularly severe when the percentage of misbehaving nodes is low. For example, when the ratio of misbehaving nodes increases up to 20%, the performance deterioration is more than 40%. When the ratio of misbehavior nodes is more than 60%, the normalized goodput is around 30%. The reason for drastic degradiation on goodput is that all abnormal nodes incursevere packet losses and disrupt normal data delivers in all network scenarios.

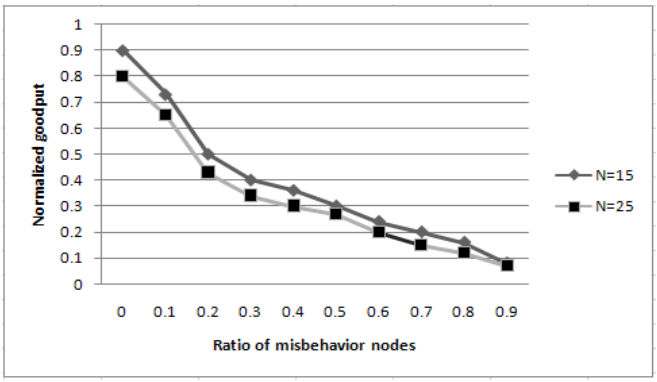


Fig. 3. Impacts of misbehavior nodes (stingy nodes and malicious nodes) on network goodput

V. Conclusion

In this paper, we have presented modeling and analysis of multi-type failures in WBAN. In order to do that, the nodes of a WBAN were classified into two types based on the node functions in the network, and then the misbehavior nodes were classified based on the node types and their operations. A semi-Markov process has been proposed for modeling the node behaviors. A simulation has been done to show the impact of misbehavior nodes on the network reliability. This is believed to be the first attempt to model the misbehavior nodes in WBANs which is very useful to analyze the reliability of the WBANs. Further research work may include performing correlation studies between real test-bed measurements and simulation results.

Acknowledgments

The authors would like to thank anonymous reviewers for their valuable comments.

References

[1] B. Latre, B. Braem, etc., "A low-delay protocol for multihop wireless body area networks," in Proceedings of the 4th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous '07), pp. 1–8, 2007.

[2] B. Zhen, M. Patel, S. Lee, and E. Won, "Body Area Network (BAN) Technical Requirements," IEEE 802.15.6 Technical Requirements Document, v 4.0, 2008.

[3] F. Xing and W. Wang, "Modeling and analysis of connectivity in mobile ad hoc networks with misbehaving nodes," in Proc. of IEEE Conf. on Comm. (ICC'06), June 2006, pp. 1879-1884.

[4] O. Omeni, A. Wong, A. and J. Burdett, "Energy efficient medium access protocol for wireless medical body area sensor networks," IEEE Trans. Biomedical Circuits and Systems, vol. 2, no. 4, 2008.

[5] S. M. Ross, Stochastic Processes, John Wiley and Sons, 1983.