Formulation of Fuzzy Correlated System for Node Behavior Detection in WSN

Noor Shahidah, A. H Azni
Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM).
shahidah_ishak93@yahoo.com

***Abstract*—Wireless Sensor Network depends highly upon the cooperation among the nodes behavior in transmission of packet data, messages and route discovery. Over open medium environment, nodes are free to move and may change their behavior arbitrarily. In the presence of misbehavior node in some cases, it may instigate its neighboring nodes to compromise with the misbehaved node. Thus, this has resulted to a spreading of correlated node behavior and the impact of this event may result in high severity in network performance. Therefore, fuzzy logic model is proposed to formulate the correlated node behavior in WSN. The formulation of correlated node behavior based on fuzzy logic function of peer nodes real parameter measurement is investigated to determine the status of the node and then the fuzzy neural network will model the correlated node behavior occurrence. The accuracy of the results is established via sensor network simulation. The result of this study is providing a fundamental guideline for network designer in order to understand the fault-tolerance in network topology.**

***Index Terms*—Correlated Node Behavior; Fuzzy Logic System; Neural Network; Wireless Sensor Network.**

I. INTRODUCTION

Wireless sensor network (WSN) with several detection stations commonly known as sensor nodes connect wirelessly with low deployment, low data usage cost and self-organized system [1]. The availability of WSN is important in many advance monitoring and control applications including telecommunication, biomedical and geographical controller. The operation of the WSN depends highly on the cooperation of nodes during routing, network monitoring and packet forwarding. In harsh environment, however, the complex structure of the network and with no central monitoring scheme of the network yield to high vulnerability of security attack in this network. Thus, it is difficult to guarantee for nodes to cooperate consistently and maintain network operation.

Early research found nodes exhibit independent failure, but it is against the recent studies. For example, Thanakornworakij in [2] stated that an interruption in network application may cause by only a single node failure. While Yu Xi in [3] also mentioned that a series of failures are instigated by the earlier nearby failure. This scenario commonly called correlated node event or correlated node failure. The correlated failure, on the other hand, imposed high severity upon network availability and connectivity. A number of methods to detect the correlated node behavior presented previously, meanwhile they did not consider the uncertainties inherited in the network environment and lack in detection accuracy.

Therefore, a novel fuzzy approached introduced by [4] is used in this research. In fact, fuzzy logic approaches in node behavior detection had a capability to blend several parameters to determine node behavior besides provide more flexibility and simplicity for accurate representation. For this research, the status of node behavior will be determined through a function of peer nodes real parameter measurement. Then a model of correlated node behavior is developed using fuzzy neural network. Next, to evaluate the model accuracy and availability, several evaluation tests will be conducted according works in [5].

The rest of this paper is organized as follows. Section II explains related work on the correlated fuzzy function in node behavior detection. Section III discusses proposed formulation of fuzzy correlated function. Evaluation metrics presented in Section IV. Then, Section V is presentation of preliminary results. Finally, Section VI offers conclusion of the works.

II. RELATED WORKS

Fuzzy behavioral model has been studied in recent years. Previous works attempt in correlated node behavior detection using fuzzy inference system which is a human-based logical interpretation that provide a powerful technique for behavioral node detection with high accuracy detection. Such work in [6] Khan et al. identified faulty node by analytical fault detection scheme. It examined the deviation of parameter measurement between fuzzy model estimation of neighboring nodes and the real parameter measurement of particular node in order to diagnose the failures in the network operation. In addition, a distribution of faulty node has determined via adaptive neuro-fuzzy inference system (ANFIS) in [7]. This work has implemented in industrial steam turbine. Here ANFIS do interpret the combinatory nature of data besides possibly able to handle high degree of interaction in systems consisting multiple inputs and outputs.

While the distribution of anomaly due to malicious behavior, study in [8] has employed Fuzzy Misuse Detector Module (FMDM) with the main objective to identify the anomaly conditions received from the traffic. The study conducted by [5] meanwhile has proposed a mixture of fuzzy logic with comparative correlation techniques namely fuzzy spatial act, fuzzy attribute act and fuzzy temporal act. This method has improved the data accuracy in the wireless sensor network together with the increased of network lifetime. Despite that previous methods only dealt with certain type of node behavior which is failed behavior or on particular malicious behavior.

According to [9] besides failed nodes, some node may in the state of malicious, selfish and also failed behavior. Therefore, this research attempt to model correlated node behavior detection which cater different state of node

behaviors which are; cooperative, selfish, malicious and failed. Parameters such as energy usage, buffer size, time response, count and data packet are the parameters that can determine the node behavior [8]

Hence, a proposed method in this study attempts to use a fuzzy correlated function to determine and formulating correlated node behavior in wireless sensor network. A function of peer nodes parameter measurement determines different state of node behavior. In addition, Fuzzy Neural Network applied for modeling correlated node behavior purposes.

III. Proposed Formulation of Fuzzy Correlated System

The fuzzy logic modelling for correlated node behavior involves two stages which are the status of node behavior determination by employing a function of peer nodes parameter and compared with its real parameter value. Meanwhile, the correlation model is adopting a fuzzy neural network to determine the correlated node behavior occurrence.

A. Status of node behavior determination

In this research, parameters such as energy level and number of data packets will determine the status of node behavior at particular time. At the first step the neighboring nodes which located at the same transmission range will decide the current status of particular node behavior using the differences of the real parameter value of specific node and its neighboring node parameters value. According to [6] the status of sensor parameter of A_i can be approximated by an m-variable function f of its neighboring sensor parameter, represented by

$$x_i^k \approx f(x_{i_1}^k, x_{i_2}^k, \dots, x_{i_m}^k) \tag{1}$$

where: x_i^k = Parameter value by node A_i at kth instant of time,t_k.

$x_{i_m}^k$ = Parameter value of peer nodes

For a homogenous parameter value, the difference between the measured values at a cooperative node behavior with the measured values of its neighbors, is bounded. Suppose A_i has m neighbors, i.e., $N(A_i) = \text{m}$. Let this neighbors be denoted by:

$$N(A_i) = \{A_{i_1}, A_{i_2}, \dots, A_{i_m}\} \tag{2}$$

Thus, if A_i and A_{i_m} are neighbors then in case of possessing misbehavior nodes (malicious, selfish or failed node) the following condition is satisfied:

$$x_i^k - x_{i_j}^k \geq \delta_{i,i_j}^k \text{ for } 1 \leq \text{j} \leq \text{m} \tag{3}$$

where: δ = Tolerance

The tolerance will vary depending the status of the nodes which denotes by δ_m, δ_s and δ_f for malicious, selfish and failed node respectively. Equivalently Equation (3) can be written as:

$$x_i^k = x_{i_j}^k + \epsilon_{i,i_j}^k \text{ for } 1 \leq \text{j} \leq \text{m} \tag{4}$$

where ϵ_{i,i_j}^k denotes the difference between the ith sensor measurement and that of its jth at the instant t_k. hence we get

$$mx_i^k = \sum_{j=1}^{m} x_{i_j}^k + \epsilon_{i,i_j}^k \tag{5}$$

$$x_i^k = \frac{1}{m}\sum_{j=1}^{m} x_{i_j}^k + \epsilon_{i,i_j}^k \tag{6}$$

where Equation (6) is the simplification of Equation (5) which represents a relationship between the real sensor parameter of the node A_i and the sensor parameter of all of its neighbors.

The process of node status determination in this part implements using fuzzy logic system, which consist of three steps as shown in Figure 1. In the first step which is fuzzification stage, the input parameter converts into related degree of membership function as Figure 2. The second step which is fuzzy inference system (FIS). Here FIS are conducted on the basis of Takagi-Sugeno-Kang (TSK) FIS. Several inference rules will be generated which can be written as the following statement:

R^l: IF x_1 is B_1^l and x_2 is B_2^l and …x_n is B_n^l THEN y is y^l

where R^l (j=1, 2, …, M) denotes the lth implication, x_j (j= 1,2, …, n) are input variables of the FIS, y^l is a singleton, B_j^l is the fuzzy membership function which can represent the uncertainty in the reasoning. In the fuzzy inference engine the corresponding rules are activated and all the activations are accumulated using min-max operations. Lastly, in defuzzification stage, the output of the fuzzy system is expressed by:

$$y = \frac{\sum_{l=1}^{n} \alpha_l y^l}{\sum_{l=1}^{n} \alpha_l} \tag{7}$$

where α_l denotes the overall truth value of the ith implication, and is computed as:

$$\alpha_i = \prod_{l=1}^{M} A_l^i(x_i) \tag{8}$$

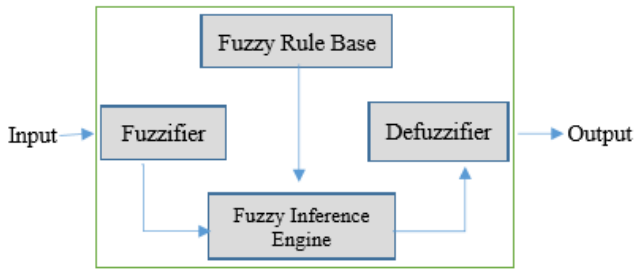

Figure 1: Fuzzy logic system

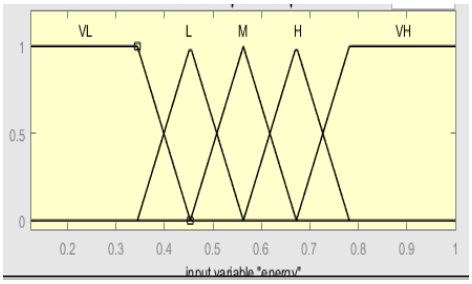

Figure 2: Input membership function

B. Correlated nodes behavior modeling

The spreading capability of node behavior is defined as a sequence of temporal and spatial dependent event. Where the sensor transmission range generally overlap and therefore when an event occur at t_i, it triggers the multiple sensors in the same region at $t_{i+1.}$ Hence, this study propose a fuzzy neural network (FNN) system illustrated in Figure 3 which imitates human brain to perform connectionist structures. In general, there are three layers in FNN [10]. First is the input layer that simply spread the inputs to the next layer. In this layer, the correlated behavior is model as the weighted of membership function of particular input variable. The second layer which is a hidden layer, fuzzifies the inputs into linguistic variables according fuzzy set membership function. While in this layer also, rules are generated where consequent fuzzy variable is represented by arrows from certain fuzzifying nodes. The last layer which is the third layer is defuzzification layer. Thus we tend to use this fuzzy NN system to model correlated node behavior detection scheme. Using FNN system, nodes in same transmission range are crossly mapped to form complex relationship between input and output variables, and thus we can directly acquire knowledge about these relationships from the data.

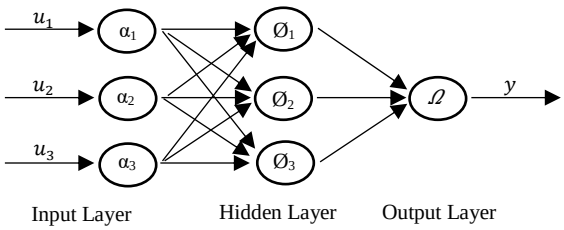

Figure 3: Fuzzy Neural Network System

In training of fuzzy NN system, the input vector $\propto = [\propto_1, \propto_2, \ldots, \propto_n]$ represent the parameter value such as energy level, distance and packets data. The M x N matrix denote by $\mathbf{U} = [\beta_{i,j}]$ and represents the input-to-hidden layer weights. The activation function of each of the hidden layer is illustrated by $\emptyset_p$ for p = 1,2,..j. The activation functions in vector form denotes by $\emptyset^T = (\emptyset_1, \emptyset_2, .., \emptyset_p)$. While the hidden-to-output layer weight illustrated by the vector $\mathbf{w}^T = (w_1, w_2, .., w_j)$. Hence the activation of the output layer is depicted by Ω. The single scalar output y is the confidence level of correlated node behavior detection and measured by Equation (9).

$$\Omega = \left\{\sum_{j=1}^{n} w_j \emptyset_j \left(\sum_{i=1}^{n} \alpha_i \beta_{i,j}\right)\right\} \quad (9)$$

Thus, the format of the rules will be described as follows:

R^l: IF x_1 is $\mu^l(x_1)$ and x_2 is $\mu^l(x_2)$ and …x_n is $\mu^l(x_n)$ THEN y is y^l

where R^l (j=1,2,…,M) denotes the lth implication, x_j (j= 1,2,…,n) are input variables of the FIS, y^l is a singleton, $\mu^l(x_i)$ is the fuzzy membership function which can represent the uncertainty in the reasoning

IV. Experimental Setup

For the evaluation purposes, a simulation will be conducted in MATLAB version 2015 environment using an experimental dataset from Cyber Security Lab Malaysia. The data has skeleton structure as illustrated in Table 1.

Table 1
Skeleton Structure of Data Set

Date: Yyy-mm-dd	Time: Hh:mm:ss: xxxx	Node ID:	Forwarding packet data:	Energy level:	Distance:

We consider a network with 100 nodes randomly distributed in a 1000 meter x 1000 meter area. Each node is free to move following random waypoint mobility model with an average speed 4 meter/second and has 500 meter transmission range. The time step to simulate the scenario is 80 hours. During the simulation, the behavior of the node changes according to the energy resources available for its routing and forwarding packet ratio. In order to calculate the correlated event occurrence, a collection of neighborhood statistics of each node per 10 hours is needed, together with the number of neighbors and behavior of each neighbor.

V. Preliminary Results

In this paper, the discussion of the result has focused mainly on the determination of the status of node behavior corresponds to the first stage of this model.

At T time, suppose one want to determine the current status of node behavior of the node $A_{i,}$ while node A_i has three neighboring nodes. Thus the input for the initial TSK FIS is $\boldsymbol{x_{FIS}} = (x_{i_1}^k, x_{i_2}^k, x_{i_3}^k)^T$ and the output $\boldsymbol{y_{FIS}} = x_i$. The type of membership function for input vector depends upon the range of parameter being measured. Suppose one is using three membership function for each peer nodes parameter value, so the total number of rules are 3^m where m represents the number of inputs.

The preliminary result in this stage is according to the work proposed by [6] whereby the deviations between the estimated parameter value from the real parameter value of node A_i are represented in Figure 4. The estimated parameter is the average parameter value of the neighboring node. For instance, this figure illustrates that for the entire 80 hours, the result shows for the first 10 hours; the node is behaving normally whereas on the 11th hours onwards, it portrayed a gradual misbehavior node pattern until the end of the simulation period. From here, we can determined the type of node behavior by comparing the deviation value of real parameter and the FIS parameter with the threshold values, δ for the malicious, selfish and failed node respectively.

In contrast to the work done in [6,8], the proposed model in this study rather capable to specify the different state of misbehavior node instead of the only failed behavior. Furthermore, the early detection of misbehave node may also

provide an opportunity for the network designer to prevent any network from further deterioration [11]. In general, this multi-nodes cooperation of misbehavior node detection is signifying an effective mechanism to improve misbehavior detection accuracy with cost effective which is without additional sensor detection for failure event occurrence. In addition, it is also improved the system detection robustness [6,12].

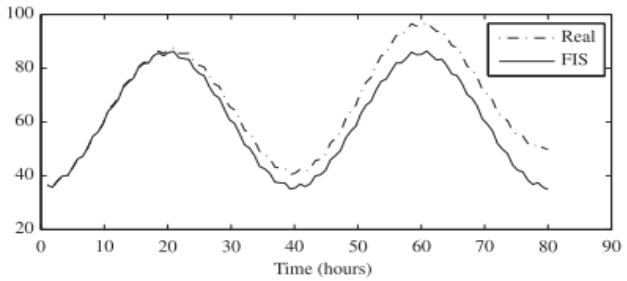

Figure 4: Real parameter value and FIS value within 80h

Once, the current status of the node has been determined, the second stage of the model which is identifying the correlated behavior event will be implemented using the fuzzy neural network. In fuzzy neural network, the spreading of correlated node behavior will be explained using the weightage or the degree of membership function of the inputs used. However, in this paper, we only interested to capture the status determination of node behavior which are selfish, malicious and fail node for the analysis. Hence, for the evaluation of the correlated node will discuss in the next paper. Since the fuzzy neural network has the combination advantage of both fuzzy theory and neural network, therefore it assumes to provide the stronger ability and self-adapting learning ability. Thus, the FNN system can enhance the accuracy detection of correlated node behavior in wireless sensor network.

VI. Conclusion

In this paper, the study proposed the formulation model of fuzzy correlated system for node behavior detection in Wireless Sensor Network. The model basically represents the flexibility of the node behavior determination using fuzzy logic. In addition, the fuzzy logic is capable to confront the uncertainties in the wireless sensor network. The model observes the neighboring node behavior in routing operation between a source and a destination. Therefore, the performance of a network is highly dependent on the performance of nodes in a cluster represented by the level of cooperation by the intermediary nodes. For this model, the behavior of node can be regulated by the energy level, packet forwarding and the distance of the nodes. The simulations results show that the node behavior detection based on fuzzy logic system outperform the existing method in terms of its accuracy.

References

[1] J. Sen, "Sustainable Wireless Sensor Networks," *Sustain. Wirel. Sens. Networks*, pp. 279–309, 2010.

[2] T. Thanakornworakij, R. Nassar, C. B. Leangsuksun, and M. Paun, "The Effect of Correlated Failure on the Reliability of HPC Systems," *Parallel Distrib. Process. with Appl. Work. (ISPAW), 2011 Ninth IEEE Int. Symp.*, pp. 284–288, 2011.

[3] Y. Xu and W. Wang, "Characterizing the spread of correlated failures in large wireless networks," *Proc. - IEEE INFOCOM*, 2010.

[4] L. A. Zadeh, "Fuzzy logic systems: origin, concepts, and trends," 2004.

[5] B. Nisha U, U. Maheswari N, V. R, and Y. Abdullah R, "Improving Data Accuracy Using Proactive Correlated Fuzzy System in Wireless Sensor Networks," vol. 9, no. 9, pp. 3515–3538, 2015.

[6] S. A. Khan, B. Daachi, and K. Djouani, "Application of fuzzy inference systems to detection of faults in wireless sensor networks," *Neurocomputing*, vol. 94, pp. 111–120, 2012.

[7] K. Salahshoor, M. S. Khoshro, and M. Kordestani, "Simulation Modelling Practice and Theory Fault detection and diagnosis of an industrial steam turbine using a distributed configuration of adaptive neuro-fuzzy inference systems," *Simul. Model. Pract. Theory*, vol. 19, no. 5, pp. 1280–1293, 2011.

[8] S. Shamshirband *et al.*, "Co-FAIS: Cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 42, pp. 102–117, 2014.

[9] T. V. P. Sundararajan and A. Shanmugam, "Modeling the Behavior of Selfish Forwarding Nodes to Stimulate Cooperation in MANET," *Int. J. Netw. Secur. Its Appl.*, vol. 2, no. 2, 2010.

[10] C. G. Looney and S. Dascalu, "A Simple Fuzzy Neural Network," *In CAINE*, pp. 12–16, 2007.

[11] V. Duraisamy, N. Devarajan, D. Somasundareswari, a. A. M. Vasanth, and S. N. Sivanandam, "Neuro fuzzy schemes for fault detection in power transformer," *Appl. Soft Comput.*, vol. 7, no. 2, pp. 534–539, 2007.

[12] J. Tian and M. Gao, "Intelligent community intrusion detection system based on wireless sensor network and fuzzy neural network," *2009 ISECS Int. Colloq. Comput. Commun. Control. Manag.*, pp. 102–105, 2009.