

Performability of Retransmission of Loss Packets in Wireless Sensor Networks

Imeh Umoren¹, Daniel Asuquo², Onukwughu Gilean³ & Mfon Esang⁴

¹ Department of Computer Science, Akwa Ibom State University, MkpataEnin, PMB 1167, Nigeria

² Department of Computer Science, Faculty of Science, University of Uyo, PMB 1017, Uyo, Nigeria

³ Department of Computer Science, Federal University of Technology, Owerri, Nigeria

⁴ Department of Computer Science, Federal Polytechnic, Ukana, PMB 2014, Ikot Ekpene, Nigeria

Correspondence: ImehUmoren, Department of Computer Science, Akwa Ibom State University, MkpataEnin, PMB 1167, Akwa Ibom State, Nigeria. Tel: 234-803-681-3637. E-mail: imehumoren@aksu.edu.ng

Received: February 1, 2019 Accepted: February 27, 2019 Online Published: March 28, 2019

doi:10.5539/cis.v12n2p71 URL: <https://doi.org/10.5539/cis.v12n2p71>

Abstract

Latest progress in wireless communication technology has enabled the development of low-cost sensor networks with major concern on quality of service (QoS) provisioning. Wireless sensor networks (WSNs) can be adopted in various application domains but each use is likely to pose peculiar technical issues. Basically, we demonstrate that congestion, packet loss and delay have strong influence on the performance of WSNs. In order to implement a realistic sensor network policy to resolve the problem of data delay and avoidance of collisions that lead to packet losses, we develop a system that guarantees QoS in WSNs using Fuzzy Logic Controller (FLC) for sensitivity analysis of the effect of adaptive forward error correction (AFEC). The AFEC approach improves the throughput by dynamically tuning FEC subject to the nature of wireless channel loss thereby optimizing throughput, sensor power utilization, while minimizing traffic retransmission, bit error rate (BER), and energy consumption. Basically, parameters such as packet delivery ratio, packet loss, delay, error rate, and throughput are appraised. The system has a spread procedure which is able to schedule the transmission of the nodes in order to have a data flow that converges from the furthest nodes toward the fusion centre. The key benefit of the scenario showed that, after extensive simulation using realistic field data, the procedure permits a practical approach to obtaining optimal solution to loss packets retransmission problem in WSNs giving a strong improvement on QoS provisioning.

Keywords: WSN, QoS guarantee, packets retransmission, bit error rate, packets deliver ratio, fuzzy logic

1. Introduction

Due to recent technological advancement in network communication, manufacturing of small and low cost wireless sensor nodes (SNs) has become technically and economically feasible. Owing to their limited size, weight and ad-hoc method of deployment, the available power and memory size are limited. Wireless sensor networks (WSNs) are a set of small sensor nodes with the sink for data collection (Akyildiz *et al.*, 2002). Wireless communication has the reputation of being unpredictable. The quality of wireless communication depends on the environment, the part of the frequency spectrum under use, the particular modulation schemes under use, and possibly on the communicating devices themselves. Communication quality can vary dramatically over time, and has been reputed to change with slight spatial displacements. As a result of this, and the paucity of large-scale deployments, it is perhaps not surprising that there have been no medium to large-scale measurements of ad-hoc wireless systems.

WSNs have a wide range of applications in environmental monitoring, habitat observation, health monitoring and so on. In a typical application, intermediate nodes (or sensors) need to forward the data originating from multiple sources. Due to limited memory, the buffer of intermediate nodes may start overflowing, resulting in loss of valuable packets. Consequently, retransmission of the same packet will be required which causes unnecessary power loss. In WSNs, the battery power and memory are available in very limited amount and efficient use of available buffer and power is highly desirable. Each SN is made of hardware components which include a radio transceiver, an embedded processor, internal and external memories, a power source and one or more sensors (Sharma & Aseri, 2012). The embedded processor schedules tasks, processes data and controls the functionality

of other hardware components; transceivers are responsible for wireless communication of SNs; memory is for storage; the power source provides power consumed through sensing, communication and data processing; while a sensor which can be more than one in each SN produces a measurable response signal to a change in physical condition of the environment in which the SNs are deployed. The nodes have certain area of coverage for which they can reliably and accurately report the particular quantity they are observing. These nodes are densely deployed in a targeted phenomenon to communicate with each other by transmitting information called packets from one point to another and then to the base station. During such transmissions, some packets may be dropped or lost due to certain factors such as data collision, buffer overflows, sensor failure, quality of wireless channel and congestion. Consequently, this results to retransmission of lost packets (Lozoya *et al.*, 2016), which invariably causes a significant amount of energy loss and delivery delay. There is need to provide packet reliability in WSN by ensuring successful transmission of all packets or at certain success ratio. To optimize the much needed system performance, transport layer protocols are used to decrease congestion and reduce packet loss so as to provide fairness in bandwidth allocation and to guarantee end-to-end reliability (Sharma & Aseri, 2012). The motivation behind congestion control is to provide high data rate transmission with high efficiency and reliability. In WSNs, fuzzy logic is used for improving decision-making, reduce resource consumption, and increase performance of the network. Some of the areas it has been applied to are cluster-head election (Kim *et al.*, 2007), security (Kim & Cho, 2007), data aggregation (Lazzerini *et al.*, 2006), routing (Kim & Cho, 2007), MAC protocols (Xia *et al.*, 2007), and QoS (Munir *et al.*, 2007). However, many existing systems have not implemented fuzzy logic to control congestion. This paper deals with Fuzzy Logic Controller (FLC) to control congestion.

This paper is aimed at identifying loss packets during transmission, which provides an opportunity to study the trend of packet loss, its effect on the network turnover and how the lost packets can be retransmitted in order to achieve intended result and meet some goals of WSNs. The approach employed in identifying and resolving packet loss problem in WSN is by simulating a wireless sensor environment. The simulation shows the model of a typical WSN with SNs communicating at different positions, each with an identity and detection of the number of packets sent by each node as they communicate via transmission of packets. The simulated sensor network enables communication by organizing sensors into clusters that pass messages to a centralized location called the base station.

2. Congestion and Packet Dropping in WSNs

Congestion generally occurs due to the packet arrival rate exceeding the packet service rate. This is more likely to occur at sensor nodes close to the sink, as they usually carry more combined upstream traffic. Data transfers over wireless networks are more susceptible to loss than over wired networks. This is because in wired networks, data loss occurs primarily due to congestion, whereas there are many other reasons for data loss in wireless networks, in particular WSNs - such as quality of wireless channel, node failures, environment interface, etc. Congestion also arises on the wireless link due to noise, interference, contention, or bit synchronization errors (Wang *et al.*, 2006). Thus, reliability is one of the important criteria for evaluating the quality of WSNs and it covers not only transport reliability issues but also the ability to sense physical phenomenon. Reliability in WSNs can broadly be categorized into two, viz; event and packet reliability. Whereas event reliability deals with reporting an event to the BS in an efficient manner, packet reliability is concerned with successful transmission of all packets or at certain success ratio. Transport layer protocols applied to WSNs can handle the communications between the sink node and sensor nodes in upstream (sensor-to-sink) or downstream (sink-to-sensor) direction (Sharma & Aseri, 2012). Although TCP and UDP are popular transport layer protocols for the Internet, neither may be good for WSN as there are no interaction between TCP or UDP with lower layer protocols such as routing and MAC algorithms (Wang *et al.*, 2005) (Sohraby *et al.*, 2007). Packet droppings in WSNs may involve the transport layer, and hence the need to study and possibly contribute to reliable protocol design of this layer. Therefore, it is necessary to retransmit lost packets in an unreliable network medium to maximize data transmission throughput. WSNs must guarantee certain reliability value at packet-level or application-level through loss recovery in order to abstract correct information. The existing approach for detecting packet dropping attacks requires that the destination is sent information about how many packets the source should send to it, next. The initial packet contains count number, i.e., the count of packets to be transmitted including sequence numbers in packets. It first finds out one shortest route using appropriate routing protocol (Kim & Cho, 2007) and then sends all packets through that selected route. If packet is received by destination node, the destination sends back the acknowledgement to the appropriate sender. A source that does not receive a reply from its destination should be able to guess that packets are being dropped by an attacker or due to collisions, congestion, buffer overflow, etc. The basic idea works as follows: an intermediate node that forwards a packet to the next node on the path but does not receive a reply within a timeout period guesses that its neighbour is dropping packets. Then, it informs the source about this

misbehaviour of the neighbour. The source node finally chooses another route to reach the destination node. The attacker can drop all the packets including the initial packet so it will not help the source node find out the particular dropped packet.

Figure 1 shows a simple structure of a WSN comprising a large number of SNs which are deployed randomly. The size of a SN is small and associated resources like battery power, processing capabilities, memory and buffer size are limited. Nodes are autonomous and sense environmental conditions like temperature, pressure, sound, etc. in order to collect the respective data and pass the data to the main server. As resources are limited, they must be put to use efficiently. Basically, the SNs sense and process the information which becomes transmitted as data packets to the sink. When an event occurs within the network, a large number of SNs will report their data packets to the sink. As these large numbers of SNs become active in transmitting data packets, the load becomes heavy as traffic increases thereby, leading to congestion in the network (Wang *et al.*, 2006) (Chakravarthi *et al.*, 2010) (Chakravarthi & Gomathy, 2011). Due to unpredictable fluctuations and bursty nature of traffic flow in the network, congestion occurs frequently (Pitsillides *et al.*, 1997). The problem of congestion has become more severe due to increased use of the internet for high speed, delay sensitive applications with varying Quality of Service (QoS) requirements (Chrysostomou *et al.*, 2009). During congestion, it is evident that the source transmission rate exceeds the data handling capacity of the network causing inefficient management of network resources and severe degradation in system performance. Furthermore, if the source delivers at a rate higher than the queue service rate, then the size of the queue is expected to grow. For a finite queue length, it is certain that the network will suffer from high error rate, low throughput, and decrease in packet delivery ratio as end users will experience packets delivery delay and packet losses (Chrysostomou & Pitsillides, 2005).

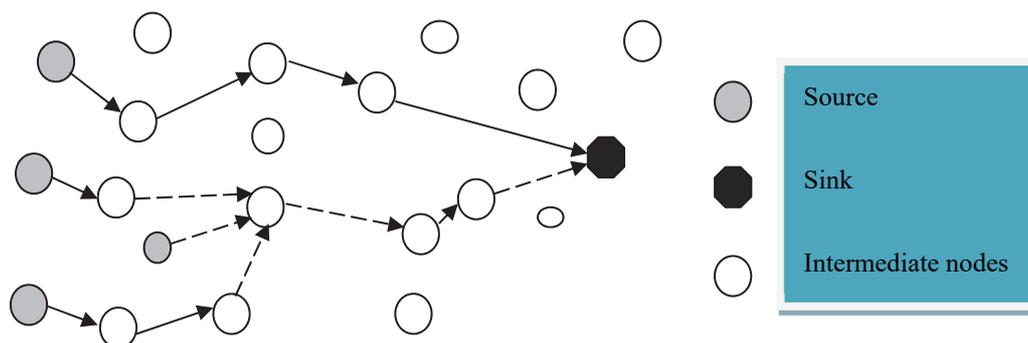


Figure 1. Simple structure of a WSN

In recent past, fuzzy logic (FL) has been used in practical applications because of its ability to reduce complexity, improve efficiency and robustness of the system under study through the incorporation of human expert knowledge into rule-based frameworks (Aggarwal *et al.*, 2013) (Ekpenyong *et al.*, 2014). FL technique is adopted in this paper to study congestion because it requires less memory and processing capability and is best suitable for systems that do not have exact mathematical models as solutions to their problems. For WSN, the topology changes very frequently due to node failure and the random deployment nature of the SNs with constraint on resources, makes FL technique best suitable for performance modelling of retransmission of loss packets. The purpose of our fuzzy routine is to adjust the transmission rate of the sensor nodes, so that the performance of the network is improved. The performance of the network can be improved by reducing the packet drop and increasing the network throughput. Thus, the fuzzy rule base has been turned so as to not only decrease packet drop but also increase the network throughput.

3. Method

The methodology adopted in this paper includes data collection and description, model formulation, design of FL-based model for performance evaluation of loss packets retransmission, as well as development of membership function (MF) plots, fuzzy rules-base (fuzzy inference mechanism) in MATLAB for prediction of impacts of considered input parameters on reliability of WSNs.

3.1 Data Collection and Description

Analytical data were collected and used since a WSN's topology changes very frequently due to node failure and random deployment nature of the SNs. The focus of this paper is on controlling congestion in WSNs which is a major cause of degraded network performance thereby leading to packets loss. Data were collected on parameters

or factors that enhance evaluation of reliability of WSNs. Factor investigated include number of packets, throughput, error rate, delay, and packet delivery rate. These data obtained are as summarized on tables 1 and 2 (Jebarani & Jayanthi, 2010).

Table 1. Values of collected data

No. of packets sent	Throughput	Error rate	Delay	Packet delivery ratio
512	4994.05	0.96	49.71	96.97
1024	5930.25	0.96	45.76	96.70
1536	10764.13	0.25	31.98	96.21
2048	14636.18	0.29	25.33	98.97
2560	31408.85	0.32	17.12	98.97

Table 2. Mean values of collected data

Parameter	Average value
No. of Packets	1536
Throughput	13546.692
Error Rate	0.556
Delay	33.98
Packet Delivery Ratio	97.564

3.2 Model Formulation

The model was formulated for the various parameters that influence performance evaluation of the reliability of WSN. These include delay, throughput, packet delivery ratio, number of packets sent, packet loss and error rate.

3.2.1 Delay

Packet delay (also called latency) is the amount of time it takes for a packet of data to get from one designated point to another, depending on the speed of the transmission medium, such as copper wire, optical fiber, or radio waves, and the delay in transmission by devices along the way, such as routers and modems. A low latency indicates high network efficiency.

Delay is expressed as the ratio of delay due to suspected node to the delay due to neighbour nodes (Kumar & Singh, 2009). The total delay occurring in the network during communication process is mathematically denoted as:

$$\text{Delay (D)} = \sum \text{Sent Time} - \text{Received Time} \quad (1)$$

3.2.2 Throughput

Throughput is the total number of packets sent from a sender to a receiver in a given amount of time. It normally decreases with increase in number of nodes because the data these messages belong to may be delivered over a physical or logical link or it may pass through a certain network node. Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. Throughput is expressed as the rate of successful message delivery over a communication channel (Kumar & Singh, 2009). It can be analyzed mathematically by means of queuing theory as:

$$\text{Throughput} = N_{\text{pack}} * 8 \text{ bit} / t_{\text{frame}} \quad (2)$$

where

N_{pack} is the size of the data packet in byte

t_{frame} is delay between frames or time interval between consecutive frames.

3.2.3 Packet Delivery Ratio

Packet Delivery Ratio (PDR) indicates how efficiently data is transmitted across the network. It is the ratio of the total packets received successfully per unit time. It can otherwise be called delivery success ratio, expressed mathematically as:

$$\text{PDR} = \sum \text{Packets Received} / \text{Time} \quad (3)$$

Equation (3) shows that delivery ratio will increase by decreasing packet retransmissions. Inasmuch as delivery ratio strongly depends on the number of packet retransmitted, this parameter is considered in this paper as an alternative factor for performance analysis.

3.2.4 Number of Packets Sent

Number of packets sent is the number of times a task went into a send sleep state while waiting for the network to send each packet to the client. The network model determines that there can be only one outstanding packet per connection at any one point in time. This means that the task sleeps after each packet it sends.

3.2.5 Packet Loss

Packet loss is the failure of one or more transmitted packets to arrive at their destination. Packet loss refers to the packets of data that are dropped by the network to manage congestion (Kumar & Singh, 2009), expressed mathematically as:

$$\rho = \text{trafficIntensity} / \text{NumberOfChannels} \quad (4)$$

3.2.6 Error Rate

Error rate is the number of received bits of a data stream over a communication channel that has been altered due to congestion, noise, interference, distortion or bit synchronization errors. Packet error rate (PER) is the number of incorrectly received data packets divided by the total number of received packets. A packet is declared incorrect if at least one bit is erroneous. The expectation value of the PER is denoted packet error probability P_p , which for a data packet length of N bits is, mathematically expressed as:

$$P_p = 1 - (1 - p_e)^N \quad (5)$$

where,

p_e is the probability of receiving erroneous data packets

N is the number of received packets

4. FL-Based Model for Reliable Packets Transmission

A congestion control system should be preventive, if possible. Otherwise, it should react quickly and minimise the spread of congestion and its duration. Good design practice is to develop a framework for the system to avoid congestion. But taken to the extreme (i.e. to guarantee zero losses and zero queuing delay), this would not be economical. Thus, as a good compromise, this paper allows for some deterioration of performance that is never intolerable (congested). The challenge is to keep the intolerance at limits acceptable to the users. The QoS guarantee can be achieved by considering and defining the fuzziness present in causative parameters when congestion is actually experienced.

Figure 2 shows the architecture of the Fuzzy Logic-based model for Wireless Sensor Network - Expert System (WSN-ES) with the fuzzifier, inference mechanism, and defuzzifier as major components. The fuzzifier receives error rate, number of packets, delay, packet delivery ratio, and throughput as input parameters or linguistic variables while reliability is the output linguistic variable, all defined within a specified range. The linguistic terms are as follows; error rate: [very low, low, high, very high]; number of packets: [less, average, more]; delay: [short, normal, long]; delivery ratio: [low, moderate, high]; throughput: [low, normal, high]. The linguistic terms for reliability are [very low, low, moderate, high, very high]. The ranges are denoted by the linguistic terms defined uniquely for each linguistic variable as shown on table 3, and are used in building the membership function (MF) plots. The MATLAB triangular MF plots for the 5 input parameters and 1 output parameter are shown in figures 3 – 8. Figure 9 shows a snippet of the fuzzy rules for inference while figure 10 shows the rule viewer for a total of 324 generated rules. The inputs to the FL system are fuzzified and processed by the WSN-ES based on the fuzzy rules and inference mechanism obtained from the knowledge base. The data are then computed into crisp output which are defuzzified and used to determine the output (reliability) of the system.

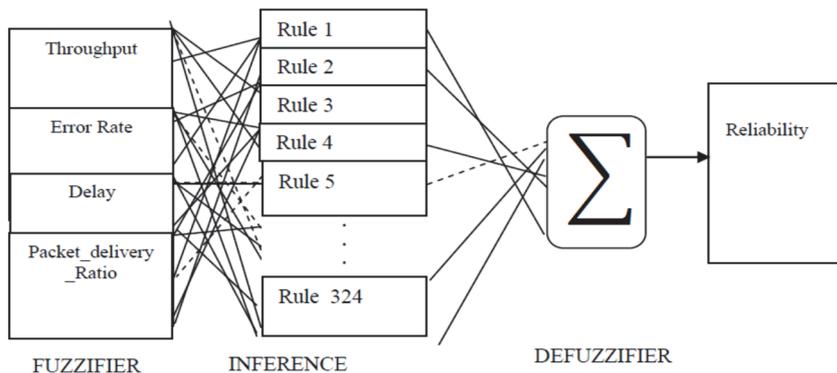


Figure 2. Fuzzy Logic Architecture for WSN-ES

Table 3. Linguistic variables, terms and their target range input

Linguistic variable	Linguistic term	Target range input
Error Rate	Very low, Low, High, Very high	<0.1; 0.1– 0.5; 0.5– 1.0, >1.0
Throughput (bps)	Very low, Low, High	<10000; 10000-20000; >20000
Delay (msec)	Short, Normal, Long	<25; 25 – 50; >50
Number of Packets (bits)	Less, Average, More	<1000, 1000-2000, >2000
Packet Delivery Ratio	Low, Moderate, High	<20, 20-80, >80

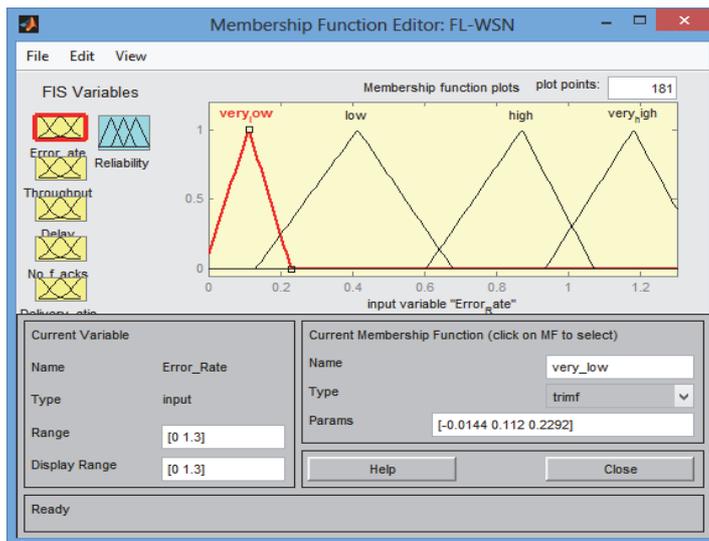


Figure 3. MF Plot for Error Rate

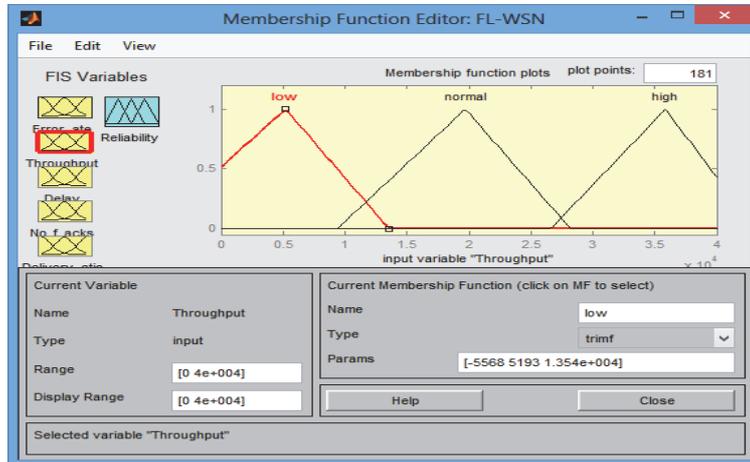


Figure 4. MF plot for throughput

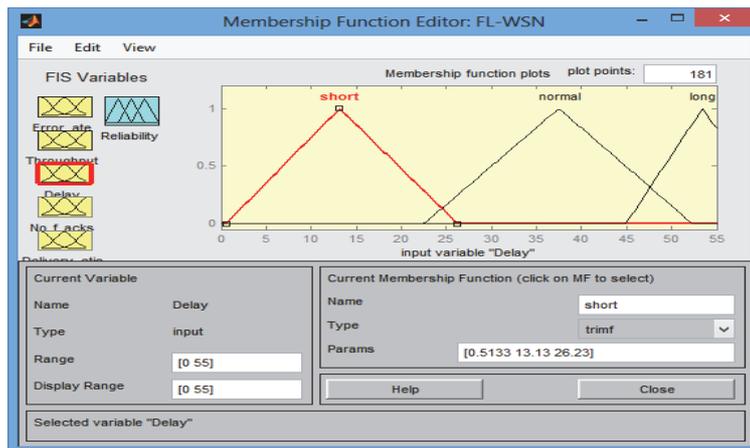


Figure 5. MF plot for delay

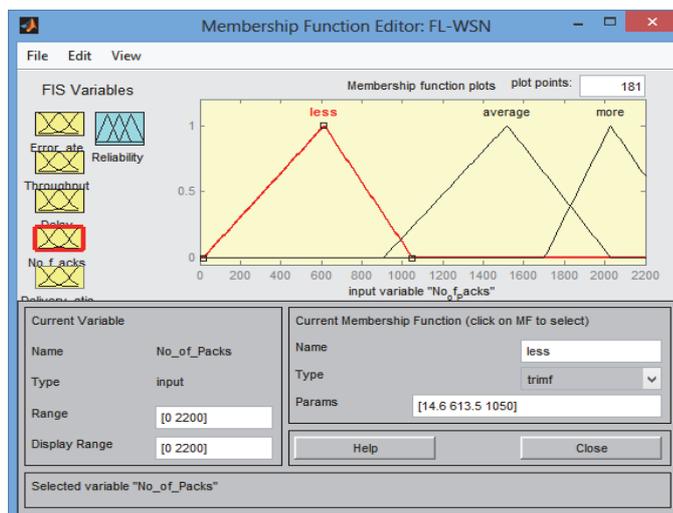


Figure 6. MF plot for number of packets

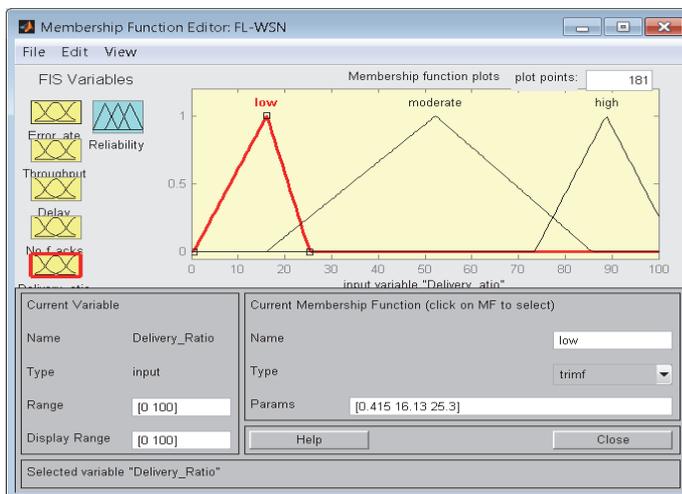


Figure 7. MF plot for delivery ratio

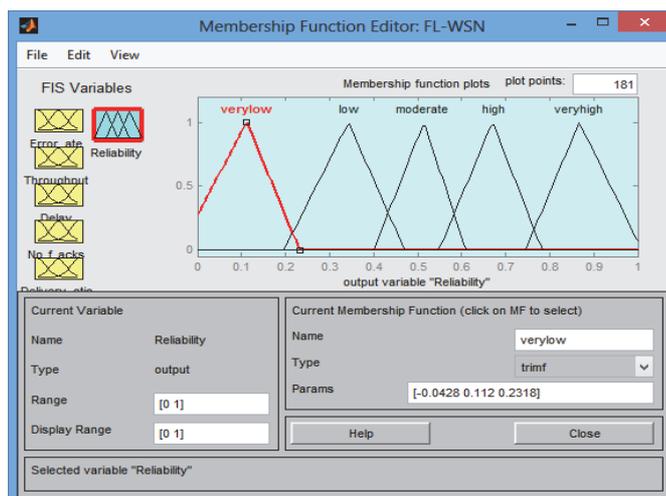


Figure 8. MF plot for output linguistic variable (reliability)

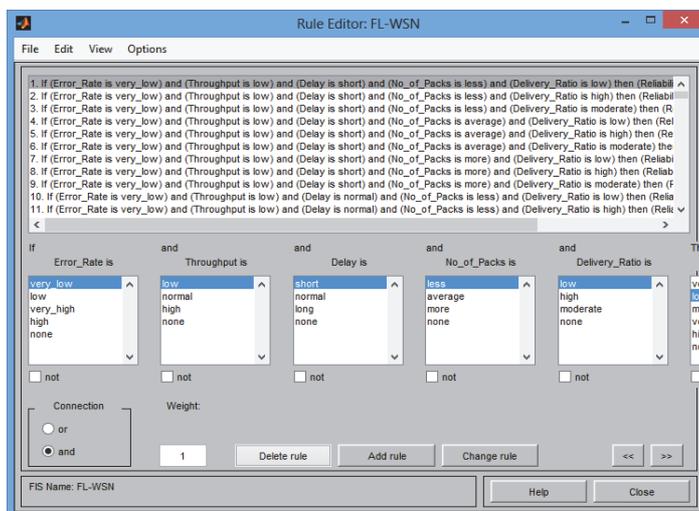


Figure 9. MATLAB rule editor showing generated FL rules

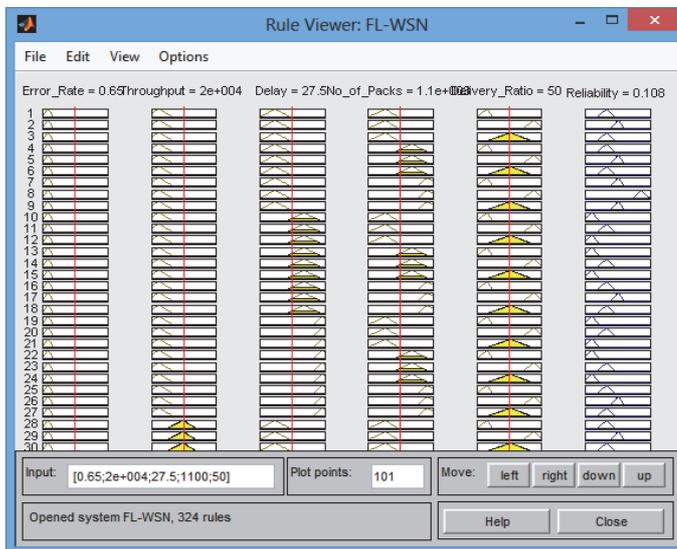


Figure 10. MATLAB rule viewer showing inference mechanism

4.1 Fuzzy Inference Engine

Basically, Mamdani fuzzy inference algorithm was adopted for mapping from a given input to an output using fuzzy inference engine. The mapping provides a basis which decisions can be made or patterns recognized. The inference process includes the following: *Block Building, Structuring, Firing, Implication and Aggregation of Rules*. The number of rules is determined by the complexity of the associated fuzzy system. Although, 324 rules were generated for the system, their firing strength has to be determined as most of them could not fire. Table 4 shows the rulesbuilding and structuring approach with keys to define the linguistic parameters used in generating these rules.

Table 4. Rules Structuring

Ert	TrPt	Dly	NoP	PdR	R
1	1	1	1	1	2
1	1	1	1	2	3
1	1	1	1	3	2
1	1	1	2	1	2
1	1	1	2	2	3
1	1	1	2	3	2
1	1	1	3	1	3
1	1	1	3	2	4
1	1	1	3	3	3
2	3	2	2	3	1
2	3	2	3	1	2
2	3	2	3	2	3
2	3	2	3	3	1
2	3	3	1	1	1
2	3	3	1	2	2
2	3	3	1	3	1

2	3	3	2	1	1
2	3	3	2	2	2
1	1	1	1	1	2
1	1	1	1	2	3
1	1	1	1	3	2
1	1	1	2	1	2
1	1	1	2	2	3
1	1	1	2	3	2
1	1	1	3	1	3
1	1	1	3	2	4
1	1	1	3	3	3
2	3	2	2	3	1
2	3	2	3	1	2
2	3	2	3	2	3
2	3	2	3	3	1
2	3	3	1	1	1
2	3	3	1	2	2
2	3	3	1	3	1
2	3	3	2	1	1
2	3	3	2	2	2

Key:

NoP = Number of Packets TrPt = Throughput Ert = Error Rate
 Dly = Delay PdR = Packet Delivery Ratio NoP {1-More, 2-Less}
 TrPt {1-High, 2-Low, 3-Verylow} Dly {1-Short, 2-Normal, 3-Long} PdR {1-Low, 2-High}
 Ert {1-Verylow, 2-Low, 3-High, 4-Veryhigh}

Analytically, there tend to exist a relationship between NoP and Ert over a given period of transmission time. Less NoP will result in reduced Ert and high TrPt. PdR has a major influence on Dly rate in WSN as high delivery ratio will guarantee less Dly. Simulation analysis is expected to verify these positions. Different implication operators correspond to different aggregation operators (e.g. union and intersection). Whereas the union operator uses the Mamdani and Larsen operators, the intersection uses the Lukasiewicz operator. This paper implements the Mamdani operator. After inference, the overall result yields a fuzzy value and is defuzzified to obtain a final crisp output. Though there are different algorithms for defuzzification namely Center of Gravity (CoG) or Centroid Average (CA), Maximum Center Average (MCA), Mean of Maximum (MoM), Smallest of Maximum (SoM) and Largest of Maximum (LoM), this work employed the CoG algorithm (Centroid). The Centroid technique is popular of the other techniques, because it finds the point where a vertical line would slice the aggregate set into two equal masses. Mathematically this centre of gravity (COG) can be expressed as:

$$CoG = \frac{\int_a^b \mu_A(x) x dx}{\int_a^b \mu_A(x) dx} \tag{6}$$

where μ_A is the set of MFs of the system.

5. Results and Discussion

Inputs to the FL-based model for the existing and optimized systems are shown on Table 5. Analytical data on the considered parameters were obtained from (Jebarani & Jayanthi, 2010) and used as inputs to the simulation. The

parameter values were the mid points of the MF ranges. Simulation experiments performed with the considered parameters - Error Rate, Throughput, Delay, Number of Packets and Packet Delivery Ratio from multiple runs have results discussed as presented in figures11 -19.

Table 5. Simulation inputs and crisp output

Data	Number of Packets (bits)	Throughput (bps)	Error Rate	Delay (ms)	OUTPUT (Reliability) (%)
Analytical System	750	1250	80	0.65	10.8
Optimized System	1700	32300	89.2	0.152	82.9

In figure 11, the optimum reliability of the system is a decreasing function of the error rate. As the error rate decreases, the packet error rate approaches zero, and the network reliability increases without bounds. Figure 12 shows the improvement of throughput with respect to reliability. If more packets are sent, usually the throughput will be less due to number of retransmissions required. However, with the optimized system it is observed that as the number of packets sent increases, the throughput also increases. With varied successful packet delivery rate as observed from the graph, the throughput increases with reliability, such that the higher the successful packet delivery rates, the higher the throughput. This shows that throughput can be jointly optimized with the reliability and packet delivery rate. Furthermore, figure 13 shows how reliability decreases due to delay. When more number of packets is sent, there will be more delay in packets deliver perhaps due to the network becoming heavily loaded. Also, figure 14 shows the decrease in reliability with respect to increase number of packets sent. In figure 4.4, it shows that the reliability is reduced as packets sent increases. If more number of packets sent there will be more number of packet losses due to errors. But with the optimized system, packet loss is reduced. If more number of packets transmitted without loss then the throughput, packet delivery ratio automatically increases which improves reliability of the system. Finally, figure 15 indicates that the reliability of a system is also dependent on the packet delivery ratio. It is observed that the packet delivery ratio of the system increases as reliability also increases. This is because reliability increases when high packet data delivery are obtained during data transmission as the transmission rate is directly proportional to the number of packets in the node.

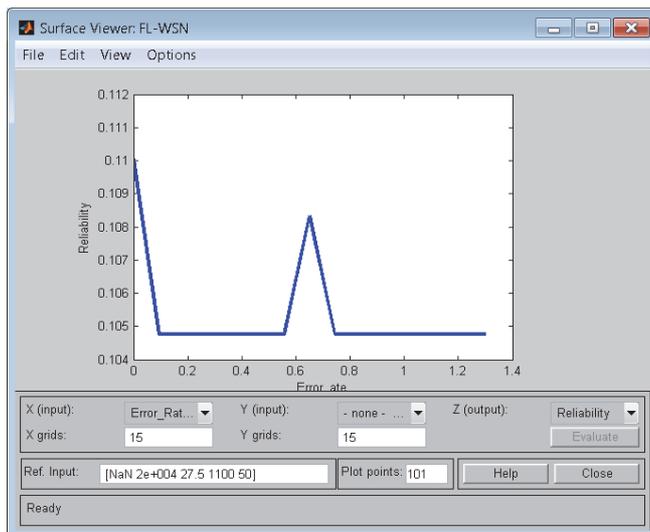


Figure 11. Optimized graph: reliability vs error rate

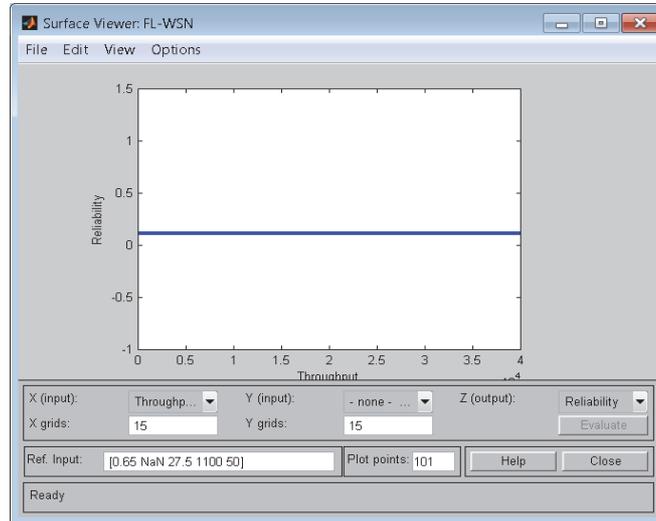


Figure 12. Optimized graph: reliability vs throughput

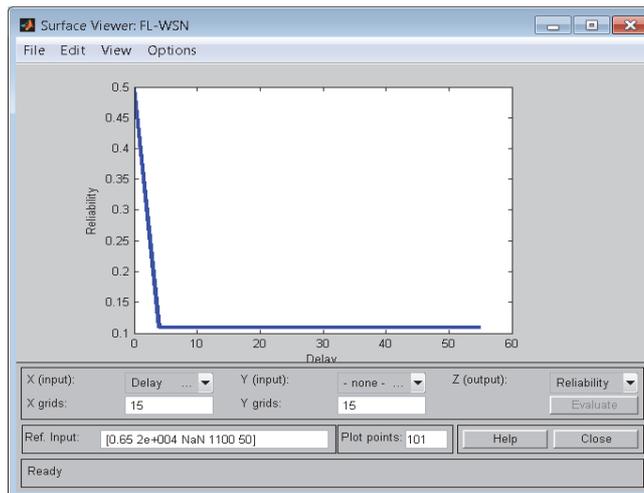


Figure 13. Optimized graph: reliability vs delay

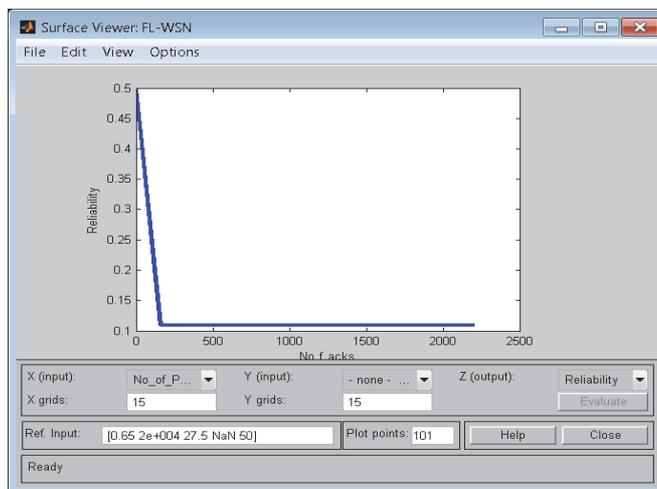


Figure 14. Optimized graph: reliability vs number of packets

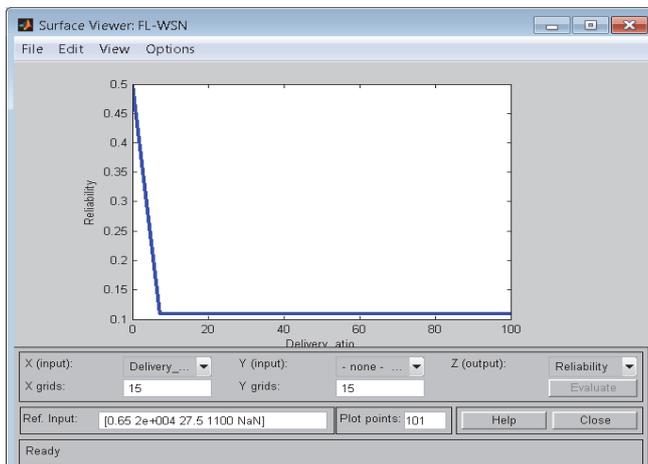


Figure 15. Optimized graph: reliability vs packet delivery ratio

Next, we investigate further the interactive effect of two related factors on network’s reliability. The graphs are three-dimensional (3D) plots and serve the purpose of our investigation. From our simulation, it is evident that for lower throughput values, the error rate increases. However, after a turning plane the throughput starts to drop extensively. This can be seen in figure16 where the data is interpolated using a cubic spline interpolation and surface plot is generated. The turning plane where throughput starts to drop is the maximum value of the throughput achieved in the network. The evident drop in throughput that does not fit the proposed model is the result of increased error rate due to the queuing of the data. When large quantities of data are streamed towards the node, the data start to drop after a turning plane located at error inflexion plane. But as number of packets arriving the network increases, delay and error rate is increased, i.e., the packet transmission rate decreases and the reliability of the system is negatively impacted upon and the system experience performance degradation as shown in figure 17. However, figure 18 shows that a decreased in number of packets implies less error rate and more channel availability and an improvement in the system’s reliability. But congestion is certainly imminent at peak periods if the number of channels becomes insufficient to transmit packets. This condition leads to frequent packets dropping and this depends on the thresholds imposed by the system’s settings. Hence network operators should implement robust congestion management protocols with fair constraints to efficiently manage network crises and still sustain optimally, the system’s performance. Figure 19 shows the effect of error rate and delivery ratio on the system’s reliability. The higher the error rate, the lower the delivery ratio. This indicates that packet transmission is dependent on the rate packets arrives at the network.

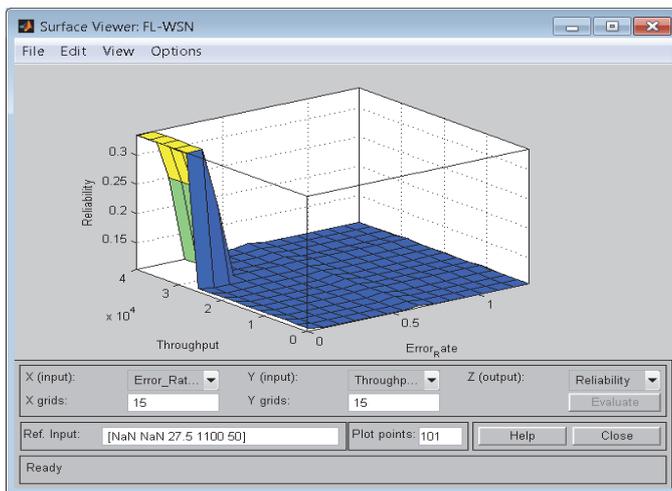


Figure 16. Optimized graph: error rate vs throughput `

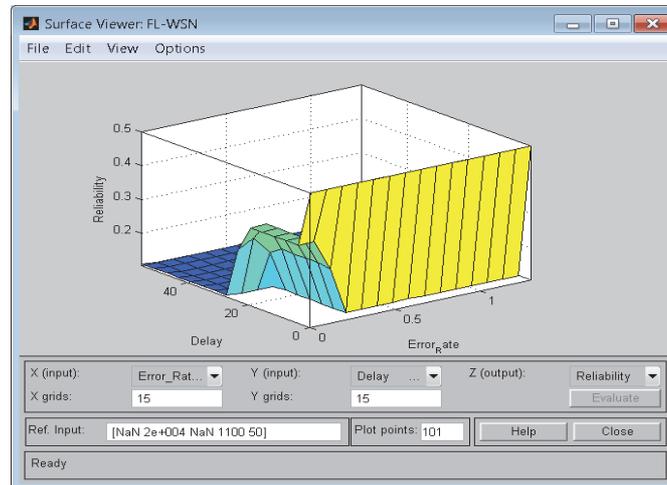


Figure 17. Optimized graph: delay vs error rate

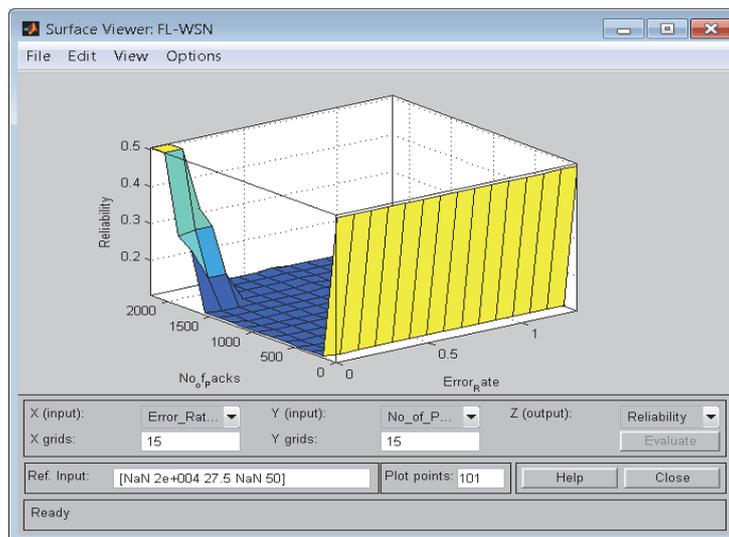


Figure 18. Optimized graph: number of packet vs error rate

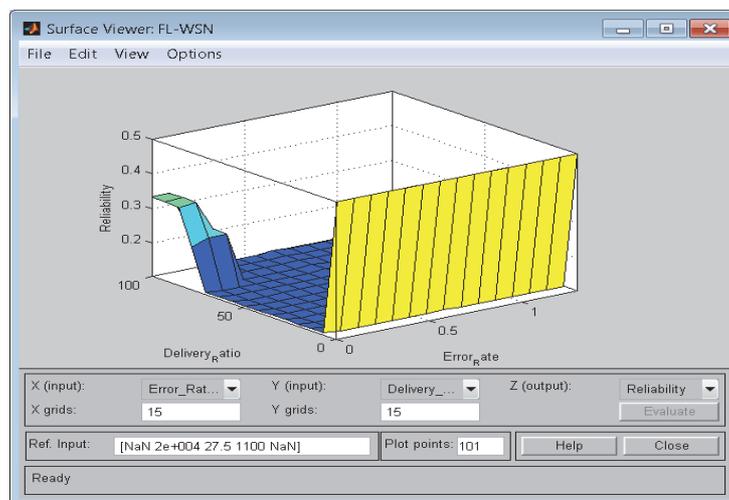


Figure 19. Optimized Graph: packet delivery ratio vs error rate

6. Conclusion

This paper hub on a realistic congestion detection control simulator that emulates and optimizes packets dropping in a WSN. The simulator allows for the determination of the system's reliability from factors that triggers congestion resulting in packets dropping. The fuzzy rule-based classifier was employed to optimize the system's performance by enhancing the service classification and QoS of the overall system. Again, the resource management technique used in the computation of weights for reliable optimization has improved the resource allocation admission of packets in the network.

Several factors that have direct consequence on congestion resulting in packets dropping have been investigated. These factors considered number of packets, throughput, packet delivery ratio, error rate and delay. To establish the threshold for the simulation, numerous data were obtained and used to simulate on the existing and optimized systems. The results showed that the proposed FL-based system outperformed the existing scheme and was more robust in terms of performance. The set of evaluation metrics form a multidimensional space that can be used to describe the capabilities of SNs. From the analysis, it is noted that many of the evaluation metrics are interrelated. Often, it may be necessary to decrease performance in one metric, such as error rate, in order to increase on additional delivery ratio or throughput. Our model sustained the congestion probability at a minimum threshold, thus guaranteeing the expected QoS provisioning in the presence of decreased delay and number of packets. These results can be useful in various WSN monitoring applications (i.e. Health, Military, Agriculture, Environment, Home, etc.). Nevertheless, investigation of the system's effectiveness using a Hybrid (Fuzzy-Neural) approach is a possible future direction to this research.

References

- Aggarwal, N., Gaur, D., Gupta, K., & Aggarwal, N. (2013). Congestion control for Internet using fuzzy logic: A review, *International Journal of Computer Networking, Wireless and Mobile Communications*, 3(1), 335-338.
- Akyildiz, I. F., Su W., Sankarasubramaniam Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Elsevier Journal of Computer Networks*, 38(4), 393-422.
- Chakravarthi, R., & Gomathy, C. (2011). Hop-by-hop rate control technique for congestion due to concurrent transmission in wireless sensor network, *World of Computer Science and Information TechnologyJournal* 1(8), 351-356.
- Chakravarthi, R., Gomathy, C., & Sebastian, S. K. (2010). A survey on congestion control in wireless sensor networks, *International Journal of Computer Science & Communication*, 1(1), 161-164.
- Chrysostomou, C., & Pitsillides, A. (2005). Using fuzzy logic control to address challenges in AQM congestion control in TCP/IP networks, *Workshop on Modeling & Control of Complex Systems (MCCS'05)*, (CD ROM Proceedings), Ayia Napa, Cyprus.
- Chrysostomou, C., Pitsillides, A., & Sekercioglu, Y. (2009). Fuzzy explicit marking: A unified congestion controller for best-effort and diff-serve networks, *Elsevier Journal on Computer Networks*, 650-667.
- Ekpenyong, M., Gibson, I., & Umoren, I. (2014). Call drop minimization using fuzzy associative memory, *Symposium Series on Computational Intelligence (IEEE - SSCI 2014)*, Flagship of International Conference sponsored by the IEEE Computational Intelligence Society (CIS), 16-23, in Orlando, Florida, USA.
- Jebarani, M. R. E., & Jayanthi, T. (2010). An analysis of various parameters in wireless sensor networks using adaptive FEC technique, *International Journal of Ad hoc, Sensor and Ubiquitous Computing*, 1(3), 33-43.
- Kim, B., Lee, H., & Cho, T. (2007). Fuzzy key dissemination limiting method for the dynamic clustering-based sensor networks, in proceedings of ICIC, 263-272.
- Kim, J., & Cho, T. (2007). Routing path generation for reliable transmission in sensor networks using GA with fuzzy logic based fitness function, in proceedings of ICCSA, 637-648.
- Kim, J., Park, S., Han, Y., & Chung, T. (2008). CHEF: Cluster head election mechanism using fuzzy logic in wireless sensor networks, in proceedings of ICACT, 654-659.
- Kumar, N., & Singh, K. (2009). An efficient approach for congestion detection in WSN through fuzzy logic, *Indian Institute of Information Technology*.
- Lazzerini, B., Marcelloni, F., Vecchio, M., Croce, S., & Monaldi, E. (2006). A fuzzy approach to data aggregation to reduce power consumption in wireless sensor networks, in proceedings of NAFIPS, 436-441.
- Lozoya, C., Rojas-Marta, F., Rodriguez-Esqueda, C., & Estrada-Ortega, J. (2016). Performance evaluation of image

- transmission over wireless sensor network for precision agriculture. *ASABE Annual International Meeting*, Orlando, Florida. July 17-20, 2016.
- Munir, S. A., Bin, Y. W., Biao, R., & Jian, M. (2007). Fuzzy logic-based congestion estimation for QoS in wireless sensor network, in proceedings of WCNC, 4336-4341.
- Pitsillides, A., Sekercioglu, A., & Ramamurthy, G. (1997). Effective control of traffic flow in ATM networks using fuzzy explicit rate marking (FERM), *IEEE Journal on Selected Areas in Communications*, 15(2), 209-225.
- Sharma, B., & Aseri, T. C. (2012). A comparative analysis of reliable and congestion-aware transport layer protocols for wireless sensor networks, ISRN sensor networks, 1-14. <https://doi.org/10.5402/2012/104057>
- Sohraby, K., Minoli, D., & Znati, T. (2007). *Wireless sensor networks technology, protocols, and applications*. New Jersey, NJ: John Wiley and Sons.
- Wang, C., Sohraby, K., Hu, Y., Li, B., & Tang, W. (2005). Issues of transport control protocols for wireless sensor networks, in *Proceedings of the International Conference on Communications, Circuits and Systems (ICCCAS '05)*, 422-426.
- Wang, C., Sohraby, K., Lawrence, V., Bo, L., & Yueming, H. (2006). Priority-based congestion control in wireless sensor networks, in *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, 22-31.
- Wang, C., Sohraby, K., Li, B., Daneshmand, M., & Hu, Y. (2006). A survey of transport protocols for wireless sensor networks, *IEEE Network*, 20(3), 34-40.
- Xia, F., Zhao, W., Sun, Y., & Tian, Y.-C. (2007). Fuzzy logic control based QoS management in wireless sensor/actuator networks, 3179-3191.

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).