IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661, ISBN: 2278-8727 Volume 5, Issue 3 (Sep-Oct. 2012), PP 21-34
www.iosrjournals.org

A Survey of Fuzzy Logic Based Congestion Estimation Techniques in Wireless Sensor Networks

[1]A. K. Singh, [2]Rahul Dekar
[1,2]Indian Institute of Information Technology, Allahabad, India

Abstract: *Congestion estimation has always been atopic of crucial importance for Wireless sensor network (WSNs). Recent developments in sensor network research have led to various new fuzzy systems, specifically designed for WSNs where congestion awareness is an essential issue.Recently someresearchers have proposed fuzzy logic based techniques for congestion estimation in order to diminish the congestion.There are several fuzzyand non-fuzzybased techniques proposed by researchers for congestion estimation and control. This paper surveys fuzzy logic based techniques of congestion estimation and also describes that how fuzzy logic based techniques are efficient than that of non-fuzzy techniques for estimating the congestion in WSNs.*
Keywords: *Wireless Sensor Network; Congestion Estimation; Fuzzy Logic; Cluster Head (CH).*

I. Introduction

Sincelastdecade the Wireless Sensor Networks Technology or WSN playssignificant role in the recent used technologies for communication. The WSN technologyconsists three basic technologies:
1. Micro-Electromechanical Systems Technology (MEMS) which helps to fit mechanical parts in a tiny chip,
2.Wireless Radio Frequency Communication, which helps the sensor nodes to initiate the communicationamong them with the help of Radio Frequency (RF) waves and, 3. Digital Electronics Technology, which makes the tiny chip of a sensor node more powerful to deal with different types of senseddata to perform the operations e.g. data fusion, data compression etc.[1][2].

In general WSNs is a collection of number of sensor nodes deployed and from some sensor nodes to hundreds or even thousands numbers of nodes, where every sensor node is associated by radio link to one or sometimes various other sensor nodes and they are independently operated. These sensors are tiny in size. A particularsensor node is comprises of sensing chip, microcontroller, power (battery), an antenna and radio transceiver in a single tiny chip in a WSN. The givenfigure 1 shows hardware components of a sensor node.

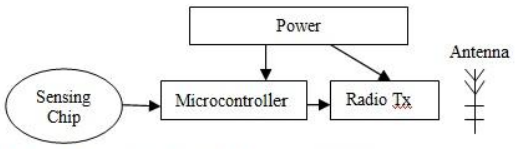


Figure 1. Sensor node's hardware components

The sensor nodes have restricted power because they are battery functioned, low memory and restricted computational power and also narrow communication range to the rest of sensor nodes and the BS(base station) too. The sensor nodes operated on RF in order to exchange the sensed data among themselves.

The sensor nodes have restricted battery life. So once the sensor nodes are spreads it is very unmanageable to exchange the batteries of sensor nodessince they are spreads in tens to hundreds or in thousands of number. Thereforeit can easilysay that sensor nodesinWSNs have very restricted lifetime.

Earlier most ofresearchers had worked on this fieldand give different techniques and protocolsto enhance the lifespanof sensor nodes inWSNsand they come uponthatthey should have to develop a better network topology in which the sensor nodes uses less power during data transmission. Sensor nodes consume more of theenergyif they are regularly awake for a long timeperiod. So the researchers suggested Sleep/Wake mechanismfor betterimprovement of this kind of energy consumption.

In order to keep the power of sensor nodes some researchersproposeddifferent methods and parameter selection for clustering. Sensor network in generally a collection of homogeneous nodes and different parameters like residual energy, centrality of node, density etc.can be considered for clustering in sensor network. Different methods like LEACH, HEED and fuzzy based clustering etc. are used to select some nodes among the various others as a Cluster-Head which gather and aggregate received sensed data from each node present in its sensing range and sends this aggregated data to theappropriate BS. In clustering mechanism only some nodes senddata to the BS, not each individual.Because of that clustering mechanism is very useful to preserve the power of sensor nodes and hence enhance the life period of wireless sensor network to a largespan.

There are several most important application areas of WSNs as, security and military sensing, health monitoring, home automation and monitoring, assets tracking and supply chain management, industrial control and monitoring etc.

Data Transmission in theWSNs:

` The sensor nodes are obligated to deployas per the application in any region as, security, home automation, and military sensing etc.and if the nodes sense any information and then to transfers the sensed information to the BS, there are two type of mechanisms which sensor nodes used. In first type,the entire sensor nodes individuallytransfer'stheir sensed data to the BS which they gather from that environment as shown in figure 2. On the basis of previous research on this field it has been demonstrated thatwhenever such type of mechanism is applied; it will causeeach sensor node to takemore energy as compared to required normally and the life of wireless sensor network is gettingdiminishesat time because each node has limited power.

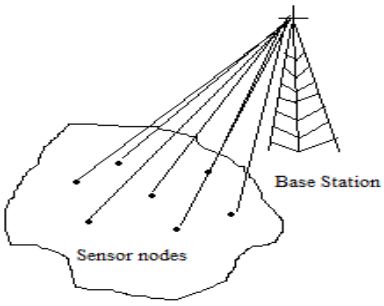


Figure2. Data transmission without clustering

So to enhance the life of wireless sensor networksresearchers suggested"Clustering", which is the second mechanism. In clustering the wireless sensor network is zoned into various clusters (a cluster is consist of tens to hundreds or in thousands of sensor nodes in WSNs which present among each other's proximity) as shown inFigure 3,each cluster has a CH (clusterhead).TheCHs gather sensed information from each node present in the cluster, aggregate the sensed data and then perform compression on the aggregated data which then transmitted to the BS[3][4].

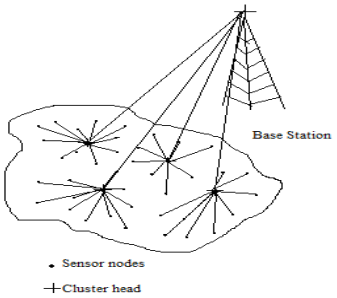


Figure3. Data transmission when clustering mechanism is used

Fuzzy Applications in WSNs:

Fuzzy logic is relatively abettertool for taking decisionsand to address uncertainties. Fuzzy logic has defined the intermediate values of input and output between high andlow conditions. There are mainly three applicationfields of Fuzzy logic in WSNs; (1) Clustering (2) Data fusion and (3) Security.

We have discussed clustering earlier in this paper. After clustering there is anothervital operation called data fusion or data aggregation. Data fusion is veryhelpful to improve the functioning of wireless sensor network. As we know that, in clustering all the sensor nodes transfers the sensed data to theirCH then the gathered sensed data is fused or aggregated at the CH[5][6]. So the CHis also creditworthy for data fusion.

The data fusion application is extremely essential and important because several nodes transmit their data to CHwhich processes the gathered data and fuses it to become more informative than the original input data[7].

There is necessity of securitytoo in WSN [8].Since sensor nodes are randomly spreads in any region and they communicate with oneanother through RF(radio frequencies) and the nodes sense data from their atmosphere and transmit it to their appropriate CH, which in turn responsible for data fusion and finally for transmission to the BS. At present the wireless sensor network is very demanding technology to gainworthy information. So it increasesthe need of security to the protection of transmitted data packets from source to sink.

The sensor nodes are self-coordinated and battery operated also they have limited energy, low bandwidth and too have very small size of memory. So at this stage Public key cryptography is very expensive to be handling by the sensor nodes to secure their transmitted sensitive information. Because of this avery fast Symmetric-key cryptography scheme is used.

The railway security and indoor child tracking[9] applications of WSNs based on fuzzy logic are the crucial examples of security in wireless sensor networks.

Congestion:

The general meaning of congestion is excessive load in the network. The congestion problem in wireless sensor network occurs when any node carrying so much data packets than their processing speed because of it quality of service deteriorates. Owing to congestion queuing delay, blocking and packet loss takes place in the network which pretends the energy consumption of nodes too. As congestion is takes place at the receiving sensor node which has slow processing power as compared to its receiving power. To hold the packets for very long time periodthe sensor nodes are alive continuously which is the cause of veryhigh energy consumption, packet lossand blocking of network. It also enhances the possibility of network failure [10].

In recent technologies,the congestion avoidance and congestion control techniques are acquiredto diminish the effect of congestion. Another technique to diminish the effect of congestion is priority based scheme called Priority Congestion Control Protocol (PCCP).

In PCCP protocol a sensor node just sense the data from their surroundings according to their application and give some priority to those data packets. And the data packets which have the higherpriority are transmitted first to the lower priority data packets.

In the wireless sensor networks, there could be two reason of congestion. The first is at node-level which is induced by the overflow of the buffer in the nodes and its consequence is increased packet loss and queuing delay. Due to packet loss it increases the retransmission attempts with consumption of additional energy.

The second is at link-levelcongestion control. Since in the wireless sensor networks, wireless channels are shared by various sensor nodes which are employing CSMA protocol (Carrier Sense Multiple Access Protocol) for getting access to the wireless medium.So the collisions of data packets occur only when several active sensor nodes are attempting to accesswireless channels at the same time.This kind of congestion results in increase of packet service time and decreases the utilization of both links and overall throughput and ultimately wastes the energy of sensor nodes.

Therefore both types of congestion (link-level and node-level) involves in energy consumption of nodes. Moreover the congestion results in decreased lifetime of WSN.

Congestion estimation and detection:

In paper [11][12] researchers proposed that inWSN there is extreme probability of congestion occurrence because the sensor nodes utilize the wireless channels to transmit theirsensed data packets. If several sensor nodes transmittheir data packets simultaneously then the probability of congestion to be occurringis increased.

If there is single sink node (base station) and several source nodes transmitting data packets at some rate to sink and the sink isunable to process all data packets (because the processing rate of sink is lesser then its receiving rate) then it will cause packet loss at the sink since the sink is congested.

An energy efficient scheme called Congestion Detection and Avoidance (CODA) is available for detection of congestion and avoidance. The CODA scheme has three mechanisms.

(i) Congestion Detection: To detect the congestion,itentails to find that where the congestion isoccurring in the sensor network? It also needs to monitoron the current andearlier wireless channels traffic conditions in the present sensor node. When congestion is detected, sensor nodes transmit a signal to its upstream sensor nodes via a backpressure mechanism.

(ii) One-hop backpressure: When congestion is detected by sensor nodesit transmits backpressure signal to one-hop upstream. If the one-hop upstream node receives backpressure signal it decreases its transmitting data packet rate. However if any upstream sensor node receives a backpressure message it checks its network condition, if it gets the network congested, it will further transmit the backpressure signal to its one-hop upstream node.

(iii) Closed-loop multisource regulation: If there aremanysources and only one sink then the close-loop rate regulation can be employed for congestion control. In this mechanism each source node compares its data packet rate to the maximum throughput of channel. If the data packet rate is lesser than the throughput it normally regulates its rate. If the rate is greater than the throughput there could be the outcome of network

congestion. Under these conditions, the closed-loop congestion control mechanism is used. The source node enters the sink regulations and it uses feedback from the sink node to manage its data packet rate.

Parameters for Congestion Estimation:

In wireless sensor networks, to estimate the congestion there are two most crucial parameters used, the net packet arrival rate (P_{net}) and the buffer occupancy (S).

The net packet arrival rate (P_{net}) is determined by equation (1).

$$P_{net} = P_{in}/P_{out} \text{ - } (1)$$

Here P_{in} is the incoming packet rate and P_{out} is the outgoing packet rate.

II. Fuzzy Logic Based Techniques For Congestion Estimation

A.Fuzzy Logic based Congestion Estimation for QoS in WSNs:

Within a proposed QoS architecture, researchers presented a sophisticated model of congestion estimation, based on fuzzy logic, using selected parameters as fuzzy variables. ForbetterQoSin WSN, researchers employed fuzzy logic approach.Fuzzy logic is proven to be abetter tool for buffer management in the wireless sensor networks[13].

So to describe the methodology for fuzzy logic approach in order to estimating and mitigating the congestion in WSNs, researchers use two most effective parameters asfuzzy variables. These are, "net packet arrival rate (P_{net})" and "the current buffer occupancy(S)". The grade values are assigned for fuzzy variables namely packet arrival rate (p) and buffer capacity (s). So the fuzzy set"A" is:

$$A = \{p, s\}$$

Here p is fuzzy variable for P_{net}(net packet arrival rate) and s is fuzzy variable for S (buffer occupancy) shows the buffer fullness at a particular time.

The grade rates for the fuzzy set variables are 1, 0.5 and 0 for high congestion, medium congestion and no congestion. These grade rates of fuzzy variables are takes between 1 & 0 and these grade rates are not absolute. For simplicity researchers take three grade values. So after assigning the values, the packet arrival rate (p) is:

$$p = \begin{cases} 0, & \text{for } P_{net} < 0.5 \\ 0.5, & \text{for } 0.5 \le P_{net} < 1 \\ 1, & \text{for } P_{net} \ge 1 \end{cases} \text{ - - - - - - - - - - - - - - - - - - } (2)$$

Similarly, the buffer size fuzzy variables s:

$$s = \begin{cases} 0, & \text{for } s = 0 \\ 0.5, & \text{for } s \le 0.6 \\ 1, & \text{for } 0.6 < s \le 1 \end{cases} \text{ - } (3)$$

Equation (2) and (3) describes the packet arrival rate and buffer size. The researchers describe earlier that the rates of fuzzy variables are not fixed & they may change according the applications & user requirement. So the fuzzy table 1 shown in below is created by the outermax product of fuzzy set values. Then the membership function for two relation P(U, V) & Q(V,W) is describes by equation (4):

$$\mu_{P*Q}(x, z) = \{(x, z), \max \lfloor \mu_P(x, y), \mu_Q(y, z) \rfloor \} \text{ - - - - - - - - - - - - - - } (4)$$

Then the fuzzy table is:

p \ s	0	0.5	1
0	0	0.5	1
0.5	0.5	0.5	1
1	1	1	1

Table1 Fuzzy Logic Table for buffer size and incoming/outgoing packet ratio

With the help of above fuzzy table researchers are able to estimating the congestion and then them also able to mitigating the congestion in wireless sensor networks.

B. Fuzzy Rate Control method in WSNs for Decreasing the Congestion:

In paper [14], researchers proposed in WSNs the main problem is "congestion". To mitigating the congestion problem researchers proposed a newly method. In this method, researchers continuously monitor the buffer (queue) length of the sensor nodes. Then based on fuzzy logic inferences, the admissible for upstream sensor nodes is calculated based upon the nodes constraints. So this technique is very simple & adaptable.

In WSNs, hop by hop flow control is very attractive since it is capable to diminish the congestion without the necessity of end to end ACKs. It can be very easily to implement and do not need of heavy process too. Table 2 demonstrates the rule base table for this approach.

f_{out} / e_q	Very Low (VL)	Low (L)	Medium (M)	High (H)	Very High (VH)
NL	VL	VL	L	M	H
NM	L	L	L	L	H
ZO	H	H	H	H	VH
PM	VH	H	H	H	VH
PH	VH	H	H	H	VH

Table 2 Fuzzy Rule Base table for Fuzzy Rate Control Technique

Protocol Design:

When researchers design a useful protocol, there are most of the things that should be considered. Firstly, the designer must explain that what types of listening mechanism is used. Since some schedule based MAC protocol (like FDMA and TDMA) waste the resource of network and also not satisfy some features of the WSNs, so they are not apply for this purpose. The second thing is Back-off mechanism selection because the synchronization among periodic stream of traffic in WSNs should be avoided by the back-off period. Third is the flow rate control since it is the best method to diminish the congestion in WSNs. Modeling & rate control, Rate propagation & Rate Control Algorithm Correction is also used for protocol design.

Fuzzy rate control with bandwidth control:

This algorithm is implemented toeach one sensornode of WSNs because of its simplicity and distributiveness. There are two phases of this algorithm; first is sending part which activated when a data packet is sent out to the next hop node. And, second part is activated after every data packet reception, consider a context that node iget a data packet from node j. First of all node j update its downstream monitoring window.

Firstly the downstream monitoring window of node j is updated by itself (node j). And by the reference of this information from next hop node the flow rate of outgoing is updated. The next data packet is send by the node j after a time period is determined by the outgoing flow rate.The upstream monitoring window will be updated and new incoming flow rate is used to inform to upstream sensor nodes and upstream sensor nodes will correct their flow rates of outgoing, when the next hop sensor node gets a data packet.

C. Trust estimation based on Fuzzy logic for congestion control in WSNs:

In paper [15],researchers proposed a congestion control techniqueand it is based on fuzzy logic. In WSNs, there are several malicious sensor nodes which are undeniable. These sensor nodes cause to increase the congestion by diffusing the useless packets. In this approach, each one of sensor node regularly monitors the behavior of its neighboring sensor nodes for estimating their related trust. Thisapproach can capable todetect and remove the malicious sensor nodes to reduce the congestion.

Proposed Trust Estimation based on Fuzzy Logic:

For efficient and safe communication between sensor nodes in WSNs, the sensor nodes should know the measurable belief of trust. For the trust estimation,there are some mechanisms are proposed by researchers.

Analyzes the misbehavior of Sensor Nodes:

To analyzing the behavior of sensor nodes intheWSNs, researchers classified the malfunctioning of sensor nodes in three particular ways:

Number:

The suspected sensor nodes may not re-forward or forward the packets several times without consideration of tracing parameters of network or suitable timeout. The *Number* (N_p)is computed by the neighbor sensor nodes of suspected node by equation (5).

$$N_p = N_f/N_{ef} \text{ - (5)}$$

Where number of packets that suspected sensor node forward after receiving it is denoted by N_f and number of packets that the sensor nodes expects by its suspected neighbor node forwards after receiving it is denoted by N_{ef}.

Delay:

The malicious sensor nodes forward the packets with high delay. The *Delay* (D_p) for every suspected neighbor nodes is computed by equation (6).

$$D_p = T_r/T_a \text{ - (6)}$$

Where T_r is delay that suspected sensor node forwards packet after receiving it and T_a is defined as delay that a sensor node expects its suspected neighbor sensor node forwards packet after receiving it.

Validity:

The suspected sensor nodes sometimes may forward some packets which are practically not valid. The neighbors of suspected sensor nodes can calculate the *Validity* (V_p) by equation (7).

$$V_p = N_v/N_{vf} \text{ - (7)}$$

Where N_v shows the number of valid packets which are forwarded by suspected sensor nodes andN_{vf}shows total number of packets which areforwarded by suspected sensor node.

Trust verification of proposed scheme:

Each sensor node estimates the related trust to its neighbor nodes with the help of FIS (Fuzzy Inference System) based on following steps:-

Fuzzification Interface:

It performs the scale mapping that transfer the range of value ofinputsintotherepresentinguniverseof discourse. Following figure 4 shows the generalized fuzzy inference system.

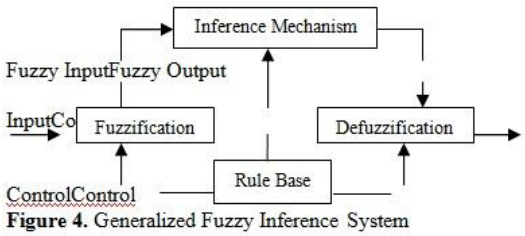


Figure 4. Generalized Fuzzy Inference System

The following equation (8) performs scale mapping and changes universes discourse for N_p the figure 5(a) shows the related MF(membership function). Then the number of forwarded packet (N_{Fp}) which is acceptable is

$-1/N_pN_f<N_{ef}$

$$N_{Fp}=1-N_pN_f = \begin{cases} N_{ef} \text{ ------- - - - - - - - - - - - (8)} \\ N_pN_f>N_{ef} \end{cases}$$

And the equation (9) performs the scale mapping for $D_p$andfigure 5(b) shows the related membership function. If the linguistic value is M then the delay is acceptable. VH shows very highest delay and VL shows the very lowest delay, then VL and VH are not acceptable.

$$D_{Fp} = 1 - D_p T_r = T_a \begin{cases} -1/D_p T_r < T_a \\ \text{----------} \\ D_p T_r > T_a \end{cases} \quad (9)$$

And$V_{Fp}$is the scale mapping form of V_p which have no change in universes discourse. The figure 5(c) shows the membership function of V_{Fp}. If linguistic value is VH then the majority of forwarded packets are useful. Figure5(d) shows the membership function of buffer capacity.

Inference Mechanism based on rules:

Figure5(e) shows the membership functions of trust. The fuzzy trust values are produced by the "inference mechanism" which will be apply on predetermined set of linguistic rules. The VH depicts trust is very high, M depicts trust is medium and VL depicts trust is very low. The table 3 demonstrates the "Rule Bases" using in inference mechanism where N_{Fp}andD_{Fp} are similar.

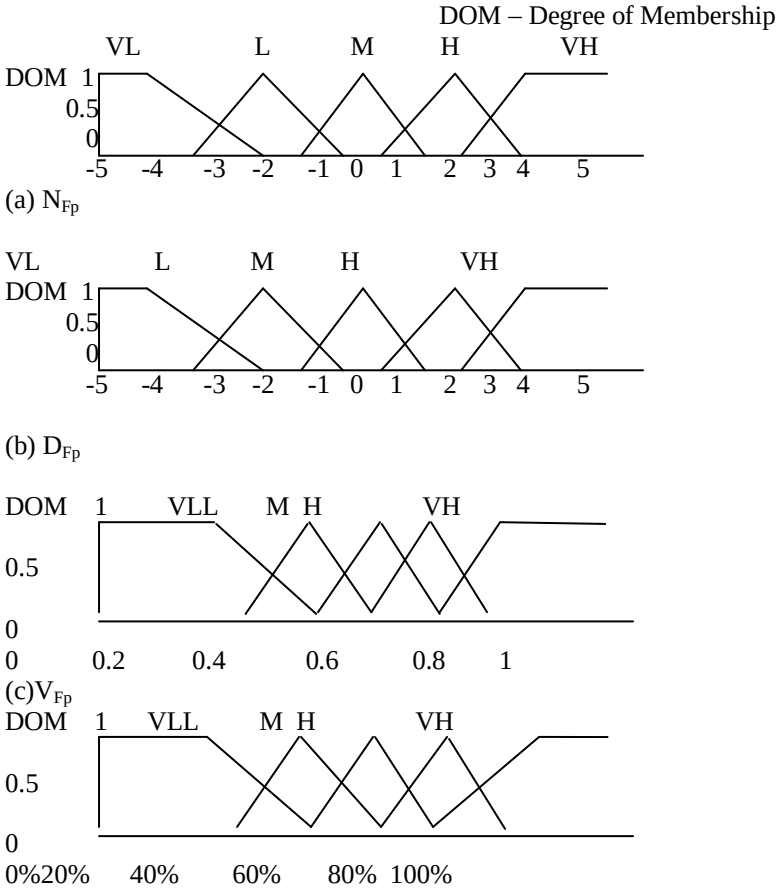


Figure 5 Input output fuzzy membership functions

Defuzzification:

It performs the scale mapping, which translates the fuzzyfied trust values into non-fuzzy form for taking decision. The range of non-fuzzy values is {0,1,2,3,……,10}. Here 10 are interpreted as a legitimate

sensor node and 0 is interpreted as malicious sensor node.Here table 3 demonstrates the Fuzzy rule base of inferring neighbour nodes for detecting Delay or Number or Validity misbehaviour.

First Input	Second Input	Output (Trust)	
N_{Fp}or D_{Fp}or V_{Fp}	B_f	If first input	
		N_{Fp}or D_{Fp}	V_{Fp}
VL (Very Low)	VL (Very Low)	VL (Very Low)	VL (Very Low)
VL (Very Low)	L (Low)	VL (Very Low)	VL (Very Low)
VL (Very Low)	M (Medium)	L (Low)	L (Low)
VL (Very Low)	H (High)	L (Low)	L (Low)
VL (Very Low)	VH (Very High)	M (Medium)	M(Medium)
VL (Very Low)	VL (Very Low)	VL (Very Low)	VL (Very Low)
L (Low)	L (Low)	L (Low)	L (Low)
L (Low)	M (Medium)	L (Low)	L (Low)
L (Low)	H (High)	M (Medium)	M (Medium)
L (Low)	VH (Very High)	H (High)	M (Medium)
L (Low)	VL (Very Low)	M (Medium)	L (Low)
M (Medium)	L (Low)	H (High)	L (Low)
M (Medium)	M (Medium)	VH (Very High)	M (Medium)
M (Medium)	H (High)	VH (Very High)	M (Medium)
M (Medium)	VH (Very High)	VL (Very Low)	H (High)
H (High)	VL (Very Low)	L (Low)	L (Low)
H (High)	L (Low)	L (Low)	L (Low)
H (High)	M (Medium)	M (Medium)	M (Medium)
H (High)	H (High)	H (High)	H (High)
VH (Very High)	VH (Very High)	VL (Very Low)	M (Medium)
VH (Very High)	VL (Very Low)	VL (Very Low)	H (High)
VH (Very High)	L (Low)	L (Low)	VH (Very High)
VH (Very High)	M (Medium)	L (Low)	VH (Very High)
VH (Very High)	H (High)	M (Medium)	
	VH (Very High)		

Table 3. Fuzzy rule base of inferring neighbour nodes for detecting Delay or Number or Validity misbehaviour

D. A Fuzzy-Based Energy Efficient Packet Loss Preventive Routing Protocol:

As we know sensor nodes have limited power, small memory, low bandwidth and limited energy. In paper[16] the authors presented a protocol called FEEPRP (Fuzzy-based Energy Efficient Packet Loss Preventive Routing Protocol) which adopts the routing algorithm that provides the security for avoiding the malicious nodes and keep the loss of data and constraint the excess energy utilization. Thereis no idea like digital signature and MAC behind FEEPRP. It is able to provide secure route from source to destination which is energy-efficient.

FEEPRP Algorithm:

The FEEPRP provides an appropriate efficient route and the decision is on certain parameters. The initial value of parameters is taken from the nodes themselves. The algorithm consist of two parts, first is "route discovery" which helps to discover all possible routes.The second part is, "selection of route" which helps to selectthe appropriate optimal route among all potential routes from source to destination (BS).

The membership graph where x-axis denotes the residual energy and y-axis denotes the degree of membership, the vertical projection of residual energy mapped the fuzzy variables in particular range from low to high and average which show the value of degree of membership of those fuzzy variables.
Similarly authorsalso make the membership graph for hop count and packet dropped.And last step is defuzzification, where it performs the scale mapping, which translates the fuzzyfied trust values into non-fuzzy form. The following table 4 demonstrates the rule base table for fuzzy controller.

Residual Energy	Packet Dropped	Hop Count	Inference (R)
H(High)	H(High)	H(High)	VL(Very Low)
H(High)	H(High)	A (Average)	L(Low)
H(High)	H(High)	L(Low)	VL(Very Low)
H(High)	A(Average)	H(High)	VL(Very Low)
H(High)	L(Low)	H(High)	L(Low)
A(Average)	H(High)	H(High)	VL(Very Low)
L(Low)	H(High)	L(Low)	VL(Very Low)
A(Average)	A(Average)	H(High)	M(Medium)
A(Average)	A(Average)	L(Low)	H(High)
H(High)	A(Average)	A(Average)	L(Low)
L(Low)	A(Average)	A(Average)	H(High)
A(Average)	H(High)	A(Average)	VL(Very Low)
A(Average)	L(Low)	A(Average)	H(High)
L(Low)	L(Low)	H(High)	M(Medium)
L(Low)	L(Low)	A(Average)	VH(Very High)
L(Low)	L(Low)	L(Low)	VH(Very High)
H(High)	L(Low)	L(Low)	VH(Very High)
A(Average)	L(Low)	L(Low)	H(High)
L(Low)	H(High)	L(Low)	L(Low)
L(Low)	A(Average)	L(Low)	VH(Very High)
H(High)	L(Low)	A(Average)	L(Low)
H(High)	A(Average)	L(Low)	L(Low)
A(Average)	L(Low)	H(High)	M(Medium)
A(Average)	H(High)	L(Low)	VL(Very Low)
L(Low)	H(High)	A(Average)	VL(Very Low)
L(Low)	A(Average)	H(High)	M (Medium)

Table 4. Rule base for Fuzzy controller

E. Fairness Congestion Control for distrustful WSNs using Fuzzy logic:

Wireless sensor networks aredeployed very dense, there are problems like congestion and packet loss happens due to distrusted packet. For such networks the researchers havesuggested FCCTF(Fairness Congestion Control for distrustful WSNs using Fuzzy logic). If there are malicious nodes in the sensornetwork then FCCTF is capable to detect and remove those malicious nodesfrom the sensor network to increase the packet delivery. But there exists a possibility of packet dropping due to overflow.
FCCTF is improved version of previous method "Trust estimation based on Fuzzy logic for congestion control in WSNs (FCC)"[17].

Fairness Congestion Control using Fuzzy Logic:

If there are some nodes which don't drop non-forwarded packets or have malfunctioned that re-transmit the duplicate packets, detectedthen those nodes are marked as malicious. Here researchers include a special term dynamic "Threshold Trust Value (TTV)" to handlecongestion and packet loss problem, which provides better measurement of fairness.

FCCTF have different operations when increasing or diminishing the number of lost packets.

Inputs for FIS (Fuzzy Inference System):

There are two kinds of inputs in FIS. The following figure 6 defines the fuzzy inference system.

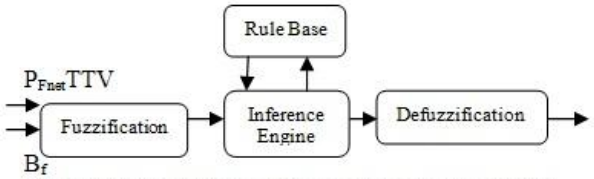


Figure 6. Fuzzy Inference System for calculating TTV

First Input:

The ratio of incomingdata packetsand outgoingdata packets (packet arrival rate Pnet) is takenas the first input for FIS. Whenever the buffer is not full then the number of incoming data packets and number of buffered data packets are equal. And whenever buffer is full then the number of incoming data packets is more than the number of buffered data packets. Then the first input for FIS is calculated by equation (7):

$$P_{net} = P_{in}/P_{out} \text{ - - - - - - - ------- - - - - - - - - - (7)}$$

Second Input:

Second input (buffer occupancy B_f)current buffer capacity which is computed by equation (8):

$$B_f = (T_p\text{-}C_p)/T_p \text{- - - -- - - - - - --- - - - - - - - - - (8)}$$

Where C_p is number of buffered packetsandT_p is buffer size. When $C_p = 0$ then B_f is maximum means buffer is empty and when $C_p = T_p$ then B_f is minimum means buffer is full.

Computing TTV as FIS output:

Evaluation of TTV as FIS output the following steps areneeded to be followed.

Fuzzification:

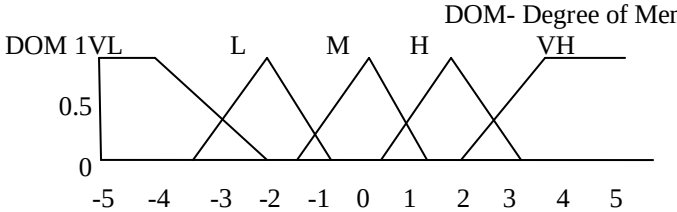
It can be determined as the operation of mapping a crisp object to a fuzzy set which is known as membership function (MF).MFs forthe inputs Pnet and Bf, whichare shown in figures7(a) and7(b).Equation (10) calculates the scale mapping and makes appropriate change on minimal and maximal of universe discourse for P_{net}.The P_{net} will be converted to $P_{Fnet}$and the related MFs, which is shown in figure7(a). The linguistic value of M shows that $P_{in} = P_{out}$. H and VH illustrate that $P_{in} > P_{out}$and L and VL illustrate that $P_{in} < P_{out}$.

MFs of B_f are drawn in figure7(b) which is second input. When buffer is at least 70% empty then it is denoted by VH and when buffer is at most 30% empty then it is denoted by VL.

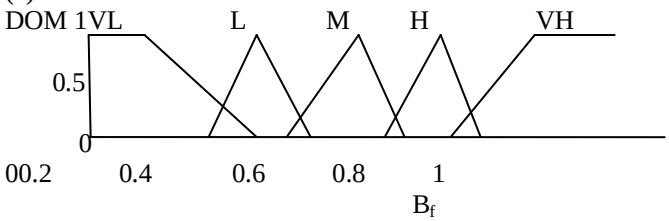
$$P_{net} = \begin{cases} -1/P_{net} & P_{in} < P_{out} \\ 1 - P_{net} & P_{in} = P_{out} \\ P_{net} & P_{in} > P_{out} \end{cases} \text{ ------ - - - - - - - - - - - - - - - (10)}$$

Inference phase based on Rules:

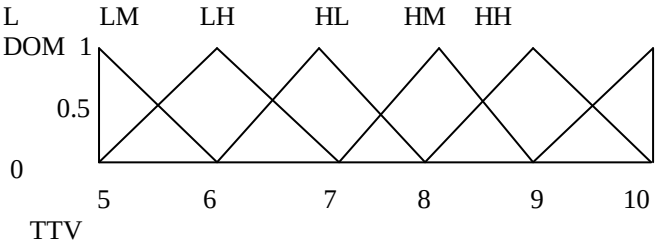
The suitable TTV in fuzzy form can be produce when the predetermined sets of linguistic rules are applied on "Inference Engine". The membership function of TTV is drawn in figure7(c), where minimum and maximum TTV is illustrated by LL and HH respectively.



(a)



(b)



(c)

Figure 7.PFnet, Bf and TTV membership functions

TTV		P_{Fnet}				
		VL(Very Low)	L(Low)	M(Medium)	H(High)	VH(Very High)
B_f	VL(Very Low)	LH(Low High)	HL(High Low)	HM(High Medium)	HH(High High)	HH(High High)
	L(Low Low)	LH(Low High)	LH(Low High)	HL(High Low)	HM(High Medium)	HH(High High)
	M(Medium)	LM(Low Medium)	LH(Low High)	LH(Low High)	HL(High Low)	HM(High Medium)
	H(High)	LL(Low Low)	LM(Low Medium)	LH(Low High)	HL(High Low)	HL(High Low)
	VH(Very High)	LL(Low Low)	LL(Low Low)	LM(Low Medium)	LH(Low High)	HL(High Low)

Table 5 Fuzzy rule table for inferring TTV based on P_{Fnet} and B_f

Defuzzification:

It performs the scale mapping and it converts the range of fuzzyfied output into corresponding non-fuzzy form. The range of converted fuzzy TTV is {5, 6, 7,….., 10} here 10 and 5 are non-fuzzy forms of HH and LL which shows the packet loss is maximum and minimum respectively.Table 5 is the rule base for this algorithm.

III. Comparison of surveyed algorithms:

The following table 6 defines the comparison of above mentioned fuzzy based congestion estimation techniques and their merits and demerits.

Table 6. Comparative Analysis of Fuzzy Based Congestion Estimation Techniques

Technique	Details of fuzzy model used in the Technique	Key Features
Fuzzy based Congestion Estimation	**Fuzzy Logic Type** - Type-1 Fuzzy Set **Input Parameters** - Net packet arrival rate - current buffer occupancy **Output Parameter** - The stringent measurement for congestion estimation	**Merits** - More Efficient than non-fuzzy Techniques. - It helps to enhance the QoS mechanisms in WSNs. **Demerits** - Limited buffer size. - Implementation works well with increased network traffic or packet generation rate, so it is not power efficient.

Fuzzy Rate Control	**Fuzzy Logic Type** - Type-1 Fuzzy Set **Input Parameters** - Queue length error - Outgoing flow rate **Output Parameter** - To achieve maximum utilization, K_q **Membership function for Input Parameters** **For Queue length error** Trapezoidal-Close(NL), Far(PH) Trapezoidal-NM, ZO, PM **For Outgoing flow rate** Trapezoidal-Close(Very-Low(VL)), Far(Very-High(VH)) Trapezoidal-Low(L), Medium(M), High(H) **Membership function for Output Parameter** Trapezoidal-Close(Very-Low(VL)), Far(Very-High(VH)) Trapezoidal-Low(L), Medium(M), High(H)	**Merits** - More Efficient than non-fuzzy Techniques. - It consumes some energy. - It is very easy to use and do not need of heavy process too. - It is implemented at each one node because of its simplicity. **Demerits** - It improves the delay per packet. - It is not capable to detect and eliminate the malicious sensor nodes.
Fuzzy Based Trust Estimation	**Fuzzy Logic Type** - Type-1 Fuzzy Set at Two Level **Input Parameters** **First Input** - Number of forward packets - Delay of forward packets - Validity of forward packets **Second Input** - Buffer Capacity **Output Parameter** - Trust value **Membership Function for First Input Parameters** **For Number** - Trapezoidal-Close(Very-Low(VL)), Far(Very-High(VH)) - Triangular-Low(L), Medium(M), High(H) **For Delay** - Trapezoidal-Close(Very-Low(VL)), Far(Very-High(VH)) - Triangular-Low(L), Medium(M), High(H) **For Validity** - Trapezoidal-Close(Very-Low(VL)), Far(Very-High(VH)) - Triangular-Low(L), Medium(M), High(H) **Membership Function for Second Input Parameters** **For Buffer Capacity**	**Merits** - It is a novel Congestion control technique. - It is in-network fuzzy based processing. - It increases packet delivery to 27.5% and reduces packet loss ratio to 40% when there are 16% of nodes are malicious. **Demerits** -It is not more energy efficient.In this technique there are several input parameters. This needs more attention.

	- Trapezoidal-Close(Very-Low(VL)), Far(Very-High(VH))) - Triangular-Low(L), Medium(M), High(H) **Membership Function for Output Parameters** - Trapezoidal-Close(Very-Low(VL)), Far(Very-High(VH)) - Triangular-Low(L), Medium(M), High(H)	
FEEPRP	**Fuzzy Logic Type** - Type-1 Fuzzy Set **Input Parameters** - Energy - Hop Count - Packet Dropped **Output Parameter** - To get appropriate choice of route **Membership function for Input Parameters** **For Residual Energy** - Trapezoidal-Average - Triangular-Low, High **For Hop Count** - Trapezoidal-Average - Triangular-Low, High **For Packet Dropped** - Trapezoidal-Average - Triangular-Low, High **Membership function for Output Parameter** - Trapezoidal-Close(Very-High(VH)), Average(Medium(M)), Far(Very-Low(VL)) Triangular-High(H), Low(L)	**Merits** - It is energy efficient because it provides secure route from source to destination. - It helps to impart effective security to the WSNs. - It is able to avoid malicious nodes and prevent data loss. - It does not adopt the idea of MAC or digital signature. **Demerits** - It is not able to improve packet delivery ratio. It finds several routes from source to destination so it is not simple to use and also it has heavy process.
FCCTF	**Fuzzy Logic Type** - Type-1 Fuzzy Set **Input Parameters** **First Input** - Ratio of received to forwarded packets (P_{Fnet}) **Second Input** - Current buffer capacity (B_f) **Output Parameter** - Threshold Trust value **Membership function for Input Parameters** **For P_{Fnet}** - Trapezoidal-Close(Very-Low(VL)), Far(Very-High(VH))	**Merits** - It is improved version of "Trust estimation based on Fuzzy logic for congestion control in wireless sensor network (FCC)". - It improves packet delivery ratio up to 18.5% more. - It reduces the packet drop of legitimate nodes is 20% less than FCC. - When TTV is increases then more malicious nodes are detected and blocked. **Demerits** - It is not more energy efficient because it uses two types of modes. It is implemented with heavy processing.

	- Triangular-Low(L), Medium(M), High(H) **Membership Function for Second Input Parameters** **For B_f** - Trapezoidal-Close(Very-Low(VL)), Far(Very-High(VH)) - Triangular-Low(L), Medium(M), High(H) **Membership function for Output Parameter** Right Triangular-Close(Low-Low(LL)), Far(High-High(HH)) Triangular-Low-Medium(LM), Low-High(LH), High-Low(HL), High-Medium(HM)	

IV. Conclusion

Congestion estimation and congestion control in wireless sensor networks is very important. We have discussed merits and demerits of each surveyed algorithm. We found that fuzzy logic is an efficient tool for congestion estimation and congestion control. We also found that fuzzy based congestion estimation techniques perform better than that of previous non-fuzzytechniques in present scenario.

References:

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci (2002), 'Wireless sensor networks: a survey', Computer Networks (Elsevier), 38, pp. 393-422.

[2] Jennifer Yick, Biswanath Mukherjee, and DipakGhosal (2008), 'Wireless sensor network survey', Computer Networks (Elsevier), 52, pp. 2292–2330.

[3] Na Xia, Mei Tang, Jian-guo Jiang, Dun Li, and Hao-weiQian (2008), 'Energy Efficient Data Transmission Mechanism in Wireless Sensor Networks', International Symposium on Computer Science and Computational Technology (ISCSCT), vol. 1, pp. 216 – 219.

[4] PengJi, Chengdong Wu, Jian Zhang, and Tianbao Wang (2011), 'A New Reliable Transmission Protocol for Wireless Sensor Network', Chinese Control and Decision Conference (CCDC), pp. 3786 – 3790.

[5] Hironori Ando, Elis Kulla, Leonard Barolli, ArjanDurresi, FatosXhafa, and Akio Koyama (2011), 'A New Fuzzy-based Cluster-Head Selection System for WSNs', International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS), pp. 432 – 437.

[6] Indranil Gupta, Denis Riordan, and SrinivasSampalli (2005), 'Cluster-head Election using Fuzzy Logic for Wireless Sensor Networks', The 3rd Annual Communication Networks and Services Research Conference, pp. 255 – 260.

[7] SercanGök, Adnan Yazıcı, AhmetCosar, and Roy George (2010), 'Fuzzy Decision Fusion for Single Target Classification in Wireless Sensor Networks', IEEE International Conference on Fuzzy Systems (FUZZ), pp.1-8.

[8] Tae Kyung Kim, and Hee Suk Seo (2008), 'A Trust Model using Fuzzy Logic in Wireless Sensor Network', World Academy of Science, Engineering and Technology, 42, pp. 63-66.

[9] Jasvinder Singh, and Dirk Pesch (2011), 'Towards Energy Efficient Adaptive Error Control in Indoor WSN: A Fuzzy Logic based Approach', IEEE 8th International Conference on Mobile Adhoc and Sensor Systems (MASS), pp. 63 – 68.

[10] Carl Larsen, MaciejZawodniok, and SarangapaniJagannathan (2007), 'Route Aware Predictive Congestion Control Protocol for Wireless Sensor Networks', IEEE 22nd International Symposium on Intelligent Control, pp. 13 – 18.

[11] SudipMisra, VivekTiwari, and Mohammad S. Obaidat (2009), 'Adaptive Learning Solution for Congestion Avoidance in Wireless Sensor Networks', IEEE/ACS International Conference on Computer Systems and Applications, pp. 478 – 484.

[12] Mohammad MasumuzzamanBhuiyan, IqbalGondal, and JoarderKamruzzaman (2010), 'CAM: Congestion Avoidance and Mitigation in Wireless Sensor Networks', IEEE 71st Vehicular Technology Conference (VTC 2010-Spring), pp. 1 – 5.

[13] Saad A. Munir, Yu Wen Bin, Ren Biao, and Ma Jian (2007), 'Fuzzy Logic based Congestion Estimation for QoS in Wireless Sensor Network', IEEE Wireless Communications and Networking Conference (WCNC), pp. 4336 – 4341.

[14] M. Ghalehnoie, N. Yazdani, and F. R. Salmasi (2008), 'Fuzzy Rate Control in Wireless Sensor Networks for Mitigating Congestion', International Symposium on Telecommunications (IST), pp. 312 – 317.

[15] Mani Zarei, Amir MasoudRahmani, AvestaSasan, and Mohammad Teshnehlab (2009), 'Fuzzy based trust estimation for congestion control in wireless sensor networks', International Conference on Intelligent Networking and Collaborative Systems (INCOS), pp. 233 – 236.

[16] SudipMisra, Sanchita Roy, Mohammad S. Obaidat, and DebashishMohanta (2009), 'A Fuzzy Logic-Based Energy Efficient Packet Loss Preventive Routing Protocol', International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), vol. 41, pp. 185 – 192.

[17] Amir MasoudRahmani, Mani Zarei, RaziehFarazkish, and Sara Zahirnia (2010), 'FCCTF: Fairness Congestion Control for a disTrustful wireless sensor network using Fuzzy logic', 10th International Conference on Hybrid Intelligent Systems(HIS), pp. 1 – 6.