Journal of Computing and Information Technology - CIT 23, 2015, 2, 95–109
doi:10.2498/cit.1002480

Trust Integrated Congestion Aware Energy Efficient Routing for Wireless Multimedia Sensor Networks (TCEER)

Arpita Chakraborty[1], Srinjoy Ganguly[2], Mrinal Kanti Naskar[2] and Anupam Karmakar[3]

[1]Department of Electronics and Communication Engineering, Techno India, Salt Lake, Kolkata, India
[2]Department of Electronics and Telecommunication Engineering, Jadavpur University, ADES Lab, Kolkata, India
[3]Department of Electronic Science, University of Calcutta, Kolkata, India

Congestion control and energy consumption in Wireless Multimedia Sensor Network is a new research subject which has been ushered in through the introduction of multimedia sensor nodes that are capable of transmitting large volume of high bit rate heterogeneous multimedia data. Most of the existing congestion control algorithms for Wireless Sensor Networks do not discuss the impact of security attacks by the malicious nodes in network congestion. Sensor nodes are prone to failure and malicious nodes aggravate congestion by sending fake messages. Hence, isolation of malicious nodes from data routing path reduces congestion significantly. Considering that, we have proposed a new Trust Integrated Congestion Aware Energy Efficient Routing algorithm, in which malicious nodes are identified using the concept of trust. The parameter Node Potential is computed, on the basis of the trust value, congestion status, residual energy and the distance of the node from the base station, using Fuzzy Logic Controller. The source node selects the node with the highest potential in its one hop radio range for data transmission which is light weight as well as energy efficient. Finally, merits of the proposed scheme are discussed by comparing them with existing protocols and the study exhibits 25% improvements in network performance.

Keywords: wireless multimedia sensor network, malicious nodes, trust, congestion control, fuzzy logic controller, energy efficient routing

1. Introduction

Wireless Multimedia Sensor Networks (WMSNs) is a new, emerging field of Wireless Sensor Networks (WSNs). They contain sensor nodes having low cost CMOS cameras, microphones and other sensor devices for retrieving video and audio streams, still images and scalar sensor data from the physical environment [1]. Similar to WSNs, WMSNs are resource constrained in terms of battery power, memory space, computational capability and communication bandwidth. The densely populated, randomly deployed sensor nodes in WMSNs are heterogeneous in nature and generate large volume of high bit rate multimedia data which are either of snap shot type or of streaming data type. Snap shot type multimedia data is bursty in nature, which is obtained through event triggered observation in a short time period whereas streaming multimedia content is generated over longer time period and requires sustained continuous delivery of information [2]. All these multimedia data may create network congestion in the upstream direction from the source node to the base station (BS), if the data processing and transmission speed lag behind the speed of the incoming traffic. Congestion creates buffer overflow, increased latency, packet drops, wastage of energy, deterioration of Quality of Service (QoS) and lowering the network throughput. Even in the worst case of severe congestion, the entire operation of the network may collapse. So, congestion detection and congestion control of a network is absolute necessity by any means. Since the traditional congestion control mechanisms are not suitable for resource constraint WSNs, the challenge is to design energy efficient and reliable congestion controlled transport mechanisms for WSNs as well as for WMSNs, to optimize network re-

sources and QoS requirements. Although some congestion control algorithms for WSNs are available in literature, most of them do not consider the impact of security attack and the role of malicious nodes on network congestion. Generally, low cost sensor nodes are prone to failure and sometimes behave as faulty nodes in due course of time. The faulty nodes are known as the malicious nodes when they behave intelligently to lead to several security threats in the sensor networks without getting detected easily. Some security attacks, as described in [3] and [4], have direct impact on the network congestion. For example, HELLO flood attacks, Jamming attacks, Sybil attacks and Node replication attacks aggravate congestion by flooding the network with fake messages, jamming intermittently, retransmitting same message several times and creating false node identification respectively. The resulting effect is additional computation and communication overhead and an increase in energy consumption which effectively reduces network lifetime.

In this paper, we are interested in reducing the network congestion in WMSNs by the detection and isolation of malicious nodes from data routing path, using the concept of trust. The proposed algorithm is the extended version of the previous work [5], in which trusted nodes forward data packets to its one hop neighboring node in radio communication range, on the basis of the parameter called *Node Potential* which is a function of trust value, congestion status, distance of the node from the BS and the remaining energy of the node. The performance analysis and the simulation results show the merits of the proposed scheme in comparison with other similar protocols.

The rest of the paper is organized as follows. In Section 2, we review related works. Detailed description of the proposed trust integrated congestion aware energy efficient routing algorithm is presented in Section 3. Simulation results, performance evaluation and comparison with peers are included in Section 4. Finally, Section 5 concludes the paper.

2. Related Works

Congestion and security attacks are common phenomena in resource constrained WSNs, especially for WMSNs, where a large volume of high bit rate multimedia data need to be managed by the network. Many novel algorithms have been proposed in literature for energy efficient routing in WSNs. But most of them do not consider practical problems that arise due to the presence of malicious nodes and congestion in the network. Trust-based congestion aware routing in WSNs is a new research topic which has not been addressed in literature to a great extent. T-LEACH [6] is the improved version of the popularly known data-gathering algorithm LEACH [7], which minimizes the number of cluster head selection and thus extends lifetime of the network, compared to that of other similar protocols. But, scope of further improvement in network lifetime is there, since T-LEACH does not consider the existence of malicious nodes and network congestion. GMTMS [8], TRANS [9], TILSRP [10], FTRSP [11] and [12] describe routing protocols equipped with trust management. However, they do not address the problem of network congestion. CODA [13] has proposed energy efficient congestion detection and avoidance scheme for sensor networks that comprises receiver based congestion detection, open loop hop-by-hop back pressure and closed loop multisource regulation. In ESRT [14] protocol, a transport solution is developed to achieve reliable event detection with minimum energy expenditure and congestion resolution functionality. In PSFQ algorithm [15], data is distributed from a source node by pacing data at a relatively slow speed called “pump slowly” and allowing the nodes that experience data loss to recover missing segments from their local immediate neighbors aggressively called “fetch quickly”. PCCP [16] is a hop by hop congestion control algorithm in the upstream direction, in which node priority index is considered and node congestion is measured by using packet inter-arrival time and service time. A fuzzy based congestion control for WMSNs is proposed in SUIT [17], where some packets of the frames are dropped and, as a result, frames are being transmitted to the BS with lower but acceptable quality. WCCP [18] has proposed a congestion control algorithm for WMSNs, in which congestion is avoided at the source by adjusting the sending rate and by distributing the departing packets from the source. In addition, intermediate nodes in WCCP [18] monitor the queue length to detect congestion. All these protocols have discussed congestion control and have tried to

improve network performances. However, aggravation of network congestion by faulty behavior of the malicious nodes has not been discussed in these protocols by any means. The congestion and trust are both discussed in [19] – [22]. In FCC [19], Zarei *et al.* have proposed a fuzzy logic based trust estimation scheme for congestion control in WSNs. FCCTF [20] is basically a modification of FCC protocol, in which Trust Threshold value is used for decision making. In TFCC [21], traffic flow from the source node to the BS is optimized by adaptive data rate control. In addition, data packet routing in TFCC [21] uses Link State Routing Protocol which shows a major improvement in network throughput compared to FCCTF [20]. TC-ACO [22] is a trust based congestion aware routing protocol for WSNs, where Ant Colony Optimization is utilized for data packet routing. In the existing work, our goal is to represent a new trust integrated congestion aware energy efficient data routing scheme for WMSNs which exhibits promising improvement in network performance compared to other similar data routing protocols.

3. Proposed Work

The trust based congestion control for WMSNs and other application specific WSNs form the new research area that shows improvement, compared to the conventional congestion control mechanisms, in terms of network throughput and QoS. In this section, we describe the proposed TCEER algorithm, which is the extended version of the work mentioned in [5]. In this research, we consider WMSNs consisting of N number of multimedia sensor nodes randomly deployed over the sensor field, under the condition of free space propagation. We assume that all sensor nodes have equal initial energy and trust value. They are able to communicate with each other in their one hop radio range. Each node maintains a database having the above information of its one hop neighboring nodes, which is updated dynamically in regular intervals.

The proposed algorithm consists of two phases. Phase I is the *initialization phase* whereas Phase II is the *routing phase*. The details of each phase are described below.

3.1. Phase I: Initialization Phase

Phase I computes four parameters, namely *trust, complementary congestion index (CCI), distance metric and energy metric*. The malicious nodes are also segregated in this phase on the basis of their trust values.

A. Trust Evaluation

- *Trust Metric*

Trust is a new idea borrowed from the human society, in which sensor nodes monitor the behavior of their one hop neighboring nodes to establish a degree of trustworthiness in forwarding packets [6]. It is a mathematical tool, in which trust values of each node with respect to its one hop neighboring nodes are evaluated dynamically on the basis of some parameters known as the *Trust Metrics (TM)*. The examples of TM that are commonly used in trust calculation are the data packet forwarded, control packet forwarded, latency in data transmission, remaining energy of the sensor nodes, packet address modified etc.

Trust is broadly classified as *Direct Trust (DT)* and *Indirect Trust (IT)* [8], [23]. DT of a node is computed on the basis of the direct observations made by the node on the behavior of its one hop neighboring nodes during the previous data transfer through this node. On the other hand, IT of a node is calculated, depending upon the recommendations received from other trusted nodes in the surrounding. IT is mainly important for newly initialized nodes or mobile nodes that have arrived recently to a new one hop neighborhood, since previous direct communication is not available in this case. In the proposed algorithm, both DT and IT are considered for calculation of overall trust of the nodes. A predefined *Trust Threshold* (T_{TH}) value is set, depending upon the application of the sensor network. A high value of T_{TH} corresponds to a high level of security of the network. The nodes having trust value greater than T_{TH} are called trusted nodes, otherwise they are termed as malicious nodes.

- *Trust Calculation and Segregation of Malicious Nodes*

Different methods are available in literature for computing trust value of the sensor nodes.

Some of them are described in [8], [10] and [23]. In the proposed TCEER scheme, trust value of a node on its neighboring nodes within the radio range is calculated by GMTMS [8]. This has certain advantages over the other models. In Momani's model [23], if one of the TM values for data packet transmission is zero and the rest of the TMs have high values, the overall trust value of the node may be above the trust threshold. In this case, the node appears to be trustworthy, which is not correct. The above difficulties can be avoided with geometric mean based calculations. So, in our proposed model, we prefer to use GMTMS [8] algorithm.

Direct Trust of node N_1 on node N_2 (DT_{N_1,N_2}) is calculated from the geometric mean of the various Trust Metrics for different events occurring between N_1 and N_2. Any number of TM can be considered for trust computation. For k TMs, it is represented by the formula given below

$$DT_{N_1,N_2} = \Big(\prod_{i=1 \to k} (TM_i) \Big)^{\frac{1}{k}} \qquad (1)$$

Indirect Trust of node N_1 on node N_2 (IT_{N_1,N_2}) is computed by the geometric mean of various Direct Trusts (DTs), obtained from different neighboring nodes of N_1. This is represented as

$$IT_{N_1,N_2} = \Big(\prod_{j=1 \to l} (DT_j) \Big)^{\frac{1}{l}} \qquad (2)$$

where $DT_1, DT_2, DT_3, \ldots, DT_l$ are the DTs from l number of neighboring nodes of N_1.

The overall trust of node N_1 on node N_2 (T_{N_1,N_2}) is the weighted sum of DT and IT which is represented by the formula.

$$T_{N_1,N_2} = W_D * DT_{N_1,N_2} + W_I * IT_{N_1,N_2} \qquad (3)$$

and $W_D + W_I = 1$.

W_D and W_I are the weights to DT and IT respectively. In some applications, DT has been given more importance than IT and, accordingly, the value of W_D is chosen higher than that of W_I. In the proposed scheme, we have considered equal values of W_D and W_I. This implies equal importance towards DT and IT respectively. For trusted node $T_{N_1,N_2} > T_{TH}$, whereas for malicious nodes $T_{N_1,N_2} < T_{TH}$. Thus, in TCEER scheme, all the malicious nodes are identified and then blocked, so that they cannot take part in the data packet routing algorithm.

B. Congestion Evaluation

- *Complementary Congestion Index (CCI)*

In the proposed work, congestion of the sensor nodes is estimated from the buffer queue size of the corresponding nodes. We have introduced a new congestion metric known as the *Complementary Congestion Index (CCI)* which measures the congestion status of the nodes. CCI is defined as the function of the buffer queue length and is quantified as described below.

- *Computation of CCI*

Computation of CCI for trusted nodes, having trust values greater than T_{TH} level, is considered. Since computation of CCI for malicious nodes is excluded, the energy overhead is reduced. Two fixed threshold values, $C_{Th}(\text{Min})$ and $C_{Th}(\text{Max})$ are defined in the range of the buffer queue length. If buffer queue length is less than $C_{Th}(\text{Min})$, congestion is low, if it is between $C_{Th}(\text{Min})$ and $C_{Th}(\text{Max})$, congestion is medium and if it is greater than $C_{Th}(\text{Max})$, congestion is high [2]. It is assumed that every sensor node has only one buffer where it stores all the packets that are obtained from its own local source as well as the packets accepted from its one-hop neighbors. Let the buffer queue length of the kth node be denoted by $Q_s(k)$.

$I_{K'} = 1 - I_K$	
$Q_s(k)$	I_k
$Q_s(k) \leq C_{TH}(\text{Min})$	$\in$ (where $\in$ is a small quantity)
$C_{TH}(\text{Min} \leq Q_s(k) \leq C_{TH}(\text{Max})$	$(1-\in)\left(\frac{Q_s(k)-C_{TH}(\text{Min})}{C_{TH}(\text{Max})-C_{TH}(\text{Min})}\right)+\in$
$Q_s(k) > C_{TH}(\text{Max})$	1

Table 1. Formulae for computation of CCI.

The *Complementary Congestion Index (CCI)* is calculated, which is the function of the buffer queue length. Let CCI for the kth node be represented by $I_{K'}$ and $I_{K'} = f(Q_s(k))$. Then $I_{K'}$ can be computed mathematically from *Congestion Index* I_K, as shown in Table 1.

- *C. Evaluation of Residual Energy*

The residual energy of the node is one of the most important parameters in hop by hop routing protocol. In the proposed work, let us consider that initial energy of all nodes is the same and is denoted by $E_{initial}$. The effective residual energy (E_{er}) of the node is normalized as:

$$E_{er} = \omega * E_{cn} + (1 - \omega) * E_{pnn} \qquad (4)$$

Here, E_{cn} denotes the energy of the present source node and E_{pnn} represents the energy of the potential next node in one hop neighbor within the radio communication range. The parameter ω is the weighing factor, usually set to a value less than 0.5 so as to give higher priority to the remaining energy of the potential next node. The potential next node is the nearest trusted node from the present source node, within its one hop neighbor radio communication range.

- *D. Evaluation of Distance Metric*

In order to ensure the direction of data transmission from the source node towards BS, we have introduced a new parameter known as the Dist_Metric which is explained below.

In Figure 1, nodes A, B and C represent the present source node, the potential next node and the BS respectively. The node B is lying within one hop neighbor radio communication range of node A, as shown by the dotted line.

Let d_1 be defined as the ratio of the distance between the present source node and the potential next node to the radio communication range of the sensor node. Similarly, d_2 is the ratio of the distance between the potential next node and BS to the distance between the present source node and BS.

Thus, from Figure 1 we get $d_1 = AB/r$ and $d_2 = BC/AC$, where radio communication range of the sensor node is specified as 'r' unit.

The parameters d_1^C and d_2^C are called the complementary distance from the present source node and the complementary distance from the BS respectively, which are given by the following relations.

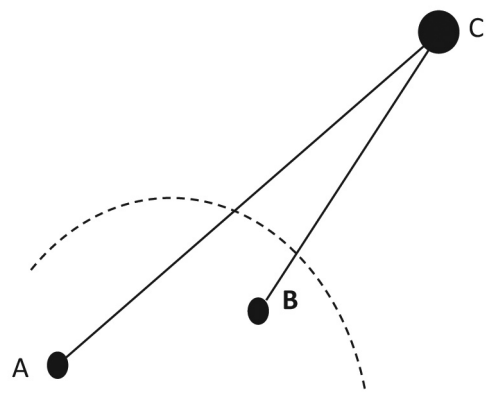

Figure 1. Computation of Distance Metric.

$$d_1^C = 1 - d_1, \quad d_2^C = 1 - d_2 \qquad (5)$$

It is obvious that lower values of d_1 and d_2 or higher values of d_1^C and d_2^C imply more desirable conditions.

The Dist_Metric of the potential next node is related to d_1^C and d_2^C, which is represented by the equation

$$\text{Dist\_Metric} = \frac{k_1 * d_1^C + k_2 * d_2^C}{k_1 + k_2} \qquad (6)$$

where k_1 and k_2 are the weights of d_1^C and d_2^C respectively. In the proposed TCEER algorithm, we have given more importance to the distance of the potential next node from the BS and hence the value of k_2 is chosen higher, compared to the value of k_1. In order to make the routing distance minimum, the potential next node should always be closer to the BS, compared to the present source node. Hence, in Figure 1, the distance BC is less than the distance AC, which implies that the ratio d_2 is always less than one.

3.2. Phase II – Routing Phase

In this phase, a Fuzzy Logic Controller (FLC) is used for the computation of the parameters known as the *Trust Congestion Metric (TCM)* and the *Energy Distance Metric (EDM)* of the trusted nodes. FLC is considered for the quantitative analysis of the parameters from the qualitative or imprecise information.

- *Fuzzy Logic Controller (FLC)*

In the proposed algorithm, Mamdani fuzzy model is used due to its widespread acceptance. The general architecture of the Mamdani FLC is shown in Figure 2. It consists of four components, namely fuzzifier, IF-THEN rule base, fuzzy inference mechanism and defuzzifier. The fuzzifier converts crisp input data to fuzzy sets. The fuzzy output is obtained from fuzzy inference mechanism by adding fuzzy rules to a mapping routine from input to output of the system. Finally, the defuzzifier extracts a crisp output value from the output fuzzy set.

- *Trust Congestion Metric (TCM)*

In the proposed TCEER algorithm, characteristics of the sensor nodes are described in terms of trust and congestion, with the help of the parameter called *Trust Congestion Metric (TCM).*

- *Energy Distance Metric (EDM)*

The residual energy and the distance of the node from the BS are quantified by the parameter called *Energy Distance Metric (EDM).*

- *Computation of TCM and EDM*

The configuration of the FLC used in TCEER algorithm is shown in Figure 3. It consists of a Fuzzifier-1/ Defuzzifier-1/ Rule Base-1/ Inference Mechanism-1 and a Fuzzifier-2/ Defuzzifier-2/ Rule Base-2/ Inference Mechanism-2, respectively. The four parameters (Trust, CCI, Effective residual energy E_{er} and Dist_Metric) obtained from phase I, are used as inputs to the FLC. The TCM and EDM are the two outputs of FLC that are inferred through the corresponding rule bases and inference mechanisms.

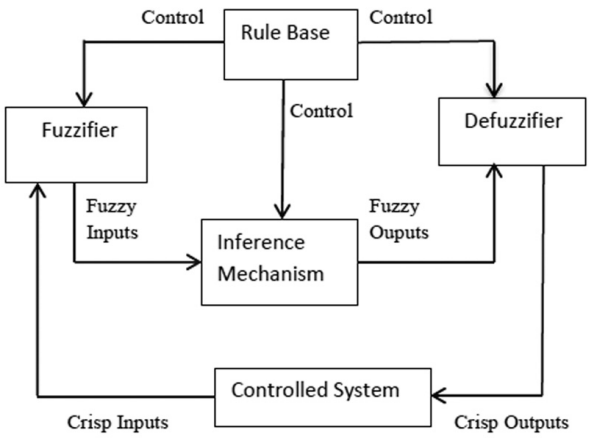

Figure 2. General Architecture of a Fuzzy Logic Controller.

The fuzzy trust values of the nodes are categorically divided into five classes, namely Very Low Trust (VLT), Low Trust (LT), Medium

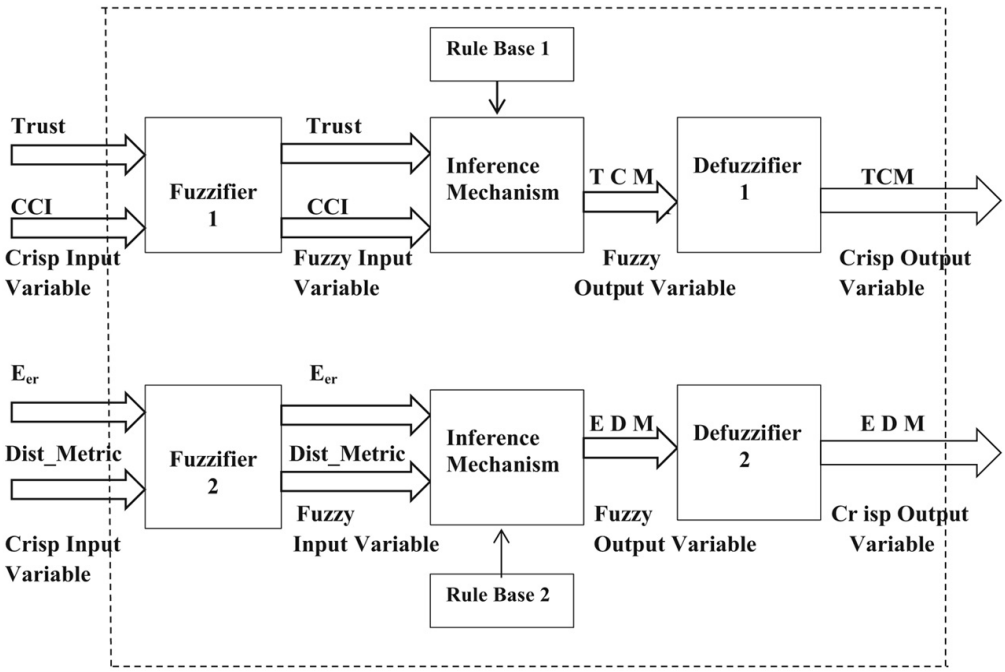

Figure 3. Schematic diagram of FLC used in TCEER.

Trust (MT), High Trust (HT) and Very High Trust (VHT). Similarly, Fuzzy CCI values of the nodes are classified as Very Low CCI (VLCC), Low CCI (LCC), Medium CCI (MCC), High CCI (HCC) and Very High CCI (VHCC). The crisp input range and fuzzy Input variable for Trust and CCI are shown in Tables 2 and 3 respectively. The inference mechanism and rule base 1 for generation of fuzzy output variable TCM are shown in Table 4, which is classified as Very Low (VL), Low (L), Medium (Medium), High (H) and Very High (VH) respectively. The crisp value of the TCM with respect to the corresponding fuzzy value is depicted in Table 5.

The residual energy E_{er} and the Dist_Metric of the nodes, obtained from the equations (4) and (6) respectively are taken as the two input variables in Fuzzifier 2. The Dist_Metric is fuzzified into five classes known as Very Far Distance (VFD), Far Distance (FD), Medium Distance (MD), Close Distance (CD) and Very Close Distance (VCD). Similarly, the residual energy is also classified as Very Low Energy (VLE), Low Energy (LE), Medium Energy (ME), High Energy (HE) and Very High Energy (VHE). Table 6 and Table 7 represent the crisp input ranges and the fuzzy input variables for Dist_Metric and the residual energy respectively. The fuzzy value of EDM is divided into five classes, namely Very Low (VL), Low (L), Medium (M), High (H) and Very High (VH). The rule base 2 and the crisp value of EDM

Crisp Input Range	Fuzzy Trust Value
0 – 0.4	VLT
0.2 – 0.6	LT
0.5 – 0.8	MT
0.75 – 0.95	HT
0.85 – 1	VHT

Table 2. Crisp input range and fuzzy trust value.

Crisp Input Range	Fuzzy CCI Value
0 – 0.3	VLCC
0.25 – 0.5	LCC
0.45 – 0.75	MCC
0.7 – 0.9	HCC
0.8 – 1	VHCC

Table 3. Crisp input range and fuzzy CCI value.

Sl no.	Fuzzy CCI Value	Fuzzy Trust Value	Fuzzy Output Variable TCM
1.	VLCC/LCC/MCC	VLT	VL
2.	HCC/VHCC	VLT	L
3.	VLCC	LT	VL
4.	LCC/MCC	LT	L
5.	HCC/VHCC	LT	M
6.	VLCC/LCC	MT	L
7.	MCC/HCC	MT	M
8.	VHCC	MT	H
9.	VLCC	HT	L
10.	LCC	HT	M
11.	MCC	HT	H
12.	HCC/VHCC	HT	VH
13.	VLCC	VHT	L
14.	LCC	VHT	M
15.	MCC	VHT	H
16.	HCC/VHCC	VHT	VH

Table 4. Rule base 1.

Fuzzy Output Variable, TCM	Crisp Value of the Output Variable, TCM
VL	0 – 0.2
L	0.1 – 0.4
M	0.3 – 0.7
H	0.65 – 0.95
VH	0.8 – 1.0

Table 5. Fuzzy TCM value and crisp output range.

Crisp Input Range	Fuzzy Dist_Metric Value
0 – 0.3	VFD
0.2 – 0.4	FD
0.35 – 0.65	MD
0.6 – 0.85	CD
0.8 – 1.0	VCD

Table 6. Crisp input range and fuzzy Dist_Metric.

Crisp Input Range	Fuzzy E_{er} Value
0 – 0.3	VLE
0.2 – 0.5	LE
0.4 – 0.7	ME
0.6 – 0.9	HE
0.8 – 1	VHE

Table 7. Crisp input range and fuzzy E_{er}.

with respect to the corresponding fuzzy value are given in Tables 8 and 9 respectively.

- *Computation of Node Potential and Data Packet Routing*

Data packet routing in TCEER algorithm is done on the basis of the parameter known as the *Node Potential (NP)* which is a function of trust value, congestion status, distance of the node from the BS and the remaining energy of the node. NP of the trusted node is calculated by the relation shown below.

$$Node\ Potential = \frac{\alpha * EDM + \beta * TCM}{\alpha + \beta} \quad (7)$$

Here, α and β are the weightage of EDM and TCM respectively that are assigned on the basis of the application of the sensor network. For example, in some security related applications, more importance is given to TCM compared to EDM and hence the value of β is kept higher than α. It is to be noted that the summation of α and β is always unity.

Sl no.	Fuzzy E_{er}	Fuzzy Dist_Metric	Fuzzy Output EDM
1.	VLE/LE	VFD	VL
2.	ME/HE	VFD	L
3.	VHE	VFD	M
4.	VLE	FD	VL
5.	LE/ME	FD	L
6.	HE/VHE	FD	M
7.	VLE/LE	MD	L
8.	ME	MD	M
9.	HE/VHE	MD	H
10.	VLE/LE	CD	L
11.	ME	CD	M
12.	HE	CD	H
13.	VHE	CD	VH
14.	VLE	VCD	L
15.	LE	VCD	M
16.	ME	VCD	H
17.	HE/VHE	VCD	VH

Table 8. Rule base 2.

Fuzzy Output EDM	Crisp Value of EDM
VL	0 – 0.25
L	0.15 – 0.35
M	0.3 – 0.8
H	0.75 – 0.95
VH	0.85 – 1.0

Table 9. Fuzzy EDM and crisp output range.

Figure 4 shows hop by hop data packet routing mechanism with TCEER protocol. The source node selects destination node with highest NP from its one hop neighboring nodes in the radio communication range. The node with NP value less than some threshold value (NP_{TH}) is not considered for data packet routing. In the next hop, the above mentioned destination node acts as the present source node and selects intermediate destination node with highest NP from its one hop neighboring nodes in the radio communication range. Similarly, in the next hop, the previously mentioned intermediate destination node acts as present source node and selects another intermediate destination node with highest NP from its one hop neighboring nodes. In this way, data packets are forwarded hop by hop until the destination node is the BS.

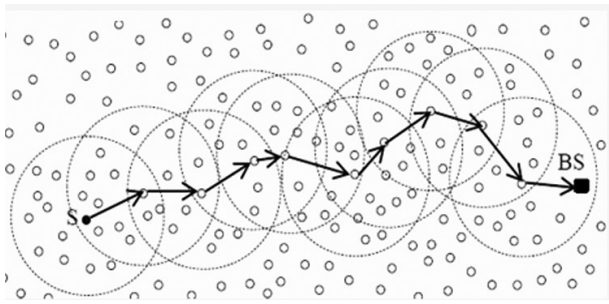

Figure 4. Route formation with TCEER algorithm.

Nomenclatures of the parameters that are used in the proposed algorithm are listed in Table 10.

4. Simulation Results

In this section, the merits of the proposed TCEER scheme have been investigated through extensive MATLAB simulations. We have considered an arbitrary network, comprising 50 multimedia sensor nodes deployed randomly into a field of dimensions 100 m * 100 m and 200 m * 200 m respectively. The distances of

Parameter	Description
DT	Direct Trust
IT	Indirect Trust
TM	Trust Metric
T_{TH}	Trust Threshold
CCI	Complementary Congestion Index
$E_{initial}$	Initial Energy of the Nodes
E_{er}	Effective Residual Energy of the Nodes
E_{cn}	Energy of the present Source Node
E_{pnn}	Energy of the potential Next Node
d_1^C	Complementary Distance from the present Source Node
d_2^C	Complementary Distance from the Base Station
Dist_Metric	Distance Metric
TCM	Trust Congestion Metric
EDM	Energy Distance Metric
NP	Node Potential
PRR	Packet Reception Ratio
MRA	Maximum Retransmission Attempts

Table 10. Nomenclatures of the parameters.

the nodes from the base station are taken stationary throughout the experiment. In the simulation experiments, any number of TMs can be considered. However, for the sake of simplicity, we have taken only three TMs, namely *data packet forwarded, packet address modified and remaining energy of the nodes*. Initially, we have considered that the sensor nodes are all trusted nodes. Trust value of a node is updated periodically after time Δt equal to 5 seconds. A Trust Threshold (T_{Th}) value is taken as 0.5 whereas minimum and maximum trust values are 0 and 1 respectively.

The values of the constant parameters that have been considered in the calculations of the proposed work are listed in Table 11. We have considered W_D equal to W_I, which implies that DT and IT are given equal importance in the computation of the overall trust of the node, as represented in equation (3). Again, ω is kept less than 0.5, in order to put more importance on the remaining energy of the potential next node compared to that of the current source node, as described in equation (4). In our simulation experiment, ω has been arbitrarily set to 0.2. Similarly, k_2 is chosen higher than k_1 so that the distance of the potential next node from the BS

Parameter	Weightage	Value
W_D	Direct Trust	0.5
W_I	Indirect Trust	0.5
ω	for calculation of Energy Metric	0.2
k_1	d_1^C for calculation of Distance Metric	2
k_2	d_2^C for calculation of Distance Metric	3
α	EDM for calculation of Node Potential	0.3
β	TCM for calculation of Node Potential	0.7

Table 11. Constant parameters used in TCEER.

is less than the distance of the present source node to the BS, as given in equation (6).

Again, as shown in Table 11, $\beta > \alpha$ implies that, during computation of NP of the corresponding node, the trust and congestion of the node are given more importance than the remaining energy and the distance of the node from the BS. Thus, the values of the constant parameters used in the proposed scheme are justified.

The graphical views of the parameters, TCM and EDM of the sensor nodes, obtained from the simulations of TCEER algorithm, are shown in Figures 5 and 6 respectively. The data packet routings in TCEER protocol for different numbers of packets are simulated in MATLAB. The route formations in TCEER with a single packet, 5 packets and 20 packets are depicted in Figure 7, Figure 8 and Figure 9 respectively. Since the nodes are deployed randomly in the sensor fields, the node position changes in each simulation experiment. It is found that the packets have taken different routes to reach the BS at

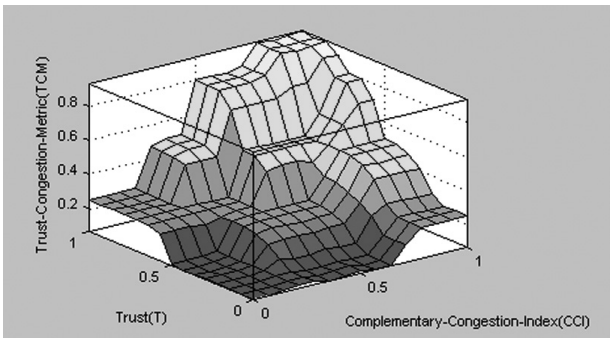

Figure 5. TCM for different values of trust and CCI.

different times, depending on the values of the NP of the intermediate nodes, which is modified dynamically at regular time interval.

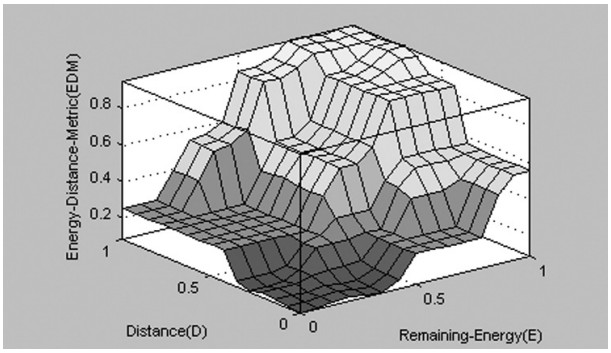

Figure 6. EDM for different values of Distance Metric and residual energy.

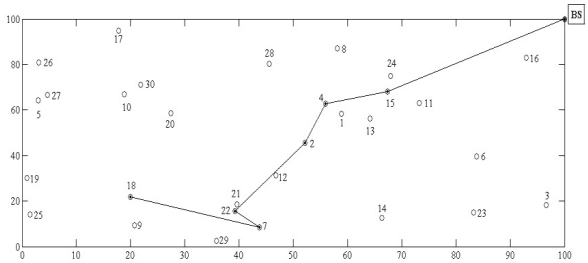

Figure 7. Routing of single packet from node 18 to the Base Station.

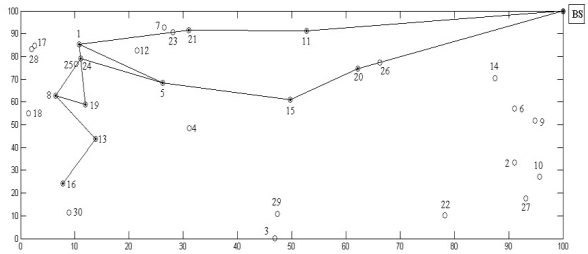

Figure 8. Routing of 5 packets from node 16 to the Base Station.

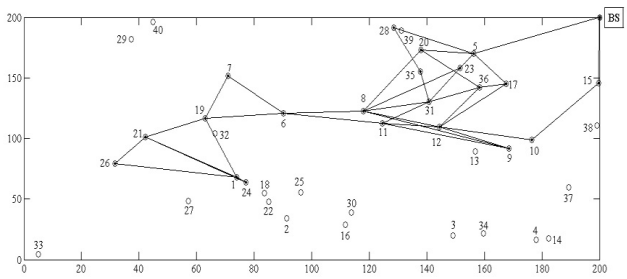

Figure 9. Routing of 20 packets from node 24 to the Base Station.

The comparison of the proposed TCEER protocol is made with the existing algorithms, namely T-LEACH [6], TRANS [9], TFCC [21] and TC-ACO [22] for different initial node energies on a 200 m * 200 m WSN field. The number of rounds versus percentage of dead nodes for the above mentioned protocols is given in Table 12, for various initial node energies. The simulation results are plotted with percentage of dead nodes as the abscissa and number of rounds as the ordinate, in Figure 10, Figure 11 and Figure 12 for initial node energy of 0.25 Joules per node, 0.5 Joules per node and 1.0 Joule per node respectively. The graphs and figures indicate that the proposed TCEER protocol provides higher network lifetime for different node energies, compared to other similar protocols and thereby outperforms its peers. It has been also observed that the proposed scheme provides better results for the initial node energy of 1.0 Joule per node in comparison to that of 0.25 Joules per node and 0.5 Joules per node respectively.

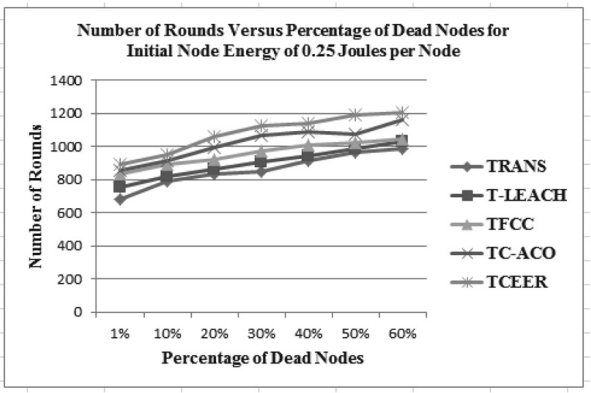

Figure 10. Performance Analysis with initial energy of 0.25 Joules per node.

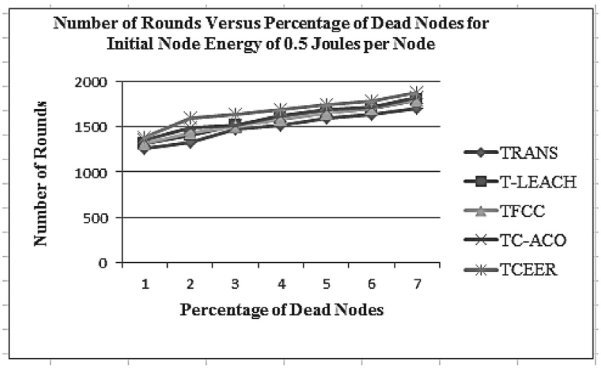

Figure 11. Performance analysis with initial energy of 0.5 Joules per node.

Inital Energy (J/node)		Protocol	Percentage of dead nodes						
			1%	10%	20%	30%	40%	50%	60%
0.25	Number of Rounds	TRANS	682	792	836	845	912	967	985
		T-LEACH	750	818	864	908	945	983	1028
		TFCC	834	892	918	970	1005	1020	1047
		TC-ACO	855	910	993	1063	1089	1075	1157
		TCEER	891	952	1060	1122	1140	1188	1202
0.5		TRANS	1258	1334	1480	1512	1604	1640	1710
		T-LEACH	1312	1405	1512	1598	1663	1710	1802
		TFCC	1320	1440	1498	1580	1647	1701	1802
		TC-ACO	1352	1495	1523	1627	1689	1723	1821
		TCEER	1386	1599	1634	1688	1745	1788	1873
1		TRANS	1965	2132	2242	2496	2701	2910	3147
		T-LEACH	2087	2221	2378	2601	2895	3020	3304
		TFCC	2223	2365	2455	2673	2812	3108	3345
		TC-ACO	2235	2413	2559	2713	2888	3217	3345
		TCEER	2406	2677	2818	2997	3108	3285	3566

Table 12. Number of rounds with percentage of dead nodes for various algorithms.

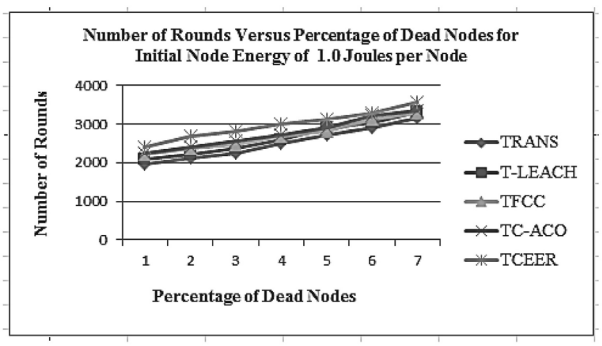

Figure 12. Performance analysis with initial energy of 1.0 Joule per node.

Next, we have studied the proposed TCEER scheme to find out the impact on *Packet Reception Ratio (PRR)* and *Maximum Retransmission Attempts (MRA)* [24], in comparison with the other existing protocols. The PRR is calculated as the ratio of the number of packets received successfully to the total number of packets transmitted. The packet retransmission is required in case of unsuccessful packet delivery. MRA means the maximum number of retransmission needed for a particular packet to send it successfully. In our experiment, we calculate the fraction of the packets reaching the BS successfully, by varying the number of retransmission attempts. As the number of retransmission attempts increases, the PRR also increases. In case of successful packet delivery, PRR is equal to one. Table 13 represents the maximum and minimum numbers of packets delivered successfully to the BS for different values of MRA for T-LEACH [6], TRANS [9], TFCC [21], TC-ACO [22] and the proposed TCEER algorithms respectively. MIN and MAX refer to the maximum and minimum values of PRR obtained over 30 runs for transmitting 25 packets.

The simulation results shown in Table 13 are based on the values of the parameters listed in Table 11. It shows that, compared to other similar algorithms, in TCEER, less number of retransmissions is required for achieving PRR value equal to one.

Next, the proposed scheme is verified under different parameter settings, where each parameter is varied, one at a time, keeping the values of other parameters constant.

Table 14 represents the number of rounds recorded, when the values of α and β are varied, keeping all other parameters at the previous values ($\omega = 0.2$, $k_1 = 2$ and $k_2 = 3$). The number of rounds at the critical point of the sensor network is recorded where 50% nodes are

Protocol	Packet Receptio Ratio (PRR)	Maximum Number of Attempts (MRA)					
		1	2	3	4	5	6
TRANS	MIN	0.53	0.61	0.74	0.81	0.96	1
	MAX	0.64	0.68	0.82	0.97	1	1
T-LEACH	MIN	0.51	0.63	0.7	0.79	0.98	1
	MAX	0.68	0.7	0.85	0.95	1	1
TFCC	MIN	0.55	0.59	0.68	0.79	0.98	1
	MAX	0.71	0.75	0.9	0.98	1	1
TC-ACO	MIN	0.62	0.65	0.72	0.96	1	1
	MAX	0.74	0.84	0.96	0.98	1	1
TCEER	MIN	0.61	0.66	0.81	0.89	1	1
	MAX	0.73	0.85	1	1	1	1

Table 13. Packet reception ratio and maximum retransmission attempts comparison.

dead. The initial node energy is considered as 0.5 Joules/node. It has been observed that maximum number of rounds is obtained for the case when α and β is equal to 0.3 and 0.7 respectively. Since the parameters α and β represent the weightage of EDM and TCM respectively, as represented in equation (7), it would imply from Table 14 that trust and congestion have greater impact on network lifetime compared to the remaining energy and the distance of the node from the BS. If β is zero, that is, congestion and trust factor are not considered at all, the number of rounds goes to minimum.

Next, the value of ω is varied from zero to one, keeping all other parameters at the previous level ($\alpha = 0.3$, $\beta = 0.7$, $k_1 = 2$ and $k_2 = 3$). The number of rounds corresponds to 50% dead nodes recorded which is shown in Table 15. The case when ω is set to zero means the energy of the current source node is not considered in the calculation of the energy metric, as represented in equation (4). On the other hand, when ω equals to one, implies that the contribution of energy of the potential next node is set to zero in the calculation of the energy metric. This is not desirable. In this case, we get minimum number of rounds, which is quite expected because energy of the potential next node has higher impact in data packet routing protocol compared to the source node. The number of rounds obtained in TCEER algorithm for 50% dead nodes is compared with that for the existing protocols. In the proposed TCEER, better results are obtained for the setting $0 < \omega < 0.5$, as shown in Table 15.

α	β	Number of rounds
0	1	1577
0.1	0.9	1687
0.2	0.8	1722
0.3	0.7	1748
0.4	0.6	1734
0.5	0.5	1691
0.6	0.4	1675
0.7	0.3	1652
0.8	0.2	1623
0.9	0.1	1594
1	0	1564

Table 14. Number of rounds when α and β is varied.

5. Conclusion

In this paper, we have discussed the relationship between trust and congestion and have proposed a novel trust based congestion aware routing protocol using Fuzzy Logic Controller for WMSNs, which is also applicable for large scale WSNs. The proposed scheme protects sensor networks against various security attacks by efficient detection and avoidance of malicious nodes. The optimum route for the data packet transfer is dynamically selected on the basis of the parameter called Node Potential (NP) which is a function of the trust and congestion

Existing Protocols	Number of Rounds at 50% Dead Nodes	Variation of ω in Proposed TCEER	Number of Rounds at 50% Dead Nodes in Proposed TCEER
TRANS	1690	ω	0
		0	1633
		0.1	1712
T-LEACH	1701	0.2	1748
		0.3	1732
		0.4	1721
TFCC	1710	0.5	1698
		0.6	1645
		0.7	1621
TC-ACO	1714	0.8	1497
		0.9	1278
		1	988

Table 15. Number of rounds with variation of ω.

status of the sensor nodes. The simulation results show that the proposed TCEER algorithm provides a significant improvement of 25% in terms of number of rounds and network lifetime, compared to the protocols T-LEACH [6] and TRANS [9]. The results are verified with different sets of parameter values. Better results of the proposed TCEER scheme are quite justified because the additional energy consumption due to the congestion obtained from the misbehavior of the faulty nodes is not considered in T-LEACH [6] and TRANS [9]. Again, the proposed TCEER algorithm shows better results of 10% and 7%, compared to TFCC [21] and TC-ACO [22] respectively. Although both parameters, trust and congestion, are considered in TFCC [21], TC-ACO [22] and TCEER protocol, the data routing algorithms are different. In TFCC [21, Link State Routing Protocol is implemented, in TC-ACO [22], it is done as per the Ant Colony Optimization whereas in TCEER, hop by hop routing on the basis of the Node Potential of the trusted nodes is implemented. In future, we would like to study the nature of congestion obtained due to the various security attacks in WMSNs. Different trust based congestion control schemes can be compared to get the improved energy efficient solution. Moreover, TCEER algorithm has been tested only on a small network. We would like to test its impact on the larger networks comprising large number of heterogeneous multimedia sensor nodes. We also desire to test its hardware implementation with IRIS motes, using TinyOS under various conditions.

References

[1] I .F. Akyildiz et al., A survey on wireless multimedia sensor networks. *Computer Networks*, **51**(3) (2007), pp. 921–960.

[2] M. H. Yaghmaee, D. Adjeroh, A new priority based congestion control protocol for wireless multimedia sensor networks. Presented in the *Proceedings of the IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks*, (2008), Newport Beach, CA.

[3] T. Kavita, D. Sridharan, Securities vulnerabilities in wireless sensor networks: A survey. *Journal of Information Assurance and Security*, **5** (2010), pp. 031–044.

[4] C. Karlof, D. Wagner, Secure routing in wireless sensor networks: Attacks and countermeasures. *AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, **1** (2003), 293-315.

[5] S. Ganguly et al., A trust-based framework for congestion-aware energy efficient routing in wireless multimedia sensor networks. Poster presented at the *Student Research Symposium of the International Conference on High Performance Computing Symposium, HiPC*, (2013), Bangalore, India.

[6] J. Hong et al., T-LEACH: The method of threshold-based cluster head replacement for wireless sensor networks. *Journal Information Systems Frontiers*, **11**(4), (2009), pp. 513–521.

[7] W. R. Heinzelman et al., Energy efficient communication protocol for wireless microsensor networks. Presented in the *Proceedings of the* 33rd *Hawaii International Conference on System Sciences*, (2000).

[8] S. S. BABU ET AL., Geometric mean based trust management system for wireless sensor networks (GMTMS). Presented in the *Proceedings of the IEEE International World Congress on Information and Communication Technologies*, (2011), pp. 444–449, Mumbai, India.

[9] S. TANACHAIWIWAT ET AL., Location-centric isolation of misbehavior and trust routing in energy constrained sensor netwoks. Presented in the *Proceedings of the IEEE International Conference on Performance Computing and Communications*, (2014), pp. 463–469.

[10] A. RAHA ET AL., Trust integrated link state routing protocol for wireless sensor network (TILSRP). Presented in the *Proceedings of the IEEE International Conference on Advanced Networks and Telecommunication Systems*, (2011), Bangalore, India.

[11] A. CHAKRABORETY ET AL., A fuzzy based trustworthy route selection method using LSRP in wireless sensor networks (FTRSP). Presented in the *Proceedings of the ACM International Conference on Computational Science, Engineering and Information Technology*, (2012), pp. 413–419.

[12] T. ZAHARIADIS ET AL., Trust management in wireless sensor networks. *European Transactions on Telecommunications*, **21** (2010), pp. 386–395.

[13] C. Y. WAN ET AL., CODA: Congestion detection and avoidance in sensor networks. Presented in the *Proceedings of the ACM International Conference on Embedded Networked Sensor Systems*, (2003), pp. 266–279, Los Angeles, USA.

[14] Y. SANKARASUBRAMANIAM ET AL., Event-to-sink reliable transport in wireless sensor networks. Presented in the *Proceedings of the ACM Symposium on Mobile Ad Hoc Networking & Computing*, (2003), pp. 177–188, Annapolis, Maryland, USA.

[15] C. Y. WAN ET AL., PSFQ: A reliable transport protocol for wireless sensor networks. Presented in the *Proceedings of the ACM International Workshop on Wireless Sensor Networks and Applications*, (2002), Atlanta.

[16] C. WANG ET AL., Priority based congestion control in wireless sensor networks. Presented in the *Proceedings of the IEEE International Conference on Sensor Netyworks, Ubiquitous, and Trustworthy Computing*, (2006).

[17] C. SONMEZ ET AL., Fuzzy based congestion control for wireless multimedia sensor networks. *EURASIP Journal on Wireless Communications and Networking*, **63** (2014).

[18] S. MAHDIZABEH AGHDAM ET AL., WCCP: A congestion control protocol for wireless multimedia communication in sensor networks. *Ad Hoc Networks*, **13** (2013), pp. 516–534.

[19] M. ZAREI ET AL., Fuzzy based trust estimation for congestion control in wireless sensor networks. Presented in the *Proceedings of the IEEE International Conference on Intelligent Networking and Collaborative Systems*, (2009), pp. 233–236, Barcelona.

[20] M. ZAREI ET AL., FCCTF: Fairness congestion control for a distrustful wireless sensor network using fuzzy logic. Presented in the *Proceedings of the IEEE International Conference on Hybrid Intelligent Systems*, (2010), Atlanta, GA.

[21] A. CHAKRABORTY ET AL., A trust based fuzzy algorithm for congestion control in wireless multimedia sensor networks (TFCC). Presented in the *Proceedings of the IEEE International Conference on Informatics, Electronics & Vision*, (2013), Dhaka, Bangladesh.

[22] A. CHAKRABORTY ET AL., A trust based congestion aware hybrid ant colony optimization algorithm for energy efficient routing in wireless sensor networks (TC-ACO). Presented in the *Proceedings of the IEEE International Conference on Advanced Computing*, (2013), pp. 137–142, Chennai, India.

[23] M. MOMANI, Bayesian methods for modeling and management of trust in wireless sensor networks. Ph.D Thesis. University of Technology, Sydney, 2008.

[24] A. CHAKRABORTY ET AL., An optimized lifetime enhancement scheme for data gathering in wireless sensor networks. Presented in the *Proceedings of the IEEE International Conference on Wireless Communication and Sensor Networks (WCSN)*, (2009), Allahabad, India.

Received: September, 2014
Revised: January, 2015
Accepted: February, 2015

Contact addresses:

Arpita Chakraborty
Department of Electronics
and Communication Engineering
Techno India, Salt Lake
Kolkata 700091, India
e-mail: carpi.technoindia@yahoo.com

Srinjoy Ganguly
Department of Electronics
and Telecommunication Engineering
Jadavpur University, ADES Lab
Kolkata 700032, India
e-mail: srinjoy_ganguly92@hotmail.com

Mrinal Kanti Naskar
Department of Electronics
and Telecommunication Engineering
Jadavpur University, ADES Lab
Kolkata 700032, India
e-mail: mrinalnaskar@yahoo.co.in

Anupam Karmakar
Department of Electronic Science
University of Calcutta
Kolkata 700009, India
e-mail: anupamkarmakar@yahoo.co.in

ARPITA CHAKRABORTY received the B.Sc. (Honours) degree in Physics, B. Tech. and M. Tech. degrees in Radiophysics & Electronics from the University of Calcutta, Kolkata, India, in 1985, 1989 and 1992 respectively. She worked at industry from 1992 to 2010. Currently she is working as Assistant Professor in the Department of Electronics and Communication Engineering in Techno India, Salt Lake, under West Bengal University of Technology, India. Her research interests include wireless sensor networks, mobile ad hoc networks and wireless communication system design.

SRINJOY GANGULY received the Bachelor of Electronics and Telecommunication Engineering degree from Jadavpur University, Kolkata, India, in 2014. Currently he is pursuing a Post Graduate Program in Management from India Institute of Management, Ahmedabad, expected to finish in 2016. His research interests include wireless sensor networks, engineering optimization and financial derivatives.

PROF. MRINAL KANTI NASKAR received both the B. Tech. and M. Tech. degrees from E & ECE Department, IIT, Kharagpur and the PhD degree from Jadavpur University. He served as a faculty member in RIT, Jamshedpur and REC, Durgapur from 1991–1996 and 1996–1999 respectively. Prof. M. K. Naskar is currently working as a Professor in the Department of Electronics and Telecommunication Engineering in Jadavpur University, Kolkata, India and is in charge of the Advanced Digital and Embedded Systems Lab. His research interests include mobile ad hoc networks, wireless sensor networks, optical networks and embedded systems.

DR. ANUPAM KARMAKAR received the B.Sc. (Honours) degree in Physics, B. Tech. and M. Tech. degrees in Radiophysics & Electronics from the University of Calcutta, Kolkata, India, in 1985, 1989 and 1991 respectively and the Ph.D. degree in Electronics and Telecommunication Engineering from the Jadavpur University, Kolkata, India in 2004. In 1991 he joined the Department of Electronics Engineering, National Institute of Technology, Jamshedpur, India as a Lecturer. In 2003, he joined the University of Calcutta as a Reader, where he is currently an Associate Professor in the Department of Electronic Science and served as Head of the Department from October, 2011 to September, 2013. His research interests include wireless sensor networks, electronic devices, optical and embedded networking.