International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 02 - Issue 09 || September 2017 || PP. 68-74

Reliable Aware Routing Protocol for Wireless Sensor Network Using Trusted Based Algorithm

[1]D.Sivakumar, [2]Dr. K. Selvakumar
[1] *Research Scholar, Manonmaniam Sundaranar University, Tirunelveli, India*
[1]*Assistant Professor,Kings College of Engineering, Pudukkottai, India*
[2]*Associate Professor, Annamalai University, Chidambaram, India*

Abstract: In wireless sensor network, the nodes are sensor used to monitor the surrounding location and send the data to the base station. The base station is also called as sink. The routing protocol is used to send the data from the sender node to the base station. In a large network, the sender cannot send the packet to base station directly. So, we have used the multi hop network. In the multi hop transmission of packets, the sender node sends the data through the neighbor node to the base station. In the existing system, the DSDV protocol is used to route the packet to the destination. In that case, the DSDV is not considering, whether the node is trusted node or not. Due to this reason the packet delivery ratio, energy of the node, bandwidth and throughput are degraded. In our proposed system, the TERP protocol is used to find the fitness value of the each node using the genetic algorithm. By using this fitness value trusted nodes can be identified. And also, the cuckoo algorithm is used to optimize the route based on the nodes fitness values. The experimental evaluation of this research work is concluded that the proposed work can provide efficient bandwidth and reduce the packet delivery ratio.
Keywords: trust, routing, drop ratio, sensor

I. INTRODUCTION

A wireless sensor network (WSN) is a large collection of tiny self-aware, analyzable sensor devices that can perceive environmental parameters and detecting emergency events in various different applications. The three key elements of WSN, i.e.,monitoring, computing, and communication whose combination in one sensor device provides ample number of remote sensing applications [1, 2]. Due to its vast and distinguishable applications, efficient design and implementation of WSNs [3, 4]makes it an influential area of research. In sensor network, there are three main components which are the sink, monitored events, and sensor nodes from a few to several hundreds or even more than hundreds. Due to mobility of node, routing of data becomes more challenging since stability of route is more important factor, in addition to energy, bandwidth, etc. A sensor network device consists of different components: a radio transceiver with an internal and an external antenna, a memory unit, an electronic circuit for interfacing with the sensors and a power source, and generally a lithium (Li-ion) battery which is non-renewable. A sensor node may change in size and cost, depending on the complexity and some factor such as energy, memory, computational speed, and communications bandwidth of the individual sensor nodes.

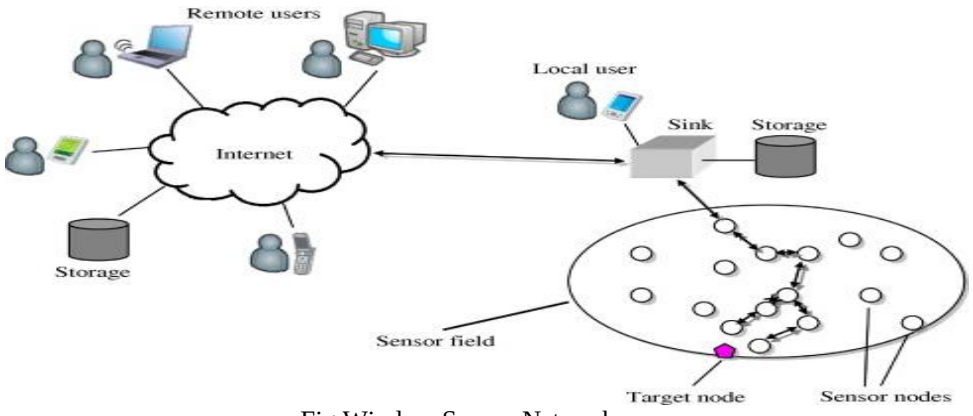

Fig Wireless Sensor Network

[TERP]There are several routing protocols that are deployed in Mobile Ad-Hoc Network and WSNs that are used for routing the packets between wireless devices. Wireless Routing protocols (WRP) are classified into three categories; proactive protocols such as DSDV, on Demand routing protocol (reactive), and Hybrid routing

(combination of proactive and on demand) [6]. On Demand routing also known as Reactive routing is one of the important protocol types that helps in reducing the wireless traffic by generating path request on demand [7]. Proactive Routing is a table driven protocol where every node maintains a table to register the next hop entry and the number of hops needed to reach the destination [8]. Hybrid protocols use the characteristics of both proactive and reactive protocols to make routing smoother and scalable. Hybrid protocols try to overcome the deficiencies of the other two classes of routing protocols [9].However, when applying such protocols many attacks could occur by malicious nodes which cause to disturb the efficient functionality of the network. As a result, in order to ensure that the network provides its services without any problem, a trust based protocol helps to resolve this issue. Based on the trust level, each node communicates with its neighbors [5]. Trust can help to sustain the stability of the network and enhance the communication process between nodes. In addition, trust can be implemented to reduce the size of the data sent from node to node and thus decrease the needed power consumption. As the trust level at each node increases, less encryption or cryptography is used. In this paper, we propose a trusted and energy efficient routing protocol (TERP). Applying the trust concept to DSDV protocol helps to increase the security level of the network as it will avoid any misbehaving actions and denying malicious nodes. Trust also can be used to increase the life of the network as it reduces the power consumption by using less encryption with the trusted nodes.

II. RELATED WORK:

[BASE PAPER] Trust based congestion aware routing in WSNs is a relatively new research topic and has not been addressed in literature to a great extent. Although a lot of energy efficient routing protocols are available, most of them do not consider network security, role of the faulty nodes and the problem of congestion in their ambit. For example, a multi path routing protocol based on dynamic clustering and ACO, is described in MRP [10], which improves the efficiency of data aggregation, thereby reducing the energy consumption. The routing protocols with trust management are described in TRANS [11] and TILSRP [12]. However all the aforementioned protocols do not address the problem of congestion. Congestion and trust both are discussed in [13-15]. In the FCC protocol [13], Zarei et al. propose a Fuzzy based trust estimation for congestion control in WSNs. FCCTF protocol [14] is basically a modification of FCC, in which the Threshold Trust Value is used for decision making. Our previous work is the TFCC protocol [15], in which traffic flow from the source to sink is optimized by implementing the Link State Routing Protocol which provides improvement in network throughput.

In [16] author proposed a dynamic trust prediction model for evaluating the trustworthiness of the nodes in MANET. The proposed model was based on the historical behaviors. By exploiting the Trust-based Source Routing (TSR) protocol, the shortest path was selected for the data packet transmission. Experimental analysis showed that the proposed prediction model increased the packet delivery ratio and reduced the average end-end delay. In [14] author suggested a secure trust-based routing protocol named Grade Trust for detecting the black hole attacks. When compared to the traditional routing protocols such as Ad hoc On-demand Distance Vector (AODV) and Fisheye State Routing (FSR), the proposed Grade Trust increased the packet delivery ratio.

In [18] author proposed a trust based routing mechanism for estimating the trust value of mobile nodes. By estimating the path with maximum path trust, the malicious nodes were prevented. For establishing a secure route, the proposed trust mechanism was integrated with the traditional optimized Link State Routing Protocol (OLSR). Simulation results proved that the proposed FPNT-OLSR produced optimal packet delivery ratio, average latency, and overhead values than the traditional OLSR. In [19] author computed the trust value of each node based on the packet forwarding capability. By exploiting the trust value, the nodes were ranked. The path with more number of trusted nodes was selected using the AODV protocol. Instead of choosing the shortest path, the proposed protocol chose the trusted path for transferring the packets. Experimental analysis proved that the proposed protocol produced minimal packet drop.

In [20] author suggested a trust based QoS model for estimating the trust degree between nodes. The suggested trust-based QoS routing algorithm created a tradeoff between trust degree and link delay. When compared to the traditional watchdog-Dynamic Source Routing (DSR) and QAODV, the proposed routing algorithm produced optimal packet delivery ratio, average end to end delay, routing packet overhead, and detection ratio of malicious nodes. In [21] author proposed a novel trust-aware geographical routing scheme for the WSN. Based on the direct, and the indirect observations, the suggested model derived the trustworthiness of each neighboring node. The experimental results proved that the suggested routing scheme achieved more than 99% of delivery ratio.

[TERP] The security of information exchanged between two nodes is a strong factor especially in military fields. SAODV is a secure routing protocol that assures the information security as well as the energy efficiency. This protocol is based on the classic AODV protocol but several mechanisms are added to deal with security issues such as AES encryption standard, digital signature mechanism, and RSA public-key encryption [14]. In

addition, many papers have discussed the importance of SAODV protocol and provided some enhancements. In [15], author has enhanced the existing SAODV protocol to deal with serious attacks from malicious nodes that are already have been authenticated by the network. This protocol is called SAODV-SDDO. In order to detect these malicious nodes, a cryptographic mechanism and a reactive approach have been used. he basically added Intrusion Detection Mechanism (IDM) and Trust Based Mechanism (TBM) to the SAODV protocol [15].

III. PROPOSED WORK

3.1 Fitness Value:

In this research work modified genetic algorithm is used for cluster head selection. In the field of artificial intelligence, a genetic algorithm (GA) is a search heuristic that mimics the process of natural selection. This heuristic (also sometimes called a metaheuristic) is routinely used to generate useful solutions to optimization and search problems. Genetic algorithms belong to the larger class of evolutionary algorithms (EA), which generate solutions to optimization problems using techniques inspired by natural evolution, such as inheritance, mutation, selection and crossover. In genetic algorithms, crossover is a genetic operator used to vary the programming of a chromosome or chromosomes from one generation to the next. It is analogous to reproduction and biological crossover, upon which genetic algorithms are based. Cross over is a process of taking more than one parent solutions and producing a child solution from them. The traditional genetic algorithm is modified in its cross over operation by introducing the k-point crossover.

3.1.1 FITNESS FUNCTION

The fitness value that is considered in this work for the optimal cluster head selection is the energy consumption. Network's current energy in k-th round is shown with EK Network. Fitness function is computed through equation that should become minimum.

$$\text{Fitness} = \left| E^{K}_{\text{Network}} - E^{K-1}_{\text{Network}} \right|$$

3.1.2 REPRODUCTION OPERATOR

Reproduction is usually the first operator applied on population. The reproduction operator selects at random a pair of two individual strings for mating.

3.1.3 CROSS OVER OPERATOR

Cross over is a recombination operator. A cross-site is selected at random along the string length and the position values are swapped between two strings. The general cross over is extended to k-point crossover, where k crossover points are Crossover is generally performed to exchange the genetic material of two parents to produce new chromosomes. A crossover point is taken for which new population is generated. The point at which crossover is performed is depend on randomly selected crossover point. The number of crossover is calculated by the crossover rate which is generally 2-5%. The concept of crossover can be considered.

3.1.4 MUTATION OPERATOR

After cross over, the strings are subjected to mutation. Mutation of a bit involves flipping it, changing 0 to 1 and vice versa with a small mutation probability. After mutation, a bit that was "0" changes to "1". It‟s possible that a regular node becomes cluster head and a cluster head becomes a regular node. After cross over operator, mutation happens in a way that a mutation may be created in a bit of one or some chromosomes. Finally, after crossover and mutation, base station selects the chromosome which has the networks least energy difference in proportion to the previous round and introduces the available nodes to network as cluster head and other nodes join to the nearest cluster head. Cluster head selection based on energy, density and centrality using GA.

The following algorithm shows the stages of the proposed algorithm:

Step-1: Initial network.

Step-2: Each node sends the position of itself in the network t o its neighbors.

Step-3: In BS using genetic algorithm based on energy, density and centrality, cluster heads are determined.

Step-4: Cluster heads are introduced to all nodes in network.

Step-5: Each sensor node will join to the nearest CH.

Step-6: Each sensor node transmits data to the CH with a multiple-hop transmission.

Step-7: After all data has been received, aggregate all data‟s of CHs using HYMN then transmit it to the BS through single hop transmission.

3.2 TRUST BASED ROUTING SCHEME

In this work, we have presented a novel trust based congestion aware energy efficient routing scheme for WSNs in which the cuckoo search algorithm is utilized to maximize the network lifetime. We consider random deployment of sensor nodes in the sensor field under free space propagation. The proposed algorithm works in two stages. In stage 1, the trust values and the congestion statuses of the nodes are calculated and thereby, the trust-congestion metric is formed. In stage 2, the cuckoo search algorithm, which utilizes the trust-

congestion metric and the distance metric, is implemented for data packet routing from source node to base station. The detailed operation of each stage is described below.

3.2.1 STAGE 1

In the proposed algorithm, stage 1 detects the mishaviour of the sensor nodes using the concept of trust. The trusted nodes are identified and congestion status are computed accordingly. The malicious nodes having trust value below the threshold level are not considered for data packet routing, due to which the congestion metric isn't computed for such nodes. This causes a reduction in the computation overhead and thereby enhances battery life time. The trust value of node i upon node j is calculated on the basis of three commonly used trust metrics namely, remaining node energy (Ne'), packet transmission ratio (PTR') and packet latency ratio (PL'). Mathematically, the net trust of node i upon node j is calculated by the formula represented as **:**

$$T_{ij} = \frac{A_1 * N_e^{'} + A_2 * P_{TR}^{'} + A_3 * P_L^{'}}{A_1 + A_2 + A_3} \quad (1)$$

where A1, A2 and A3 are the corresponding weights used for Ne'.

The congestion level of a valid node is estimated with the help of the parameter known as the Congestion Index. It is assumed that each node maintains a queue for storing data packets in its buffer. As packets are transmitted from a particular node serially towards the next node, buffer space is cleared and the packets waiting in the queue go to the empty buffer space of the node. When the packet received rate of the node is greater than the packet transmission rate, queue length increases, buffer overflows, congestion level of the node increases. If a node is not able to clear the data packet in its queue, then it waits for a certain number of pre-defined cycles (say, WCmax) and holds the packets in each cycle until the packets are finally dropped (at the end of WCmax cycles). The Congestion Index of the kth node is computed by the equation given as**:**

$$CI_k = \frac{\bar{r}_{in}^{k} + Q^k(c-1) - \bar{r}_{out}^{k}}{\bar{r}_{in}^{k} + Q^k(c-1)} \quad (2)$$

where $Q^k(c-1)$ is the empty space left in the queue of the kth node till (c-1)th cycle.

The Trust Congestion Metric (TCM) of each trusted nodes, also called as the valid node, is computed by the equation**:**

$$TC_{ij} = \alpha * CI_j + (1-\alpha) * T_{ij} \quad (3)$$

where node *i* and node *j* are considered as the source node and the destination node, respectively. CIj is the Congestion Index of the destination node and Tij is the trust value of source node i upon the destination node j. The constant α is denoted as Trust Congestion Coefficient which belongs to [0,1].

3.2.2 STAGE 2

In stage 2, the data routing protocol using cuckoo search algorithm is implemented. The Cuckoo search algorithm (CSA) is a meta-heuristic optimization algorithm to solve the problem and provides an optimal solution. The CSA was inspired by the breeding behavior of some cuckoo species for their re-production process. The cuckoo species lay their eggs in the nests of host birds, after evaluating the host bird's nest. The evaluation is carried over based on the colors and patterns of the eggs of a few chosen host species. This reduces the probability of the eggs being abandoned and, therefore, increases their re-productivity parasitic cuckoos often choose a nest where the host bird just laid its own eggs. The cuckoo eggs hatch slightly earlier than their host eggs. When the first cuckoo chick is hatched, his first instinct action is to evict the host eggs by blindly propelling the eggs out of the nest. This action results in increasing the cuckoo chick's share of food provided by its host bird. The CSA models can be applied to various optimization problems. The detailed clarification of route selection process is offered in subsections.

Initialization

At first, number of solutions or nests is randomly generated in the initialization process. The initialization process of nest is illustrated in table 3. Here, "0" and "1" are randomly initialized for each nest. N

Fitness selection

The selection of the fitness is a crucial aspect in cuckoo search algorithm. It is used to evaluate the aptitude (goodness) of candidate solutions. Here, minimum distance is selected as the best fitness to find the optimal route. To evaluate an individual, an objective function (i.e., fitness function) is applied that considers the shortest path from the source to the destination as the best one. In other words, the fitness fi of the individual 'i' is the sum of the distance (dis) between each two adjacent nodes 'nj' and 'nj+1' in the path from the source node 's' to the destination node 'd', calculated by the following formula:

$$\text{Fitness}\left(\text{nest}_n^k\right) = \sum_{j=s}^{d} \text{dis}\,(n_j, n_{j+1}) \quad (4)$$

In our proposed research methodology trust congestion metric is taken as fitness function. Cuckoo Search Algorithm is as follows:

ALGORITHM

Input: Trust Threshold Level, Trust Congestion Metric

Output: Optimal Route

Objective function: f (X), X = (x_1, x_2,…,x_d)

Generate an initial population of n host nests;

While (t < MaxGeneration) or (stop criterion)

Get a cuckoo randomly (say, i) and replace its solution by performing Lévy flights;

Evaluate its quality/fitness Fi

[For maximization, $F_i \propto f(x_j)$];

Choose a nest among n (say, j) randomly;

if ($F_i > F_j$) ,

Replace j by the new solution;

end if

A fraction (Pa) of the worse nests are abandoned and new ones are built;

Keep the best solutions/nests;

Rank the solutions/nests and find the current best;

Pass the current best solutions to the next generation;

end while

New solution generation using Levy flight

To generate novel solution, levy flight method is applied at this point. It is a type of random walk. It will arbitrarily search for length to produce novel solution which has a heavy-tailed distribution. Levy flight has a huge coverage range in search space.

Both, original and adapted codes employ random step sizes. We employ different function set for computing this step size compared to the original code. In the original code, step size is computed by subsequent code expression:

$$\text{Stepsize} = 0.01 * \frac{u}{|v|^{1/\beta}} \oplus (S_i^t - S_{best}) \qquad (5)$$

Where,

0.01 → a factor for controlling step size of cuckoo walks/flights,

S_i^t → is current solution i of iteration t

S_{best} → is the global best solution

Stepsize → is the length of walk step

⊕ → is entry-wise product

U and v → are random value

β → Levy distribution parameter

From the above defined algorithm, better route establishment can be done effectively with the satisfaction of the research objectives namely energy, trust, reliability, trust and so on. After successful establishment of route paths, packets would be forwarded where there may be chance of the packet corruption/loss due to run time attacks such as worm hole attack. The protection of network from the worm hole attacks are discussed detailed in the following section.

I. EXPERIMENTAL RESULTS

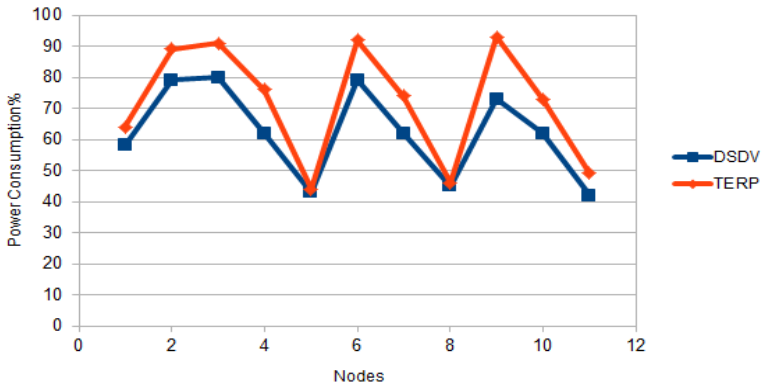

Figure: Power Consumption

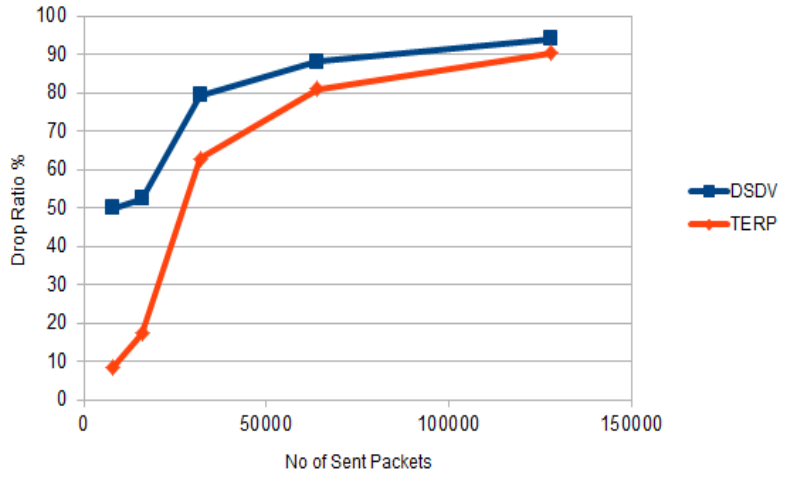

Figure: Drop Ratio

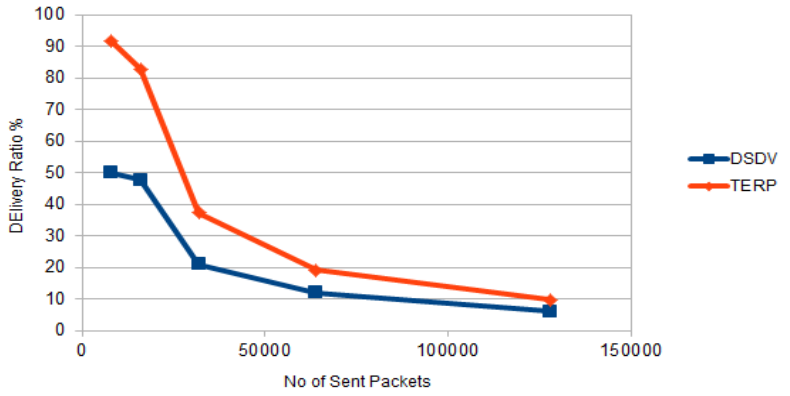

Figure: Delivery Ratio

CONCLUSION

In this paper, the TERP protocol is used for find the trusted node and the cuckoo search algorithm is used to find the optimized path from sender to base station. With help of the optimization techniques, the result shows that the packet drop ration is drastically reduced and increase the packet delivery ratio. In future, the security mechanism can be added to find the malicious nodes.

References

[1]. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks.IEEE Commun. Mag. 40(8), 102–114 (2002)
[2]. Puccinelli, D., Haenggi, M.: Wireless sensor networks: applications and challenges of ubiquitous sensing. IEEE Circ. Syst. Mag. 5(3), 19–31 (2005)
[3]. Hac, A.: Wireless Sensor Network Designs. Wiley, New York (2003)
[4]. Raghavendra, C., Sivalingam, K.M., Znati, T.: Wireless Sensor Networks. Springer, Berlin (2006)
[5]. Pushpa, A.M., "Trust based secure routing in AODV routing protocol,"*Internet Multimedia Services Architecture and Applications (IMSAA),2009 IEEE International Conference on* , vol., no., pp.1,6, 9-11 Dec.2009.
[6]. Pandey, A. K., & Fujinoki, H. (2005). Study of MANET routing protocols by GloMoSim simulator. *International Journal of Network Management , 15*, 393-410.
[7]. Koliousis, A., & Sventek, j. (n.d.). Proactive vs Reactive Routing for Wireless Sensor Network. 7-8.
[8]. Tyagi, S. S., & Chauhan, R. K. (2010). Performance Analysis of Proactive and Reactive Routning Protocol for Ad hoc Networkds.*International Journal of Computer Applications , 1*, 27-28.
[9]. Sharma, m., & Singh, G. (2011). Evaluation of proactive, Reactive and Hybrid Adhoc Routing. *International Journal of Smart Sensors andAd Hoc Networks , 1* (2), 65-66

[10]. Jing Yang, Mai Xu, Wei Zhao and Baogue Xu, " A Multipath Routing Protocol Based on Clustering and Ant Colony
[11]. Optimization for Wireless Sensor Networks", Sensors ISSN 1424-8220, 10,4521-4540, doi : 10.3390/s 100504521'
[12]. 2010.
[13]. S. Tanachaiwiwat, P. Dave, R. Bhindwale and A. Heimy, "Location-centric Isolation of Misbehavior and Trust Routing
[14]. in Energy Constrained Sensor Netwoks", IEEE International Conference on Performance Computing and
[15]. Communications, 2004.
[16]. Raha, M.K. Naskar, S.S. Babu, Omar Alfandi, and D. Hogrefe, " Trust Integrated Link State Routing Protocol for Wireless Sensor Network (TILSRP), proceedings of 5th IEEE ANTS, Dec 2011.
[17]. Mani Zarei, Amir Msoud Rahmani, Avesta Sasan, Mohammad Teshnehlab, "Fuzzy based trust estimation for congestion control in wireless sensor networks", 2009 International Conference on Intelligent Networking and Collaborative Systems.
[18]. Mani Zarei, Amir Msoud Rahmani, Razieh Farazkish, Sara Zahirnia,"FCCTF: Fairness Congestion Control for a distrustful wireless sensor network using Fuzzy logic", 2010 10th International Conference on Hybrid Intelligent Systems.
[19]. A.Chakraborty, S.Ganguly, M.K.Naskar, A.Karmakar, "A Trust Based Fuzzy Algorithm for Congestion Control in Wireless Multimedia Sensor Networks (TFCC)", proceeding of 2nd International Conference, ICIEV , Dhaka, Bangladesh, 2013.
[20]. Xia H, Jia Z, Li X, Ju L & Sha EHM 2013, 'Trust prediction and trust-based source routing in mobile ad hoc networks', Ad Hoc Networks, vol. 11,no. 7, pp. 2096-2114.
[21]. Airehrour D, Gutierrez J & Ray SK 2015, 'GradeTrust: A secure trust based routing protocol for MANETs', International Conference on Telecommunication Networks and Applications Conference (ITNAC), pp. 65-70.
[22]. Tan S, Li X & Dong Q 2015, 'Trust based routing mechanism for securing OSLR-based MANET', Ad Hoc Networks, vol. 30, pp. 84-98.
[23]. Bar RK, Mandal JK & Singh MM 2013, 'QoS of MANet Through Trust based AODV Routing Protocol by Exclusion of Black Hole Attack', Procedia Technology, vol. 10, pp. 530-537.
[24]. Wang B, Chen X & Chang W 2014, 'A light-weight trust-based QoS routing algorithm for ad hoc networks', Pervasive and Mobile Computing, vol. 13, pp. 164-180.
[25]. Zahariadis T, Trakadas P, Leligou HC, Maniatis S & Karkazis P 2013, 'A novel trust-aware geographical routing scheme for wireless sensor networks', Wireless personal communications, vol. 69,no. 2, pp. 805-826.