European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 09, 2020

SECURED RELAY SELECTION AND CONGESTION AWARE ROUTING FOR MANET'S

[1]Dr. A. Karthikayen, [2]M. Ayyadurai, [3]S. Lekashri [4]Dr. M. Venkatesan,

[1]Professor, Visvodaya Engineering College, AP

[2]Assistant Professor, Saveetha School of Engineering

[3]Assistant Professor, Kings Engineering College, TN

[4]Professor, Visvodaya Engineering College, AP

Abstract

Due to decentralised architecture the nodes present in mobile ad-hoc networks nodes can able to move freely in the environment. Hence the nodes are characterised as self organised and self healing. Due to rapid movement of nodes link failures exists frequently between the nodes and if two nodes present in the range of communication, then the sensed data is passed directly to the sink node. To identify an efficient and concurrent bandwidth and trustable path between sending and receiving nodes; the communication link weight and node trust score factors are examined. The weight of the links is calculated by estimating longer link connectivity period and the bandwidth channel availability. Once the trust ratio for the nodes is evaluated through ratings then efficient bandwidth nodes are selected. Therefore the data is passed through the trusted node with high channel bandwidth towards the gateway.

Keywords: Trust factor; Node Ratings; Longer Link connectivity; Bandwidth utility; MANET.

1. Introduction

In Mobile Ad-hoc Network (MANET), the nodes present in the network have ability to move with their mobility factors. Range of communication that the node can communicate is based on the communication area either it can be processed through single-hop or multi-hop communication area. With the help of assistant nodes the data packets is carried out to the destination in multi-hop communication [1]. Scalability in MANET shows the network quality in spite of specifying the node capability therefore the sensed information delivery process is done successfully with energy efficient metric [2]. Also swarm intelligence techniques are used for the current communication path and establish their routes using enhanced dynamic source routing [3]. The node position is upgraded using link scheduling procedure; a relative transmission is obtained by tracing the nodes [4].

Transmitting nodes are selected with minimum number of adjacent node to progress the data transmission in the direction of the shortest path [5]. Increasing in node density is directly proportional to the broadcasting failures, hence many recipients might experience from quality deficiencies [6]. Therefore numerous error rectification methodologies were also implemented for reducing retransmission rate with the requirement of error rectification techniques [7]. If receiver finds any kind of failure in received packets then it expects source to resend the data therefore this process consumes extra bandwidth [8] and some other network parameters like energy, memory, etc.

2. Related Works

Several trust based and traffic aware routing protocols were proposed and some of the mechanism is discussed here. To achieve load balancing, multipath routing methods have been

proposed in [9]. Multipath routing method helps in distributing the traffic load in all possible routing paths thereby reduces traffic congestion in the network a particular path. Hence, routing in multipath simultaneously increases the route maintenance during reliable transmissions and end-to-end delay will be reduced [10]. Location-based method of routing reduces the route maintenance cost between the active paths. Reliable communication carried out within the communication area was discussed in Zone Routing Protocol (ZRP) [11].

Forecast Function based Congestion Control in MANET Routing (FFCC) was proposed in [12], here congestion rate is applied for measuring the highest congested node and isolates that node from the routing path. In general multipath routing methods are dependable on adjacent nodes to detect minimum hop-count path which avoids the data packets from the network traffic. Adjacent nodes may have transmission delay during broadcasting of data to other nodes when congestion occurs due to overload. Therefore to reduce optimization problem Link Disjoint Multipath (LDM) routing scheme was proposed [13].

Providing security measures for the protected communication between mobile nodes in a hostile environment is mandate. Contrasting to wired networks, the unique characteristics of MANET's pose several numbers of challenges during security design, like data sharing medium, freely accessible peer-to-peer network design, severe resource parameters and highly dynamic structure [14]. In most reputation based schemes, each node relies on overhearing to monitor the packet forwarding status of neighbouring nodes. Forwarder's evaluates the reputation levels according to the monitoring results [15].

However building trust level in the network consumes large energy therefore watchdog mechanism is applied for energy optimization [16]. At the same time, monitoring node may disseminate these reputation levels to help peers to obtain further trust information about the network. Later the nodes can translate these collected reputation levels into a usable trust metric through an abstract mathematical specification. Finally, each node will use these trust values to distinguish malicious and benign nodes.

Evolutionary Self Cooperative Trust (ESCT) scheme was proposed [17] to prevent a variety of routing interruption attacks that imitates human cognitive process and relies on trust-level information. Mobile nodes exchange their trust information and analyze the trust information received based on their own cognitive judgment. Each node presented here dynamically evolves its cognition for excluding malicious entities. The system cannot be easily compromised even in the presence of internal attackers is the most prominent feature of ESCT.

3. Proposed Scheme: SRSCAR

In order to deliver the packets securely and efficiently without congestion a scheme named Secured Relay Selection and Congestion Aware Routing (SRSCAR) is proposed. The trusted nodes are selected based on the node rating then channel availability and link connectivity are determined for the selected trust nodes which moves towards the destination. The nodes with minimum channel interference and good link connectivity with one another are selected as bandwidth efficient nodes.

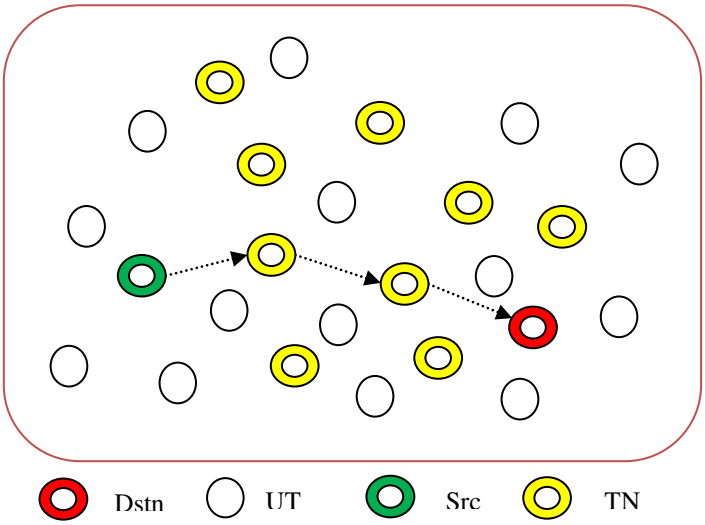

Figure 1: Example Scenario of SRSCAR

The mobility model for the MANET architecture is usually done with random waypoint that describes the nodes movement pattern in easier terms and provides accurate information by tracing the mobility model of the nodes. Figure 1 shows the example scenario for SRSCAR scheme. Here Trust Nodes (TN) is selected from the Un-trustable Nodes (UN) at first then link connectivity and channel rates are determined for the selected trust relay nodes.

a. Selection of trustable relay nodes on basis of mobility direction

The trustable nodes are selected in the basis of ratings that are participated in the node challenge contest. Nodes that have successfully completed the challenge contest are added in the relay node list. Based on the rating level the nodes are selected for the transmission. A node that does not complete the challenge (i.e. not processing the route reply request) is kept under the low rating level and will not selected for routing. A node rating is fall under the range between zeros and five. Therefore the node's with high rating comparatively higher than the average rating that falls greater than 3.5 rating nodes is selected for further process. Therefore high rating nodes are taken as trustable nodes and from these higher bandwidth nodes are selected for data transmission.

Algorithm for NR detection

Input: Passage of Cntrl_msg to neighbour nodes
Output: Detection of trustable nodes on basis of ratings
Begin
Set 'n' nodes
Broadcast Rq
Calculate NR
if NR > 3.5
    Node added to trusted relay node list
else
    Fall under un-trustable node category
End

Node Ratings (NR) for the nodes are calculated through the control messages such as route request (Rq) and route reply (Rp) that is passed among the nodes present within the communication system. Depending upon the variations in count of Rq and Rp passed to the particular node and received from that particular node NR can be measured. The NR for the node is calculated by equation 1 and 2.

$$NR = \left(\frac{\{Rq - Rp'\}}{Rq} \right) * 100 \tag{1}$$

Where Rq represents successfully sent route request and Rp' represents unsent route replies for the received request.

$$Rp' = 1 - Rp \tag{2}$$

Where Rp denotes successfully replied for the request received.

b. Evaluation of node connecting utility factor

After selecting the trustable nodes with their ratings node connecting utility factor is determined through the evaluation of available channel to pass the sensed data through the relay nodes. The control packets passed between the nodes is used to estimate the available bandwidth between the nodes. Scheduling the packets as per the available bandwidth makes the network congestion free and the data can be delivered efficiently without any losses. Long time link connectivity and bandwidth availability is measured through the hello scheme (control packets) and it is given in equation 3 and 4.

$$Bw(n) = \left(\frac{\sum_{(n_i, n_j)}^{data\_rate} \{\omega(n), \theta\}}{T_\tau} \right) \tag{3}$$

Here Bw(n) is the bandwidth measurement, ω(n) represents node's own sensed data rate and θ denotes channel overheads. The moving nodes that are connected among them for a longer period of time have been estimated through the reference value of link connectivity. The reference value of the link duration is set by evaluating the outage probability of moving nodes. Outage probability is said to be the least connected nodes with less data rate i.e. the nodes that are presented too far to communicate and not in the range of communication and it is measured using equation 5.

$$LC_{long} = t0 + t1 + T \tag{4}$$

$$L_{(outage)} = 1 - t0 \| T \tag{5}$$

Probability of link availability prediction can be obtained by taking the communication range exists between the adjacent nodes in the path. Source node 'S_i' selects the intermediate node 'A_i' with their distance metric (p, q) present in their communication range towards the sink node (C_R) and is shown in equation 6.

$$P\left((S_p, S_q) < A_i\right) = P\left(nodes\ in\ C_R\right) \tag{6}$$

Therefore the channel intrusion or congestion caused due to high data traffic can be greatly reduced by choosing large channel bandwidth and high link connectivity nodes for transmission. Figure 2 describes about the flowchart of the proposed scheme.

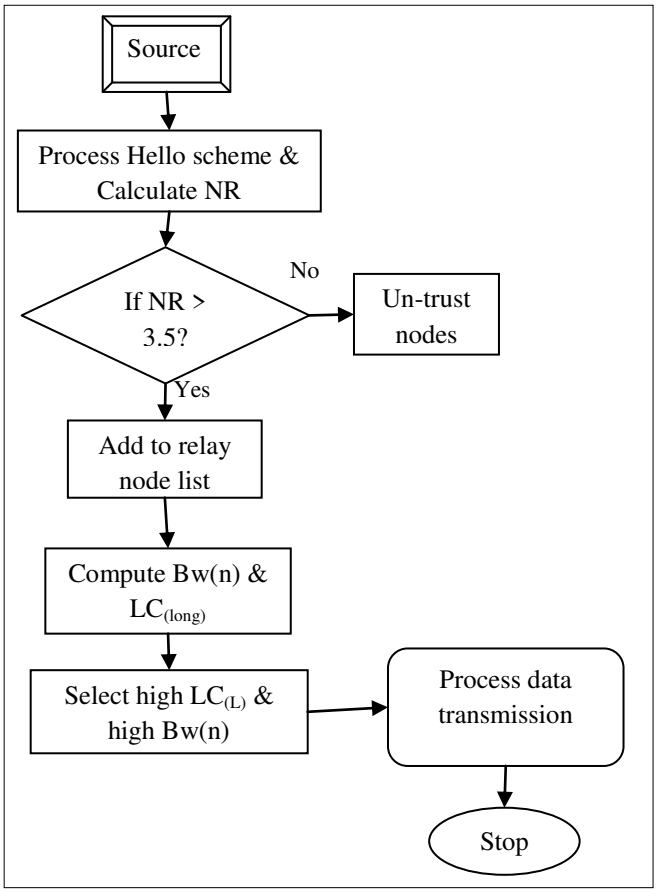

Figure 2: Flowchart of SRSCAR

4. Results and Discussion

The simulation analysis is carried for the analysis of efficiency for the proposed mechanism using simulation tool called Network Simulator version 2. It is possible to examine the events in a network scenario discreetly.

To assess the network performance we evaluate the packet delivery rate, packet loss rate, delay and false positive ratio metrics of the network before and after adopting the proposed scheme. The simulation parameters for performance analysis are listed in Table 1.

Table 1: Simulation Metrics

Parameters	Value
Traffic model	Constant Bit Rate
Simulation Area	600 x 600m, 600 x 600m
Transmission range	250mts
Antenna Type	Omni antenna

Mobility Model	Random Way Point
Network Interface Type	WirelessPhy
Channel Type	Wireless channel

(a) Packet Received Rate

Packet Received Rate (PRR) is defined as the amount of packets that delivered at the receiver end with respect to the total amount of sent packets from source. PRR is measured using equation 7.

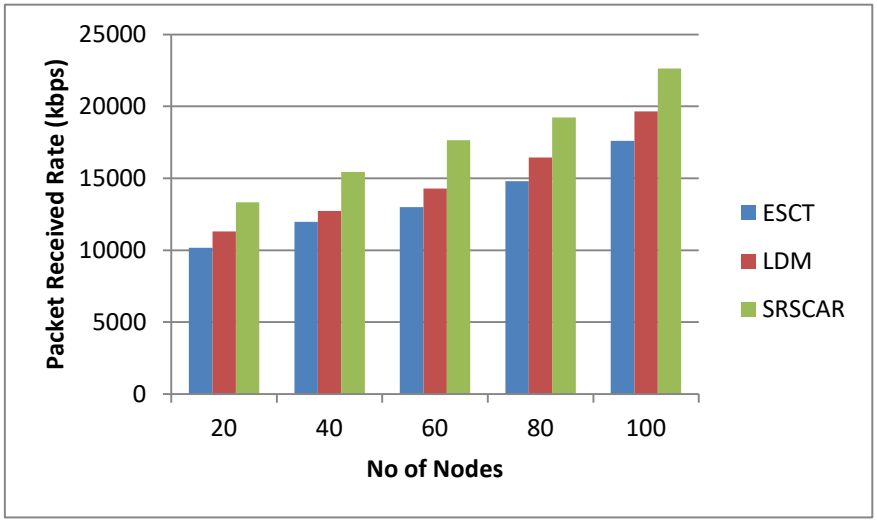

Figure 3: PRR

$$PRR = \frac{Pkts\ dlvrd\ Rate}{Pkts\ sent\ Rate} \quad (7)$$

From the figure 3, it is clear that the PRR of the proposed scheme SRSCAR is greater than both conventional protocols such as ESCT and LDM. The increase in the number of nodes simultaneously increases the PRR values at the destination, which proves the efficiency of the proposed technique.

(b) Transmission Overhead

The transmission overhead is determined for the proposed scheme SRSCAR and the conventional schemes. Proposed scheme have the minimum overhead value when compared to the existing schemes of ESCT and LDM which is demonstrated in figure 4. Minimum overheads during transmission is obtained because the proposed scheme SRSCAR develops the routing with minimum hop count results in selection of shortest path, when latest routing path is included in the network then this will leads to additional transmission overhead.

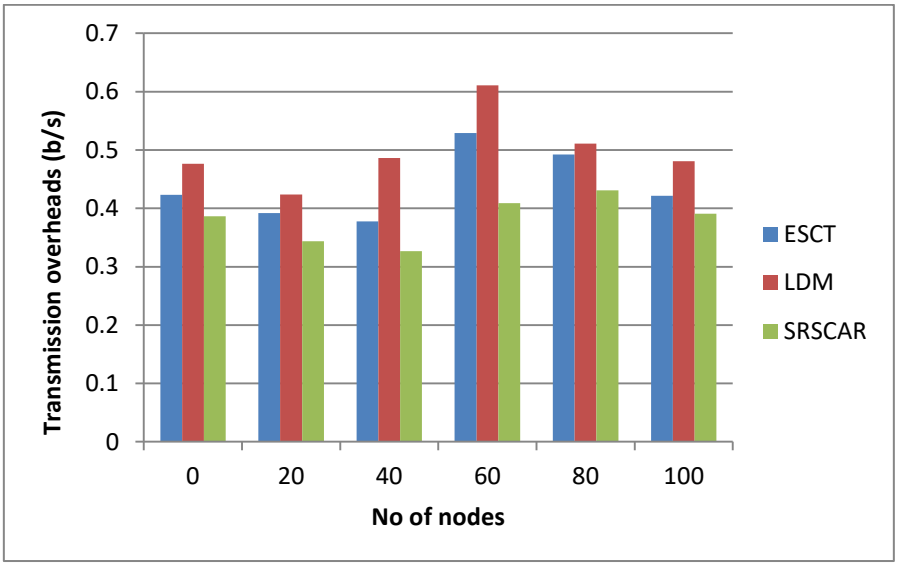

Figure 4: Transmission Overheads

(c) End to End Delay

The end to end delay is estimated as the difference in a packet sent time and receiving times for all nodes as in equation 8. The values obtained are the end to end delay values for a presented node density in the network.

$$Delay = \frac{\sum_{0}^{n}(Pkt\ Rcvd\ Time - Pkt\ Sent\ Time)}{n} \tag{8}$$

The figure 5 shows the difference in the end to end delay values for SRSCAR, LDM and ESCT schemes in a 100 number of node density scenario. Proposed SRSCAR scheme has lower delay values and proves that it consumes lesser time for the transmission compared to ESCT and LDM schemes.

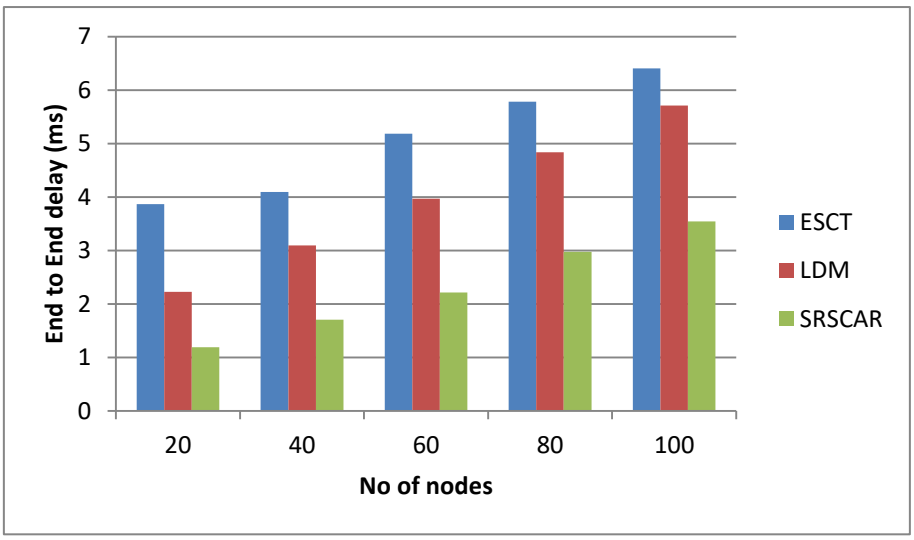

Figure 5: End to End Delay

(d) Traffic Load Distribution

In this proposed network setting, the trusted and bandwidth efficient adjacent node takeover the system state and tag on all the system metrics frequently for the data transmission while routing. In addition, with all system constraints, the scheme SRSCAR is capable of reducing energy expiration rate for all the nodes and frequently forwards the data packets to minimize the network traffic and it is the major intention of this proposed scheme.

Figure 6 shows the traffic load distribution for both the proposed SRSCAR scheme and existing ECST and LDM schemes. SRSCAR scheme has better load distribution compared to other schemes.

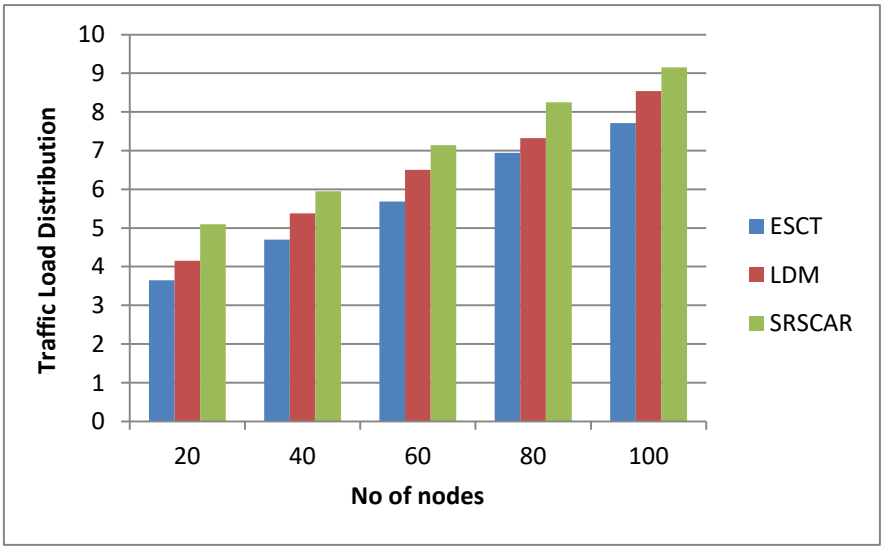

Figure 6: Traffic Load Distribution

5. Conclusion

To deliver the sensed information securely and efficiently without congestion Secured Relay Selection and Congestion Aware Routing scheme is proposed. Here, the trusted nodes are chosen on basis of node rating then channel availability and link connectivity are determined for the selected trust nodes which move towards the destination. The nodes with minimum channel intrusion and high link period of connectivity are selected as bandwidth efficient nodes. Therefore passing the data in larger bandwidth nodes greatly supports path traffic and reduces network congestion rate. Simulation results show that SRSCAR scheme has better consequences in terms of data rates delivered and load distribution over the network.

References

1. Basurra, S. S., De Vos, M., Padget, J., Ji, Y., Lewis, T., & Armour, S. (2015). Energy efficient zone based routing protocol for MANETs. Ad Hoc Networks, 25, 16-37.
2. Cheng, B., & Hancke, G. (2016, October). Energy efficient scalable video manycast in wireless ad-hoc networks. In IECON 2016-42nd Annual Conference of the IEEE Industrial Electronics Society (pp. 6216-6221). IEEE.
3. Chatterjee, S., & Das, S. (2015). Ant colony optimization based enhanced dynamic source routing algorithm for mobile Ad-hoc network. Information Sciences, 295, 67-90.

4. Abdulwahid, H., Dai, B., Huang, B., & Chen, Z. (2016). Scheduled-links multicast routing protocol in MANETs. Journal of Network and Computer Applications, 63, 56-67.
5. Ghahremani, S., & Ghanbari, M. (2017). Error resilient video transmission in ad hoc networks using layered and multiple description coding. Multimedia Tools and Applications, 76(6), 9033-9049.
6. Islam, S. N. (2016). Achievable rate and error performance of an amplify and forward multi-way relay network in the presence of imperfect channel estimation. IET communications, 10(3), 272-282.
7. Jose, J., & Sameer, S. M. (2015, February). A new unequal error protection technique for scalable video transmission over multimedia wireless networks. In 2015 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES) (pp. 1-5). IEEE.
8. Periyasamy, P., & Karthikeyan, E. (2017). End-to-end link reliable energy efficient multipath routing for mobile ad hoc networks. Wireless Personal Communications, 92(3), 825-841.
9. Wu, J., Yuen, C., Wang, M., & Chen, J. (2015). Content-aware concurrent multipath transfer for high-definition video streaming over heterogeneous wireless networks. IEEE Transactions on Parallel and Distributed Systems, 27(3), 710-723.
10. Periyasamy, P., & Karthikeyan, E. (2014). Energy optimized ad hoc on-demand multipath routing protocol for mobile ad hoc networks. International Journal of Intelligent Systems and Applications, 6(11), 36.
11. Minh, T. P. T., Nguyen, T. T., & Kim, D. S. (2015, September). Location aided zone routing protocol in mobile Ad Hoc Networks. In 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA) (pp. 1-4). IEEE.
12. Suresh, G., Kumar, S., Kavitha, V., & Lekashri, S. (2020, September). Forecast Function Based Congestion Control in MANET Routing. In IOP Conference Series: Materials Science and Engineering (Vol. 925, No. 1, p. 012074). IOP Publishing.
13. Robinson, Y. H., Julie, E. G., Saravanan, K., Kumar, R., Abdel-Basset, M., & Thong, P. H. (2019). Link-disjoint multipath routing for network traffic overload handling in mobile ad-hoc networks. IEEE Access, 7, 143312-143323.
14. Kumar, A. S., & Logashanmugam, E. (2014, July). To enhance security scheme for MANET using HMAC. In Second International Conference on Current Trends In Engineering and Technology-ICCTET 2014 (pp. 467-471). IEEE.
15. Gong, W., You, Z., Chen, D., Zhao, X., Gu, M., & Lam, K. Y. (2010). Trust based routing for misbehavior detection in ad hoc networks. Journal of Networks, 5(5), 551.
16. Zhou, P., Jiang, S., Irissappane, A., Zhang, J., Zhou, J., & Teo, J. C. M. (2015). Toward energy-efficient trust system through watchdog optimization for WSNs. IEEE Transactions on Information Forensics and Security, 10(3), 613-625.
17. Cai, R. J., Li, X. J., & Chong, P. H. J. (2018). An evolutionary self-cooperative trust scheme against routing disruptions in MANETs. IEEE transactions on Mobile Computing, 18(1), 42-55.
18. Kumar A, Senthil & Logashanmugam,. (2017). Article Secured Optimal Routing Based on Trust and Energy Model in Wireless Sensor Networks. IIOAB Journal. 9. 3-13. 10.17485/ijst/2016/v9i40/96063.
19. G. Suresh and A. Senthil Kumar, "Secure Transmission Using Bivariate Principle System for WSN", Helix, vol. 10, no. 03, pp. 47-51, Jul. 2020.
20. Dr. A. Senthil Kumar, Dr. G. Suresh, Dr. R. Dinesh Kumar. (2020). Reputation based Routing for Data Transmission (RRDT) scheme for Mobile Ad Hoc Networks. International Journal of Advanced Science and Technology, 29(7), 1001 - 1006.
21. Kumar, A. S., & Logashanmugam, E. (2016). Secure Acknowledgement based Misbehavior Detection in WSN (S-ACK). Indian Journal of Science and Technology, 9(40), 96063.