ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

FLC based Wireless Sensor Routing with Trust Mechanism

Anju[1] , Er.Manwinder Singh[2]

M.Tech Student, Department of Electronics and Communication Engineering, Rayat Institute Of Engineering and Information Technology, Railmajra, Punjab, India.[1]

Associate Professor, Department of Electronics and Communication Engineering, Rayat Institute Of Engineering and Information Technology, Railmajra, Punjab, India.[2]

ABSTRACT: The WSNs are the popular wireless networks used for the purpose of data collection from the real-life scenarios. The popular applications of WSNs are healthcare, pollution monitoring, water quality or level monitoring, snow & avalanche monitoring, defense applications, etc. The routing mechanisms play the significant role in the case of WSN connectivity, where the link failure is the major problems. The low computational powered and low memory nodes are also equipped with smaller batteries. There are several attacks such as blackholes, connectivity holes, etc, which causes the data drops. In order to overcome such attacks, the WSN routing protocols must be made capable of automatically identifying the node failures caused by such attacks, and to recompute the paths between the affected nodes. In this paper, the FLC based routing mechanism coupled with Dijikstra Routing algorithm to provide the vital and vigorous connectivity around the blackhole nodes. The performance of the proposed model has been evaluated in the form of end-to-end delay and packet delivery ratio, which is compared to the existing model. The proposed model has outperformed the existing models on the basis of both of the parameters. The proposed model outperforms the existing model on the basis of end-to-end delay. The existing model is observed between 0.01 and 0.085 seconds, which is outperformed by the proposed model (0.00014 and 0.0015 seconds). Additionally, the existing model is outperformed by proposed model in the terms of PDR with average value 99.19% (proposed) against 98.93% (existing).

KEYWORDS: Fuzzy logic controller, Fuzzy routing, WSN, WSN Routing.

I. INTRODUCTION

Wireless Sensor Networks are those networks in which communication is carried out through a wireless channel. [1] In a wide area there are multiple users say as an example: mobile users. Numbers of towers in area act as sensors are called as nodes in wireless sensor networks. Thus from one node to other, communication is carried out without any physical link. [1-2] Wireless sensor networks are formed by small devices communicating over wireless links without using a fixed networked infrastructure. Because of limited transmission range, communication between any two devices requires collaborating intermediate forwarding network nodes, i.e. devices act as routers and end systems at the same time. [3] A network consists of numbers of nodes with one as a source and one as a destination. One of the advantages of wireless sensor networks is their ability to operate unattended in harsh environment in which manually human monitoring schemes are inefficient and risky.[6] Communication between any two nodes may be trivially based on simply flooding the entire network. However, more elaborate routing algorithms are essential for the applicability of such wireless networks, since energy has to be conserved in low powered devices and wireless communication always leads to increased energy consumption.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

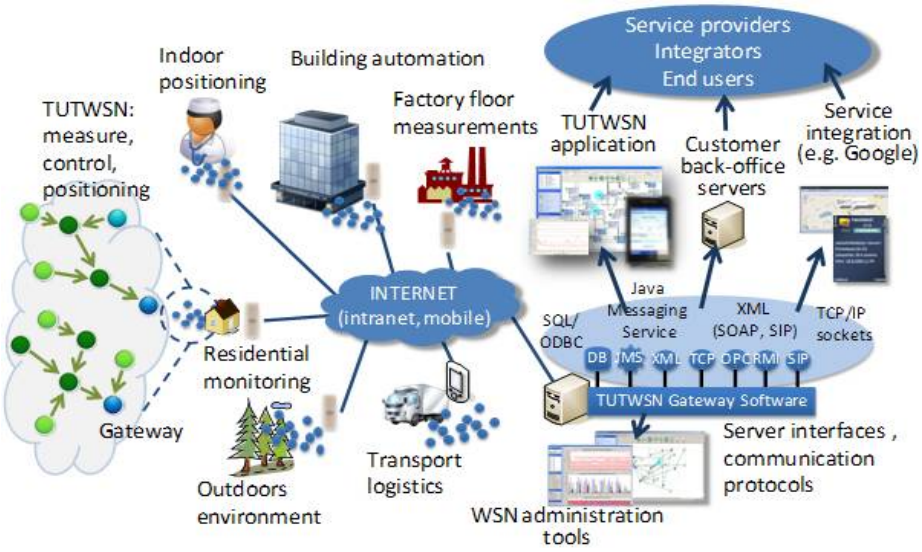

Fig 1.1: Wireless Sensor Network [11]

In figure 1.1, the WSN network has been explained in the various aspects, which involves the various angles of the generalized networks. This figure elaborates the applications of the WSN in the various domains. Wireless sensor networks (WSN) are starting to become a reality, and therefore some long-neglected limits have become an important area of research. [4-5] During the last half century, computers have increased exponentially in processing power and at the same time decreased in size and price. [7] This rapid progress leads to a very fast market in which computers would participate in more daily activities of our society. In recent years, such a revolution has taken place, where computers have become so small and cheap that disposable computers with integrated sensors are almost practice both economic and theoretical perspectives. [8]

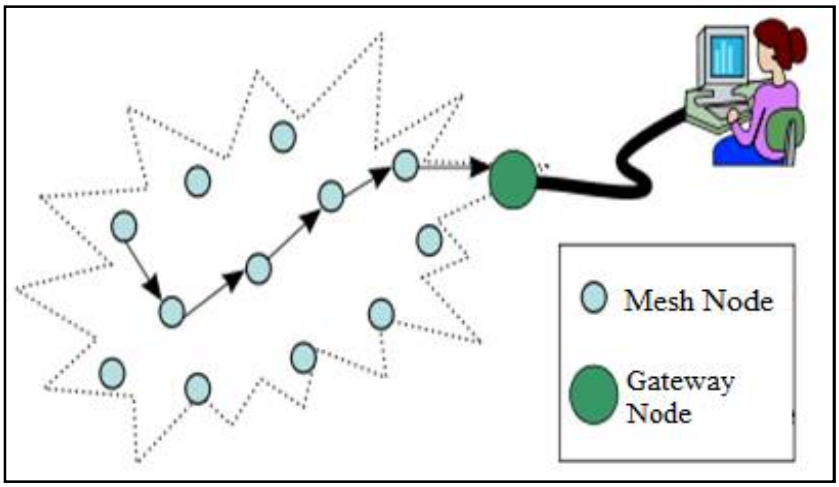

Figure 1.2: Wireless mesh network Architecture [12]

In figure 1.2, the wireless networks has been demonstrated, which shows the best route selection. Also, the data integrator has been shown in the figure 1.2, which collects the whole data in order to process the useful patterns from the collected data. [8-9] In the latest research on WSN, researchers are trying to find and overcome the limitations of

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

wireless mesh networks such as limited energy resources, ranging energy consumption by location, the high cost of transmission, and limited processing capabilities. [9] Routing approaches that have worked so well for traditional networks over twenty years will not be enough for this new generation networks. [10] All these characteristics of wireless mesh networks are totally opposed to their cable counterparts network, which energy consumption is not an issue, the cost of transmission is relatively cheap, and network nodes have a lot of processing power.

II. LITERATURE REVIEW

Seema et. al. [1] has worked on the various deployment methods in the WSN paradigm. The efficiency of sensor networks analyzed to determine the coverage of the target area. Although, in general, a sufficient number of sensors were used to ensure a certain degree of redundancy in coverage, a good sensor deployment method was still necessary to balance the workload of sensors in target area. Amith et. al. [2] performed the comparison on the various wireless routing protocols for WSNS. The protocols analyzed under this survey were connected via wireless channels and can use multiple hops to exchange data. Routing protocols covered in the survey were needed for communication in such Ad hoc networks, where it targets for efficient and timely delivery of message. **Vibha Yadav et. al. [3] developed the 3D approach for GPS enabled WSNs to improve the low level connectivity.** Location awareness among the participating nodes was observed as one of the crucial requirements in designing of solutions for various issues related to Wireless Sensor Networks (WSNs). This paper discussed about a range free localization mechanism for WSN that operate in a three dimensional space**. Rajesh Sharma et. al. [4] worked on the improvement of DSR protocol for WSNs in order to improve the conserve the energy in network related transactions.** DSR allowed the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administratio**n. Amit Thakare et. al. [5] analyzed the performance of the AODV & DSR routing protocols for the WSNs.** MANET were observed as autonomous system of mobile nodes connected by wireless links in this paper. Each node operated not only as an end system, but also as a router to forward packets. The nodes were free to move about and organize themselves into a network. These nodes changed position frequently. **Rajeshwar Singh et. al. [6] involved the various routing protocols for the performance analysis on WSNs.** The WSN simulation was observed as the collection of autonomous mobile nodes that communicate with each other over wireless links without any fixed infrastructure. The nodes used the service of other nodes in the network to transmit packets to destinations that were out of their range.

III. EXPERIMENTAL DESIGN

The WSN networks are the sensor networks involving larger number of nodes to collection data from certain source. The WSN routing protocols typically involve the ad-hoc routing architecture properties, and there are multiple chances of link failures due to the various reasons. [13] The primary reasons of link failures are node failures, limited battery resources, faulty nodes, blackhole attacks, software error (connectivity hole), etc. In this paper, the routing model is designed with the fuzzy logic controller (FLC) to manage the routes between source and destination nodes. The hacking attempts on the node availability are checked under this FLC oriented routing model. The FLC based routing model is combined with dijikstra algorithm to discover the best routes among the given scenario. The blackhole attacks are detected and the blackhole nodes are effectively removed from the given network segment by analyzing the various network parameters.

Generally (First case), when a network load failure occurs, the node sends the route error (RERR) to the neighboring nodes. When a node failure suddenly occurs (Second case) in a WSN node, the RERR is not sent to the neighboring nodes.[14] In the second case, the neighboring node waits for a certain period, which is known as wait timer, for a hello packet from target node. Once the wait timer expires, the node is automatically flushed out of the routing table. For the waiting time in the wait timer, the network convergence does not occur. [15] The network convergence is the criteria to find the new route, when existing route goes down. The data drop drastically increases for the wait period, and no convergence can occur before the route is marked unavailable. In the case of blackhole node, generally the second case takes place, and neighboring nodes are not updated properly with RERR updates. [16] In this case, the latent discovery

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

increases the propagation hurdles in the network. Hence, the fuzzy routing based mechanism has been proposed to detect the path performance, and to enable to early detection of node failures. In the proposed model the FLC design can be elaborated with the following diagram:

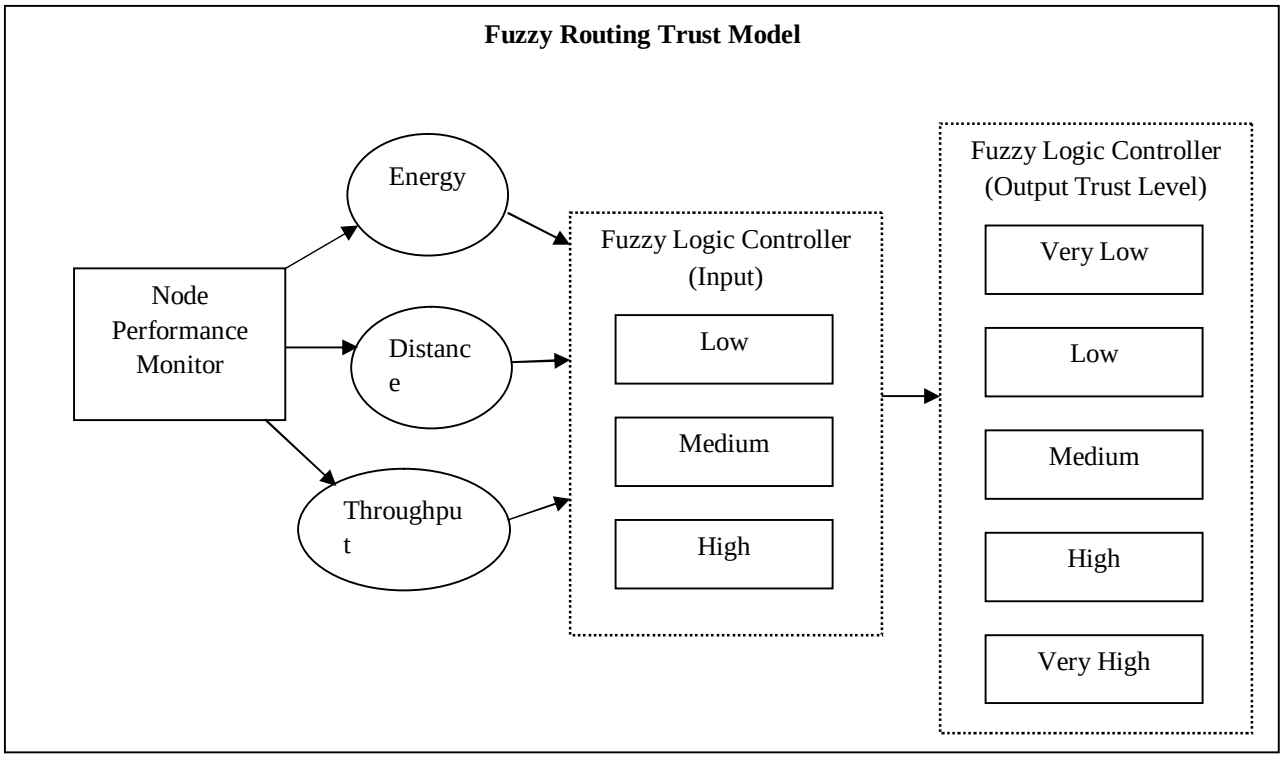

Figure 3.1: Fuzzy Routing Trust Model

In the figure 3.1, the fuzzy model has been explained in detail. This figure reveals the major factors used to determine the network performance and trust level of the wireless nodes, which involves distance, throughput and energy.
The trust based fuzzy routing model works on the basis of three input parameter of energy, distance and throughput, where the throughput is computed in the form of packet delivery ratio (PDR) instead of data volume. Each of the parameters is evaluated on the three-step scale mentioning low, medium and high values. The combinations of the parameters are defined in the FLC as rule list, which are observed and the current trust of the nodes is notified. The inclusion of exclusion of current node in the network route is based upon the output trust value by the FLC. The FLC works in collaboration with the dijikstra based routing model, which is used to decide the end-to-end route between the source and destination nodes. The following algorithm describes the overall working of the routing algorithm used to discover the paths among the WSN:

Algorithm 1: Best Path Selection Algorithm

(1) Obtain the source and destination nodes
(2) Run the best path selection model
(3) Obtain the sparse matrix showing the one-hop connectivity map between the network nodes
(4) Run the path lookup procedure:
  a. Find the seed node, which is the source node
  b. Find all possible next-hop nodes with the help of 1-hop sparse matrix
  c. Run the FLC approach over next-hop nodes

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

d. Shortlist the next-hop node with best trust score
e. If current node is destination node
  i. Assign the path
  ii. Connect source and destination over the given path
f. Otherwise
  i. Go to step 4(a)

IV. RESULT ANALYSIS

The result analysis has been performed on the basis of the performance parameters of packet delivery ratio (PDR) and end-to-end delay, which are also compared with the existing model. The proposed model has been found consistently better than the existing model in the terms of both of the performance parameters. The proposed model has been found efficient with average PDR of 99.19% against the 98.93% in the existing model. The maximum PDR of proposed model remain at 99.99% against 100% in the existing model, whereas the minimum PDR of proposed model is 99% in comparison with the 98% in the existing model.

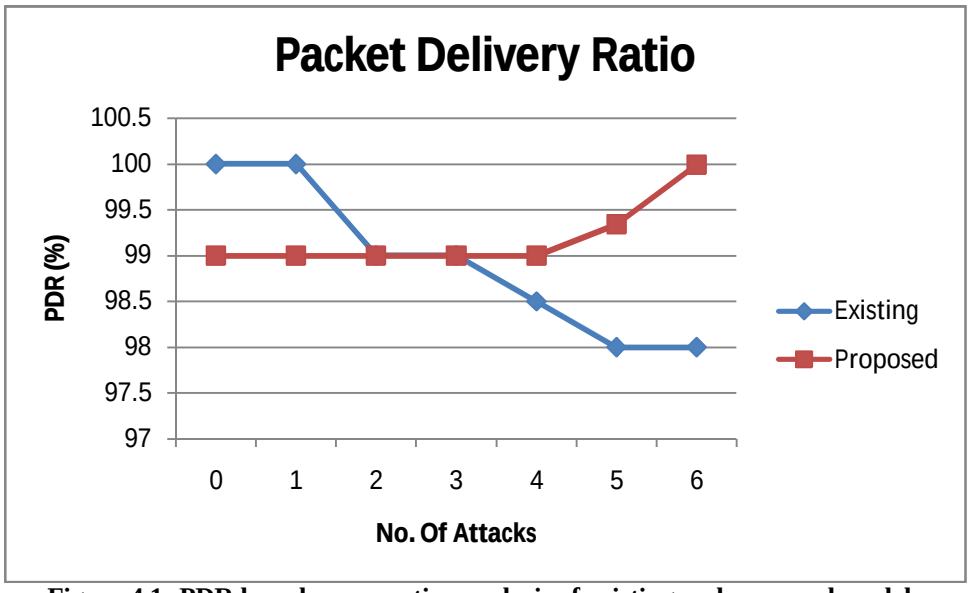

Figure 4.1: PDR based comparative analysis of existing and proposed models

The figure 4.1 explains the performance of the proposed model in form of packet delivery ratio (PDR). The PDR parameters measures the percentage of the successfully processed packets in the given network segments. According to figure 4.1, the comparative analysis of proposed and existing models displays the robustness of the proposed model in nearly all aspects. The proposed model has been recorded below existing model is maximum PDR, where the difference of 0.01% is observed. The existing model is observed between 98 and 100 percent, whereas the average PDR for existing model is observed below 99%. The proposed model is observed between 99 and 100 percent, whereas the average value remains above 99%, which is certainly better and shows the significant improvement in the case of proposed model.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

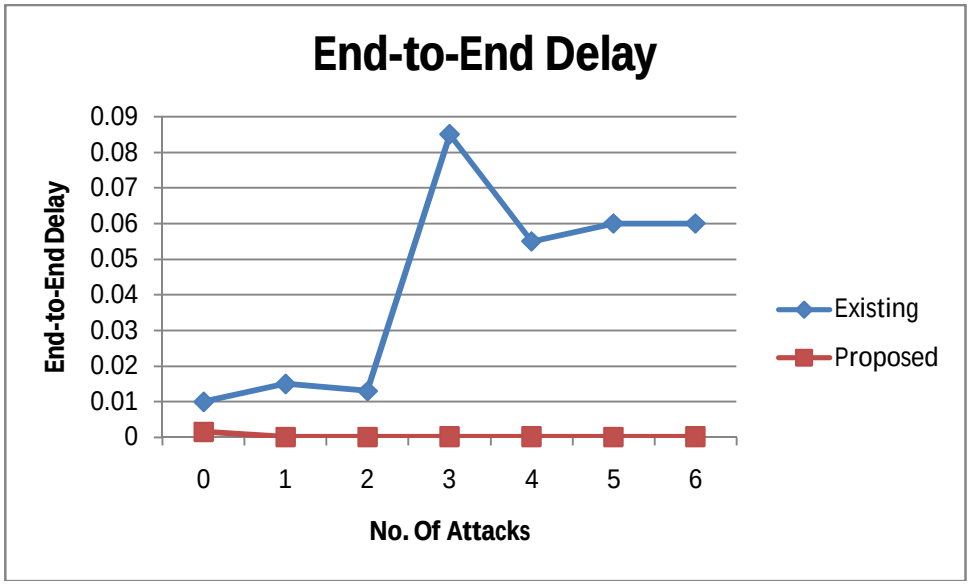

Figure 4.2: End-to-End delay based comparative analysis of existing and proposed models

In figure 4.2, the end-to-end delay is compared, where the proposed model results are observed consistently lower than the existing model. The end-to-end delay is the parameter to measure the time taken for the packets to reach the destination from source node. The existing model is recorded greater than 0.01 seconds on all of the events, whereas the proposed model is recorded lower than 0.01 seconds in all of the transactions. The average delay in existing model is observed at 0.04 seconds, which is outperformed by 0.0004 seconds for the proposed model.

V. CONCLUSION

The proposed model is based upon the attack detection and recovery path planning across the wireless sensor networks. WSNs are highly prone to the several kinds of network attacks due their lack of computational power and memory. The limited computation resources prevents us from implementing the dedicated security solutions on the sensor nodes, which means the security paradigm must be infused in the routing mechanism in order to prevent the external attacks such as blackhole, wormhole, etc. The fuzzy logic controller (FLC) based mechanism has been proposed in this paper, which has outperformed the existing model on the basis of end-to-end delay and packet delivery ratio (PDR). The existing model has been outperformed on the basis of end-to-end delay where proposed model has been recorded between 0.00014 and 0.0015 seconds against range of 0.01 and 0.085 seconds. Also, the packet delivery ratio of proposed model has been recorded between 99 and 99.99% against the range of 98 and 100% in existing model.

REFERENCES

[1] Seema, Reema Goyal, "A Survey on Deployment Methods in Wireless Sensor Networks", ijarcsse, vol 3 (7), Pp 540-544, 2013
[2] Amith Khandakar , " Step by Step Procedural Comparison of DSR, AODV and DSDV Routing protocol ", ICCET, vol 40, Pp 36-41, 2012
[3] Vibha Yadav , "Localization Scheme For Three Dimensional Wireless Sensor Networks Using Gpsenabled Mobile Sensor Nodes",ijngn, vol 1(1), Pp 60-73, 2009
[4] Rajesh Sharma, " Dynamic Source Routing Protocol (DSR) ", ijarcsse, vol 3 (7), Pp 239- 241, 2013
[5] Amit N. Thakare , "Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks", ijca, vol 4, 2010
[6] Rajeshwar Singh , "Performance Evaluation of DSR and DSDV Routing Protocols for Wireless Ad Hoc Networks. " ,ijana, vol 2(4), Pp 732-737, 2011
[7] Pallavi Sahu, , " Deployment Techniques in Wireless Sensor Networks", ijsce, vol 2(3), Pp 525-526, 2012
[8] Guoyou He," Destination-Sequenced Distance Vector (DSDV) Protocol, An ad hoc network is a collection of mobile nodes forming an instant network without fixed topology." ,

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

[9] Hemanth Narra, "Destination-Sequenced Distance Vector (DSDV) ", 2011.
[10] Manish Kushwaha, "Sensor Node Localization Using Mobile Acoustic Beacons", IEEE, Pp 1-9, 2005
[11] Chen, Hao, Xiaoyun Xie, Wanneng Shu, and Naixue Xiong. "An Efficient Recommendation Filter Model on Smart Home Big Data Analytics for Enhanced Living Environments." *Sensors* 16, no. 10 (2016): 1706.
[12] Patil, Manjusha, and Vasant N. Bhonge. "Wireless sensor network and RFID for smart parking system." *International Journal of Emerging Technology and Advanced Engineering* 3, no. 4 (2013): 188-192.
[13] Tan, Shuaishuai, Xiaoping Li, and Qingkuan Dong. "A trust management system for securing data plane of ad-hoc networks." *IEEE Transactions on Vehicular Technology* 65, no. 9 (2016): 7579-7592.
[14] Han, Guangjie, Jinfang Jiang, Lei Shu, Jianwei Niu, and Han-Chieh Chao. "Management and applications of trust in Wireless Sensor Networks: A survey." *Journal of Computer and System Sciences* 80, no. 3 (2014): 602-617.
[15] Raje, Radhika A., and Apeksha V. Sakhare. "Routing in wireless sensor network using fuzzy based trust model." In *Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on*, pp. 529-532. IEEE, 2014.
[16] Khare, Ashish Kumar, J. L. Rana, and R. C. Jain. "Detection of Wormhole, Blackhole and DDOS Attack in MANET using Trust Estimation under Fuzzy Logic Methodology." (2017).