Gyancity Journal of Engineering and Technology,
Vol.5, No.1, pp. 6-15, January 2019
ISSN: 2456-0065 DOI: 10.21058/gjet.2019.51002

Fuzzy Logic Trust Based Routing in Wireless Sensor Network

Manwinder Singh[#], Ashima Rai[*], Dr. Manoj Kumar[§]

[#]Research scholar, Dept. of Electronics and Comm. Engg. IKG-PTU Jalandhar. India

*Research Scholar, Dept. of Electronics and Comm. Engg.NIT, Delhi, India

[§]Principal, DAVIET, Jalandhar, India

#Singh.manwinder@gmail.com
*Ashimarai1708@gmail.com
[§]drmanojkumarindia@gmail.com

Abstract- ***Wireless Sensor nodes are usually equipped with the computationally limited abilities. The low computational powered and low memory nodes are also equipped with smaller batteries. This prevents them from performing the larger computations as well as handling the large volumes of data in the runtime memory. The route discovery in WSNs is based upon the route request (RREQ) and route reply (RREP). The fuzzy logic system (FLS) mechanism is developed for the proposed fuzzy routing mechanism along with Dijikstra's shortest path selection based routing algorithm. The Dijikstra's algorithm is incorporated to compute the shortest and best paths between the sensor nodes Evaluation in the performance of the proposed model has been taken place in the form of throughput, energy consumption as well as packet delivery ratio (PDR), which is compared with the existing model. Proposed model outperformed existing methods.***

Keywords: ***WSN, Fuzzy logic system, FRTB.***

1. Introduction

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[1-10]. 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 black-holes, grey holes, 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 re-compute the paths between the affected nodes[11-14].

In this paper, the Fuzzy logic system (FLS) based routing mechanism is developed which is coupled with Dijikstra routing algorithm to provide the vital and vigorous connectivity around the black-hole nodes. The WSN networks are the sensor networks involving larger number of nodes to collect data from certain sources. The WSN routing protocols typically involve the wireless sensor routing architectural properties, and there are multiple chances of link failures due to the various reasons. The primary reasons of link failures are node failures, due to limited battery resources, faulty nodes, black-hole attacks, software error (connectivity hole), etc. In this paper, the routing model is designed with the help of FLS to manage the routes between source and destination nodes. The hacking attempts on the node availability are checked under FLS model. The black-hole attacks are detected and effectively removed from the network by analyzing the various network parameters.

2. Related Work

Raymond et al. [2005] took the primary step in addressing each shortcoming by introducing two new distributed multi-resolution transforms [15-16]. Scott Briles et al. [2005] described the graphical programming tools used to implement a new geo-location algorithm composed of Windowing, FFTs, complex multiplies, spectral averaging, and the arctan function. The presentation may be of interest to our GUI efforts [17]. Alain Bertrand Bomgni et al. [2010] proposed clique based algorithm. In this algorithm packets sent by the sink node to all nodes were deployed in different geo-cast regions, the network was partitioned into cliques by using an existing energy-efficient protocol based on clustering. Secondly, the cluster-heads of cliques were separated into sets using an energy-efficient hierarchical clustering turn-by-turn [18].This approach consumed less energy due to which it came into the category of energy-efficient clustering algorithm. Harilton da S. Araújo et al. [2010] proposed Directed Diffusion routing protocol to reduce energy usage in network. This proposal uses Geocast approach in which all broken paths were repaired by reconstructing new routing tree so that cost of energy can be reduced [19]. Abdellah et al. [2011] proposed a hierarchic adjustive balanced energy economical Routing Protocol (HABRP) to decrease likelihood of failure nodes and to prolong the quantity before the death of the primary node (stability period) and was increasing the period of time in heterogeneous WSNs, that was crucial for several applications It also proposed an energy efficient routing protocol for heterogeneous wireless sensor network. [20]. Xu Jiu-qiang et al. [2011] had proposed the algorithm for discovering and computing the connected key nodes. The additional mobile nodes were introduced to enhance the topology connectivity in WSN. A path planning algorithm was also proposed so that the lifetime prolonged and reduced the effects caused by connected key nodes [21].Young-Chul Shim, et al. [2011] introduced different geocast algorithms using the information about hop-to-hop neighbour [22]. Krishnan S. R. et al. [2012] had worked on the Energy consumption and CO_2 emissions by the Indian mobile medium business. During this paper, the mobile medium business was disaggregated into varied segments, supported the lifecycle of the device, and every segment's contribution to the general energy consumption, and its individual CO2 emissions were mentioned [23]. Sonam Palden Barfunga et al. [2012] proposed energy efficient routing protocol which was hierarchical and based on clustering [24]. Ahlawat A,. et al. [2013] had worked on the economical analysis of the Leach protocol for energy potency within the wireless networks. To increase the period of WSN the LEACH protocol was enforced by forming clusters for routing during a massive scale network [25]. Dai et al. [2013] proposed the workload through a wireless node in which load balancing dropping the hot-spots in the sensor array as well as increase the existence of the energy of the sensor node. According to this article the author designed a node-centric algorithm that built a network loads balancer shaft asymmetric architecture sensors. The author evaluated the algorithm reaches routing trees which were more effectively balanced routing based on the BFS and shortest path obtained by the Dijkstra algorithm [26]. Rambabu A. Vatti et al. [2014] worked on the wireless networks to analyze their overall throughput under the various circumstances. In this paper, the authors had projected an answer to resolve the matter of packet loss because of over usage of the intermediate nodes. Remaining energy based mostly reconciling multi-hop rule (RAMA), that took routing selections supported the remaining energy at every of the neighbouring nodes and adopted short distance multi hop communication to relay the information from supply to sink node [27]. Ji et al. [2015] had worked on the throughput-outage trade-off [28].Jiang, Jinfang et al. [2015] had proposed the robust trust model for the distributed computing environments, specifically in the sensor networks. In this paper, the authors had worked upon the implementations of efficient distributed trust model (EDTM) [29]. Tang, Di et al. [2015] had developed the cost aware secure routing (CASER)

mechanism for the WSN networks [30]. Ahmed, Adnan et al. [2016] had also worked on the implementation and design of the trust based routing mechanism for the sensor networks. The new trust and energy aware routing protocol (TERP) was designed to handle the data transmissions with the higher efficiency, when keeping an eye on the security management by the means of trust management protocol on the sensor networks [31]. Elhoseny, Mohamed et al. [2016] had worked on the data security scheme for the WSN networks using the encryption based on elliptic curve cryptography [32].Lv et al. [2016] had worked on the energy-balanced model for the information compression mechanism for WSNs [33]. Zeinali et al. [2016] this work was to analyzed completely different compression techniques within the context of the good grid communication infrastructure [34]. Jan, Mian et al. [2017] has developed the authentication scheme for sensor networks, known as the payload based mutual authentication (PAWN) mechanism [35].

In the literature review section, the study of the various network related models has been conducted in order to obtain in-depth knowledge about the working of sensor networks. The studies related to the security protocols, routing algorithms, clustering and other aspects would be covered under this section. The routing model security has been determined as the primary issue in the case of WSNs as they are empowered with the low computational resources. The constraint of lower computational capability limits the abilities of sensor networks to tackle the attacks. Hence, in this paper an improved model has been presented, which is integrated into the routing model, which preserves the computational power in comparison with standalone security solutions and provides the robust level of security. This model is designed to prevent the malicious routing attacks over the sensor networks.

3. Proposed Method

The problem which occurs due to traditional routing algorithms is that they were not capable to generate the optimized route to any destination. So in this work we developed a new approach which has the capability to generate the optimal path for data transmission. In this proposed work, a fuzzy logics system is used to optimize and secure routing considering the parameters like distance, energy and throughput in order to select the nodes for route creation using trust based routing protocol.

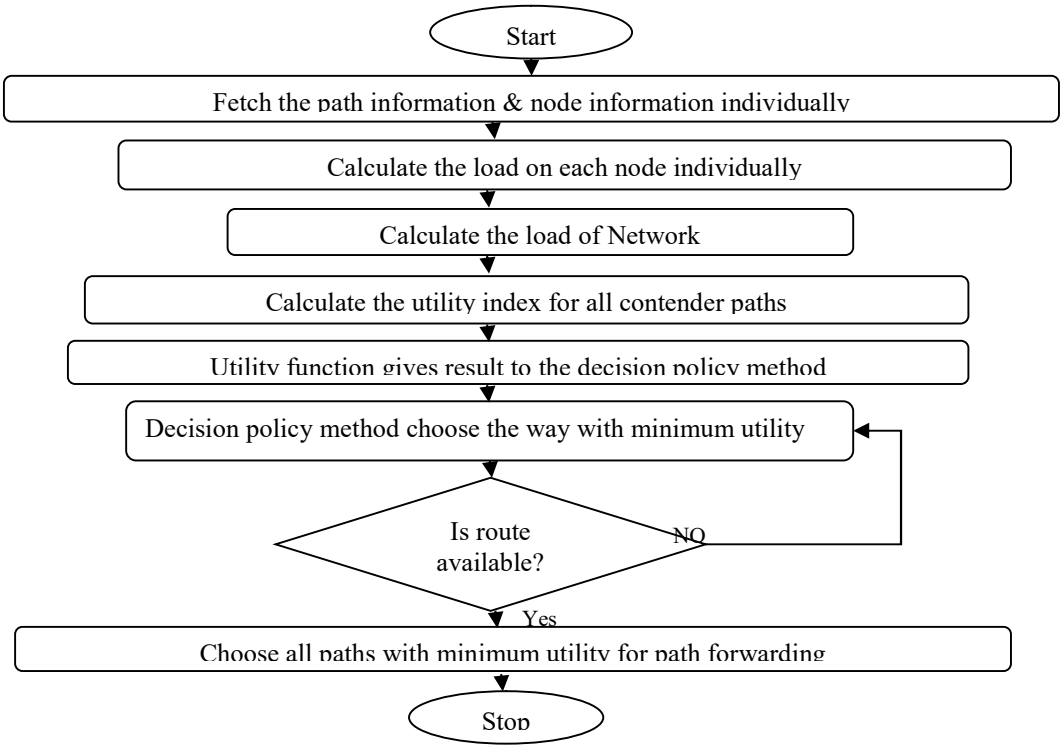

Fig. 1: Load Balancing Algorithm

In Fig. 1, the network first fetch the path and node information for calculation of the load on each node, load of network as well as the utility index for all paths. Thereafter, it uses the decision policy for choosing the minimum utility, when a network load failure occurs, the node sends route error (i.e. RERR) signal to the neighboring nodes. Whenever a node failure suddenly occurs (Fig. 2) in a WSN node, the RERR is not deliver to the neighboring nodes. When the route is available, it forwards all the paths with the minimum utility. Consequently, it controls flow of the load balance of network paths. The WSN routing protocols typically involve the wireless sensor routing architecture properties, and there are multiple chances of link failures due to the various reasons.

In the Fig. 2, 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. 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 black-hole node, generally the second case takes place, and neighboring nodes are not updated properly with Route error (RERR) updates. In this case, the latent discovery 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.

Gyancity Journal of Engineering and Technology,
Vol.5, No.1, pp. 6-15, January 2019
ISSN: 2456-0065 DOI: 10.21058/gjet.2019.51002

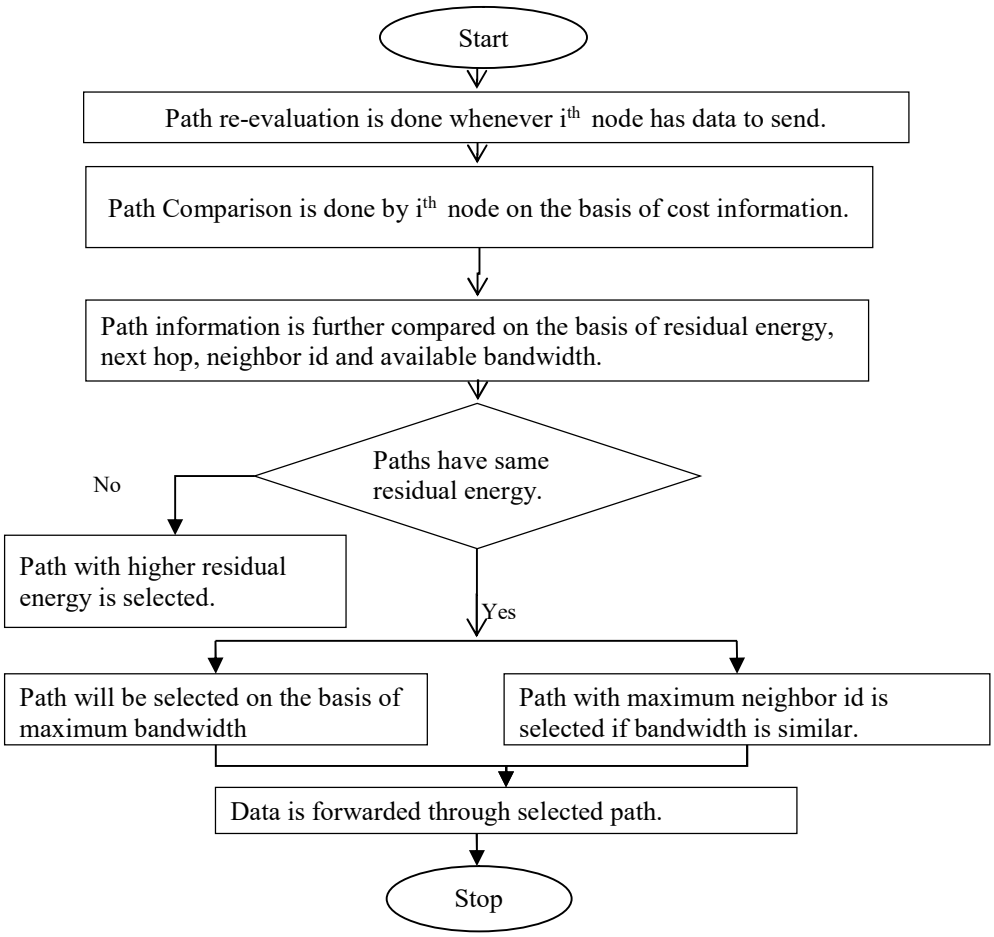

Fig. 2: Optimal path Selection Algorithm

The WSN networks are the sensor networks involving larger number of nodes to collect data from certain source. The primary reasons of link failures are node failures, limited battery resources, faulty nodes, black-hole attacks, software error (connectivity hole), etc. In the proposed model the FLS design can be elaborated with the following diagram(Fig.3):

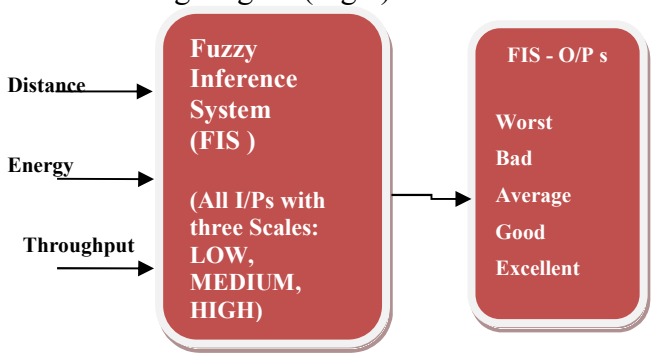

Fig. 3: Fuzzy Routing Trust Model (FRT)

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 Fuzzy controller as rule list (as shown in

Table1), which are observed and the current trust of the nodes is notified. The inclusion and exclusion of current node in the network route is based upon the output trust value by the Fuzzy controller (FC). The FC 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.

Table 1 Fuzzy rules for FIS to calculate Trust of Nodes

(Rules) Sr. no	Distance	Energy	Throughput	Trust of Nodes
1.	Low	Low	Low	Worst
2.	Low	Low	Avg.	Bad
3.	Low	Low	High	Bad
4.	Low	Avg.	Low	Bad
5.	Low	Avg.	Avg.	Avg.
6.	Low	Avg.	High	Avg.
7.	Low	High	Low	Avg.
8.	Low	High	Avg.	Good
9.	Low	High	High	Good
10.	Avg.	Low	Low	Worst
11.	Avg.	Low	Avg.	Bad
12.	Avg.	Low	High	Bad
13.	Avg.	Avg.	Low	Bad
14.	Avg.	Avg.	Avg.	Avg.
15.	Avg.	Avg.	High	Good
16.	Avg.	High	Low	Good
17.	Avg.	High	Avg.	Good
18.	Avg.	High	High	Excellent
19.	High	Low	Low	Bad
20.	High	Low	Avg.	Bad
21.	High	Low	High	Avg.
22.	High	Avg.	Low	Avg.
23.	High	Avg.	Avg.	Good
24.	High	Avg.	High	Good
25.	High	High	Low	Good
26.	High	High	Avg.	Excellent
27.	High	High	High	Excellent

Algorithm 1: Load Balancing Algorithm (Fuzzy Mechanism)

(1) Collect the path information and node information individually.
(2) Evaluate the load on the each node and path individually.
(3) Evaluate load of network.
(4) Calculate the utility index for all contender paths.

Note: Utility depicts the resources used on the node.

(5) Utility function results to the decision policy method.
(6) Decision policy method chooses the way with minimum utility.
(7) Choose all paths with minimum utility for path forwarding.

Algorithm 2: Optimal Path Selection Algorithm (OPSA)

The WSN algorithm boots up the routing operations after the network nodes boots up.
(1) A continuous look up procedure is started by smart path selection.
(2) After sourcing verification of the local partial connection assessment, the path selection procedure is started by path discovery.

a) The agent is registered and initiated if sourcing and verification stage is not failed.
b) Otherwise error is generated by the partial connection assessment module and terminates the path backup.

(3) If sourcing and verification stage passes then follow the following procedure:
a) Use the partial connection assessment algorithm to examine the connectivity holes in the given path.
b) Source node is dropped after the reception of negative response.
c) Hurdle recognition method initializes after the reception of ping.
d) Otherwise toggle to 2(a) state.

(4) If ping is received , perform the following procedure:
a) Partial connection assessment algorithm based on link health evaluation is started for each N-hop node over the given path.
b) Following equation is used to mark node with connectivity hole[CH timeTot]. = f(x) { n (x), X, Y };

Where Tot is amount of delay, CH is connectivity hole index, n(x) is node id, X and Y are coordinates of the wireless node.

(5) Another node research is started rather than the connectivity node hole.
If (An extra node is created over the route, then routing procedure remains in continuity).
Else
"No path available" message is returned between source and destination and Close the node backup procedure.

Algorithm 3: 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 FLS approach over next-hop nodes
    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)

4. Results and Discussion

The results of the new proposed reproduction have been obtained in the form of throughput,

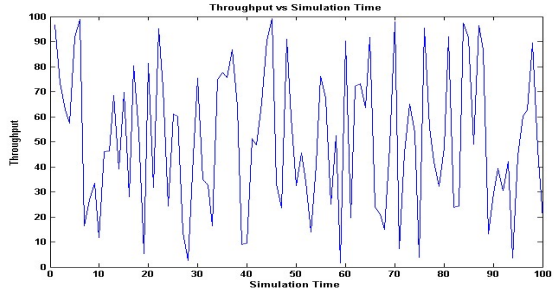

Fig. 4: Throughput v/s Simulation time

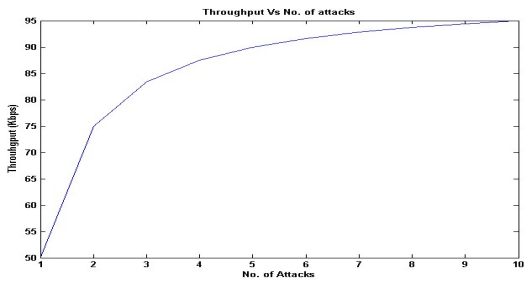

Fig. 5: Throughput v/s No. of Attacks

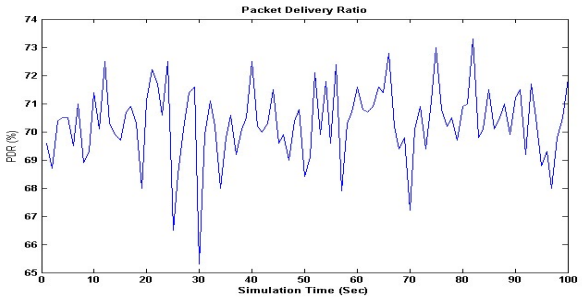

Fig 6: PDR Vs Simulation Time

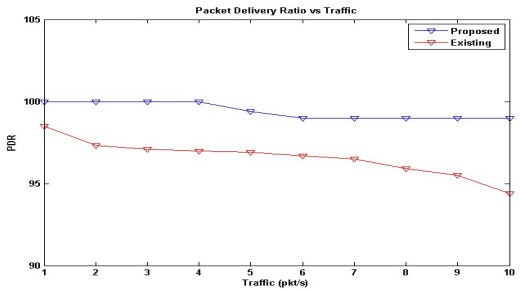

Fig 7: PDR Vs Traffic across nodes

energy consumption, delay, packet delivery ratio and residual energy based analysis. According to this simulation, the future model performance has observed before and after attack situations. Fig. 4 shows the performance of throughput under the normal network situations. The data processing capability of the network is measured in KBPS (Kilobytes per seconds). The average value of throughput in all of the rounds is observed at 47.46 Kbps, whereas the median value of the simulation model is observed at 45.16 Kbps. The throughput of the proposed model under the attack scenario is observed in Fig. 5 to analyze the network performance in the presence of the attacker nodes. The network attack nodes are increased on each round with one attacker. The throughput value is observed between 50 and 95 Kbps. The mean value of throughput in all of the rounds (with 10 attackers) is observed at 83.36 Kbps and median value at 90.83 Kbps. Fig. 6 shows the performance of packet delivery ratio under the normal network situations. The production model has been initialized with PDR between the range of 66.5% and 73.9% in the dense network. The average PDR has been recorded nearly at 70.1%, whereas the median value for the observation in all simulation rounds at 70.3%, which shows the significant performance. In Fig. 7, the proposed model is found to be more efficient in delivering the data than the existing model. The proposed model is observed as the more consistent again, where the rising volumes of traffic doesn't affect its performance much, whereas the existing model is observed with lower PDR with the rise in the traffic volume.

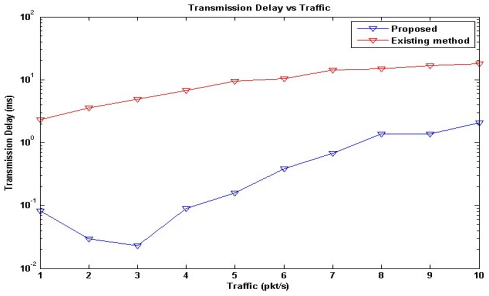

Fig. 8: Transmission delay v/s Traffic

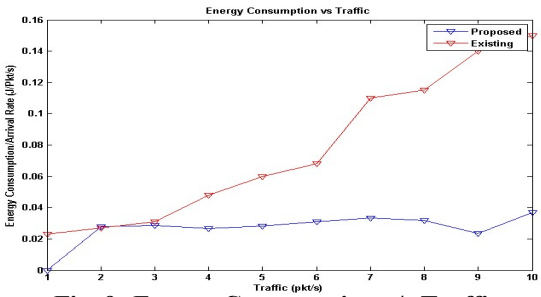

Fig. 9: Energy Consumption v/s Traffic

In Fig. 8 the proposed and existing models are compared on the transmission delay parameter to understand the impact of rising traffic with rising number of attacks over the network. The results of delay obtained from the proposed model designed using the fuzzy logic model based upon the combination of multiple factors to ensure the trust level of the wireless nodes. This phenomenon is promised to create the secure network model, which is essential to prevent the malicious nodes from joining the network. This means that the proposed model is expected to consume lower energy than its existing counterpart. However, the fluctuations are observed for the lower traffic volumes, but widen the performance gap with the increase in the traffic volumes.

The proposed model consumed lower amounts of energy with rising traffic volumes in comparison with existing model as shown in Fig. 9. The performance gap is widened with the rise in the traffic volume, which is the key performance indicator for the proposed model. This means the proposed model can efficiently handle the higher volumes of data, which favorable for the wireless networks.

5. Conclusion

The proposed model is based upon the WSN routing to resolve the routing related issues in the traditional WSN networks. This model is designed with FLS to predict the trust value of the sensor node. This trust values helps the routing algorithm to take decision on involvement of the node in the appropriate path. The idea behind the trust value is to eliminate the attack nodes from the routing paths in the network cluster, which is supposed to improve the network performance. In most of cases, the major reason behind data drop in sensor networks lies in the network attacks, connectivity holes and non-target nodes influenced by the network attacks. The proposed model is designed with aim to improve the overall performance of the sensor networks by eliminating the attack nodes. This model verifies the trust value of each next-hop node, when choosing the path between sources and destinations. The performance of the proposed model is analyzed and compared on the basis of PDR and throughput parameters. The proposed model is found better nearly on all simulation events in the terms of PDR. The PDR in this simulation is recorded between 99 and 99.99 percent. The average value of PDR is recorded at 99.19%, which is improved than existing model (98.93%). The minimum PDR based comparison proves the efficiency of proposed model (99%) against the existing (98%) on the standard WSN simulation. The average transmission delay is recorded significantly lower in proposed model (0.0004 seconds) in comparison with existing model (0.04 seconds) and consume $1/8^{th}$ energy as compare to existing methods for high traffic environment.

6. References

[1] Al-Karaki JN, Kamal AE. Routing techniques in wireless sensor networks: a survey. IEEE wireless communications. 2004 Dec;11(6):6-28.

[2] Araújo HD, de Castro WL, Holanda Filho R. A proposal of self-configuration in Wireless Sensor Network for recovery of broken paths. InSensors Applications Symposium, 2010 IEEE 2010 Feb 23 (pp. 245-250).

[3] Awada A, Wegmann B, Viering I, Klein A. A game-theoretic approach to load balancing in cellular radio networks. InPersonal Indoor and Mobile Radio Communications (PIMRC), 2010 IEEE 21st International Symposium on 2010 Sep 26 (pp. 1184-1189).

[4] Bao F, Chen R, Chang M, Cho JH. Hierarchical trust management for WSNs and its applications to trust-based routing and intrusion detection. IEEE transactions on network and service management. 2012 Jun;9(2):169-83.

[5] Bechkit W, Koudil M, Challal Y, Bouabdallah A, Souici B, Benatchba K. A new weighted shortest path tree for convergecast traffic routing in WSN. InComputers and Communications (ISCC), 2012 IEEE Symposium on 2012 Jul 1 (pp. 000187-000192).

[6] Alla SB, Ezzati A, Hssane AB, Hasnaoui ML. Hierarchical adaptive balanced energy efficient routing protocol (HABRP) for heterogeneous wireless sensor networks. InMultimedia Computing and Systems (ICMCS), 2011 International Conference on 2011 Apr 7 (pp. 1-6).

[7] Briles SD, Arrowood J, Cases T, Turcotte D, Fiset E. Real-time implementation of an adaptive bayesian beamformer. InStatistical Signal Processing, 2005 IEEE/SP 13th Workshop on 2005 Jul 17 (pp. 259-264).

[8] Byers, J., & Nasser, G. (2000). Utility-based decision-making in wireless sensor networks. In Mobile and AdHoc Networking and Computing, 2000. MobiHOC. 2000 First Annual Workshop on (pp. 143-144)IEEE

[9] Delaney, D., Russell Higgs, and G. O'Hare. "A stable routing framework for tree-based routing structures in wsns." (2014): 1-1.

[10] Dufwenberg, M., & Kirchsteiger, G. A theory of sequential reciprocity. Games and economic behavior, (2004). 47(2), 268-298.

[11] Ghadimi E, Landsiedel O, Soldati P, Duquennoy S, Johansson M. Opportunistic routing in low duty-cycle wireless sensor networks. ACM Transactions on Sensor Networks (TOSN). 2014 Jun 1;10(4):67

[12] Goyal D, Tripathy MR. Routing protocols in WSNs: A survey. In2012 Second International Conference on Advanced Computing & Communication Technologies 2012 Jan 7 (pp. 474-480). IEEE.
[13] Han, Z. Game theory in wireless and communication networks: theory, models, and applications. Cambridge University Press(2012).
[14] Ishmanov F, Malik AS, Kim SW. Energy consumption balancing (ECB) issues and mechanisms in WSNs: a comprehensive overview. European Transactions on Telecommunications. 2011 Jun;22(4):151-67.
[15] Wagner R, Choi H, Baraniuk R, Delouille V. Distributed wavelet transform for irregular sensor network grids. InStatistical Signal Processing, 2005 IEEE/SP 13th Workshop on 2005 Jul 17 (pp. 1196-1201).
[16] Wagner R, Sarvotham S, Baraniuk R. A multiscale data representation for distributed sensor networks. InAcoustics, Speech, and Signal Processing, 2005. Proceedings.(ICASSP'05). IEEE International Conference on 2005 Mar 18 (Vol. 4, pp. iv-549). IEEE.
[17] Briles S, Arrowood J, Turcotte D, Fiset E. Hardware-In-The-Loop Demonstration of a Radio Frequency Geolocation Algorithm. InProceedings of the Mathworks Int. Aerospace and Defense Conference 2005
[18] Bomgni AB, Myoupo JF. An energy-efficient clique-based geocast algorithm for dense sensor networks. Communications and Network. 2010 May 31;2(02):125.
[19] Araujo HD, Holanda Filho R, de Castro WL. Wsn routing: An geocast approach for reducing consumption energy. InWireless Comm. and Networking Conference (WCNC), 2010 IEEE 2010 Apr 18 (pp. 1-6).
[20] Alla SB, Ezzati A, Hssane AB, Hasnaoui ML. Hierarchical adaptive balanced energy efficient routing protocol (HABRP) for heterogeneous wireless sensor networks. InMultimedia Computing and Systems (ICMCS), 2011 International Conference on 2011 Apr 7 (pp. 1-6). IEEE.
[21] Xu, J. Q., Wang, H. C., Lang, F. G., Wang, P., & Hou, Z. P. (2011, June). Study on WSN topology division and lifetime. In Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on (Vol. 1, pp. 380-384). IEEE.
[22] Shim YC. An efficient geocast algorithm using 2-hop neighbor knowledge in sensor networks. International journal of latest trends in computing. 2011 Dec 28;2(4).
[23] Ranjani SS, Krishnan SR, Thangaraj C. Energy-efficient cluster based data aggregation for wireless sensor networks. InRecent Advances in Computing and Software Systems (RACSS), 2012 International Conference on 2012 Apr 25 (pp. 174-179). IEEE.
[24] Barfunga SP, Rai P, Sarma HK. Energy efficient cluster based routing protocol for WSNs. InComputer and Communication Engineering (ICCCE), 2012 International Conference on 2012 Jul 3 (pp. 603-607). IEEE
[25] Ahlawat A, Malik V. An extended vice-cluster selection approach to improve v leach protocol in WSN. InAdvanced Computing and Communication Technologies (ACCT), 2013 Third International Conference on 2013 Apr 6 (pp. 236-240). IEEE.
[26] Dai, H., & Han, R. A node-centric load balancing algorithm for wireless sensor networks. In Global Telecommunications Conference, 2013. GLOBECOM'03. IEEE (Vol. 1, pp. 548-552).
[27] Rambabu A. Vatti, A.N. Gaikwad, "Throughput Improvement of Randomly Deployed Wireless Personal Area Networks", IERI Procedia, Elsevier, 2014. Vol. 7, pp.42-48.
[28] Ji M, Caire G, Molisch AF. The throughput-outage tradeoff of wireless one-hop caching networks. IEEE Transactions on Information Theory. 2015 Dec;61(12):6833-59.
[29] Jiang J, Han G, Wang F, Shu L, Guizani M. An efficient distributed trust model for wireless sensor networks. IEEE Transactions on Parallel & Distributed Systems. 2015 May 1(1):1-.
[30] Tang D, Li T, Ren J, Wu J. Cost-aware secure routing (CASER) protocol design for wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems. 2015 Apr 1;26(4):960-73.
[31] Ahmed A, Bakar KA, Channa MI, Haseeb K, Khan AW. A trust aware routing protocol for energy constrained wireless sensor network. Telecommunication Systems. 2016 Jan 1;61(1):123-40.
[32] Elhoseny M, Elminir H, Riad A, Yuan X. A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption. Journal of King Saud University-Computer and Information Sciences. 2016 Jul 1;28(3):262-75.
[33] Lv C, Wang Q, Yan W, Shen Y. Energy-balanced compressive data gathering in wireless sensor networks. Journal of Network and Computer Applications. 2016 Feb 29;61:102-14.
[34] Zeinali M, Thompson JS. Impact of compression and aggregation in wireless networks on smart meter data. InSignal Processing Advances in Wireless Communications (SPAWC), 2016 IEEE 17th International Workshop on 2016 Jul 3 (pp. 1-5). IEEE
[35] Jan M, Nanda P, Usman M, He X. PAWN: a payload-based mutual authentication scheme for wireless sensor networks. Concurrency and Computation: Practice and Experience. 2017 Sep 10;29(17):e3986.