iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** XII **Month of publication:** December 2020

DOI: https://doi.org/10.22214/ijraset.2020.32635

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue XII Dec 2020- Available at www.ijraset.com

An Improved Approach for Secure Routing using Weight Selection with Grey Wolf Optimization

Faheam Un Nisa[1], Harmandeep Kaur[2]
[1]*Research Scholar of ECE Dept., SVIET, Banur, I.K. Gujral Punjab Technical University Punjab, India*
[2]*Asst. Prof. of ECE Dept., SVIET, Banur, I.K. Gujral Punjab Technical University Punjab, India*

Abstract: ***In WSN, data is transmitted from source nodes to the destination nodes. There are different ways of transmitting the data. For this purpose, effective and secure communication is the imperative demand these days. However, malicious nodes in WSN affect the transmission of the data. These nodes acts like an attack to other nodes present in the network. Various researches proposed different technologies to eliminate malicious nodes from the network to attain efficacious communication but still there is lack in the performance. Thus, a novel approach is projected to cope with certain issues. The novel method would increase the Quality of service (QoS) parameters to deeply analyze the entire network. The parameters taken into consideration are Distance between nodes, Trust, Residual energy and Hop Count. Along with this, the optimization technique- Gray Wolf Optimization Algorithm is introduced to determine the weight values of the factors in order that optimal communication from one node to another can be achieved. Simulation results are performed using MATLAB tool and eventually, performance analysis is executed to compare the efficiency of the proposed work with the existing technique. The obtained results of the simulation demonstrate the superiority of the proposed approach over the traditional approaches.***
Keywords**: *WSN, attacks, GWO, energy consumption, network throughput.***

I. INTRODUCTION

WSN is a wireless network which is made up of number of nodes and small base stations, called sensor. These sensor nodes use battery and made up with joined sensors, a data-processing unit, short -range radio communication and a small storage memory [1]. As the nodes are arbitrarily distributed in the network, it makes sensor nodes prone to security threats such as malicious attacks in which the malicious node tends to be the network node and result in misleads the other nodes.

In Comparison to outdated wireless networks, sensor networks should be wisely considered for security and performance matters [2]. For instance, in the sensor network having an independent nature, numerous attacks could be launched by an attacker. So, attacks can be avoided due to robust nature of sensor network. But if the attacker succeeds in attacking the network, its impact can be reduced.

There are many considerable parameters but one of important facets is energy efficiency. Further sensor node in WSN is needed to be supported by different communication models such as unicast, multicast and broadcast. As sensor nodes comprise limited energy, the mechanisms used for securing the networks must be energy efficient. Specially, the total of expensive computation and the number of message transmissions should be limited as required.

Actually, for the wireless sensor network an attacker can launch several attacks once the particular numbers of sensor nodes have been settled. In Fiction, for example: there are number of attackers which an attacker can introduce against a WSN when they assure amount of sensor nodes have been conceded. In Fiction, for example:

A. HELLO flooding attacks [3]
B. Sybil attack[4]
C. Sink hole attacks [3]
D. Worm hole attack[5]
E. Or DDoS attacks [6]
F. Black hole attack [7],

Are the multiple choices for an attacker

Due to this, attacks can cause anomalies in network which are detectable. These attacks should be detected by checking the anomalies.

In WSN there are two types of attacks i.e. Passive and Active attacks. In active attack, data tempering is done by the authorized or certified node whereas in passive attack network operations are perform without disturbances and unauthorized node achieve the access over the information[8].

Walking into the detail, attacks further divide into two groups' external attack and internal attack. Internal attack is the kind of attack in which attacker is associate with the network while in the external attack the attacker node belongs to outside the network. External attacks is consider to be less rigorous as compare to internal attack because in internal attack the targeted node have all the access to the confidential information[9].In the past, due to several security issues worm hole attacks , grey hole attack, Denial of service attacks these type of attacks are formed[10] . If any of the attacks generated in the network then the data over the WSNs can get corrupted. These attacks can be described in several parts: Black Hole Attack, Worm Hole Attack, Sink Hole Attack, Grey Hole Attack, DoS Attack etc.

In order to cope with various malicious attacks in the network, number of measures has been adopted such as key management, trust modeling, various security mechanisms and different secure routing protocols.

In order to enhance the performance of the system by resisting the malicious nodes efficiently, several researchers have been conducted. Various measures and approaches were proposed in literature to protect the network from the malicious nodes attack, and some of the proposed approaches are discussed in the next section:

II. LITERATURE REVIEW

Authors in [11] described a trust estimation approach (LTS) for large scale WSN that utilized clustering for improving the cooperation, trustworthiness and safety from detecting malicious (flawed or selfish) sensor node with less resources(power and memory)consumption.

Majid Alotaibi [12] designed a technique known as hamming residue method (HRM) for mitigation of the malicious attacks. The performance analysis of this method ensured its effectiveness.

Ahmed et al. [13] presented an Energy-aware Secure Trust Routing Scheme (ESRT), which preserves a trustworthy environment and isolates mischievous nodes. For routing decisions, ESRT includes confidence, energy and hop counts.

The article [14] provided a game-oriented theoretical derivation of energy-aware trust mechanism that managed overhead while preserving adequate security for WSNs.

Author in [15] proposed CANFIS which is an energy-efficient method of detection of malevolent nodes that detects the presence of maliciously occurring nodes in the WSNs by considering the spatial and heuristic characteristics of nodes.

In [16] authors established a public key authentication and en-route filtering (PKAEF) scheme that can prevent falsification of data injections, prevent disruptions and recorded selective transmission attacks and mitigated the effects of malicious nodes.

In paper [17], author used the weight-trustworthy routing mechanism (WTR) to identify and exclude the suspicious nodes in routing paths in intelligent-home environments where the routing of communicators is done through a mesh. In addition, the proposed method used Dijkstra's shortest path algorithm to secure communication against mischievous actions of nodes, utilizing other parameters like the node-distance, packet loss, and trust value of each node determined using an optimizer.

In [18], author proposed protocol called FEEPRP which adopts an algorithm for routing that guaranteed the safety to avoid malicious nodes and avoids data loss and restricts the use of excess power.

The paper [19] presented an EOSR (Energy optimized Secure Routing) technique which was dependent on distributed trust evaluation model to recognize and separate the malicious node in WSN in order to cope with the malicious attacks. In this approach, author used multiple parameters such as trust level of node, path length and level of node's energy to design a routing mechanism.

This proposed approach of EOSR was considered as the most efficient approach than other ones in identifying and isolating malicious node. It gave effective results.

However, the static weight values are taken in this approach to meet the required results. Although, if some other weight values are taken then it is possible that it can lead to more efficient system, and thus it is very difficult to decide the optimal static weight value randomly. For this, an automated system is required which can make decision that which value can be taken that results in more efficient system.

Also, in the conventional work, only three factors i.e. trust value, the remaining energy and the count of hop are considered, but these are not sufficient enough for achieving an enhanced system.

Therefore, there arises a requirement of new approach in order that these previous limitations can be overcome..

III.PRESENT WORK

In the above section II, various approaches proposed in literature have been reviewed, among which the EOSR technique proposed in [19] was found quite efficient. However, as mentioned in above section, it is analyzed that this approach lacks in several aspects which are needed to be improved.

Therefore, a novel approach is proposed in this paper that takes into consideration the previous limitations.

As stated earlier that conventional work consists of only three factors which are not sufficient enough and thus it is required to consider more efficient factor.

Therefore, in the proposed work, another factor i.e. distance between nodes is taken into account. It is very significant factor as it will determine the quality of the system. The energy also depends on the distance factor in such a way that with the increase in distance between nodes, the nodes require to travel more to reach destination node and thus it consumes more amount of energy.

Thus, the proposed work consists of total four factors which are:

A. Distance between nodes
B. Trust factor
C. Residual energy
D. Hop Count

Now, with the increase in number of parameters, it is required to determine the weight value for increased factors also. Instead of defining the weight values statically (as previous approach), the proposed approach has make the system automated for which optimization algorithm is used.

In the proposed work, GWO algorithm is used which will automatically make decision that what weight value of four factors should be taken. It will help to choose optimal weight value so that the packet delivery ratio and network throughput can be enhanced.

GWO algorithm is used in this because it consists of only few parameters and its implementation is simple due to which it becomes greater as compared to conventional ones. And it has optimal discovery and exploitation than other approaches. And it has versatile features such as simplicity, flexibility, derivative free and local minimal prevention.

Therefore, the proposed approach with GWO optimization and enhanced number of parameters can helps to achieve an efficient system performance.

IV.METHODOLOGY

The flow diagram of the proposed is represented in figure 1, which illustrates the stepwise processing of the work:

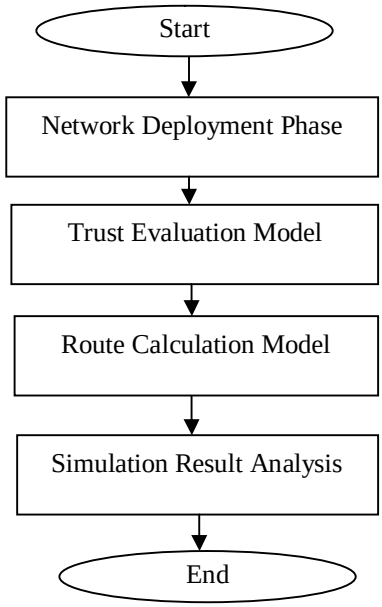


Figure 1: Flow Diagram of proposed work

V. RESULTS AND DISCUSSIONS

As stated in present work section, in the proposed work, four factors are taken into account i.e. Distance between nodes, Trust, Residual energy and Hop Count, to deeply analyze the performance of the system, and also GWO approach is proposed to determine the weight values. In order to demonstrate the performance of this proposed approach, the simulation is carried out. And the results obtained from the simulation are represented and discussed in this section as below:

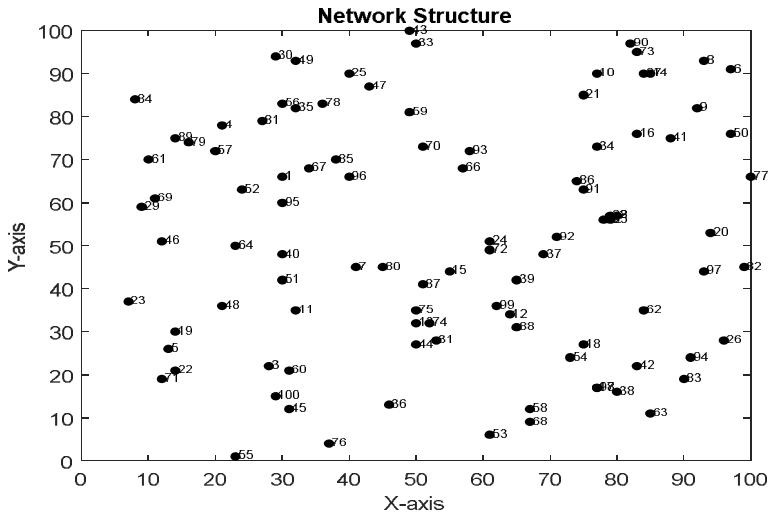


Figure 2: Network Structure of proposed system

The network structure of the proposed system is exemplified in graph of figure 2. In the graph, the y-axis and x-axis calibrates the number of nodes ranging from 0 to 100. In the network, total number of nodes present is 100, and their distribution in the system is clearly observable from the above figure. Now, in this network, communication of data has to be performed between these nodes. The process of communication from source to destination in this network of proposed system is shown in figure 3.

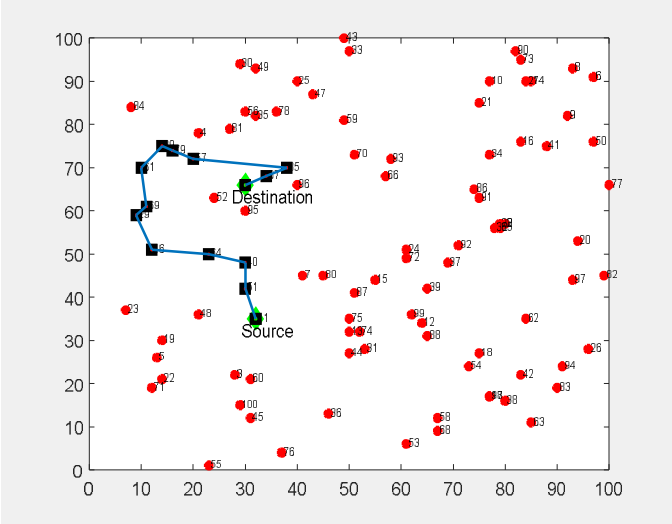


Figure 3: Communication between nodes of the network

Thus, as it can be seen from the above figure that while communication, two different nodes are selected as source and destination among which communication is to be performed. Then, for this process of communication, the routing is performed for which different nodes are chosen and on the basis of this formed route, the communication of data occurs from source to destination. In the proposed work, the routing is performed efficiently on the basis of different parameters i.e. Distance between nodes, Trust, Residual energy and hop-count. And also, to determine the weight values of the factors GWO approach is used. Thus, this routing helps to achieve an energy-efficient, reliable and effective communication in the network.

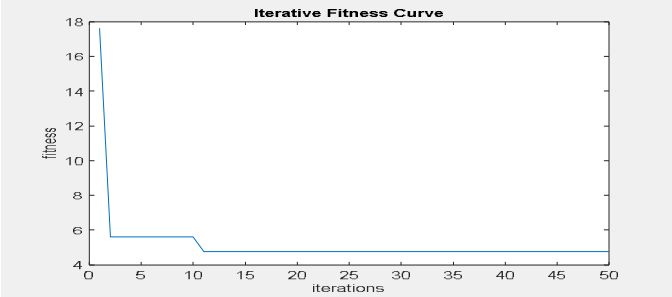


Figure 4: Iterative Fitness Curve

The iterative fitness curve of the proposed work is illustrated in figure 4. In this graph, the y-axis calibrates the value of fitness varying from 4 to 18, and x-axis calibrates different numbers of iterations ranging from 0 to 50. This graph shows the steep decrease in fitness value of proposed work at initial iterations, and then has constant fitness value from iteration 2 to 10, then again shows decrease in value and then again it became constant and remains constant for rest number of iterations.

Now, the comparative analysis between proposed approach and traditional approaches i.e. EOSR (Energy-Optimized Secure Routing), TARF (Trust Aware Routing Framework), EN-AODV (Enhanced Ad hoc On-Demand Distance Vector routing) is performed in terms of network throughput and average energy consumption,

A. Throughput

Throughput is referred to the rate at which the data is transmitted in the network. It is computed in terms of bits per second. Throughput of the network is calculated from the following equation:

$$\text{Throughput} = N/1000 \text{ --- (1)}$$

B. Energy Consumption

The energy is the major source of the nodes in the wireless sensor network for survival. Basically, each node utilized certain energy to transmit the data from source to destination node. The energy consumption of the nodes should be low so that the network can survive for long and hence more data can be transmitted. The energy dissipated by the nodes in the network can be calculated as:

$$E_{Tx}=P_{Tx}\cdot t_t$$

$$E_{Tx}=E_{Tx}=V_{dd}\cdot I_{Tx}\cdot t_t \text{ ----} \quad (2)$$

The results obtained in terms of these parameters are represented below:

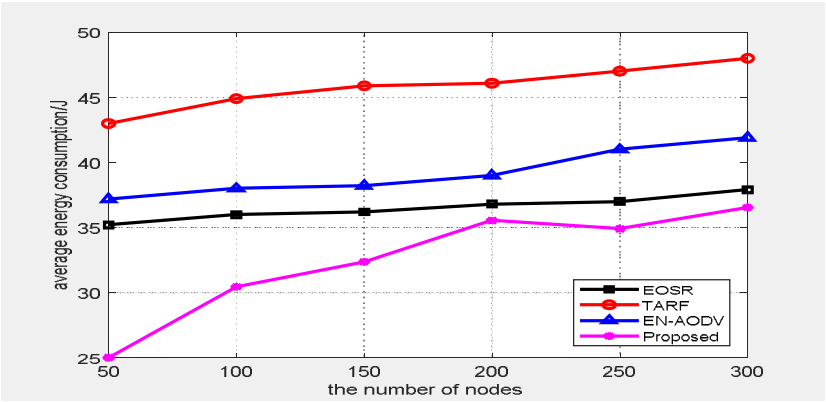


Figure 5: Comparative analysis in terms of average energy consumption

The proposed approach is compared with different traditional approaches i.e. EOSR, TARF, EN-AODV in terms of average energy consumption at different number of nodes, results of which are represented graphically in figure 5. In this, TARF has the highest value of energy consumption followed by EN-AODV and then EOSR; however, proposed approach has the lowest value of energy consumption. Thus, it is clearly comprehensible from this obtained graph that proposed approach is the most efficient technique as compared to all traditional approaches as it shows lowest energy consumption at different number of nodes than the conventional approaches, and low consumption of energy consequently leads to long network lifetime and thus, energy efficient and reliable system can be attained.

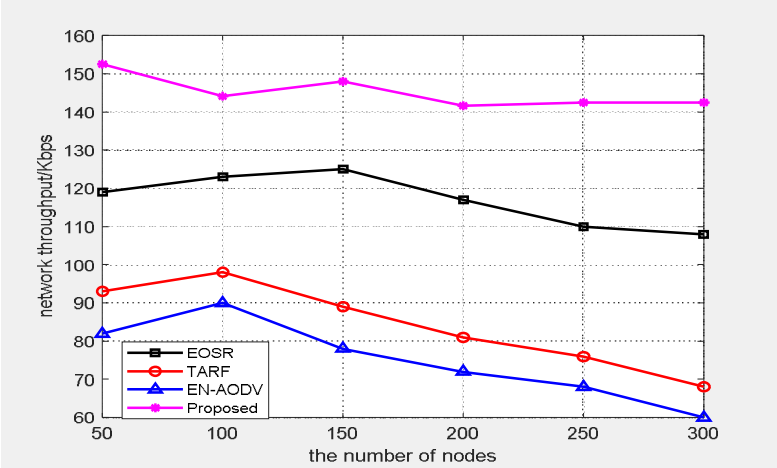


Figure 6: Comparative analysis in terms of network throughput

Figure 6 delineates the results of comparative analysis among proposed and traditional approaches in terms of network throughput at different number of nodes. It is clearly observable from the above graph that EN-AODV is the most inefficient technique followed by TARF and EOSR as they have low network throughput, and low throughput of network results in inefficient performance of the system. However, proposed approach has the highest value of network throughput at different number of nodes in contrast to all the conventional approaches. And thus, high network throughput consequently leads to highly efficient system performance.
Thus, all the obtained results represented in this section demonstrate the efficiency of the proposed approach in terms of network throughput and energy consumption.

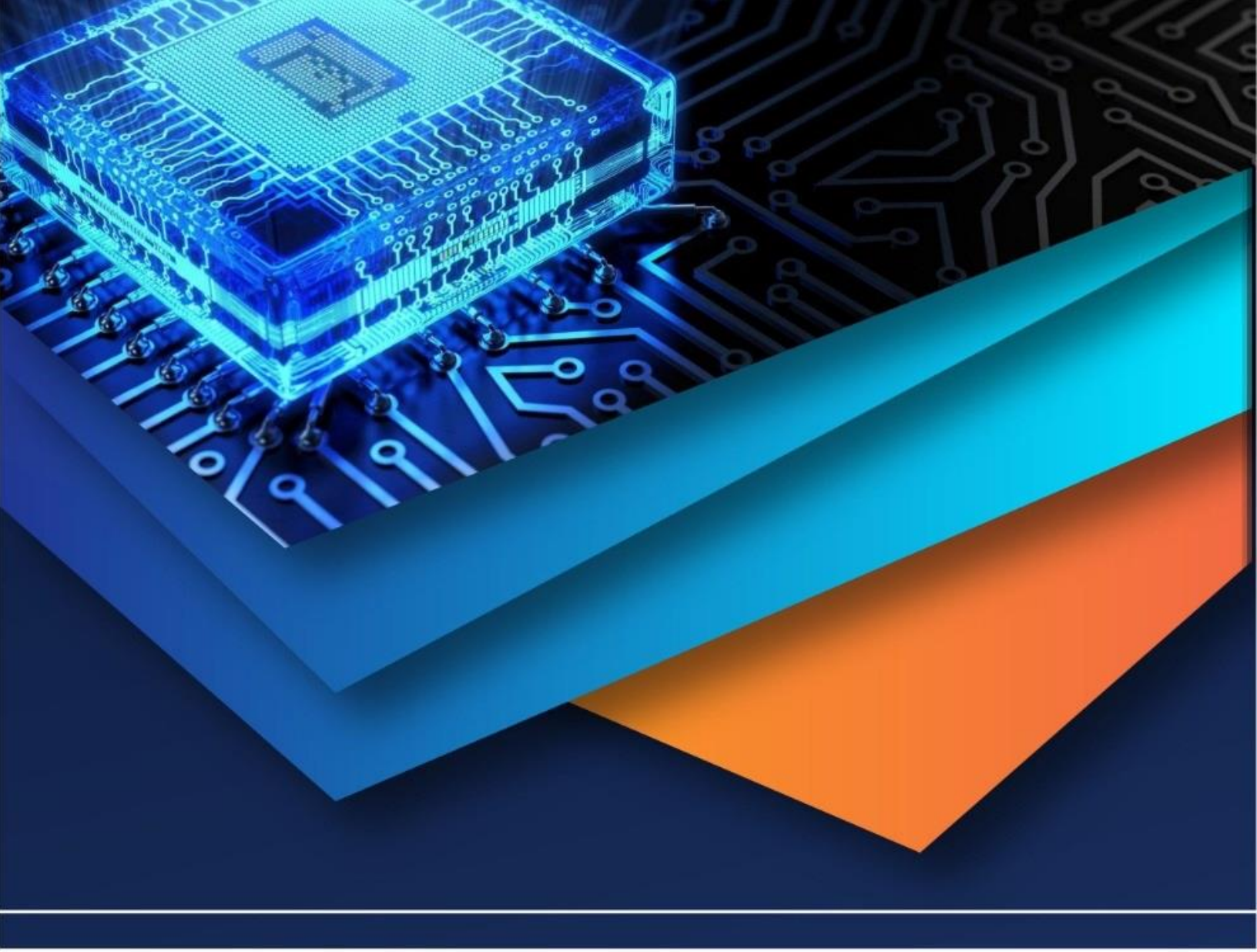
VI. CONCLUSION

In order to reduce the impact of malicious nodes in WSN and thus to make the communication more efficient, a new approach is proposed in this paper. In this proposed approach, increased QoS parameters are taken into consideration such as distance between nodes, trust factor, residual energy and hop count. Also, unlike defining the weight values statically as previous approach, the proposed approach has make the system automated for which GWO optimization algorithm is used. With the help of this optimization technique the weight values of the considered factors is determined efficiently. In order to demonstrate the efficacy of this proposed work, the simulation is carried out in MATLAB environment. In the simulation, the performance of the proposed approach is analyzed in terms of two different parameters i.e. network throughput and energy consumption. Also, the comparative analysis between proposed and traditional approaches is performed. From all the obtained results, it is demonstrated that proposed approach is more efficient than all other conventional approaches as it has high network throughput and low energy consumption values at different number of nodes.

REFERENCES

[1] M.A.M. Vieira, D.C. da Silva Jr., C.N. Coelho Jr., and J.M. da Mata., “Survey on Wireless Sensor Network Devices,” Emerging Technologies and Factory Automation (ETFA03), September 2003.
[2] L. Zhou and Z. Haas, “Securing Ad Hoc Networks,” IEEE Network Special Issue on Network Security, 13, 6, 24-30, November 1999
[3] C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Journal of Ad Hoc Networks, Elsevier, 2003
[4] J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil Attack in Sensor Networks: Analysis and Defense,” International Symposium on Information Processing in Sensor Networks, Vol. 1(2004)
[5] Y. Hu, A. Perrig, and D. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks,” IEEE INFOCOM, 2003
[6] W. Du, L. Fang, and P. Ning, “LAD: Localization Anomaly Detection for Wireless Sensor Networks,” the 19th International Parallel and Distributed Priocessing Symposium (IPDPS’05), April 3 – 8, 2005, Denver, Colorado, USA.
[7] B. Sun, K. Wu, and U. Pooch, “Secure Routing against Black-hole Attack in Mobile Ad Hoc Networks,” in Proceedings of Communications and Computer Networks, 2002.
[8] T. G. Dhanalakshmi ; N. Bharathi ; M. Monisha,“Safety concerns of Sybil attack in WSN” ,IEEE, International Conference on Science Engineering and Management Research (ICSEMR)2014.
[9] Shanshan Chen ; Geng Yang ; Shengshou Chen, “A Security Routing Mechanism Against Sybil Attack for Wireless Sensor Networks”, IEEE, International Conference on Communications and Mobile Computing, 2010.
[10] Shahrzad Golestani Najafabadi ; Hamid Reza Naji ; Ali Mahani, “Sybil attack Detection: Improving security of WSNs for smart power grid application”, IEEE, Smart Grid Conference (SGC), 2013.

[11] T. Khan et al., "A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks," in IEEE Access, vol. 7, pp. 58221-58240, 2019:
[12] Majid Alotaibi, “Security to wireless sensor networks against malicious attacks using Hamming residue method”, EURASIP Journal on Wireless Communications and Networking volume 2019
[13] Ahmed A, Bakar K A, et al. “Energy-aware and secure routing with trust for disaster response wireless sensor network”, J Peer-to-Peer Networking and Applications 2015;14(4):216-237
[14] J. Duan, et al., "An Energy-Aware Trust Derivation Scheme With Game Theoretic Approach in Wireless Sensor Networks for IoT Applications"
[15] J. Santhosh, G. Arulkumaran, P. Balamurugan, “Improved Energy Intrusion Detection System using Fuzzy System in Wireless Sensor Network”, International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-7 Issue-4S2, December 2018
[16] Chuanjun Yi , Geng Yang, Hua Dai, Liang Liu and Ning Li, “Public Key-Based Authentication and En-Route Filtering Scheme in Wireless Sensor Networks”, Sensors 2018, 18, 3829.
[17] Rathee, G.; Saini, H.; Singh, G. “Aspects of Trusted Routing Communication in Smart Networks”, Wirel. Pers. Commun. 2018, 98, 2367–2387.
[18] S. Misra, S. Roy, M. S. Obaidat and D. Mohanta, "A Fuzzy logic-based Energy Efficient Packet Loss Preventive Routing Protocol," 2009 International Symposium on Performance Evaluation of Computer & Telecommunication Systems, Istanbul, pp. 185-192.
[19] Tao Yang, et al., “A secure routing of wireless sensor networks based on trust evaluation model”, Procedia Computer Science 131 (2018) 1156–1163



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY