Shailendra Kumar Tiwari, 2022, 10:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

Genetic Algorithm Based Routing and Adamic Adar Trust for Secured IOT Network

Research Scholar Shailendra Kumar Tiwari, Department Of Computer Application, LNCT University, Bhopal, Madhya Pradesh,, India

Asscoiate Prof. Dr.Ravindra Kumar Tiwari Department Of Computer Science and Engineering,

Abstract- IOT devices ave plays an important role in daya to day life. So its network need lot of protection from attackers who may increase the load. This paper has developed a genetic algorithm based model that estimates the trust value of the nodes on the basis of social trust evaluation function adamic adar. At the same time network communication need packet transfer, hence each of such packets path is identify by the genetic algorithm. As IOT network is dynamic in nature, so genetic algorithm provides a good path in short time. Experiment was done on different artificial network conditions and results shows that proposed model has improved the work performance.

Index Terms - Sink hole attack, Gray Hole attack, Genetic Algorithm, Wireless Sensor Network, Trust Based Model.

I. INTRODUCTION

Networks has evolved as a result of recent advancements in wireless communication such as Bluetooth (WSN). A wireless sensor network (WSN) is made up of sensor devices that are powered by batteries and have computation, data processing, and communication capabilities. For a variety of applications, wireless networks offer a potential network infrastructure. The data collection and transmission are handled by the tiny wireless sensor nodes.

These randomly placed nodes, on the other hand, are vulnerable to assaults such as selective forwarding, flooding, and other types of attacks. These attacks have a direct impact on network performance while also probing network security. This paper presents an effective trust-based attack detection module for detecting denial of service attacks including selective forwarding and flooding [1]. To determine the packet forwarding behaviour from the sensor nodes, the proposed approach extracts and estimates multi-dimensional trust parameters. The battery energy [2] is consumed by sensing, listening, processing, transmission, and reception of packets, and because these processes are not scheduled optimally, the energy depletes at a faster pace, and the node dies. The loss of a node affects not only the sensing coverage area, but also the routing. Multi-hop routing is disrupted, and network reliability is reduced as a result of the communication holes produced in the network. Battery replacement for dead nodes is not possible due to the unattended nature of the system. In this case, conserving energy is the most effective strategy to extend the life of nodes and the network. WSNs are vulnerable to attacks such as message dropouts, message tampering, and denial of service through message flooding due to their wireless architecture.

The detection and mitigation of these attackers [3] is critical for the reliability of applications that use the sensor network. Implementing a higher-complexity security algorithm necessitates more energy [4] for processing at sensor nodes, which affects the node's life span. Because nodes are the network's routing medium, assaulting them destroys the network. Because routing is a trust-based procedure between nodes, attackers have a decent chance of disrupting the process [5]. Because these networks are typically constructed without prior design and are only used for a brief period of time, security investigations into

them are conducted individually. As a result, countermeasures must be implemented to defend the WSN from security assaults.

II.RELATED WORK

A Levenberg–Marquardt neural network (LMNN) is used in [6] to improve performance in terms of energy efficiency. Furthermore, a sub-cluster LEACH-derived methodology is developed in order to improve performance. The Sub-LEACH with LMNN surpassed its competitors in terms of energy efficiency, according to simulation data. Furthermore, the end-to-end delay was assessed, and the Sub-LEACH technique was shown to be the most effective among existing solutions. Furthermore, an intrusion detection system (IDS) based on the support vector machine (SVM) approach for optimal feature selection has been presented for anomaly detection.

An Energy Efficient Intrusion Detection System (EE-IDS) for IEEE 802.15.4-based WSNs has been proposed in [7] to detect and reduce the effect of wormhole attacks. Statistical Analysis/Methods: Using the enhanced watchdog system, the wormhole attack is identified. The optimal watchdog mechanism is a trust-based approach for determining the authenticity of all of the network's nodes. The suggested approach optimises the selection of watchdog nodes in order to consume less energy than previous approaches. The three primary variables of trustworthiness, packet delivery ratio, and end-to-end delay are also used to detect wormhole attacks. Findings: The proposed EE-IDS is put through its paces in thorough simulations, taking into account both static and mobile models, before being compared to existing IDS for detecting wormhole assaults.

Four types of attacks were identified in [8] by Xu et al., and specific methods to recognise them were created. The first strategy is based on signal strength, because signal strength might fluctuate abnormally during an attack. The Carrier sense intervals are the second method. During an attack, the Carrier sense intervals are widened. Controlling packet arrival rates is the other option. These values, of course, are insufficient on their own. Under certain circumstances, these ratios may exhibit unexpected changes even if there is no attack on existing nodes in the network. To detect a node replication assault, the author presented a secured Ant Colony Optimization (SACOP) based on a trust sensing model in [9]. To begin, the malicious node in the clustered network is identified by estimating the node's trust value using direct and indirect trust evaluation models. Second, the ant colony routing algorithm is used to identify the secure best path for data forwarding by using probability to select the next hop node. Energy expenditure among all nodes is balanced since the likelihood is determined using residual energy, trust, and pheromone levels.

III. PROPOSED METHODOLOGY

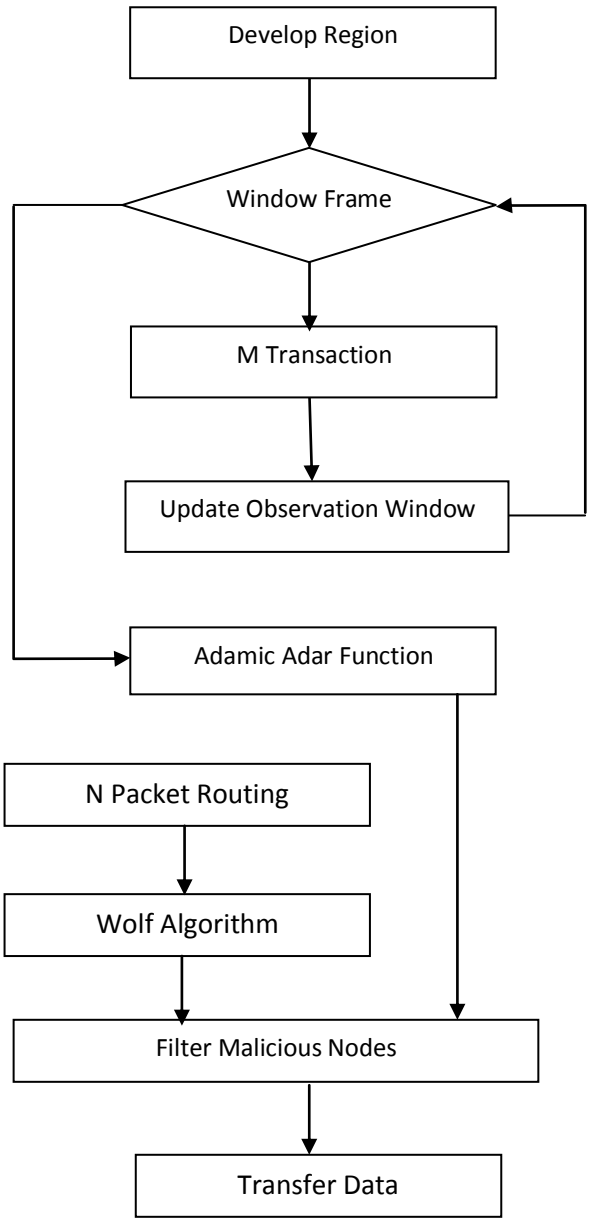

Fig.1 Wolf and Adamic Adar based proposed model flow diagram.

Whole work was divide into two section first was to generate the trust and other was to generate path. In first section a observation window was create to find the trust of the wireless nodes. Working steps of model is shown in fig. 1. Second section finds the route from the source to destination in wireless network with an objective of optimizing the channel utilization.

Develop Virtual Region and Place Node position

This work start with placement of N number of nodes and in an MxM region. In order to assume the initial stage of the network some energy need to be set for each node in the network [10, 11]. Each link between node have fix spectrum channel to communicate.

Observation Window: It's a centralized data storage in manage by fusion center where each transaction related information was maintain. fusion center store node specific transaction count, successful transaction count, failed transaction count and transaction node ID. This bridge store data as per window. After completion of window trust value of the nodes were evaluate as per the trasaction behavior done by node in window. Wireless radio needs a fix size time. So in one window more than one node may initiate a transaction.

Adamic-Adar

This is similar to Resource Allocation, but the denominator of the fraction is the log of the degree of the shared neighbor, rather than simply the degree [19].

$$Aa = \sum_{x \in a \cap b} \frac{1}{\log(d(x))} \text{----Eq. 1}$$

Where d(c) is the sum of the of the degrees of vertices adjacent to both a and b. d(x) is degree of x and y.

Each node in the observation matrix has a trust value. This value may increase or decrease as per the behavior of the nodes in form of transaction success. Storage tables were used to evaluates this value of work. So let successful transaction count between i, j node is represent by Ts_{ij} and total number of transaction represent by Tt_{ij} [45]. Estimation of this trust done by:

$$D_{ij} = \sum_{i,j=1}^{n} Aa_{ij} \text{----Eq. 2}$$

Above eq. gives n number of trust value for each node, but behaviors of node with node may be different. As malicious node provide good service to some node and poor service to others. This function takes all Adamic-Adar value of a node and generates a single value of the node as per different behavior operations done by node with other nodes.

Generate wolfs

Wolfs are group of chromosome and a chromosome is possible solution of path [20]. So a wolf is a vector of e number of elements, where e is number of possible nodes in the path. So if w number of wolfs generate then WP is wolf population matrix. Selection of n number of feature in vector done by random value generator function Gaussian. As per weblog pattern wolf element values select by Gaussian function randomly.

$$WP \leftarrow \text{Generate\_Wolf}(w, e, n, S, R) \text{ ----Eq. 3}$$

Fitness Function

Each wolf were rank as per hunting skill and assign in sub group. So evaluation of hunting skill done by fitness value. Wolf element vector pass in the fitness function for finding the value sum of each element in the vector. In order to find a good route for transferring D fitness value of each route help to select a path. In this work two objectives were taken for getting optimum path first was spectrum utilization and other was energy dissipation. Eq. shows estimation of energy for the path as per nodes and its distance from other.

$$F_{h,e} = \sum_{n=1}^{P'} (E_t^n + E_r^n) \text{ ----Eq. 4}$$

P′ is number of nodes in route P of habitat h from H. Eq. 6 shows estimation of spectrum utilization for the path as per nodes.

$$F_{h,s} = \sum_{n=1}^{P'} (S^n - D) \text{ ----Eq. 5}$$

Final fitness value was estimate by summation of energy and spectrum value from eq. 5, 6.

$$H_h = \beta_1 F_{h,s} + \beta_2 F_{he} \text{----Eq. 6}$$

Where β_1 and β_2 are constant to normalize values at same scale because energy loss value is very low as compared to spectrum utilization.

This fitness H value is hunting parameter in the work to rank or assign a wolf in sub category of alpha,

beta, delta and gamma. H is hunting skill value of wolf.

Update Wolf position

Once H value obtain by fitness function then sort H in deseeding order and find wolf sub category. First sorted fitness value is consider as alpha wolf, then next m/3 consider as beta wolfs and next m/3 wolfs consider as delta wolfs [20, 21]. Position of each wolf were modified by the Eq 7 to 9.

$$A=Pos-Ct*(Pos/Mt)*r- Pos- Ct*(Pos/Mt)- \text{----Eq. 7}$$

$$D_w=c.* (Delta\_Wolf-Alpha\_Wolf)\text{----Eq. 8}$$

$$X_1=Delta\_Wolf -A.*abs(D_w) \text{------Eq. 9}$$

Where Pos is position of wolf range{0,1,2,3} from Prey, c obtain by Pos*r and r is random number range from {1 to n}.

Similarly

$$D_w =c.* (Beta\_Wolf-Alpha\_Wolf)\text{-------Eq.10}$$

$$X_2= Beta\ \_Wolf -A.*abs(D) \text{--------Eq. 11}$$

$$X_3=Alpha\_Wolf\text{--------Eq. 12}$$

Final position shifting value estimate by Eq. 12

$$\mathbf{X} = \frac{\mathbf{X_1}+\mathbf{X_2}+\mathbf{X_3}}{\mathbf{3}}\text{--------Eq. 13}$$

Crossover

Genetic algorithm success depends on change of chromosomes, hence as per X values number of random position value of wolfs were modified. This operation was not done in alpha wolf. In this step each wolf X number of positions were modified randomly as per alpha wolf element set. These wolf were further test for hunting skill and compared its hunting skill with parent wolf if child wolf has better values then remove parent otherwise parent will continue. After this step if maximum iteration steps occur then jump to filter feature block otherwise evaluate fitness value of each wolf.

New wolf fitness value is better than parent wolf then replace parent with new wolf in the population this is population updation in the work. After this population update perform same operation with other wolf in beta, delta and omega category. Once all wolf get update then check for iteration count if count is less than max iteration then jump to fitness value evaluation of updated population.

Hunting Rule

After t number of iteration steps (fitness function, wolf position update, crossover) final wolf population pas through fitness function and best fitted wolf is consider as alpha wolf [21]. This wolf element nodes are predicted possible path to transfer data packet.

Filter Malicious Nodes

Path generate by wolf algorithm is further scanned by the system to identify malicious node from the path. As per Adamic Adar trust value nodes having low value is consider as the malicious and other are consider as the real node. If path have malicious node then packet is not transfer on that path and it saves the spectrum and energy of the network.

IV.EXPERIMENT AND RESULTS

Experimental work was done on MATLAB platform having machine of I3 processor and 4GB RAM. For comparison existing model proposed in SACR [22] was implement on MATLAB and run in same environment. To proof the dynamic adoptability of work experiment was done on different conditions, such as number of nodes, region size,, packets movement [16, 17]. Evaluation parameters were taken from [23, 24].

Results

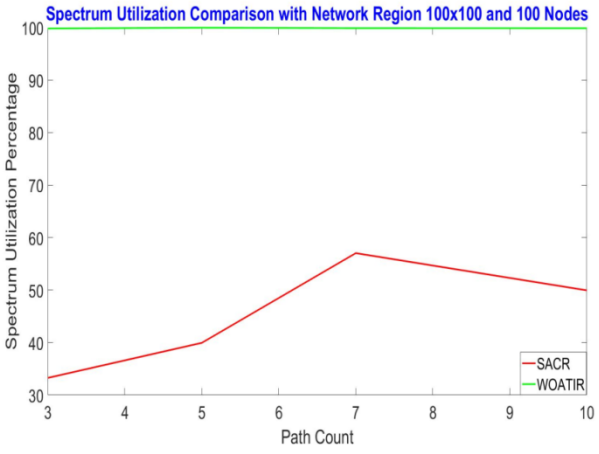

Fig. 2 Spectrum utilization based comparison of path count routing algorithms.

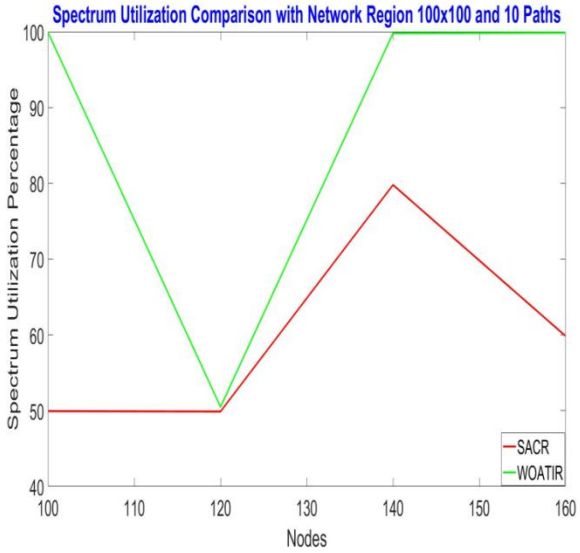

Fig. 3 Spectrum utilization based comparison of node routing algorithms.

Fig. 2 and 3 shows the spectrum utilization percentage of the IOT routing models. Table shows that WOATIR model is better as compared to SACR [22]. It was found that with increase of network area spectrum utilization get decreases. Impact of number of route in same set of nodes do not affect the spectrum utilization.

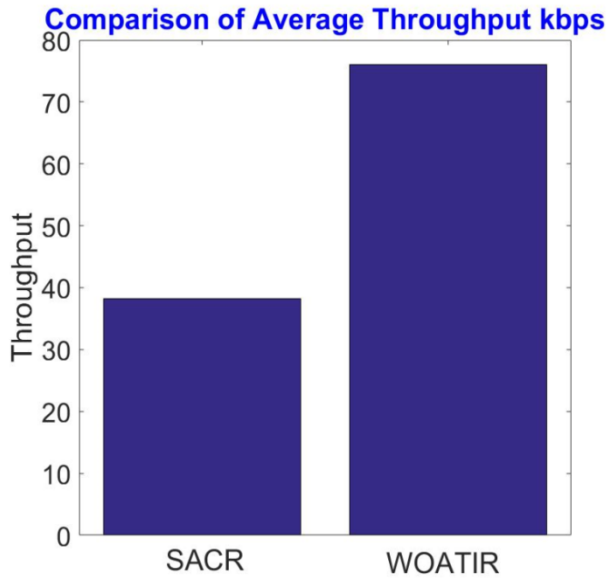

Fig. 4 Average throughput based comparison of routing models.

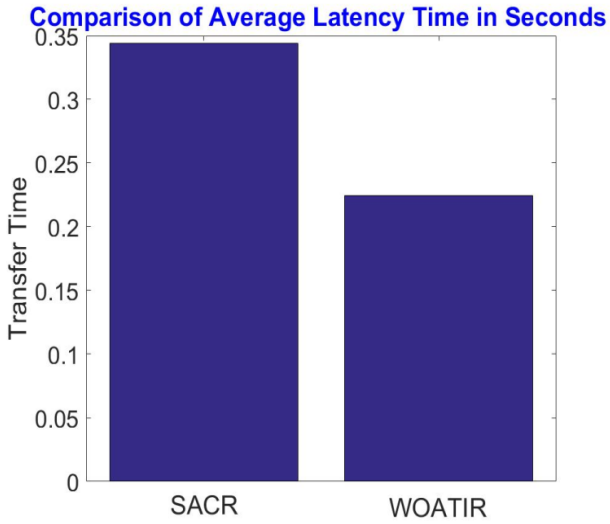

Fig. 5 Average transfer time based comparison of routing models.

Fig. 4 and fig. 5 shows that transfer time of the model proposed by this paper is more efficient as compared to SACR. Use of wolf genetic algorithm in the model for path node selection has increases the work efficiency. Alpha, Beta concept of wolf algorithm directly affect the node selection criteria of the work. It was found that with increase of network area spectrum utilization get decreases. Impact of number of route in same set of nodes do not affect the spectrum utilization.

V.CONCLUSION

Wireless radio network increase spectrum as non-licensed users get chance to transfer there data. To achieve spectrum utilization objective genetic algorithm wolf Optimization was used. Genetic algorithm generate dynamic path as per node positions and spectrum channel. This work apply wolf hunting for finding end to end path. Further paper evaluate Adamic Adar trust value help work to identify malicious node and stop packet routing in malicious path, this increase channel utilization of the work. Hybrid combination of trust evaluation and routing algorithm has increases the IOT performance. Experiment was done on different number of secondary nodes for various possible links. Results were compared with previous existing approach and it was found that WOATIR has low transfer time values as compare to the previous approaches work.

REFERENCES

1. Karthikeyan, T., V. Brindha, and P. Manimegalai. "Investigation on Maximizing Packet Delivery Rate in WSN Using Cluster Approach." Wireless Personal Communications 103.4 (2018): 3025-3039.
2. Chowdary, Krishna, and K. V. V. Satyanarayana. "Malicious Node Detection and Reconstruction of Network in Sensor Actor Network." Journal of Theoretical & Applied Information Technology 95.3 2017.
3. Gummadi, Annapurna, and K. Raghava Rao. "EECLA: Clustering And Localization Techniques To Improve Energy Efficient Routing In Wireless Sensor Networks." Journal of Theoretical & Applied Information Technology 96.1 2018.
4. Zhang T, Zhang D, Qiu J, Zhang X, Zhao P, Gong C. A kind of novel method of power allocation with limited cross-tier interference for CRN. IEEE Access. 2019.
5. Montoya M, Bacles-min S, Molnos A, Fournier J, inventors; Commissariat al Energie Atomique et aux Energies Alternatives, assignee. Transmission/reception device with wake-up radio resistant to attacks by denial of sleep. United States patent application US 16/054,291. 2019 Feb 7.
6. Mohit Mittal, Rocío Pérez de Prado, Yukiko Kawai, Shinsuke Nakajima and José E. Muñoz-Expósito. "Machine Learning Techniques for Energy Efficiency and Anomaly Detection in Hybrid Wireless Sensor Networks". MDPI Energies 2021.
7. Wireless Sensor Networks using Intrusion Detection System G. Jegan and P. Samundiswary. "Wormhole Attack Detection in Zigbee". Indian Journal of Science and Technology, Volume: 9, Issue: 45 2016.
8. W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '05), pp. 46–57, Chicago, Ill, USA, May 2005.
9. S. Anitha, P. Jayanthi, K. Lalitha and V. Chandrasekaran. "Secured Ant Colony Optimization based on Energy Trust System for Replica Node Attack Detection". International Journal on Emerging Technologies 11(2): 2020.
10. Dr. Shweta Singh, Jamvant Omkar. "Wireless Sensor Node Energy Optimization by Packet Routing and Clustering". Ijsret.com IJSRET Volume 7 Issue 4, July-Aug-202.
11. Pragya Richhariya, Dr. Shailja Sharma. "A Survey on Cloud Virtual Machine Management Techniques and Features". ijset.in IJSET, vol 9 issue 42021.
12. T. Sorensen. A method of establishing groups of equal amplitude in plant sociology based on similarity of species content and its application to analyses of the vegetation on Danish commons. Biol. Skr., 5, 1948.
13. Mahesh Patidar, Dr. V. B. Gupta, Seema Patidar. "PHRASE BASED USER SENTIMENT DETECTION USING FROG JUMP GENETIC ALGORITHM ". International Journal of Advanced Research in Engineering and Technology (IJARET) Volume 11, Issue 12, December 2020.
14. Dinh-ThuanDo, Anh-TuLe, Narayan C.Debnath. Signal-to-Interference-Plus-Noise Ratio, Security and Privacy Issues in IoT Devices and Sensor Networks, 2021.