www.ijecs.in
*International Journal Of Engineering And Computer Science*
*Volume 11 Issue 06June 2022, Page* **No.25535-25542**
*ISSN: 2319-7242 DOI: 10.18535/ijecs/v11i06.4671*

# Artificial Immune Algorithm and Adamic Adar based Wireless Sensor Network Optimization

M. Tech. Scholar Shireen Fatima[1]
Dr. Shaheen Ayyub[2]
Department Of Computer Science And Engineering
Technocrats Institute Of Technology, Bhopal Mp, India

Email Address: shireenfatema30@gmail.com

**Abstract:**

As different types of dynamic networks are developed by easy means of devices, people start using them for various means. Such vulnerable networks are easy places to attack and perform malicious activities. This work develops a model that can generate a path from source to destination in a dynamic node environment without prior information. Path generation artificial immune genetic algorithms will be used, as this algorithms find a good path in a short time. In order to detect the malicious activity, such nodes need to be identified. Hence identification of attackers nodes is done by trust model where Adamic Adar trust function finds the mutual trust value of node as per past performance of nodes.

Index Terms— Adhoc Network, Wireless Sensor Network, Communication Attacks, Virtual machines.

## Introduction:-

The Internet of Things (IoT) is a critical stage in the evolution of the information age. Individuals, and even governments, are paying more attention to social information as it continues to develop. The Internet of Things is viewed as the next trillion-dollar market opportunity [1] due to massive market demand and vast development opportunities. Many governments throughout the world now place a high value on the Internet of Things. The Internet of Things (IoT) is an open, intelligent system in which the majority of nodes are unmanaged and susceptible to malicious attacks [2]. In another approach, the external environment might harm IoT devices. For example, IoT nodes with a single function and low computer resources can easily infiltrated and turned into malevolent nodes that conduct internal attacks with legal status and pose serious security issues [3].Multi-hop routing is used by all other nodes to send data to the data collection node [1, 2]. The security of data collecting, on the other hand, is a critical problem [4]. Many IoT devices can be joined to the network on their own because of the network's openness [5]. As a result, rogue IoT devices will obstruct conventional data collecting. The black hole attack [6] is the most common. Malicious nodes drop all packets forwarded by themselves in such an attack

to destroy the data gathering [7]. The other is a sophisticated attack known as selective forwarding attack (SFA) [8]. Malicious nodes in SFA attacks do not simply discard data packets into a black hole, but rather selectively drop packets of selected nodes [8]. As a result, the wireless network has a certain packet loss rate. Malicious nodes can selectively drop some packets to avoid being identified, allowing them to launch assaults at a vital time to cause longer-term and more severe harm [8]. Data consistency is extremely important for data-driven applications. Insecure behaviours, such as data interception by malicious nodes, can result in packet loss, causing the control centre to make the wrong decision in the event of a data shortage, resulting in catastrophic losses.Network assaults on the Internet of Things will not only inflict material harm, but also pose a threat to human life. As a result, developing a security plan for the IoT environment is very critical and important. In any IoT implementation, privacy, security, and trust are critical [2], [3], [4], [5]. In IoT networks, trust can be divided into two categories: (1) trust in the interactions between network entities, and (2) trust in the network itself [4]. This research focuses on assessing an IoT node's trustworthiness, and in particular, techniques allowing a user to assess the trustworthiness of an IoT node's pass.

**II. Related Work:**

Yu, Jia, and Tao devised a new quantitative method for assessing IoT trust. Integrity, Delay, Packet consistency, Repetition rate, and forwarding capacity were utilized to test the trustworthiness of a node in this approach. To synthesize and deduce trust, Shannon entropy and D-S theory are used to determine each and every trust factor [9].

In the Internet of Things, Hellaoui, Bouabdallah, and Koudil devised a trust adaptive security system (TAS-IoT). The trust evaluation in this approach is based on three factors: personal experience, observations, and recommendations. An evaluating node validates the authenticity of packets originating from the evaluated node under Own Experience. If the packet is authenticated, the node is trustworthy; otherwise, the node is malicious. Then, under suggestion, another neighbor node recommends the nodes' trustworthiness [10].For the Internet of Things, D. Chen and G. Chang proposed a Trust and Reputation mode (TRM-IoT). End-to-end packet forwarding ratio (EPFR), Average Energy Consumption (AEC), and Packet Delivery Ratio were used to evaluate trust in this method (PDR). This method also assessed local and global trust, modeling them using a fuzzy reputation model [11].

M. Elkhodr and B. Alsinglawi introduced a new trust management solution that provides a trust establishment method among IoT communication devices, focusing on data provenance. This approach verifies the data's freshness, originality, traceability, and accuracy using data provenance [12].

Contrast, a novel trust evaluation methodology based on everyday life inspiration, was proposed by V. Suryani, S. Sulistyo, and W. Widyawan. ConTrust evaluates trust based on two factors: historical reputation and present trust rating. The reputation based on history denotes previous object encounters. The nodes are categorized as Very Trusted, Trusted, Very Untreated, and Untreated using a trust rating. Contrast, on the other hand, did not pay attention to energy consumption at the node level [13].

V. M. Carolina and H. K. Joo [14] introduced a new

trust management strategy to mitigate on-off assaults to a multiservice IoT. This approach analyses the behavior of any node by using information collected from directly connected links between nodes [14] [15].

The defection of three insider assaults, black hole, sink hole, and wormhole, was studied by K. N. Ambili and J. Jose. For detection, a distributed trust management approach is proposed. The current trust score is compared to the previous trust score, and a decision is made whether or not to include or exclude a node [18].

Based on the Improved Bacterial Foraging Optimization (IBFO) method, P. K. Reddy and R.S. Babu proposed an Optimal Secure and Energy Aware Protocol (OSEAP) for IoT. The Fuzzy Cmeans method is used for clustering, while IBFO is used for cluster head selection in this approach. Group key distribution is also used to increase security. IBFO [19] is used to determine the best key pick.

## I. Proposed Methodology :

Whole work was divide into two section first was to generate the trsust 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. 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 transaction 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 $Tt_{ij}$ [5]. Estimation of this trust done by:

$$d_{ij} = \sum_{j=1}^{n} Aa_{ij} \text{----Eq.}$$

Above eq. gives n number of trust value for each node, but behaviors of node with node may be different.

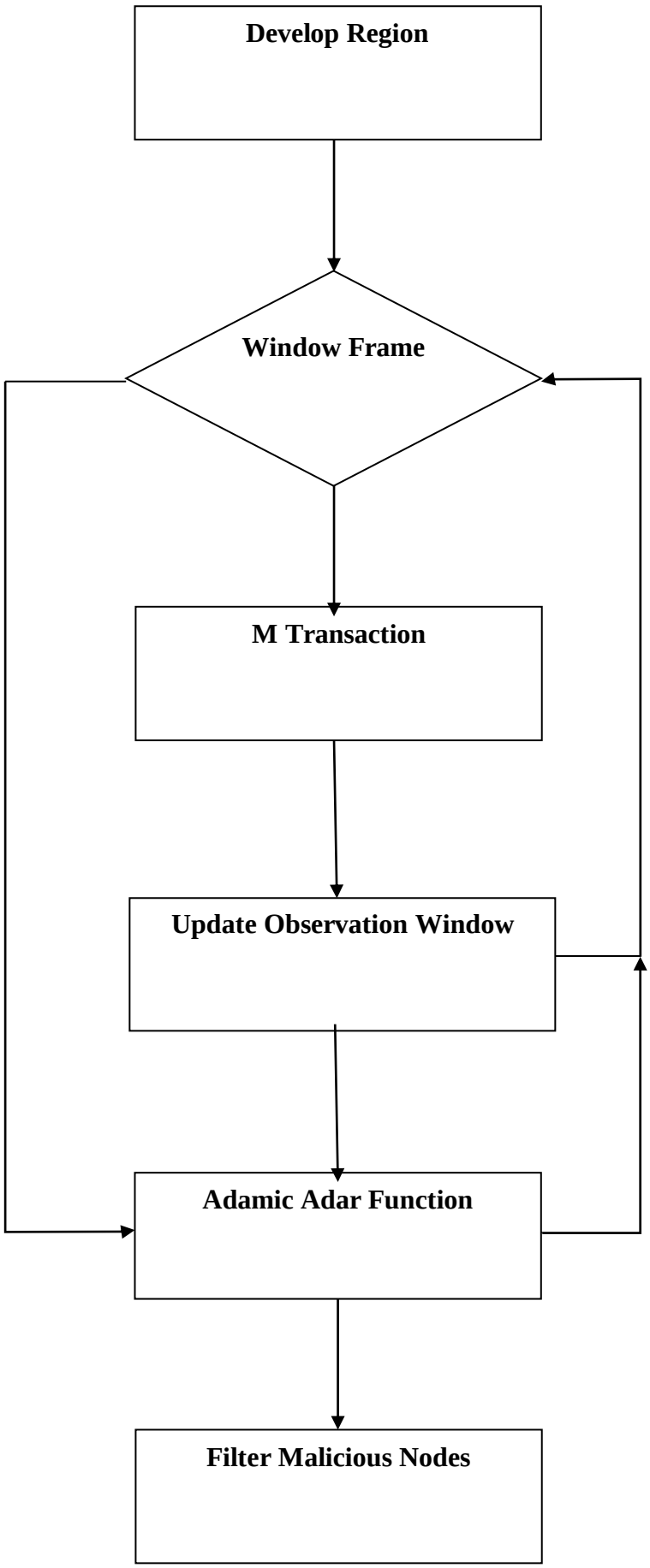


**Fig. 1 Proposed Work Training Module.**

**Generate Antibodies:**

Here assume some chromosome set that are the combination of different node as per link starting and ending node. So chromosome have p links where each link has some set of nodes Ch={$L_1$, $L_2$,…..$L_p$}. So m number of antibodies A, is a collection represent initial population.

**A←Generate_Antibody(m)**

**Affinity:**

Affinity of antibody present in the population were estimate by Signal-to interference plus-noise ratio (SINR). This is used to measure the quality of communications [12]. For a link (*i*; *j*) on spectrum channel *m*, its SINR can be calculated as follows:

$$SINR_{ij}(m) = \frac{h_{ij}P_i}{\sigma^2 + \sum_{(a,b)\in I(m)} h_{aj}P_a}$$

where *pi* denotes transmission power of sender *i*. In this paper, assume that the transmission power of all links is at the fixed level. *hij* represents the channel gain between sender *i* and receiver *j*, which can be denoted by $k/d_{ij}^{\sigma}$ . Here *k* is the path loss constant. *dij* is the distance between *i* and *j*. $\sigma^2$ is the path loss exponent. _2 is the thermal noise that can be considered as a constant, and sigma notation presents the aggregate interference at receiver *j*, which is generated by the links transmitting concurrently on the current spectrum channel. Here, *I* (*m*) presents the set of links sharing spectrum channel *m*. To guarantee the effective link transmission, each intended signal should be successfully decoded at the receiver. For the SINR, there exists a desired value denoted by β, which indicates the threshold of successful decoding. So, if link (*i*, *j*) intends to access spectrum channel *m* for its transmission, the

constraint is satisfied as follows:

$$SINRij(m) > \beta$$

For link ($i$; $j$), the efficient link transmission opportunity $Tij$ is de_ned as follows:

$$Tij = \min(Ti; Tj)$$

$Tij$ evaluates the transmission opportunities on both sides of link ($i$; $j$). If the link transmits the data of _ow $f$ on spectrum channel m, the maximum data rate that the link can maintain is denoted by the following:

$$Rij(m) = Tij \text{ x } Cij(m)$$

Thus, due to the constraint of the resource competition, link ($i$; $j$) only applies a portion of its link capacity for the flow transmission.

$$F_{1\_max} = \max(Rf)$$

$$F_{1\_min} = \min(Rf)$$

$$F_{2\_max} = \max(|L|/|M|)$$

$$F_{2\_min} = \min(|L|/|M|)$$

if (F1_max-F1_min)Not Equal 0

$$D = \sum_{k=1}^{2} \frac{R_n + R_{n+1}}{F_{k\_Max} - F_{k\_Min}}$$

EndIf

$$D = D + \sum_{k=1}^{2} \frac{(|L|/|M|)_n + (|L|/|M|)_{n+1}}{F_{k\_Max} - F_{k\_Min}}$$

Fitness ←Sort(D)

**Cloning:**

As per affinity value of each antibody in population, best solution $A_b$ is obtained. As per best antibody $A_b$ feature set few status were randomly change. By change in feature status present to absent or absent to present cloning of the model is done.

A←Cloning($A_b$, A)

**Hyper Mutation:**

The clones are then subjected to a hyper mutation procedure, in which they are mutated in inverse proportion to their affinity, with the best antibody's clones being mutated the least and the poorest antibody's clones being mutated the most. The clones and their original antibodies are then analyzed, and the best N antibodies are chosen for the next iteration. It's possible for the mutation to be uniform, Gaussian, or exponential.

A←Hypermutation(A)

**Population Updates:**

Accept Xnew if it gives a better function value. Once hyper mutation phase is over then check for the maximum iteration if iteration not reach to the maximum value then GOTO step of Affinity else stop learning and the best solution from the available population is consider as the final centroid of the work.

**Final Path:**

Proposed work gives final path set which can be known as best chromosome in the available population. As per obtained path each node in the path was further check by trust value. In this check if trust value of a node crosses a threshold (0.5) value then consider it as real node otherwise malicious node. So if a path have malicious node in the route then packet was not transfer in the route. Based on trust value decision of malicious node was taken.

## II. Experiment and Results

**Table 1 Comparison of secured packet routing algorithms spectrum utilization.**

| Spectrum Utilization | | | | |
|---|---|---|---|---|
| **Network Dimension** | **Nodes** | **Links** | **AIRWSN** | **Previous Work** |
| **100x100** | **50** | **5** | **60.3995** | **20.3996** |
| **100x100** | **75** | **5** | **80.1999** | **40.1992** |
| **100x100** | **100** | **5** | **80.1982** | **20.1998** |
| **100x100** | **100** | **10** | **60.3994** | **10.4993** |
| **100x100** | **100** | **20** | **65.3494** | **30.2328** |
| **100x100** | **100** | **30** | **47.1993** | **27.1659** |

Table 1 shows that proposed model AIRWSN has improved the spectrum utilization. It was found that use of artificial immune algorithm for routing has improved the channel utilization by 62.23% as compared to previous model proposed in [21].

**Table 2 Comparison of secured packet routing algorithms throughput.**

| Network Dimension | Nodes | Links | AIRWSN | Previous Work |
|---|---|---|---|---|
| **100x100** | **50** | **5** | **79.9736** | **39.9801** |
| **100x100** | **75** | **5** | **87.9955** | **47.9680** |
| **100x100** | **100** | **5** | **89.9101** | **35.9805** |
| **100x100** | **100** | **10** | **89.9536** | **41.9558** |
| **100x100** | **100** | **20** | **94.4498** | **41.9411** |
| **100x100** | **100** | **30** | **87.9454** | **60.6126** |

Table 2 shows throughput of channel by use different routing algorithm. Paper has improved the throughput by use of adamic adar as malicious nodes routes are identified and such packets are not delivered. This precaution reduces the channel waste. It was found that proposed FLRWSN has improved the throughput by 49.37% as compared to previous model proposed in [21].

**Table 3 Comparison of secured packet routing algorithms transfer time.**

| Transfer Time in Seconds | | | | |
|---|---|---|---|---|
| **Network Dimension** | **Nodes** | **Links** | **AIRWSN** | **Previous Work** |
| **100x100** | **50** | **5** | **102.1097** | **129.1617** |
| **100x100** | **75** | **5** | **94.0571** | **119.8730** |
| **100x100** | **100** | **5** | **98.3587** | **153.985** |
| **100x100** | **100** | **10** | **110.4607** | **130.8079** |
| **100x100** | **100** | **20** | **84.1627** | **101.1411** |
| **100x100** | **100** | **30** | **91.6427** | **102.9175** |

Transfer time of the models shown in table 3. It was obtained form table 3 that proposed AIRWSN model has improved this parameter values.

**Table 4 Comparison of secured packet routing algorithms execution time in seconds.**

| Execution Time in Seconds | | | | |
|---|---|---|---|---|
| **Network Dimension** | **Nodes** | **Links** | **AIRWSN** | **Previous Work** |
| **100x100** | **50** | **5** | **0.9233** | **1.194** |
| **100x100** | **75** | **5** | **1.22** | **1.26** |
| **100x100** | **100** | **5** | **1.53** | **1.1409** |
| **100x100** | **100** | **10** | **2.1432** | **2.5905** |
| **100x100** | **100** | **20** | **2.0083** | **2.7916** |
| **100x100** | **100** | **30** | **3.6551** | **4.1608** |

Algorithm routing time for the packet routing increases with increase in number of paths, as routing algorithm has to run for each path. Artificial immune algorithm takes less time as compared to previous model by 12.61%. Average time for finding the path of proposed model FLRWSN is sec.

## III. Conclusion:

Wireless Sensor networks are dynamic in nature this feature make a wide range of application in different area. As vulnerable nature of network is open for malicious nodes to attack. In order to make a secured communication this paper has applied a Adamic Adar model that nodes trust. As per node trust value secured routes were identified by the use of artificial immune algorithm. Experiment was done on different environmental situations of region size variation, number of nodes and paths. Comparison of proposed model was done on different evaluation parameters and results shows that proposed AIRWSN has improved the spectrum utilization by 62.23%, throughput by 49.37% and reduced the execution time by 12.61%. In future scholar can implement this work in under water environmental conditions.

## References:


1. Liu Y, Dong M, Ota K, Liu A (2016) ActiveTrust: secure and trustable routing in wireless sensor networks. IEEE Trans Inform Forensics Secur 11(9):2013
2. Wang T, Luo H, Zeng X, Yu Z, Liu A. Sangaiah A. (2020) Mobility based trust evaluation for heterogeneous electric vehicles network in smart cities, IEEE Trans Intell Transp Syst.
3. Wang T, Cao Z, Wang S, Wang J, Qi l, Liu A, Xie M, Li X. (2020) Privacy-enhanced data collection based on deep learning for internet of vehicles. IEEE Trans Ind Inform 16(10):6663–6672
4. Wang H, Ma S, Dai H. N, Imran M, Wang T. (2020). Blockchain-based data privacy management with nudge theory in open banking. Futur Gener Comput Syst, 110, 812–823
5. Li T, Liu W, Wang T, Zhao M, Li X, Ma M (2020) Trust data collections via vehicles joint with unmanned aerial vehicles in the smart internet of things. Trans Emerg Telecommun Technol.
6. Zhuo C, Luo S, Gan H, Hu J, Shi Z (2019) Noise-Aware DVFS for Efficient Transitions on Battery-Powered IoT Devices. IEEE Trans Comput Aided Des Integr Circuits Syst 2019.
7. Liu A, Zheng Z, Zhang C, Chen Z, Shen X (2012) Secure and energy-efficient disjoint multi-path routing for WSNs. IEEE Trans Veh Technol 61(7):3255–3265

8. Xiao B, Yu B, Gao C (2007) CHEMAS: identify suspect nodes in selective forwarding attacks. J Parallel Distributed Comput 67(11):1218–1230
9. Y. Yu, Z. Jia, W. Tao, B. Xue, and C. Lee, “An efficient trust evaluation scheme for node behavior detection in the internet of things”, Wireless Personal Communications, Vol. 93, No. 2, pp. 571–587, 2017.
10. H. Hellaoui, A. Bouabdallah, and M. Koudil, “TAS-IoT: Trust-Based Adaptive Security in the IoT”, In: Proc. of the 41st IEEE Conf. on Local Computer Networks, Dubai UAE, pp. 599–602, 2016.
11. D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, “TRM-IoT: A trust management model based on fuzzy reputation for internet of things”, Computer Science and Information Systems, Vol. 8, No. 4, pp. 1207-1228, 2011.
12. M. Elkhodr and B. Alsinglawi, “Data provenance and trust establishment in the Internet of Things”, Security and Privacy, pp. 1- 11, 2020.
13. Suryani, S. Sulistyo, and W. Widyawan, “ConTrust: A Trust Model to Enhance the Privacy in Internet of Things”, International Journal of Intelligent Engineering and Systems, Vol. 10, No. 3, pp. 30-37, 2017.
14. L. M. Carolina and H. K. João “Mitigating On-Off Attacks in the Internet of Things Using a Distributed Trust Management Scheme”, International Journal of Distributed Sensor Networks, Vol. No., pp. 1-8, 2015.
15. Y. Chae, L. C. DiPippo, and Y. L. Sun, “Trust management for defending on-off attacks”, IEEE Transactions on Parallel and Distributed Systems,