Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Detection and Prevention of Wormhole Attacks in Wireless Data Network Using Smart Neighbour Discovery Algorithm

Udeani Ifeanyi Damian*, Prof. Onoh Greg Nwachukwu**

Department of Electrical and Electronics Engineering, Enugu State University of Science and Technology

Email: ifeanyiudeani@gmail.com

----------**********----------

Abstract:

This research presented the detection and prevention of wormhole in wireless data network using smart Neighbour Discovery Algorithm (NDA). The study performed empirical data collected from a wormhole attacked network and then developed a neighbour discovery algorithm to solve this problem using structural and mathematical modelling method. The algorithm was implemented with simulink and tested. The result showed that the NDA was able to detect wormhole on the network based on the variation of energy level and then isolate from the network. From the result it was observed that the average throughput with the NDA was 92.50% as against 56.940%. The percentage improvement recorded with NDA is 35.56%. The result when compared with the characterized testbed showed that the quality of service indicators achieved better results with the NDA.

Keywords: **Wormhole, Neighbour Discovery Algorithm, Wireless Network, Energy Level, Simulink**

----------**********----------

I. INTRODUCTION

In wireless data network, wormhole attack is considered as one of the most essential formidable security attacks. It is also considered as a network layer attack, launched by venomous nodes for generating tunnels for packet data transfer through those tunnels.

The attackers can use outside band channel, more power transmission, packet relay or binding technique to pass the packets to these colluding nodes. This process makes an illusion, that the nodes which are multi hops apart are immediate neighbours. These wormhole nodes can also create a tunnel even for those packets which are not the part of them. Due to this wireless network nature it is possible that the packets can overhear. The wormhole or the tunnel creates a path that is much smaller in size than that of the original route and thus legitimate nodes believe the path through these types of nodes as the smallest path. This hallucination can be considered in future to degrade, disrupt, or examine the traffic stream in this network. The attack is equally harmful for both proactive and reactive protocols. It is possible that the attacker can execute this tunnelling honestly and assuredly and no harm is done. The attacker literally provides a useful service in connecting the network more systematically. However, the wormhole gives a strapping position to the attacker as juxtapose to other nodes, and the attacker can misemploy this position. The intruders can at any time employ the link as they want. Since the wormhole attack involves off-channel transmission of data, it is very difficult to be detected by the nodes participating in the wireless data network. This results in rendering the network fragile in terms of security and confidentiality.

To solve this problem, many solutions have employed machine learning solutions, encryption, fuzzy logic, genetic algorithm, etc. (Mahendra et al., 2019; Shruti et al., 2021), however despite their success, the solutions was not able to address this wormhole problem effectively due to their dynamic nature and has remained a very big challenge till date. The use of machine learning which over the years has gained the most attention to solve this cyber threat as a pattern recognition problem is no longer reliable due to perturbation of wormhole attack. To address this problem, the research proposes an approach which monitors the energy level of nodes to detect

wormhole (Gayathri et al., 2019) using neighbour discovery algorithm. This when achieved in this paper will provide data confidentiality, integrity and reliability of data networks for communication purposes.

II. LITERATURE REVIEW

Table 1: Systematic review of Literatures

Author	Research title	Technique	Work done	Research gap/ limitation
Singh et al (2016)	A Wormhole Resistant Hybrid Technique (WRHT) for Wireless sensor network	Hybrid	They employed the concept of watchdog and Delphi scheme to detect wormhole attack.	Throughput rate of 89.92% was achieved but the WRHT is computational complex.
Xiao et al. (2019)	A novel secured neighbour discovery algorithm or wormhole attack	Neighbour discover algorithm	Neighbour discovery algorithm was develop for fast detection of wormhole attack	Other quality of service was not considered
Khobragade and Padiya (2016)	Wormhole attack prevention and detection using authentication based delay per hop technique	Encryption	Uses authentication based delay per hop technique to detect wormhole attack in a network	Throughput is 89.12% but the algorithm is not smart.
Tamilarasi and Santhi (2020)	Detection of wormhole attack and secure path selection in wireless sensor network	Particle Swarm Optimizatio n (PSO)	They developed a method against wormhole attack in MANET through identifying the wormhole and select the best path	Not smart
Sundararajan et al. (2014)	Biologically inspired artificial intrusion detection system (BAIDs)	Machine learning	The study collected data of wormhole and train neural network for intelligent detection	Cannot detect pertubated wormhole data

III. CHARACTERIZATION

For this study, empirical data was collected from Destinet Smart Technologies (DST) LTD. This data was generated from their network when tested of wormhole vulnerabilities using XM cyber software. The network performance was monitored using throughput, latency and packet loss model in Hans et al. (2009) and the results are presented in table 2;

Table 2: Characterization data from DST

Packet sent (mbps)	Throughput (%)
79.2570	74.464
89.9930	72.257
84.9060	68.827
92.9930	65.684
86.9060	63.906
89.0000	63.257
92.5000	60.906
93.2570	59.123
98.8270	58.530
100.530	58.464
102.950	56.024
116.020	55.993
120.020	54.684
131.640	53.642
113.640	51.642
115.680	50.500
115.680	50.123
118.460	50.024
169.120	49.993
121.120	46.000
124.460	45.684
124.680	42.957
Average	56.940

The result in the table 2 showed that the average throughput is 56.940%. The result when analyzed by the Nigerian Communication Commission (NCC) (Anabi et al., 2021) showed that the throughput, latency are not satisfactory due to poor quality of service as they not satisfy the 70% requirement for good throughput for data. To solve this problem, the wormhole was formulated and then neighbour discovery algorithm was developed to detect it based on energy level variation of nodes.

IV. FORMULATION OF THE WORMHOLE PROBLEM

The model of the wormhole is developed considering the targeted infrastructure which is the source nodes (S_t), the attacker nodes which is the infectious nodes (Z_t) and other necessary parameters defined in the table 3; where used to define the threat model presented in the structural figure 1;

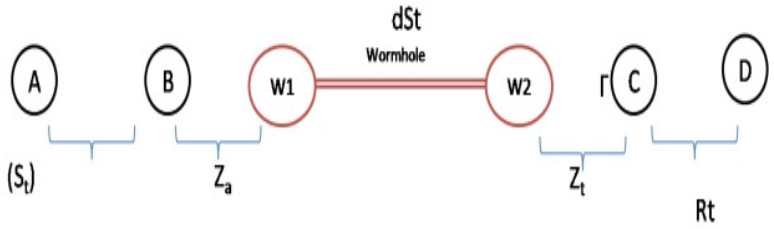

Figure 1: Wormhole modeling diagram

Table 3: Data table of the Wormhole (Mahendra et al., 2019)

S/N	Feature names	Data Type
1	Duration	Continuous
2	Protocol	Discrete
3	Packet size	Continuous
4	Flag	Discrete
5	Header length	Continuous
6	Hop count	Continuous
7	Life time	Continuous
8	Message type	Continuous
9	Destination sequence number	Continuous
10	Stream index	Continuous
11	Land	Discrete
12	Message transfer mode	Discrete
13	Number of neighbours	Continuous
14	Highest data flow	Continuous
15	Average data flow	Continuous
16	Lowest data flow	Continuous
17	Average number of hop count	Continuous
18	Number of drop box	Continuous
19	Rate of drop box	Continuous
20	Label	Discrete

V. DEVELOPMENT OF NEIGHBOUR DISCOVER ALGORITHM

Due to the dynamic nature of nodes during communication process, the wormhole attack through various fake hops creates tunnel in the inner or outer nodes, thus lading to traffic by attracting normal nodes towards it paths. The neighbour discovery algorithm can detect outer wormholes; however most time hardly finds the inner wormhole. Secondly, most times the wormholes are created simultaneously to attack both inner and outer nodes, depending on the routing protocol, for this reason the detection and combating of this wormhole entirely becomes challenging. Therefore, there is need for a smart neighbour discovery algorithm which can sense variation in the behaviour of nodes based on their energy level and then detect wormhole (Gayathri et al., 2019).

a. Energy Level Threshold Model

The model to compute the energy level of the nodes are presented using the relationship between distance and neighbour ratio threshold, position, hopping patterns and power; where the length between neighbouring nodes (Mosmi and Jitendra, 2015) is presented using the model in equation (1).

$$D_n = r\tan\left(\frac{1}{2arccosd/2r}\right) \quad (1)$$

The model in figure 1 presented the length between two neighbouring nodes determined based on routing protocol and poison distribution function in (Haight, 1967). To compute the time taking to form a new link between the neighbouring nodes and other nodes, the model in equation (1) was used to for the equation (2), making t the subject as;

$$t = 4\tan\left(\frac{\frac{1}{2}arccosd}{2r}\right) \quad (2)$$

The model in equation (1) and (2) resented the length and time variables of the nodes. Differentiating the above presented the threshold for each node as equation (3)

$$\mathbf{F'(d)} = \frac{1}{+r.[cos(\frac{1}{2}\arccos d/2r)]^2 \cdot \sqrt{1-(\frac{d}{2r})^2}} \quad (3)$$

Where F' is energy level, r is neighbour ratio threshold; d is distance between nodes. To compute the total energy at t+1, the model in equation (4) was used;

$$\mathbf{Fn} = \sum_{j=c} \frac{F'}{d(i,j)} \quad (4)$$

Where c is clusters of the nodes within the network, i and j are interconnected nodes.
The energy model in equation 4 was used to monitor the behaviour of the nodes within the interconnected network to detect changes in power consumption of the nodes based on hoping patters. Then the energy level for each node is computed and the average determined to get the energy level of the nodes. Two neighbouring nodes in the network are then compared for energy level variation an if difference is detected in the energy level, then wormhole is detected, else wormhole not detected and the monitoring process continuous.
The pseudo code of the algorithm is presented below;

The Pseudo Code of the Algorithm

1. **Start**
2. Detect nodes in the wireless network as x
3. Identify node random position with poisson distribution
4. Compute node energy level
5. Determine reference energy level
   Compare energy level of neighbouring nodes
6. **If**
   Wormhole is detected = True
7. **Then**
8. Isolate nodes from network
9. **Else**
10. Return to monitoring
11. End if
12. **End**

VI. IMPLEMENTATION OF THE ALGORITHM

The algorithm was implemented using communication toolbox, and Matlab. The algorithm and the mathematical models were integrated on the network using Matlab Editor and then simulated using the parameters in table 4 collected from the testbed;

Table 4: Programming settings

Coding parameters	Values
Channel type	Wireless
Simulation area	1400 * 1400sqm
Frequency	914MHz
Number of nodes	500
MAC types	IEEE802.11
Transmission range for normal network	250m
Transmission range for wormhole network	500m
Mobility velocity	Random way point
Simulation time	30s
Packet size	256bytes
Queue type and length	500
Traffic type	TCP/CBR
Pause time	0.1m/s
Wormhole link length	4 hops

VII. RESULTS OF SIMULATION

The result of the simulation was done using the parameters in the table 4 to evaluate the performance for the algorithm via security against wormhole. The network structure and size was first presented as a sparse matrix in figure 2;

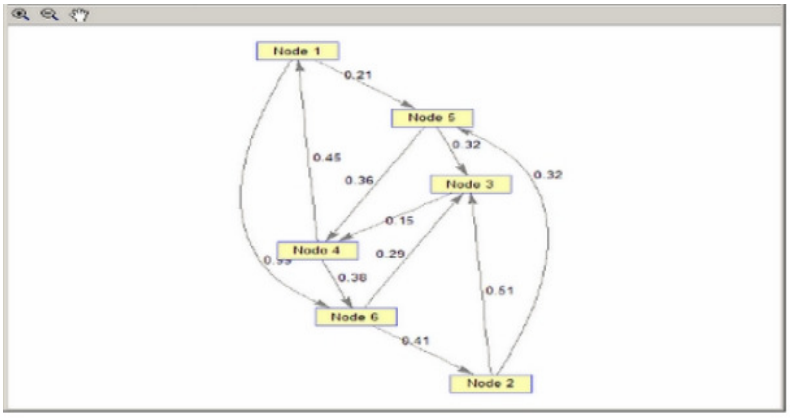

Figure 2: Sparse matrix of the wifi network

The result in figure 2; shows the resultant space matrix of the network structure with six nodes and their energy levels computed by the algorithm developed. The wormhole model was used to induce wormhole on the network with the algorithm disabled as shown in figure 3;

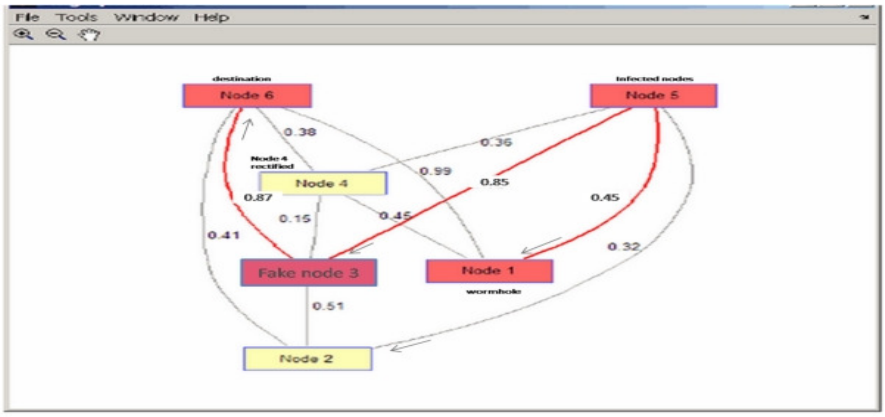

Figure 3: initiation of the wormhole attack on the network

The result in figure 3 shows how the wormhole was originated from node 1 and then infected node 5. The network shows how the wormhole was able to create a fake node which the node 5 used to communicate to node 6. The result shows also the variation in energy level f each node due to the effect of the wormhole on the network, while the nodes not directly affected maintained the same energy level for communication.

The result in figure 4 showed how the algorithm developed was able to detect this wormhole and mitigate it from the network. This was done by via the computation of the energy level of each of the nodes with equation 3 on the network and check if it varies from the original reference values as modeled in the algorithm. The total energy level is computed with time using equation 4 for the network clusters of nodes. The variation in energy values is used as criteria to read wormhole and then isolate the node from the network. The result is presented in figure 4;

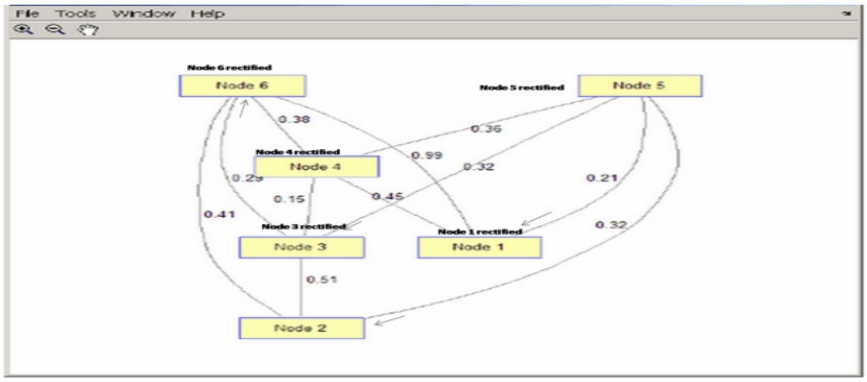

Figure 4: Complete inner and outer wormhole isolation result

From the result in figure 4; it shows how the neighbour discovery algorithm was able to detect the internal node 5 and 3 and also the outer node 1 which initiates the wormhole in the first place and then isolate them from the network. The result in figure 5 shows how the wormhole was isolated from the network with the normal energy level restored.

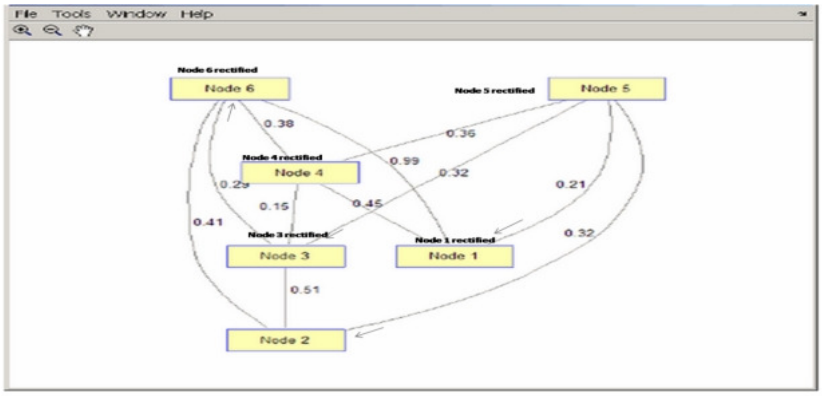

Figure 5: complete wormhole attack isolation

The result in figure 5 shows that the network is free from wormhole and the throughput performance was also measured as in figure 6;

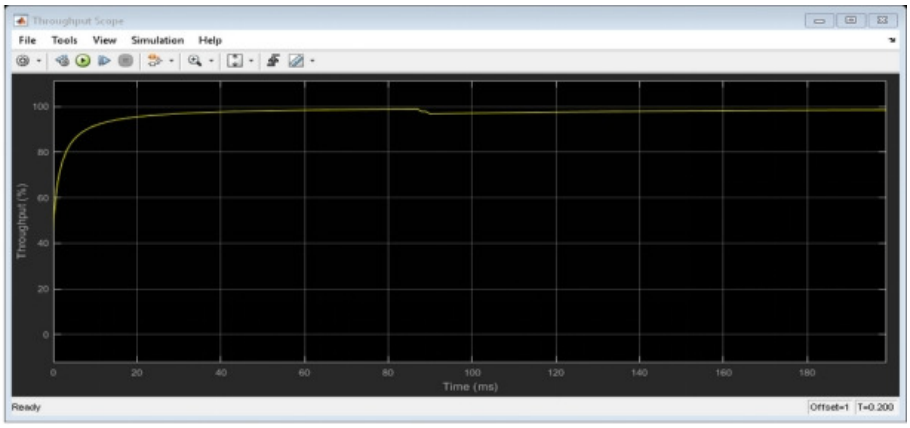

Figure 6: Throughput performance

The figure 6 was used to measure the quality of service on the network after wormhole was removed. The result showed that the average throughput recorded is 92.80% as against 56.90 in the characterized. The algorithm was deployed at the testbed and evaluated as shown in table 5;

Table 5: Result of the algorithm on testbed

Packet sent (mbps)	Throughput (%)
79.2570	92.90
89.9930	92.80
84.9060	92.80
92.9930	92.70
86.9060	92.70
89.0000	92.70
92.5000	92.70

93.2570	92.60
98.8270	92.60
100.530	92.60
102.950	92.50
116.020	92.40
120.020	92.40
131.640	92.40
113.640	92.40
115.680	92.40
115.680	92.40
118.460	92.40
169.120	92.30
121.120	92.30
124.460	92.30
124.680	92.10
Average	92.50

From the table 5 the performance of the wireless data network when the new algorithm was deployed and the result showed that the average throughput is 92.50%. The result achieved is good as it satisfied the NCC standard for quality of service. The result achieved was compared with the testbed during characterization and presented in the table 6;

Table 6: Comparative Analysis

Packet sent (mbps)	Throughput (%) with neighbour discover algorithm	Throughput (%) without neighbour discover algorithm
79.2570	92.90	74.464
89.9930	92.80	72.257
84.9060	92.80	68.827
92.9930	92.70	65.684
86.9060	92.70	63.906
89.0000	92.70	63.257
92.5000	92.70	60.906
93.2570	92.60	59.123
98.8270	92.60	58.530
100.530	92.60	58.464
102.950	92.50	56.024
116.020	92.40	55.993
120.020	92.40	54.684
131.640	92.40	53.642
113.640	92.40	51.642
115.680	92.40	50.500
115.680	92.40	50.123
118.460	92.40	50.024
169.120	92.30	49.993
121.120	92.30	46.000
124.460	92.30	45.684

124.680	92.10	42.957
Average	92.50	56.940

From the result it was observed that the average throughput with the NDA was 92.50% as against 56.940%. The percentage improvement recorded with NDA is 35.56%. The NDA was also compared with existing algorithms and the result presented in table 7;

Table 7: Comparative Technique

Author	Technique	Throughput performance
Khobradade &Padiya (2016)	Hop techniques	89.17
Singh et al. (2016)	wormhole resistance hybrid technique (WHRH)	89.92
New system	Neighbour Discovery algorithm	92.50

The table 7 presented the comparative technique of the some of the relevant approaches employed over the year to mitigate wormhole on wireless network. The performances are analyzed with the new system as shown in figure 7;

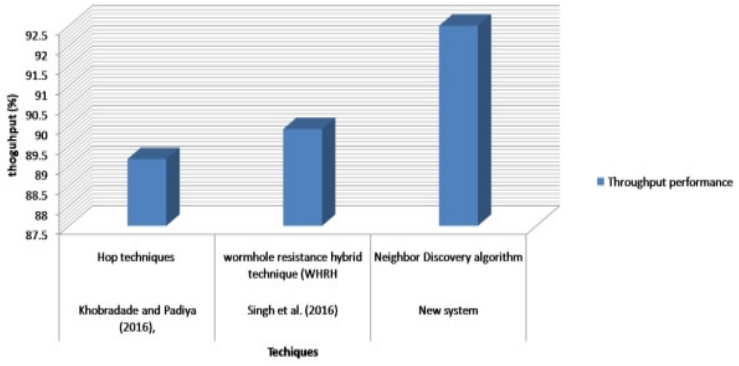

Figure 7: Comparative techniques

The figure 7 presented the comparative performance of the various wormhole detection algorithms and their impact on the wireless network. From the result it was observed that the use of neighbour discover algorithm developed achieved accuracy of 92.50% which according to the NCC standard is very good. Furthermore, the algorithm is very easy and cheap to implement as it involves simple logical configuration of the service based on the model developed.

VIII. CONCLUSION

This work has successfully developed and implemented an improved wormhole detection algorithm using the neighbour discovery technique. This new system was developed by making the existing neighbour discovery algorithm adaptive to real time wormhole threat. This was done following the system analysis of the past selected techniques and review of recent epistemologies relating to the principal system. The work designed various models which were used to implement the study, in line with Mathlab and other implementation toolbox. The performance showed that the algorithm was able to detect nodes behaviour based on their level of energy threshold and then detect wormhole. The performance showed that algorithm never affects the quality of service on the network as throughput of 92.80% and packet loss of 7.20% was achieved which according to Nigerian Communication Commission is optimal.

CONTRIBUTION TO KNOWLEDGE

The study presented a smart neighbour discovery algorithm which protects wireless data network, (WLAN) against wormhole attack.

ACKNOWLEDGEMENT

I extend my profound gratitude to God the Father Almighty who in his infinite mercy and goodness that made this research work comes to a completion and grand success ever adored.

To my beloved parents Mr. And Mrs. Udeani of whom am still an existing entity under the guidance of the Almighty, pronounce my sincere appreciation for their immeasurable contribution to the success of his research work; financially, morally, spiritually and otherwise, I say may they ever be blessed.

I will never fail to acknowledge the relentless effort of my capable and ever hardworking supervisor, Prof. Greg. N Onoh for his inspiration, valuable ideas, guidance and constructive criticism throughout my Masters studies despite his tight schedule and my other departmental lecturers who in one way or the other also helped.

And to my beloved siblings and friends for their untiring efforts towards making my research composition a fulfilling venture. I say a very big thanks to you all and pray for God's divine rewards and blessings upon you all.

REFERENCES

[1] Anabi H.K., Uyi A. Mathew S., Okoyeigbo O., Aligbe A., Atayero A., (2021) " The quality of service of the deployed LTE technology by mobile operators in Abuja-Nigeria" IJECE; Vol 11; no 3; pp- 2191-2202; ISSN: 2088-8708

[2] Gayathri S., R. Seetharaman; L.Harihara Subramanian; S. Premkumar; S. Viswanathan; S. Chandru (2019) "Wormhole Attack Detection using Energy Model in MANETs" 2nd International Conference on Power and Embedded Drive Control (ICPEDC): INSPEC Accession Number: 19455674; DOI: 10.1109/ICPEDC47771.2019.9036536

[3] Haight, Frank A. (1967), *Handbook of the Poisson Distribution*, New York, NY, USA: John Wiley & Sons, ISBN 978-0-471-33932-8

[4] Hans van den Berg; Thomas Michael Bohnert; Dmitri Moltchanov (2009) "Performance Evaluation and Traffic Modeling" In book: Traffic and QoS Management in Wireless Multimedia Networks (pp.89-150); DOI:10.1007/978-0-387-85573-8_3

[5] Khobragade and Padiya P., (2016), "Detection and prevention of wormhole attack based on delay per hop technique for wireless mobile ad-hoc network", in Int. Conf. Signal Process. Commun. Power Embed. Syst., pp. 1332-1339.

[6] Mahendra P., Tripathi S., Dahal K. (2019) "Wormhole attack detection in ad hoc network using machine learning technique"10th International Conference on Computing, Communication and Networking Technologies (ICCCNT); OI:10.1109/icccnt45670.2019.8944634; Corpus ID: 209696530

[7] Majid Farzaneh (2020). Wormhole detection in MANET using MLP (https://www.mathworks.com/matlabcentral/fileexchange/74104-wormhole-detection-in-manet-using-mlp), MATLAB Central File Exchange. Retrieved February 9, 2020

[8] Mosmi Tiwari, Jitendra Choudhary (2015) "Wormhole Attack in Wireless Sensor Networks "International Journal of Computer Application (2250-1797) Volume 5– No. 4,

[9] Shruti D., Grjarathi J., Chandre P., Pravin Nerkar (2021)"A comparative analysis of machine deep learning algorithms for intrusion detection in WSN"In BOOK: Security Issues and Privacy Threats in Smart Ubiqutous Comuting (PP. 173-193).

[10] Singh, Singh J. and Singh R., (2016). "WRHT: a hybrid technique for detection of wormhole attack in wireless sensor networks", Mob. Inf. Syst.

[11] Sundararajan T. Ho, Medard M., Koetter R., Karger D. R., Effros M., Shi J., and Leong B., (2014). "A random linear network coding approach to multicast," IEEE Transactions on Information Theory, vol. 52, no. 10, pp. 4413–4430,

[12] Tamilarasi N., Santhi S., (2020) "Detection of Wormhole Attack and Secure Path Selection in Wireless Sensor Network" Wireless Personal Communications 114(12); DOI:10.1007/s11277-020-07365-4

[13] Xiao L., Yanru C., Miao L., Qian L., (2019) "CREDND: A Novel Secure Neighbour Discovery Algorithm for Wormhole Attack" IEEE Access PP(99):1-1DOI:10.1109/ACCESS.2019.2894637

