RESEARCH ARTICLE OPEN ACCESS

Securing MANETs Against Routing Attacks: A Comprehensive Study on Black Hole and Related Threats

Ms. Jyoti Kataria[1], Dr. Ankit Kumar[2], Dr. Ganesh Kumar Dixit[3]
Ph. D. Scholar Computer Science, Starex University, Binola, Gurugram[1]
Assistant Professor, NIET, Greater Noida, U.P.[1]
Email: jyotiktr8@gmail.com)
Associate Professor, Computer Science, Starex University, Binola, Gurugram[2]
HOD, Dept. of Artificial Intelligence and Data Science, Arya College of Engineering, Jaipur, Rajasthan[3]

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

Abstract:

MANETs are vulnerable to several security threats because they lack infrastructure and are dynamic. The Black Hole attack is one of the many destructive ones, which impairs performance, interferes with routing, and results in significant packet loss. This article provides a detailed analysis of the Black Hole assault in MANETs, including its consequences and the weaknesses of existing defences. The examination of current research indicates that prompt and precise responses are still necessary. Next, a Support Vector Machine (SVM) is employed to evaluate the features of the gathered data in direction to identify and eliminate harmful nodes. In addition to successfully tackling collaborative assaults and differentiating malicious activity from typical network dynamics, the research describes the difficulties in attaining precise real-time detection with little cost.

Keywords — MANET, anomaly detection, NS – 3, trust management.

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

INTRODUCTION

Information about neighbouring nodes is transmitted via a transitory configuration in a dynamic wireless network known as a Mobile Ad hoc Network (MANET) [1-3]. When Mobile devices' connections to other devices fluctuate, the MANET devices are autonomous and free to travel in any direction [4]. In some situations, such military applications, A collection of mobile, self-organizing, decentralized nodes is called a MANET. [5-6]. In order to connect inside the wireless transmission range of other nodes, each MANET node is outfitted with a wireless transmitter and receiver [7-8]. These days, MANETs are widely used in many applications, including disaster assistance, space communication, commercial exhibitions, sports stadiums, retail centres, road or accident advice, mission-critical military communication, and avoiding auto accidents [9]. Due to their intricate characteristics, IoT and RPL networks are susceptible to a variety of assaults, including Specific Forwarding, Gray Hole, Wormhole, Sybil, Flood, Sinkhole, Jamming, and the lethal Black Hole attack. These assaults jeopardize “Wireless Sensor Networks” (WSN) reliability and security. [10-14]. Numerous strategies and tactics have been created to counter these attacks. For instance, many methods for detecting intrusions have been created to identify frequent network assaults, with an emphasis on other routing attacks including hello flood, wormhole, black hole, Sybil, identity replication, and selective forwarding [15]. Because it may result in large
The Black Hole attack is the most harmful since it causes energy losses, network congestion, and

decline in performance. Regarding the Black Hole assault, it acts as the primary point of contact within the tiered architecture. Verification agents, Safe routing, hierarchical methods, and trust-based multi-hop systems strategies are all examples of current solutions [16].

A malicious group of nodes or a single node initiates a black hole attack on the network, significantly impairs MANET performance [17]. Full packet-dropping attacks, also known as black hole attacks, occur when a malevolent node delivers a fake route response to lose every packet that passes through it [18]. Due to deterioration, it not only leads to low throughput but also lowers network performance. Black hole attacks are more difficult to identify and need for specialized attention as well as clever defences [19]. The lack of effective This study's primary goal is to address the issue of mobile ad hoc network security approaches. Wormhole and blackhole attacks against ad hoc mobile networks are attempted to be prevented in the literature are not very precise. Thus, new techniques that can accurately and precisely identify and stop these assaults in real time are required [20].

Review work:

(**Hajar Fares et. al, 2025**) In order to obtain high accuracy and a low error rate in a shorter amount of time, the selected properties were included into the models. With a success rate of 99.76%, the KNN model is robust, and the decision tree model comes in second with an accuracy of 99.69%, according to the experiment's results, which show that all three models worked well. Furthermore, the implemented KNN and decision tree techniques have class-specific accuracy of around 99% to 100%. A variety of techniques, including confusion matrix, recall, f1-score, precision, etc., were used to confirm the results, which were then compared to contemporary research [21]. **(Ahsan Saud Qadri Syed et. al, 2024)** in order to guarantee uninterrupted service, handovers are required for smooth network connectivity and rapid authentication. Because of their quick asymmetric key encryption-decryption and exchange, the RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptography)
For authentication, algorithms are frequently utilized, although they are not as secure against black hole attacks. Chaos-based algorithms are effective against false behavior black hole attacks and offer a quicker authentication procedure. shows that using the chaos algorithm to provide quick authentication and stop rogue nodes from interfering with the network is a good idea [22]. **(Aurelle Tchagna Kouanou et. al), 2023** A new method for detecting and countering artificial learning-based attacks. Wormhole and blackhole assaults were then put into practice after a 26-node MANET was constructed for the study using NetSim (Network Simulator) software. To predict and detect these assaults, using data. A machine-learning model was developed using the network traffic gathered throughout the simulations. Excellent sensitivity, precision, and 99% f1 scores were attained by the model. By creating a real-time application, the model's efficacy was evaluated. This technique is applicable to any wireless network but is especially pertinent to businesses that communicate over ad hoc networks [23]. **(Gurung and Chauhan, 2019)** The Detection and Prevention-Ad hoc on Demand Distance Vector (MBDP-AODV) protocol is a dynamic method for mitigating the effects of black holes sequence number threshold-based mechanism was created. Although the technique greatly decreased network packet losses, the Normalized Routing Load (NRL) was high since the destination nodes were recording fewer data packets [24]. **(Sweta Dixit et. al (2020)**, The two most dangerous attacks on MANETs are blackhole and gray hole attacks. A black hole attack happens when a hostile protuberance is unable to deliver data packets to their intended location. A specific type of black hole assault that is hard to identify is known as a "gray hole attack." Numerous scholars have put up a variety of strategies to stop and identify the black hole and gray hole problems [25].

Summarization of existing research work:

Author	**Methodology**	**Research work done/limitation**	**Used Machine-learning or not**
Ahsan Saud Qadri Syed Sheikh Abdullah Technical [22]	By facilitating quicker and more secure node verification, a chaotic map-based technique can improve authentication speed and lessen black hole threats in MANETs.	lowering calculation time and thwarting black hole attacks in contrast to conventional RSA and ECC techniques	Not
Jaspal Kumar et. al [26]	examining the effects on routing protocol performance metrics of MANETs with and without black hole attacks in a variety of scenarios.	degradation in MANET routing protocol performance	Not
Himani Yadav and Rakesh Kumar [27]	A new way to detect and eradicate MANET black hole attacks, implementing it in a network simulator, and evaluating its performance through various metrics.	developing and evaluating an innovative technique for identifying and removing black holes attacks in MANETs to ensure secure communication.	Yes
Christeena Joseph et. al [28]	simulating MANETs under black hole attacks across diverse network scenarios (varying size, mobility, traffic, etc.) and comparatively analyzing the resulting performance degradation using key metrics.	how MANET performance is affected by black hole attacks metrics across diverse simulated network scenarios	Not
Pooja Jaiswal and Dr. Rakesh Kumar [29]	proposing and evaluating a novel or enhanced mechanism (likely through simulation) to prevent black hole nodes	The proposed prevention mechanism might introduce overhead or have limitations in handling complex and dynamic network scenarios or sophisticated attacks.	Yes

Any malevolent activity or behaviour by a node (internal or external to the network) intended to interfere with regular operations, jeopardize security, or impair network performance is referred to as an attack in a Mobile Ad hoc Network (MANET). MANETs are susceptible to a variety of attacks because of their special features, which include wireless communication, changeable topology, absence of permanent infrastructure, and frequently constrained resources which includes:

- Disrupting Communication
- Disrupting Routing
- Gaining Unauthorized Access
- Compromising Data Integrity
- Degrading Performance

Type of attacks:

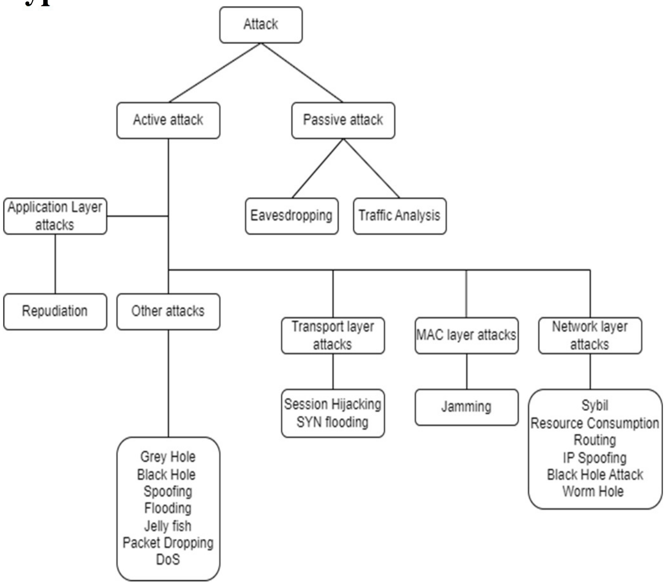

Fig. 1: Type of attacks in MANET [30]

Active attacks:

An attacker often attempts to breach the protected network in this kind of attack. Usually, it makes use of Trojan horses, worms, viruses, or stealth. Active attacks often aim to alter or steal data, introduce fraudulent code, and breach security measures.

Passive attacks:

Congestion analysis, monitoring of unsecured information transmission or reception, decrypting poorly encrypted congestion, and collecting authentication data, such as passwords, are typical components of this kind of attack. It allows the assailant to see what will happen next. Through passive assaults, an attacker gains access to data files or information without the user's awareness.

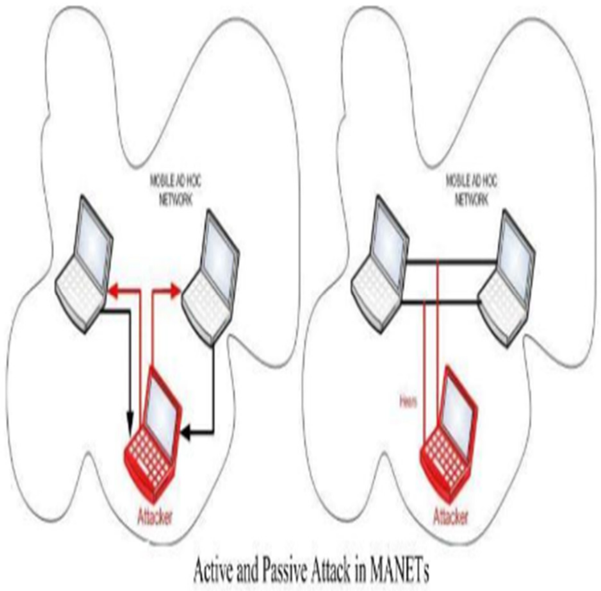

Fig. 2: Active and Passive attacks [31]

Black Hole Attack:

One type of active attack that significantly reduces network performance in Mobile Ad hoc Networks (MANETs) is the “black hole” attack. This attack involves a rogue node pretending to have the shortest way to a target node by manipulating the route discovery process.
When the black hole node makes a route request (RREQ), it immediately sends a bogus route reply (RREP) with a high sequence number or low hop count to trick the source node into believing it has the optimal path.
After being added to the routing path, the malicious node has the ability to discard or absorb data packets that are traveling through it, preventing them from getting to where they are supposed to. It may result in:

- Packet loss
- Reduced throughput
- Increased end-to-end delay
- Network disruption
- Resource depletion

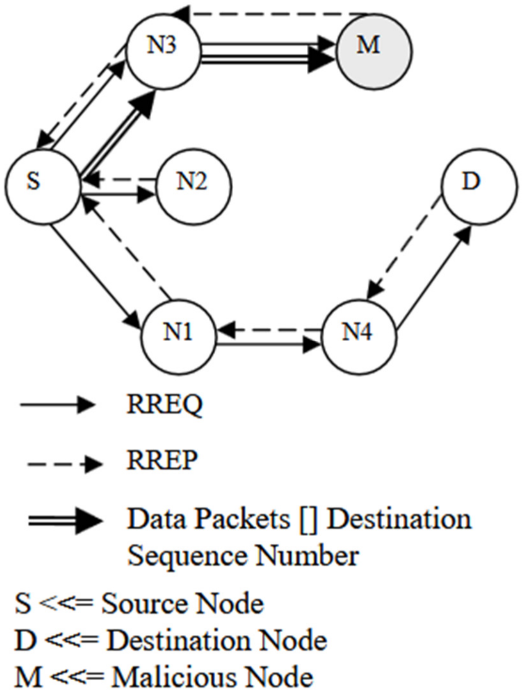

Fig. 3: Black Hole attack [29]

Problem statement:

The "black-hole" attack is a type of denial-of-service attack that focuses on a single rogue node. The malicious attack node takes part in the path in this type of attack discovery procedure [32]. This is achieved by including a fake destination sequence number in the route request along with a bogus route reply message, which deceives the requesting source node into thinking because it is the quickest way to get at the intended message. Then, it either decreases, modifies, or even passes the packets [33]. The technology "wireless sensor network" has expanded dependability in a variety of settings, with control technique needs like static power management and dedicated power quality assurance standing out [34].

Proposed methodology:

Creating the data needed for machine learning analysis is the initial step. To create traffic data that closely resembles actual traffic while undergoing a black hole attack, an OMNET++/NS -3 simulator is used. The produced data is then gathered in a specific manner for subsequent analysis. All of the traffic records that are gathered have certain traits or attributes. A support vector machine (SVM) is castoff to assess these characteristics and categorize the traffic into harmful and regular traffic. This analysis makes it possible to identify and stop malicious nodes.

Proposed solution:

1. Every node in a MANET should cooperate. To put it another way, they should depend on one another to fill in the gaps caused by the lack of infrastructure. If not, the network as a whole won't function correctly. One of the attacks used to corrupt MANETs is a blackhole. The behaviour of such malevolent nodes inside a network may be examined to identify such assaults. The following is a summary of some of their shared behavioural traits:

- To reply to the majority of the RREQ, they boost their transmission power.
- Rarely do they send any RREQ.
- They hardly ever transmit and always unicast.

2. Data generation
3. Data collection
4. Feature selection
5. Data-preprocessing
6. Using any supervised machine learning algorithms i.e. SVM

Challenges:

1. **Accurate Differentiation from Network Dynamics:** It is essential to create detection systems that can differentiate between real black hole assaults and normal network oscillations.
2. **Real-time Detection with Low Overhead:** Numerous detection methods now in use have substantial overhead in terms of computing, communication, and energy usage. It is still very difficult to create techniques that may accurately identify black hole assaults in real time and low resource consumption, particularly in MANETs with limited resources.
3. **Addressing Collaborative Black Hole Attacks:** The detection and mitigation of attacks involving many cooperating black

hole nodes is more complicated and necessitates sophisticated coordination across detection entities, whereas many solutions concentrate on single malevolent nodes.

4. **Integration with Existing Routing Protocols:** The underlying routing protocols should preferably not be significantly disrupted when security measures are implemented. It can be difficult to design solutions that smoothly interface with protocols like AODV or DSR without materially changing how they function at their core.
5. **Formal Verification and Performance Guarantees:** Formal verification and thorough performance study across a range of network circumstances and attack scenarios are lacking in many suggested solutions. One significant unresolved issue is the establishment of theoretical assurances for detection overhead and accuracy [35, 36].

Conclusion and future:

The difficulty of identifying and reducing these dangers is made much more difficult by MANET's dynamic and infrastructure-less features. The development of more precise, effective, and resilient security solutions against black hole attacks in MANETs can be greatly advanced through tackling these issues and following these future research directions. This will open the door for the more secure and dependable deployment of these dynamic wireless networks in a number of crucial applications. More accurate and effective solutions that can function in the resource-constrained and extremely dynamic environment of MANETs are still desperately needed.

References:

[1] Alhaidari FA, Alrehan AM., "***A simulation work for generating a novel dataset to detect distributed denial of service attacks on Vehicular Ad hoc Network systems*", International Journal of Distributed Sensor Networks**. 2021; 17(3):1-25. Available from: https://doi.org/10.1177/15501477211000287.

[2] Aluvala S, Sekhar R, Vodnala D., "***An empirical study of routing attacks in mobile Ad-hoc networks*", Procedia Computer Science**. 2016; 92: 554-561. Available from: https://doi.org/10.1016/j.procs.2016.07.382

[3] Tseng FH, Chou LD, Chao HC., "***A survey of black hole attacks in wireless mobile ad hoc networks***", **Human-Centric Computing and Information Sciences**. 2011; 1(1): 4.

[4] Farahani, G., "***Black hole attack detection using k-nearest neighbour algorithm and reputation calculation in Mobile Ad hoc networks***", Elsevier, Computers & Security 148 (2025) 104166, https://doi.org/10.1016/j.cose.2024.104166

[5] Abdelhaq M, Alsaqour R, Abdelhaq S., "***Securing mobile ad hoc networks using danger theory-based artificial immune algorithm***" PLoS ONE. 2015; 10(5): e0120715. Available from: https://doi.org/10.1371/journal. pone.0120715.

[6] Anusha K, Sathiyamoorthy E., "***A new trust-based mechanism for detecting intrusions in MANET***", Information Security Journal: A Global Perspective. 2017; 26(4): 153-165. Available from: https://doi.org/10.1080/19393555.2017.1328544.

[7] Subba B, Biswas S, Karmakar S., "***Intrusion detection in mobile Ad-hoc networks: Bayesian game formulation***" Engineering Science and Technology, an International Journal. 2016; 19: 782-799.

[8] Amiri E, Keshavarz H, Heidari H, Mohamadi, E, Moradzadeh H., "***Intrusion detection systems in MANET: A review***", Procedia-Social and Behavioral Sciences. 2014; 129: 453-459. Available from: https://doi.org/10.1016/j.sbspro.2014.03.700.

[9] Thanuja R, Umamakeswari A. Unethical network attack detection and prevention using fuzzy based decision system in mobile Ad-hoc networks. Journal of Electrical Engineering and Technology. 2018; 13(5): 2086-2098. Available from: https://doi.org/10.5370/JEET.2018.13.5.2086

[10] lheeti KMA, Gruebler A, McDonald-Maier K. Intelligent intrusion detection of grey hole and rushing attacks in self-driving vehicular networks.

Computers. 2016; 5(3): 16. Available from: https://doi.org/10.3390/ omputers5030016.

[11] Popli R, Sethi M, Kansal I, Garg A, Goyal N. Machine learning based security solutions in MANETs: State of the art approaches. Journal of Physics: Conference Series. 2021; 1950: 012070. Available from: https://doi.org/10.1088/1742-6596/1950/1/012070.

[12] Imran M, Khan FA, Jamal T, Durad MH. Analysis of detection features for wormhole attacks in MANETs. Procedia Computer Science. 2015; 56: 384-390. Available from: https://doi.org/10.1016/j.procs.2015.07.224.

[13] Gopal U., Subramanian K., "***A secure cross-layer AODV routing method to detect and isolate (sclardi) black hole attacks for MANET"***, Turk. J. Electr. Eng. Comput. Sci. 25 (4) (2017) 2761-2769

[14] Z. Pala, N. ˙ Inanç, "***The impact of disabling suspicious node communications on network lifetime in wireless ad hoc sensor networks***", Turk. J. Electr. Eng. Comput. Sci. 24 (5) (2016) 4429–4444.

[15] Ezhilarasi M, Gnanaprasanambikai L, Kousalya A, "***Shanmugapriya M. A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks***",Soft Computing. 2022; 27: 4157-4168. Available from: https://doi.org/10.1007/s00500-022-06915-1.

[16] I.A. Reshi, S. Sholla, "***Challenges for security in iot, emerging solutions, and research directions***", Int. J. Comput. Digit. Syst. 12 (1) (2022) 1231–1241.

[17] Bhagat, S.P., Padiya, P., Marathe, N., 2017, "***A generic request/replybased algorithm for detection of blackhole attack in MANET***", In: Proceedings of International Conferenceon Smart Technologies for Smart Nation (SmartTechCon). IEEE, pp. 1044–1049.

[18] Shahabi, S., Ghazvini, M., Bakhtiarian, M., 2015, "***A modified algorithm to improve security and performance of AODV protocol against black hole attack***", Wirel. Netw.

[19] Jagadeesan, S., Parthasarathy, V., 2019, "***Design and implement a cross layer verification framework (CLVF) for detecting and preventing blackhole and wormhole attack in wireless ad-hoc networks for cloud environment***", Clust. Comput. 22 (1), 299–310

[20] Kouanou A. T, "***Machine Learning for Intrusion Detection in Ad-hoc Networks: Wormhole and Blackhole Attacks Case***", Cloud Computing and Data Science http://ojs.wiserpub.com/index.php/CCDS/, Universal Wiser Publisher, DOI: https://doi.org/10.37256/ccds.5120243516

[21] Hajar Fares et. al, ***"Intrusion Detection in Wireless Sensor Networks using Machine Learning",*** www.sciencedirect.com, ScienceDirect, Procedia Computer Science 252 (2025) 912–921

[22] Ahsan Saud Qadri Syed et. al, "***A Chaotic Map-based Approach to Reduce Black Hole Attacks and Authentication Computational Time in MANETs***", Engineering, Technology & Applied Science Research Vol. 14, No. 3, 2024, 13909-13915 13909

[23] Aurelle Tchagna Kouanou et. al, ***"Machine Learning for Intrusion Detection in Ad-hoc Networks: Wormhole and Blackhole Attacks Case",*** Cloud Computing and Data Science: http://ojs.wiserpub.com/index.php/CCDS/, DOI: https://doi.org/10.37256/ccds.5120243516, Volume 5 Issue 1|2024| 79Volume 5 Issue 1|2024| 62-79

[24] Gurung, S., Chauhan, S., 2019, "***A dynamic threshold-based algorithm for improving security and performance of AODV under black-hole attack in MANET***", Wirel. Netw 25 (4), 1685–1695.

[25] Sweta Dixit, Krishna Kumar Joshi and Neelam Joshi, ***"A Review: Black Hole & Gray Hole Attack in MANET",*** International Journal of Future Generation Communication and Networking, Vol. 8, No. 4 (2015), pp. 287-294, http://dx.doi.org/10.14257/ijfgcn.2015.8.4.28

[26] Jaspal Kumar et. al, ***"Effect of Black Hole Attack on MANET Routing Protocols",*** J. Computer Network and Information Security, 2013, 5, 64-72, Published Online April 2013 in MECS (http://www.mecs-press.org/), DOI: 10.5815/ijcnis.2013.05.08

[27] Himani Yadav and Rakesh Kumar, ***"Identification and Removal of Black Hole Attack for Secure Communication in MANETs",*** International Journal of Computer Science and

Telecommunications [Volume 3, Issue 9, September 2012], page no: 60 – 67

[28] Christeena Joseph et. al, "***Performance Evaluation of MANETS under Black Hole Attack for Different Network Scenarios***", Indian Journal of Science and Technology, Vol 8(29), DOI: 10.17485/ijst/2015/v8i29/84653, November 2015, ISSN (Print) : 0974-6846, ISSN (Online): 0974-5645

[29] Pooja Jaiswal and Dr. Rakesh Kumar, "***Prevention of Black Hole Attack in MANET***", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501, Vol.2, No5, October 2012

[30] Sarit Pal et. al, "*The Sybil attack in Mobile Adhoc Network: Analysis and detection*", January 2013, DOI: 10.1049/cp.2013.2629, Conference: Third International Conference on Computational Intelligence and Information Technology (CIIT 2013), ResearchGate

[31] Sweta Dixit et. al, "***A Review: Black Hole & Gray Hole Attack in MANET***", International Journal of Future Generation Communication and Networking, Vol. 8, No. 4 (2015), pp. 287-294, **http://dx.doi.org/10.14257/ijfgcn.2015.8.4.28**

[32] T. Link and B. D. Gadong, "***Performance analysis of MANET under black hole attack using AODV, olsr and tora***," in Computational Intelligence in In- formation Systems: Proceedings of the Computational Intelligence in Information Systems Conference (CIIS'16), vol. 532, Springer, pp. 198, 2016.

[33] M. Gupta and K. K. Joshi, "***A review on detection and prevention of gray-hole attack in MANETs***," International Journal of Scientific & Engineering, vol. 4, no. 11, 2013.

[34] Dr. Ganesh Kumar Dixit et. al, "***Wireless Sensor Network using Control Communication and Monitoring of Smart Grid***", 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE).

[35] G. K. Dixit, V. Ch, V. J. Barbosa, S. H. Jeelani, L. Johari and S. K. Shukla, "***Comparative Analysis of Neural Networks and Deep Learning using Wireless Communication***", 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022, pp. 1585-1588, doi: 10.1109/ICACITE53722.2022.9823530. Published by: IEEE Xplore: 18 July 2022

[36] T. C. A. Kumar, G. K. Dixit, R. Singh, B. K. Narukullapati, M. K. Chakravarthi and D. Gangodkar, "***Wireless Sensor Network using Control Communication and Monitoring of Smart Grid***", 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022, pp. 1567-1570, doi: 10.1109/ICACITE53722.2022.9823448. Published by: IEEE Xplore: 18 July 2022