International Journal on Wireless, Networking & Mobile Communication Innovations
Vol. 5, Issue 1 – 2021
ISSN: 2581-5113

A Survey on Advance Black/Grey hole Detection and Prevention Techniques in DSR & AODV Protocols

Dr. T. Ananth Kumar[1], A. Devi[1], N.Padmapriya[1], S. Jayalakshmi[1], P. Divya[1]

[1]IFET College of Engineering, India,

Abstract

DTN is vulnerable to the black hole and gray hole attacks due to its limited connectivity. A malicious node is identified during data transmission. However, the basic methodology captures all attacks made by individuals and does not obscure the path from source to destination. The AODV routing protocol is used to determine the smallest possible size of a data packet. Additionally, provide the shortest path to the destination node from the other neighboring road. We can access files and directories if changes to the system's network security occur due to hacking, misuse, or unauthorized access. It enables secure data transmission over a network without data loss. This article is a survey of techniques for detecting and preventing black/grey holes in DSR and AODV protocols.

Keywords: DTN (Delay Tolerant Network), Gray Hole Attacks, Black Hole Attacks, AODV Protocols.

Introduction

The black hole attack on a computer network is a cyber-attack in which packets are discarded rather than relayed through a router. This typically occurs as a result of a router that a variety of factors has compromised. A black hole attack is a routing attack that has the potential to destroy an entire network. Grey Hole Attacks are one of the most prevalent types of attacks on mobile ad hoc networks (MANETs), in which a malicious node permits routing but rejects data transmission. Security is a primary concern in WSNs, as they are much more vulnerable to attacks than wired or infrastructure-based systems are Network of cells and Wireless network. The development of a robust WSN protection protocol. It is a challenging task. This is primarily due to the unique characteristics of WSNs, namely mutual radio lines and unsafe service. Climate change, a lack of central authority, a lack of consumer associations, and limited supply and physical scarcity of services contribute to this situation.

Literature Survey

Small-signal oscillations are emphasized in this paper under operational conditions, and a number of the results indicate insufficient operation in power systems. Diverse management functions gravitate toward one another, such as power transmission over long distances and tielines that run close to the most extreme limits[1]. The small-signal stability of the system precludes rapid energy resource integration (DER)[2]. The loss of thirty,390 megawatts of load and the resulting impact on 7.49 million customers in the Western Electricity Council (WECC). The Phasor Mensuration Unit is used to determine the voltage-current phasors and frequency (PMU). Electricity's Workplace Cybersecurity has aided in developing the Global Positioning System (GPS) for the energy delivery system (CEDS). Synchrophasor are used in power grid applications that involve short-term oscillation[3]. There is a stability issue that must be addressed in order for alarms to be issued once. This means that remediation measures are necessary to maintain the required level of damping, thereby increasing the system's stability and operational responsibility. There are no restrictions on the media used to transmit these data between the source and target nodes. Dedicated non-public management networks frequently invest in existing public networking infrastructure [4]. The impact of the gray hole attack is analyzed using oscillation observation [5].

A gray-hole attack is a type of cybercrime in which an adversary gains control of a middle router by selecting data passing through it. Grid adapts to the progression of PMU oscillation observation [6]. The presence of packets in a congested network is well-known. However, packet loss is minimal in comparison to such instances. The authors examine oscillation observation algorithms in order to determine the impact of congestion-related packet losses (i.e., low share of packet drops). This analysis effort is indirect access to information that contributes to the quality of the synchrophasor network[7]. The PMU-based approach does not provide a straightforward method, which may have a broader application. The author predicted a variety of malicious attacks, including key encoding and trust management. In this article [8], we incorporate native and global agents to ensure that watchdogs recover all ancient and relayed data packets during transmission. The randomness of the method approach is that global agents intercept not all data packets; rather, malicious nodes alter or forward packets. Another disadvantage of these works is that the high apparent density of nodes does not account for packet collisions. With a graded routing protocol and dynamic group head selection, the performance of Low-energy adaptive clustering hierarchy (LEACH) was analyzed. Through torrents, seeding and leeching are used to connect to peer nodes. It examines the relationship between delay, outturn, and magnitude. Attack makes no mention of energy consumption. The prediction algorithm is based on Markov processes that detect abnormal energy consumption in malicious clusters[9]. Residual energy prediction aides in the selection of packet forwarding nodes. As a result, this paper did not cover every aspect of network security. This algorithm generates a collection of exact solutions by starting with a sample set of possible solutions. The primary advantage is that it provides higher solutions while keeping the total set the same size. These algorithms are used to determine the number of shortest paths across the network's connected bandwidth. Khattak et al.[10] explain that the unexpected multiple wireless routes occur during changes in topology and competition avoidance. In this case, an alternate route is used in case one of the nodes becomes disconnected, which has no effect on the data transmission. Route modification is minimized in a high-quality network. The AODV protocol is used to determine the optimal route and to avoid black and grey hole attacks. This is primarily to improve transmission between the source and destination. A new feature is added to the existing network to apply it to data that must be transmitted to the receiver node. It compares to the amount it receives from supply. Assume that both are equal, and that there is no malicious node along the path. The planned work failed to materialize in the case of a single peer. Sharma et al.[11] investigates how to choose a safe route among multiple paths based on shared hopes. There is no communication performed prior to receiving the RREQ message in this case. This will clarify the disadvantage of delay.

Selvi et. al..[12] state that one way to prevent region attacks is through negotiation of nodes for the purpose of determining locations, with an emphasis on node honesty. When the RREQ message reaches its destination, it immediately returns to the source node to inform it that the route to the receiver was discovered. Once the sender has collected data and suggestions from neighboring nodes. Finally, determines whether or not the receiver is malicious. During this time period, the neighbor's suggestion may be false.

ArulRathi et. .al[13] A wait and check technique was used to prevent multiple malicious nodes. This "wait and check" methodology follows the secure path by collecting messages (RREPs) from nearby nodes using the perennial next node method. The sender node must imagine that the path is safe and secure. If it cannot locate a perennial node, it creates its own path for data packet transmission. Additional delay occurs as a result of the Wait Strategy, which adds additional processing time to complete different nodes. In AODV, the attacker attempts to supply a node in order to move to the receiver node via the shortest path with the fewest hope counts.

The trust management proposal favors the relationship between the magnitude of the common signal and the magnitude of the interference. Trust values are determined by the square value used in the construction of trustworthy structures. Multiple objectives are also taken into account in the length. Trust is made possible by the associate agent's ability to detect an action before it occurs. During communications with the alternate agent, the trust agent was mentioned. Each node detects data forwarding to its neighboring nodes and then measures the sharing of data that is properly shared. Its data can be gathered through referrals and direct observations. Because the performance of a MANET is inherently unstable, a trust change algorithm was introduced. Three modules were mentioned by the author. Certificate Authority had an excellent node result. The following proposal addresses the issue of multi-hop recommendation. It employs a probabilistic method for trust computation and receives the square measure. There was an issue with taking issues into account and establishing accountability gaps.

They previously proposed a trust management system in conjunction with Intrusion Detection Systems (IDS's). The key to a trust management system is a delay-tolerant network. Trust is determined by the creation of a mobile context, the interaction of time, status, and location, and the interaction of users. The Manet square value is dependent on the disruption of the route and the consumption of resources. Disruptive attacks on routes and path messages rearrange the routes and path messages. The second method of attack is to consume energy and fill the nodes' memory with erroneous data packets. They may contain erroneous information in order to disrupt connections between nodes. Alternative nodes disseminate erroneous information to their respective nodes. Malicious nodes may also take advantage of energy and network information. These are the specific ways in which square measure can be expressed. Internal or external attacks on ad-hoc networks occur due to a lack of infrastructure. This attack is mitigated through the use of cryptographic algorithms. Encryption and decryption are performed using both public and private keys. To ensure that the cryptographic asymmetric uses the Secure Ad-hoc On-Demand Distance Vector, authentication is required (SAODV). Checking is accomplished in a point-to-point fashion. Additionally, malicious nature is detected via hop-by-hop checks, and the payment method is used to avoid selfishness.

Safety and Energy consumption is critical, as batteries have a finite capacity. Protocol packets are constructed with the constraint of limiting routing protocols in mind. Energy consumption has a significant impact on hash function encryption algorithms. CPU operations are extremely expensive for hash function encryption algorithms. MANET's analysis is presented in terms of reactive and proactive protocol energy consumption. DTN is evaluated in terms of the effect that energy consumption has on various routing protocols. Epidemic is a routing optimization scheme that aims to improve energy consumption and message delivery. The algorithm for the Digital Signature Scheme identifies the lightest one. MANET routing protocol is used in trust management systems because it consumes more energy. Generally, the Trust Management System manages energy consumption, and simulations can be run with or without a malicious node in the network. Transmission and cryptography operations require additional energy as a result of these analyses.

Kanthe et al.[14] proposed a method for counting false values and maintaining a counter on the receiver side. During the traffic, an honest node converts and sends the requesting node a false response. When a grey hole is detected, the count exceeds the predefined threshold. According to them, crosschecking with the True Link algorithm is proposed to detect black holes. True Link is a technique for verifying black hole entries. Additionally, it conducts cross-checking of cooperative black hole attacks. Routing overhead increases with double cross-checking security factors are high, but the method is time consuming. Jeyarani et al.[15] coined the term "wormhole attack." The timestamp determines a genuine link. It directly connects two nodes and also verifies the connection. Completely autonomous protocols operate in two distinct phases. The communication path does not include any malicious nodes; severe time constraints only constrain it.

J.Sen[16] proposed a new gray hole attack detection algorithm to detect local anomalies and cooperative anomalies. The DRI table is used to determine which nodes are suspect and which are reliable in a network. Throughout the process, the probability of false detection of local anomaly detection decreases.Manet travels via any other route and sponsors network-connected mobile devices. This path modification enabled the use of alternate devices for a brief period[20]. The mobile host must be a self-contained system. Moreover, immediately apply changes to the connected network. Researchers introduce novel techniques to address challenges in Manet's security. The presence of a malicious node complicates security.

In the Impromptu, low-cost mobile devices are used directly. It facilitates the establishment of wireless sensor networks. The primary issue with impromptu wireless networks is their energy inefficiency. Another type of attack is referred to as flooding. During these attacks, a malicious node sends erroneous data packets in order to consume network resources. It is possible to compromise all on-demand protocols along the path. This compromises the data's integrity and confidentiality. The fabled approach of Ad-hoc networks is to modify the topology, the quality of nodes, and the inconvenience instantly. This created an opening for a variety of security issues. Previous attacks have slowed the network's performance. Both AODV and DSR have made contributions to address some security concerns[17].

Unplanned network communities focus on security concerns and social cohesion. Hu et al. [18] propose new techniques for securing the routing layer via cryptographic techniques, which the certificate authority will handle and they projected evidence based on PGP. Path rater identifies and monitors misbehaving nodes through an observation-based technique. However, this method does not penalize malicious nodes; rather, it alleviates their packet burden. Pavithra et al. [19] modified the AODV protocol's defense mechanism against Vicinity attacks. Technique for detecting gray-hole nodes in wireless mesh networks. They discovered new methods for detecting gray-hole attack squares. This new scheme utilizes their adjacent nodes. As a result of these distributed wireless peer networks, infrastructure and fundamental nodes are not affected. Now, the WMN square measure is detecting gray-hole attacks and adult male node stagnation.

Shila et al. mentioned a game theory for locating gray-hole attacks and selecting many feasible routes[20]. They proposed a distributed detection method for gray-hole attacks based on projected thresholds. This method determines whether or not gray-hole nodes have an opposite square measure through adult male nodes. Assume that multiple adult nodes are chosen to serve as gray-hole nodes. It will result in the onset of a broadcast storm.

Devadhasini et .al[21] proposed new technique for detecting malicious nodes. It will trace malicious node easily. The packet forwarding node monitors the transmission of packets in this case. If the watchdog determines that the next node is malicious, it waits a predefined amount of time. They have favored a novel mechanism for verifying the data's path. By transmitting an alternate route request to the next node along the path from source to destination. This method is ineffective at detecting multiple malicious nodes but is effective at eradicating a single malicious node's black hole. To address these issues, A.Sharma et al.[22] developed a new node called the IDS node using secure AODV protocols. By sending the sequence number to the source node, this IDS node updates their routing table. This way, the precise route can be determined and a black hole attack can be detected. The primary disadvantage is that it cannot be used within the communication range of an IDS node.

Z.Alishahi et al.[23] perform a check on the intermediate node's forwarding packets RREQ and

RREP. Based on the RREP, the sender can choose the most secure route to the receiver. They proposed a novel method for determining end-to-end verification. Additionally, determine whether or not the packets reach their destination. If the check fails, the backbone network begins detecting malicious nodes. It is entirely based on the assumption that this will be extremely difficult if there are more malicious nodes.

Chen et al.[24] developed two algorithms: a gossip protocol that makes use of a management algorithm, and an aggregate signature algorithm that makes use of a detection algorithm. Each node should generate a proof with the received message in accordance with these scenarios. When the sender suspects some misbehavior, the checkup algorithm verifies the intermediate node. The Diagnosis algorithm is used to track down malicious nodes. They demonstrate this method by sending a message to the source node prior to sending the block. At the end of transmission, neighbours monitor traffic flow. The destination sends a confirmation message that includes the count of packets received. Monitoring nodes are responsible for collecting responses from malicious nodes and detecting and removing them. These data losses occur when the range of acceptable values is exceeded. Due to the routing overhead mechanism, additional routing packets are generated. Oscar et al.[25] proposed a novel algorithm for detecting packet forwarding inconsistency. This mechanism will classify nodes as well-behaved or misbehaved. Although the average throughput does not reach the network, the algorithm requires perfect timing to extract the necessary data to identify misbehaving nodes. During the Initial phase, misbehaving nodes may drop their data packets as a result of being accused and cut off from the network path. They introduced two-packet AODV routing protocols:. When a node wishes to access the channel, these response sequence packets and code sequence packets are transferred to the MAC layer. Each intermediate node transmits a code sequence, which neighbouring nodes respond to with their own response message. Neighboring nodes exchange data with one another. If they allow connection, they will proceed in their own manner. Otherwise, identify the remaining node as malicious. From the start, malicious nodes are selected without delay. Generally, malicious nodes with the highest destination id are malicious.

Bobby Sharma[26] proposed a cooperative distributed algorithm for detecting and separating gray hole attackers. When the system detects the presence of gray hole attackers, it notifies neighboring nodes. They will monitor the state and response of adjacent nodes. If an attacker is discovered, that node's communication is terminated. They developed a new algorithm known as Bulwark-AODV protocols. This prevents both single and cooperative black hole attacks and identifies malicious route replies between source and destination nodes. Additionally, it determines the shortest valid path. By comparing data packets to ACKs, this algorithm discovers gray holes. And, they used the multiple path technique to create their intermediate node. That nodes respond and determine whether or not the path between the intermediate node and the destination node is available. When the next hop is unavailable, it does not send data packets.

Al Yahmadi, et al.[27] proposed a new method for tracing malicious nodes through the use of a watchdog. For packet forwarding, a predefined threshold time is maintained. If the next node does not transmit data packets, it is referred to as a malicious node. They have proposed a cluster-based algorithm for preventing MANET black hole attacks. The Friendship Table is used to assist us in locating the malicious node and its precise location at the appropriate time. The trust estimator is used to determine the updated value. They also described a suitable two-stage method for detecting multiple malicious nodes in their paper. Two tables will be maintained: a series table and a status table. Each node includes a list of its neighbors for additional information. An intermediate node will detect a suspicious decision-making node. An alert message is sent to the other network, and the information in its status table is modified. A watchdog is a system security tool that guards against specific software or hardware failures that could result in a system ceasing to respond. In route determination, the watchdog function is used to detect malicious nodes. Additionally, it provides a different path to the source node. This makes use of tables to store information about pending packets and also retains node scores. This is entirely dependent on the dissipated mode. The CPU transmits frames to a wireless network interface controller or a wired network interface via a wireless network interface controller.

Table 1.Simulation framework

No. of Nodes	30,60,90,120,150,180
Pause time	10 Seconds
MAC layer	IEEE 802.11
Simulation run time	120 seconds
Packet size	512 bytes
Attack type	Black hole Attack

Table 1 shows the simulation parameters for NS2 simulation. Table 2 shows the various techniques adopted in Wireless Sensor Networks.

Table 2.Comparison Table for Various WSN techniques

Author	Advantages	Disadvantages	Techniques
N. Dharini1, Ranjith Balakrishnan2 and A. Pravin Renold3	Faster intrusion detection because of distributed detection architecture. Early detection of attacker nodes.	Extensive performance detection algorithm needed	Wireless Sensor Network
Kriti Chadha , Dr. Sushma Jain	The network performance can be measured using throughput	End to end packet delay in the transmission	VANET
Hizbullah Khattak, Nizamuddin	To prevent black/grey hole attack by using second shortest route for security purpose	The measure of throughput and delay are not taken in simulation	MANET (Mobile Ad-hoc Network)
Seemita Pal, Aditya Ashok, Siddharth Sridhar	Simulation results are used to impact the different types of packet	For more comparison of the drop-rates the more sturdy	PMU (Phasor Measurement Unit)

	droplet attack.	algorithms are needed.	
Yugandhara S. Patil, Dr. Ashok M. Kanthe	False message is identified by TrueLink concept and redirect the communication path.	It takes more time for identifying the false message	TrueLink Concept is used.
Kusumlata Sachan, Manisha Lokhande	It produce better results for larger number of nodes.	Need for better performance enhancement.	MANET using DSR protocols
Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar	Security mechanism is used against cooperative grayhole attack	network traffic overhead.	MANET (Mobile AD-hoc Network)
Jyoti Prabha Singh, Jyoti Prabha Singh, Savita Shiwani, Vishal Gaur	Individual nodes are moving with own decided routes	Delay in transferring data packets	Denial of Service attack (DOS)
Moirangthem Marjit Singh, Jyotsna Kumar Mandal	Larger number of nodes are used in the communication link	The performance decrease with increasing the number of malicious nodes	AODV protocol
G.Usha, Dr.S.Bose	These simulations of grey hole attack is taken for packet delivery ratio, dropped packets, overhead.	Additional attack such as collision and sink attacks are not detected	MANET using AODV protocols

Conclusion

In this paper, black hole attack and gray hole attack analysis in DSR and AODV protocols are explained with its reliability and measures are presented. The various WSN techniques are compared as the result, when the number of nodes is increases and the reliability also increases.

References

1. Canizares, C., T. Fernandes, E. Geraldi, L. Gerin-Lajoie, M. Gibbard, I. Hiskens, J. Kersulis et al. "Benchmark models for the analysis and control of small-signal oscillatory dynamics in power systems." *IEEE Transactions on Power Systems* 32, no. 1 (2016): 715-722.
2. Rueda, José L., and István Erlich. "Impacts of large scale integration of wind power on power system small-signal stability." In *2011 4th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT)*, pp. 673-681. IEEE, 2011.
3. John A., Ananth Kumar T., Adimoolam M., Blessy A. (2021) Energy Management and Monitoring Using IoT with CupCarbon Platform. In: Balusamy B., Chilamkurti N., Kadry S.

(eds) Green Computing in Smart Cities: Simulation and Techniques. Green Energy and Technology. Springer, Cham. https://doi.org/10.1007/978-3-030-48141-4_10.

4. ArjunaraoVatti, R., Kumar, K., Haripriya, D. et al. Design of low power RF CMOS power amplifier structure with an optimal linear gain controller for future wireless communication. J Ambient Intell Human Comput (2021). https://doi.org/10.1007/s12652-021-03011-4.
5. Kumar, Sudheer, and Nitika Vats Doohan. "A modified approach for recognition and eradication of extenuation of gray-hole attack in MANET using AODV routing protocol." In *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, pp. 1-5. IEEE, 2016.
6. R. Kalaipriya, S. Devadharshini, R. Rajmohan, M. Pavithra and T. Ananthkumar, "Certain Investigations on Leveraging Blockchain Technology for Developing Electronic Health Records," 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), 2020, pp. 1-5, doi: 10.1109/ICSCAN49426.2020.9262391.
7. Jafarigiv, Danial, Keyhan Sheshyekani, Houshang Karimi, and Jean Mahseredjian. "A Scalable FMI-Compatible Cosimulation Platform for Synchrophasor Network Studies." IEEE Transactions on Industrial Informatics 17, no. 1 (2020): 270-279.
8. Liu, Anfeng, Zhuangbin Chen, and Neal N. Xiong. "An adaptive virtual relaying set scheme for loss-and-delay sensitive WSNs." *Information Sciences* 424 (2018): 118-136.
9. Gomathy, V., Neelamadhab Padhy, Debabrata Samanta, M. Sivaram, Vishal Jain, and Iraj Sadegh Amiri. "Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks." *Journal of Ambient Intelligence and Humanized Computing* 11, no. 11 (2020): 4995-5001.
10. Liu, Jun, and Asad J. Khattak. "Delivering improved alerts, warnings, and control assistance using basic safety messages transmitted between connected vehicles." Transportation research part C: emerging technologies 68 (2016): 83-100.
11. Sharma, Suraj, and Sanjay Kumar Jena. "A survey on secure hierarchical routing protocols in wireless sensor networks." In Proceedings of the 2011 international conference on communication, computing & security, pp. 146-151. 2011.
12. S. A. Selvi, T. A. kumar, R. S. Rajesh and M. A. T. Ajisha, "An Efficient Communication Scheme for Wi-Li-Fi Network Framework," *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2019, pp. 697-701, doi: 10.1109/I-SMAC47947.2019.9032650.
13. Design and Development of an Efficient Branch Predictor for an In-order RISC-V Processor [Текст] / C. Arul Rathi, G. Rajakumar, T. Ananth Kumar, T.S. Arun Samuel // Журнал нано- та електронної фізики.-2020.-Т. 12, № 5.-05021.-DOI: 10.21272/jnep.12(5).05021.
14. Shukla, Parineet D., Ashok M. Kanthe, and Dina Simunic. "An analytical approach for detection of gray hole attack in mobile ad-hoc network (MANET)." In 2014 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-5. IEEE, 2014.
15. J. Jeyaranjani, T. Dhiliphan Rajkumar, T. Ananth Kumar, Coronary heart disease diagnosis using the efficient ANN model, Materials Today: Proceedings, 2021, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2021.01.257.

16. Sen, Jaydip. "An intrusion detection architecture for clustered wireless ad hoc networks." In 2010 2nd International Conference on Computational Intelligence, Communication Systems and Networks, pp. 202-207. IEEE, 2010.
17. T. Ananth Kumar and R. S. Rajesh, "Towards power efficient wireless NoC router for SOC," *2014 International Conference on Communication and Network Technologies*, 2014, pp. 254-259, doi: 10.1109/CNT.2014.7062765.
18. Wang, Yujie, Pu Chen, Jiang Hu, and Jeyavijayan JV Rajendran. "Routing perturbation for enhanced security in split manufacturing." In 2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 605-510. IEEE, 2017.
19. Pavithra, M., R. Rajmohan, T. Ananth Kumar, and R. Ramya. "Prediction and Classification of Breast Cancer Using Discriminative Learning Models and Techniques." *Machine Vision Inspection Systems, Volume 2: Machine Learning-Based Approaches* (2021): 241-262.
20. Shila, Devu Manikantan, and Tricha Anjali. "A game theoretic approach to gray hole attacks in wireless mesh networks." In MILCOM 2008-2008 IEEE Military Communications Conference, pp. 1-7. IEEE, 2008.
21. S. Devadharshini, R. Kalaipriya, R. Rajmohan, M. Pavithra and T. Ananthkumar, "Performance Investigation of Hybrid YOLO-VGG16 Based Ship Detection Framework Using SAR Images," 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), 2020, pp. 1-6, doi: 10.1109/ICSCAN49426.2020.9262440.
22. Sharma, Himanshu, Ahteshamul Haque, and Zainul A. Jaffery. "Solar energy harvesting wireless sensor network nodes: A survey." Journal of Renewable and Sustainable Energy 10, no. 2 (2018): 023704.
23. Alishahi, Zahra, Javad Mirabedini, and M. Rafsanjani. "A new method for improving security in MANETs AODV Protocol." Management Science Letters 2, no. 7 (2012): 2271-2280.
24. Chen, Rui-Yang. "A traceability chain algorithm for artificial neural networks using T–S fuzzy cognitive maps in blockchain." Future Generation Computer Systems 80 (2018): 198-210.
25. Vučinić, Mališa, Bernard Tourancheau, Franck Rousseau, Andrzej Duda, Laurent Damon, and Roberto Guizzetti. "OSCAR: Object security architecture for the Internet of Things." Ad Hoc Networks 32 (2015): 3-16.
26. Kakoty, Bobby Sharma, S. M. Hazarika, and N. Sarma. "NAODV-Distributed Packet Dropping Attack Detection in MANETs." International Journal of Computer Applications 83, no. 11 (2013).
27. Al Yahmadi, Faisal, and Muhammad R. Ahmed. "Taxonomy of Threats and Vulnerabilities in Smart Grid Networks." International Journal of Energy and Power Engineering 15, no. 4 (2021): 168-171.