iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XII **Month of publication:** December 2021

DOI: https://doi.org/10.22214/ijraset.2021.39567

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 9 Issue XII Dec 2021- Available at www.ijraset.com

Security Techniques in MANET: A Study

Atul Patial
Research Scholar, Computer Science and Engineering, Chandigarh University, Gharuan, Mohali (Punjab)

Abstract: ***MANET (mobile ad hoc network) is considered to be a network with no centralized control. This network typically faces two major challenges related to routing and security. Both these issues affect the performance of this network to a large extent. The black hole attack belongs to the category of active attacks that are launched to reduce the network throughput and other parameters. The research works carried out in the past used different techniques to isolate malicious nodes, but with the inclusion of extra hardware and software tools. The various techniques for the security in MANET are analyzed in terms of certain parameters.***

Keywords: MANET, Black Hole, Security Techniques

I. INTRODUCTION

MANET becomes an interesting field for research as this network is less expensive and contains mobile devices of small as well as big sizes. This innovative genre of self-organizing network leads to integrate the wireless communication with a node having higher mobility. Different from the conventional wired networks, this kind of network is not consisted of any permanent model such as sink, central control point etc.

The relationship among nodes is assisted in developing a random topology. MANET has acquired the popularity among researchers for their implementation in various applications such as applications of armed forces in which topology of network is changed rapidly for representing the operational activities of army and disaster recovery movements and the current framework has not contained any functionality [1].

These networks are effective for the virtual conferences as it has self-organized infrastructure at which a conventional network set-up is established that is a tedious and costly task. The conventional networks are utilized to accomplish diverse tasks to transmit the packet, perform the routing, and to manage the network with the help of dedicated nodes. Consequently, all the existing nodes are implemented to perform these tasks collaboratively. In MANETs, the deployed nodes focus on multi-hop strategy for establishing the communication with each other. It means that the motes that are within radio range of each other are free to interact via wireless channels in direct manner where as the nodes that are far away must rely on intermediate nodes for acting like the routers in order to deliver the message. Mobile nodes are capable of moving, exiting and joining the networks. To update the routes is required as these networks have dynamic topology.

The security has been a major field of research since last decades in wire line networks. Thus, various novel non-trivial issues are occurred in Mobile as hoc Networks for security design as this network has effective attributes. Consequently, the standard security techniques of wired networks cannot be applied directly to MANET domains. The main objective of security techniques is that security services must be offered, such as privacy, integrity and availability to mobile users. To achieve this goalmouth, security techniques must be capable of securing all the algorithms. The technique to protect MANETs has two categories. The proactive technique focuses on implementing diverse kinds of cryptographic techniques for prohibiting an attacker when it launches the attacks in the first area. The reactive technique can detect security threats in advance and reverts back accordingly. Due to the deficiency of a clear line of defence, the major purpose of whole security technique is to combine both techniques and include all 3 elements. To illustrate, we can use proactive technique for ensuring the accuracy of routing positions, whereas the packet relaying operations are protected with the deployment of reactive method. Security is a chain, and considers as a secure link. In case of absence of single component, the strength of the entire security solution faces the degradation.

Mobile ad hoc Networks have susceptibility against routing attacks namely blackhole and Gray hole due to unavailability of any existing substructure along with the dynamic topology characteristic. Black hole attack is such a DoS attack. The blackhole attack allows a node for relaying a malevolent message in which direct route is constructed to the destination for intercepting the messages [5]. Hence, a malevolent node is able to transmit false RREP messages for attracting all packets, and deceitfully claiming that it contains forge direct route to the destination and then leads to drop these packets without sending them to the destination. An example of black hole node is shown in Fig. 1.

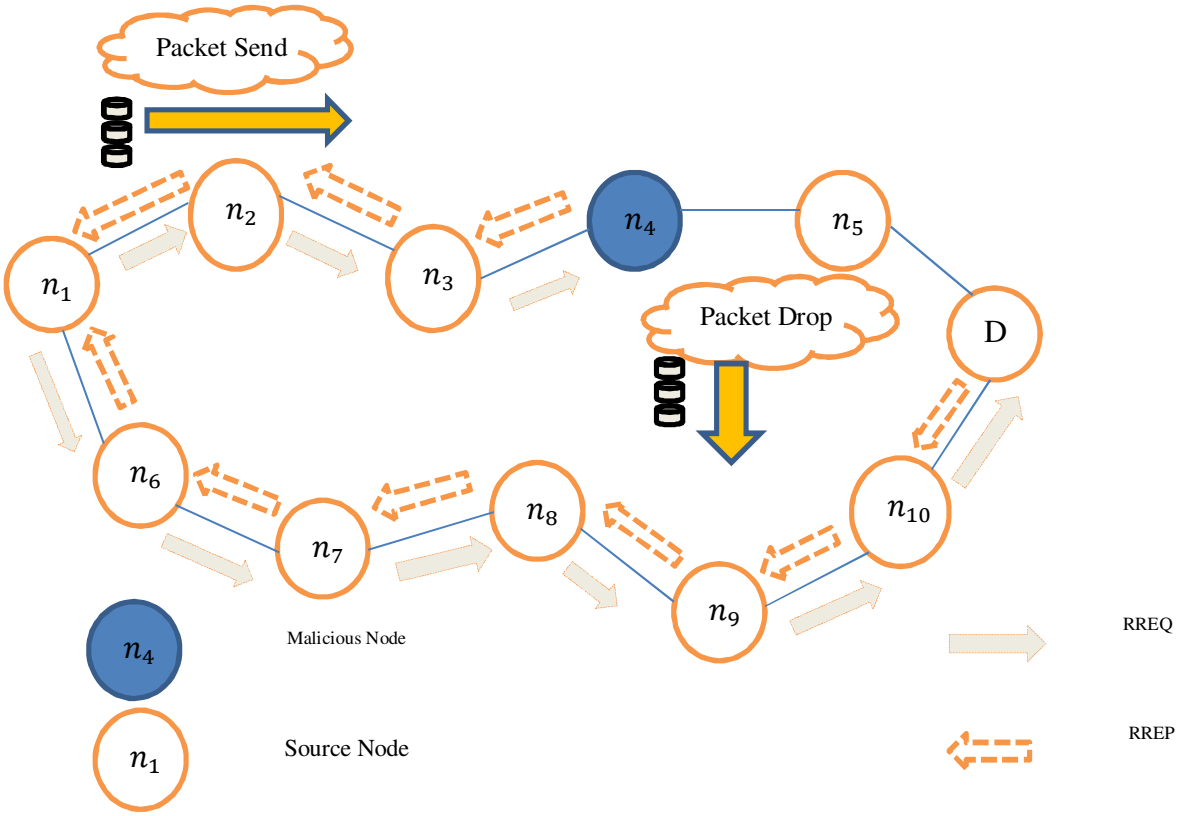


Figure 1: Blackhole attack–node n4 drops all the data packets.

The source node is represented withn_1 and the node D denotes the destination node. $n_4$is responsible for transmitting the forged route request packets. The source node is utilized for forwarding RREQ to its neighbouring nodes for establishing a path towards destination. $n_6$is deployed to forward the route request packet to n_7 and n_8, n_9, n_{10} nodes assist insending the packet to the destination. Thereafter, node D is used to revert back to route request packet and represent it as target node. But, on the other path,$n_3$is utilized to forward the route request packet ton_4. Generally,$n_4$must have potential for sending the route request packet to $n_5$tocreate the routing path [6]. The malicious mote$n_4$sends forged packet and claims that it has the shortest path to destination. Moreover, the noden_4 drops the received packet that $n_3$has transmitted and forwarded it to target. Network operation stops working due to the inaccurate routing as the malicious node n_4 is present. Consequently, the network has poor PDR as the blackhole node is present in the network.

II. LITERATURE REVIEW

Elbasher Elmahdi, et.al (2020) projected an innovative method in order to transmit the data with reliability and security in MANETs when the blackhole attacks were occurred on the basis of AOMDV algorithm [7]. The message was split into diverse paths and HE was implemented to perform the cryptography. The constancy of the projected method was proved as it attained higher PDR and resistance for dealing with the attack. The experimental outcomes indicated the supremacy of the projected method over the traditional model and assisted in boosting the packet delivery ratio and throughput when the blackhole attack was activated in network.

Sijan Shrestha, et.al (2020) discussed that the blackhole attack had interrupted the flow of data to mitigate the network efficacy [8]. Thus, an algorithm was suggested on the basis of a technique utilized to change the sequence number of control packets such as the Route Reply Packets of AODV routing algorithm so that the blackhole nodes were detected and the data loss was diminished with the elimination of the route via Blackhole nodes. The experimental outcomes demonstrated that the suggested algorithm performed effectively in IDS.

Shweta Pandey, et.al (2020) introduced a mechanism to establish using which higher QoS parameters were obtained because of the behavior of Mobile ad-hoc Network [9]. The trust was computing using Ad-hoc-on-Demand Distance Vector. Artificial Neural Network and Support Vector Machine algorithms were implemented to identify the black hole attack in network. The outcomes were generated after comparing the introduced mechanism with others. An analysis was performed on acquired outcomes considering several nodes. The experimental results depicted the efficacy of introduced mechanism for mitigating the energy use up to54.72%, enhancing the throughput by 88.68kbps, PDR up to 92.91% and E2E delay by 37.27ms.

Vedant Sharma, et.al (2020) developed TCP analysis so that the blackhole attack was detected [10]. In diverse circumstance, reliable transport layer algorithm TCP was analyzed for the effects of the attack on network. For this, a set of metrics was utilized to analyze the effects in the simulation. The simulation results indicated that the developed approach had attained superior throughput and E2E delay.

Aly M. El-Semary, et.al (2019) established a secure MANET algorithm known as BP-AODV in order to address the security issues about Secure-Ad hoc On-Demand Distance Vector [11]. Furthermore, a cooperative blackhole attack occurred in routing process was mitigated and the preventive measures were obtained to deal with the attack while transmitting the data using this algorithm. The chaotic map attributes were exploited to expand the functionality of the Ad hoc on-Demand Distance Vector so that the established algorithm was constructed. The experimental outcomes revealed that the established algorithm was more secure as compared to the SAODV protocol and offered protection against the blackhole attack.

ElbasherElmahdi, et.al (2018) designed a reliable and secure technology of data transmission for MANETs (mobile ad-hoc networks) to counter blackhole attacks [12]. Two strategies called AOMDV (Adhoc On-Demand Multipath Distance Vector) protocol and HE (Homomorphic Encryption) system were presented for this purpose. The new technology met the standard of scalability. In simulation-based results, the devised methodology showed considerable improvement in PDR (Packet Distribution Ratio) and network throughput under blackhole attack scenario.

Mohammed Baqer M. Kamel, et.al (2017) developed a STAODV (secure and trust-based approach method based on ad hoc on demand distance vector) protocol to make AODV protocol securer [13]. This protocol helped identify adversaries who used preceding information to activate attack in the network. A confidence level was attached to each node that took part in the detection of that node's trust level. The black hole attack was dealt with by examining every packet received. The developed algorithmic scheme provided an improved PDR and throughput to counter black hole attack activated by multiple spiteful nodes.

Amar Taggu, et.al (2018) presented a basic and effectual IDS (Intrusion Detection Scheme) for the application layer of ad hoc networks for blackhole detection [14]. Subsequently, reverse root detection techniques were carried forward to detect blackholes in the network. These Multiple black holes were discovered in the DSR protocol-supported MANET (Mobile Ad-hoc Network) through Mas (Mobile Agent) and this approach was extended to trace route. The MA confirmed that that there was no need to modify existent routing algorithms or other lower layers. In the simulation results, the formulated algorithmic scheme discovered single and multiple blackhole nodes at different speeds of the mobile nodes.

Preeti Tonane, et.al (2018) introduced trust technique based on vector. This approach was applied to the conduct of nodes during the broadcast and plunging of the data packets for deciding the trust on all nodes [15]. The ECR (Enhanced Certificate Revocation) technique was carried out for keeping away from the aggressor for which the blackhole assailant was boycotted. The configuration and node were made safer by allocating a novel key for each individual node that was equipped for keeping away from the greater part of the assaults in MANETs.ECR was aimed at performing proficient denial of nodes that behaved mischievous. Subsequently, the time revocation got improved. The introduced framework was relevant for mitigating the energy utilization of the nodes with less interaction and computation cost.

Table 1: Table of Comparison

Author	Year	Description	Outcomes
Elbasher Elmahdi	2020	An innovative method in order to transmit the data with reliability and security in MANETs when the blackhole attacks were occurred on the basis of AOMDV algorithm. The message was split into diverse paths and HE was implemented to perform the cryptography	The experimental outcomes indicated the supremacy of the projected method over the traditional model and assisted in boosting the packet delivery ratio and throughput when the blackhole attack was activated in network.

Sijan Shrestha	2020	The blackhole attack had interrupted the flow of data to mitigate the network efficacy. Thus, an algorithm was suggested on the basis of a technique utilized to change the sequence number of control packets such as the Route Reply Packets of AODV routing algorithm so that the blackhole nodes were detected and the data loss was diminished with the elimination of the route via Blackhole nodes.	The experimental outcomes demonstrated that the suggested algorithm performed effectively in IDS.
Shweta Pandey	2020	The trust was computing using Ad-hoc-on-Demand Distance Vector. Artificial Neural Network and Support Vector Machine algorithms were implemented to identify the black hole attack in network.	An analysis was performed on acquired outcomes considering several nodes. The experimental results depicted the efficacy of introduced mechanism for mitigating the energy use up to54.72%, enhancing the throughput by 88.68kbps, PDR up to 92.91% and E2E delay by 37.27ms.
Vedant Sharma	2020	In diverse circumstance, reliable transport layer algorithm TCP was analyzed for the effects of the attack on network. For this, a set of metrics was utilized to analyze the effects in the simulation	The simulation results indicated that the developed approach had attained superior throughput and E2E delay
Aly M. El-Semary	2019	A secure MANET algorithm known as BP-AODV in order to address the security issues about Secure-Ad hoc On-Demand Distance Vector. Furthermore, a cooperative blackhole attack occurred in routing process was mitigated and the preventive measures were obtained to deal with the attack while transmitting the data using this algorithm	The experimental outcomes revealed that the established algorithm was more secure as compared to the SAODV protocol and offered protection against the blackhole attack
Elbasher Elmahdi	2018	A reliable and secure technology of data transmission for MANETs (mobile ad-hoc networks) to counter blackhole attacks. Two strategies called AOMDV (Adhoc On-Demand Multipath Distance Vector) protocol and HE (Homomorphic Encryption) system were presented for this purpose	In simulation-based results, the devised methodology showed considerable improvement in PDR (Packet Distribution Ratio) and network throughput under blackhole attack scenario.
Mohammed Baqer M. Kamel	2017	A STAODV (secure and trust-based approach method based on ad hoc on demand distance vector) protocol to make AODV protocol securer	The developed algorithmic scheme provided an improved PDR and throughput to counter black hole attack activated by multiple spiteful nodes.
Amar Taggu	2018	A basic and effectual IDS (Intrusion Detection Scheme) for the application layer of ad hoc networks for blackhole detection . Subsequently, reverse root detection techniques were carried forward to detect blackholes in the network.	In the simulation results, the formulated algorithmic scheme discovered single and multiple blackhole nodes at different speeds of the mobile nodes.

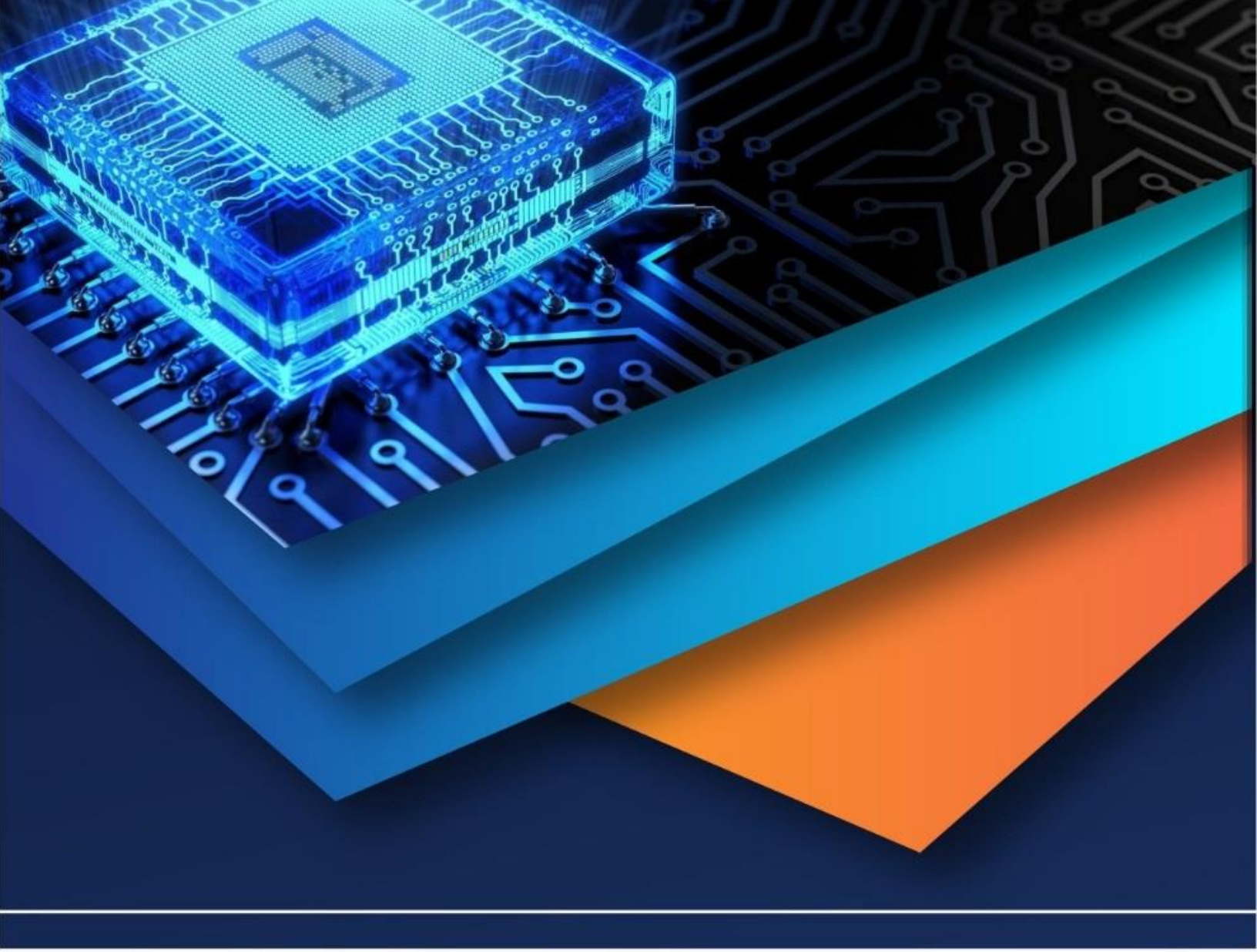
Preeti Tonane	2018	This approach was applied to the conduct of nodes during the broadcast and plunging of the data packets for deciding the trust on all nodes. The ECR (Enhanced Certificate Revocation) technique was carried out for keeping away from the aggressor for which the blackhole assailant was boycotted.	The introduced framework was relevant for mitigating the energy utilization of the nodes with less interaction and computation cost.

III. CONCLUSION

In a nutshell, MANET is a distributed network in which moving nodes have freedom of joining or leaving the network at will. Security is a crucial issue in such networks. The lack of security badly affects the networks' productivity. This research project presents a new methodology to remove or detect a variety of damaging attacks or adversaries from the network. To trace and insulate the affected nodes, a trust-based mechanism has been applied in the network. The various security related techniques to mobile ad hoc network is reviewed in terms of certain parameters

REFERENCES

[1] Vaishali Gaikwad Mohite, Lata Ragha, "Security agents for detecting and avoiding cooperative blackhole attacks in MANET", 2015, International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Vol. 6, No. 10, pp. 865-870
[2] Avni Tripathi, Amar Kumar Mohapatra, "Mitigation of Blackhole attack in MANET", 2016, 8th International Conference on Computational Intelligence and Communication Networks (CICN),Vol. 1, No. 27, pp. 119-124
[3] S. Sivanesh, V.R. Sarma Dhulipala, "Comparitive Analysis of Blackhole and Rushing Attack in MANET", 2019, TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW), Vol. 14, No. 6, pp. 207-211
[4] Guoquan Li, Zheng Yan, Yulong Fu, "A Study and Simulation Research of Blackhole Attack on Mobile AdHoc Network", 2018, IEEE Conference on Communications and Network Security (CNS), Vol. 3, No. 1, pp. 588-593
[5] Alpana Kumari, Shoba Krishnan, "Analysis of Malicious Behavior of Blackhole and Rushing Attack in MANET", 2019, International Conference on Nascent Technologies in Engineering (ICNTE), Vol. 14, No. 25, pp. 293-297
[6] Ali Hameed, Alauddin Al-Omary, "Survey of blackhole attack on MANET", 2019, 2nd Smart Cities Symposium, Vol. 2, No. 18, pp. 80-85
[7] ElbasherElmahdi, Seong-Moo Yoo, Kumar Sharshembiev, "Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks", 2020, Journal of Information Security and Applications, Vol. 11, No. 9, pp. 676-682
[8] Sijan Shrestha, Ranjai Baidya, BivekGiri, Anup Thapa, "Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol", 2020, 8th International Electrical Engineering Congress (iEECON), Vol. 15, No. 1, pp. 352-357
[9] Shweta Pandey, Varun Singh, "Blackhole Attack Detection Using Machine Learning Approach on MANET", 2020, International Conference on Electronics and Sustainable Communication Systems (ICESC), Vol. 6, No. 23, pp. 398-403
[10] Vedant Sharma, Renu, Tanu Shree, "An adaptive approach for Detecting Blackhole using TCP Analysis in MANETs", 2020, 2nd International Conference on Data, Engineering and Applications (IDEA), Vol. 15, No. 20, pp. 404-408
[11] Aly M. El-Semary, Hossam Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map", 2019, IEEE Access, Vol. 1, No. 19, pp. 753-758
[12] ElbasherElmahdi, Seong-Moo Yoo, Kumar Sharshembiev, "Securing data forwarding against blackhole attacks in mobile ad hoc networks", 2018, IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Vol. 4, No. 25, pp. 267-272
[13] Mohammed Baqer M. Kamel, Ibrahim Alameri, Ameer N. Onaizah, "STAODV: A secure and trust-based approach to mitigate blackhole attack on AODV based MANET", 2017, IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Vol. 10, No. 2, pp. 825-829
[14] Amar Taggu, Abhishek Mungoli, Ani Taggu, "ReverseRoute: An Application-Layer Scheme for Detecting Blackholes in MANET Using Mobile Agents", 2018, 3rd Technology Innovation Management and Engineering Science International Conference (TIMES-iCON), Vol. 14, No. 17, pp. 577-582
[15] PreetiTonane, Sachin Deshpande, "Trust Based Certificate Revocation and Attacks in MANETs", 2018, Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Vol. 21, No. 9, pp. 754-760



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY