International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Efficient Approach for Prevention of Blackhole Attack in MANET

[1]Jyoti Dhanke, [2]Shishir Rastogi, [3]Kamaljeet Singh, [4]Komal Saxena, [5]Kaushal Kumar and [6]Prateek Mishra

Submitted: 23/11/2023 **Revised**: 28/12/2023 **Accepted**: 07/01/2024

Abstract: A structure known as a Mobile Ad-Hoc Network (MANET) is formed when mobile nodes come together to communicate with each other, offering a broad spectrum of applications. MANET, characterized by its lack of a central monitoring authority and absence of a fixed infrastructure, gains popularity due to its ubiquitous nature. However, the openness of MANET introduces security challenges that require detection and resolution. One prevalent issue is the Packet Drop Attack, wherein an intruder falsely claims to possess the shortest route to the destination, dropping all packets without forwarding them. This paper addresses the mitigation of this problem, focusing on the optimal solution for the Blackhole Attack. Researchers employ various techniques, such as Opinion-based, Trust-based, Intrusion Detection, Crypto-based, and Destination Sequence Number (DSN) based methods. The proposed method specifically employs DSN, where the attacker lures packets by sending a forged RREP message to the source node. To thwart this, the DSN in the proposed method is compared to a threshold value, allowing the rejection of forged RREP messages.

Keywords: *MANET; Blackhole attack; DoS attack; AODV; Routing Attack*

Introduction

Mobile ad hoc networks (MANETs) have gained popularity due to their cost-effectiveness and flexible network access services for various portable devices, including PDAs, laptops, mobile phones, notepads, etc. These devices play a pivotal role in transitioning from the personal computer age to the ubiquitous computing age. Leveraging wireless communication, they have spurred research activities in wireless networking technology over the last decade. With applications in crucial sectors like finance, healthcare, retail, transportation, and data transmission relying on the Internet, these devices have become integral to daily life. However, the increasing prevalence of malicious anomalies introduced by various attackers has prompted a surge in the popularity of network security, offering mechanisms to protect and safeguard networks from security attacks. Computer networks are broadly categorized into wired and wireless, with wireless networks featuring mobile nodes without physical connections. These networks utilize radio frequency for communication, offering advantages such as mobility, cost efficiency, and easy installation. The key conveniences provided by wireless networks include:

- Mobility: Wireless networks allow mobile users to easily join and use network resources while on the move.
- Flexibility: Unlike wired connections, wireless networks can cover areas inaccessible to wires, enabling connectivity while driving or roaming.
- Simplicity: Wireless networks are easy to install as they lack a fixed infrastructure, allowing nodes to be present anywhere within the network's range.

Routing Mechanism in MANET: MANET routing protocols are categorized into four types based on their use, as outlined by Agrawal et al. (2011):

Proactive Routing Protocol: This type involves every mobile node maintaining complete network information to expedite the route discovery process.

[1]*Department of Engineering Science (Mathematics), Bharati Vidyapeeth's College of Engineering, Lavale, Pune 412115, Maharashtra, India, jyoti.dhanke@bharatividyapeeth.edu, Orcid ID :0000-0002-1817-9438*
[2]*Roots Group of Institutions, Bijnor, rastogi.shishir@yahoo.com*
[3]*School of Computer Application, Lovely Professional University Phagwara Punjab, kamaljeet.sbbs@gmail.com*
[4]*Amity Institute of Information Technology, Amity University, Noida, ksaxena1@amity.edu*
[5]*Department of Computer Science & Engineering, Manav Rachna International Institute of Research and Studies Faridabad, India, kaushalkumar.set@mriu.edu.in*
[6]*Department of Computer Science and Engineering, Asia Pacific Institute of Information Technology SD INDIA, PANIPAT, HARYANA, prateekmishra25@rediffmail.com*

However, the high mobility of nodes can result in the dissemination of invalid information. Examples of proactive routing protocols include Destination Sequenced Distance Vector (Perkins et al., 1994), Topology Broadcast based on Reverse Path Forwarding (Ogier et al., 2004), Optimized Link State Routing (Thomson et al., 2001), and Cluster-head Gateway Switch Routing (Chinang et al., 1997).

Reactive Routing Protocol: In this category, a mobile node seeks to discover a route to a destination only when necessary. Examples of reactive routing protocols encompass Dynamic Source Routing (Johnson et al., 1996), Ad-hoc On-Demand Distance Vector (Perkins et al., 2003), Temporally Ordered Routing Algorithm (Park et al., 1997), and Dynamic MANET On Demand (Chakeres et al., 2006).

Hybrid Routing Protocol: This protocol type combines proactive and reactive routing features. Noteworthy examples of hybrid routing protocols include Zone-based Hierarchical Link State Routing Protocol (Joa-Ng and Lu, 1999), Cluster-head Gateway Switch Routing (Chinang et al., 1997), Order One MANET Routing Protocol (Macker, 1999), and Zone Routing Protocol (Haas, 1997).

Hierarchical Routing Protocol: In hierarchical routing protocols, mobile nodes can select either proactive or reactive routing protocols based on a hierarchy label. Examples of hierarchical routing protocols include Cluster-Based Routing Protocol (Roth, 2011), Fisheye State Routing Protocol (Iwata et al., 1999), and Zone-based Hierarchical Link State Routing Protocol (Joa-Ng and Lu, 1999).

Related work

Numerous studies have addressed the security concerns, particularly the Blackhole attack, in MANET. These investigations predominantly focus on the reactive routing protocol, such as Ad-hoc On-Demand Distance Vector (AODV), where a Blackhole attack disrupts the MANET performance. Attackers send forged RREP messages to the source with elevated destination sequence numbers and lower hop counts. Exploiting the route selection criteria of the source node, which prioritizes lower hop counts and higher destination sequence numbers, the attacker successfully diverts data packets through a path of their choosing. This malicious strategy, known as a packet drop attack, has prompted the development of various preventive solutions. Researchers have proposed different methods, including sequence number-based, intrusion detection-based, cryptography-based, and trust-based solutions. Each solution, however, comes with its own set of challenges, such as computation overhead, time delay, routing overhead, and cooperative Blackhole problems. For instance, Deng et al. (2002) introduced an algorithm to prevent AODV networks from Blackhole attacks, crosschecking RREP packets with the next node on the route for an alternate path.

Ghosh et al. (2004) incorporated a trust field in RREQ messages, allowing the source node to select a path with the highest trust value.

Tamilselvan and Sankaranarayanan (2007) proposed a timer-based approach to identify repeated next nodes in RREP messages.

Sachan and Khilar (2011) employed cryptographic methods using HMAC for fast message verification. Gajera and Sowmya (2012) used a threshold and cryptographic mechanisms to thwart Blackhole attacks.

Jaiswal and Kumar (2012) focused on the sequence numbers of destination and source nodes, while Maheshwar and Singh (2012) introduced an intrusion prevention system acknowledging misbehaving nodes. Singh and Singh (2013) collected RREP messages, discarding those with high DSN compared to SSN. Varshney et al. (2014) proposed the WAODV protocol, incorporating watchdogs to confirm proper packet forwarding.

Aware and Bhandari (2014) introduced an approach to ignore the first RREP, using SHA-1 hash function for data packet verification. Gurung et al. (29) introduced dynamic threshold values for destination sequence numbers to mitigate Blackhole attacks, outperforming existing approaches.

Shukla et al. (30) used ECC to mitigate Blackhole and wormhole attacks, showing superior performance in terms of packet delivery ratio, energy consumption, and end-to-end delay.

Talukdar et al. (31) presented three approaches, utilizing IDS and encryption to detect and prevent Blackhole attacks, demonstrating improved performance metrics in simulations conducted using

Proposed Work

In AODV routing protocol source node broadcast the RREQ message to all its neighbors, when it wants to transmit data. Route finding is based on ring search algorithm. Figure 1 shows the RREQ and RREP in AODV protocol. This RREQ message has following structure.

$$< S, D, 10{,}120, , 0 >$$

This RREQ has source S, destination D, broadcast id 10, SSN 120 and hop count 0. This RREQ is broadcast to all the neighbors**.**

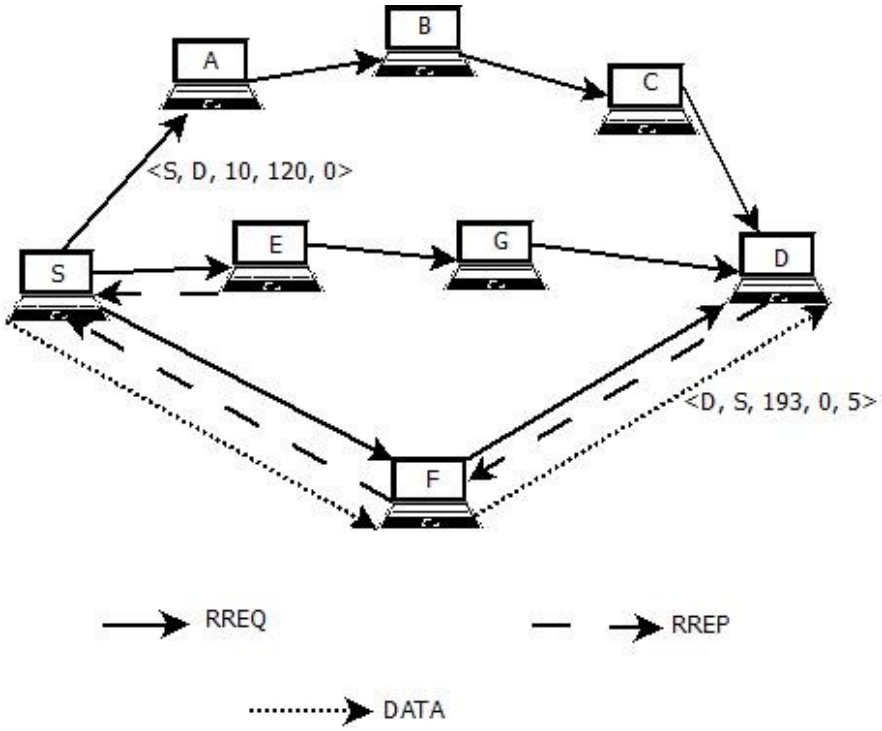

Fig 1: RREQ and RREP messages in AODV

After getting the RREQ message form any node, mobile node compares the DSN of RREQ with the DSN of its own routing table. If the DSN of routing table is greater than the RREQ DSN then it unicast the RREP, otherwise broadcast the RREQ to all to its neighbours. When RREQ reached to the destination, destination unicasts a RREP with sequence number with an incremented value [32-35].

In Figure 1 shows that destination node D, generate a RREP message after getting RREQ from the source node. This RREP have the following:

$$< D, S, 193, 0, 5 >$$

When destination node sending the RREP then is works as a source node. So, RREP works as a source node and S works as a destination node. This REEP has DSN 193 and number of hop count is 0. When this RREP traverses from intermediate nodes, hop count is incremented by 1.

In this RREP packet last field is TTL of the message. Sequence number has minimum value 0 and maximum value is 32 bits arithmetic (2^{32}). If the reaches to its maximum value, then it reset to zero.

$$DSN_{min} = 0$$

$$DSN_{max} = 4294967295$$

In case of Blackhole attack, when attacker gets the RREQ message, it immediately generates a fabricated RREP message with very high sequence number and lower hop count. In Figure 2 attacker node E generates the RREP with sequence number of 32 bit arithmetic. When this fabricated message reached to the source node, it will be considered as a fresh route to the destination and the source node starts the transmission of the through that route and malicious node drops all the data packets [36][37][38].

In order to prevent the above describe problem, we propose a new mechanism to prevent the attack. This new mechanism prevents the Blackhole attack as well as maintains the data integrity during the transmission of data to use identity-based signature scheme. Identity based signature scheme maintains data integrity, authentication and non- repudiation (Kumar and Kumar, 2016).

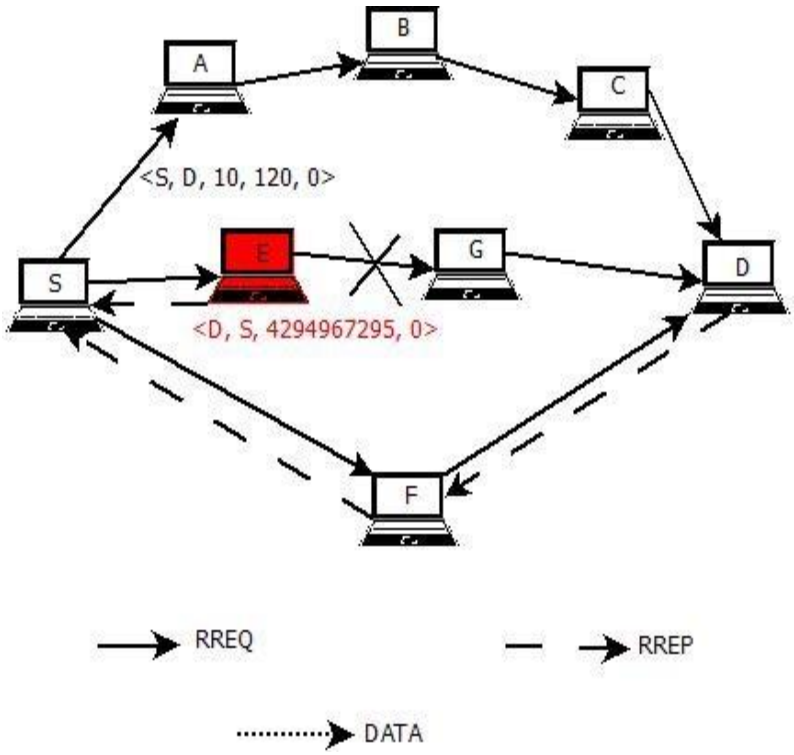

Fig 2: Blackhole Attack Mechanism

A. Calculation of Threshold

As we studied above that sequence number has minimum value 0 and maximum value is 32 bit arithmetic (2^{32}).

$$DSN_{min} = 0$$

$$DSN_{max} = 5294967295$$

In the proposed approach, we are defining a threshold value for the elimination of malicious node. As we studied that malicious node send very high sequence number, nearer to the DSNmax. So we are defining the threshold by the calculation of following formula [39][40][41].

$$T_n = DSN_{max} * 97\%$$

Where T_n is the defined threshold. By defining this threshold, actually we are eliminating 3% of maximum sequence number, because attacker used sequence number nearer to maximum sequence number.

Flow Diagram for Additional Process:

Once threshold is defined, RREP message is verified by using that threshold value. When source node gets RREP message for the RREQ message which the source node generates it verify those RREP messages. Figure 6 shows the processing flow chart at the source node [42][43][44].

In case of Blackhole attack, when attacker gets the RREQ message, it immediately generates a fabricated RREP message with very high sequence number and lower hop count. In Figure 4 attacker node E generates the RREP with sequence number of 32 bit arithmetic. When this fabricated message reached to the source node, it will be considered as a fresh route to the destination and the source node starts the transmission of the through that route and malicious node drops all the data packets. We propose a new mechanism to prevent MANET from the blackhole attack. This new mechanism prevents the Blackhole attack as well as maintains the data integrity during the transmission of data to use identity-based signature scheme. Identity based signature scheme maintains data integrity, authentication and non- repudiation (Kumar and Kumar, 2016).

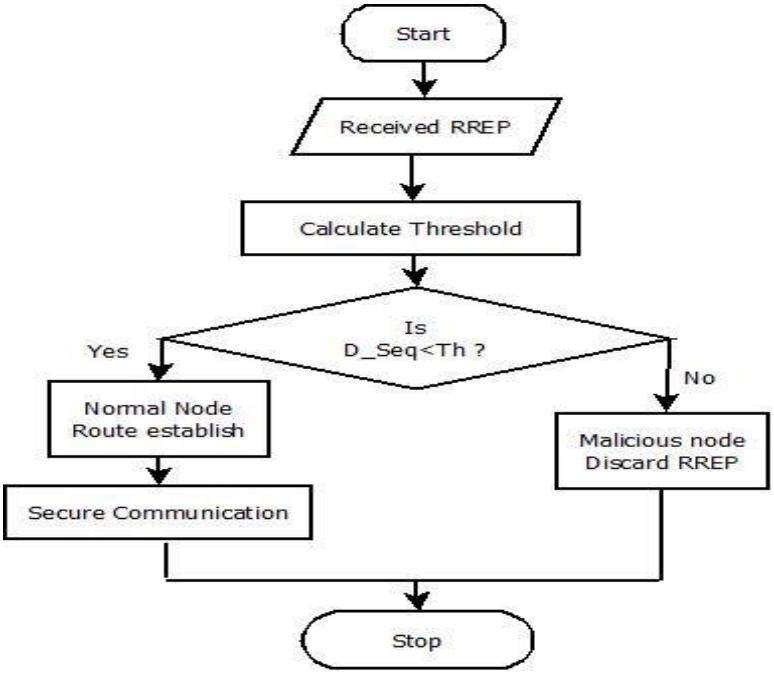

Fig 3: Flow Diagram for Additional Process

Calculation of Threshold: As we know higher value of sequence number is 2^{32} while lower value is *0*.

$$DSN_{min} = 0$$

$$DSN_{max} = 4294967295$$

In the proposed approach, we are defining a threshold value to elimination of the malicious node.

B. **Analysis of Improved Mechanism**: Improved mechanism based on DNS. It checks the received RREP message whether it came from destination, genuine node or from the attacker node. Suppose source node sends DSN 120 when broadcast RREQ message. Attacker node gets this RREQ message and generates a forged RREP message with DSN 4294967280 and hope count 0. When source node get this forged RREP messages this checks this hope count and DSN which pretend that this node has fresh and optimal route to the destination, then source node establishes a route through this node to transmit data to destination node and also attacker node drops all the receive packets without forwarding it to destination. When improved AODV mechanism is used, it does not forward data immediately. Firstly, it calculates the threshold value for comparing the DSN received in RREP message [45][46][47].

$$DSN_{rec} = 5294967280$$

$$T_n = DSN_{max} * 97\% = 4166118276$$

It compares the DSN of received RREP, which is greater than the threshold value, then it discards the received RREP and wait for other RREP message.

Results and Discussion

Performance evaluation of our proposed scheme has been carried out using network simulator(ns2). The performance here is measured by analyzing the node mobility. All the simulation parameters has been presented in Table 1.

Table 1: Simulation Parameters

Constraint	**Value**
Simulator	ns2
No. of Nodes	10-90
Routing Protocols	SAODV, AODV
Speed	2-9 m/s

Packet Size	512 bytes
MAC Protocol	IEEE 802.11
Simulation Time	100 Seconds
Traffic Model	CBR
Terrain Area	1000m x 1000m
No. of Malicious node	1
Speed of traffic agent	15 m/s
Pause time	6 s
Transmission range	250 m
Used mobility Model	Random waypoint

Simulation Results: A comparison graph between standard AODV protocol in presence of blackhole node, Singh et al. (2016) scheme and proposed scheme using packet delivery ratio (PDR) metric is presented in Figure 4. From our result analysis proposed scheme has 98.15% where AODV with Blackhole attack has 4% PDR and Singh et al. (2016) scheme having 98% for average packet delivery ratio (PDR) metric.

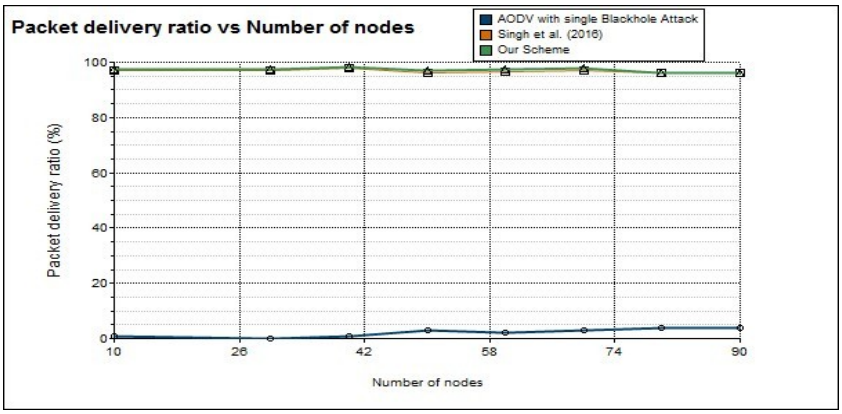

Fig 4: PDR with single Blackhole Attack

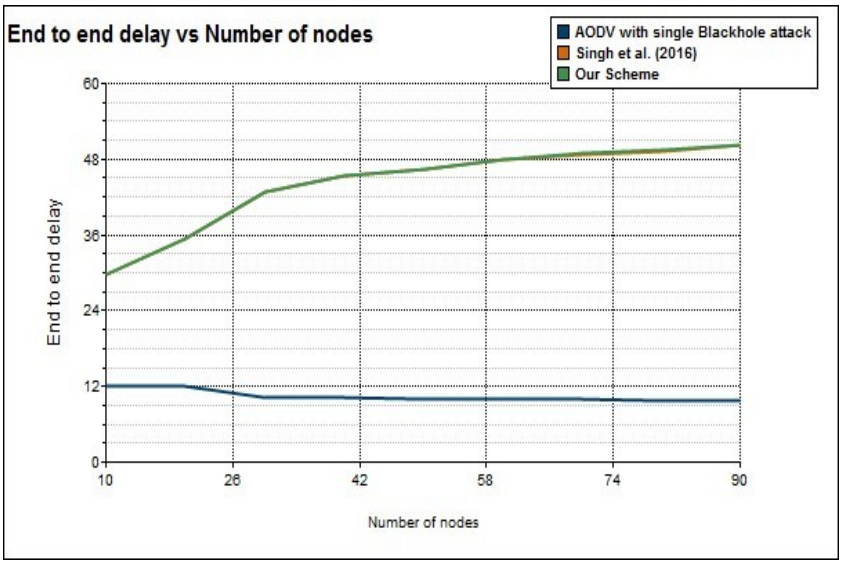

Fig 5: End-to-end delay with single Blackhole Attack

A comparison graph between proposed and existing schemes in terms average end-to-end delay metric is depicted in Figure 5. It shows that maximum end to end delay in standard AODV is lower than proposed scheme. Standard AODV have end to end delay 12.02ms and Singh et al. and proposed scheme having maximum end to end delay 50.36 milliseconds.

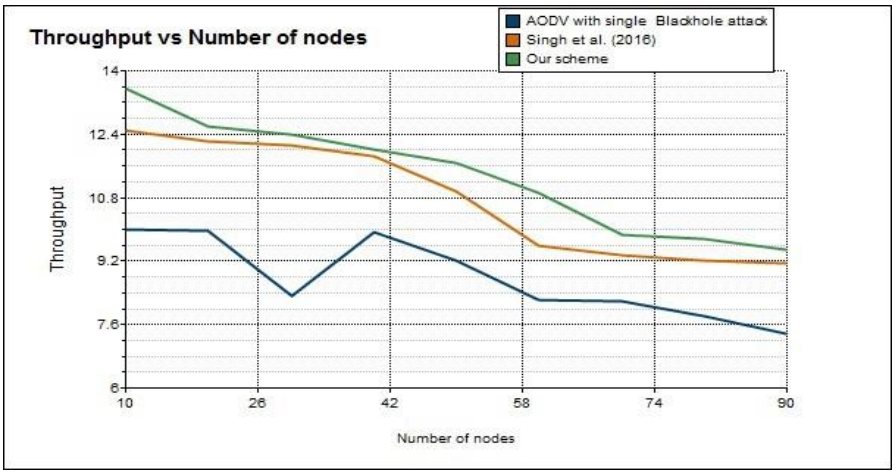

Fig 6: Average Throughput with single Blackhole Attack

Figure 6 shows the average throughput of the network in presence of single Blackhole node. It clearly shown in graph that average throughput of standard AODV is 10.01 and Singh et al. (2016) scheme having throughput 12.48 while our proposed scheme having throughput 13.57. It clearly shows that proposed scheme having better throughout in comparison to other two schemes.

Conclusion and future wok

We introduced a novel approach in this paper to counteract the blackhole attack using a certificate-less signature scheme. Our proposed scheme not only thwarts single blackhole attacks but also cooperative blackhole attacks. According to simulation results, our scheme achieves a 98.15% Packet Delivery Ratio (PDR), while the standard AODV yields a 4% PDR, and the approach by Singh et al. (2016) achieves a 98% PDR in the case of a single blackhole attack. For cooperative blackhole attacks, our scheme attains a 98.12% PDR, whereas the standard AODV, Tamilselvan et al. (2008), and Singh et al. (2016) approaches achieve 3%, 97%, and 98.04% PDR, respectively.

Regarding throughput, our proposed scheme achieves a throughput of 13.57, while the standard AODV and Singh et al. (2016) schemes achieve 10.01 and 12.48, respectively, in the case of a single blackhole attack. In the case of cooperative blackhole attacks, our scheme attains a throughput of 13.10, whereas the standard AODV achieves 10.01, and the Singh et al. (2016) scheme achieves 12.48 throughput. Considering maximum end-to-end delay, our scheme exhibits a delay of 50.36 ms, while the standard AODV and Singh et al. (2016) demonstrate delays of 12.02 ms and 50.36 ms, respectively, in the case of a single blackhole attack. In the case of cooperative blackhole attacks, our scheme incurs a delay of 50.16 ms, while the standard AODV, Tamilselvan et al., and Singh et al. (2016) schemes exhibit delays of [insert values for Tamilselvan et al.] milliseconds. (2008) and Singh et al. (2016) has delay 12.02ms, 50.36ms and 50.36ms respectively.

References

[1] Singh A, and Hasan M, “An Analysis of Prevention Mechanism of Blackhole Attack” 2016 International Conference on Innovations in information Embedded and Communication Systems (ICIIECS’16), Tamilnadu, vol. 1, pp. 117-122.

[2] Murthy, C. Siva Ram, and B. S. Manoj. Ad hoc wireless networks: Architectures and protocols. Pearson education, 2004.

[3] Aware, Anand, and Kiran Bhandari. "Prevention of black hole attack on AODV in MANET using hash function." Reliability, Infocom Technologies and Optimization

(ICRITO)(Trends and Future Directions), 2014 3rd International Conference on. IEEE, 2014.

[4] Clausen, Thomas, et al. "The optimized link state routing protocol, evaluation through experiments and simulation." IEEE Symposium on" Wireless Personal Mobile Communications. 2001.

[5] Ogier, Richard, Fred Templin, and Mark Lewis. Topology dissemination based on reverse-path forwarding (TBRPF). No. RFC 3684. 2004.

[6] Perkins, Charles E., and Pravin Bhagwat. "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers." ACM SIGCOMM computer communication review. Vol. 24. No. 4. ACM, 1994.

[7] Chiang, Ching-Chuan, et al. "Routing in clustered multihop, mobile wireless networks with fading channel." proceedings of IEEE SICON. Vol. 97. No. 1997.4. 1997.

[8] Perkins, Charles, Elizabeth Belding-Royer, and Samir Das. Ad hoc on-demand distance vector (AODV) routing. No. RFC 3561. 2003.

[9] Johnson, David B., and David A. Maltz. "Dynamic source routing in ad hoc wireless networks." Mobile computing. Springer US, 1996. 153-181.

[10] Park, Vincent D., and M. Scott Corson. "A highly adaptive distributed routing algorithm for mobile wireless networks." INFOCOM'97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution., Proceedings IEEE. Vol. 3. IEEE, 1997.

[11] Chakeres, Ian D., and Joseph P. Macker. "Mobile ad hoc networking and the IETF." ACM SIGMOBILE Mobile Computing and Communications Review 10.1 (2006): 58-60.

[12] Haas, Zygmunt J. "A new routing protocol for the reconfigurable wireless networks." Universal Personal Communications Record, 1997. Conference Record., 1997 IEEE 6th International Conference on. Vol. 2. IEEE, 1997.

[13] M.Joa-Ng and I.T.Lu, "A Peer -to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1415-1425, August 1999.

[14] Macker, Joseph. "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations." (1999).

[15] Roth, Uwe. "Cluster Based Routing Protocol." (2011).

[16] Iwata, Atsushi, et al. "Scalable routing strategies for ad hoc wireless networks." Selected Areas in Communications, IEEE Journal on 17.8 (1999): 1369-1379.

[17] Agrawal, Sudhir, Sanjeev Jain, and Sanjeev Sharma. "A survey of routing attacks and security measures in mobile ad-hoc networks." arXiv preprint arXiv:1105.5623 (2011).

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

[19] Sachan, Preeti, and Pabitra Mohan Khilar. "Securing AODV routing protocol in MANET based on cryptographic authentication mechanism." International Journal of Network Security & Its Applications 3.5 (2011): 229.

[20] Deng, Hongmei, Wei Li, and Dharma P. Agrawal. "Routing security in wireless ad hoc networks." Communications Magazine, IEEE 40.10 (2002): 70-75.

[21] Varshney, Tarun, Toshi Sharma, and Parmanand Sharma. "Implementation of watchdog protocol with AODV in mobile ad hoc network." Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on. IEEE, 2014.

[22] Maheshwar, Kamini, and Divakar Singh. "Black Hole Effect Analysis and Prevention through IDS in MANET Environment." European Journal of Applied Engg. and Scientific Research (2012).

[23] Harmandeep Singh and Manpreet Singh. "Securing MANETs Routing Protocol under Black Hole Attack." International Journal of Innovative Research in Computer and Communication Engineering 1.4 (2013): 808-813.

[24] Latha Tamilselvan and V. Sankaranarayanan. "Prevention of blackhole attack in MANET." Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on. IEEE, 2007.

[25] Tirthankar Ghosh, Niki Pissinou, and Kia Makki. "Collaborative trust-based secure routing against colluding malicious nodes in multi-hop ad hoc networks." Local Computer Networks, 2004. 29th Annual IEEE International Conference on. IEEE, 2004

[26] Kumar, V., & Kumar, R. (2015). An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network. Procedia Computer Science, 48, 472-479.

[27] Kumar, V., & Kumar, R. (2015, June). A Cooperative Black Hole Node Detection and Mitigation Approach for MANETs. In International Conference for Information Technology and Communications (pp. 171-183). Springer International Publishing.

[28] Kumar, V., & Kumar, R. (2016). Prevention of Blackhole Attack using Certificateless Signature (CLS) Scheme in MANET. Security Solutions for Hyperconnectivity and the Internet of Things, 130.

[29] Gurung, S. and Chauhan, S., 2018. A dynamic threshold based approach for mitigating black-hole attack in MANET. *Wireless Networks*, *24*(8), pp.2957-2971.

[30] Shukla, M., Joshi, B.K. and Singh, U., 2021. Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET. *Wireless Personal Communications*, *121*(1), pp.503-526

[31] Talukdar, M.I., Hassan, R., Hossen, M.S., Ahmad, K., Qamar, F. and Ahmed, A.S., 2021. Performance improvements of AODV by black hole attack detection using IDS and digital signature. *Wireless Communications and Mobile Computing*, *2021*.

[32] Kumar, V. and Kumar, R., 2015. An adaptive approach for detection of blackhole attack in mobile ad hoc network. *Procedia Computer Science*, *48*, pp.472-479.

[33] Kumar, V. and Kumar, R., 2015. An optimal authentication protocol using certificateless ID-based signature in MANET. In Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3 (pp. 110-121). Springer International Publishing.

[34] Kumar, V. and Kumar, R., 2015, April. Detection of phishing attack using visual cryptography in ad hoc network. In *2015 International* Conference on Communications and Signal Processing (ICCSP) (pp. 1021-1025). IEEE.

[35] Kumar, V., Shankar, M., Tripathi, A.M., Yadav, V., Rai, A.K., Khan, U. and Rahul, M., 2022. Prevention of Blackhole Attack in MANET using Certificateless Signature Scheme. Journal of Scientific & Industrial Research, 81(10), pp.1061-1072.

[36] Narayan, Vipul, et al. "7 Extracting business methodology: using artificial intelligence-based method." Semantic Intelligent Computing and Applications 16 (2023): 123.

[37] Narayan, Vipul, et al. "A Comprehensive Review of Various Approach for Medical Image Segmentation and Disease Prediction." Wireless Personal Communications 132.3 (2023): 1819-1848.

[38] Mall, Pawan Kumar, et al. "Rank Based Two Stage Semi-Supervised Deep Learning Model for X-Ray Images Classification: AN approach toward tagging unlabeled medical dataset." Journal of Scientific & Industrial Research (JSIR) 82.08 (2023): 818-830.

[39] Narayan, Vipul, et al. "Severity of Lumpy Disease detection based on Deep Learning Technique." 2023 International Conference on Disruptive Technologies (ICDT). IEEE, 2023.

[40] Saxena, Aditya, et al. "Comparative Analysis Of AI Regression And Classification Models For Predicting House Damages İn Nepal: Proposed Architectures And Techniques." Journal of Pharmaceutical Negative Results (2022): 6203-6215.

[41] Kumar, Vaibhav, et al. "A Machine Learning Approach For Predicting Onset And Progression"“Towards Early Detection Of Chronic Diseases “." Journal of Pharmaceutical Negative Results (2022): 6195-6202.

[42] Chaturvedi, Pooja, Ajai Kumar Daniel, and Vipul Narayan. "Coverage Prediction for Target Coverage in WSN Using Machine Learning Approaches." (2021).

[43] Chaturvedi, Pooja, A. K. Daniel, and Vipul Narayan. "A Novel Heuristic for Maximizing Lifetime of Target Coverage in Wireless Sensor Networks." Advanced Wireless Communication and Sensor Networks. Chapman and Hall/CRC 227-242.

[44] Dhanke, Jyoti, Naveen Rathee, M. S. Vinmathi, S. Janu Priya, Shafiqul Abidin, and Mikiale Tesfamariam. Smart Health Monitoring System with Wireless Networks to Detect Kidney Diseases. Computational Intelligence and Neuroscience 2022 (2022).

[45] Atul, Dhanke Jyoti, R. Kamalraj, G. Ramesh, K. Sakthidasan Sankaran, Sudhir Sharma, and Syed Khasim. A machine learning based IoT for providing an intrusion detection system for security. Microprocessors and Microsystems 82 (2021).

[46] Dhanke, Jyoti, M. Pradeepa, R. Karthik, Veeresh Rampur, I. Poonguzhali, and Hemanand Chittapragada. Heterogeneous sensor data fusion acquisition model for medical applications. Measurement: Sensors 24 (2022): 100552.

[47] Jagan, S.; Ashish, A.; Mahdal, M.; Isabels, K.R.; Dhanke, J.; Jain, P.; Elangovan, M. A Meta-Classification Model for Optimized ZBot Malware Prediction Using Learning Algorithms. Mathematics 2023, 11, 2840.