ENHANCED ALGORITHM FOR REDUCTION OF BLACKHOLE'S RE-JUDGMENT DELAY FOR REAL-TIME TRAFFIC IN MOBILE ADHOC NETWORK

Sarah Florence Massae and Joseph Chrisant Pengo

Department of Computing and Communication Technology (CCT), National Institute of Transport, Dar es Salaam, Tanzania

ABSTRACT

Mobile Ad-hoc Network (MANET) is a prominent technology in wireless communication in which mobile nodes operate in a distributed manner without having central control devices; This lack of control over network devices and over changing topology aspects of the network allows malicious nodes gain opportunities to join the network. The blackhole attack is one of the security risks that increases the network overhead. In this attack, the malicious node advertises itself as having the shortest path to the destination and falsely replies to the route requests, and drops all receiving packets. Therefore, the paper proposes a trust-level based re-judgment algorithm. Experiments were set up in the NS3 networking simulation tool. Simulations results showed that the proposed trust-level based re-judgment algorithm improves network throughput and packet delivery rate by 82.8% and 146.6 Kbps respectively. Also, reduces the end-to-end delay by an average of 24.17 milliseconds.

KEYWORDS

Mobile Ad-hoc Network (MANET), Ad-hoc on-demand Distance Vector (AODV)

1. INTRODUCTION

Mobile Ad hoc Networks (MANETs) describe networks with autonomous mobile nodes that can re-arrange themselves in various topologies and operate without strict top down network administration to provide multi-hope communication between the source and the destination nodes [1], [2][3]. Unstructured topology and self-configured properties of MANETs make them find an application in desired as well as temporary communication networks such as in military and relief as well as rescue operations. Such networks are primarily made to transmit quick information exchange between participating nodes by using routing protocols that support the best effort type of traffic [4].

Lack of a central control node makes the process of maintaining accurate information about network routes in MANETs challenging. Also, it subjects such kind of networks to many types of attacks like blackhole, wormhole and denial of service (DoS) attacks[5], [6], [7][8][9]. Blackhole attacks are the mostly experienced attacks whereby malicious node pretends to be a normal node and makes the source to believe that it has the actual least distance path to the destination, but in real scenario, it drops the packets instead of forwarding to the destination or to neighboring node [7], [10].

Different blackhole detection mechanisms proposed by scholars were designed such that every node in the network keeps a record of blacklisted nodes and periodically, re-judges its list to

DOI: 10.5121/ijnsa.2024.16401

identify wrongly blacklisted nodes so that a normal node may not be permanently blacklisted [6], [11], [12], [13]. The re-judgment process or the process of recovering normal nodes from the blacklist is done after the node's slot time has expired and hence, time to transmit is delayed [14]. Nodes with real time traffic may not catch up with their elapsed time. This is a serious problem in real-time traffic, especially in disaster management. Therefore, the need to reduce the re-judgment delay constitutes the focal point of this dissertation. An algorithm was proposed to anticipate the re-judgment compared to when the slot time expiration is considered so as to reduce end-to-end delay. Sakshi and Khuteta (2015) proposed an algorithm to detect and overcome blackhole's attack in MANET. In their solution, it was uncovered that malicious node advertises itself as having the best path to destination and thus, interrupting real time communication as well as decreases network performance, a pattern, which causes end to end delay. Their proposed solutions showed weakness in handling the real time traffic due to delay and wrongly blacklisting the safe nodes as the malicious nodes.

Nishu (2016) proposed a method handles with multiple blackhole's nodes attack in MANET. To deal with the numerous blackhole's nodes attack, the source hub utilizes the sequence number idea to distinguish the various blackhole's nodes in MANET. The source sequence number is utilized by the source hub to detect the blackhole's attack. In this solution, the fake routing information is used by the source node in order to detect the multiple blackhole's nodes present in the wireless ad hoc networks and their proposed mechanism is implemented in NS-2.34. Kamel and colleagues (2017) proposed an algorithm to detect black hole attack by isolating malicious nodes. In their solution, they attached a trust value to each node in which the incoming packet with higher destination sequence number than threshold value was termed as blackhole's node. The proposed solutions show weakness in handling the real time traffic due to delay caused by re-judgment delay and wrongly blacklisting the safe nodes as the malicious nodes.

Taku and Takaya (2017) proposed a new threshold based black hole attack detection and prevention technique. In their proposed solution, the threshold is based on the destination sequence number where the normal nodes have the destination number below the threshold and the malicious nodes are those with the destination sequence number greater than the threshold number. The blackhole's listed nodes are judged periodically to determine if there is a normal node blacklisted wrongly. The throwback of this approach is false detection problem where normal nodes are blacklisted as malicious during black hole re-judgment, which causes network delay. Furthermore, Anshu et. al. (2020) proposed blackhole's attack implementation and its performance evaluation using AODV routing MANET. In their work, they simulated the blackhole's attack in AODV reactive routing protocol of MANET and investigated its viability by considering various performance metrics. But it was found that because of single blackhole's node present in the system packet, drop increased, which debates the PDR, value and throughput of the entire system and also, they did not consider end to end delay in their simulation. Most of the existing research studies discussed methods for detecting and preventing blackhole attacks against MANET's that are based on the AODV protocol and other proactive protocols based on DSDV or OLSR, and DSR. Both routing protocols methods scales poorly however, our proposed algorithm detects, prevents and improves mitigation on blackhole attack by provide high performance in terms of PDR, throughput and end to end delay on AODV routing protocol.

2. METHODOLOGY

This study uses experimental research method whereby an enhanced algorithm of re-judgment process in MANET was modeled in NS3 simulation packet and its performance compared with similar AODV-based algorithm. During the experiment, the quality of service (QoS) parameters such as Packet Delivery Rate, throughput, and end to end delay were observed to evaluate

performance of the proposed algorithm. Data of these parameters were collected in a period of 100 seconds, exported and summarized in tabulated form, and then analyzed in plotted graphs.

2.1. Algorithm Design

The re-judgment process in other AODV-based algorithms generate dummy packets so that if a blacklisted malicious-node replies to dummy packets the algorithm keeps the node in the blacklist, otherwise it is considered as a safe node and dropped out the list. This process consumes additional bandwidth not only due to resources required for transmission of dummy packets but also responses to the dummy packets. Also, the use of dummy packets in the re-judgment process causes an additional delay, packet loss and lower throughput in the transmission process because nodes have to wait for dummy packets responses as illustrated in figure 1 below.

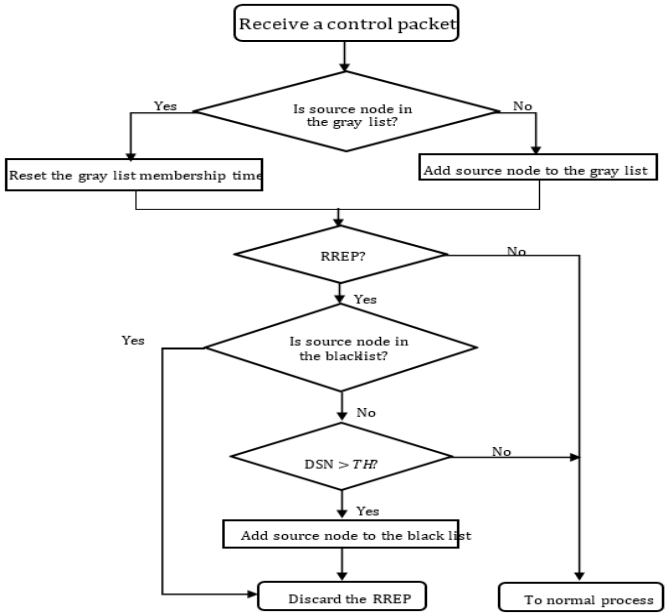

Figure 1: Black hole node detection flow (Source: Taku Noguchi and Takaya Yamamoto (2017))

As depicted in Figure 1, nodes that blacklisted by using the detection flow chart in AODV-based algorithm will maintain correspondences (packet transmission or reception) in the network but only restricted to reply to RREP control packets. A blacklist entry has two information field; node address and membership time. If the source node of the RREP packet is blacklisted, it drops the received RREP packet. Otherwise, it checks whether the destination sequence number (DNS) is higher than threshold (TH). If DNS > TH, the source node is blacklisted: otherwise, it processes the RREP packet in the normal way.

Assuming that all safe nodes in the MANET have in their buffers some packets or data to transmit, a re-judgment mechanism that focuses on the transmitted and received packets is envisioned as presented in the proposed black hole node detection flow chart with trust level-based re-judgment as shown in Figure 1. Trust level is dynamic, based on transmission or reception of data and control packets by the node. The following is consideration of trust level as presented by Apurva and colleagues (2016). It is assumed in this dissertation that trust level (TL) of each node increases based on received or transmitted packets as in equation (1), below.

$$TL = (\alpha * RevSendPackets(\tau) + \beta * SendPackets(\tau)/\tau,$$

Where, α and β represent the weights assigned to packet reception and packet transmission, respectively. The components $RevSendPackets(\tau)$ and $SendPackets(\tau)$ represent the received and sent packets in an observation windowτ. In this case, these packets are assumed to be sent or received via the node that wants to establish a session.

The proposed black hole node detection flow chart with trust level-based re-judgment is used such that when trust level of a blacklisted node is greater or equal to a specified threshold$TLTH$ 1, the node is allowed to participate in the forwarding process but it still being monitored as a possible threat. When TL of a blacklisted node reaches or exceeds the threshold $TLTH$ 2, the node is removed from the blacklist as shown in Figure 2.

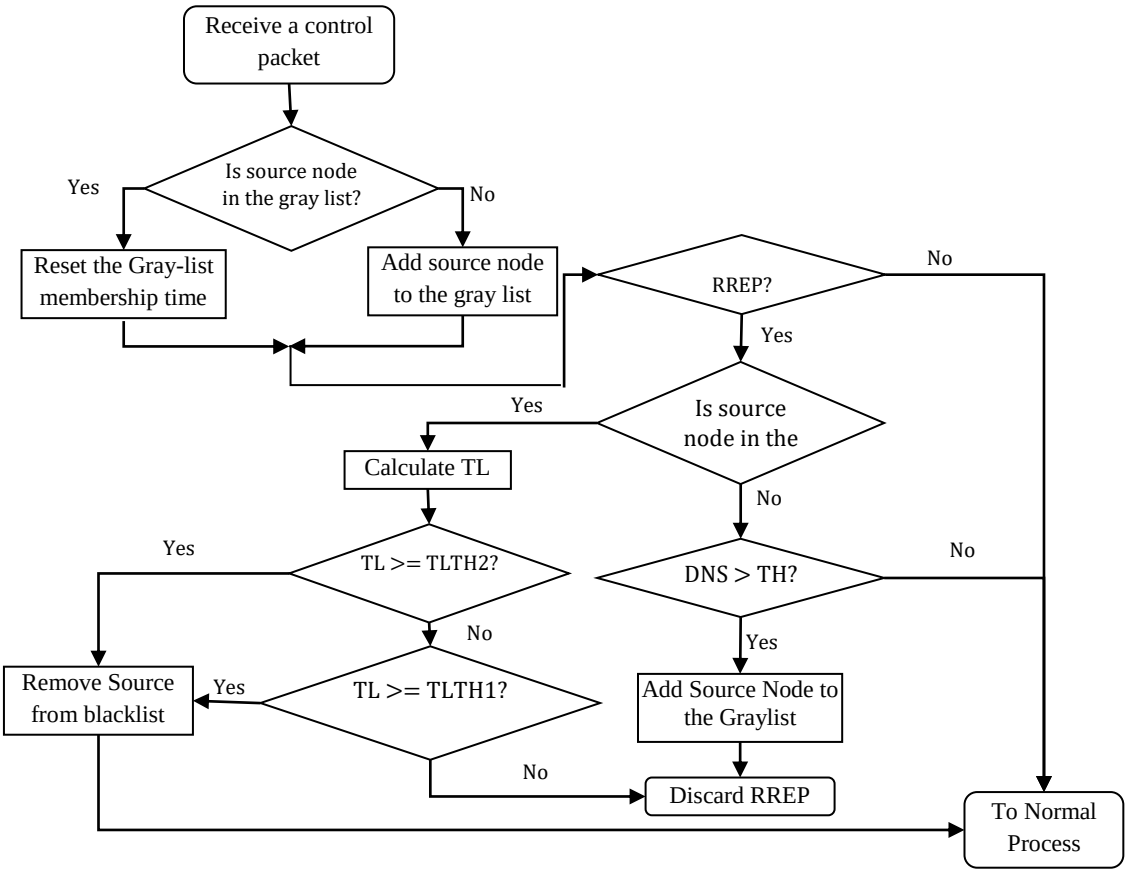

Figure 2: Proposed Blackhole Node Detection Flow Chart with Trust Level-Based Re-judgment

2.2. Simulation Design

2.2.1. Adding Blackhole's Features on AODV

To enable nodes on MANET, operate as malicious or non-malicious node, the code snippet shown in Figure 3was added on RecvRequest method so that nodes can be switched to operate either as malicious or non-malicious node by setting isMalicious attribute to true or false when configuring AODV protocol. When IsMalicious attribute is set to true, the node will act as a

black hole node and be able to create false routing table entry having sequence number much higher than that in RREQ message. Figure 4 shows the snippet code, which attracts nodes to set up path through malicious node by setting hop count as 1 on RREP message. Snippet code as shown on Figure 3 was added to Forwarding method on RoutingProtocol class to enable malicious node on figure 5 to drop all packets and it receives before forwarding to intermediate nodes.

```
if(IsMalicious)
{
  Ptr<NetDevice> dev = m_ipv4->GetNetDevice (m_ipv4->GetInterfaceForAddress (receiver));
  RoutingTableEntry falseToDst(dev,dst,true,rreqHeader.GetDstSeqno()+700,m_ipv4->GetAddress (m_ipv4->GetInterfaceForAddress

  SendReplyByIntermediateNode (falseToDst, toOrigin, rreqHeader.GetGratuitousRrep());
   return;
}
```

Figure 3: Blackhole's features on AODV

```
if(IsMalicious)
{
    rrepHeader.SetHopCount(1);
}
```

Figure 4: Malicious feature on AODV

```
if(IsMalicious)
  {//When malicious node receives packet it drops the packet.
        std :: cout <<"Launching Blackhole Attack! Packet dropped . . . \n";
        return false;
  }
```

Figure 5: Packet Dropped

2.2.2. Adding Blackhole's Attack Prevention Feature on AODV

Blackhole's attack prevention feature was re-implemented on AODV model. The implementation of this feature was based on Noguch and colleagues (2017) on which they proposed threshold-based black hole attack prevention method. Threshold value is dynamically updated based on the total number of nodes in the network and time elapsed after it knows the last sequence number of the destination node. To reduce the rate of false detection, CalcculateTL method on the snippet code shown in Figure 6 was added on AODV model. This method is used to calculate the Trust Level value based on number of packets received and sent by a particular node.

```
uint32_t RoutingProtocol::CalculateTL(Ipv4Address src){
  std::map<Ipv4Address,PacketStats>::iterator it= receivedSentStats.find(src);



  if (it != receivedSentStats.end()){


    uint32_t tl=recvWeight*it->second.getRecvPackets()+sendWeight*it->second.getSentPackets();

  std::cout<<"Weight"<<tl<<std::endl;

    return tl;
  }



  return 0;
}
```

Figure 6: BH Attack Implementation

Blackhole's attack prevention feature was re-implemented on AODV model. The implementation of this feature was based on Noguch and colleagues (2017) on which they proposed threshold-based black hole attack prevention method. Threshold value is dynamically updated based on the total number of nodes in the network and time elapsed after it knows the last sequence number of the destination node. To reduce the rate of false detection, calculated method on the snippet code shown in Figure 6 was added on AODV model. This method is used to calculate the Trust Level value based on number of packets received and sent by a particular node.

2.3. Simulation Setup

Table 1 summarizes important parameters used in simulations and Figure 7 shows the simulation area with malicious nodes colored in red and non-malicious nodes colored in blue.

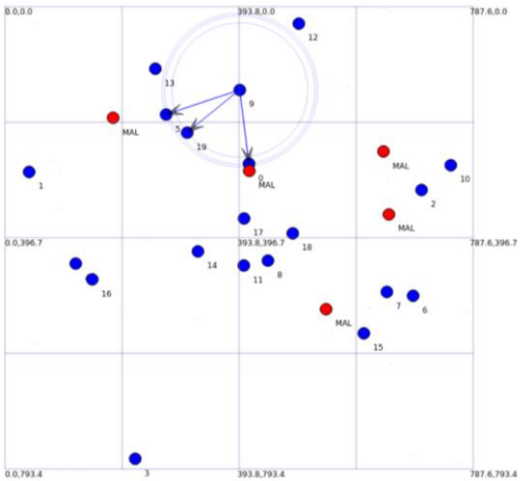

Figure 7: Malicious and non-malicious nodes simulation

2.4. Simulation Parameters

The simulation was conducted by developing an algorithm based on AODV routing protocol, with 10 iterations. Numbers of nodes used were 100 which have 512bytes. Each node original rate per second was 100 as shown in Table 1.

2.4.1. Simulation Parameters and Configuration

Table 1: Simulation environment parameters

Simulation Parameters	Configuration Value
Simulator version	NS-3.32
Mobility model	Random Waypoint
Physical/MAC layer	802.11b
Routing Protocol	AODV
Propagation Models	Friis Loss Model
Antenna Model	Omni Antenna
Bandwidth	2.048Kbps
Simulation area	800m * 800m
Simulation time	100sec
Node Density	20, 30, 40, 50, 60, 70, 80, 90, 100
Speed	20m/s
Pause time	0sec
Iteration	10
Number of Blackhole's Nodes	5
Propagation Delay Model	Constant Speed
Number of sinks	10
Traffic Type	CBR
Transmit Power	7.5dBm
Packet Size	512Bytes

3. RESULTS AND FINDINGS

3.1. Performance Results

For better analysis of the results, the researcher considered changing number of nodes (20, 30, 40, 50, 60, 70, 80, 90 and 100). After simulation, packet delivery rate, throughput and end to end delay were calculated considering the following definitions.

3.1.1. Packet Delivery Rate (PDR)

The ratio of the number of packets received by TCP sink to the number of packets delivered by the TCP source. The ratio of received packets by UDP sink at destination over sent packets by the constant bit rate source. The metrics tell how reliable the protocol is and show number of packets received by node including the number of packets forwarded by node[16] [17]. Table 2 shows packet delivery performance for the proposed method, AODV with/without BH attacks.

Number of Nodes	AODV (w/ BH Attack)	Naguchi & Yamamoto	Proposed Method
20	1.67	67.36	70.60
30	2.67	70.12	72.46
40	1.72	75.87	78.24
50	1.95	76.99	85.12
60	1.69	77.45	86.32
70	1.71	88.18	87.23
80	3.32	91.97	94.70
90	4.23	95.11	96.69
100	5.9	98.54	99.64

Table 2: Packet Delivery Rate

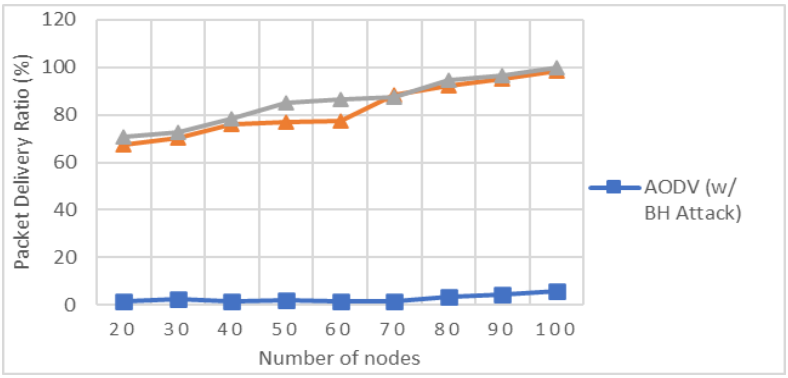

Figure 8: Number of nodes vs PDR

3.1.2. End to End Delay

The cumulative delay might come about as a result of buffering during discovery of routes querying at interference, delay in retransmission at the MAC, and the time taken for propagation and transfer[16] [17]. Table 3 shows end to end delay for the proposed method, end to end delay and AODV with /without BH attack.

Number of Nodes	AODV (w/ BH Attack)	Naguchi & Yamamoto	Proposed Method
20	79.17	60.54	54.51
30	177.86	150.56	121.62
40	280.29	199.86	189.51
50	294.63	250.15	228.71
60	335.73	300.43	275.53
70	391.01	360.55	339.73
80	421.50	392.69	388.59
90	542.64	525.26	456.40
100	649.90	580.39	548.28

Table 3: End to End Delay

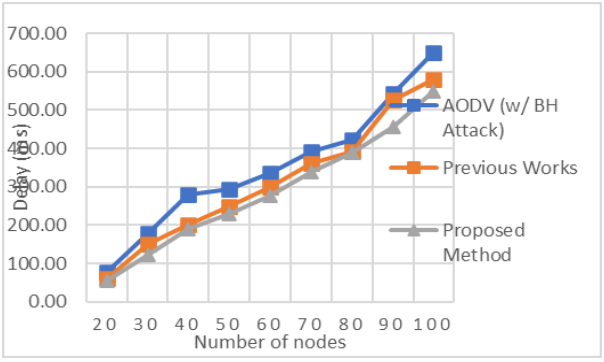

Figure 9: Number of Nodes vs Delay (ms)

3.1.3. Throughput

Throughput of the network is defined as the number of bits of data that are received by the goal node per unit time. It is the ratio of number of bits received by the goal node to total time taken[16] [17].

The amount of data that is transmitted per unit time (that means data bytes delivery to their destination per second [19]. Table 4 shows the throughput performance of the proposed method, AODV with/without BH attack.

Number of Nodes	AODV (w/ BH Attack)	Naguchi & Yamamoto	Proposed Method
20	1.75	100.06	103.62
30	2.63	112.56	126.98
40	3.34	119.56	127.39
50	3.78	120.32	128.22
60	4.35	122.78	133.32
70	8.87	120.11	140.04
80	6.94	119.25	148.41
90	13.44	117.34	159.72
100	15.38	116.38	161.93

Table 4: Throughput

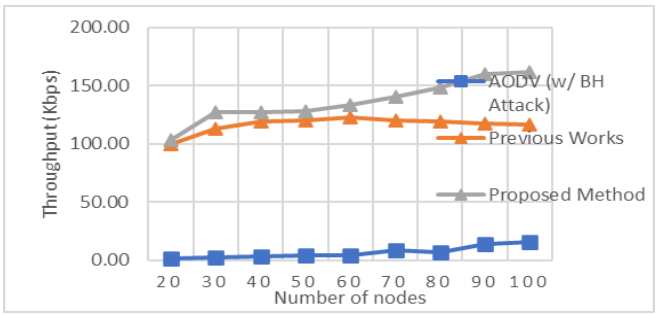

Figure 10: Number of nodes vs Throughput (Kbps)

4. CONCLUSION

This study simulated the blackhole's attack in NS3 by modifying the current AODV protocol. Results were analyzed graphically by taking different system attributes such as Packet Delivery Rate, Throughput and End to end Delay. Data analysis showed that because of blackhole's nodes found in the system, Packet Delivery Ratio and network throughput were negatively affected.

Simulation results showed the proposed trust-level based re-judgment algorithm improves the network throughput and the packet delivery ratio by 82.8 percent and as 146.6Kbps, respectively, compared to algorithm proposed by other studies. Also, it reduces the end-to-end delay by an average of 24.17ms compared to when the blackhole's attacks are assumed.

Despite the observed performance, the established trust-level equation took into account sent and received packets only. It should capture several parameters that vary, based on real-time activities of nodes including throughput and packet rates in the networks. The integration of these parameters remains open research for future studies.

REFERENCE

[1] Natarajan and Mahadevan, "Towards a parametric analysis and evaluation of seven MANET routing protocols," vol. 4, no. 1, pp. 69–76, 2017.

[2] S. Gurung and S. Chauhan, "A survey of black-hole attack mitigation techniques in MANET : merits , drawbacks , and suitability," *Wirel. Networks*, vol. 26, no. 3, pp. 1981–2011, 2019, doi: 10.1007/s11276-019-01966-z.

[3] A. H. Wheeb and D. N. Kanellopoulos, "Simulated performance of SCTP and TFRC over MANETs: The impact of traffic load and nodes mobility," *Int. J. Bus. Data Commun. Netw.*, vol. 16, no. 2, pp. 69–83, 2020, doi: 10.4018/IJBDCN.2020070104.

[4] K. Juneja, "Random - Session and K - Neighbour Based Suspected Node Analysis Approach for Cooperative Blackhole Detection," *Wirel. Pers. Commun.*, vol. 110, no. 1, pp. 45–68, 2020, doi: 10.1007/s11277-019-06711-5.

[5] I. Ahmad, H. Jabeen, and F. Riaz, "Improved Qality of Service Protocol For Real Time Traffic In Manet," *Int. J. Comput. Networks Commun.*, vol. 5, no. 4, pp. 75–86, 2013, doi: 10.5121/ijcnc.2013.5407.

[6] T. Noguchi and T. Yamamoto, "Black Hole Attack Prevention Method Using Dynamic Threshold in Mobile Ad Hoc Networks," *2017 Fed. Conf. Comput. Sci. Inf. Syst. (pp. 797-802). IEEE.*, vol. 11, pp. 797–802, 2017, doi: 10.15439/2017F101.

[7] R. Chakravorty, "A Review on Prevention and Detection Schemes for Black Hole Attacks in MANET," *2020 8th Int. Conf. Reliab. Infocom Technol. Optim. (Trends Futur. Dir. Amity Univ. Noida, India.*, vol. 5, no. 4, pp. 801–806, 2020, doi: 10.1109/ICRITO48877.2020.9197810.

[8] A. H. Wheeb and M. T. Naser, "Simulation based comparison of routing protocols in wireless multihop ad hoc networks," *Int. J. Electr. Comput. Eng.*, vol. 11, no. 4, pp. 3186–3192, 2021, doi: 10.11591/ijece.v11i4.pp3186-3192.

[9] A. H. Wheeb and N. A. S. Al-Jamali, "Performance Analysis of OLSR Protocol in Mobile Ad Hoc Networks," *Int. J. Interact. Mob. Technol.*, vol. 16, no. 1, pp. 106–119, 2022, doi: 10.3991/IJIM.V16I01.26663.

[10] Sakshi & Khuteta, "Detecting and Overcoming Black hole attack in Mobile Adhoc Network," *2015 Int. Conf. Green Comput. Internet Things*, pp. 225–229, 2015, doi: 10.1109/ICGCIoT.2015.7380462.

[11] L. Tamilselvan and V. Sankaranarayanan, "Prevention of blackhole attack in MANET," in *In The 2nd international conference on wireless broadband and ultra wideband communications (AusWireless 2007) (pp. 21-21). IEEE.*, Sydney, NSW, Australia: IEEE,The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), 2007. doi: 10.1109/AUSWIRELESS.2007.61.

[12] S. Tan and K. Kim, "Secure route discovery for preventing black hole attacks on AODV-based MANETs," *Proc. - 2013 IEEE Int. Conf. High Perform. Comput. Commun. HPCC 2013 2013 IEEE*

Int. Conf. Embed. Ubiquitous Comput. EUC 2013, pp. 1159–1164, 2013, doi: 10.1109/HPCC.and.EUC.2013.164.

[13] D. Kshirsagar and A. Patil, "Blackhole attack detection and prevention by real time monitoring," *2013 Fourth Int. Conf. Comput. Commun. Netw. Technol.*, pp. 1–5, 2013, doi: 10.1109/ICCCNT.2013.6726597.

[14] D. Gautam and V. Tokekar, "ScienceDirect NSES 2018 A novel Approach for Detecting DDoS Attack in MANET," *Mater. Today Proc.*, vol. 29, pp. 674–677, 2020, doi: 10.1016/j.matpr.2020.07.332.

[15] M. B. M. Kamel, I. Alameri, and A. N. Onaizah, "STAODV: A secure and trust based approach to mitigate blackhole attack on AODV based MANET," *2017 IEEE 2nd Adv. Inf. Technol. Electron. Autom. Control Conf. (pp. 1278-1282). IEEE.*, no. March, 2017, doi: 10.1109/IAEAC.2017.8054219.

[16] T. Noguchi and T. Yamamoto, "Black hole attack prevention method using dynamic threshold in mobile ad hoc networks," *Proc. 2017 Fed. Conf. Comput. Sci. Inf. Syst. FedCSIS 2017*, vol. 11, pp. 797–802, 2017, doi: 10.15439/2017F101.

[17] A. Kumari Madhvi, S. Nishi, and YadavEmail, "Blackhole Attack Implementation and Its Performance Evaluation Using AODV Routing in MANET," R. Á. Ranganathan G., Chen J., Ed., Singapore, Singapore: Springer, Singapore, 2020, pp. 431–438. doi: https://doi.org/10.1007/978-981-15-0146-3_41.

[18] V. S. Bhargavi and S. V. Raju, "Enhancing security in MANETS through trust-aware routing," *Proc. 2016 IEEE Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2016*, pp. 1940–1943, 2016, doi: 10.1109/WiSPNET.2016.7566481.

[19] A. Suganya, S. Manojkumar, and A. G. Vigneshwari, "A Study on Discovering Malicious Nodes on MANET through Secure Intrusion Detection," vol. 25, no. 3, pp. 2444–2452, 2021.