Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.027819
Article

Tech Science Press

Avoid Suspicious Route of Blackhole Nodes in MANET's: Using A Cooperative Trapping

Abdllkader Esaid[1,*] and Mary Agoyi[2]

[1]Department of Computer Engineering, Faculty of Engineering, Cyprus International University, Nicosia, Cyprus
[2]Information Technology Department, School of Applied Sciences, Cyprus International University, Nicosia, Cyprus
*Corresponding Author: Abdllkader Esaid. Email: Aawatas2@gmail.com
Received: 27 January 2022; Accepted: 03 May 2022

Abstract: Mobile *Ad hoc* Network (MANET) is decentralized wireless network and can communicate without existing infrastructure in many areas. MANET is vulnerable to various attacks that affect its performance such as blackhole attack. Blackhole attacker, inject fault routing information to persuade the source node to select the path with malicious node as the shortest path. To eliminate malicious nodes from launching any collaborative attack. A cooperative Trapping Approach (CTA) was proposed based on modifying Ad-hoc On-demand Distance Vector (AODV) routing protocol and trapping the malicious nodes by responding to the trap request message. The approach aims to eliminate and rule out both single and collaborative malicious blackhole nodes from any attack. The approach realizes a backward tracking mechanism to perform the elimination process. The proposed algorithm (CTA) was executed using NS-2 network simulator. The performance metrics that has been considered to evaluate the performance of the proposed algorithm such as throughput, end to end delay, packet delivery ratio, and consuming energy. The experimental results have shown the performance metrics of the proposed approach outperformed other state of at algorithms.

Keywords: AODV; Blackhole; MANET; Malicious node

1 Introduction

Nowadays, mobile *ad hoc* networks (MANETs) are very common and employed due to many important characteristics such as ease of implementation in regions where geographical limitations [1]. Mobile Ad-hoc network is infrastructure less network where communication takes place between collections of mobile hosts. MANET is a dynamic network and open medium as well, where the mobile node can join to the network or leave without any restriction. This leads to changing network topology overtime [2]. The mobile nodes will operate as hosts and routers whenever participating in forwarding data packets and cooperating to form a local area network [3,4]. MANET is vulnerable to different types of attacks that affect its functionality and connectivity [5,6]. One of the nodes attacks is the black-hole attack is seriously declining the performance of the network, due to the malicious node activity of dropping all incoming packets [7–9].

There are two types of black-hole attacks, single and collaborative attack [10]. Whenever all the network traffic is changed to a single node, then it is considered a single black-hole attack where the malicious node will drop all the transmitted packets. While in collaborative black-hole attack, there will be more than one malicious node collaborate with each other to route required information [11,12].

In black-hole attack, the malicious node will prevent the network traffic to route the packet to the destination node and drop it. To specify the malicious node, this node will check its routing table and directly send a forged route reply (RREP) with the smallest number of hops counts and largest sequence number to indicate that it has the shortest path to the destination node [13–15]. Source node will receive many replies request (RREP) from different nodes, but it will respond to the one with largest sequence number that is generated by the malicious node. Consequently, the malicious node will drop all the received packets rather than forwarding them to the intended destination [16]. Then the malicious node will take all the routes towards itself and attack all the RREQ packets and accordingly will generate the forged RREP, which will be transmitted to the source node, which has the route for the destination node. In response to the RREP, the source node will send the packets to the malicious node that will drop all the packets received from the source node [17].

The malicious node will try to deceive the source node as it is a legitimate node by sending a fake reply message. Then, the malicious node may respond a high sequence number to the sending node which will be considered as the target node. Fig. 1 shows that the source node denoted as *S* is willing to communicate with destination node denoted as *D*, and to do this it will broadcast a RREQ packet to all the active nodes in the network.

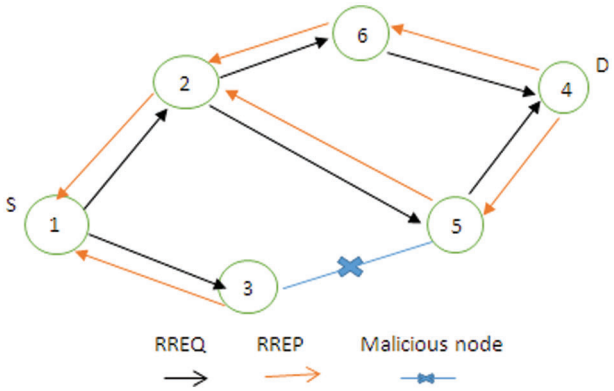

Figure 1: Blackhole attack node [18]

If node 3 is a malicious node, since all nodes receive the RREQ, check whether a route is available in the routing table. It will generate RREP packet and forward it to the source node, otherwise, it will forward it to other nodes in the network. The malicious node 3 whenever it receives RREQ packet from the source node 1 will send a forged RREP to the source node, which will accept the first reply from the malicious node since it will not check its routing table. Moreover, the malicious node will intercept the transmitted packets and drop them. In addition, the malicious node will intercept the RREQ packets and will not allow the establishment of any route in the network and use the whole power energy for sending its own packets [18]. *Ad hoc* On Demand Distance Vector (AODV) routing is very popular routing protocol for Mobile *Ad hoc* Network (MANET). The AODV suffers from many serious security problems and vulnerable to single and cooperative black-hole attacks. The malicious nodes in black-hole attack will attract the nodes to send data packets and later drop them rather than forwarding them [19,20]. Many algorithms were developed for detecting and preventing black-hole attacks based on AODV routing protocol. In this

paper, an elimination approach was developed based on modifying the AODV and then trapping the malicious nodes to send RREP. The proposed approach can be applied for elimination and ruling out of both single and collaborative black-hole attacks. The remaining of this paper is organized as follows. Section 1 provides the introduction. Section 2 related works. Section 3 overview of AODV. Section 4 Attack Model in MANET. Section 5 Blackhole elimination method. Section 6 Performance evaluation. Finally, section 7, the conclusion.

2 Related Work

Many approaches were developed for detecting malicious nodes in *ad hoc* networks (MANET). Most the proposed approaches were based for detecting black-hole attacks for single malicious node or detecting cooperative black-hole attacks. An approach for Detecting Collaborative blackhole Attacks (so-called DCBA) for detecting collaborative blackhole attacks in MANETs is introduced which about merges the advantage of proactive detection in the initial stage and reactive mechanism at later stages if the proactive detection approach fails to identify the malicious blackhole nodes. Malicious nodes are identified by means of our so-called suspicious values of nodes. [21]. A modified algorithm for a dynamic source routing (DSR) protocol (so-called detecting blackhole attack based on DSR (DBA-DSR)) is proposed to fight blackhole attacks in MANET networks. In this approach the blackhole nodes are identified whenever the attack occurred in the network. The DBADSR approach detects and isolates the blackhole nodes before any routing process. This is manipulated by implementing fake route request packets [22].

However, another scheme was developed based on AODV protocol. The scheme will be able to find a set of single malicious nodes for blackhole attack. Whenever a source node receives the RREQ_ACK message, it carries out a comparison between the destination sequence number (DSN) and the source sequence number (SSN) values. If SSN value is less than DSN value, then remove that node from quarantine list [23]. However, a new scheme is proposed to reduce the storage, routing overhead, and computational time for both single and cooperative blackhole attacks. The scheme includes forged route request, next hop information, and destination sequence to minimize the limitations of available schemes. The solution for these limitations was developing a fabricated RREQ and information of the next hop to mitigate both single blackhole attacks and collaborative blackhole attacks [24]. A smart blackhole detection and isolation scheme was introduced. The Timer Based Baited Technique (TBBT) integrated both baiting and timers' methods to detect the blackhole attack while keeping the performance measurements close to the original AODV [25]. A new approach was introduced for detection and prevention of both single and collaborative blackhole and grey hole attacks. The Enhanced Modified AODV (EMAODV) is preventing a full utilization of MANET network resources which is better than the original AODV, but it is increasing the routing overhead whenever the MANETs size is increasing [26].

Overview of AODV

There are several types of Routing protocols. One of the popular reactive routing protocols is Ad-hoc On-demand Distance Vector (AODV) that is intended for use in wireless and mobile ad-hoc networks. AODV uses low energy and memory overhead during transmission processes. AODV support both unicast and multicast routing, which employ when there is no valid route to the destination in the routing table. Therefore, the source node will initiate route request (RREQ) and then transmit a packet through various network nodes to the appropriate destination. AODV employs four various types of messages, Route Request (RREQ), Route Reply (RREP), Route Error (RERR), and hello (HELLO), to discover the shortest path to the destination [27].

3 Attack Model in MANET

In blackhole attack, the node that has suspicious behaviors and include themselves in the route replies to the route requests it receives, and then it creates illusion thought announce that have shortest path to a destination with minimum hop count. These fake replies can be fabricated to divert network traffic through the malicious node to attract all traffic to perform its attack by dropping the packet that has been received [28] blackhole attack consist of two types which are, single and cooperative blackhole.

Single blackhole, as showed in Fig. 2, only one malicious node exists in the network that incorrectly sends the RREP that has a latest route with minimum hop count to destination and then it drops all the receiving packets [29].

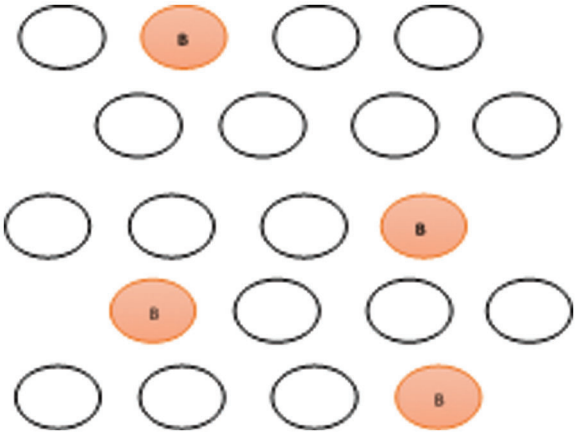

Figure 2: Single black-hole [28]

Cooperative black hole, as showed in Fig. 3 there are when multiple malicious nodes cooperate with each other to captures packets and not forwards them in the network, then it will advertise themselves as having the shortest path to the destination [29].

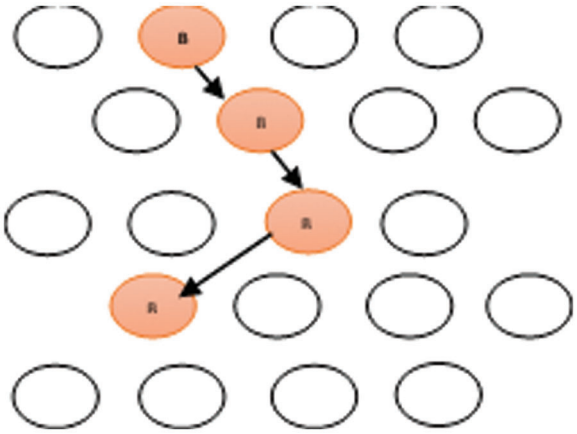

Figure 3: Cooperative black-hole [29]

4 Blackhole Elimination Algorithm

The cooperative trapping approach is developed for eliminating and ruling out malicious nodes that perform collaborative black hole attacks in MANETs. The source node (SCN) will select one of the neighboring nodes for cooperation, where the address of this node will be used as an address of the trapping destination node to trap malicious nodes to respond to RREQ message by sending RREP message. Thus, the malicious nodes will be eliminated and ruled out from taking part in the routing process by backward tracking technique. The approach can provide elimination for both single and collaborative blackhole attacks. It is based on AODV protocol by modifying this protocol to operate for elimination and ruling out attacks in cooperative blackhole which we called CB-AODV. Moreover, the collaborative trapping elimination technique also has the capability to act as a proactive response as well as for reactive response to minimize the MANET's resources as shown in Fig. 4. The proposed approach consists of the following main steps which is given in the below flowchart.

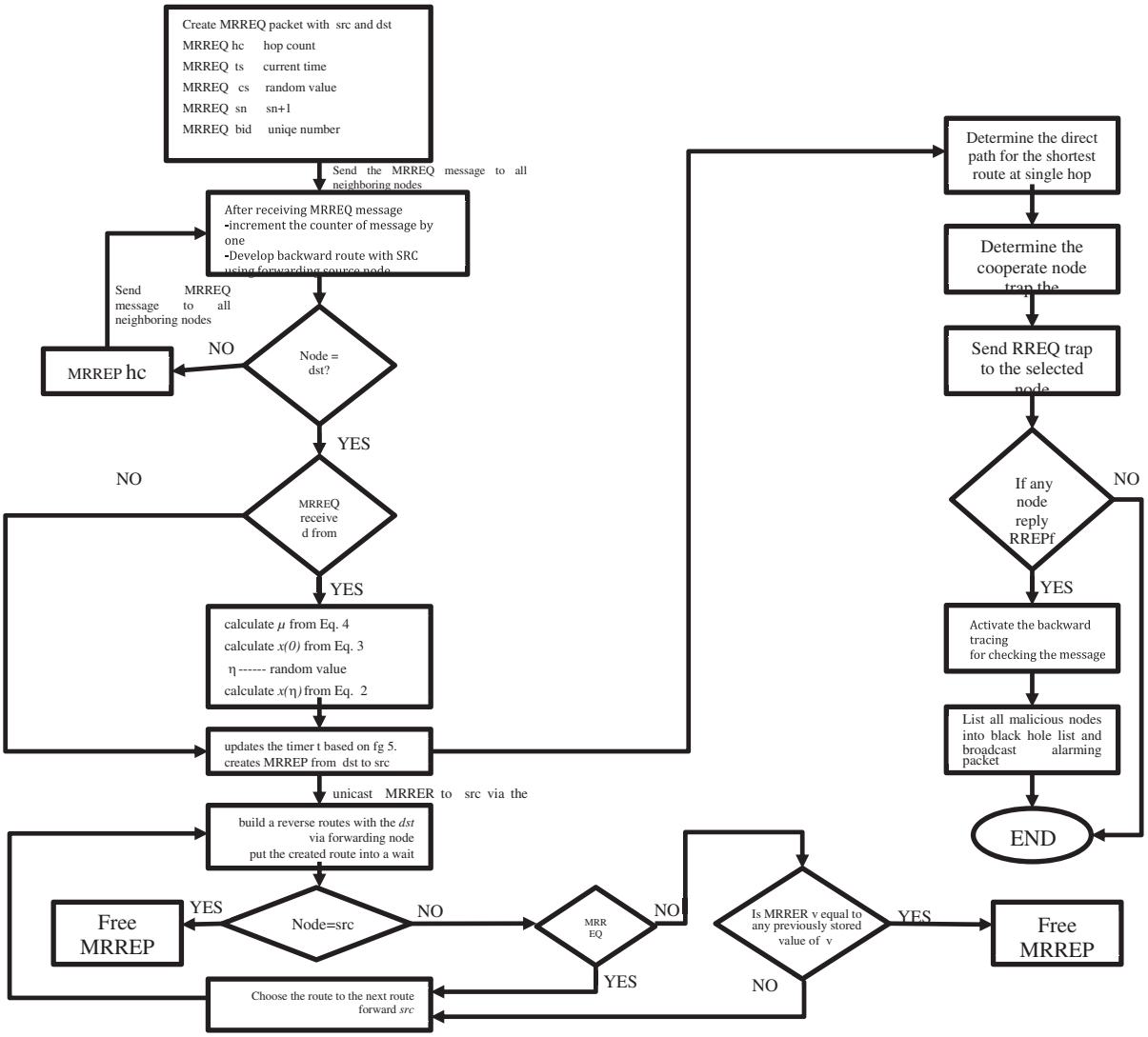

Figure 4: Flowchart of the proposed approach

4.1 Collaborative Blackhole-AODV

In this step collaborative Blackhole *Ad hoc* On-demand Distance Vector (CB-AODV) was developed which is based on AODV routing protocol, where four types of messages will be generated as follows: MRREQ "Modified Route REQuest", MRREPLY "Modified Route REPly", HLO "HELLO", and RCONF "RCONfirm". The CB-AODV modified the RREQ and RREP while adopted the HELLO message developed in [30].

4.1.1 Modified Route Request (MRREQ)

The source node (SCN) will send the MRREQ message to all neighboring nodes and then to the destination node (DSN). wo field are introduced to the original message RREQ of the AODV which are referred as Check Random Number (CRN) that used in sender node. The source node will generate MRREQ that is including the required parameters such as check random number (crn) which is generated by the source node randomly, hop count (hc) where each node increments the number of hops by one count, broadcasting ID (bid) is generated by the source node to enable neighboring nodes to respond whenever the data is obtained, and time stamp (ts).

4.1.2 Modified Route Reply (MRREP)

The destination node (DSN) upon receiving the MRREQ will start calculating the responsive (V) value and send this value on the route paths to the nodes and backward routes that are generated by the DSN.

The value (V) can be calculated using Eq. (1).

$$\mathrm{V} = \left[X(h) * 10^{14}\right] \tag{1}$$

where x(η) is the Logistic chaotic map that is used to employ the many useful features such as randomness, ergodicity, and sensitivity, and can be calculated using Eq. (2)

$$X(h) = \mu x(h-1)[1 - x(h-1)] \tag{2}$$

where X (0) Î (0,1) and η Î (0,4]

where η is a randomly generated value by the DSN and is considered as a secret value to display the number of iterations of the chaotic map. To find out the best value for calculating the chaotic behavior of the map, the value μ should be kept within the range μÎ [3.5699456,4] [28]. To calculate X(0) as well as μ, Eqs. (3) and (4), can be applied respectively

$$X(0) = (crn/N1)\ mod\ 1 \tag{3}$$

$$\mu = 3.5699456 + 0.43((crn/N2)\ mod\ 1) \tag{4}$$

To modify the timer by the destination node (DSN), the timer t can be calculated by applying Eq. (5).

$$t = \sum_{i=1}^{n} (t_{ri} - t_s)/2n \tag{5}$$

where ts is the stamp time that calculated by the destination node at the time of MRREQ message generation in millisecond.

4.1.3 Route Confirmation (Rcon)

The RCON message will be generated by the destination node (DSN) whenever the timer's value will reach the zero value. The DSN will send the RCON message to all neighboring nodes which involve the confidential values of η, N1, and N2 that stored at the DSN node to other nodes. Moreover, it detects the malicious nodes that were intended to act as blackhole attacking nodes and deleting these routes that include malicious nodes. Moreover, when any intermediate node will receive many "RCON" messages

from various nodes that is not in route paths in each interval of time. This intermediate node should compare N1, N2, and η values. If most of the messages of RCON have the same value, then, the intermediate node will broadcast only one of these messages. Otherwise, if the intermediate node received many RCON messages with same value, then the intermediate node should neglect this message. In the other side, when intermediate nodes will receive many messages from various nodes in the given time, it can do one of the following actions.

- The node computes the value (n) using Eq. (1) for all "RCON" messages that are received and that depend on the obtained values for R1, R2, and η associated with the value of cnr that is available in the routing table of the node.
- The node will make a comparison of each value of (n) to find out the best-matched value designated by nm.
- The intermediate node will make a comparison of the value of nm with every value ni related to the ith position in its routing table.
- Whenever the nm and ni have the same values, then the intermediate node puts the ith route into a working status. Else, the node declares that the forwarded node relative to the ith position in routing table is a node that has suspicious behavior. Accordingly, it will delete this node from the routing table.
- Whenever the intermediate node is not the source (SCN) node, it sends the mostly matched value with nm to its neighboring nodes. Else, the SCN node forwards the data packets to the DSN.

4.1.4 Hello Message (HLO)

The task of HELLO message is realized in the approach to assist every node to indicate which nodes are their neighboring nodes within one hop. This message will help in broadcasting the trapping address to attract the malicious nodes to use the back-tracking procedure to determine the exact the addresses of the malicious node. The message includes (destination node IP address, destination node sequence number, current hop count, which is zero, and lifetime).

4.2 Step 2: Trapping Node Initialization

The trapping RREQ′ message is like the original RREQ message, except the destination addresses is the trapping address. The aim of this procedure is to attract the malicious node to respond to RREQ′ by sending a reply message RREP. Once the source node (SCN) selects any neighboring node nr that is within its one-hop neighboring nodes and collaborates with this node by making its address as the destination address of the Trapping RREQ′. This neighboring node will be changed whenever the node will be moved. So, the trapping node will also be changing as well. The trapping procedure will be switched whenever the trapping RREQ′ will be sent earlier before requesting for the initial routing path. The trapping procedures can be described as follows:

- Whenever a node Ni is not performing any a blackhole attack then after the SCN node sending a RREQ′ message there may be other nodes will send RREP besides to the Ni node. This means that the malicious node is available in in the routing reply to nodes. Thus, the backward tracking approach will be executed. In case only Ni node has sent reply, this means there is no other malicious node in the routing paths.
- Whenever Ni node is a malicious node and performed a blackhole attack. And after SCN node sent the RREQ′ message and beside this node other nodes had sent a RREP message. This means that there is a malicious node available in the reply route and backward tracking procedure will be executed.
- Whenever Ni node intentionally will not send RREP message, then this node will be placed in the blackhole list.

- Whenever only Ni node sent a RREP reply, it means that there are no more nodes that are malicious except that routing table distributed by Ni node.

4.3 Step 3: Backward Tracking Initialization

The backward tracking procedure is employed to detect the malicious nodes through the route reply to the RREQ′ message. Whenever a malicious node receives RREQ′ then it will send a fake RREP. Then the backward tracking procedure will be carried out for the nodes that receive RREPs messages to find the information for suspicious path, and for not suspicious paths in the route. The approach has the capability to discover many malicious nodes simultaneously. If a malicious node send a fake RREP message, then a n address list will be formed L= {N1, ..Nj, …Nk,… Nl} and these addresses are included in the RREP message. When for example Nj node receives RREP message, then this node will place in the list all the nodes based on the destination address of N1 of the RREP, L′ = {N1, …Nj}. Next, the Nj node will find the difference between the address list L and L′ and thus to obtain:

$$L'' = L - L' = \left\{N_{j+1}, \ldots, N_k, \ldots, N_l\right\} \tag{6}$$

where L″ list contains the information stored in Nj to the destination node. This information will be included in RREPs "backward field" then backward to the source node. The source node will receive RREP and the L″ list addresses of the nodes that obtained RREP. Once the node Nj will carry out a comparison for:

a) The address part in the IP fields of the source node in RREP
b) Compare the next hop of Nj in the L′.
c) Next hop of Nj

Whenever I is different from II, and III, then the received L″ can backtrack. Otherwise, N_j has to backtrack the L″ that was generated by itself.

4.4 Step 4: Reactive Defense Procedure

Whenever the route is generated, and it was shown the packet delivery ratio (PDR) at the destination node reaching to the threshold value. This will activate the detection procedure to follow up the maintenance and checking the efficiency. It was assumed that the threshold value is between 85% and 95% and this value can be adjusted based on the network efficiency. A procedure for controlling the packet delivery ration reduction with the time will be employed. In case of any reduction then it indicates that there are malicious nodes available at the network, which requires changing in the threshold value according to the PDR value.

5 Performance Evaluation

To evaluate the performance of the proposed approach, a simulator NS-2 was used with different number of nodes in the network [29]. During the testing scenario, several malicious nodes are collaborating to carry out this attack. The performance is tested and measured form different networks metrics such as packet delivery ration (PDR), throughput, end to end delay, and consumed energy. The obtained results are compared with the performance of two other approaches Modified AODV (M-AODV) [30], and IDS-AODV (intrusion detection system) [31]. The simulation parameters are shown in Tab. 1.

Table 1: List of simulation parameters

Parameter	Value
Simulator	NS-2.3/Ubuntu 16.04 LTS
Topological area	800 m × 800 m
Simulation time	100 s
Node locations	Randomly
Radio propagation model	Two-ray ground reflection
Antenna type	Omni antenna
Mobility model	Way point
Traffic type	CBR
Packet size	512 bytes
Number of nodes	25,50,75,100 nodes
Protocol	AODV
Channel type	Wireless channel 802-11
Mobility	Dynamic

5.1 Throughput

The obtained result for the throughput is shown in Fig. 5 for different number of nodes in the network. The results for throughput show that the proposed approach (CTA) outperforms other compared approach such as AODV, M-AODV and IDS-AODV for different number of nodes (*e.g.*, 25, 50, 100), with values (198.336, 289.158, and 331.402) respectively. While it is (40,25, and 40) for AODV while (38.162, 25.644, and 41.051) for M-AODV, and (90, 88, 79) for IDS-AODV. The result of AODV whenever there is blackhole node in the network is the minimum due to the drop in the packets which is performed by blackhole node. While the proposed approach was the highest and has shown an improvement, which is due to capability of dropping any reply from any malicious node.

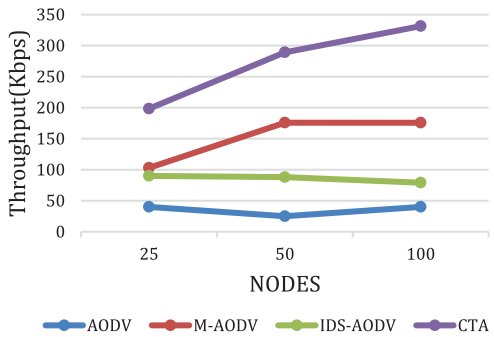

Figure 5: Results of throughput for CTA compared with AODV, MAODV and IDS-AODV

5.2 Delivery Ratio

The obtained results of packet delivery ratio (PDR) are shown in Fig. 6. The comparison results show that the packet delivery ratio for the proposed approach (CTA) and other three approaches AODV, M-ADOV and IDS-AODV. The packet delivery ratio results are (88.895, 89.695, and 87.104) respectively. While it is

(35, 25, and 40) for AODV, M-ADOV is (36.15, 32.19 and 38.48), and IDS-AODV is (80, 78, and 76) respectively. The reason behind that, because of CTA forward large amount of packet to the destination and less packet drop compared with other approaches. Thus, the proposed approach outperformed the other three approaches under black hole attack. The AODV approach has shown the lowest value of PDR whenever there is a blackhole node in the network because it will try to cut any connection between the nodes whenever they try to communicate with each other. The proposed approach (CTA) has shown the highest PDR among the compared approaches. The improvement of the PDR while employing CTA is due to the drop of any replay that is from a malicious node which may minimizes the PDR value.

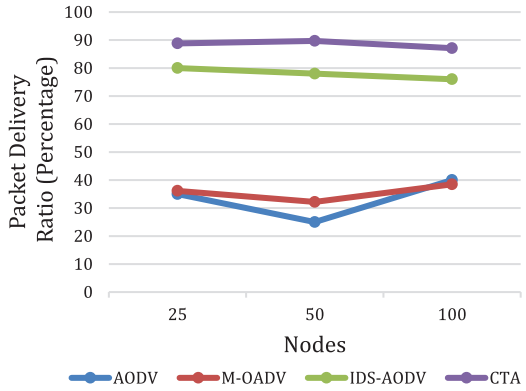

Figure 6: Results of PDR for CTA compared with AODV, MAODV and IDS-AODV

5.3 End to End Delay

End to end delay is the measured time for the packet takes from the source node to the destination. The obtained result for the end-to-end delay is shown in Fig. 7 for different number of nodes in the network (25, 50, 100). The obtained result of the proposed approach (CTA) is (0.2353, 0.1476, 0.10269) respectively, due to a smaller number of hops across the network where the packet does not require long time to reach the destination. The result of end-to-end delay shows that the MAODV is the highest whenever there is blackhole nodes, while the proposed approach CTA is less than the AODV, MAODV, and IDS-AODV.

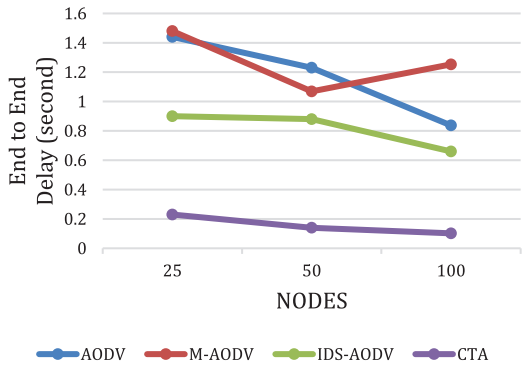

Figure 7: Results of end-to-end delay for CTA compared with AODV, MAODV and IDS-AODV

5.4 Consumed Energy

The proposed approach is tested against the energy consumption and compared with two approaches AODV and S-AODV developed for blackhole attack with different numbers of nodes [32,33]. The

obtained results have shown that, the proposed algorithm is consuming less energy than AODV and S-AODV approaches when the network under attack as shown in Fig. 8.

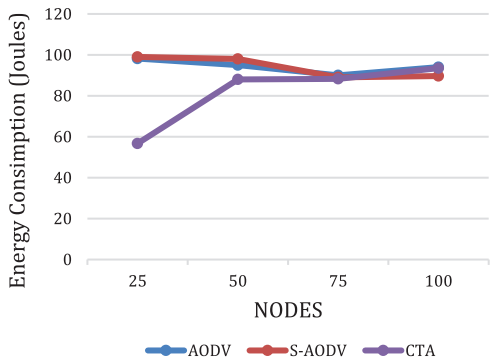

Figure 8: Energy consumption for CTA compared with AODV and SOVAD

5.5 Routing Overhead

The Fig. 9 below shows the performance of a network in terms of routing overhead in the proposed approach CTA compared with other approaches over different network density. There is increase in routing overhead in CTA approach compared with IDS-AODV, and less overhead compared with AODV and M-AODV. The reason behind that, due to more control messages transmitted or forwarded to discover the routes. Thus, CTA has high routing overhead among some other approaches, due to more control packets has been transmitted while simulation processing [34].

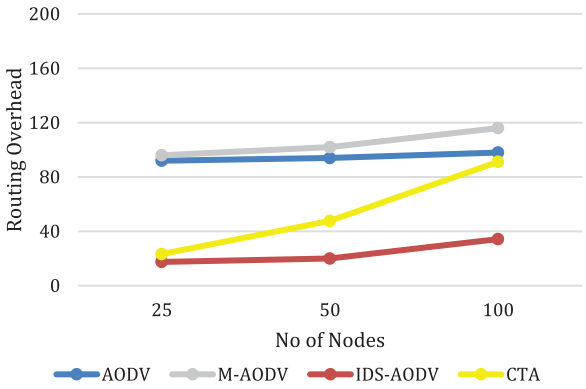

Figure 9: Routing Overhead for CTA compared with AODV, M-AODV and IDS-AODV

5.6 Detection Rate

The use of CTA proposed approach can increase the probability of detection of malicious nodes as shown in Fig. 10 compared with DSCL approach. The detection rate used to evaluate the efficiency of any proposed detection mechanism, which is the number of malicious nodes that have been detected by the system. It shows that the CTA significantly increase this probability of detection along with various number of nodes up to 2% compared with DSCL approach. This is justified by the fact that CTA disregards the untrustworthy evidence upon building the final decisions [35]. Moreover, the neighboring nodes will be used as trapping for detection process, which will lead to increase detection rate. On the other hand. DSCL approach based on watchdog architecture, which increase the possibility of ambiguous

collision and delay. CTA approach provide more accurate detection on each node and enhancing hence the probability of detection.

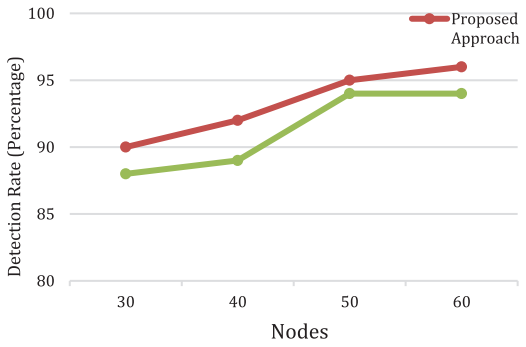

Figure 10: Detection rate between CTA compared with DSCL

5.7 False Negative Rate

False negative rate (FNR) occurs when an actual attack cannot be detected. Fig. 11 reveals that using CTA approach can minimize considerably the percentage of false negatives compared with DSCL approach. This is since the source node in CTA may not receive RREP from the malicious node. Increasing number of nodes will increase the connectivity between them, which will make the malicious node discovered by its neighbors. However, the FNR rate was not relatively high compared with DSCL approach, where it reaches the maximum 0.29 in CTA approach, because the malicious node refuses to unicast the RREP message and the trap will not be able to detect them [36].

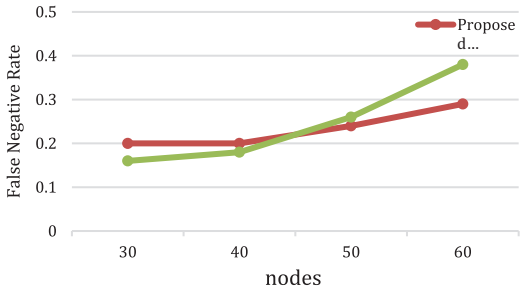

Figure 11: False negative rate between CTA compared with DSCL

5.8 False Positive Rate

Fig. 12 shows the CTA proposed approach minimizes the false positive rate (FPR) with increasing number of nodes, and the reason behind that due to the fast recognition of malicious nodes and eliminating them with the cooperation of neighboring legitimate nodes will increase the FPR. In fact, the false positive rate is included between zero and reach maximum 2.1 percent, which lower value of FPR compared with DSCL approach [36].

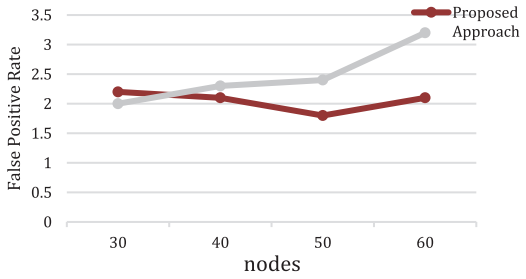

Figure 12: False positive rate between CTA compared with DSCL

6 Conclusion

A Cooperative Trapping Approach (CTA) was proposed for eliminating malicious nodes in MANET networks under blackhole attacks. The collaborative blackhole (CB-AODV) was introduced based on the original AODV routing protocol for ruling out any blackhole attack from any malicious nodes that act maliciously during forwarding process. While a collaborative trapping part was employed for backward backtring to trap the malicious nodes by sending RREP. The CTA was implemented using network simulator NS-2 and the obtained results were compared with other protocols and approaches for different metrics and the experimental results outperformed of the proposed approach by others.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Kalita, B. Sharma and U. Sharma, "Attacks and countermeasures in mobile *ad hoc* network analysis," *Inernational. Journal on Advanced Computer Theory and Engineering*, vol. 4, no. 3, pp. 16–21, 2015.

[2] M. Tahboush and M. Agoyi, "A hybrid wormhole attack detection in mobile *ad hoc* network (MANET)," *IEEE Access*, vol. 29, pp. 11872–11883, 2021.

[3] I. Chlamtac and M. Contiband J. Liuc, "Mobile *ad hoc* networking: imperatives and challenges," *Ad Hoc Networks*, vol. 1, no. 1, pp. 13–64, 2003.

[4] H. Ting and R. Chang, "Improving the performance of broadcasting in *ad hoc* wireless networks," *Journal of Internet of Things*, vol. 4, no. 4, pp. 209–216, 2003.

[5] H. Yang, H. Lou, F. Ye, S. Lu and L. Zhang, "Security in mobile *ad hoc* networks: Challenges and solutions," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 38–47, 2004.

[6] P. Papadimitratos and Z. Haas, "Secure data transmission in mobile *ad hoc* networks," in *2nd ACM Workshop on Wireless Security (WiSe 03)*, San Diego, CA, pp. 41–50, 2003.

[7] J. Huang, I. Woungang, H. Chao, M. Obaidat, T. Chi and *et al.,* "Multi-path trust-based secure AOMDV routing in *ad hoc* networks," in *Global Telecommunications Conf. (GLOBECOM 2011)*, Kathmandu, Nepal, pp. 1–5, 2011.

[8] A. Dureja and V. Dahiya, "Comparative study of collaborative attacks and security mechanism in MANET," *International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)*, vol. 4, no. 3, pp. 139–148, 2014.

[9] A. Sharma, R. Singh and G. Pandey, "Detection and prevention from black hole attack in AODV protocol for MANET," *International Journal of Computer Applications*, vol. 50, no. 5, pp. 1–4, 2012.

[10] W. Saetang and S. Charoenpanyasak, "CAODV free blackhole attack in *ad hoc* networks," in *Int. Conf. on Computer Networks and Communication Systems*, vol. 35, pp. 63–68, 2012.

[11] S. Padmavati, "Performance analysis of black hole attack on vanet's reactive routing protocols," *International Journal of Computer Applications*, vol. 73, no. 9, pp. 22–26, 2013.

[12] D. Patel and K. Chawda, "Blackhole and grayhole attacks in MANET," in *Int. Conf. on Information Communication and Embedded Systems*, vol. 6, pp. 4799-3834-6/14/, 2014.

[13] W. Wang, B. Bhargava and M. Lindeeiman, "Defending against collaborative black-hole packet drop attacks on MANETs," in *2nd Int. Workshop on Dependable Network Computing and Mobile Systems (DNCMS'2009) in Conjuction with IEEE SRD'2009)*, NewYork, vol. 27, pp. 1–6, 2009.

[14] R. Kaur and J. Kalra, "A review paper on detection and prevention of black hole in MANET," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 6, pp. 37–40, 2014.

[15] S. Padmavati, "Performance analysis of black hole attack on vanet's reactive routing protocol's," *International Journal of Computer Applications*, vol. 73, no. 9, pp. 22–26, 2013.

[16] M. Roopak and B. Reddy, "Performance analysis of AODV protocol under black hole attack," *International Journal of Scientific & Engineering*, vol. 2, no. 8, pp. 1–13, 2011.

[17] M. Ghonge and S. Nimbhorkar, "Simulation of AODV under blackhole attack in MANET," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 2, pp. 1–5, 2012.

[18] F. Seng, L. Chou and H. Chao, "A survey of black hole attacks in wireless mobile *ad hoc* networks," *Humen-Centric Computing and Information Sciences*, vol. 1, no. 4, pp. 1–16, 2011.

[19] M. Brindha Devi, T. Kalaikumaran and S. Karthik, "A survey on attacks in adhoc on demand distance vector protocol," in *11th Int. Conf. on Intelligent Systems and Control (ISCO17)*, pp. 485–488, 2017, DOI 10.1109/ISCO.2017.7856041

[20] N. Mistry, D. C. Jinwala and M. Zaveri, "Improving AODV protocol against blackhole attacks," in *Int. Multi Conf. of Engineers and Computer Scientists*, Hong Kong, vol. 2, pp. 17–19, 2010.

[21] I. Woungang, S. Kumar, R. Dheeraj and I. Traore, "Mitigating collaborative blackhole attacks on DSR-based mobile *ad hoc* networks," in *5th Int. Symp. FPD2012*, Monterial, Canada, pp. 308– 323, 2012.

[22] I. Woungang, S. Kumar, M. Obaidat and R. Dheeraj, "A DSR-based routing protocol for mitigating blackhole attacks on mobile *ad hoc* networks," *Security Communication Networks*, vol. 9, pp. 420–428, 2016.

[23] H. Changela and A. Lathigara, "Algorithm to detect and overcome the black hole attack in MANETs," *International Journal of Computer Applications*, vol. 124, no. 8, pp. 22–26, 2015.

[24] M. Sathish, K. Arumugam, S. Neelavathy and V. S. Harikrishnan, "Detection of single and collaborative black hole," in *Attack in MANET, 2016 Int. Conf. on Wireless Communications, Signal Processing and Networking (WiSPNET)*, India, IEEE, IEEE WiSPNET conference, pp. 2040–2044, 2016

[25] A. Yasin and M. Abu Zant, "Detecting and isolating black-hole attacks in MANET using timer based baited technique," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 9812135, Hindawi, https://doi.org/10.1155/2018/9812135. 2018.

[26] A. Rana, V. Ranab and S. Guptac, "EMAODV: Technique to prevent collaborative attacks in MANET's," *Procedia Computer Science*, vol. 70, pp. 137–145, 2015.

[27] M. Tahboush, M. Agoyi and A. Esaid, "Multistage security detection in mobile ad-hoc network (MANET)," *International Journal of Engineering Trends and Technology*, vol. 68, no. 11, pp. 97–104, 2019.

[28] A. Esaid, M. Agoyi and M. Tahboush, "A Hybrid encryption algorithm for mitigating the effects of attacks in *ad hoc* networks," *The ISC International Journal of Information Security*, vol. 12, no. 3, pp. 19–27, 2020.

[29] V. G. Mohite and L. Ragha, "Security agents for detecting and avoiding cooperative blackhole attacks in MANET," in *2015 Int. Conf. on Applied and Theoretical Computing and Communication Technology (iCATccT)*, pp. 306–311, DOI 10.1109/ICATCCT.2015.7456900, 2015.

[30] N. Kalia and H. Sharma, "Detection of multiple blackhole node attack in MANET by modifying ADOV protect," *International Journal on Computer Science and Engineering*, vol. 8, no. 5, pp. 160–174, 2016.

[31] G. Sharma, "A Modified approach of preventing and minimizing the black hole attack in VANETs (Vehicular Ad-hoc Network Systems)," *International Journal of Advanced Science and Technology*, vol. 29, no. 5, pp. 8713–8717, 2020.

[32] I. Nurcahyani and H. Hartadi, "Performance analysis of ad-aoc on-demand distance vector (AODV) and dynamic source routing (DSR) under black hole attacks in mobile *ad hoc* network (MANET)," in *Int. Symp. on Electronics and Smart Devices (ISESD)*, pp. 1–5, 2018. DOI 10.1109/ISESD.2018.8605445.

[33] M. Goswami, P. Sharma and A. Bhargava, "Black hole attack detection in MANETs using trust based technique," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 9, no. 4, pp. 1446–1451, 2020.

[34] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc on demand distance vector (AODV) routing document RFC:3561," *IETF MANET Working Group*, pp. 70–575, 2003.

[35] M. Wang, X. Wang, Y. Zhang and Z. Goa, "A novel chaotic encryption scheme based on image segmentation and multiple diffusion models," *Optics & Laser Technology*, vol. 108, no. 2, pp. 558–573, 2018.

[36] T. Issariyakul and E. Hossain, "Introduction to network simulator NS2," *Computer Science and Engineering*, vol. 8, no. 5, pp. 160–174, 2016.