Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7704740

DETECTION AND REMOVAL OF MALICIOUS NODE IN AD-HOC NETWORK USING DSR ROUTING ALGORITHM AND CBDS METHOD

Pragati Singh[1], Ashok Kumar Yadav[2] and Sanjeev Gangwar[3]
[1]Research Scholar, Dept. of CSE, UNSIET, VBSPU Jaunpur, Emai id: pragatisingh552@gmail.com
[2]Asst.Prof., Dept. of CSE, UNSIET, VBSPU Jaunpur, Email id: ashok231988@gmail.com
[3] Asst.Prof. & HEAD, Dept. of CSE, UNSIET, VBSPU Jaunpur, Email id: gangwar.sanjeev@gmail.com

Abstract-Now-a-days, mobile ad-hoc network is growing tremendously. Establishment of communication between nodes is very hectic and required task. A primary requirement for the establishment of communication among nodes in mobile ad hoc network (MANETs) is that nodes cooperate with one another. This requirement may raise serious security concerns in the presence of malicious node; for example, such nodes may disrupt the routing process. Preventing or detecting malicious nodes launching gray-hole or collaborative black hole attacks is a challenge in the context. This paper attempts to address this issue by developing the cooperative bait detection scheme, a dynamic source routing mechanism that combines the benefits of both proactive and reactive defense architectures. To help achieve the stated goal, our CBDS method employs a reverse tracing technique. In our proposed work black-hole nodes are detected and removed from communication path, with the help of CBDS algorithm. CBDS algorithm detects node with the Bait RREQ and RREP messages.

I. INDEX TERMS— Dynamic Source Routing (DSR), Cooperative Bait Detection Scheme (CBDS), RREQ, RREP, Bait RREQ.

1. INTRODUCTION

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. Mobile ad-hoc networks (MANET) are self-organizing and self-configuring multi hop wireless networks that changes dynamically. This is mainly due to the random mobility of the nodes in the network to access wireless channel.

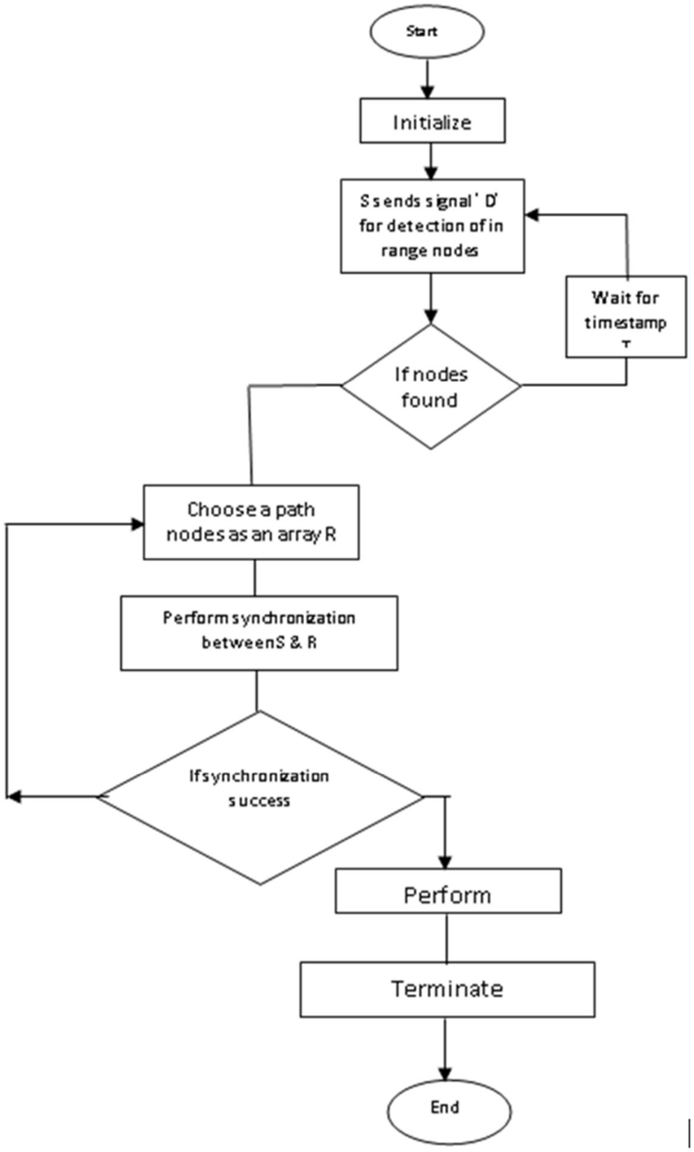

Start
Initialize
Ssends signal ' D' for detection of in range nodes
Wait for timestamp T
If nodes found
Choose a path nodes as an array R
Perform synchronization betweenS & R
If synchronization success
Perform
Terminate
End

Figure 1. Flowchart of ad-hoc network

Mobile ad-hoc networks open the window for the fixed devices to establish networks on the fly, i.e., formally, a The node in the network not only acts as hosts but also as routers that route data to/from other nodes in network in multi hop way. MANET is collection of mobile devices which form communication network with no pre-existing wiring or infrastructure.

1.1 Dynamic Source Routing Protocol (DSR):

Dynamic Source Routing Protocol, is a reactive/on-demand routing protocol, discovers routes only when needed. The route discovery process is performed by flooding route request packets throughout the network. DSR uses different phases as:

Route Discovery: This phase determines the best path for the transmission of data packets between source and destination mobile nodes.

Route maintenance: This phase performs route maintenance work. This is because the topology of mobile ad-hoc networks is dynamic in nature and there are many cases of lost connectivity leading to network failures between mobile nodes.[1]

1.2 Co-operative Bait Detection Schema (CBDS):

Recognizable evidence of malicious hub is critical for recovering the organization from any attacks. A DSR-based methodology called the Cooperative Bait Detection Scheme (CBDS). Suggested identifying the dark opening assault as the next step, this methodology demonstrates valuable distinguishing proof and receptive reaction. It is completed by selecting the neighboring hubs to collaborate in identifying the malevolent hub when the neighboring hub address is used the malignant hub also sends the target location for the trap. The RREP reaction accepting and grouping the malicious hub, the opposite follow-up method is employed. Following are CBDS, baiting, invert follow, and receptive assurance.[2]

1.3 Malicious node:

Malicious node is under attacks as a result of breaches in the security principle and is said to be acting maliciously for example, in black-hole and gray-hole attacks, malicious node can disrupt the routing process and network performance of decreases. A malicious node lures all packets in a black-hole attacks. Using RREP's replica to falsely claim that it has the shortest and a new path to the destination so, once it begins to receive is a distinct type of black-hole in which nodes can exist. Reject packets based on a probabilistic condition that forwards data packets cooperative black-hole attacks there are numerous malevolent nodes.[3]

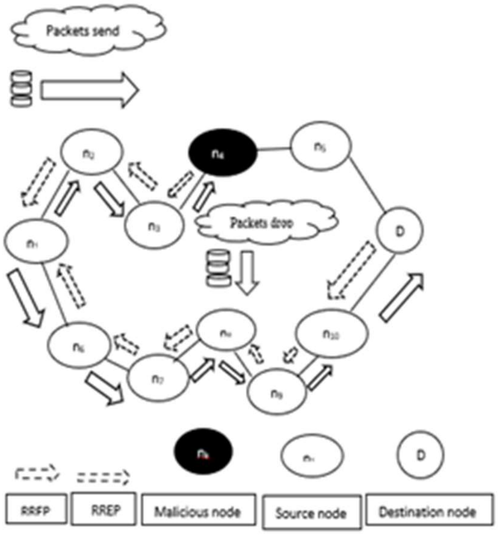


Figure 2. Black hole[4]

2. LITERATURE REVIEW

Khan et al. In this paper, the source node detects and prevents black hole attacks. By employing a binary partition clustering algorithm we compared the performance of the proposed solution with existing solution and demonstrated that our solution outperforms it the current one.[5]

Chang et al. this paper describes a mechanism for detecting malicious nodes initiating black-hole/grey-hole attacks as well as cooperative black-hole attacks. Cooperative Bait Detection Scheme attacks (CBDS). it combines proactive and reactive defense architectures cooperates at random with a stochastic adjacent node by utilizing as the bait algorithm we compared the performance of the proposed solution with existing solution and demonstrated that our solution outperforms it the current one.[4]

Woungang et al. this paper introduction a novel scheme for detecting black hole attacks in MANETs (dubbed DBA-DSR). The BDA-DSR protocols recognizes and avoids before the actual routing mechanism is implemented, there is a black hole problem. Began by impersonating RREQ packets in order to catch the malicious nodes. The simulation result demonstrate that the in terms of performance, the proposed DBA-DSR scheme outperforms DSR. Chosen as packets delivery ratio and network throughput when black hole nodes are present, performance metrics the system.[6]

Dumne et al. we proposed a method to solve this problem in this paper by using a malicious node detection scheme based on the DSR mechanism cooperative bait detection (CBDS) that employs hybrid defense architectures. CBDS by employing a reverse search technique, malicious node can be identified. Trace technique the fundamental and proposed CBDS schemes are as follow: NS-2.35 include this feature. The outcomes are evaluated using PDR, throughput.[3]

Emimajuliet et al. the modified cooperative bait detection scheme is a technique proposed in this paper. It is better suited to countering collaborative attacks. CBDS, in addition to the Destination Sequenced Distance Vector protocols is used superior to DSR and 2ACK schemes.[7]

Patel et al. In this paper, I implemented a malicious node that drops packets on a regular basis and investigated its impact on wireless LAN and AODV routing. Have also implemented an enhanced AODV that detects and avoid such nodes while the AODV route is being established. The results of the simulation show that the route discovery time and throughput is higher in modified AODV than in standard AODV.[8]

Guruprasanna et al. In this paper, we present a novel solution to this problem. This paper describes a novel method known as CBDS (co-operative bait detection discovery method) for detecting a malicious attacks caused by malicious node in the MANET, and create an efficient route in the network to transport data from the source node to the destination node without data loss and set up the DSR is a routing scheme that provides an efficient route. (Dynamic Source Routing Scheme). This CBDS procedure uses a novel technique to determine the precise location of reverse trapping technique refers to malicious nodes in the network. To achieve the goal of this paper, the CBDS scheme employs both proactive and reactive mechanisms.[9]

3. PROPOSED APPROACH

3.1 Proposed Dynamic Source Routing Protocol (PDSR)

It involves two processes: route discovery and route maintenance. To perform the route discovery phase, the source node broadcasts Route Request (RREQ) packets through the network. If an intermediate node has routing information for a destination in its route cache, it will reply to the source node with RREP. When RREQ is forwarded to a node, the node adds its address information to the route record in the RREQ packets. When the destination receives the RREQ, it can know the address of each intermediary node in the middle of the route. The destination node relies on the routing information gathered between packets to send a reply message to the source node with complete routing information for the established route. There is no detection mechanism in DSR. But the source node can get all the route information related to the nodes on the route.

3.1.1 Advantages and Disadvantage of PDSR:

Advantages of PDSR:

- A perfect route is discovered always.
- Highly efficient
- Low bandwidth consumption

Disadvantages of PDSR:

- If the route gets broke, data transmission cannot happen.
- Time taking algorithm – slow.
- If network is large, then it is impossible for the data packets header to hold whole information of the routes.

3.2 PCBDS (Proposed Co-operative Bait Detection Scheme)

The CBDS method is used to detect the malicious node.

There are three phases of the CBDS method.

1. Bait phase
2. Reverse tracing phase
3. Reactive defence phase

3.2.1 Bait phase:

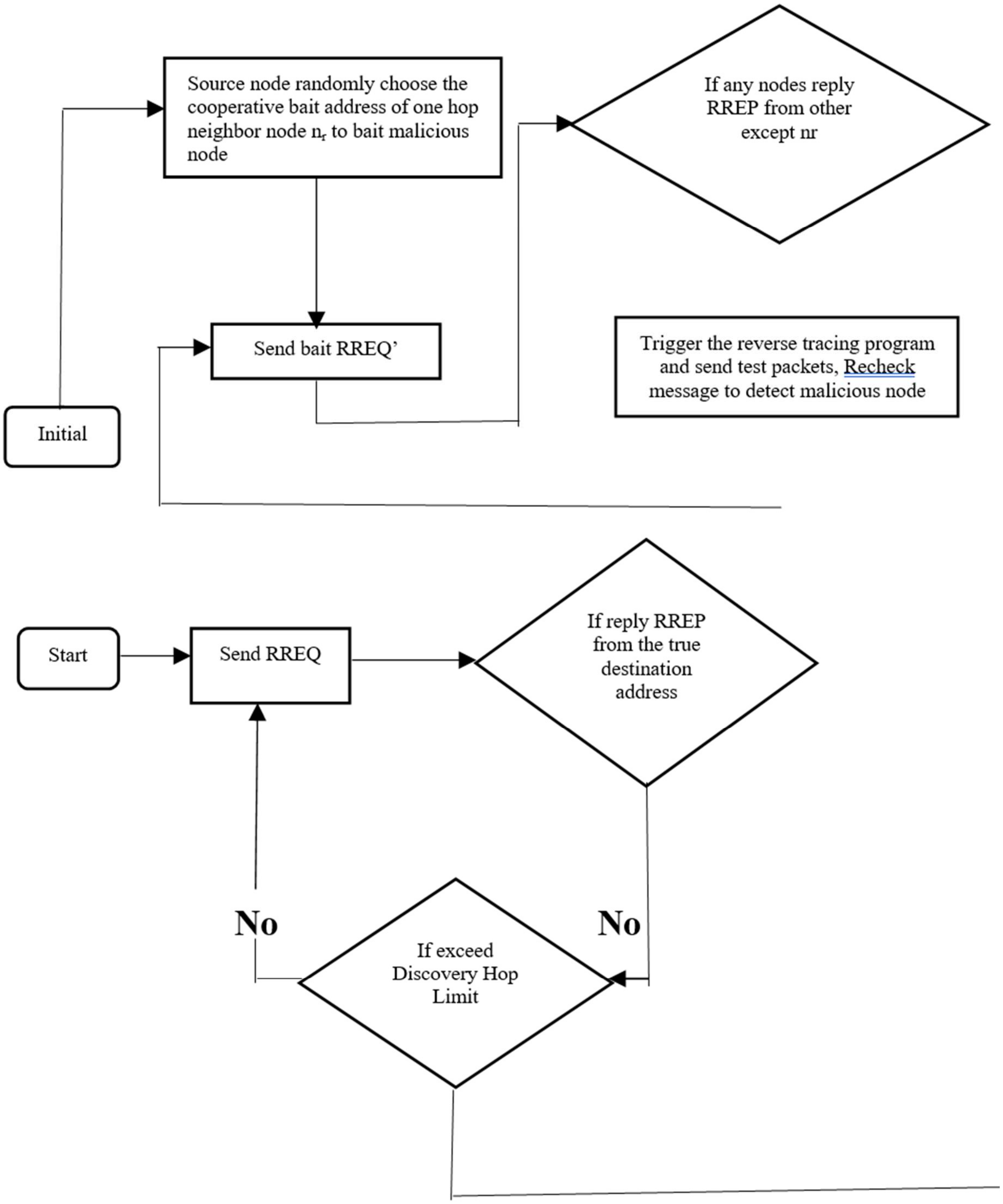
In this phase the malicious node sends a RREP when we send it the bait RREQ'. This is accomplished by creating the address of the address of the target RREQ' which is the address of a randomly chosen neighbor node within a source hop-node. The bait phases begins when the bait RREQ' is used for initial routing and waiting for a reply.

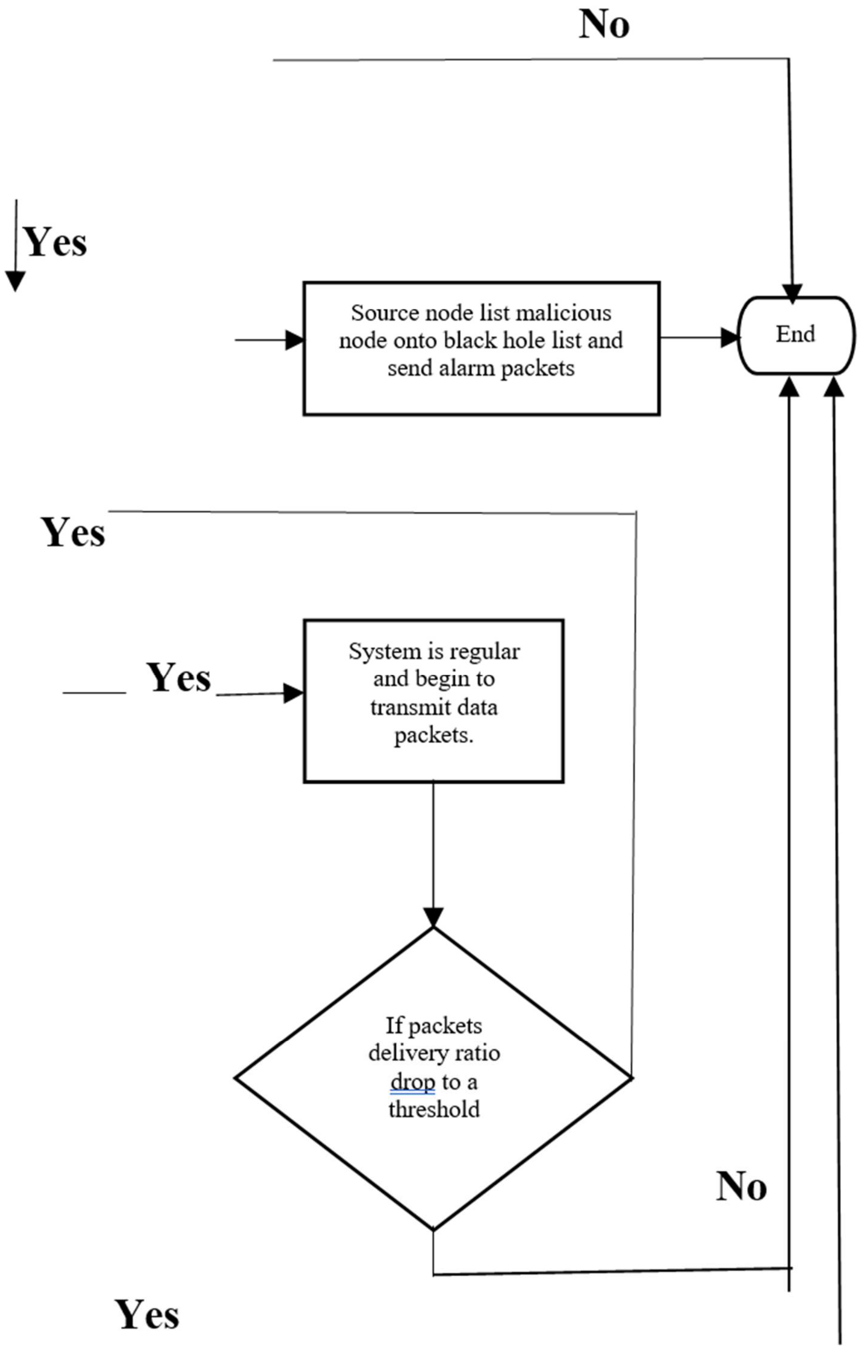
3.2.2 Reverse tracing phase:

The purpose of this step is to find out the exact location of the malicious node. When RREQ' is received by a malicious node, if will reply with a forged false RREP. After that using that false answer we can detect the malicious node. After detection, we have to generate, lists for worthy node and malicious node. For ex:-

If my network has n nodes i.e. n1, n2…………..nn. in these node Nm and Nm+1 are detected as malicious node then we have these list:-

List 1: N1, N2……….Nm-1 (worthy node)………..... (1)
List 2: Nm, Nm+1 (malicious node ……………….... (2)
List 3: Nm+2……….Nn (worthy node)…………….. (3)


Source node randomly choose the cooperative bait address of one hop neighbor node n_r to bait malicious node
If any nodes reply RREP from other except nr
Send bait RREQ'
Trigger the reverse tracing program and send test packets, Recheck message to detect malicious node
Initial
Start
Send RREQ
If reply RREP from the true destination address
No
No
If exceed Discovery Hop Limit


No
Yes
Source node list malicious node onto black hole list and send alarm packets
End
Yes
Yes
System is regular and begin to transmit data packets.
If packets delivery ratio drop to a threshold
No
Yes

Algorithms for Dynamic Source Routing (DSR)

Step 1: Start from source node N1 and broadcast the information about it to its neighbors i.e. in this case the route information is‟<1>″, because of its one-to-one link between node N1 and N2.

Step 2: Broadcast previous route information to neighbors of node N2 i.e. to node N3, N4, N5. The new route will remain same‟<1, 2>″ in all the cases.

Step 3: Take node N3 and broadcast previous route (<1, 2>) to next neighboring nodes i.e. node N6. New route till node N6 will be‟<1, 2, 3>″ and same process can be done for other nodes i.e. node N4 and N5.

Step 4: Further, broadcast the new routes i.e. < 1, 2, 3, 6 >, < 1, 2, 4 >, < 1, 2, 5 > to nodes N8, N7 & N9 respectively.

Step 5: Repeat the above steps until destination node is reached via all the routes.

Algorithms for Co-operative Bait Detection Scheme (CBDS)

Algorithms 1: CBDS

```
Step 1: Source node start sending RREQ packets for route discovery
Step 2: if source received route reply within time, it means destination node is true destination, and then start forwarding data to it.
Step 3: else if current time is greater than discovery time threshold value, then current time is stored into T1
Step 4: else start resending the RREQ packets, measuring another threshold value of time in T2.
Step 5: computer the current communication PDR performance
 PDR = no _ received/no _ sent;
Step 6: set threshold = 0.9;
Step 7: if (PDR < threshold), sending bait RREQ
Step 8: update dynamic threshold value
Step 9: if (T2<T1), then
If (threshold < 0.95), the
Threshold = threshold + 0.01;
Else
If (threshold > 0.85), then
Threshold = threshold – 0.01;
Step 10: if (Time < 800), then
Return threshold;
Else
Threshold = 0.9;
Step 11: Stop
```

Algorithms 2: Disjoint Path Communication

```
Step 1: Find all available disjoint paths from source to sink through routing protocols.
Step 2: Consider hop count of all nodes from sink.
Step 3: Source node calculates its upstream nodes (say n) and keep only one path from each node towards destination.
Step 4: Calculate New Source Initiated Bulged Reporting Rate by dividing current RR by neighboring nodes of source and then assign new RR to each path.
Step 5: If received packets is
i.      From higher Hop count node and
ii.     From the path of which the current node is member then accept and forward the packet.
```

Step 6: Else drop the packet.
Step 7: Repeat step 5 and 6 till packet reaches the destination.

4. RESULT AND DISCUSSION:

In our work; we are using dynamic source routing protocol (DSR) with co-operative bait detection scheme (CBDS). The reason of using DSR algorithm is that; this algorithm is able to configure path in runtime mode. Our proposed algorithm detects black hole attacks with the help of bait route request and maintains an array for malicious node in reverse tracing steps. After malicious node detection our actual communication is started by eliminating malicious nodes from the communicating path.

For implementation of our proposed algorithm, we are using network simulation tool of version 2.35 which includes network animation 1.15. All these setups are installed on UBUNTU 14.04. Our simulation contains 6 nodes. Node 0 is source node and node 5 is destination node. Our communication starts at time 0 with bait route request. Initially, we have to design a path which contains no any malicious node. For doing so (detecting malicious node) we start bait route request procedure. After the completion of bait route procedure, we found that node 1 is malicious. Hence node 1 is removed from our communication path. For actual communication; CBDS algorithm helps for designing desired path. The path contains four node including source and destination node i.e. node 0, node 5 node 2 and node 3. Node 2 takes the place of malicious node 1 form completion of communication path.

Simulation Parameters:

Parameter	**Size**
Simulator Version	NS 2.35
Number of Node	6
Type of Traffic	CBR
Interface Que length (iql)	6
Size of Packet	512byte
Max Speed	20m/second
Channel data Rate	11mbps
Simulation time	400s

Table 1: Parameters used for simulation

A simulation is performed on NS2 which is shown below:

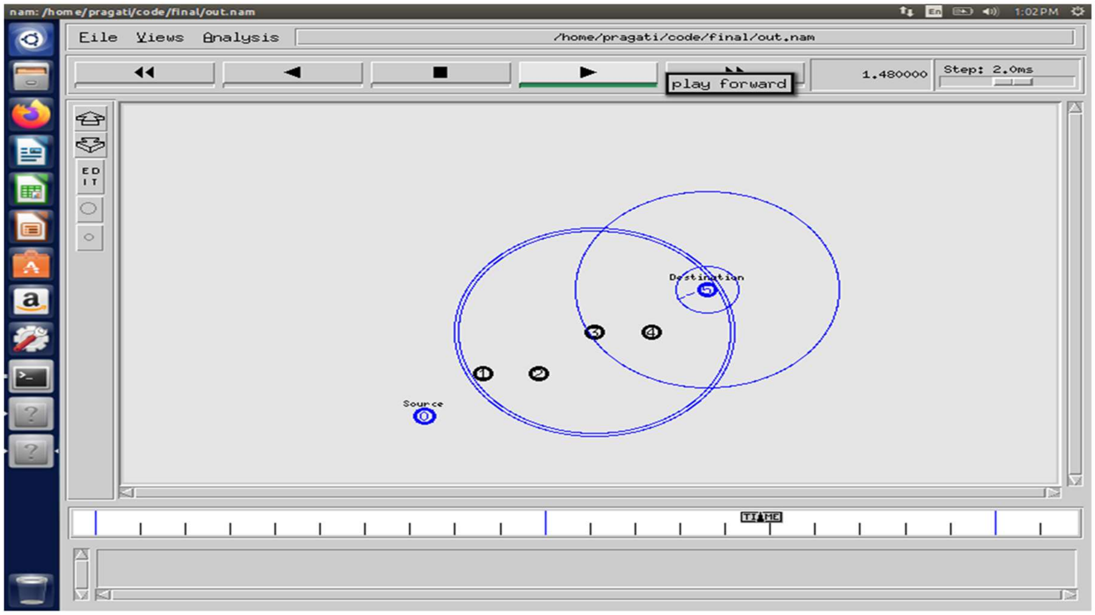


Figure 4. Initial stage of network

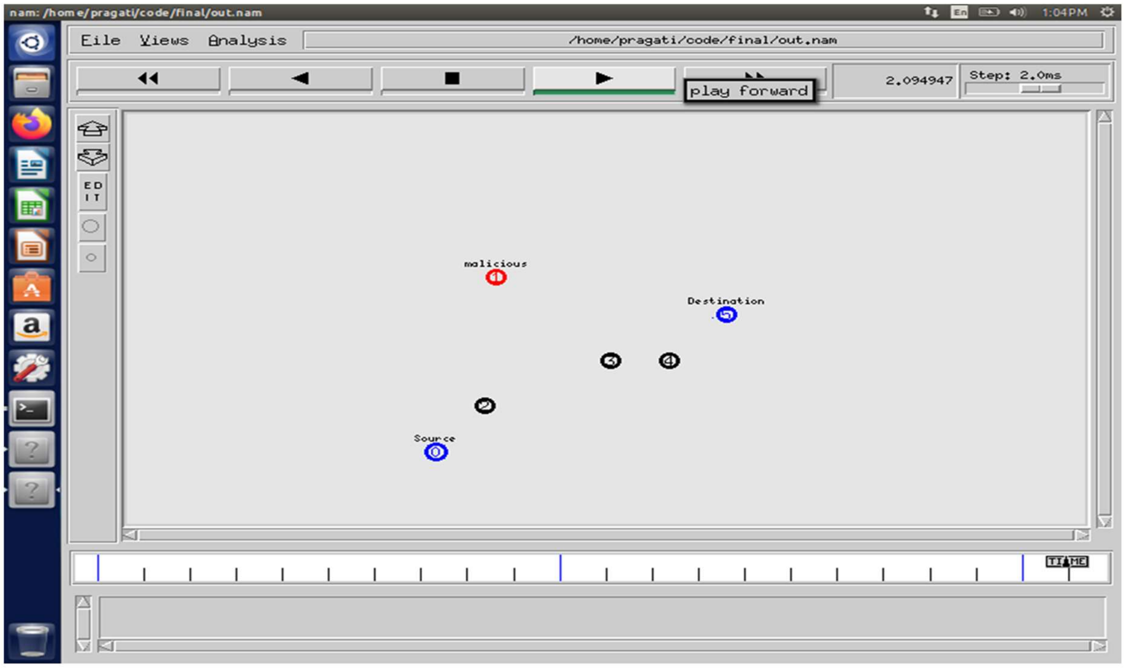


Figure 5. Malicious node Detection and Communication

DSR protocol drops packets due to presence of black-hole attack in MANET. The diagram above shows an indicating that the source cannot communicate with the destination node.

Figures 4 and 5 show that while the DSR protocol is more vulnerable to attacks, the CBDS scheme is much stronger, able to prevent and detect attacks within the network. In CBDS, CBDS using the proposed AODV scheme uses the AODV routing protocol and CBDS using DSR uses the DSR routing protocol. Simulation results show that CBDS with AODV is more efficient than CBDS with DSR.

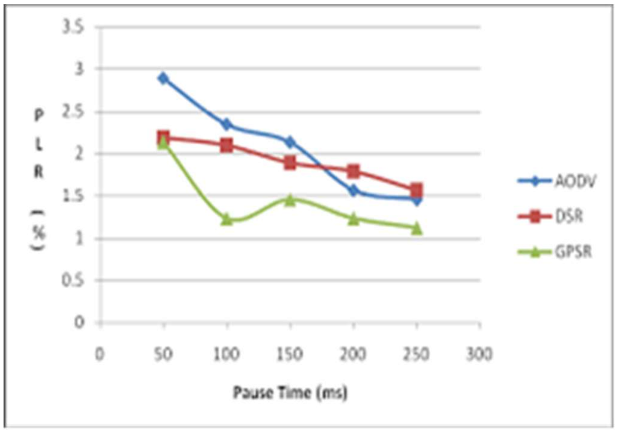


Fig. 6: Packet Lost Ratio

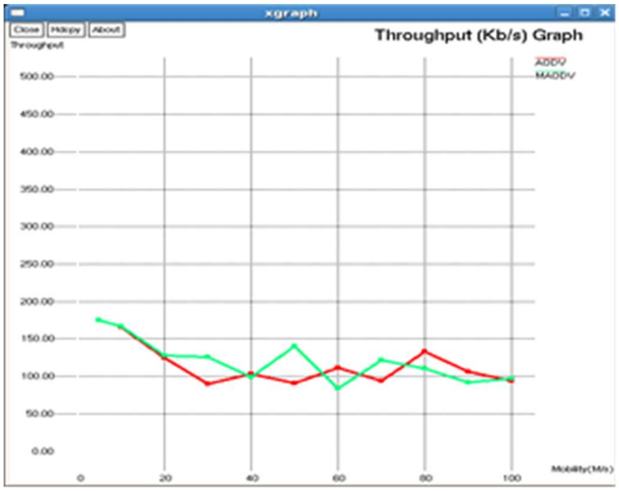


Fig. 7: Throughput of proposed algorithm

5. CONCLUSION:

MANET security is a major challenge, and research work on is at an early level. Routing protocols are vulnerable to joint black-hole attacks in MANET. In this article, we used the CBDS (Cooperative Bait Detection System) approach. CBDS uses proactive defense and reactive defense architecture to detect malicious nodes launching joint black-hole attacks, modified CBDS using AODV protocol. We propose a scheme to detect a lower routing overhead called CBDS using AODV. Simulation results show that CBDS with DSR is more effective than the DSR protocol in terms of throughput and packet delivery rate, and CBDS with AODV outperforms CBDS with DSR. In this paper, we have proposed a new mechanism called proposed cooperative bait detection scheme (PCBDS) for detecting malicious nodes in MANET under black hole attacks, and this detection method employs detection technique.

REFERENCE

[1] G. Singh and N. Bhagat, “Removal of selective Black hole attack in Dynamic Source Routing (DSR) Protocol by alarm system,” no. 6, pp. 129–131, 2015.

[2] O. I. Khalaf, F. Ajesh, A. A. Hamad, G. N. Nguyen, and D. N. Le, “Efficient dual-cooperative bait detection scheme for collaborative attackers on mobile ad-hoc networks,” IEEE Access, vol. 8, pp. 227962–227969, 2020, doi: 10.1109/ACCESS.2020.3045004.

[3] P. R. Dumne and A. Manjaramkar, “Cooperative bait detection scheme to prevent collaborative blackhole or grayhole attacks by malicious nodes in MANETs,” 2016 5th Int. Conf. Reliab. Infocom Technol. Optim. ICRITO 2016 Trends Futur. Dir., pp. 486–490, 2016, doi: 10.1109/ICRITO.2016.7785004.

[4] J. M. Chang, P. C. Tsou, H. C. Chao, and J. L. Chen, “CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture,” 2011 2nd Int. Conf. Wirel. Commun. Veh. Technol. Inf. Theory Aerosp. Electron. Syst. Technol. Wirel. VITAE 2011, pp. 1–5, 2011, doi: 10.1109/WIRELESSVITAE.2011.5940839.

[5] A. U. Khan, R. Puree, B. K. Mohanta, and S. Chedup, “Detection and prevention of blackhole attack in AODV of MANET,” 2021 IEEE Int. IOT, Electron. Mechatronics Conf. IEMTRONICS 2021 - Proc., pp. 1–7, 2021, doi: 10.1109/IEMTRONICS52119.2021.9422643.

[6] I. Woungang, S. K. Dhurandher, R. D. Peddi, and M. S. Obaidat, “Detecting blackhole attacks on DSR-based mobile ad hoc networks,” IEEE CITS 2012 - 2012 Int. Conf. Comput. Inf. Telecommun. Syst., pp. 2–6, 2012, doi: 10.1109/CITS.2012.6220364.

[7] P. Emimajuliet and V. Thirilogasundari, “Defending collaborative attacks in MANETs using Modified Cooperative Bait Detection Scheme,” 2016 Int. Conf. Inf. Commun. Embed. Syst. ICICES 2016, no. Icices, pp. 1–6, 2016, doi: 10.1109/ICICES.2016.7518906.

[8] K. S. Patel and J. S. Shah, “Detection and avoidance of malicious node in MANET,” IEEE Int. Conf. Comput. Commun. Control. IC4 2015, 2016, doi: 10.1109/IC4.2015.7375729.

[9] R. M. Sujatha, “A novel Approach to avoid malicious attack to enhance network in WSN,” pp. 1686–1690, 2016.

[10] Gurbir Singh and Nitin Bhagar, "Removal of selective Blackhole attack in dynamic source routing (DSR) protocol by alarm system" pp. 129-131, IJTER, 2015.

[11] L.Baghel et.al., "Detection of blackhole attack in mobile ad hoc network using adaptive approach," pp.626-630, ICECA, 2017.

[12] J.M chang et.al., "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," pp. IEEE 2014.

[13] S. K. Prasad, J. Rachna, O. I. Khalaf, and D-N, "Map matching algorithm: Real time location tracking for smart security application," Telecommun, Radio Eng., pp. 1189-1203, 2020.

[14] A. Puran and S.T. Imeci,"Design and analysis of compact dual resonance patch antenna," Heritage Sustain . develop., pp. 38-45, Jun.2020

[15] M. L. Thivagar, M. A. Ahmed, V. Ramesh, and A. A. Hamad, "Impact of non-linear electronic circuits and switch of chaotic dynamics," Periodicals Eng. Natural Sci., pp. 2070-2091, 2020.

[16] L. M. Thivagar, A. A. Hamad, and S.G. Ahmed, "Conforming dynamics in the metric spaces," J. Inf. Sci.Eng., pp. 279-291, 2020.

[17] O. I. Khalaf, G. M. Abdulsahib. H. D. Kasmaei. and K. A. Ogudo, "A new algorithm on application of blockchain technology in live stream video transmission and telecommunication," Inf. J. e-collaboration, pp. 16-32, Jan.2020.

[18] O. I. Khalaf, G. M. Abdulsahib, and B. M. Sabbar. "Optimization of wireless sensor network converage using the bee algorithm," J. Inf. Sci., pp.377-386, 2020.

[19] R. Sheokand and M. Gupta, "Detection and Prevention of Black-Hole attacks in MANETS," IJCSMC, May 2019, pp. 239-251.

[20] M. S. Pathan, J. He, N. Z. A. Zardari, M. Q. Memon, and A. Azmat, "An Efficient Scheme for Detection and prevention of black-Hole Attacks in Aodv-based manets,"IJACSA, 2019, PP. 243-251.

[21] A. Yasim and . Abu Zant, "Detecting and Isolating Black-Hole Attacks in MANET using Timer Based Baited Technique, "Wireless Communication and Mobile Computing, Wiley. 2018, pp. 1-10.

[22] T. Delkesh and M. A. Jamali, "FAODV: detection and removal of multiple black hole atttacks through forged packets in MANETs," Springer, 2018, pp. 1897-1914.

[23] K. Juneja, "Random-Session and K-Neighbour Based Suspected Node Analysis Approach for Cooperative Black-hole Detection in MANET," Springer, 2019, pp.45-68.