International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Secured Routing Protocol for Mobile Ad hoc Networks to Defend Collaborative Black-hole and Gray-hole Attacks by Malicious Nodes

Madugundu Neelakantappa [1]* **Amjan Shaik [2]**

[1]*Department of Information Technology,*
B.V.Raju Institute of Technology, Narsapur, Medak, Telangana State, India
[2]*Department of Computer Science & Engineering,*
B.V.Raju Institute of Technology, Narsapur, Medak, Telangana State, India
* Corresponding author's Email: m.neelakanta@gmail.com

Abstract: Mobile Ad hoc Network (MANET) is a ubiquitous, infrastructure less and self-containing wireless network. In this networks nodes that are in mobility forms a temporary network without any infrastructure. In MANETs every node acts as host as well as router and therefore communication can be established on need basis without use of any fixed network equipment. But in presence of malicious nodes, this network leads to major security concerns as these nodes may disrupt the process of routing. In this scenario, detecting or preventing malevolent nodes, launching collaborative gray-hole or black-hole attacks is a major challenge. In this paper, a new secured routing protocol referred to as "Malicious Node Detection by Collaborative Bait (MNDCB)". This protocol can be regarded as hybrid protocol as it poses the advantage of both reactive and proactive defending architectures. This MNDCB protocol is defined with a reverse tracking method to detect the malicious nodes and there by defending their collaborative attacks. Simultaneous results proves that in the presence of malevolent node attacks, the MNDCB gives better performance over their best counter parts base DSR, 2-ACK and best effort fault tolerant (BFTR) routing protocols in-terms of performance metrics: packet-delivery-ratio, throughput and routing overhead.

Keywords: Black-hole, Gray-hole attacks, Malicious nodes, MANET security, Proactive and reactive defend architecture.

1. Introduction

As mobile devices are widely available, Mobile Ad hoc Networks (MANETs) [1, 2] have been widely used in variety of applications like military operations, disaster recovery and commercial applications. Infrastructure less property is to the primary cause for its wide-spread applications. In MANETs every node will act as a host as well as a router. Due to absence of base stations, every node need to forward the packets of other nodes their by forming a wireless Local Area Network [2]. But, these features invite serious threats to the network in terms of security. These applications impose certain rigid constraints on the security of the routing, data traffic and network topology. For example, the existence of malevolent nodes and their collaboration may lead to disrupt the routing process, which intern leads to mal-functioning of the network operations.

Extensive research work has been carried out on the MANETs security. Much of this work is focused on dealing with detection and prevention approaches to face individual malicious nodes. In this context, these techniques can't be effective when dealing with multiple malicious nodes working together initiating a collaborative attack. In these cases, more devasting domains may result to the network.

The dynamic topology added with infrastructure-less feature of ad hoc networks will make them highly vulnerable to attacks on routing like black-hole and gray-hole. As shown in Fig. 1, in black-hole attack, a malicious node transmits a falsie broadest informing that, it contains short path

Received: March 15, 2018

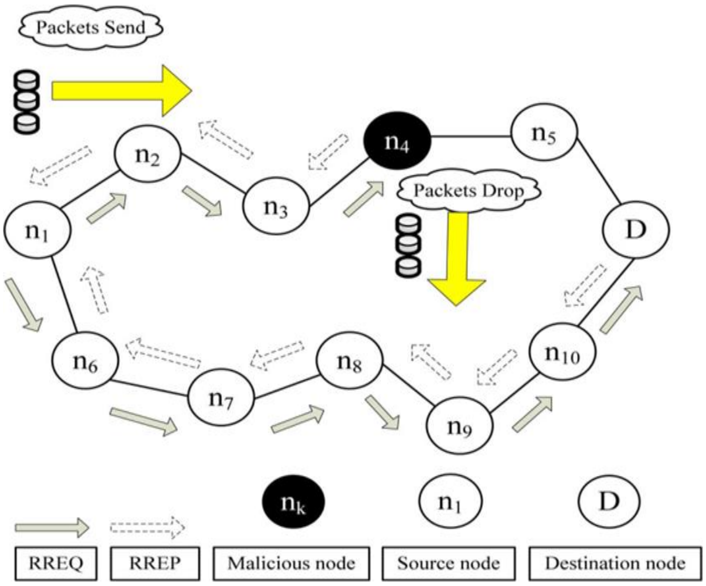

Figure. 1 Black-hole attack-dropping packets by node n_4

to the destination-node, with goal of misguide the messages. In this attack, a black-hole node (called as malicious node) gets most of the packets of the network, by claiming "fake" shortest-route to its destination and discards all these packets without considering them to forward towards destination. In gray-hole attack, the malevolent node cannot be detected as such since it selectively discards every packet. In this paper, we focus on identifying & combining gray-hole and collaborative black-hole attack using a Dynamic Source Routing (DSR) [2] based routing method.

DSR contains two main steps: route-discovery & route-maintenance. During route-discovery phase, source-node broadcasts a route-request (R-REQ) packet throughout the network. If any intermediate-node has router to destination in its cache, it will send route reply (R-REP) packet back to the source-node. Otherwise, R-REQ packet is forwarded to the adjacent-node after adding its address into the R-REQ packet in route-record field. When destination receives R-REQ packet, it notices the complete path from source node through its record-route field. The destination-node uses this collects route information to send R-REP reply back to the source-node. Even though DSR doesn't have any route detection technique, source node gets all route information though R-REP message. In this paper, we make use of this approach.

Our proposed protocol, "Malicious Node Detection by Collaborative Bait (MNDCB); a technique is devised which effectively detects the malicious-nodes which attempt to launch collaborative black-hole or gray-hole attack. In this method, the address of neighbor node is used to bait, the malicious node to send R-REP message using a reverse tracing of the route technique, malevolent nodes will be detected. Every detected malevolent node is stored in black-hole list in order to caution all other nodes not to send their packets through these listed nodes. In contrast to existing work, our MNDCB protocol integrates both pro-active and re-active defend architecture to perform its function.

In the reminder of this paper, Section 2 illustrates various methods discovered to defend Black hole and Gray hole attacks, Section 3 describes the mechanism and operation of our MNDCB protocol, the performance evaluation with experimental results along with comparison to existing approaches is specified in Section 4 and Conclusion along with future plans for modifications is summarized in Section 5.

2. Related work

In existing literature, most of the research work has been contributed in detecting malicious nodes in ad hoc networks. Majority of these solutions handles the problem of detecting a single malevolent node or they need huge resources in-terms of cost and time to detect collaborative black-hole attacks [8]. Moreover, some of these techniques need specific environments [8] or presumptions for their functioning. The malicious node detection techniques can be divided broadly into 2 groups.

1. Pro-active detection techniques [3, 4] need to continuously detect and monitor near-by nodes. In this technique, due to continuous monitoring, overhead will be high resulting wastage of resources irrespective of existence of malevolent nodes. But the major advantage of these type of techniques

is that it can prevent attack at initial stage, preventing the damage to the network.

2. Re-active detection technique [9], acts only when the destination node identifies a significant reduction in packet-delivery-ratio.

The most basic prior work for our mechanism is illustrated in the paper [7] by I.J.Jenifhar Jolla and R.Dhanalakshmi. According to their BPRT protocol, there are two important phases that are carried out to detect and prevent the gray-hole attacks in MANET. Initially in the baiting process, the source node broadcasts the bait request RREQ' to attract the malicious gray-hole nodes to reply and thereby the reverse tracing mechanism is started to detect and prevent the gray-hole nodes in the network. Finally, the alarm packets are sent by the source node to all other nodes in the network and prevent the blacklisted malicious nodes from communicating with the legitimate nodes. The whole process is incorporated with the Dynamic Source Routing (DSR) protocol and holds the features of proactive defence architecture.

Among the other techniques, 2-ACK scheme [3] and BFTR scheme [8] can be considered for compare the performance. In 2-ACK scheme [3] proposed by Liu, 2-hop acknowledgement packets will be sent in the reverse direction of the routing path for indicating data-packet were successfully received.

For controlling the number of data packets received for which acknowledgement is needed, a parameter, acknowledgement ratio (Rack) is used. This technique is proactive scheme and therefore causes additional routing over-head irrespective of existence of malevolent node. In their proposal [8], Nahr Stedt and Xne introduced best effort tolerant router (BFTR). This BFTR protocol applies end to end acknowledgments for monitoring the destination selected routing path which is measured using metrics packet-delivery-ratio and time-delay.

In case of routing-path deviates from a predefined threshold behavior set to determine good-routes, the source-node will lose a new route. The major disadvantage of BFTR is, malevolent nodes can still exist in newly selected routes and this technique leads to repeated discovery of routes which intern adds to routing overhead. Our proposal detection technique takes benefit of features of both re-active as well as pro-active schemes in designing the DSR based routing protocol capable of detecting gray-hole and collaborative black-hole attacks in ad hoc networks.

3. Proposed method

Our proposal is referred as “Malicious Node Detection by Collaborative Bait” (MNDCB), detects and prevents malevolent node launching gray-hole or collaborate black-hole attacks in ad hoc networks. In this method, the source-node intensively chooses neighbor role as the collaborate node. This nodes address is used as bait destination-address for baiting malevolent nodes for sending R-REP reply messages, malevolent nodes will be trapped and can be deleted and presented to participate in network routing operations by applying a reverse tracing method. In this scheme, the presumption is that whenever significant drop in packet-delaying-ratio occurs, an alert is sent back to the source-node by destination-node to initiate the mechanism again. This MNDCB method integrates the advantage of pro-active detection at initial step with the superiority of re-active responds in subsequent steps and timely reduces the wastage of resources.

As our MNDCB is DSR-based protocol [2], once the R-REP message received, source-node can find addresses of all intermediate nodes in the chosen routing path from source to destination. But, the source-node will not be able to find which of these intermediate-nodes has route to destination-node or which are R-REP reply messages or which are malevolent node forged R-REP reply message. This case will result in trapping of source node as it sends packets through the fake shortest-path sent by malevolent node, leading to the black-hole attack.

For resolving the problem, the HELLO message feature [14] is applied to MNDCB through which every node can identify its neighbor nodes reachable within hop. This functionality aids in delivering the bait address to trap the malevolent nodes and to apply reverse tracing technique of MNDCB for detecting the exact address of malevolent nodes.

The R-REQ packets for baity [16] will be similar in format as that of original R-REQ packets with exception of bait address being set as their destination address. This modified format of packets is depicted in Table 1.

Our MNDCB protocol functions in 3 steps:

1. The initial baiting-step
2. The reverse tracing-step
3. The shift to reactive define-step, which is the basic DSK route-discovery-phase.

Among these, the initial 2 steps are proactive defensive steps and the last step is a reactive defensive step.

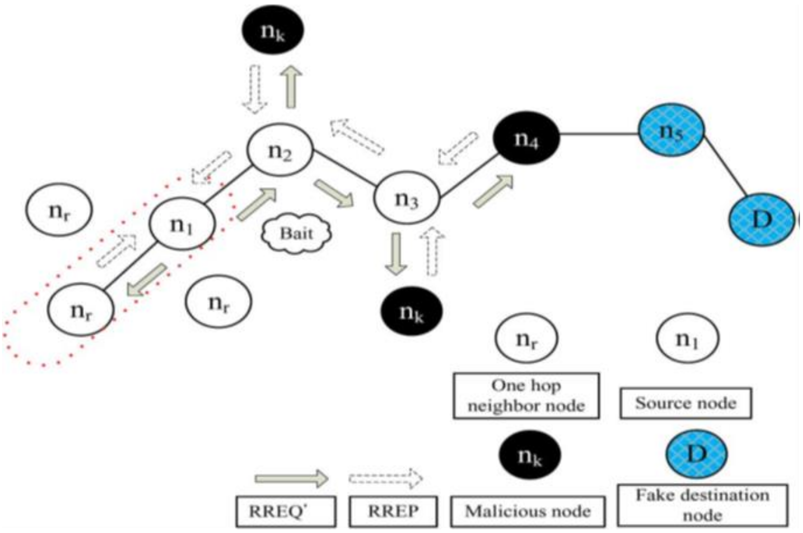

Figure. 2 Random selection of cooperative bait address

Table 1. R-REQ packet Format

Option Type	Opt Data Length	Request ID
Target Address (R-REQ^1) : Bait Address		
Address[1]		
Address[2]		
Address[3]		
......		
Address[n]		

i) Initial baiting step:

The main function of the baiting step is to make malevolent-node to send a R-REP reply message by sending the baited R-REQ' packet. The malevolent node claims as if, it has a shortest path to that target node, so that it can detain the packets which were sent thorough it. To accomplish this, the following method is used for generating destination-address for R-REQ' bait packet.

Initially the source-node randomly chooses neighbor node **n_b**, which is within its i-hop distance and collaborates with this node by making its address as destination-address for R-REQ' bait. As every bait steps is done randomly, the collaborate neighbor node will change (node may be moved beyond 1-hop from source-node) and hence the bait address will not remain same. As shown in Fig. 2, baiting step is activated whenever the R-REQ' bait is send prior to seek the route path. The analysis of baiting-phase follow-up process is illustrated below. If the n_r node had not initiated a block-hole attack, when in reply to source node R-REQ^1 message, there will be other nodes R-REP reply message along with that of the n_b node. This will clearly shows the existence of malevolent nodes as illustrated in Fig. 2. Hence, the reverse trace process in next-step will be activated in-order to detect them route-path. In case, if R-REP reply message had received only from **n_b** node, it indicates there were no malevolent nodes exist in the network and MNBCD protocol has initial the route-discovery program of DSR [2].

On the other hand, if **n_r** is a malevolent node of black-hole attack, then after source-node had sent R-REQ' other nodes (along with **n_r** node) would have also transmit reply R-REP messages. It is the indication or existence of malevolent nodes in the reply route-path. In such cases, the next-step of reverse tracing process will be activated to detect this route. In case if **n_r** deliberately avoids sending R-REP reply message then it will be directly placed in the black-hole list by the source-node. If R-REP reply is received only from **n_r** node, it indicates that there were no malevolent nodes in the network, except on the route-path that **n_r** node had sent. In such case, the basic DSR route-discovery step [2] will be initiated. The route provided by **n_r** node, will not be considered for route-discovery process.

ii) The Reverse Tracing Process

As illustrated in [7], by I.J.Jenipher Jolla and R.Dhanalakhmi, the reverse tracing process is applied for detecting the behavior of malevolent nodes by making use of route-reply to R-REQ' message.

In case of a malevolent node has received R-REQ' message, it will respond with a false reply R-REP message. In accordance to it, the reverse tracing process will be applied for those nodes who received R-REP messages, with an intention for deducing the dubious-path information and

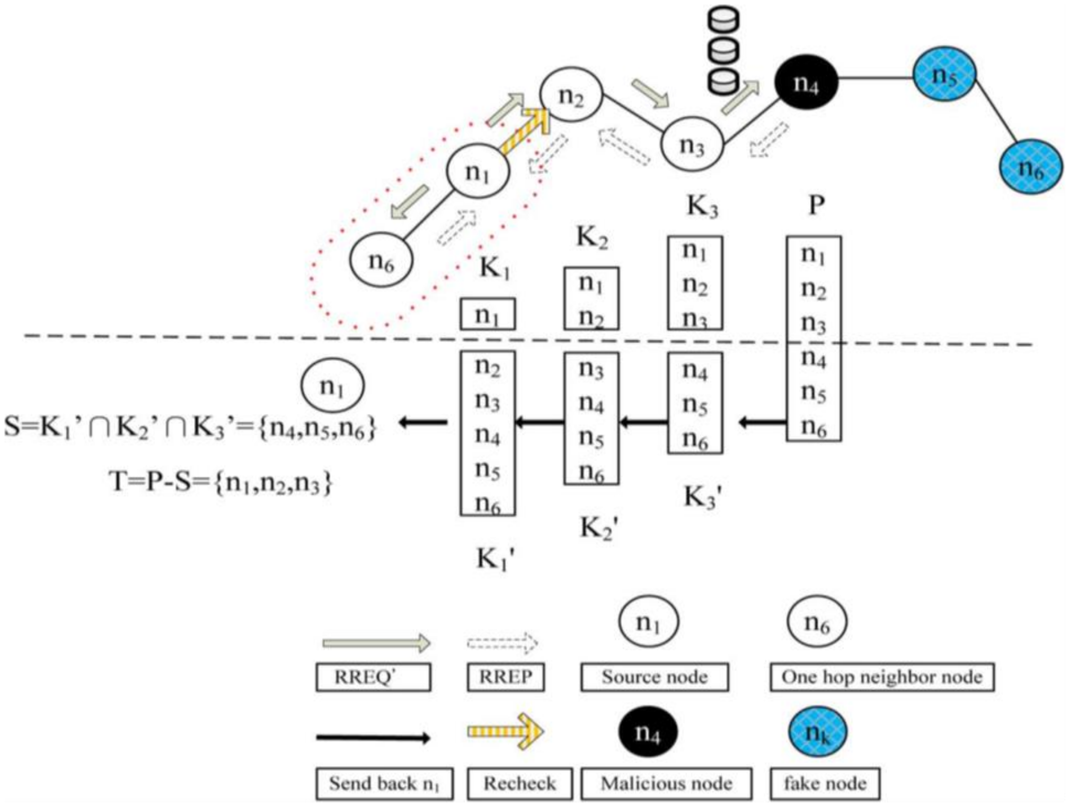

Figure. 3 CBDS approach-reverse tracing process

temporarily trusted-zone in the route-path. It is clear that, MNDCB protocol can detect multiple malevolent nodes simultaneously, when these nodes responds with R-REP messages.

For instance, when a malevolent node n_m sends a false R-REP message, an address-list L= {n_1, n_2, n_3,...n_k....n_m.....n_b} is stored in the R-REP message. If n_k node receives the R-REP message, it separates the L-List by destination address n_1 of R-REP message in IP-field and obtains address-list L_k= {n_1, n_2, n_3,..., n_k} in which L_k refers to the route-path from source-node n1 to the destination node n_k. Afterwards, n_k node will find the difference between the address-list L= {n_1-n_2-n_3-...n_k....n_m.....n_b} stored in R-REP message and L_k= {n_1, n_2, n_3,..., n_k}.

Hence we obtain

$$L_k^1 = L\text{-}L_k = \{n_{k+1}, n_{k+2}, n_{k+3}, ...n_m.....n_b\} \quad (1)$$

Here L_k^1 refers to the route-path information to the destination-node n_b from n_{k+1} ,which is a node after n_k.

The resulted route L_k^1 is recorded in R-REP "reserved field", which is sent back to the source-node. This node receives R-REP message and the address-list L_k^1 of the nodes, which received R-REP message. For avoiding interference of malevolent nodes in-order to ensure that the list L_k^1 doesn't received from malevolent nodes, when a nk node receives R-REP message, it will compares:

i) A, the source- address recorded in IP-field of R-REP
ii) B, the next-hop node n_k in the list

$$L = \{n_1\text{-}n_2\text{-}n_3\text{-}...n_k....n_m.....n_b\}$$

iii) C, one-hop node of n_k

From the above, if A is not equals to B & C, then the received list L_k^1 will perform a forward-back. Else, n_k should forward-back the list L_k which was generated through it-self.

In Fig. 3, even-though n_4 node can respond with L_4^1={n_5,n_6}, n_3 will verify and it removes L_4^1 after receiving the R-REP message. When the source-node gets intersection-set of L_k^1, the dubious-path information S replied from malevolent nodes will be detected.

$$S = L_1^1 \cap L_2^1 \cap L_3^1 \cap ....L_k^1 \quad (2)$$

As every malevolent node replies R-REP message to each R-REQ message, nodes which exist in the route before this process happened were assumed to be trust worthy. The set-difference of sets L & S is computed for getting temporary trusted list T as,

$$T = L - S \quad (3)$$

For conforming that the malevolent node exists in set S, the source-node transmits text messages through this route and will transmit re-check packet to second-node towards the last-node i the set T. This needs that, the node would be in a promiscuous-mode for listening to which node the last-node in se T had transmitted the messages to and sends back the result to the source-node. Now, the source-node will record this node's address in a black-hole-list. Also it broadcasts the alert messages all through the network, informing other nodes to withdraw their operation performing to this node. In case if last node had dropped messages instead of diverting them, the soure-node will record it in blackhole-list.

The malevolent node scenario [12] is shown in Fig. 3. In this scenario, the route contains a malevolent node n4 and the source-node n_1 presents to transmit a message-packet to the destination-node n6. When source-node n1 broadcasts R-REQ packet, the node n4 responds with a fake R-REP packet, with an address-list L= $\{n_1,n_2,n_3,n_4,n_5,n_6\}$. In this list, n_5 is a random-node field by node n4. When the node n_3 receives the reply packet R-REP sent by n_4, it separates the L-list by the destination-address n1 of R-REP in IP field and obtains address-list $K_3=\{n_1,n_2,n_3\}$. By performing the set difference process between address lists L and K3 to get $K_3^1=P-K_3 =\{n_4,n_5,n_6\}$ and node n3 replies with K_3^1 and R-REP to the source-node n1 in accordance with route information in the list L. Similarly nodes n2 and n1 perform same operation when they receive R-REP; to get $K_2^1=\{n_3, n_4,n_5,n_6\}$ and $K_1^1=\{n_2,n_3, n_4,n_5,n_6\}$. These lists will be send back to the source-node for intersection operation. The suspicious-path information of malicious-node is derived by the intersection operation as follows.

$$S= K_1^1 \cap K_2^1 \cap K_3^1 = \{n_4,n_5,n_6\} \quad (4)$$

To obtain a temporary trusted set, the source-node computes

$$T = L\text{-}S = \{n_1,n_2,n_3\} \quad (5)$$

Finally, source-node n_1 will transmits testing packets to the nodes on this path for rechecking the message n_2, requesting for entering into the promiscuous-mode, and listen to n_3. With this listening mode, it identifies that n_3 might divert packets to the malevolent node n_4. Therefore n_2 will sends this listening result back to the source-node n_1, which in-turn records n_4 into the blackhole-list.

Table 2. Dynamic-threshold algorithm

```
float threshld=0.9;
IntialProactveDefnse();
float Dynmic(threshld)
{    float t1,t2;
t1=compute the reqd-time of PDR down-to-threshld;
if(PDR<threshld)
IntialProactveDefnse();
t2=compute the reqd-time of PDR down-to-threshld;
if(t2<t1) {
if(threshld<0.95)
threshld=threshld+0.01;
}
else{
if(threshld>0.85)
threshld=threshld-0.01;
}
if(Simulation-time <900)
{
return(threshld);
Dynmic(threshld);
else return 0.9;
}
```

As illustrated in Fig. 3, in case of having single malevolent node n4 in the route, with response fake R-REP and address-list L= {n1,n2,n3,n4,n5,n6}, then this node had intentionally chosen a fake node n5 in R-REP address-list for interfering in follow up action of the source-node n1. But this source-node will intersect this received Kk1 for obtaining S= K11∩ K21∩ K31 = {n4,n5,n6} and T = L-S = {n1,n2,n3}and so it requests its neighbor node n2 for listening mode, the packets which were diverted by n3 to n5 should have been transmitted to n4. The source-node will records this node in the black-hole list. It is clear that, even in case of malevolent node co-operated with a fake R-REP, it would be still identified by our MNDCB protocol. As shown in Fig. 3, if n5 & n4 were malevolent nodes, the list T would contain T = L-S = {n1,n2,n3} and n2 had requested for listening to which, n3 might send packets. In case n5 or n4 would have been detected for which co-operation might be stopped. Therefore remaining nodes will be baited and detected. The Fig. 2 shows that, even for more malevolent nodes in the ad hoc network, our MNDCB would still succeeds in detecting them simultaneously after receiving their reply R-REP.

iii) Shifting to Reactive Defense Step

After the execution of above two steps of initial pro-active defense, the basic DSR route-discovery operation [22] is initiated. After route establishment, if the packet-delivery-ratio (PDR) observed to be

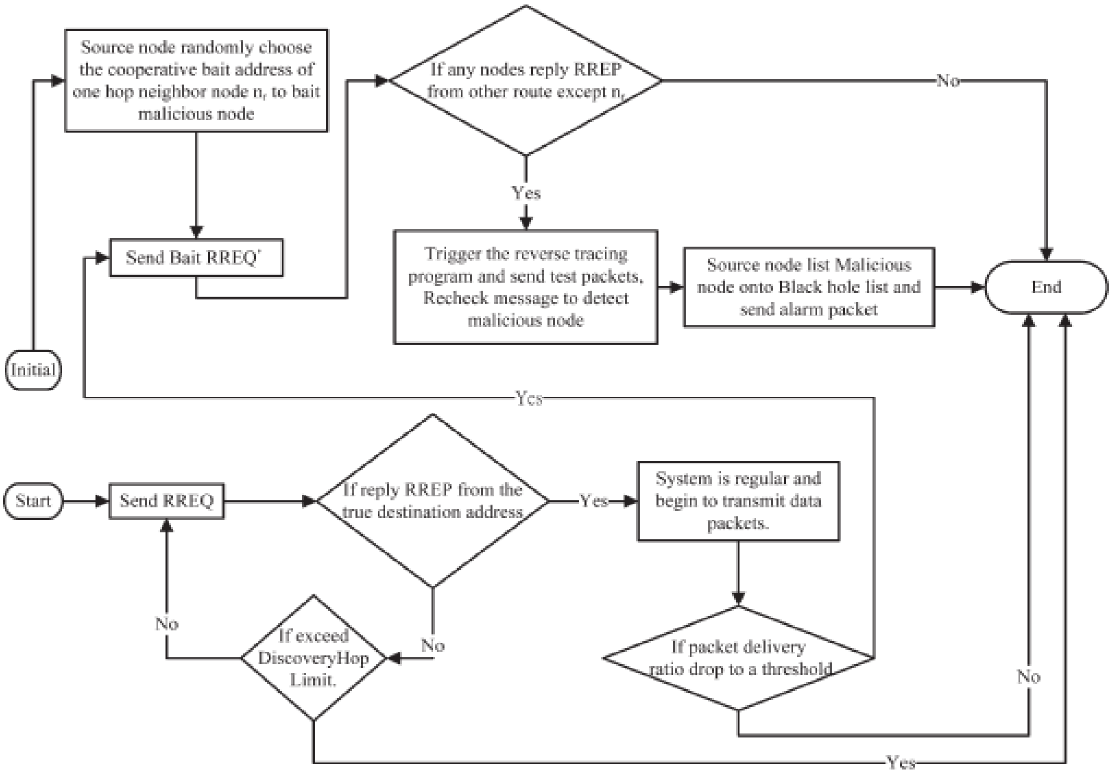
Source node randomly choose the cooperative bait address of one hop neighbor node n_r to bait malicious node
If any nodes reply RREP from other route except n_r
No
Yes
Send Bait RREQ'
Trigger the reverse tracing program and send test packets, Recheck message to detect malicious node
Source node list Malicious node onto Black hole list and send alarm packet
End
Initial
Yes
Start
Send RREQ
If reply RREP from the true destination address
Yes
System is regular and begin to transmit data packets.
No
If exceed DiscoveryHop Limit.
No
If packet delivery ratio drop to a threshold
No
Yes

Figure. 4 Operation of MNDCB protocol

falling below threshold value, then the detection process is applied again for detecting, which enables continuous maintenance and reactive real time efficiency. The threshold range will be varying 85% and 95% which can be adjusted in accordance to the efficiency of the current network. Initially, the threshold value can be set to 90%.

For this operation, a dynamic threshold-algorithm is designed as shown in Table-II, which is controlling the time when the PDR falls below the threshold. In case of obtaining short descending time, it indicates that malevolent nodes are still exists in the network. In such cases, the threshold- value of PDR can be adjusted to higher value. Otherwise, the PDR threshold can be reduced.

The flow of operation of our MNDCB algorithm is illustrated in Fig. 4. This algorithm enables to get the uncertain path information of malevolent nodes along with that of true nodes. Hence it can find the trusted-zone by observing the replies of malicious nodes. Also, our MNDCB protocol has ability to observe whether a malevolent-node drops the packet or not. It results in the disregarding the fraction of dropped packets, by which a gray-hole attack launched by malevolent nodes would be detected, similar to the detection of launching black-hole attacks.

4. Performance evaluation

The QualNet Simulator [10] is used for studying performance of our MNDCB protocol. In our simulation environment, IEEE 802.11 MAC is used with channel data-rate of 10 Mb/s. The default threshold of MNDCB is set to 90%. Malicious nodes are selected randomly to perform attacks and their ratio is varied from 0 to 30%. Simulation is performed in 700 x 700 m^2 area with transmission rate 4 packets/sec. Other simulation parameters are shown in Table 3.

Table 3. Simulation parameters

S.No.	Parameter	Value
1	Radio range	250 mtrs
2	Application traffic	10 CBR
3	Transmission rate	4 pkts/sec
4	Packet size	512 bytes
5	Channel data rate	10 Mbps
6	Pause time	0 sec
7	Maximum speed	20 mtrs/sec
8	Number of nodes	50
9	Simulation time	900 sec
10	Simulation area	700 x 700 m^2
11	Malicious nodes	0% to 40 % in steps of 5%
12	Threshold	Dynamic threshold

ii) Performance Metrics:

In the evaluation through experimental analysis, we compared our MNDCB protocol against the basic- DSR[2], and also other recent protocol BPRT[7], in-terms of performance metrics [10][11], packet-delivery-ratio, routing-overhead, end-to-end delay and throughput as defined below in all cases existence of percentage of malicious nodes.

a) **Packet-Delivery-Ratio(PDR):** It is the ratio between number of packets received at the destination-node and number of packets sent by the source-node. For each of the n number of applications traffic, packets delivered (Pd_i) and packets received (Pr_i) is collected and average PDR can be calculated as

$$PDR = \frac{1}{n}\sum_{i=1}^{n}\frac{Pdi}{Pri} \qquad (6)$$

b) **Routing-overhead:** It refers to the ratio between routing related number of control packets transmitted and data packets transmitted. Similar to the above notation, the average routing-overhead can be calculated as

$$RO = \frac{1}{n}\sum_{i=1}^{n}\frac{Cpkti}{Pri} \qquad (7)$$

c) **Average End-to-End Delay:** It defines the average time taken by a packet to reach destination-node from source-node. If the total delay of packets received by the destination is d_i and packets received is pkt_i for i^{th} application traffic, then average end to end delay is given by

$$ED = \frac{1}{n}\sum_{i=1}^{n}\frac{di}{pkti} \qquad (8)$$

d) **Throughput:** It indicates the ratio of total data amount received at destination (b_i) to total time taken to receive all packets (t_i). Average throughput is calculated as

$$T = \frac{1}{n}\sum_{i=1}^{n}\frac{bi}{ti} \qquad (9)$$

Simulation scenario is created by varying the number of malevolent nodes (percentage) by fixing the mobility to a fixed value. In this scenario, the effect of different threshold values of MNDCB protocol is evaluated based on above mentioned performance parameters.

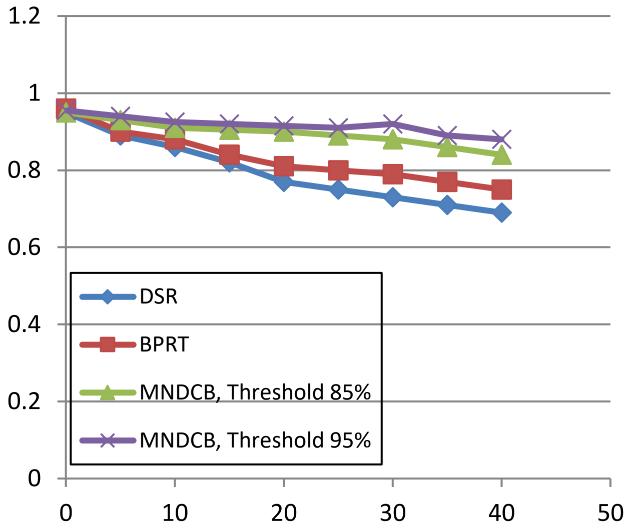

Figure. 5 Comparison of PDR vs. % of malicious nodes

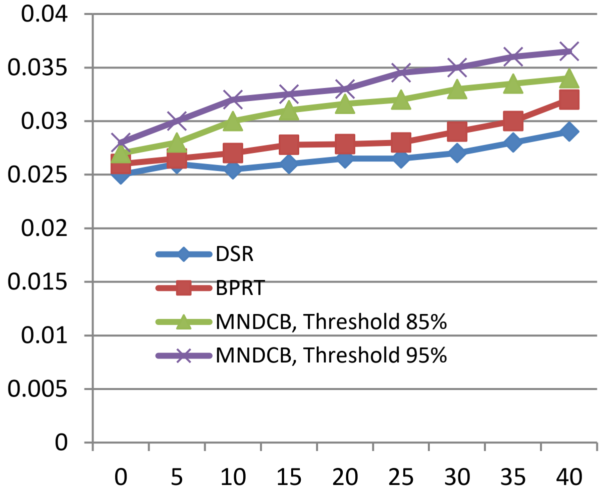

Figure.6 Comparison of routing overhead vs. % of malicious nodes

At first, PDR of MNDCB is compared with that of basic DSR [2] and BPRT protocols [7], at different thresholds by varying percentage of malevolent nodes between 0% and 40%. As shown in Fig. 5, it is observed that, as percentage of malevolent nodes increases, DSR suffers drastically by black-hole attacks. Our MNDCB protocol achieves higher PDR compared with basic-DSR, even at higher percentage of malicious nodes (40%). The PDR is higher when using 95% threshold compared to 85% threshold, due to early detection of malevolent nodes in the first case.

Second, we evaluate routing-overhead of MNDCB and basic-DSR for different thresholds. As illustrated in Figure-6, it is observed that DSR [2] and BPRT [7] protocol results in lower routing-overhead compared to MNDCB protocol due to fact that they have no defensive mechanism internally.

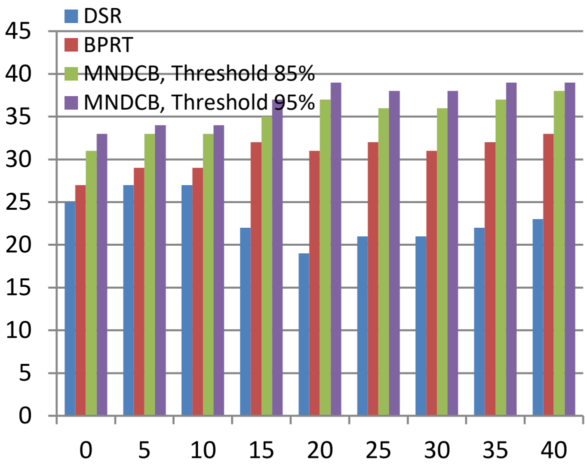

Figure. 7 Comparison of end delay (msec) vs. % of malicious nodes

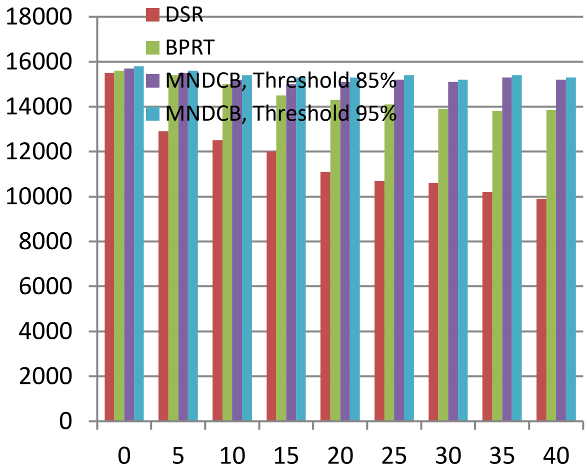

Figure. 8 Comparison of throughput (bits/s) vs. % of malicious nodes

It is evident that MNCBD has highest routing-overhead at 95% threshold as detection process triggers fast at higher threshold values.

In Fig. 7, end-to-end delay comparison is shown for MNDCB, basic-DSR [2] and BPRT [7] protocol. It is evident from this result that, our protocol exhibits a little higher delay compared to basic-DSR and BPRT protocol due to its internal process of detection. Hence a trade-off can be made between PDR and delay. As our MNDCB protocol detects presence of any number of malicious nodes simultaneously, delay will not be increased much with increase in percentage of malicious nodes.

Finally, we studied throughput for MNDCB, DSR and BPRT protocols for various thresholds. As shown in Figure-8, throughput for DSR drastically reduced with increase in percentage of malevolent nodes. Our protocol incurs higher throughputs at all threshold values and in all cases of percentage of malicious nodes, due to high success rate of packet delivery.

5. Conclusion

The main research direction here, we presented in this paper is that, to handle the common problem of attacks in mobile ad hoc network. In this paper, we proposed a novel approach for detecting malevolent nodes in mobile ad hoc networks to defend collaborative black-hole or gray-hole attacks named as “Malicious Node Detection by Collaborative Bait (MNDCB)”. It can be a hybrid protocol, poses the advantage of both reactive and proactive defending architectures and is defined with a reverse tracking method to detect the malicious nodes there by defending their collaborative attacks. The simulation outcomes proves that our MNDCB protocol gives much better performance when compared to basic DSR[2] and also other recent protocol BPRT[7], in-terms of, packet-delivery-ratio and routing-overhead in all cases existence of percentage of malicious nodes. This indicates huge growth and scientifically scope, to do research in networking to detect attacks.

In future research work, there is an intended scope to work for (a) Modifying MNDCB scheme to defend other type of collaboration attacks on ad hoc networks and for (b) Investigating integration of MNDCB with other proven security protocols to construct comprehensive secured framework for protecting MANETs against all threats.

Acknowledgments

We would like express our gratitude to all the authors in the reference list for making this research paper in an optimistic way.

References

[1] Y.C. Hu, A. Perrig, and D. B. Johnson, “Wormhole attacks in wireless networks,” *IEEE Journal on Selected Areas of Communication*, Vol. 24, No. 2, pp. 370–380, 2006.

[2] D. Johnson and D. Maltz, “Dynamic source routing in ad hoc wireless networks”, *IEEE Journal on Mobile computing*, pp. 153–181, 1996.

[3] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehavior in MANETs”, *IEEE Transactions on Mobile Computing*, Vol.6, No.5, pp. 536–550, 2007.

[4] H. Deng, W. Li, and D. P. Agrawal, “Routing security in wireless ad hoc networks”, *IEEE Commun. Magazine*, Vol. 40, No. 10, pp. 70–75, 2002.

[5] S.M. Shivamallaiah and K. Karibasappa, “An Efficient Detection of BH Attack with Secured Routing Using ACO and DualRSA in MANETs”, *International Journal of Intelligent Engineering and Systems*, Vol.11, No.2, pp. 246-255, 2018.

[6] R. Adimalla, V. ValliKumari, and C. S. Reddy, “Genetic algorithm based Backup Route Establishment for QoS Routing”, *International Journal of Intelligent Engineering and Systems*, Vol.10, No.3, pp. 38-46, 2017.

[7] I. J. J. Jolla and R. Dhanalakshmi, “Mitigation of Gray hole Attacks in MANET using Baiting Process and Reverse Tracing*”, Global Journal For Research Analysis*, Vol. 4, No. 5, pp. 11-14, 2015.

[8] K. Nahrstedit and Y. Xue, “Providing fault-tolerent ad hoc routing service in adversarial environments”, *Journal of Wireless Personnel Communication*, Vol.29, pp 367-388, 2004.

[9] W. Wang, B. Bhargava, and M. Linderman, “Defending against collaborative packet drop attacks on MANETs”, In: *Proc. of 28th IEEE Int. Conf. on Symp. Reliable Distrib. Syst.*, 2009.

[10] QualNet Simulaton Tool, Scalable Network Technologies. (Last retrieved March 18, 2013). *[Online]. Available: http://www.qualnet.com*

[11] The Network Simulator-ns-2. *[Online]. Available*: *http://www.isi.edu/nsnam/ns/. [Accessed: 31-Dec- 2014]*.

[12] M.Y. Su, “Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems”, *IEEE Trans. on Computer Communications.*, Vol. 34, No. 1, pp. 107–117, 2011.

[13] T. Poongodi and M. Karthikeyan, “Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks”, *IEEE Trans. on Wireless Personal Communications.*, Vol. 90, No. 2, pp. 1039–1050, 2016.

[14] S. Djahel, F. Nait-Abdesselam, and A. Khokhar, “An acknowledgment- based scheme to defend against cooperative black hole attacks in optimized link state routing protocol”, *In Proc. of IEEE Int. Conf. Communications*, pp. 2780–2785, 2008.

[15] M. S. Khan, Q. K. Jadoon, and M. I. Khan, “A comparative performance analysis of MANET routing protocols under security attacks”, In: *Proc. of Mobile Wireless Technol.*, pp. 137–145, 2015.

[16] J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao, and C. F. Lai, “Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach”, *IEEE Journal of Systems*, Vol. 9, No. 1, pp. 65–75, 2015.

[17] R. H. Jhaveri and N. M. Patel, “A sequence number based bait detection scheme to thwart grayhole attack in mobile Ad Hoc networks”, *IEEE Journal of Wireless Networks*, Vol. 21, No. 8, pp. 2781–2798, 2015.

[18] A. D. Patel and K. Chawda, “Dual Security Against Gray-hole Attack in MANETs”, In: *Proc. of Springer Conference*, pp. 33–37, 2015.

[19] H. Weerasinghe and H. Fu, “Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation”, In: *Proc. of IEEE ICC*, pp. 362–367, 2007.

[20] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, and J. Tolle, “Detecting black hole attacks in tactical MANETs using topology graphs”, In: *Proc. of 32nd IEEE Conf. on Local Computer Netwetworks*, pp. 1043–1052, 2007.

[21] W. Yu, Y. Sun, and K. J. R. Liu, “HADOF: Defense against routing disruptions in mobile ad hoc networks”, In: *Proc. of the 24th Annual Joint Conf. IEEE Computer and Communication*, Vol. 2, pp. 1252– 1261, 2005.

[22] W. Wang, B, Bhargava, and M. Linderman, “Defending against collaborative packet drop attacks on MANETs”, In: *Proc.of 2nd International Workshop on Dependable Network Computing and Mobile Systems*, 2009.

[23] S. Ramaswamy, M. Sreekantaradhya, K. E. Nygard, H. Fu, and J. Dixon, “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”, In: *Proc. of International Conference on Wireless Networks*, 2003.

[24] M. Mohanapriya and I. Krishnamurthi, “Modified DSR protocol for detection and removal of selective black hole attack in MANET”, *Journal of Computers & Electrical Engg*, Vol.40 No.2, 530–538, 2014.

[25] J.-M. Chang, P.-C. Tsou, H.-C. Chao, and, J.-L. Ming, “CBDS: a Cooperative Bait Detection Scheme to prevent malicious node for MANET based on hybrid defense architecture”, In: *Proc. of the 2nd IEEE International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology*, 2011.

[26] W. Kozma and L. Lazos, "REAct: resource-efficient accountability for node mis-behavior in ad hoc networks based on random audits", In: *Proc. of IEEE Int. Conf. on WiSec*, pp. 103–110, 2009.