International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

Defending Malicious Nodes against Collaborative Black-Hole and Gray-Hole Attacks in Mobile Ad Hoc Networks

Dr. Madugundu Neelakantappa[1], Dr. Amjan Shaik[2]

[1]Associate Professor of Information Technology, B.V.Raju Institute of Technology, Narsapur, Telangana State, India
[2]Professor of Computer Science & Engineering, B.V.Raju Institute of Technology, Narsapur, Telangana State, India

---

Abstract: *Mobile Ad hoc Network (MANET) is an infrastructure-less self-containing and ubiquitous wireless network. In MANETs, mobile nodes forms an ad hoc network without any physical infrastructure. In these networks, each node plays a role of host and a router as well and hence communication will be established on demand without need of any fixed equipment of network. This network faces major security concern, in case of presence of malicious node, as these nodes can distracts the routing process. In this context, the major challenge is the detection and prevention of malicious nodes, launching collaborative gray-hole or black-hole attacks. In this paper, a novel secured routing protocol known as "Malevolent Node Detection Protocol by Collaborative Bait (MNDPCB)". This technique acts as hybrid protocol as it have the advantages of defending architectures of both reactive and proactive. This MNDPCB protocol is processed with a reverse tracking technique for detecting the malevolent nodes and there by defend their attacks of collaborative nature. Simulation results demonstrates that in the presence of malicious node attacks, the MNDPCB provides better performance when compared with 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: MANET, *Black hole attack, Gray hole attack, malevolent nodes, MANET security, proactive and reactive defend architecture*

1. INTRODUCTION

Due to wide availability of mobile devices, Mobile Ad hoc Networks MANETs [1][2] have been extensively used in large set of applications like disaster-recovery, military-operations and commercial applications. The major cause for its wide spread applications is its Infrastructure less nature. In MANETs, each node will play a role of a host and a router as well. In absence of base-stations, each node requires to forward the other nodes packets, resulting the formation of wireless network on ad hoc basis [1]. However, this nature invite serious security threats to the network, in presence of malicious nodes. The ad hoc network applications will apply specific rigid constraints on the routing security, data-traffic and topology of the network. For instance, the presence of malicious nodes and their collaboration will lead to disturb the process of routing, which results in mal functioning of all the defined operations of the network.

In the recent past, elaborative research has been carried out on the security of the MANETs. This research work mainly focused on techniques for defending the malicious node attacks by detection and prevention approaches to face individual malicious nodes. In this scenario, these methods have no use in dealing collaborative attacks posed by multiple malevolent nodes working together. In these situations, more disaster may result to the network, resulting the failure in its functioning of the application.

The infrastructure less feature along with the dynamic topology of MANET will makes it highly vulnerable to attacks on routing process such as black-hole and gray-hole. In Figure-1, black-hole attack scenario is illustrated. A malevolent node broadcasts a false packet, which have the shorter path to the destination-node, with the intention of misguide the source nodes. With this approach, a black-hole node, known as malicious (malevolent) node can get majority of the packets to route, by claiming "fake" shortest-path to its destination. All these received packets will be discarded, avoiding the forwarding the packets towards the destination. As a variation for this technique, to avoid the detection of malevolent node, it selectively discards the packets rather than discarding every packet. In this paper, we mainly concentrate on the process of identification and combating gray-hole and collaborative black-hole attacks using a basic-Dynamic Source Routing (DSR) routing protocol.

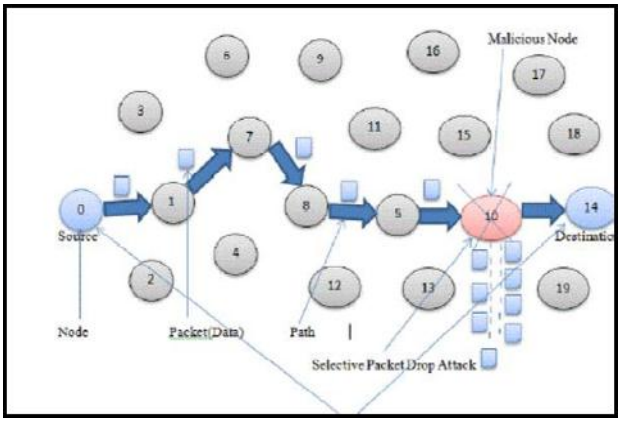

Fig-1: Black-hole attack-dropping packets by node 10

DSR [2] contains two major steps: 1) route-discovery process and 2) route-maintenance process. During route-discovery process, source-node broadcasts a packet of route-request (R-REQT) across the network. Upon receipt of this R-REQT packet, every node checks its cache for a route to the destination. If it find the route, route reply (R-REPY) packet will be sent back to the source-node. If it not finds a route in its cache, it adds IP-address onto the R-REQT packet in route-record field and forwards to the adjacent-node. In this way, the R-REQT packet will reach to the destination-node. When the destination-node receives the R-REQT packet, it finds the complete route-path from source-node in its record-route field. The destination-node sends reply (R-REPY) packet back to the source-node along with the discovered route. Although DSR didn't have any separate route-detection method, source-node will get all the route information though R-REPY message. In this paper, we make use of this approach.

In our novel protocol, MNDPCB; a method is applied which effectively detects the malevolent-nodes which tries to launch collaborative black-hole attack or gray-hole attack. In this proposed technique, the address of neighbor-node will be used to bait, the malevolent-node to send R-REPY message using a reverse trace of the routing method, there by detecting the malicious nodes. Each detected malicious node will be stored in black-hole-list. By frequent broadcast of this list, all other nodes can be cautioned, not to transmit heir packets along these listed nodes. In contrast to existing techniques, to perform its function our MNDPCB protocol will integrate both pro-active and re-active defend architectures.

2. RELATED WORK

In each attack prevention technique, "Security parameters" are important metrics in a MANET. Without using these parameters, security approach will be useless [7]. The Reference [11] proposes a malevolent node detection scheme (MNDCB) for preventing cooperative black-hole attacks; the scheme applies detection and defense techniques for removing intruders with the consideration of both normal and abnormal functionalities. Mainly, the fake R-REPY parameters, like destination sequence-number, hop-count, destination IP-address and time-stamp, will be considered for identification of attacks. The MNDCB protocol will improves the packet delivery ratio by 80%–90%. In this technique, source-node takes decisions on un-safe routes, thereby avoids any additional overhead during routing process. In another method [12], a novel protocol is proposed to secure the routing process of DSR protocol to mitigate black-hole attacks; the DSR R-REPY format is changed for generating a plain-packet during the destination reply to source-node through reverse-path nodes. If this packet is received, then that node will be considered as normal node; else, the node is categorized as malevolent node [11]. These protocols need monitoring of the temporal and spatial nature of MANETs. The performance of the MANET in terms of security of the networks should be monitored at frequent intervals. For validating the performance of the method, elaborative set of experiments were done in the proposal [11]. But, this protocol have a threat of exposing to further attacks during exhaustive data-transmission cycles. In the proposed protocol [11], defending protocol is designed and demonstrated the MNDCB approach, which is based on DSR. The simulation outcomes indicate that CBDS protocol outperforms the basic DSR, BFTR, and 2-ACK techniques. MNDCB provides higher packet delivery ratio than base DSR, BFTR and 2ACK at the cost of little high overhead. MNDCB protocol also presents higher throughput when compared to the DSR in simulations. However, the 2-ACK policy will provides the highest routing overhead in comparison to DSR, MNDCB and BFTR, irrespective of the percentage of malicious nodes present in the network. The authors demonstrated MNDCB protocol is an efficient technique in terms of packet delivery ratio and routing overhead and PDR. However, in this paper, simulations cases were considered only by varying the percentage of malicious nodes, without

considering the mobility. The speed of the node plays a vital role in the performance of the network, especially in the presence of the malicious nodes. This paper focus on the performance of the protocol with varying node speed. Figure 2 shows the random selection of a cooperative bait address.

3. PROPOSED METHOD

Our proposal is referred as "Malevolent Node Detection Protocol by Collaborative Bait" (MNDPCB), 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 MNDPCB 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 MNDPCB is DSR-based protocol, once the R-REPY 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. Also it cannot detect which of R-REPY reply messages are malevolent node forged R-REP reply messages. 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 is applied to MNDPCB 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 MNDPCB for detecting the exact address of malevolent nodes.

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

Table-1: R-REQT packet Format

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

Our MNDPCB protocol functions in 3 steps:

i) The initial baiting-step

ii) The reverse tracing-step

iii) The shift to reactive define-step, which is the base- DSR route-discovery-phase.

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

3.1 Initial Baiting Step:

The main function of the baiting step is to make malevolent-node to send a R-REPY reply message by sending the baited R-REQT 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-REQT bait packet.

Initially the source-node randomly chooses neighbor node $\mathbf{n_b}$, which is within its i-hop distance and collaborates with this node by making its address as destination-address for R-REQT 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 Figure-2, baiting step is activated whenever the R-REQT bait is send prior to seek the route path. The analysis of baiting-phase follow-up process is illustrated below.

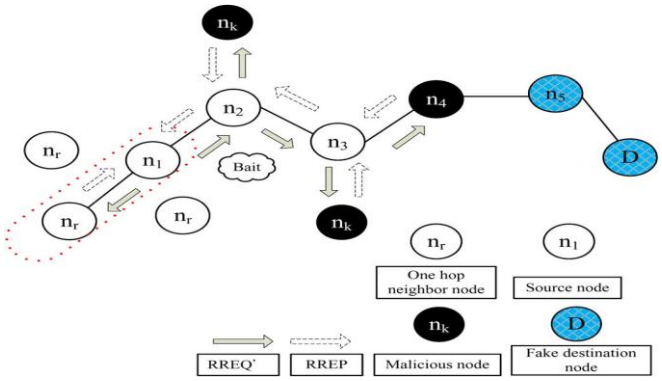

Fig-2: Random selection of cooperative bait address

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 Figure-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 $\mathbf{n_b}$ node, it indicates there were no malevolent nodes exist in the network and MNBCD protocol has initial the route-discovery program of DSR.

On the other hand, if $\mathbf{n_r}$ is a malevolent node of black-hole attack, then after source-node had sent R-REQ' other nodes (along with $\mathbf{n_r}$ node) would have also transmit reply R-REPY 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 $\mathbf{n_r}$ 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 $\mathbf{n_r}$ node, it indicates that there were no malevolent nodes in the network, except on the route-path that $\mathbf{n_r}$ node had sent. In such case, the basic DSR route-discovery step will be initiated. The route provided by n_r node, will not be considered for route-discovery process.

3.2 The Reverse Tracing Process

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-REQT 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-REPY messages, with an intention for deducing the dubious-path information and temporarily trusted-zone in the route-path. It is clear that, MNDPCB protocol can detect multiple malevolent nodes simultaneously, when these nodes responds with R-REPY 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= $\{n_1\text{-}n_2\text{-}n_3\text{-}...n_k....n_m.....n_b\}$stored in R-REP message and L_k= $\{n_1,n_2,n_3,...n_k\}$.

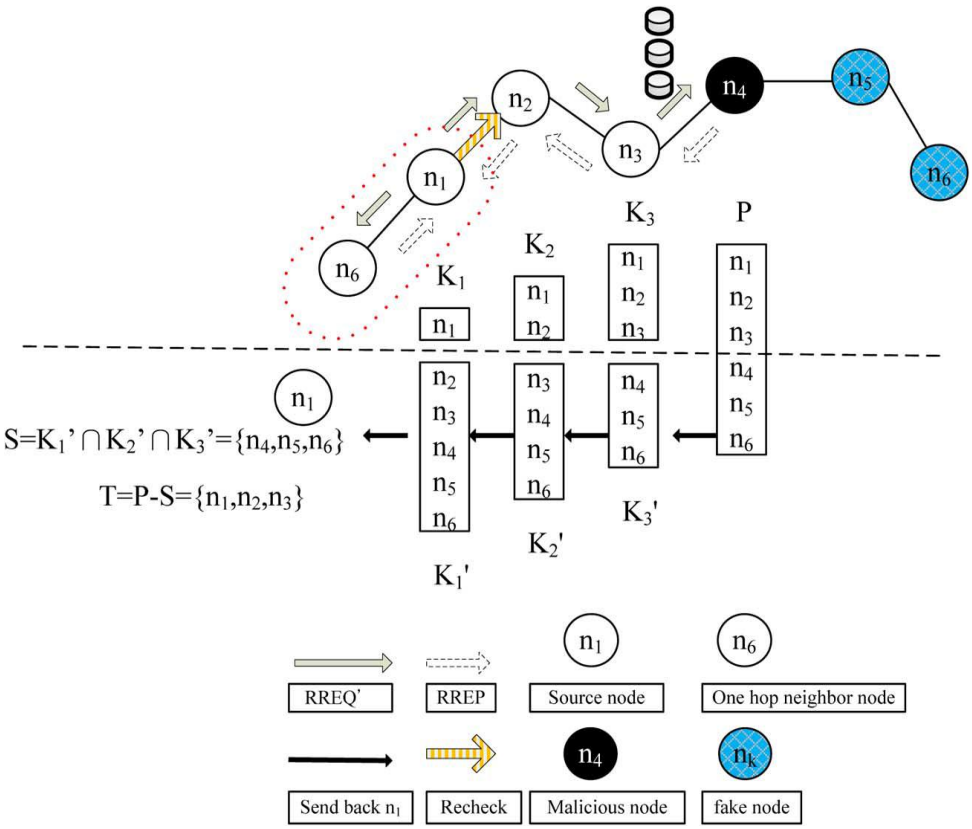

Fig-3: CBDS approach-reverse tracing process

Hence we obtain

$L_k^1 = L - L_k = \{n_{k+1}, n_{k+2}, n_{k+3}, \ldots\ldots n_m \ldots\ldots n_b\}$ ------>(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
$L = \{n_1\text{-}n_2\text{-}n_3\text{-}\ldots n_k \ldots n_m \ldots\ldots n_b\}$
iii) C, one-hop node of n 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 the Figure-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.

$S = L_1^1 \cap L_2^1 \cap L_3^1 \cap \ldots\ldots\ldots L_k^1$ ---->(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,

$T = L - S$ ---->(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 is shown in Figure 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.

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

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

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

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.

```
float Threshold-Value=0.90;
Initial-Proactive-Defense();
float Dynamic(Threshold-Value)
{    float t1,t2
t1=compute the required-time of PDR down-to-
Threshold-Value;
if(PDR<Threshold-Value)
Initial-Proactive-Defense();
t2=compute the required-time of PDR down-to-
Threshold-Value;
if(t2< t1)
{
if(Threshold-Value<0.9)
Threshold-Value=Threshold-Value+0.01;
}
else{
if(Threshold-Value>0.8)
Threshold-Value=Threshold-Value-0.01;
```

Table-2: Dynamic-Threshold Algorithm

As illustrated in Figure-3, in case of having single malevolent node n4 in the route, with response fake R-REP and address-list L= $\{n_1,n_2,n_3,n_4,n_5,n_6\}$, 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 K_k^1 for obtaining S= $K_1^1 \cap K_2^1 \cap K_3^1 =\{n_4,n_5,n_6\}$ and T = L-S = $\{n_1,n_2,n_3\}$and so it requests its neighbor node n_2 for listening mode, the packets which were diverted by n_3 to n_5 should have

been transmitted to n_4. 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 MNDPCB protocol. As shown in Figure-3, if n_5 & n_4 were malevolent nodes, the list T would contain T = L-S = {n_1,n_2,n_3} and n_2 had requested for listening to which, n3 might send packets. In case n_5 or n4 would have been detected for which co-operation might be stopped. Therefore remaining nodes will be baited and detected. The Figure-2 shows that, even for more malevolent nodes in the ad hoc network, our MNDPCB would still succeeds in detecting them simultaneously after receiving their reply R-REP.

3.3 Shifting to Reactive Defense Step:

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

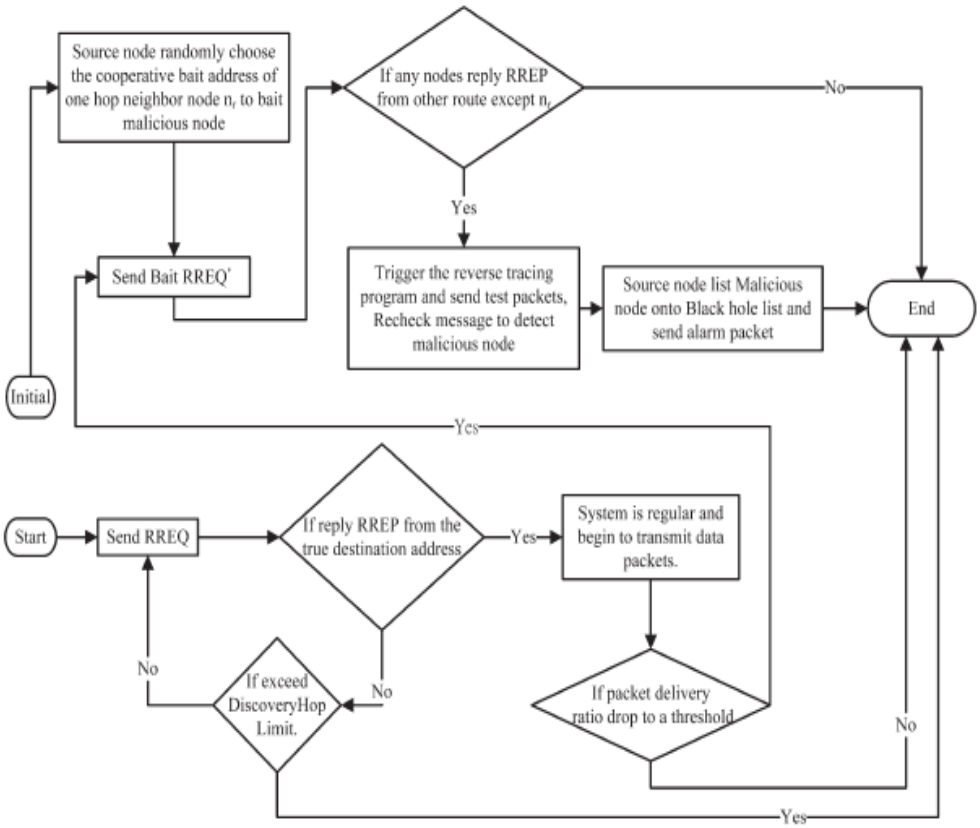

Fig-4: Operation of MNDPCB protocol

4. PERFORMANCE EVALUATION

4.1 Simulation parameters:

To study the performance of our MNDPCB protocol, the Qual-Net Simulator[10] is used. For the simulation environment, IEEE802.11 MAC is used with channel data-rate at 10 Mb/s. The performance of MNDPCB is measured for threshold at 85%, 95% and varying dynamically. Malicious nodes are added into the network environment to perform the attacks and their ratio is fixed at 10%. Simulation is performed in 1000 x 1000 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 meters
2	Application-traffic	10 C-B-R
3	Transmission-rate	4 pkts/ sec
4	Packet-size	512Bytes
5	Channel-data-rate	10Mbps
6	Pause-time	0 Seconds
7	Node speed	0-20 mtrs/sec in steps of 5%
8	Number-of-nodes	50
9	Simulation-time	1000 sec
10	Simulation-area	1000 x 1000 m^2
11	Malicious nodes	10%
12	Threshold	85%, 95%, Dynamic threshold

4.2 Simulation Results

Simulation scenario is created by varying the node speed, while fixing the number of malevolent nodes (percentage) to 10%. In this case, the effect of different threshold values of MNDPCB protocol is evaluated based on the standard performance parameters.

At first, the packet-delivery-ratio of MNDPCB is compared with that of basic DSR at different node mobility varying from 0-20 mtrs/sec in steps of 5%.

As illustrated in Chart-1, it is shown that, as node mobility increases, base-DSR suffers drastically by black-hole attacks in terms of packet delivery ratio. Our MNDPCB protocol achieved higher packet delivery ratio compared with base-DSR, even at node mobility of 20 mtr/sec. The MNDPCB protocol can detect malevolent nodes by maintain the packet delivery ratio above 90% at all threshold values.

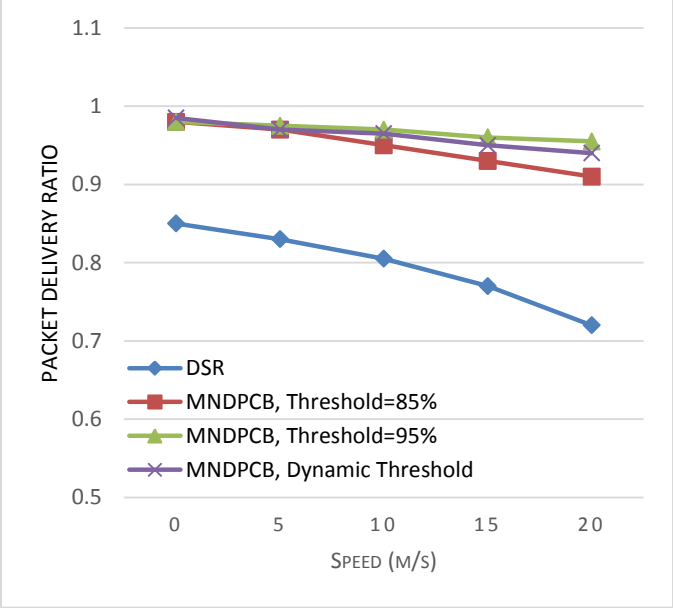

Chart-1: Comparison of PDR Vs varying node speed

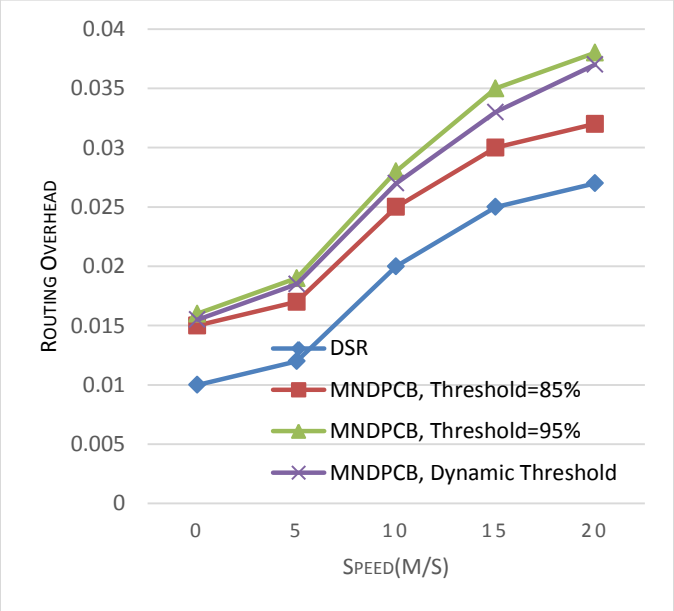

Chart-2: Comparison of Routing Overhead Vs varying node speed

Second, we examine routing-overhead of MNDPCB protocol and base-DSR for different node mobility cases. As illustrated in Chart-2, it is shown that base-DSR results in lower routing-overhead compared with MNDPCB protocol. This is due to fact that, base-DSR will don't have internal defensive mechanism. It is demonstrated that MNCBD protocol can still detect malevolent nodes, with routing-overhead slightly higher than base-DSR at variable threshold values.

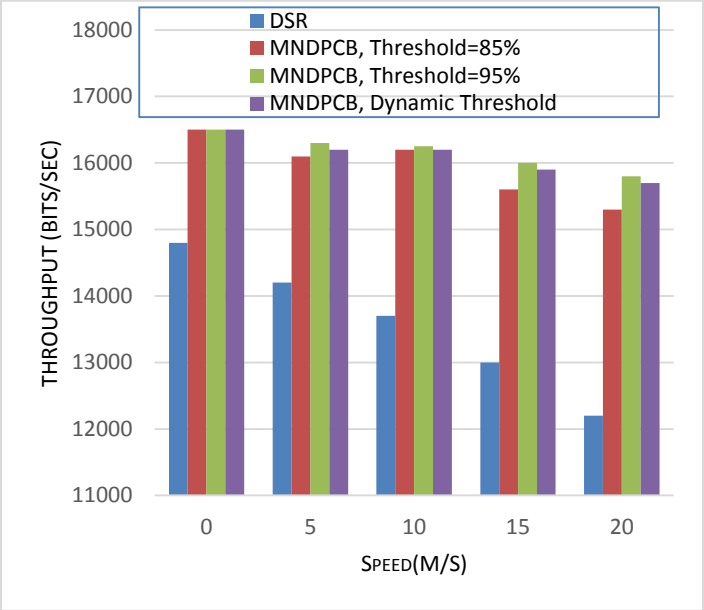

Chart-3: Comparison of Throughput Vs varying node speed

Finally, in Chart-3 we study the throughput for both MNDPCB protocol and base-DSR for various thresholds. As shown in Fig.8, the throughput for base-DSR suffers drastically with increase in the node speed. Our MNDPCB-protocol achieves higher throughputs when compared to Base-DSR at all node speeds for all considered threshold values, due to high success rate of packet delivery.

5. CONCLUSION

This paper proposes the novel protocol for detection and prevention and of a gray-hole attack by means of MNDPCB protocol in MANET. This work is mainly focused on gray-hole as a malicious attack and discovers its prevention and elimination as well. This novel approach detects malevolent nodes in MANETs for defending collaborative black-hole and gray-hole attacks. The simulation results shows that our MNDPCB protocol gives better performance upon comparison to base-DSR in-terms of performance metrics: packet-delivery ratio, throughput and routing-overhead in all cases of mobility speed. It is proved that, our MNDPCB protocol outperforms base-DSR with better performance, while detecting and defending the collaborative black-hole and gray-hole attacks. In future, we planned to work for investigating the integration of MNDPCB protocol with other security protocols, there by constructing the comprehensive secured framework to protect mobile ad hoc networks against all threats.

Acknowledgements

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 J. Select. Areas Commun., vol. 24, no. 2, pp. 370–380, Feb. 2006.

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

[3] 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. Local Computer Netwetworks, pp. 1043–1052, Oct.2007.

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

[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, N0.2, 2018.

[6] R.Adimalla, V.ValliKumari and Ch.S Reddy, "Genetic algorithm based Backup Route Establishment for QoS Routing", International Journal of Intelligent Engineering and Systems, Vol.10, No..3, 2017.

[7] I.J.Jenifhar Jolla and R.Dhanalakshmi, "Mitigation of Gray hole Attacks in MANET using Baiting Process and Reverse Tracing", Global Journal For Research Analysis, Volume 4, Issue 5, ISSN No.2277- 8160, pp. 11-14, May 2015.

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

[9] W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," In: Proc. 28th IEEE Int. Symp.Reliable Distrib. Syst., New Delhi, India, Sep. 2009.

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

[11] M.Neelakantappa, Amjan Shaik, "Secured Routing protocol for Mobile Ad hoc Networks to defend collaborative Black-hole and Gray-hole attacks by malicious nodes", IJIE, Vol.11, No.5, 2018.

[12] Bhandare, A., Patil, S.: Securing MANET against co-operative black hole attack and its performance analysis-a case study, ICCUBEA-15, pp. 301–305 (2015).

[13] T. Poongodi and M. Karthikeyan, "Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks," 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. IEEE Int.Conf. Communications, pp. 2780–2785, May 2008.

[15] M. S. Khan, Q. K. Jadoon, and M. I. Khan, "A comparative performance analysis of MANET routing protocols under security attacks," in Mobile Wireless Technol., Berlin, Germany: Springer, 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 Syst. J.,vol. 9, no. 1, pp. 65–75, Mar. 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," 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", New Delhi, India: Springer, 2015, pp. 33–37, 2015.

[19] Baadache, Abderrahmane, and Ali Belmehdi, "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks", arXiv preprint arXiv, 1002 (1681), 2010.

[20] Liu and Kejun, "An acknowledgment-based approach for the detection of routing mis-behavior in MANETs", Mobile Computing, IEEE Transactions on 6 (5), 536–550, 2007.

[21] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," IEEE Commun. Mag., vol. 40, no. 10, pp. 70–75, Oct. 2002.

[22] Mark Linderman , Wang, Weichao, and Bharat Bhargava, "Defending against collaborative packet drop attacks on MANETs", In: Proc.of 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009)(in Conjunction with IEEE SRDS 2009), New York, USA, 27, 2009.

[23] Ramaswamy, Sanjay, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", In: Proc.of. International Conference on Wireless Networks, 2003.

[24] Mohanapriya, M., and I Krishnamurthi, "Modified DSR protocol for detection and removal of selective black hole attack in MANET", Journal of Computers & Electrical Engg, 40 (2), 530–538, 2014.

[25] Chang and, Jian Ming, "CBDS: a cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture", In: Proc.of. Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on. IEEE, 2011.

[26] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[27] 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.

[28] K. Nahrstedt and Y. Xue, "Providing fault-tolerant ad hoc routing service in adversarial environments," Wireless Communications, vol. 29, pp. 367–388, 2004.