ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(36), DOI: 10.17485/ijst/2016/v9i36/95632, September 2016* ISSN (Online) : 0974-5645

An Effective CBHDAP Protocol for Black Hole Attack Detection in Manet

K. Vijayakumar[1*] and K. Somasundaram[2]

[1]Department of Computer Science and Engineering, Karpagam University, Coimbatore - 641021, Tamil Nadu, India; vijay_kollati@yahoo.co.in
[2]Department of Computer Science and Engineering and IT, Aarupadai Veedu Institute of Technology, Paiyanoor, Chennai - 603104, Tamil Nadu, India; soms72@.yahoo.com

Abstract

Objective: The various features of mobile adhoc networks (MANET's) are open medium, dynamic topology and absence of centralized monitoring point which introduces various security challenges. One among the security attacks are defined as the black hole attack in this article. **Methods:** In this paper we introduce a protocol for detecting and avoiding the black hole attacks in MANET's by an efficient Crypto-key based Black Hole Detection and Avoidance Protocol (CBHDAP). **Findings:** The suggested protocol generates a group key using Diffie-Hellman (DH) based key agreement black hole detection algorithm then the generated key is forwarded to the authenticated group members. The validation of the nodes in the route from the source to the destination is done before initiating the transmission. The black hole attacks are avoided during transmission by considering the parameters such as time taken for Route Reply (RREP), hop count, Packet Delivery Ratio (PDR) are used. To validate the performance of the proposed approach, it is compared with the existing protocols for the metrics such as detection probability, throughput, end-to-end delay, etc. **Improvements:** The validation results prove that the CBHDAP provides optimal results for all the metrics like detection probability, throughput, E2E delay etc when compared with the algorithms existed.

Keywords: CBHDAP, Blackhole Attack, Diffie-Hellman Algorithm, MANET's, Security Attacks

1. Introduction

MANET (Mobile Ad hoc Network) is a gathering of independent mobility nodes that transmit information with each other through multi-hop wireless links[1]. The characteristics of the MANET such as open medium, absence of centralized monitoring, dynamically changing network topology, limited bandwidth and multi-hop nature[2] introduces the various attacks leading to failure of security like rushing attacks, Sinkhole attacks, blackhole attacks, wormhole attacks, replay attacks etc.

The distinguishing proof and avoidance of the security issues has dependably been a difficult task[3]. Among the security challenges, the black hole assault is a genuine risk to MANET. The black hole assault is a kind of active attack[4] and also a routing layer assault in which the malignant nodes misuse a routing protocol for propagation itself as having the most undeviating path to the destination hub. When the source node ahead the information packets the malicious node drops information packets and do not notify the source node that the packet has received by the destination hub. Figure 1 shows an illustration for the black hole attacks where node A is the source node and node E is the destination node. The source node A broadcasts RREQ (Route Request) message to all its neighbors to initiate the transmission. The neighboring nodes on receiving the RREQ message, present the RREP messages with the number of hops required for reaching the destination node. The source node finds the nodes among the neighboring nodes which forms a shortest path for transmitting the data packets. If any of the neighbor nodes is malicious a false message RREP is sent back to the source node. Regardless of the connectivity to the destination node the neighbor node fake RREP message informs that it has the undeviating path to reach the target node. On getting the information packets it

* *Author for correspondence*

drops it and don't notify the source node with respect to the status of the transmission.

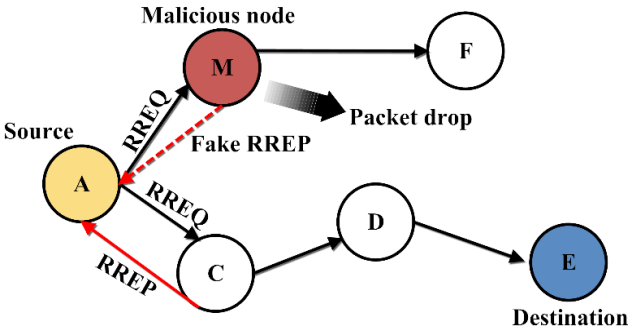

Figure 1. Black hole attack.

There exist multiple techniques such as MEAODV, Modified Enhanced Ad hoc On-demand Distance Vector[5], GBHASM, Grouped Black Hole Attack Security Model[6], MDSR, Modified Dynamic Source Routing[7], etc. for black hole attacks detection. The above said techniques detect only the collaborative black hole attack. Therefore the suggested protocol CBHDAP addresses many issues related to security; it also finds single black hole and collaborative black hole attacks with a strategy of minimum message delay and routing overhead. In accumulating with the detecting the black hole attack, the proposed CBHDAP protocol also avoids it by considering the parameters such as time consumed for RREP messages, packet delivery ratio and hop count.

The fundamental goals of the proposed CBHDAP protocol are

- To execute the key agreement black hole detection algorithm for finding the nearness of black hole assault in MANET.
- To maintain a strategic avoidance from the black hole assault by accepting the parameters, for example, packet delivery ratio, hop count and time.

Whatever remains of the article sorted out as takes after. The next Section 2 summarizes various existing protocols utilized for distinguishing and avoiding the black hole assault in mobile adhoc networks. In section 3 we give a point by point description on the proposed CBHDAP protocol for black hole attack detection in MANET. Section 4 discusses the execution consequences of the proposed protocol. Section 5 presents the conclusion and future work.

2. Blackhole Attacks Prevention and Detection Recommendations

This section gives the various existing protocols for detecting and prevention of black hole attacks in MANET's.

The authors in[7] suggested a Modified Dynamic Source Routing (MDSR) protocol for detecting and preventing the black hole attack in MANET. The suggested protocol exploited the Intrusion Detection System (IDS) for isolating the malicious nodes from the network. When compared to the traditional Dynamic State Routing (DSR), the proposed protocol minimized the energy loss and packet loss rate.

In[8] a new approach to deduct the detection time of nodes in selfish and collaborative watchdogs suggested. In this the selfish and the collaborative nodes form a MANET that contains both these kinds of nodes. The watch dog among the collaborative nodes detects the selfish node with a given probability of detection. The detection time of the selfish nodes was reduced, and the overall communication overhead was minimized.

The authors[9] proposed technique for prevention which finds the malicious nodes and separates these nodes from the network which is actively routing and forwarding the data packets by sending alarm packets to its nearby nodes upon reaction. The results specify that with minimum increase in average end to end delay and normalized routing overhead, the packet delivery ratio increases.

Anchugam et al.[10] suggested a method ACO for black hole detection where security and performance parameters are improved but this method can detect only one attack and effective for black hole.

Kumar et al.[11] proposed an adaptive approach for detecting the black hole attack. When compared to the Ad hoc On-demand Distance Vector (AODV) routing protocol, the proposed approach provided efficient black hole attack detection and an optimal packet delivery ratio and throughput.

A trusted AODV routing algorithm for detecting and preventing the warm hole attack and collaborative black hole attack in MANET suggested by authors[12] provides optimal detection performance.

In[13] the authors suggested an energy efficient black hole attack detection and avoidance algorithm for

MANET. The suggested algorithm provided an optimal throughput, secure routing, and resource utilization.

Wahane et al.[14] proposed a modified AODV protocol and crosschecking based true-link concept for detecting the black hole attack. When compared to the existing protocols, the suggested concept produced optimal detection performance.

The authors[15] proposed a timer based detection approach for detecting the black hole node. The suggested approach enhanced the packet delivery ratio and detection performance. Sen, et al.[16] suggested a defense mechanism for the black hole node enabled coordinated attack. The suggested mechanism produced an optimal attack detection performance. But, the throughput of the suggested mechanism was not reasonable.

In[17] suggested Baited-Black-hole DSR (BDSR) protocol for detecting and preventing the black hole attacks integrates the proactive and reactive defense architecture of MANET for enabling the malicious node to reply the RREP.

A fuzzy logic technique based Intrusion Detection System (IDS) for detecting the black hole attack, gray hole attack, and warm hole attack was proposed by[18] where the experimental results proved that the proposed system was optimal for detecting the black hole attack. As the presence of attacks introduced route modifications, the jitter value was very high.

Manoranjini et al.[19] proposed a hybrid automatic detector and kalmanbucy filter based protocol for detecting the black hole attacks. Experimental results proved that the suggested protocol increased the speed of detecting the black holes and enhanced the consistency of identifying the black hole attack. But, it was not optimal for the larger network group.

The authors[20] suggested a trust based dynamic source routing protocol for securing the end-to-end route from the black hole nodes. Experimental results proved that when compared to the traditional Dynamic Source Routing (DSR) the proposed protocol increased the packet delivery ratio by 42% and reduced the packet loss rate by 37%.

In[21] a Novel Honey pot Based Detection and Isolation (NHBADI) approach for detecting the black hole attack in MANET was suggested where the simulation results proved that the proposed approach minimized the network overhead, packet drop ratio and also normalized the routing load. In addition to detecting the attack, the proposed approach also isolated the vulnerable black hole nodes from MANET.

Dorri et al.[22] suggested an Extended Data Routing Information (EDRI) table based approach for detecting and isolating the cooperative black hole nodes in MANET. Simulation results proved that the proposed approach minimized the packet overhead and enhanced the network throughput.

The authors[23] suggested a novel approach for detecting the single black hole and cooperative black hole attacks. By using the advanced DRI table, the proposed approach enhanced the security of the AODV protocol. Simulation results proved that the proposed approach increased the network performance and minimized the packet dropping ratio.

Vijaya kumar et al.[24] proposed a Proximity Set Method (PSM) for detecting the malicious nodes in MANET. Simulation results proved that the proposed AODV with PSM provided optimal black hole detection routine than the traditional Adhoc on demand distance vector routing protocol. But, the E2E deferral was not optimal.

In[25] RSA and sequence number calculation based algorithm for preventing the black hole attack was suggested where the experimental results show that the proposed algorithm produced optimal delay and throughput. But, the performance of the suggested algorithm was not optimal for detecting the worm hole and gray hole attacks.

In[26] authors proposed black hole detection by using IDS technique. In this a better QoS is achieved by using highest sequence number of the node and on analysis the PDR is enhanced by 60%.

Junhai et al.[27] addressed the black hole problem using the Message Authentication Code (MAC) and Pseudo Random Function (PRF). Experimental analysis proved that the proposed mechanism efficiently identified the black hole attack and also detected a safe route that avoids the black hole attack.

Detected and prevention of the black hole attacks using IDS was proposed by[28]. In this Anti-Blackhole Mechanism (ABM) was deployed in the sniff mode. The analysis results proved that the proposed IDS efficiently blocked the malicious node with minimal false positives.

Shahabi et al.[29] suggested a modified algorithm for enhancing the security of AODV routing protocol in detecting the black hole attacks. The simulation results proved that the suggested algorithm produced an optimal end-to-end delay and packet delivery ratio.

The authors[30] proposed an efficient solution for the

AODV protocol in MANET. The suggested solution exploited the promiscuous mode for detecting the black holes. Even in the observations of black hole attacks the proposed solution maintains the throughput.

The authors[31] proposed a method where the malicious nodes may react to packets carry invalid IP addresses which leads to a chance that there will be no chance of false detection. This method which do not need threshold value for intrusion detection which may give rise to the rate of fake node detection.

From the study of the various existing detection and prevention techniques of black hole attacks, the observations state that there are many drawbacks due to more jitter value and unable to maintain and handle larger networks after the completion of transmission. And also it is clear that the techniques for detection do not consider any measures for the avoidance of black hole attacks. So as to manage these issues an efficient algorithm, CBHDAP protocol is projected for detecting and avoiding the black hole attack in MANET.

3. CBHDAP: Proposed Protocol for Black Hole Attack Detection and Avoidance

The proposed CBHDAP protocol represents the black hole attack detection and avoidance. Figure 2 demonstrates the general stream of the CBHDAP protocol and it is clear that the CBHDAP protocol includes the following steps,

- Network formation
- Group key sharing
- Route discovery
- Packet transmission

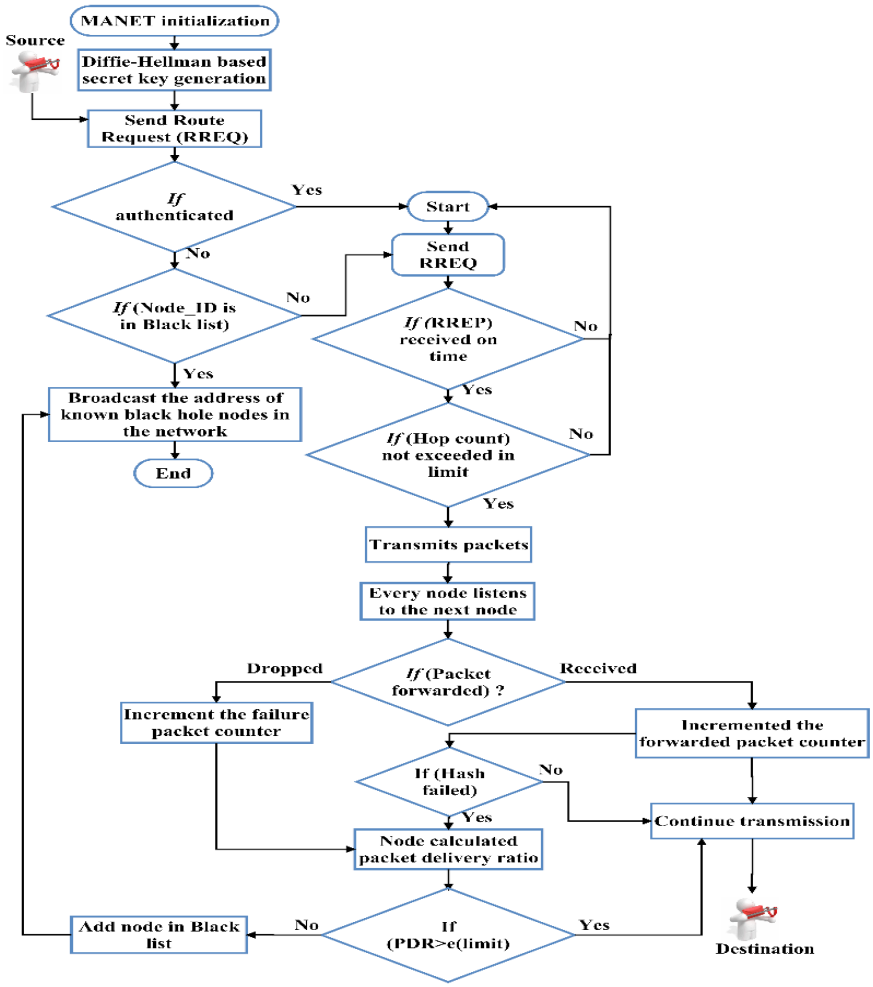

Figure 2. Overall flow of the proposed CBHDAP protocol.

3.1 Network Formation

The initial step involved in the deployment of the proposed CBHDAP protocol is network formation. Using NS2 tool, the MANET is initialized with 100 number of nodes. Every node communicates with the other node using random waypoint model. The mobile nodes exploit IEEE 802.11 standard for communication. The radio range of the communication is initialized as 250 meter whereas the interference range is initialized as 550 meters. The simulation runs for 50 simulated seconds.

3.2 Group Key Sharing

After the initialization of MANET, a group key that enables the communication between the group members is generated using Diffie-Hellman based key agreement black hole detection algorithm. The steps involved in the suggested protocol are illustrated below,

Algorithm: Key agreement black hole detection algorithm

Input: Path Length (PL), source (src), destination (Dst), next_hop, transmission time (T_{xT}), timer (T) and processing time (P_{xT}).

Key Agreement {

Step 1: Message ($I \rightarrow R:N_i, g^i$) (1)

where,

I represent the sender
R denotes the responder
N_i represents the random bit-string of the sender
g^i is the sender exponential

Step 2: Message (($R \rightarrow I:N_i, N_r, g^r, GRPINFO_r, HMAC\{HK_r\}(g^r, N_r, N_i, IP_i)$) (2)

where,

N_r is the random bit-string of the responder
g^r represents the receiver exponential
GRPINFOr denotes the list of Diffie-Hellman groups supported by the responder
HK_r is the transient hash key private to the responder
IP_i denotes the network identifier of the sender

Step 3:

Message ($I \rightarrow R:N_i, N_r, g^i, g^r, HMAC\{HK_r\}(g^r, N_r, N_i, IP_i)$ $E\{Ke\}(ID_i, ID_r, sa, SIG)\{i\}(N_i, N_r, g^i, g^r, GRPINO_r$,

$$HMAC\{Ka\}\left('I', E\{Ke\}\left(ID_i, ID_{r'}, sa, SIG\{i\}\left(\begin{matrix} N_i, N_r, g^i, g^r, \\ GRPINOr \end{matrix}\right)\right)\right) \quad (3)$$

where,

$Ke\ and\ Ka$ denotes the shared key derived from g^i, g^r, N_i, N_r

$ID_i\ and\ ID_{r'}$ represents the certificates of the sender and responder

sa is the security association that the sender wants to establish

$SIG\{i\}$ denotes the digital signature of $N_i, N_r, g^i, g^r,$ using the private key of the sender.

$GRPINOr$

Step 4: Message ($R \rightarrow I$:

N_i, N_r, E{Ke}(ID_i, $ID_{r'}$, sa', SIG{r})(g^r, N^r, g^i, N_i)), HMAC {Ka}('R' E(Ke)(ID_r, Sa', SIG{r}(g^r, N_r, g^i, N_i))) (4)

where,

$SIG\{r\}$ is the digital signature of $g^r, N_r,$ g^i, N_i using the private key of the responder

sa' represents the information that the receiver wish to send to the sender

}

```
Set Src_Args [] =Source;
Set next [] [] = next_hop [source] [destination]
WHILE (source! =destination)
    Set T :=( PL+1)*2*(T_xT + P_xT)
    PL = PL-1
    Source=next
    next := next-hop[source][destination]
END WHILE
IF (TIMEDOUT)
    Set Black_list [next]:= TRUE
END IF
Set source = Src_Args[][]
next = next_hop[Dst][Src]
WHILE (Dst!=Src)
    Dst := next
    next := next_hop[Dst][Src]
END WHILE
END
```

The CBHDAP protocol consumes the inputs such as PL, src, Dst, next hop, transmission time, timer and processing time for deploying the key agreement algorithm. Initially, the source node (I) broadcasts the HELLO packets using (1) for discovering its neighbors. By using (2) all the neighbor nodes (R) reply the source with all the achievable routes to reach the destination. The source node applies the Hash Message Authentication Code (HMAC) using (3) for the information obtained

from neighboring nodes and forwards back to R. By exploiting the private key of the receiver, the responder or the neighboring node applies the digital signature for the message using (4).

3.2 Route Discovery

Route discovery is the process of estimating the optimal route between the sender and receiver. The estimation of the optimal route is based on two steps such as,

- Node authentication
- Black list verification

3.2.1 Node Authentication

This step validates the authenticity of the nodes using two metrics such as time and hop count. At first to decide the conceivable paths to the destination hub, the source hub broadcasts the RREQ messages to its neighboring hubs. On accepting the RREQ message, the neighboring node evaluate the number of hops required for achieving the destination hub then replies the RREQ message with RREP messages. If the time interval between RREQ and RREP message satisfy the Time to Live (TTL), then the corresponding responder node is considered to authentic else it is considered as unauthentic and added to the black list. Another metric used for validating the authenticity of the nodes is hop count. The number of hops required for transmitting the data packets from the source node to the destination node is given by the hop count. From the RREP messages of every neighboring node, the number of hops required for reaching the destination is obtained. If the hop count exceeds the hop limit the corresponding node is considered as malicious and added to the black list.

3.2.2 Black List Verification

Black list is a list that contains the ID of the malicious nodes obtained from the previous attack history. Every node in MANET maintains a black list, subsequently when the source node needs to communicate the RREQ messages to its neighboring nodes it verifies its black list and forwards the RREQ messages to the nodes that are not present in the black list. When a node in MANET detects a black hole node, it adds the ID of the corresponding node in its black list and broadcasts the ID of the same to all other nodes in the network.

3.3 Packet Transmission

After verifying the authenticity of the nodes and the black list, the packet transmission is initiated. During the transmission of the packets, every node listens to the next node. The successful transmissions of the packets increment the forwarded packet counter and the unsuccessful transmission of the packets increment the failure packet counter. The hash value of the packets is validated, to avoid the black hole attacks during transmission. If the hash value fails it specifies the nonappearance of black hole attack and hence the transmission is continued, or else to the node PDR (Packet Delivery Ratio) is calculated. If the PDR is more than the limit, it indicates that there is no packet drop hence the communication is proceeded else to the black list this node is added as a black hole node.

4. Performance Analysis

This section illustrates the behavior and the results of the CHBDAP protocol for detection and avoidance of black hole attacks. Ad-hoc On demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Modified Reverse AODV[32] (MRAODV) are several existing algorithms whose performances are taken into consideration and compared with the proposed CBHDAP protocol. The existing algorithms and the proposed protocol are implemented in NS2 tool and their results are compared for the parameters like average PDR (Packet Delivery Ratio), Routing overhead, Detection of black hole nodes, E2E (End to End) delay, Throughput, Node outage count, Packet transfer rate, Remaining energy and Energy consumption.

4.1 Detection of Black Hole Nodes

Figure 3 shows the number of successful black hole attack detection for the existing DSR, AODV, MRAODV algorithms and the proposed CBHDAP protocol and it is analyzed that the proposed CBHDAP protocol provides higher black hole detection probability than the existing algorithms.

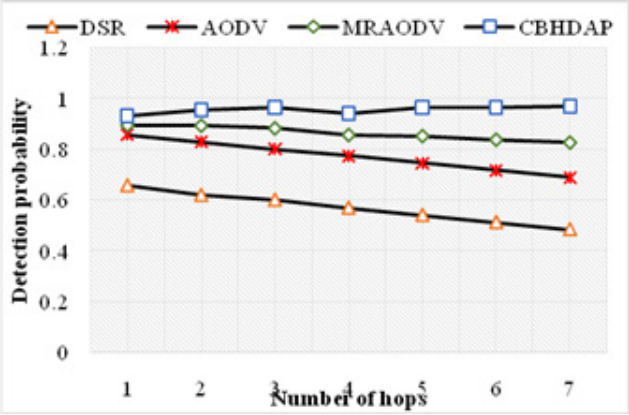

Figure 3. Comparison of detection of black hole nodes for the existing and proposed protocols.

4.2 Throughput

The rate of the received packets from the destination hub to the sent data packets from the source hub is given by throughput. The throughput is ascertained from the accompanying condition,

$$\frac{rdp}{sdp} * 100\% \quad (1)$$

where, rdp speaks to the quantity of packets got at the destination node, sdp is the quantity of packets sent from the source node. Figure 4 portrays the examination of throughput for the current DSR, AODV, MRAODV algorithms and the proposed CBHDAP convention which obviously demonstrates that when contrasted with the current algorithms, the proposed protocol provides higher throughput for the increasing number of nodes.

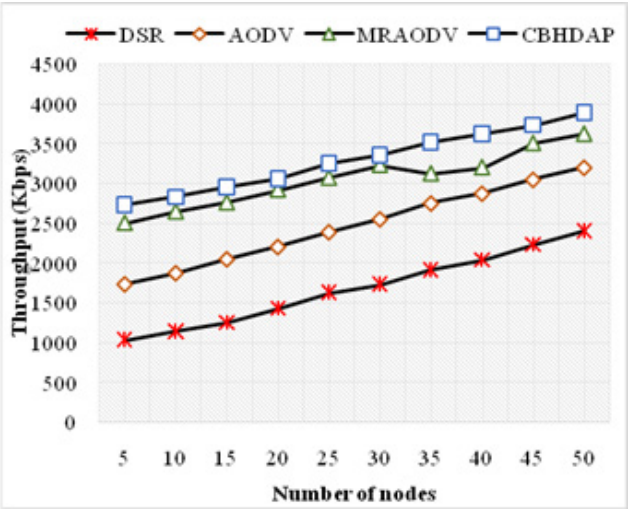

Figure 4. Comparison of throughput for the existing and the proposed protocols.

4.3 E2E (End to End) Delay

The parameter end to end deferral is characterized as the average time taken by the packet of information to achieve the goal. This E2E delay occurs due to discovery latency, buffering and queuing. This end-to-end delay is calculated by,

$$End - to - End\ delay = \sum \frac{T_d - T_s}{N} \quad (2)$$

Where,

T_d represents the time the data packet arrives the destination

T_s denotes the time the source sends its first packet

N denotes packets transmitted count.

Figure 5 represents the comparison of end-to-end delay with respect to the number of attacker nodes where the results show that the CBHDAP provides minimal end-to-end delay comparing with the existing DSR, AODV, and MRAODV algorithms.

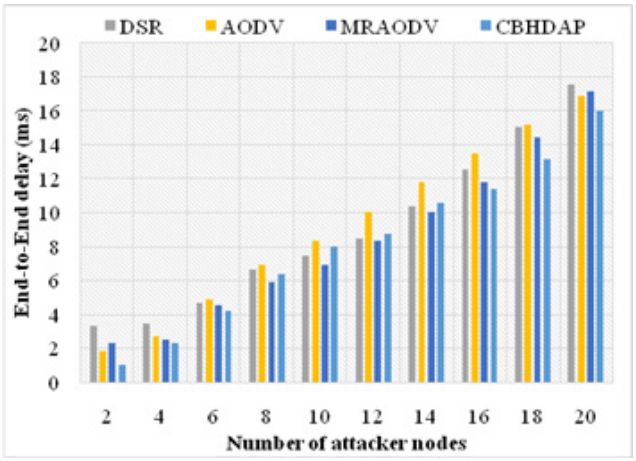

Figure 5. Comparison of End-to-End delay for the existing and the proposed protocols.

4.4 Routing Overhead

Routing overhead specifies the overhead created for routing the data packets between the nodes to detect the black hole attack. As shown in (Figure 6), the comparison of routing overhead for the existing DSR, AODV, MRAODV algorithms and the proposed CBHDAP protocol results prove that irrespective of the number of nodes, the proposed CBHDAP protocol provides minimal routing overhead than the existing algorithms.

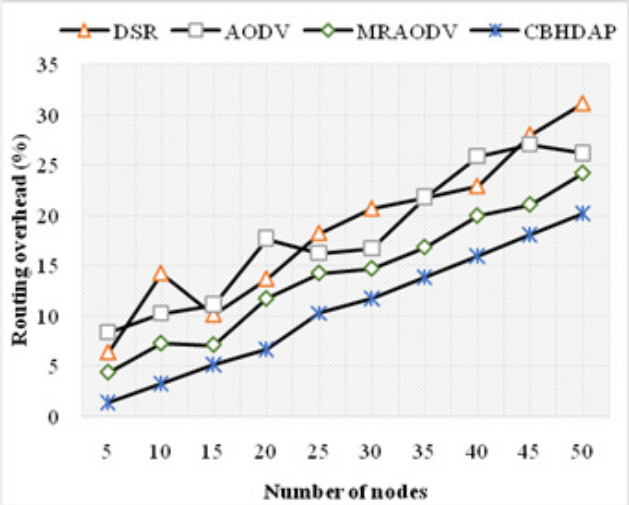

Figure 6. Comparison of routing overhead for the existing and proposed protocols.

4.5 Remaining Energy

Remaining energy is the amount of energy that the intermediate nodes have for performing the future transmissions. If a node has lower remaining energy, alternate node will be chosen for transmitting the data packets. The comparison of remaining energy with respect to the simulation time is performed, where the comparison results show that the proposed CBHDAP protocol provides higher remaining energy than the existing algorithms such as DSR, AODV and MRAODV and is depicted in Figure 7.

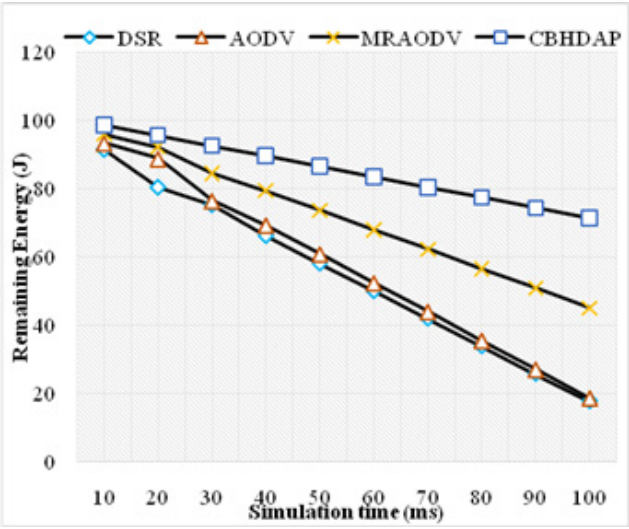

Figure 7. Comparison of remaining energy for the existing and the proposed protocols.

4.6 Energy Consumption

In MANET, the intermediate nodes consume energy for transmitting the data packets towards the destination which can be said as energy consumption. Figure 8 shows the comparison of energy consumption with respect to the simulation time, where the results on comparison prove that the proposed CBHDAP protocol provided minimal energy consumption than the existing algorithms such as DSR, AODV and MRAODV algorithms.

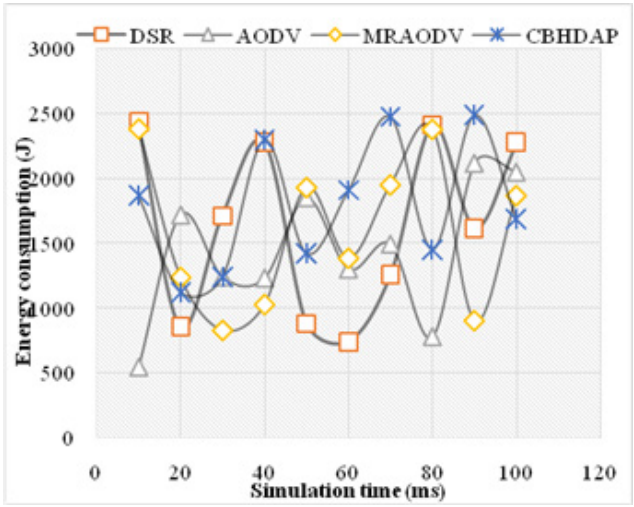

Figure 8. Comparison of Energy consumption Vs simulation time.

4.7 Number of Node Outage

The node outage creates more number of colliding packets during the data transmission thus exhausting the energy of the intermediate nodes. The presence of more number of node outages affects the MANET functionality. As shown in (Figure 9), the comparison of number of outage for the existing DSR, AODV, MRAODV algorithms and the proposed CBHDAP protocol is represented, moreover it is analyzed that the proposed CBHDAP protocol provides minimal number of node outage than the existing algorithms.

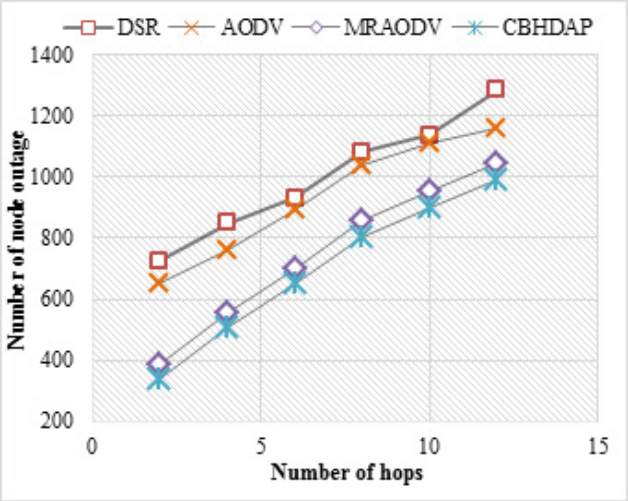

Figure 9. Comparison of number of node outage for the existing and the proposed protocols.

4.8 Average PDR (Packet Delivery Ratio)

The proportion of the quantity of data packets got at the destination to the quantity of data packets sent from the source is characterized by the average PDR. The average PDR is estimated based on the following equation,

$$Average\ PDR = \frac{\sum total\ number\ of\ received\ packets}{\sum total\ number\ of\ sent\ packets} \quad (3)$$

Figure 10 depicts the analysis of PDR for the existing AODV, MRAODV, PSM methods and the proposed CBHDAP protocol, furthermore it is analyzed that the proposed CBHDAP protocol specifies elevated on comparison with the existing methods packet delivery ratio.

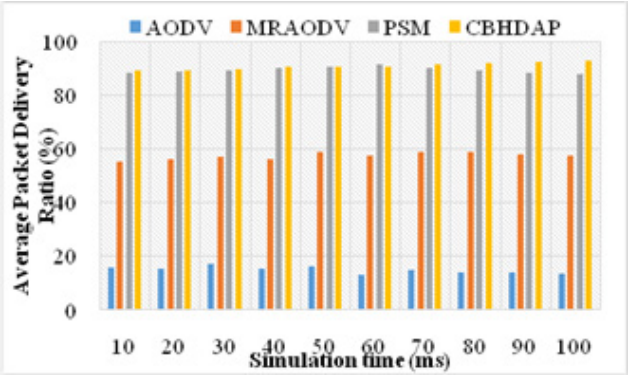

Figure 10. Packet delivery ratio comparison for the existing and the proposed protocols.

4.9 Packet Transfer Rate

The amount of data packets transmitted in an instant run is called Packet transfer rate. Figure 11 represents the comparison of packet transfer rate over the number of nodes, also it is analyzed that when compared to the existing AODV, MRAODV and PSM protocols, the proposed CBHDAP protocol provides higher packet transfer rate for the increasing number of nodes.

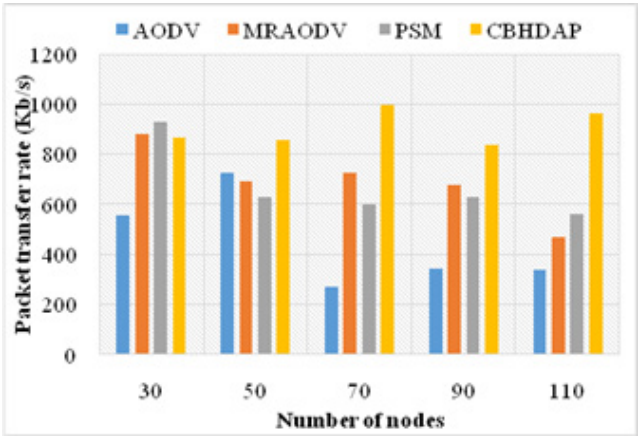

Figure 11. Comparison of packet transfer rate for the existing and the proposed methods.

5. Conclusion and Future Work

The conclusion and future work of the proposed technique is summarized in this part of the article. The CBHDAP protocol is efficient for detecting and avoiding the attacks like black hole in MANET. Initially, the sender deploys the Diffie-Hellman based key agreement black hole detection algorithm by which the secret keys are generated, and then generated keys are forwarded to the group members. The transmission between the sender and receiver is initiated by broadcasting the RREQ messages. On receiving the RREQ messages, every group member provides the RREP messages. If the RREP is found to un-authentic, in the black list the corresponding node-ID is added and address of it is broadcasted to the remaining group members. On the other hand if the RREP is found to be authentic, the time consumed for replying the RREQ messages is checked. If the time consumption is compelling, it checks the hop count to attain the destination. When the number of hops is also satisfactory, the transmission is initiated. During the transmission, every node listen's the next node for forwarding the data packets. When the data

packets are forwarded successfully, the forwarded packet counter is incremented else the failure packet counter is incremented.

After incrementing the forwarded packet counter, the hash is checked for failure. The failure in the hash value initiates the estimation of packet delivery ratio. If it is greater than the limit, the transmission is continued else the node is added to the black list. The existing protocols like DSR, AODV and MRAODV are taken to compare with the proposed CBHDAP protocol for the parameters like E2E (end to end) delay, detection probability, number of node outages, overhead caused by routing, throughput, remaining energy, and energy consumption. From the results compared and observed, the proposed CBHDAP protocol is clearly providing elevated detection probability, throughput, remaining energy and minimal end-to-end delay, routing overhead, energy consumption and number of node outages. In future, the proposed protocol will be extended to detect other security attacks with more detection probability.

6. References

1. Funde NA, Pardhi PR. Detection and prevention techniques to black and gray hole attacks in MANET: A Survey. International Journal of Advanced Research in Computer and Communication Engineering. 2013; 2(10):4132–36.
2. Maheshwari N, Parihar PS. An enhanced approach to avoid black hole attack in mobile ad hoc networks using AOMDV routing protocol. International Jounal for Scientific Research and Development. 2013; 1(7):1494–502.
3. Vijaya Kumar K, Kancherla S. An empirical model of malicious node detection and prevention with data rating. International Journal of Engineering Trends and Technology. 2014; 2(17):56–9.
4. Vijaya Kumar K, Somasundaram K. Study on reliable and secure routing protocols on manet. Indian Journal of Science and Technology. 2016; 9(14):1–10.
5. Gupta A. Black hole attack mitigation method based on route discovery mechanism in AODV protocol. IEEE International Conference on Computational Intelligence and Computing Research, Kerala, India. 2013; 2(9). p. 1–6.
6. Bajwa SS, Khan MK. Grouped Black hole Attacks Security Model (GBHASM) for Wireless Ad-Hoc Networks.The 2nd International Conference on Computer and Automation Engineering (ICCAE). Pakistan. 2010. p. 756–60.
7. Mohanapriya M, Krishnamurthi I. Modified DSR protocol for detection and removal of selective black hole attack in MANET. Computers and Electrical Engineering. 2014; 40(2):530–8.
8. Hernandez-Orallo, Olmos MDS, Cano J-C, Calafate CT, Manzoni P. A fast model for evaluating the detection of selfish nodes using a collaborative approach in MANETs. Wireless Personal Communications. 2014; 74:1099–116.
9. Raj PN, Prashant SB. DPRAODV: A dyanamic learning system against blackhole attack in aodv based manet. IJCSI International Journal of Computer Science. 2009; 2:54–9.
10. Anchugam CV, Thangadurai K. Detection of Black Hole Attack in MobileAd-hoc Networks using Ant ColonyOptimization – simulation Analysis. Indian Journal of Science and Technology. 2015; 8(13):1–10.
11. Kumar V, Kumar R. An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network. Procedia Computer Science. 2015; 48:472–79.
12. Arya N, Singh U, Singh S. Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm. International Conference on Computer, Communication and Control (IC4), India. 2015. p. 1–5.
13. Biswas S, Nag T, Neogy S. Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET. Applications and Innovations in Mobile Computing (AIMoC), Kolkata, India. 2014; 157–64.
14. Wahane G, Kanthe AM, Simunic D. Detection of cooperative black hole attack using crosschecking with truelink in MANET. IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Zagreb. 2014. p. 1–6.
15. Choudhary N, Tharani L. Preventing Black Hole Attack in AODV using timer-based detection mechanism. International Conference on Signal Processing and Communication Engineering Systems (SPACES), India. 2015. p. 1–4.
16. Sen J, Koilakonda S, Ukil A. A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks. Second International Conference on Intelligent Systems, Modelling and Simulation, India. 2011. p. 338–43.
17. Tsou PC, Chang JM, Lin YH, Chao HC, Chen JL. Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs. 13th International Conference on Advanced Communication Technology (ICACT), Taiwan, R.O.C. 2011. p. 755–60.
18. Balan EV, Priyan MK, Gokulnath C, Devi GU. Fuzzy Based Intrusion Detection Systems in MANET. Procedia Computer Science. 2015; 50:109–14.
19. Manoranjini J, Chandrasekar A, Rajinigirinath D. Hybrid Detector for Detection of Black Holes in Manets. IERI Procedia. 2013; 4:376–82.
20. Mohanapriya M, Krishnamurthi I. Trust Based DSR Routing Protocol for Mitigating Cooperative Black Hole Attacks in Ad Hoc Networks. Arabian Journal for Science and Engineering. 2014; 39(3):1825–33.
21. Babu RM, Usha G. A Novel Honeypot Based Detection and Isolation Approach (NHBADI) To Detect and Isolate Black Hole Attacks in MANET. Wireless Personal Communications. 2016; 1–15.
22. Dorri A. An EDRI-based approach for detecting and elim-

inating cooperative black hole nodes in MANET. Wireless Networks. 2016; 11(1):1–12.
23. Mishra A, Jaiswal R, Sharma S. A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in Ad hoc Network. IEEE 3rd International Conference on Advance Computing Conference IACC. 2013. p. 499–504.
24. Vijaya Kumar K, Somasundaram K. Detection of black hole attacks in manets by using proximity set method. International Journal of Computer Science and Information Security. 2016; 14(3):136–45.
25. Vennila G, Arivazhagan A, Manickasankari N. Prevention of co-operative black hole attack in manet on DSR protocol using cryptographic algorithm. International Journal of Engineering and Technology. 2014; 6(5):2401–05.
26. Arora SK, Vijan S, Gaba GS. Detection and analysis of black hole attack using IDS. Indian Journal of Science and Technology. 2016; 9(20):1–5.
27. Junhai L, Mingyu F, Danxia Y. Black hole attack prevention based on authentication mechanism. 11th IEEE Singapore International Conference on Communication Systems, China . 2008. p. 173–77.
28. Su MY. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Computer Communications. 2011; 34(1):107–17.
29. Shahabi S, Ghazvini M, Bakhtiarian M. A modified algorithm to improve security and performance of AODV protocol against black hole attack. Wireless Networks. 2015; 22(5):1–7.
30. Singh PK, Sharma G. An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, India. 2012. p. 902–06.
31. Amiri R, Rafsanjani MK, Khosravi E. Black Hole Attacks Detection by Invalid IP Addresses in Mobile Ad Hoc Networks. Indian Journal of Science and Technology. 2014; 7(4):401–8.
32. Jhaveri RH. MR-AODV, A Solution to Mitigate Blackhole and Grayhole Attacks in AODBased MANETs. Third International Conference on Advanced Computing and Communication Technologies, India. 2013. p. 254–60.