Asian Journal of Information Technology 15 (12): 1996-2004, 2016
ISSN: 1682-3915

Avoidance of Black Hole Attack in MANET Using Intrusion Detection with Credit Based Ranking Algorithm

[1]K. Mahalakshmi and [2]D. Sharmila
[1]Jay Shriram Group of Institutions, 638660 Tamil Nadu, India
[2]BannariAmman Insitute of Technology, Sathyamangalam,
638401 Tamil Nadu, India

Abstract: Mobile Ad hoc network (MANET) is an infrastructure less multi-hop network which makes it more vulnerable to various security threats. The black hole attack is one of the severe threat that affects the routing in MANET. To prevent this black hole attack, an efficient Intrusion Detection Agent Node using Credit Based Ranking (IDAN-CBR) Model is developed. The IDA node performs the credit value estimation and assign the rank to all nodes in the network at regular interval. Then, Anti-Block hole Mechanism (ABM) is applied to easily calculate the suspicious value of a node along with the anomalous difference between the routing messages transmitted from the node. If the suspicious value of the node is greater than the threshold value, IDAN transmits a block message, notifying all nodes on the network, requesting them to collaboratively avoid the malicious node in the network. The Intrusion Detection Agent Node using Credit Based Ranking (IDAN-CBR) addresses all types of black hole attacks in mobile networks. Simulation is carried out on the factors such as the packet delivery ratio, packet delivery overhead due to black hole attacks, time to identify the black hole attack and black hole attack avoidance rate.

Key words: MANET, intrusion detection agent node, credit based ranking, anti-block hole mechanism, packet

INTRODUCTION

Mobile Ad hoc Network (MANET) is a group of mobile nodes which transmit packets in a multi-hop approach without any centralized network. The mobile nodes perform packet transmission from one end to another end with the mobility of nodes. Hence, a wide range of attack occurs in MANET. Malicious nodes continuously attack the network's accessibility through common techniques such as flooding, black hole and Denial of Service (DoS).

In MANET, the routing is done by various types of protocols. Among these protocols Adhoc On-demand Distance Vector routing (AODV) protocol is the most commonly used because of its high efficiency. But the performance is degraded on the security aspect due to the attack by the malicious nodes. One of the severe attack in AODV is Black hole attack. Hence, in this study, AODV protocol is used as the basic protocol for simulation and the performance is analyzed by applying the proposed credit based ranking procedure and intrusion detection method with this protocol.

The Detection of Black hole Attack scheme using Control Packets (DBA-CP) was designed by Dhaka *et al.* (2015). The control sequence is sent to neighbor nodes and wait for a node's response. Based on the node response the malicious node is identified. Forwarding Assessment based Detection (FADE) (Liu *et al.*, 2013) focused on denial-of-service attack known as gray hole attack through two-hop acknowledgement monitoring with the aim of reducing the false positive and false negative rate. However, the mechanisms to address other colluding malicious router attacks were not concentrated.

The different protocols and secure algorithms have been introduced but it does not have the entirely secured protocols. An efficient algorithm (Ranaa *et al.*, 2015) to detect the collaborative attacks on MANETs is developed. However, it's difficult for determining various compatible collaborative attacks in MANETs. In general, Black hole attack is mainly occurred in the MANET and very difficult to detect which is performed on the network layer. In Ankita, the EBAODV (Enhance Black hole AODV) approach was used in which the leader nodes are used for identifying black hole nodes. The modified AODV (Zamani and Soltanaghaei, 2016) is a type of overhearing backup protocol improves the packet delivery rate and reduced the overhead and delay. However, the other types of attacks like malicious node identification were not addressed.

Corresponding Author: K. Mahalakshmi, Jay Shriram Group of Institutions, 638660 Tamil Nadu, India

MANETs are more susceptible to several routing attacks. An efficient Detection Feature for Wormhole Attacks scheme was introduced by Imran *et al*. (2014, 2015) but it does not construct IDS for MANETs based on RREQ. Kaur and Singh (2014) study, the OLSR protocol was applied to detect the Gray hole attack and Gray hole attack in Wireless Mesh networks.

The Neighbor Defense Technique for Ad hoc On-demand Distance Vector (NDTAODV) routing protocol was designed by Aggarwal *et al*. (2014) for handling the flood attack by using timers, peak value and hello alarm system. However, it does not deal with other types of attacks such as greyhole attack, black hole attack and wormhole attack.

Risk assessment of mobile applications has received greater attention never before with the increasing use of its applications worldwide. Jing *et al*. (2015) study, attacks related to mobile applications and measure for avoiding it was addressed using risk assessment baseline on sensitive information and permission revocation. But channel quality information with respect to mobile applications was not concentrated. A new intrusion detection system based on k-nearest neighbor classification algorithm was designed by Li *et al*. (2014) for improving the intrusion detection accuracy and speed appropriate to the requirement of wireless sensor network intrusion detection.

In this study, an efficient Intrusion Detection Agent Node using Credit Based Ranking (IDAN-CBR) procedure is developed with the objective of addressing black hole and other types of vulnerability attacks. To address black hole and other types of vulnerability attacks in MANET using credit based ranking procedure. Initially, the credit value estimation for effective ranking is carried out in IDA node. Followed by this, the rank is allocated to all nodes in the network at regular interval. By performing the credit value estimation, the selfish nodes are easily identified and removed the black hole attacks. Then the Anti-Block hole Mechanism (ABM) is used to easily calculate the suspicious value of a node according to the anomalous difference between the routing messages transmitted from the node. The malicious nodes are easily identified in MANET by using threshold values.

The black hole attack is a vulnerable attack in wireless ad hoc networks that can occur, especially in case of packet transmission between the mobile nodes. Detection and Prevention System (DPS) was introduced by Imram *et al*. (2015) for identifying black hole attack in MANETs. The DPS node successively monitors RREQs broadcasted by other nodes and detects the malicious nodes. However, it failed to detect and prevent the other types of attacks. The modifications to the AODV protocol used in MANET an algorithm (Choudhury *et al*., 2015) for minimizing the black hole attack and it has minimum delay and congestion in implementing.

The behavior of Blackhole nodes in AODV protocol in NS2 and developed a technique to reduce the black hole node using Triangular Encryption has been selected by Chatterjee and Mandal (2013) due to its minimum computation overhead. However, it does not detect and eliminate black hole nodes. The clustering approach in Ad-hoc On-demand Distance Vector (AODV) routing protocol was designed by Rashmi (2014) for efficient detection and avoidance of black-hole attack in MANETs.

Kumar *et al*. (2013) study, the effects of the black hole attack on mobile ad hoc routing protocols are analyzed based on two protocols namely AODV and Improved AODV. However, the early detection of Black hole attacks was not performed. An efficient algorithm was used by Modi and Gupta (2014) for identifying the malicious node. After identifying the malicious node, it will be detached from the neighboring table, select a different path for secure transmission between the nodes in the network. However, it does not analyze the performance of packet overhead, memory usage and mobility of the nodes.

A method to remove Gray Hole attack was focused on Mehdi Medadian by establishing neighbor nodes. A security solution was developed by Shree and Ogwu (2013) for multiple black-hole attack in wireless mesh networks. However, the RID-AODV protocol improved the network overhead. Elhadi a new intrusion-detection system called Enhanced Adaptive Acknowledgment (EAACK) developed for reducing the packet-dropping attack to improve the security in MANETs (Shakshuk *et al*., 2013). Bar *et al*. (2013), a trust value for every node has been attained depending upon the packet transmitting ability of the node hence it reduces the black hole attacks. This helps in reducing the packet loss and improves the network performance.

Based on the above mentioned methods and techniques, an efficient intrusion detection agent node using the credit based ranking model is developed to avoid the black hole attacks in MANET.

MATERIALS AND METHODS

Mobile Ad hoc Network (MANET) comprises independent mobile nodes without any fixed infrastructure. All mobile nodes considerably transmit

their packets to other mobile nodes in the network within their communication range. During packet forwarding, black hole node cause vulnerability to the routing system and further affect the performance of the network. The main aim of our research work is to easily analyze the occurrence of level of black hole attacks in MANET. When a node need to transmit a packet to a destination, the source node 'S' establishes a route path to destination node 'D' (Fig. 1).

As shown in Fig. 1, MANETs provides the packet transmission to the destination node with the cooperation of movable node. At first, for each packet transmission, the source node sends the route request message to the neighbor nodes to select the route path. The neighbor nodes send the route reply message to source node regarding route to destination. A malicious node gives fake reply to the source node with the shortest path to destination. Due to this fake reply, packet drop (i.e., black hole attack) occurs during the packet transmission between the source and destination. This black hole attack is prevented in the proposed IDAN-CBR procedure using a credit based ranking value and the anti-block hole mechanism. The main section of IDAN-CBR procedure consists of two components such as Credit based Ranking procedure and the anti-block hole mechanism for estimating the suspicious value of a node.

Credit based ranking estimation: The mobile nodes in the ad-hoc network select the appropriate route path for efficient packet transmission from source node to the destination node. Among these normal nodes, the Intrusion Detection Agent (IDA) node is deployed to identify the black hole attack. The number of IDA nodes deployed in the network depends upon the network size. In IDAN-CBR, the agent node estimates the credit value for efficient ranking. The rank is assigned to all nodes in the network at regular interval. Credit value estimation helps to handle the selfish nodes and identify the black hole attacks in MANET.

The credit based ranking procedure performed in IDA node is illustrated in Fig. 2. Initially, the IDA node calculates the credit value of all the mobile nodes in the network periodically. The IDAN-CBR procedure separates the types of routing request through the packet transmission. The credit estimation is formularized as follows:

$$CVE = \{C_1(RREQ), C_2(REQ), ..., C_n(RREQ) \quad (1)$$

In Eq. 1 CVE represent Credit Value Estimation, C_1, C_2....C_n denotes the credit of the routing request in network. The request classification results are used for further updation of credit state in the proposed work. The effect of the updated credit based value improves the ranking process for identifying the black hole attacks in MANET.

Upon the successful classification of the routing request, the updated credit is calculated based on the previous analysis of the routing and the intermediate node reputation status:

$$UpdatedCredit = CurrentCredit + \{RREQ\,from\,(nodes)\} \quad (2)$$

Credit score value is incremented by '1' if the effective selection of routing is performed without any packet drop. Higher the reputation status level, the system efficiently detects the attacks in routing path. Based on the credit score value, the IDA node periodically assigns the rank to all the mobile nodes in the network. The IDA node maintains the routing information of entire nodes in the mobile network. When the source node wants to transmit the packet to a destination node,

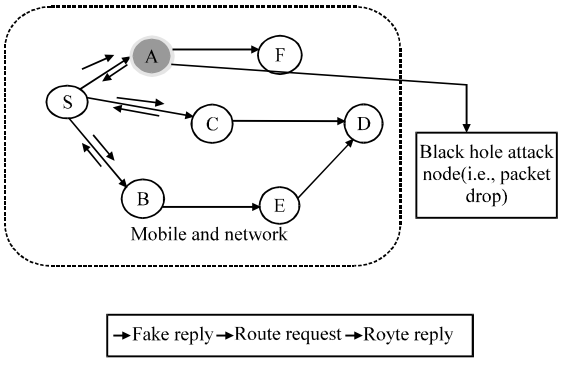

Fig. 1: Black hole attacks of packets transmission in mobile Ad hoc network

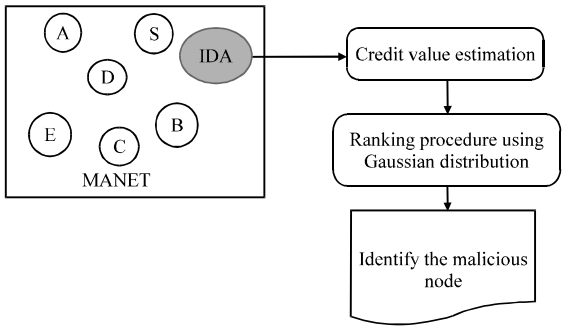

Fig. 2: Flow process of credit based ranking procedure in intrusion detection system

it refers the IDA node that has previously been assigned the rank for each node in the mobile network. Ranking in IDAN-CBR is an efficient algorithm used for ranking the nodes based on the product of the local rank route path of packet transfer and local rank route path of packet depending on previous mobile node position. The previous mobile node position uses the updated credit value to detect the black hole attacks with minimum time. Gaussian distribution function continuously ranks the transmission route path to easily identify the node reputation status. It uses the transfer and break operation in the routing path of the movable nodes for packet transmission. Transfer the packet at time, 't' of nodes is described as:

$$\text{transfer}(SN \rightarrow IN) = \frac{\partial^2 P(t)\,\text{transfer}\ SN(T) \rightarrow IN(T)}{\partial S\ \partial N} \quad (3)$$

In, transfer the packet 'P' from source node 'SN' to 'IN' intermediate node 'at time't'. While transfer the packet, each source node refers the IDA node can periodically transmit the ranking information to all nodes in the network. This helps to easily identify the black hole attack and improves the packet delivery ratio. The break operation is performed to identify the position where the black hole attack occurred. The break point in the route path is formularized as:

$$\text{Break}(IN) = \frac{\partial P(t)\,\text{break}\,N(t)}{\partial N} \quad (4)$$

The break point is where the packet drop occurred (i.e., black hole attack) in IDAN-CBR through the intermediate nodes 'IN' while packet transfer. The packet 'P' break on intermediate node 'IN' is easily identified as black hole attack position in MANET. The algorithmic representation of credit based ranking is described as follows:

Algorithm 1: (credit based ranking algorithm):

Input: Number of nodes, Intrusion Detection Agent (IDA) node
Output: Minimize the black hole attacks
Step 1: For each mobile node
Step 2: IDA node Perform credit value and separates the routing request using (Eq. 1)
Step 3: Updated Credit Value Score is initialized using (Eq. 2)
Step 4: Different node select route path for packet transfer
Step 5: Rank is assigned based on the updated credit value
Step 6: Current Updated credit value and past position of packet transfer through the path is analyzed.
Step 7: Evaluate the packet transfer of mobile nodes using (Eq. 3)
Step 8: Identify black hole attack node using (Eq. 4)
Step 9: Black hole attack on route path is identified
Step 10: End for Step 11: End

The algorithm description reveals that the credit based ranking of each mobile node. Initially, the IDA node performs credit value estimation and assigns the rank to all the mobile nodes in network at regular interval. The ranking is assigned based on current updated credit value and past position of packet transmits through the routing path. While performing the packet transmission, each source node refers the IDA node that transmits the ranking sequence. Subsequently, the packet transmission and black hole attack detection are carried out using the Gaussian distribution function. The transfer operation is evaluated for efficient data transmission from source to destination. The break operation is carried out for identifying the black hole attack with a minimum time interval.

Through the credit based ranking procedure, the IDA node identifies the black hole node. Based on the ranking, the suspicious value of the node is identified and informed to the source node using anti-black hole mechanism. The detailed explanation of anti-black hole mechanism is described in below subsection.

Anti-black hole mechanism: Once the ranking is performed, the anti-block hole mechanism is applied for calculating the suspicious value of a node based on the credit value ranking along with the irregular variation between routing messages (i.e., RREQ and RREP). In this mechanism, the IDA node and other nodes are positioned inside the communication range to forward block messages. The IDA node detects the fake RREP message using the routing table which contains the source sequence number and a destination sequence number. In case of an absence of this access, a new entry is introduced in a route path and the source ID, hop count and RREQ broadcasting messages are copied into the new entry and the ending time is set. Based on the time interval, the RREQ message run over the entire network to arrive at the destination node and the RREP replied back to the intermediate node. In cases of the presence of this entry, the ID of the broadcasting node is added into the Broadcasting nodes field and then, verifies the hop count in RREQ is higher than Maximal hop count of this entry. The AODV routing protocol presets at a time interval clear the irrelevant entries in an RQ table along with the ending time.

When an IDA node detects a RREP message it verifies whether the RREP transmitting node is the destination node, if yes, no action is processed. Otherwise, the source node and destination node in RREP are guided to the request of the RQ table in the following three cases. In the first case, there is no equivalent entry

in the RQ table, it specifies the RREP forwarding node is not within the transmission range of the IDAN that previously transmitted the equivalent RREQ. The entry is introduced in RQ table, the transmitting nodes consist of the RREP forwarding node ID and it states it is a valid reply to RREQ. Finally, the corresponding entry in the RQ table and the broadcasting nodes does not have RREP forwarding node ID and shows it is not a sensible RREP reply.

Block message transmission: The IDA node detects the malicious nodes based on the credit value already evaluated and sends the block message with the details about the malicious nodes to all the nodes in the network at regular interval. It maintains a table for listing the nodes that are suspected to be malicious. The suspicious node (SN) table is shown in Table 1. It contains node id, suspicious value and status of the node. It continuously checks the behavior of all the nodes and if there is any such node and the status is inactive, then the IDA node retransmits this Block message to inform the normal nodes within its transmission range.

When the node is in an active condition then the suspicious value is incremented. If the suspicious value of the node is greater than the threshold value, then IDA node transmits a block message, notifying all nodes to considerably avoid the black hole node in packet forwarding. The flow process of the IDA node block message distribution is showd in Fig. 3.

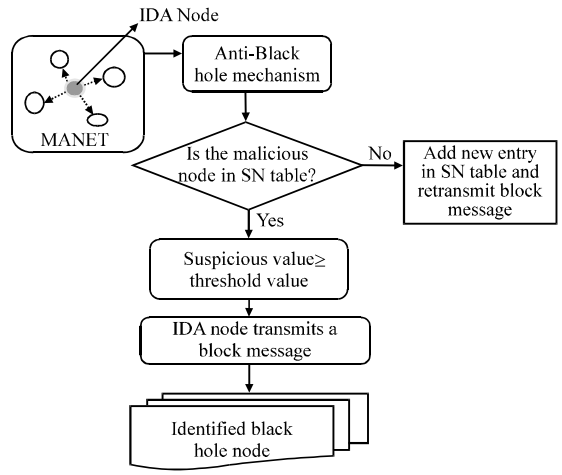

Fig. 3: Flow process of block message distribution

Table 1: SN table

Node ID	Suspicious value	Status
5	2	Inactive
8	6	Active
10	7	Active

The IDA node transmits a block message to inform other normal nodes in its coverage area. All the nodes in the communication range of the IDS node can simultaneously receive this block message. Anti-black hole mechanism is applied to easily measure the suspicious value of a node with the anomalous variation between the routing messages based on rank assigned to each node. As a result, the source node refers the IDA node that transmits the ranking information to all nodes in the network at regular interval. The IDA node communicates with the source node and it intimates there is a black hole node. Thus, the anti-black hole mechanism effectively avoid the black hole node and increases the packet transmission rate.

Experimental settings: An efficient Intrusion Detection Agent Node using Credit Based Ranking (IDAN-CBR) Model is implemented in NS-2 simulator with the network range of 1200×1200 m size. The mobile network consists of 80 nodes in the network structure and uses the Random Way Point (RWM) Model. The RWM uses a typical number of mobile nodes for locating the movable nodes. The dynamic topology uses the Ad hoc On-demand Distance Vector (AODV) routing protocol to perform the experimental work.

Moving speed of the mobiles in MANET for AODV routing framework is about 2.5 m sec^{-1} for each mobile node and the simulation of 30 milliseconds and totally 100 milliseconds are observed to carry out the process of single packet from source to destination end. The parameters and their values for conducting experiments are shown in Table 2. The experiment is conducted on the factors such as packet delivery ratio, time to identify the black hole node, packet delivery overhead and black hole avoidance rate. These parameters result percentage of the IDAN-CBR Model is compared against the existing work such as Detection of Black hole Attack scheme using Control Packets (DBA-CP) (Dhaka *et al*., 2015) and Forwarding Assessment based Detection (FADE) Qiang (Liu *et al*., 2013) mechanism (Table 2).

Table 2: Simulation setup

Parameters	Values
Protocols	AODV
Simulation time	100 s
Number of nodes	10, 20, 30, 40, 50, 60, 70
Black hole nodes	2 (fixed/moved)
Network load	4 packets/sec
Pause time	10 s
Simulation Area	1200×1200 m
Traffic type	Constant bit rate
Minimum	2.5 m sec^{-1}
Maximum speed	10 m sec^{-1}
Mobility model	Random way point
Network simulator	NS 2.34

RESULTS AND DISCUSSION

Experimental data and analysis: To validate the efficiency and theoretical advantages of the proposed Detection Agent Node using Credit Based Ranking (IDAN-CBR) Model with Detection of Black hole Attack scheme using Control Packets (DBA-CP) (Dhaka *et al*., 2015) and Forwarding Assessment based Detection (FADE) (Liu *et al*., 2013) mechanism simulation results under NS2 are presented. The experiment is conducted on the factors such as packet delivery ratio, time to identify the black hole node, packet delivery overhead and black hole attack avoidance rate. Performance is evaluated along with the following metrics with the help of tables and graph values.

Impact of packet delivery ratio: Packet delivery ratio using IDAN-CBR Model is defined as the ratio of umbers of packets sent by source nodes to the number of packets correctly received at the corresponding destination nodes:

$$PDR = \frac{No.of\ packet_R}{No.of\ packet_S} \times 100 \quad (5)$$

From Eq. 8, packet delivery ratio PDR is $packet_R$ number of packets received, $packet_S$ No. of packets sent. It is measured in terms of percentage (%). Higher the packet delivery ratio more efficient the method is said to be.

The simulation values of packet delivery ratio with respect to the number of packets sent is illustrated in Table 3. The convergence plot of seven different values is shown in Fig. 4.

The simulation results of packet delivery ratio based on three methods, namely, IDAN-CBR, DBA-CP (Dhaka *et al*., 2015; Liu *et al*., 2013). From the Fig. 4, it is clear that while increasing the number of packets being sent, the packet delivery ratio is also increased in all the three methods. But comparatively, the proposed IDAN-CBR Model is high. This is because of the credit value estimation through Gaussian distribution function. This function uses the transfer and break operation in the routing path for efficient packet transmission. Each source node refers the IDA node frequently sent the ranking information to other neighboring node in the network. This helps to easily detect the black hole attack and improves the packet delivery ratio. The packet delivery is increased by 6% as compared to existing DBA-CP (Dhaka *et al*., 2015). In addition, the break operation is carried out to identify the position where the black hole attack occurred. As a result, the packet delivery ratio is improved by 9% compared to FADE (Liu *et al*., 2013).

Impact of time to identify the black hole node: The average time in identifying black hole attack is measured using the number of nodes and the time taken to identify the black hole attack during the packet transmission in MANET. The mathematical formulation for average time is as given below:

$$T_{BA} = No.of\ nodes \times Time(identifying\ black\ hole\ attack) \quad (6)$$

From Eq. 9, the time to identify the black hole attack T_A which is measured in terms of milliseconds (ms). In Table 4, the analysis of black hole attack detection time based on the number of node ranges from 10-70 is shown. The targeting results of black hole attack detection time using IDAN-CBR, DBA-CP Dhaka and FADE Liu is shown in the graph.

Figure 5 depicts the simulation results of time to identify the attack with respect to number mobile node in

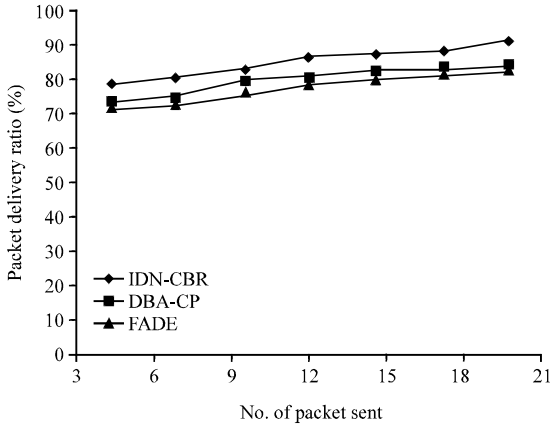

Fig. 4: Measure of packet delivery ratio

Table 3: Tabulation for packet delivery ratio

No. of packet sent	Packet delivery ratio (%) IDAN-CBR	DBA-CP	FADE
3	78.68	73.11	70.25
6	80.38	75.23	72.68
9	83.35	79.68	75.65
12	86.54	80.12	78.56
15	87.25	82.35	80.26
18	88.35	83.25	81.32
21	90.65	84.02	82.62

Table 4: Tabulation for time to identify the black hole attack

No. of node	Time to identify the black hole attack (ms) IDAN-CBR	DBA-CP	FADE
10	0.95	1.25	1.47
20	1.45	1.89	2.12
30	1.98	2.35	2.58
40	2.36	2.87	3.12
50	2.96	3.98	4.13
60	3.89	4.35	4.78
70	4.12	4.86	5.08

MANET. The figure illustrates, our proposed IDAN-CBR Model improved the performance by reducing the time to identify the attacks than the other state-of-art- methods. Based on the credit score value, the IDA node assigned the rank to all the mobile nodes at regular interval. The IDA node maintains routing information of entire mobile nodes in the network. This helps to easily identify the malicious node with minimum detection time of 24% compared to DBA-CP (Dhaka *et al*., 2015). Moreover, ranking is carried out for efficient prediction of the location of the destination node for transmitting the ackets based on the updated credit value and it easily detects the black hole attacks with minimum time of 35% compared to FADE (Liu *et al*., 2013).

Impact of packet delivery overhead: Packet delivery overhead is defined as the average time taken by a data packet to arrive in the destination. The overhead is measured in terms of milliseconds (ms). Lower the packet delivery overhead, more efficient the method is said to be.

The simulation result of packet delivery overhead of IDAN-CBR, DBA-CP (Dhaka *et al*., 2015) and FADE (Liu *et al*., 2013) is shown in Table 5.

In Fig. 6, the targeting results of packet delivery overhead using IDAN-CBR Model with two state-of-the-art methods is presented for visual comparison based on packet sent. The proposed method has lower overhead than DBA-CP and FADE. This confirms the efficiency of the proposed IDAN-CBR Model. The packet delivery overhead is reduced by the effective update of credit state. The effective update of credit performed based on the previous analysis of the routing and the intermediate node reputation status reduces the packet delivery verhead by 28% compared to DBA-CP (Dhaka *et al*., 2015). Due to the Anti-Block hole Mechanism, the suspicious value of a node helps in identifying the abnormal variation between the routing messages. This avoids the data retransmission of source node each time when the packet loss occurs. As a result it avoids the black hole attacks and improves the packet transmission with minimum overhead. The packet delivery overhead is reduced by 37% compared to FADE (Liu *et al*., 2013).

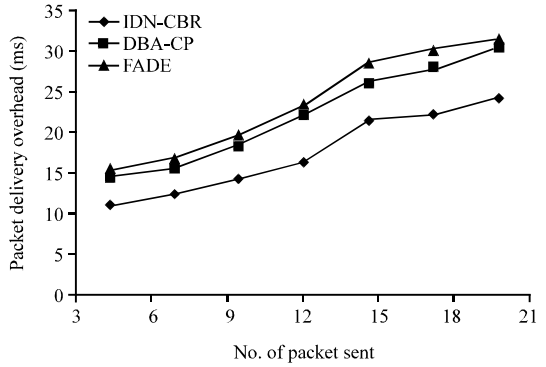

Fig. 5: Measure of time to identify the black hole attack

Table 5: Tabulation for packet delivery overhead

No. of node	Time to identify the black hole attack (ms)		
	IDAN-CBR	DBA-CP	FADE
3	11.24	14.67	15.67
6	12.35	15.67	16.98
9	14.31	18.54	19.68
12	16.21	22.37	23.54
15	21.24	25.92	28.56
18	22.35	28.12	30.27
21	24.32	30.25	31.68

Impact of black hole attack avoidance rate: The black hole attack avoidance rate is measured based on IDAN-CBR, DBA-CP (Dhaka *et al*., 2015) and FADE (Liu *et al*., 2013). The attack avoidance rate is shown in Table 6.

Figure 7 shows the impact of Black hole attack avoidance rate using three methods IDAN-CBR, DBA-CP and FADE. From the figure, it is evident that the attack avoidance rate is improved using Intrusion Detection Agent Node using Credit Based Ranking (IDAN-CBR). This improvement is because of the application of credit rank procedure. During the credit value estimation, the IDA node assigns the rank to all mobile nodes in the network. The source node refers the IDA node to transmit the packet to the other neighboring nodes. This helps to avoid the black hole node and reduces the packet drop. The Black hole attack avoidance rate is increased by 7% compared to DBA-CP (Dhaka *et al*., 2015). In addition, the anti-black hole mechanism is applied in IDAN-CBR

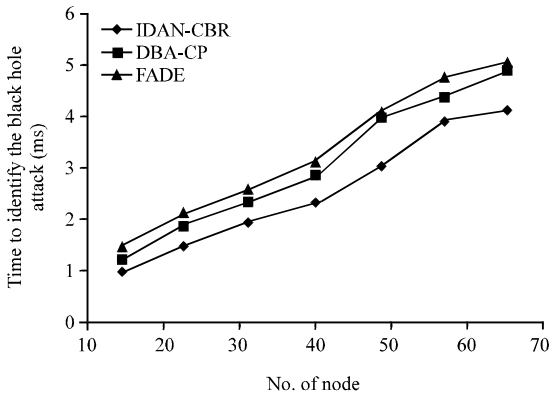

Fig. 6: Measure of packet delivery overhead

Table 6: Black hole attack avoidance rate

Methods	Black hole attack avoidance rate (%)
IDAN-CBR	92.58
DBA-CP	85.67
FADE	80.13

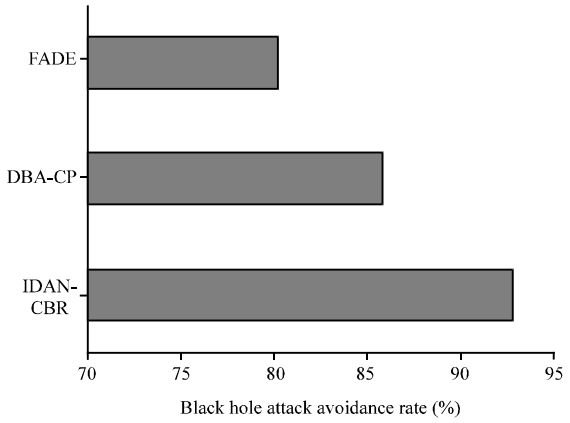

Fig. 7: Measure of black hole attack avoidance rate

for calculating the suspicious value of a node along with the irregular difference between routing messages. When the suspicious value of the node is greater than the threshold value IDA node transmits a block message to all nodes on the network, requesting to collectively prevent the malicious node in MANET. Thus, it improves the black hole attack avoidance rate of 15% more compared to FADE (Liu *et al*., 2013).

CONCLUSION

In this study, an efficient Intrusion Detection Agent Node using Credit Based Ranking (IDAN-CBR) Model is introduced for detecting the black hole attack in MANET. Initially, the IDA node performed credit value estimation using break and transfer operation for ranking the nodes. Credit value estimation based ranking procedure is used to remove the black hole attack and improves the packet delivery ratio. Based on updated credit value, each source node refers the IDA node for transmitting the packet to other nodes in network at regular interval. The Anti-Block hole Mechanism (ABM) is applied in IDAN-CBR for measuring the suspicious value of a node in accordance with the anomalous variation between the routing messages. Finally, the suspicious value of the node is greater than the threshold value, the IDA node transmits a block message to all nodes requesting for detecting the malicious node in MANET. This helps to reduce the packet drop (i.e., black hole attacks) and improves the network performance in mobile networks. The simulation results reveal that the IDAN-CBR mechanism improves the packet delivery ratio and minimizes the packet delivery overhead. Therefore, the IDAN-CBR odel increases the black hole attack avoidance rate with minimum time compared to state-of-art methods.

REFERENCES

Aggarwal, A., S. Gandhi, N. Chaubey, N. Tada and S.Trivedi, 2014. Neighbor defense technique for Ad Hoc On-Demand Distance Vector (AODV) to mitigate flood attack in manets. Intl. J. Comput. Networks Commun., Vol. 6,

Bar, R.K., J.K. Mandal and M.M. Singh, 2013. QoS of MANet through trust based AODV routing protocol by exclusion of black hole attack. Proc. Technol., 10: 530-537.

Chatterjee, N. and J.K. Mandal, 2013. Detection of blackhole behaviour using triangular encryption in NS2. Procedia Technol., 10: 524-529.

Choudhury, D.R., L. Ragha and N. Marathe, 2015. Implementing and improving the performance of aodv by receive reply method and securing it from black hole attack. Procedia Comput. Sci., 45: 564-570.

Dhaka, A., A. Nandal and R.S. Dhaka, 2015. Gray and black hole attack identification using control packets in manets. Procedia Comput. Sci., 54: 83-91.

Imran, M., F.A. Khan, H. Abbas and M. Iftikhar, 2014. Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks. In: International Conference on Ad-Hoc Networks and Wireless. Pineda, G.M., J. Lloret, S. Papavassiliou, S. Ruehrup and C.B. Westphall (Eds.). Springer Berlin Heidelberg, Berlin, Germany, ISBN: 978-3-662-46337-6, pp: 111-122.

Imran, M., F.A. Khan, T. Jamal and M.H. Durad, 2015. Analysis of detection features for wormhole attacks in manets. Procedia Comput. Sci., 56: 384-390.

Jing, Y., G.J. Ahn, Z. Zhao and H. Hu, 2015. Towards automated risk assessment and mitigation of mobile applications. IEEE. Trans. Dependable Secure Comput., 12: 571-584.

Kaur, R. and P. Singh, 2014. Black hole and greyhole attack in wireless mesh network. Am. J. Eng. Res., 3: 41-47.

Kumar, J., M. Kulkarni and D. Gupta, 2013. Effect of black hole attack on manet routing protocols. Intl. J. Comput. Network Inf. Secur., 5: 64-72.

Li, W., P. Yi, Y. Wu, L. Pan and J. Li, 2014. A new intrusion detection system based on KNN classification algorithm in wireless sensor network. J. Elect. Comput. Eng., 2014: 1-8.

Liu, Q., J. Yin, V.C. Leung and Z. Cai, 2013. FADE: Forwarding assessment based detection of collaborative grey hole attacks in WMNs. IEEE. Trans. Wireless Commun., 12: 5124-5137.

Modi, N. and V.K. Gupta, 2014. Prevention of black hole attack using aodv routing protocol in manet. Intl. J. Comput. Sci. Inf. Technol., 5: 3254-3258.

Rana, A., V. Rana and S. Gupta, 2015. EMAODV: Technique to prevent collaborative attacks in manets. Procedia Comput. Sci., 70: 137-145.

Rashmi, A.S., 2014. A novel approach for preventing black-hole attack in manets. Intl. J. Ambient Syst. Appl., 2: 01-09.

Shakshuki, E.M., N. Kang and T.R. Sheltami, 2013. EAACK- A secure intrusion-detection system for Manets. IEEE. Trans. Ind. Elect., 60: 1089-1098.

Shree, O. and F.J. Ogwu, 2013. A proposal for mitigating multiple black-hole attack in wireless mesh networks. Wireless Sensor Network, Sci. Res., 5: 76-83.

Zamani, E. and M. Soltanaghaei, 2016. The improved overhearing backup AODV protocol in MANET. J. Comput. Networks Commun., 2016: 1-8.