

## Detection and avoidance of black-hole attack in mobile adhoc network using bee-ad-hoc on-demand distance vector

Srikanth Pala, Prasad Maddula, Kiran Sree Pokkuluri, Sunil Pattem, Ramachandra Rao Kurada, Ramu Yadavalli

Department of Computer Science and Engineering, Shri Vishnu Engineering College for Women, Bhimavaram, India

### Article Info

#### Article history:

Received Jan 15, 2024

Revised Oct 18, 2024

Accepted Oct 23, 2024

#### Keywords:

Ad-hoc on-demand distance vector

Bee- ad-hoc on-demand distance vector

Bee algorithm

Black-hole attack

Mobile adhoc network

Quality of service

### ABSTRACT

Mobile adhoc networks (MANETs) are self-configuring networks with a dynamic infrastructure suit for real world applications. Due to the exponential increase in the network devices an efficient routing algorithm for dynamic network adhering the security issues is a critical challenge needs to be addressed. This article attempts to address this issue with the implementation of ad-hoc on-demand distance vector (AODV) routing approach, which is the best of its kind in the dynamic network design of MANETs. The primary goal is to address security attack weaknesses through the implementation of dynamic topologies and reactive routing. To this end, a bio-inspired swarm intelligence algorithm called Bees algorithm is used to emulate the AODV technique. In order to provide a lightweight solution that integrates the Bee algorithm and AODV routing, this study presents a unique algorithm called Bee-AODC. The proposed Bee-AODC algorithm possess the both the AODV's dynamic topology construction capabilities and the Bee algorithm's foraging strategy which effectively address security weaknesses by creating a dynamic network topology for ad hoc routing. By using the suggested Bee-AODC algorithm instead of the traditional AODV routing method, throughput is increased by 12.87% while packet loss, latency, and energy consumption are reduced by 20%, 40%, and 18%, respectively.

*This is an open access article under the [CC BY-SA](#) license.*



### Corresponding Author:

Srikanth Pala

Department of Computer Science and Engineering, Shri Vishnu Engineering College for Women  
Bhimavaram, Andhra Pradesh, India

Email: sreekanth.pala@gmail.com

## 1. INTRODUCTION

The global market is marching towards the digitization due to the emerging information and communication technology (ICT) tools [1] where the data seamlessly needs to be transferred digital format for ease of accessibility over the smart devices connected in a wired or wireless approach. In the current scenario the global market is focusing on data transfer using the wireless medium. Wireless ad-hoc networks (WANETs) uses the wireless medium for the data transfer among the heterogeneous static nodes in a network using a centralized infrastructure framework. Mobile adhoc network (MANETs) are the extension of WANETs incorporates the heterogeneous nodes with mobile nature and doesn't bind to the centralized frameworks. MANETs are independent and infrastructure less networks which doesn't maintain a centralized node for controlling and coordinating the different networking nodes. Routing of data from the source to receiver node, a route needs to be established among the nodes by vicinity and coverage between the nodes using the interference range. Routing of data from a source to destination in the MANETs needs to adopt for network topology in a dynamic approach [2].

MANETs are basically deployed in any personal area network for the disaster management, military bases, defense system for monitoring system. MANETs are low power energy equipped devices with limited bandwidth, less computational capabilities with limited hardware resources makes data transfer a challenging issue [3], [4]. An effective routing protocol must handle establishing network link between nodes so that data may be traversed from the source to the destination while utilizing energy resources and avoiding network security flaws. A routing protocol that is effective must convey data in response to dynamic topological changes by modifying the network connection without depleting the battery. An attacker using a passive attack on a network will listen in and take material from the data flow. An attacker engaged in an active attack [5] is eager to collect content that compromises network integrity and attempts to bring the network to a complete stop by reducing its functionality. The black hole attack can use the routing protocol; this issue can be resolved by integrating the bioinspired bee algorithm with the current ad-hoc on-demand distance vector (AODV).

Black-hole attack is an extensive active attack which deteriorates the performance of the network and transforms the existing network to unreliable. This attack consists of a malicious node, which creates an illusion to the network a reliable node for a best route towards the destination node by constantly sending route-reply (R-REP) with highest sequence number. Due to the highest sequence if the data traverses through this node, will never reach the destination node and tends to decrease the throughput and increase the network delay. Real-world applications are well-suited for MANETs, which are self-configuring networks with a dynamic architecture. An effective routing algorithm for dynamic networks that adheres to security problems is a significant topic that has to be solved due to the exponential rise in network devices. By applying the AODV routing technique, the best of its type in the dynamic network architecture of MANETs, this paper tries to solve this problem. The main objective is to mitigate security attack vulnerabilities by utilizing reactive routing and dynamic topologies. In order to do this, the AODV method is imitated by the Bees system, a bio-inspired swarm intelligence system. This work introduces a novel method called Bee-AODC, which combines the Bee algorithm and AODV routing to produce a lightweight solution. The suggested Bee-AODC algorithm successfully addresses security flaws by generating a dynamic network topology for ad hoc routing. It does this by combining the AODV's dynamic topology creation capabilities with the foraging approach of the Bee algorithm.

The overall content of the paper is as mentioned. Section 2 explains the operational functioning AODV routing protocol with black-hole attack. Section 3 describes the review of similar works for this work. Section 4 emphasizes on the methodological implementation. Section 5 focuses on the results obtained. Section 6 illustrates the conclusion with its future scope.

## 2. FUNCTIONING OF AODV ROUTING PROTOCOL WITH BLACK-HOLE ATTACK

Black-hole attack is an attack which is deliberately active in nature where the node tries to deceive the other nodes in the network as an active functional node with minimal distance for the operational destination node. In-order to deceive the source node the black hole node send its routing-table to a source node as a reliable intermediate node. The nodes adjacent to source is drawn into an illusion as the data is traversing to reliable node with minimal distance to the destination node. Subsequently the illusion is created for the operational-nodes in this network, try to send the data through this node but needs to identified as a black hole node. Black-hole node receives all the data packets from the distinguished nodes in that network acting as reliable intermediate node for their data traversal from its source to the destination. Black-hole node instead of forwarding the packets, discards the packets in the network, may lead to the increase in network traffic and creating a congested network will collapse total network. Data-transmission from source node to the destination node actually initiates with a request message from the source node to neighboring nodes with in its vicinity range. Source node after receiving an acknowledgement for its request by the routing tables from its corresponding neighbor nodes in regards the destination node. Source node forwards the data packets to its corresponding neighbor nodes to traverse to its appropriate destination. Black-hole node creates an illusion to its corresponding nodes as a reliable node and receive the packets from its neighbor and discards the received packets from the source node. Ideally the categorization of the black-hole is based upon its functional operation, single attacker node operating individually and co-operative black-hole attack where attacker is operated collectively with other functionally active nodes. Black-hole attack degrades the performance of the network throughput [6], [7] losses the reliability of the network and finally communication system it totally collapsed. The Figure 1 specifies the black-hole attack in MANETs, data packets need to be routed from the source 'S' to the destination 'D' but the intermediate node 'B' will be a black hole node and it drops all the packet before reaching to the destination.

### 2.1. Ad-hoc on-demand distance vector routing protocol

AODV is reactive routing protocol used in MANETs, combines the functioning of re-active and pro-active routing protocols like dynamic source routing (DSR) and destination sequenced distance vector

(DSDV). AODV is having better performance metrics [6], [7] when compared to the other reactive routing protocol DSR. AODV [8] uses two control messages route-request (R-REQ) and R-REP for the connection establishment from the source to the destination. In the context of connection establishment, the source node broadcasts the R-REQ control message to all of its adjacent nodes and the intermediate nodes forwards the control messages to destination node. The destination node acknowledges the intermediate nodes with reply message R-REP for the request message it has received. Source node upon receiving the reply message from the destination node stops broadcasting of the request messages to its adjacent nodes. The performance of the protocol degrades as the intermediate node are vulnerable for attacks like black-hole attack. Black-hole attack significantly affects the network performance metrics like the packet-delivery-ratio, throughput, end-to-end delay.

## 2.2. Challenges

The basic issue needs to be addressed in any network is the scalability [9] problem. If the nodes of the network 'n' increases, then the the throughput of the network decreases in the  $1/\sqrt{n}$  percentage. Here the basic 'n' value depends upon the the simulation conducted squared area. AODV is one of the efficient reactive routing protocols for the connection establishment from the source to destination. It finds a shortest optimal path for the communication by maintaining the decent security standards. Black hole is the one of the popular attacks aims to prevent the communication between the nodes. AODV aims on connection establishment for effective routing between the nodes but not focuses on identifying the black hole attack in the network. This paper focuses on the improving the AODV algorithm in detection and prevention of the black hole attack using the bio-inspired techniques like Bee's algorithm [10]. A swarm intelligence algorithm like Bee-AODV used for developing a dynamic network topology aims on black hole attack.

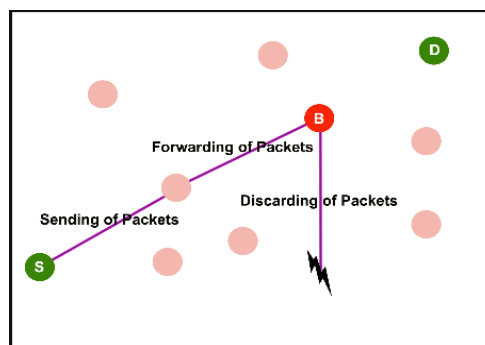


Figure 1. Black-hole attack in a network

## 3. LITERATURE REVIEW

This section discusses about the detection and prevention of black-hole attack in the MANETs. The characteristics of the node and deployment of the nodes in the network exploits the vulnerability of the network are liable for the black-hole attack. This section clearly emphasizes the role of bio-inspired algorithms for detection and prevention of black-hole attack in MANETs. Nodes in MANETs are low power energy equipped devices, there is a need for the time synchronization process among the nodes for the proper end-to-end delay among the nodes. A secure synchronization protocol is always robust from the attacks. AODV to be robust there is higher importance for time-to-live (TTL) for the synchronization among the control messages R-REQ and R-REP. Kalia and Sharma [11] specifies a new baiting technique developed by the source routing node itself. RREQ control message consisting of the source-id and source sequence number (SSN) is broadcasted to all adjacent nodes in the respective network. The black node in the corresponding network responds with R-REP with a destination sequence number (DSN) greater than the SSN but there is no such node in this group greater the specified SSN which the source-node is aware of it. Then source node signals alert message by raising an alarm to all the neighboring nodes regarding the effected node. Initial limitation with this technique is, there is a possibility assuming that effected node is not smart enough. If it is a smart black hole node, then it recreates the source node as attacker node and source node itself blacklisted by all the other nodes in the network.

Alotaibi [12] proposed a co-operative bait detection scheme (CBDS) consisting of the three phases baiting-phase, reversing trace and defending reactively. In the phase of baiting, the source-node randomly identifies an adjacent node and send a request using its id. In the second phase source basing upon R-REP

received for its corresponding R-REQ then it creates a list of suspicious nodes in the network and source converts into promiscuous node for identification of the attacker nodes. The source node in the promiscuous mode raise a black hole alarm all of its neighboring nodes of the attacker node, as it is in the promiscuous mode neighbor nodes may not receive the alarm from it. In the third phase source node will check the throughput of the suspicious node, if less than the threshold then once again the baiting phase is applied. A smart black-hole node will raise a false alarm message and makes authenticated nodes also to isolate from the network. The source nodes send a fabricated request to assuming that node as a black-hole node, if that corresponding node responds the R-REQ. Source node maintains the average value of DSN, if any node acknowledges with R-REP for corresponding R-REQ for the source node verifies the DSN value it has obtained. The source node checks the DSN if it closes to average DSN the source node treats as black-hole node or else as a normal node. Here the it uses digital signature for authentication in identifying the black-hole node [13].

Dhende *et al.* [14] proposes a SAODV protocol for identifying the black-hole and gray-hole node basing on opinion of the neighboring nodes. In this technique each node maintains two tables neighbor-list (NL) and opinion-list (OL). Here the source node generates R-REQ message for connection establishment to the destination node. Source node upon receiving the reply message for the corresponding request message from any of its neighboring node then source node broadcast opinion message claiming that this node shortest path to the destination. The rest of neighboring nodes responds with YES or NO message. If remaining nodes responds with NO message then source node claims that node as a black-hole node and raises a black-hole alarm in the network, if responded YES message it is claimed as a normal node, else responded with both YES and NO messages then it is claimed as a Gray-Hole node [15], [16].

Due to the excessive transmission of control messages between the source and neighboring nodes the control overhead increases in the network, leads to congestion in the network which affect the quality of service (QoS) metrics. Detection and isolation of the black-hole node in network using the AODV routing protocol can be achieved by the various techniques [11]–[14]. Mostly all the techniques use the DSN for the effective route establishment from the source to the destination, but always a black-hole node claim with a highest DSN. Watch-dog techniques have been employed for the forwarding of the packets and followed by some truth-based algorithms in identifying the normal nodes and black hole nodes. So, there is need for the proper correlation between the sender request message with neighbor's response message. Therefore, in all the above-mentioned techniques there is need of proper time synchronization techniques are needed for the request and response packets in identifying the path as well as the malicious nodes black-hole nodes in that network.

Bio-inspired algorithms for optimization take reference from the networked aggregate behavior of living species, namely insects and animals, in addition to the principles of natural evolutionary processes in order to determine the most effective approaches for challenging and complex optimization problems [17]. From the work of [18] researchers are driven to seek for and develop efficient methods for discovering and enhancing the solutions of complex and optimization problems by the increasing complexity of real-world problems. In computing, one of the more renowned evolutionary-based techniques is the genetic algorithm (GA). Stochastic search techniques referred to as evolutionary-based algorithms (EA) simulate the communal dynamics and natural evolutionary processes of living things, encompassing recombination, mutation, and adaptation in reproduction. Massive optimization problems can go above the reach of standard mathematical techniques; in such instances, EA have been created to identify the optimal or nearly optimal response of swarm intelligence is concerned with developing intelligent, dynamic systems with multiple agents that cooperate to achieve a common goal that is outside the abilities of a single agent. Especially comparing to other traditional methods, bio-inspired optimization algorithms exhibit outstanding variance, resilience, flexibility, level of complexity, and unique events, which have contributed to their developing are attractive in the realm of computation. The basic steps for identifying the malicious node in the network using the literature review conducted as follows:

- a) Initially a back-bone network is created, the source node raises a request for unused restricted IP. Backbone networks searches for the new unused network IP and forwards it to the source node [11], [12].
- b) Request initiated from the source-node for the data transmission to its respective destination using a restricted IP generated by the back bone network.
- c) Destination node upon receiving the request from the source node, it enters IP address in the routing table send back to source node. Upon establishing the link, the source will initiate the further transmission of data between the nodes [19].
- d) If the node accepting the data is not destination node, then it forwards neighboring nodes by making it IP entry in the routing table. Source node only responds and sends the data only if it is a destination node. But if response obtained from the destination having a restricted IP address, then it starts sending the dummy messages for identifying the malicious node.
- e) Sender node initiates a caution alert notes to its neighbors to enter into a safe zone and to keep a track of the maliciously effected node. If the source node obtains a DSN value greater than the threshold value for the dummy message it has generated [11]. The source nodes generate a black hole alarm to all the

neighboring nodes and tries to determine a new safe and secure path to the destination. Thereby increasing the throughput of the network and decreasing the end-to-end delay.

#### 4. PROPOSED RESEARCH

The initial random population is utilized by the bee life algorithms to populate the area of search. A colony of bees includes 'W' workers, 'D' drones, and '1' queen. The two distinct bee behaviors which make up every algorithm cycle include searching for food and reproduction. In reproduction, the fitness of the broods is determined after generation 'N' broods by mutation and crossover. The fittest brood succeeds the queen for a subsequent population if it is a better fit than the queen. Then, using the 'D' fittest drones and broods of the current colony, the 'D' best bees are chosen to produce the next generation of drones. 'W' best bees are then chosen from the 'W' fittest surviving hovers and workers of the current community to ensure food gathering; if otherwise, the algorithm is aborted. When it comes to food foraging behavior, 'W' workers in 'W' regions look for sources of food first. subsequently bees are chosen for neighborhood searches in each location. The fittest bees in each location will be chosen to create the following bee population, and its fitness will be evaluated. If the halting requirement is not met after these two bee behaviors, a new bee life cycle is carried out; if not, the algorithm is terminated. The protocols use the Bee's behavior in solving the surviving the fittest function in identifying the black-hole attack. BeeAdhoc [20] routing algorithm, that borrows its clues from honey bee foraging behavior, is intended for use in mobile ad hoc networks. It functions as an energy-efficient reactive source routing algorithm. To find new pathways and move data from source to destination, the algorithm uses scouts and foragers, respectively involves the following steps as shown.

- Step 1 Route-discovery: A forward-looking scout is broadcast to each neighbor of a node with an increasing TTL when a route for a destination is needed. Down until the point of destination, intermediate nodes append their addresses to the scout's source route.
- Step 2 Backward-scout: The target node gives back the scout to source route for configuring the backward scout after the forward scout reaches at the destination. The source receives this backward scout afterwards.
- Step 3 Route-advertisement: The backward scout notifies subsequent foragers regarding the route after finding its way returning to the initial node.
- Step 4 Data-transport: Data routed to the target node by foragers using a dance metaphor as an aid. To determine the dancing number, suggesting standards of the routing path, alongside gathering the routing data

Mazhar and Farooq [21] have specified the above framework, BeeSec, a secure alternative of BeeAdHoc which enables the use of digital signatures based on asymmetric cryptography. Scouts and foragers in BeeSec rely on digital signatures which have been generated using various parameters such as source and destination addresses, packet IDs, and routing information. Additionally, the source route's integrity is preserved to make sure that malevolent nodes can't eliminate legitimate nodes from the path. As a result, BeeSec successfully thwarts attempts to tamper with or fabricate attacks in BeeAdHoc and counters attacks directed towards the routing. The pseudocode of the basic Bee-algorithm.

##### Pseudo-Code for Basic Bee-Algorithm

Initialization: Population is assigned with Random Solutions

Fitness function evaluation

Repeat-until (Stopping criteria is met)

1. Choose the sites for neighborhood-search
2. Recruit the Bees for chosen sites
3. Choose the fittest Bee from each site
4. Assign the Bees for random search

End-repeat

Detection mechanism needs to protect the data both in rest and transmission state, data protection in the rest state is a likely approach. If malicious node enters into the network, it is likely to destroy the data and manipulate the network heuristics to increase the network traffic. So, there is a need for the network surveillance system to defend the forthcoming attacks in the network. Identification of the effected node in the MANETs is shown in Figure 2 basing on the network incoming traffic module, root node for increasing in the network load with traffic inception module, analysis module with event generation for identification of the node. On simulating the Bees approach to the network for identifying the malicious node, whenever food is

needed, the scout bees from each node are sent to the nectar area to search for it. Scout bees were sent out to collect data in the nectar area, which resulted in obtaining of the node's routing information. The scout bees gather data regarding the nodes they have visited, including the distance and time delay. The movements that the scout bees conducted in the hive upon getting back are shared along with this information. Besides having access to information from the paths they have already walked, the scout bees also carry information from neighbor nodes to the next node. Research refers to the scout bees that transmit this data as "accumulator scout bees." The pseudocode of the elimination of malicious node.

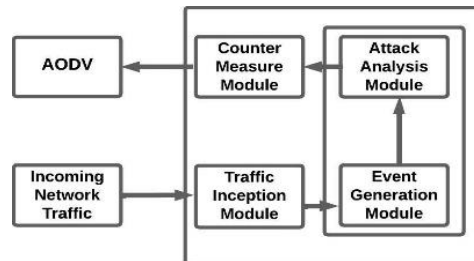


Figure 2. Approach for identifying black-hole attack

Pseudo-code of elimination of Malicious Node

Step 1: Identification of Malicious Node

1.1: Adding Malicious Node to the Cluster Head in the routing table

Step 2: Broadcasting the Malicious node to all the Cluster Heads in the MANET Network

Step 3: Cluster Head Broadcast list to all the Nodes in its Region

Step 4: Drops the Packets Received from the Malicious Node

The neighborhood search of every element is obtained by the solution vector consisting of routing table for each node  $X_i$ ,  $X_{pi}$  is the solution vector and 'ngh' is the radius where the neighborhood is obtained is range of the transmission of the node is shown in the (1).

$$X_{pi} = (x_i - ngh) + 2 * i * ngh \quad (1)$$

On reaching the specific condition the loop gets terminated through the neighborhood searches signifies it. The propose Bee-AODV algorithm.

Algorithm: Bee-AODV

Initialize: n - number of paths available

Repeat -Until (termination condition)

1. Select 's' number of paths from the source to the destination
2. Choose 'e' from the 's' having minimum distance from the source to destination
3. nsp: Number neighborhood searches performed around 's' in identifying the black-hole nodes
4. nep: Number neighborhood searches performed around 'e' in identifying the black-hole nodes
5. Identify the best path among the 's' and 'e' i.e nep>nsp
6. Select the remaining 'n-s' paths and verify whether the paths exists from source to destination and just cumulate to 's'

End-Repeat

## 5. RESULTS AND DISCUSSION

The discussion can be made in several sub-sections. The research findings consist of the qualitative and quantitative research metrics [22] that involves the three techniques from mathematical, experimental and simulation approaches [23], [24]. Here the simulation approach is chosen for the inferential conditions. Quantitative approach involves a series of experiments to be conducted at different situations consisting various network sizes, transmission range, interference range, number of black-holes in determining the efficient route from the transmitter to its respective delivery node. All these factors have a greater impact on the QoS metrics

like throughput, network delay, packet-delivery ratio and energy utilized by the nodes in the network-region. This research uses network-simulator version 2 (NS-2) simulator towards setting up the simulation environment of proposed work and evaluation with QoS metrics.

### 5.1. Network-simulator version 2

NS-2 [25] is an open-source simulator work on discrete event driven approach which is highly accustomed for the most of the communication protocols in the network stack. The characteristic features of the NS-2 simulator include:

- As it is discrete event simulator which supports the new designs for the existing communication protocols.
- A sustainable comparative study of the new protocols with the existing protocols in performance metrics for enhancing the quality of routing in the network.
- NS-2 is a unix based system uses the tool-command-language (TCL) and object oriented tool-command-language (OTCL). TCL can be flexibly integrated with any of the platform, so the protocol specification is really flexible.

### 5.2. Parameter for the simulation

In this study, NS-2 is used for the performance analysis of QoS metrics on the normal AODV [26] and Bee-AODV routing protocol for the black-hole attack. Simulation is conducted for 10, 20, 30, 35 nodes, simulation area of 1000\*1600 meters, transmission range of 250 meters, and simulation of 150 seconds. The parameter used in the article is shown in Table 1.

Table 1. Simulation parameters	
Specification parameters	Standards
Protocol	AODV routing protocol
Simulation-time	150 seconds
Mode-speed	40 meters/second
Size of network (nodes)	10, 20, 30, 35 nodes
Area of simulation (quad)	1000 × 1600
Type of traffic	Constant-bit-rate (CBR)
MAC-type	802.11
Size of packet	512 Bytes
Simulator	Network simulator

The main objective of accumulators, which boost network resource productivity, is to decrease the number of scout bees that have travelled over the network. The scout bees in the network increases can cause to the network infringement due to overlapping of the transmission range and interference range of the scout bee nodes. The control request (HELLO-Req) message from the scout bees leads to the network congestion.

AODV protocol on implementation the HELLO message is broadcasted to neighboring nodes as the R-REQ will acknowledge R-REP by its neighboring nodes for the corresponding source node. In case if no notification is obtained for its corresponding for HELLO packet the link failure notification [27] is obtained, upon obtaining the response then a bi-directional connectivity will be established. Local connection management will maintain a routing table consisting of the address of the both nodes and identification number. Link failure notification is determined by TTL for every corresponding HELLO packet given by the source node.

### 5.3. Parameter for the Simulation

The AODV routing protocol is reasonably affected by QoS metrics, and the black hole attack deteriorates the routing protocol's performance in MANETs. The throughput, energy consumption, packet loss, and latency are the elements influencing performance. All of these indicators' performance analyses are contrasted at networks of 10, 20, 30, and 35 nodes, in varying sizes. After impacted nodes in that network region are removed, an analysis is conducted comparing the performance of AODV with Bee-AODV.

#### 5.3.1. Packet loss

Packet loss measures the number of the acknowledgement received from the receiver, used to justify the reliability of the protocol. Loss of packets simply signifies the number of the packets received at receiver for the number of the packets send by the sender, here we are using the sequence number for every HELLO in identifying the number of packet. The packet loss ratio [28] is signified as the drop ratio in (2).

$$\text{Drop Ratio} = \frac{\text{Number of Packets Dropped}}{\text{Packets Send+Forwarded packets+packets dropped}} \quad (2)$$

The Figure 3 packet loss for the AODV routing protocol in the black-hole attack at different intervals in pause time for every 10 seconds, the bytes/sec specifies that the number of the data in the bytes is lost. The percentage of the packet loss compared to normal AODV to Bee-AODV is reduced in the network with different range of nodes.

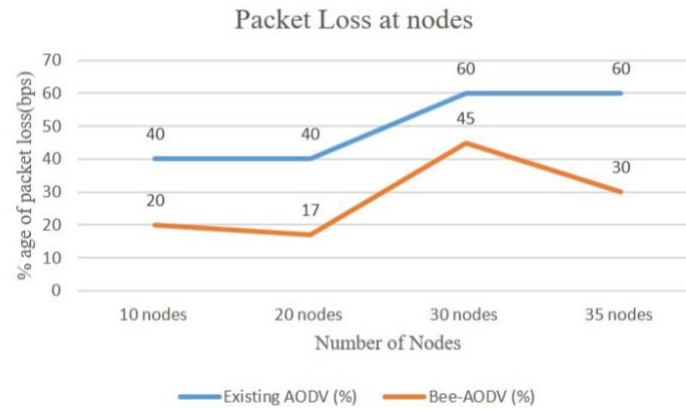


Figure 3. Packet loss comparison in percentage between AODV and Bee-AODV

### 5.3.2. Throughput

Throughput in routing protocol signifies the number of traffic packets that each node in the network receives over a certain time interval and is measured in megabytes (Mbps). Every possible delay observed while transmitting the data packet from the source node to the destination nodes is included in the average end-to-end latency [29].

$$\text{Throughput} = \sum_{n=1}^{\text{Nodes}} \left( \frac{\text{packets delivered} * \text{average packet size (MB)}}{\text{Total Packets send}} \right) \quad (3)$$

The throughput at different pause time and simulations for AODV routing protocol in the black-hole attack with percentage of improvement in throughput when compared with normal AODV routing protocol to the Bee-AODV routing protocol is shown in the Figure 4.

### 5.3.3. End-to-end delay

End-to-End delay clearly specifies the average time taken for the transmission of the data packet from the source to the destination. Delay includes factors like the transmission time, waiting time, receiving time [30].

$$\text{Delay} = \sum_{i=1}^{\text{Node}} \text{Transmission time} + \text{Receiving time} + \text{Waiting Time} \quad (4)$$

The percentage improvement in the delay when compared normal AODV with Bee-AODV routing protocol is shown in the Figure 5. The graph clearly signifies that Bee-AODV clearly reduces the end-to-end delay in comparison with the normal AODV routing protocol. As Bee-AODV aims in elimination of the malicious nodes, definitely improves the end-to-end delay between the source to the destination.

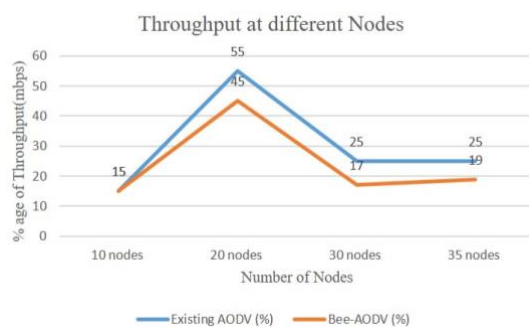


Figure 4. Throughput comparison in percentage between AODV and Bee-AODV

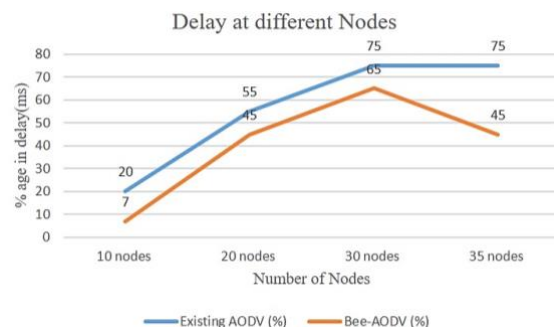


Figure 5. End-to-end delay comparison in percentage between AODV and proposed Bee-AODV



### 5.3.2. Energy-consumed

Energy-consumed [31] is significant factor for enhancing the performance. As the MANETs low power energy equipped devices there is need for the energy optimization. Energy consumed consists of the total energy required for dissemination of the data packet from the initial to the target node, receiving energy for acquiring the data at target node and waiting energy at intermediate nodes.

$$\text{Energy Consumed} = \sum_{i=1}^{nodes} \text{Total Energy} + \text{Receiving Energy} + \text{Waiting Energy} \quad (5)$$

The energy consumed in percentage compared to conventional AODV to Bee-AODV routing protocol is shown in Figure 6. Here also the graph clearly signifies the improvement in the energy consumption when compared with the conventional AODV to Bee-AODV routing protocol. The overall performance of parameters on average analysis of the conventional AODV routing protocol compared with the proposed Bee-AODV routing protocol is shown in Table 2. It is clearly inferring from the performance metric analysis that the proposed Bee-AODV routing protocol performs better than conventional normal AODV routing protocol in all the parameters like packet loss, end-to-end delay, and energy-consumption.

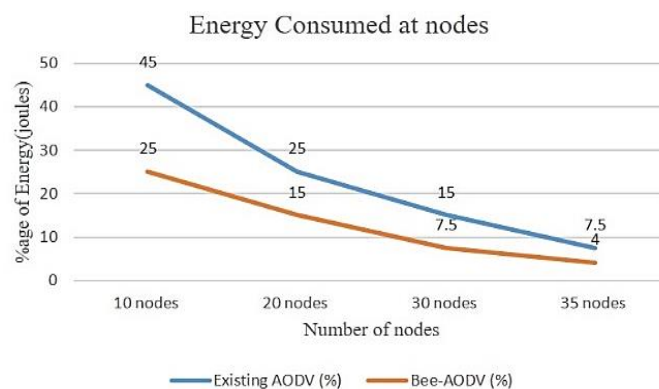


Figure 6. Energy consumed comparison in percentage between AODV and proposed Bee-AODV

Table 2. Performance comparison of conventional AODV and proposed Bee-AODV protocol

Parameter protocol	Packet loss (%)	End-to-end delay (%)	Throughput (%)	Energy consumption (%)
Conventional AODV	50	56.25	40	23.125
Proposed Bee-AODV	20	40.5	18	12.875

## 6. CONCLUSION AND FUTURE SCOPE

The research work aims for identification of malicious node in the network and to counteract for the black-hole attack in AODV routing protocol. AODV routing protocol integrated with bioinspired bee algorithm (Bee-AODV) not only enhances the security but also out rates the performance of normal AODV routing protocol in the QoS metrics. The proposed Bee-AODV routing algorithm decreases the packet loss, delay, and energy consumption by 20%, 40.5%, and 12.875%. The throughput is improved on 18% but not a reasonable improvement compared to normal AODV routing protocol. Thus, the article justifies the use of conventional AODV protocol mimicked with bee algorithm, identified and removed the number of black-holes while establishing a safe path by redirecting the attacking nodes. A further research can be carried out in the future using soft computing techniques for enhancing the QoS metrics of the AODV.




## REFERENCES

- [1] X. H. Wang *et al.*, "The role of E-leadership in ICT utilization: a project management perspective," *Information Technology and Management*, vol. 24, no. 2, pp. 99–113, 2023, doi: 10.1007/s10799-021-00354-4.
- [2] A. Yasin and M. A. Zant, "Detecting and isolating black-hole attacks in MANET using timer based baited technique," *Wireless Communications and Mobile Computing*, vol. 2018, 2018, doi: 10.1155/2018/9812135.
- [3] S. Mirza and S. Z. Bakshi, "Introduction to MANET," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 1, pp. 17–20, 2018.
- [4] K. K. Kommineni and A. Prasad, "A review on privacy and security improvement mechanisms in MANETs," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 2, pp. 90–99, 2024.
- [5] V. Goyal and G. Arora, "Review paper on security issues in mobile Adhoc networks," *International Research Journal of Advanced Engineering and Science*, vol. 2, no. 1, pp. 203–207, 2017.




- [6] S. Akourmis, Y. Fakhri, and M. D. Rahmani, "Protecting AODV protocol from black hole attack in WSN," *Preprints Engineering*, vol. 1, p. 6, 2023, doi: 10.20944/preprints202306.2186.v1.
- [7] R. Agrawal *et al.*, "Classification and comparison of ad hoc networks: A review," *Egyptian Informatics Journal*, vol. 24, no. 1, pp. 1–25, 2023, doi: 10.1016/j.eij.2022.10.004.
- [8] A. K. S. Ali and U. V. Kulkarni, "Comparing and analyzing reactive routing protocols (AODV, DSR and TORA) in QoS of MANET," in *2017 IEEE 7th International Advance Computing Conference (IACC)*, 2017, pp. 345–348, doi: 10.1109/IACC.2017.0081.
- [9] A. Shrestha and F. Tekiner, "On MANET routing protocols for mobility and scalability," in *2009 International Conference on Parallel and Distributed Computing, Applications and Technologies*, 2009, pp. 451–456, doi: 10.1109/PDCAT.2009.88.
- [10] Z. Wang, H. Ding, B. Li, L. Bao, and Z. Yang, "An energy efficient routing protocol based on improved artificial bee colony algorithm for wireless sensor networks," *IEEE Access*, vol. 8, pp. 133577–133596, 2020, doi: 10.1109/ACCESS.2020.3010313.
- [11] N. Kalia and H. Sharma, "Detection of multiple black hole nodes attack in MANET by modifying AODV protocol," *International Journal on Computer Science and Engineering*, vol. 8, no. 5, pp. 160–174, 2016.
- [12] B. Alotaibi, "A survey on industrial internet of things security: requirements, attacks, AI-Based solutions, and edge computing opportunities," *Sensors*, vol. 23, no. 17, 2023, doi: 10.3390/s23177470.
- [13] M. Sathish, K. Arumugam, S. N. Pari, and V. S. Harikrishnan, "Detection of single and collaborative black hole attack in MANET," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2016, pp. 2040–2044, doi: 10.1109/WiSPNET.2016.7566500.
- [14] S. Dhende, S. Musale, S. Shirbahadurkar, and A. Najan, "SAODV: Black hole and gray hole attack detection protocol in MANETs," in *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2017, pp. 2391–2394, doi: 10.1109/WiSPNET.2017.8300188.
- [15] M. S. Abood, H. F. Mahdi, M. M. Hamdi, O. J. Ibrahim, R. Q. Mohammed, and S. F. Ahmed, "Black/gray holes detection tools in MANET: comparison and analysis," in *2020 IEEE 7th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, 2020, pp. 1–8, doi: 10.1109/ICETAS51660.2020.9484203.
- [16] A. Abdelhamid, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, "A lightweight anomaly detection system for black hole attack," *Electronics*, vol. 12, no. 6, 2023, doi: 10.3390/electronics12061294.
- [17] R. Yadav, I. Sreedevi, and D. Gupta, "Bio-inspired hybrid optimization algorithms for energy efficient wireless sensor networks: a comprehensive review," *Electronics*, vol. 11, no. 10, 2022, doi: 10.3390/electronics11101545.
- [18] J. H. Holland, "Genetic algorithms and adaptation," in *Adaptive Control of Ill-Defined Systems*, Boston, MA: Springer, 1984, pp. 317–333, doi: 10.1007/978-1-4684-8941-5\_21.
- [19] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," *Experimental Protocol for the Internet Community*, Jul. 2003, doi: 10.17487/rfc3561.
- [20] J. Wang, Y. Cao, B. Li, H. Jin Kim, and S. Lee, "Particle swarm optimization based clustering algorithm with mobile sink for WSNs," *Future Generation Computer Systems*, vol. 76, pp. 452–457, 2017, doi: 10.1016/j.future.2016.08.004.
- [21] N. Mazhar and M. Farooq, "Vulnerability analysis and security framework (BeeSec) for nature inspired MANET routing protocols," in *9th annual conference on Genetic and evolutionary computation*, 2007, pp. 102–109, doi: 10.1145/1276958.1276973.
- [22] B. T. Khoa, B. P. Hung, and M. Hejsalem-Brahmi, "Qualitative research in social sciences: data collection, data analysis and report writing," *International Journal of Public Sector Performance Management*, vol. 12, no. 1–2, pp. 187–209, 2023, doi: 10.1504/IJPSPM.2023.132247.
- [23] T. Eldabi, Z. Irani, R. J. Paul, and P. E. d. Love, "Quantitative and qualitative decision-making methods in simulation modelling," *Management Decision*, vol. 40, no. 1, pp. 64–73, 2002, doi: 10.1108/00251740210413370.
- [24] S. Moss and B. Edmonds, "Sociology and simulation: Statistical and qualitative cross-validation," *American Journal of Sociology*, vol. 110, no. 4, pp. 1095–1131, 2005, doi: 10.1086/427320.
- [25] K. Fall and K. Varadhan, "The ns manual (Formerly ns notes and documentation)," *The VINT project*, no. 3, 2011.
- [26] H. Ghaffarian and M. Sadeghizadeh, "Parsim : A parametric simulation application for wireless sensor networks based on NS2 simulator," *International Journal of Nonlinear Analysis and Applications (IJNAA)*, vol. 14, no. 1, pp. 2603–2616, 2023.
- [27] S. Sarkar and R. Datta, "AODV-based technique for quick and secure local recovery from link failures in MANETs," *International Journal of Communication Networks and Distributed Systems*, vol. 11, no. 1, pp. 92–116, 2013, doi: 10.1504/IJCND.2013.054858.
- [28] P. Gupta and P. Bansal, "Packet drop analysis with variation in area and number of nodes in MANET," *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology*, vol. 11, no. 1, pp. 9–16, 2019, doi: 10.18090/samriddhi.v11i01.2.
- [29] T. Høiland-Jørgensen, B. Ahlgren, P. Hurtig, and A. Brunstrom, "Measuring latency variation in the internet," *CoNEXT 2016 - Proceedings of the 12th International Conference on Emerging Networking EXperiments and Technologies*, pp. 473–480, 2016, doi: 10.1145/2999572.2999603.
- [30] R. Kango, N. Jamal, and M. I. Abas, "Analysis of end-to-end delay video conferencing services on a mobile ad hoc network," *Journal of Informatics and Telecommunication Engineering*, vol. 6, no. 2, pp. 393–402, 2023, doi: 10.31289/jite.v6i2.8231.
- [31] V. Dattana and P. K. Krishna, "Optimizing routing in MANETs with energy conservation," *International Journal of Applied Engineering and Management Letters*, pp. 75–87, 2023, doi: 10.47992/ijaeml.2581.7000.0189.

## BIOGRAPHIES OF AUTHORS






**Srikanth Pala**    holds a Ph.D. degree in Computer Science Engineering from Andhra University, Visakhapatnam, 2022. He is currently working as the Associate Professor in Computer Science Engineering, Shri Vishnu Engineering College for Women's since 2015. His research interests include the routing protocols in IoT & MANET's, soft computing approaches like fuzzy logic and ANFIS for the time series problems. He can be contacted at email: sreekanth.pala@gmail.com.






**Prasad Maddala**    working as an Associate Professor in Department of Computer Science & Engineering at Shri Vishnu Engineering College for Women (Autonomous), Bhimavaram, West Godavari Dist, Andhra Pradesh, India. He completed his bachelor's, master's, and doctorate degree in Computer Science and Engineering. He has 19+ years of teaching experience. He has two years of international teaching experience in Ethiopia. He has guided more than 25+ projects at UG/PG level. He is guiding two Ph.D. research students also. His primary areas of interest are machine learning, data mining, cloud computing, mobile application development using Android, MANET routing, network & system security, visual data analytics, IoT, and ethical hacking. He can be contacted at email: prasads.maddula@gmail.com.






**Kiran Sree Pokkuluri**    received his B.Tech. and M.E. in computer science and engineering from JNTU and Anna University, respectively. He has obtained his Ph.D. degree in the area of AI from JNTU-Hyderabad. He has authored six textbooks for UG and PG students of engineering in AI and published more than 100+ research articles in various international journals and conferences. He has filed and published SIX patents in the areas of deep learning and AI. His bibliography was listed in Marquis Who's Who in the World, 29th Edition (2012), USA. He is the recipient of Bharat Excellence award. He has got 20+ years of teaching experience and working as Professor in the Department of Computer Science and Engineering at Shri Vishnu Engineering College for Women(A), Bhimavaram. He has delivered 100+ technical talks on deep learning and AI in various international conferences, FDP'S, and webinars. He is the Faculty Champion of the University Innovation Fellows program by Stanford University, USA. He can be contacted at email: drkiransree@gmail.com.






**Sunil Patten**    holds a Master of Science (M.Sc.) in computer science, Master of Technology (M.Tech.) in computer science and engineering, pursuing Ph.D. in computer science and systems engineering from Andhra University. He is currently lecturing with the Department of Computer Science and Engineering at Shri Vishnu Engineering College for Women, Bhimavaram, Andhra Pradesh. He is a member of CSI and ISTE. His research areas of interest include image processing and deep learning. He can be contacted at email: sunilpatten1979@gmail.com.



**Ramachandra Rao Kurada**    holds a Doctor of Computer Science and Engineering degree from Acharya Nagarjuna University, Nagarjuna Nagar, Guntur, India in 2019. He also received his M.Tech. in Computer Science and Engineering and M.Sc. (CS) in 2012 (JNTUK) and 1999 (AU), respectively. He is currently working as Professor at Department of Computer Science and Engineering, Shri Vishnu Engineering College for Women, Bhimavaram, India. He has 23 year of teaching experience and his research includes AI, machine learning, computational intelligence, networking, and blockchain. He has published over 36+ papers in international journals and conferences. He is life member of CSE, IETE, IEI and reviewer/board member for reputed journals, and IEEE conferences. He can be contacted at email: ramachandrarao.kurada@gmail.com.



**Ramu Yadavalli**    holds an M.Tech. in computer science and engineering from Bharath Institute of Higher Education and Research (2015) and an M.Sc. in computer science from Andhra University (2000). He is currently an Associate Professor in the Department of Computer Science & Engineering at Shri Vishnu Engineering College for Women (Autonomous), Bhimavaram, India. With over 22 years of teaching experience, his expertise spans AI, data analytics, machine learning, software project management, and blockchain. He has supervised more than 15 postgraduate and 25 undergraduate projects. He has published over 25 papers in international journals and conferences and serves as a reviewer for IEEE conferences and textbooks from reputed publishers. He is also a life member of CSI, IETE, and IEI. He can be contacted at email: yramumail@gmail.com.