IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 26, No. 6, December, 2021, pp. 549-557
Journal homepage: http://iieta.org/journals/isi

# Detection of Black Hole Attack Using Honeypot Agent-Based Scheme with Deep Learning Technique on MANET

Venkatasubramanian Srinivasan

Computer Science and Engineering Department, Saranathan College of Engineering, Trichy 620012, India

Corresponding Author Email: veeyes@saranathan.ac.in

https://doi.org/10.18280/isi.260605

**Received:** 6 October 2021
**Accepted:** 19 November 2021

***Keywords:***
*blackhole attack, deep learning, honeypots agents, internet of things, intrusion detection systems*

**ABSTRACT**

Mobile Ad-Hoc Networks (MANETs) due to their reconfigurable nature are being integrated into new and futuristic knowledge such as Internet of Things (IoT), cloud, reconfigurable networks, etc. To attain such credibility of integration, the routing protocols associated with these mobile nodes have to connect, perform and facilitate routing that offers a high level of security and resistance to all possible threats and security issues that may emanate in the network. One of the solutions used to maintain network security is intrusion detection systems (IDSs). This article primarily emphasis on the network's susceptibility to a suction assault known as a black hole attack. The investigations about the employment of intelligent agents called Honeypot Agent-based detection scheme (HPAS) with Long-Short Term Memory (LSTM) in identifying such assaults. Hence, the proposed method is named HPAS-LSTM, where honeypots are roaming virtual software managers that create Route Request (RREQ) packets to attract and entrap black hole attackers. Extensive model results utilizing the ns-2 simulator are used to demonstrate the presence of the suggested detection technique. The simulation outcomes demonstrate that the suggested technique outperforms current black hole detection methods in terms of throughput (TH), packet loss rate (PLR), packet delivery ratio (PDR), and total network delay (TND).

## 1. INTRODUCTION

In many contexts today, safety is predicated on an in-depth defense strategy that employs numerous layers of defense to keep intruders from violating security standards. Even if the opponent manages to breach one of the defensive levels, he will be helpless to do anything because the other layers will protect him [1]. A MANET is a wirelessly-connected network of mobile devices that does not have any underlying infrastructure. There are no restrictions on where a device can go in a MANET; this means that the connections between mobile devices are constantly changing. Because they do not require a fixed telecommunications infrastructure to make a dynamic network, MANETs are becoming increasingly important in applications such as military battleground communication systems, relief and case of emergencies operations, ecological conservation, taxi networks, and individual space infrastructures [2]. The rising use of MANETs has sparked many questions concerning their security, particularly for high-value security applications that may be at risk. Because of the shared wireless standard and lack of centralized control, MANETs are inherently vulnerable compared to conventional networks. Because of MANETs' special properties, creating secure systems has become more difficult [3]. MANETs are at risk, just like any other radio-based network knowledge. These dangers include intruders from other countries as well as abusers already on the network. The protection of these kinds of networks necessitates the use of a wide range of information and tools in many different technologies [4, 5].

Traditional wired networks have had several intrusion detection tests done on them. Due to fundamental architectural incompatibilities, transferring wireless network research from wired networks is a difficult undertaking. Designing IDS for MANETs is more complex because of its weaknesses [6]. Even though these defenses are effective against malevolent users, a further layer of security known as intrusion detection is frequently employed to keep networks safe. The IDS's primary goal is to identify harmful behavior, such as attacks from inside the defense environment [7, 8]. The dearth of a stable topology and restricted capitals, such as memory and power, are further sources of security difficulties in a wireless network. Audit data collected from the network serves as the primary input for the IDS, which uses that data to detect intrusions. IDSs in MANETs can be divided into two categories based on detection methods: anomaly detection and misuse detection. The most serious active assault in ad hoc networks is the black hole attack. Blackhole node responds to altogether path request packets imagining to have the finest path and subsequently destroys all received packets [9, 10].

Honeypots [11], an intelligent software agent is used in this research to suggest a pervasive monitoring strategy. When used in conjunction with an IDS, honeypots are effective tools for catching malicious attackers [12]. Due to MANET's dynamic nature, deploying a honeypot on a node leaves the detection strategy with insufficient coverage. Secret police operatives who perform random investigations are referred to as honeypot operators. Using a honeypot, an attacker can create a RREQ with a predetermined destination and path. Blackhole nodes are attracted solely to send a forged response. A malicious blackhole node (RREP) fabricates a route reply after observing the honeypot's RREQ. It promotes itself as the

most direct route (with a high sequence amount and the fewest amount of intermediate stops) to a specific location. This principally takes advantage of MANET's multipath routing feature and verifies the integrity of a route reply sent by a node to do so. The honeypot logs are an invaluable resource for figuring out how the black hole node operates so that fresh exploitation strategies can be devised. The rest of the paper is prearranged as follows. We'll take a look at some of Part 2's related work in the next section. The security and risks in MANET are shown in Section 3 along with a description of a blackhole assault in Section 3. Also in section 4 describes the architecture of the proposed honeypot-based blackhole attack detection approach using deep learning. Section 5 summarizes the results of the suggested approach's performance analysis, which was conducted using ns-2 simulator simulations. Section 6 concludes the paper with plans for the future.

## 2. LITERATURE REVIEW

A decentralized-based substructure is mentioned as MANET. IoT strategies form in a MANET, there are devices close by. The MANET is made up of a large number of endpoints, all of which employ a peer-to-peer technique to exchange data. There is no need for wireless devices or wireless networks while using a specifically allocated device. The self-built network is useful for MANET creation, but it is much more appealing when linked to the Internet. Because the Internet provides a wide range of administration, it assumes a significant role in many people's daily lives. For the MANET and the associated outer spaces, access points are being employed as a bridge.

Talukdar et al. [13] used the two types of techniques to detect the blackhole attacks, where the first type includes IDS and the second type includes digital signature with the prevention concept. Three types of attacks such as normal, black hole AODV and detected black hole AODV are implemented by this technique. The NS2 simulator is used for validation analysis and the parameters such as PDR, delay, and overhead are used for the simulation process. However, the performance of the network is highly degraded by blackhole attacks.

Elmahdi et al. [14] provided a secure and reliable data transmission under blackhole attacks and developed a modified multipath distance vector (MMDV) protocol. To reach the destination, messages are divided into multiple paths and a homomorphic encryption scheme is used to secure the message transmission. Network throughput and PDR are used for the simulation analysis and the results proved that the MMDV achieved better performance.

Naveena et al. [15] suggested a trust-based routing scheme for secure routing. Two stages are used in this scheme, where the first type is data retrieval and the second stage is data transfer mechanism. In a routing environment, identification and preservation of each node data transfer are carried out by the first stage, where the prediction of the safe path for transmission of the data packet to the target node is processed by the second stage. However, the energy consumption of nodes is high in this approach.

Kowsigan et al. [16] proposed alleviating the effects of a black hole through the identification and protection (ABIP) technique. According to the non-static threshold value of the succession number of receivers, the ABIP technique will be processed. The high receiver succession number is produced by the nodes that produce wrong information. The simulation results proved that the ABIP technique minimized the black hole attack and increased the performance in terms of PDR.

Verma et al. [17] present an effective and safe approach for MANET node confirmation. It's a validation mechanism that's based on the exchange of testaments among the nodes. To maintain the trustworthiness of authentications, their system also uses computerized signatures with debris functions. The re-enactment demonstrated that this protocol performed better in terms of quantity, start-to-finish postponement, and bundle dropping when hostile nodes in the MANET were nearby. The overhead of calculation and correspondence was also reduced, making it appropriate for MANETs.

According to Jain et al. [18], MANETs are a collection of wirelessly connected scheme gadgets. To exchange data, it's used this way. As a result, they researched a procedure based on the trust method to verify MANETs besides attacks. Through the processing of the node's trust estimation, their proposed methodology separates healthy nodes from malignant nodes. The approach makes use of a source node's old sham packets and sends them to the destination node. The goal was to provide a methodology that could validate and enhance the way the Reactive Routing Protocol family was presented.

Mapenduka [19] illustrates techniques that should be effective across the entire protocol stack because assaults are directed at levels that are explicitly identified. While listening to their presentation, they discuss current MANET attack detection tactics. The authors also suggest a half-and-half cross-layer strategy suitable for classifying several known and novel attacks that can be researched to enhance current plans in developing successful security solutions for MANET. Using a fluffy standard-based methodology, Gargan et al. [20] presented a MANET Trust-Based Secure Routing Protocol for planning and examination (TBSRPM). Because nodes have such strong behavior, even a short course does not guarantee a safe path. As a result, security isn't given any care because dynamic MANETs can easily break the rules. Consequently, it's critical to charting a course that you believe in. Their computation is an improvement to the AODV, developed for ensuring a safe path from the source to the destination. They're using it. In the end, the TBSRP improved MANETs.

Individuals who work with Yan and Wang [21] will learn how to overcome their fears of vulnerability and danger by participating in trusted social activities. For controlling PSN statistics access in a heterogeneous approach using property-based encryption, they use two mechanisms of trust levels assessed either by a trusted server or by separate PSN nodes, or both. They formally establish the safety of our strategy and dismantle its correspondence and unpredictability in calculations. According to a thorough investigation and execution valuation based on actual usage, their proposed strategy was both extremely effective and indubitably safe.

Using three indisputable group dropping attacks as a stimulus, Jhaveri et al. [22] examined Trusted Routing Scheme (TRS)-based Pattern Discovery (PD) by modifying the characteristics of several parameters, specifically the framework conditions. To oppose the adversaries that search for specific attack plans near a variety of foes, their work also collects the attack structure disclosure framework, trust model, and routing segment seized by TRS-PD Analyses conducted using the arrange test framework 2 display that the parameter selections made are correct under the given conditions.

Cai et al. [23] suggested an evolving self-cooperative trust

(ESCT) plot that mimics the human dynamic approach and relies on trust-level data to anticipate certain coordination disruptive impact ambushes. Adaptable focuses will trade and evaluate trust data obtained from all alone enthusiastic judgment as part of their game plan. It takes time for each node in the network to change its perspective to allow only legitimate parts to pass through the firewall. It's the most enticing feature of ESCT that they can't deal with the scheme regardless of whether the internal attackers know exactly how the security instrument functions. They look at how the ESCT plot displays under various types of routing interruption attacks. To the best of their knowledge, these results show that ESCT plans improve organizational adaptability while also ensuring that routing disruption aggressors cannot disrupt them in MANETs.

Nodes communicate, hand-off, and get traffic from neighbors as the scheme topology changes, according to Jim and Gregory [24]. For MANET, security is critical, and trust calculation is used to boost cooperation among nodes. Maintaining a trusted state for all nodes in a MANET network requires performing trust calculations regularly. If the trust computation is vulnerable to attack, then the trust values recorded may be suspect. It was proposed that an Artificial Immune System (AIS) be used to cope with register trust and to provide a powerful reputation instrument.

For Internet of Things coordination to support dependability and security while carrying finding methods in out of reach frameworks, Dhanya [25] proposes an assessment on TBRP. When dealing with node registration trust, there are several approaches to consider, including the fluffy trust strategy, the trust organization strategy, the crossover strategy, and others. In a dynamic and enigmatic MANET environment, they quickly implement these approaches for establishing trust in the sharing center points. Using the trust model established by Riaz et al. [26], the instant connection trust is determined using the Bayesian measurable technique and proposals from the neighbors. Essential trust can be determined using measurements like the received sign quality, the time it takes to cooperate, and how close nodes are to one another. Traditional Dynamic Source Routing (DSR) serves as the foundation for this trust-based strategy. Observations from the simulations show that the proposed approach improves routing adequacy even with malicious friends in the MANETs.

## 3. SECURITY AND THREATS IN MANET

MANETs offer infrastructure-free communication between mobile nodes and this feature has enhanced its usage in Internet of Things (IoT). IoT employs the cloud to provide data availability. The integration of the mobile nodes of MANETs in IoT could change the face of data processing and analysis as the task will be shifted to the mobile devices in the network. Processing data at mobile nodes increase the data processing speed, provides finer management of redundancy of data, and better emergency service supportability. Because of dynamic changes in topology, the mobile nodes are exposed to numerous networks and are susceptible to attacks by viruses, malware, and Spywares. These researchers are looking into the black hole assault, one of the possible attacks on MANETs. A rogue node may only do this if it falsely pretends to have the direct path between the source and destination, and then destroys every packet it receives as a result. A design of this assault-type can be seen in Figure 1.

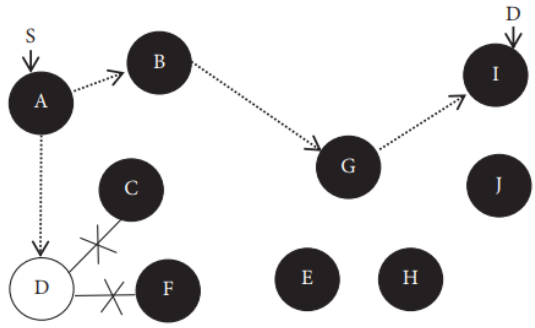


**Figure 1.** Representation of Blackhole attack

As can be seen in Figure 1, node A is acting as a source node and attempting to communicate with node I, which is the intended recipient. There are several ways to transport this data, including ABGI, though node D behaves as a disruptive node by claiming to have the shortest path from the source to the destination. It responds to A's route request (RREQ) incorrectly. As a result, every data packet that comes into contact with the rogue node is destroyed. A few damaging nodes cooperate and their destructive activity impacts the entire network in various types of black hole assault, different features are mixed. Interrupting routine is one way to avoid a black hole attack. Selecting many routes from the source to the destination is suggested when using this strategy. In each situation, it is suggested that three different routes from the source to the destination be considered. The RREP packet is kept in the source's buffer until two more routes are received. Following that, all packets are gathered and examined to determine the optimal path. The source node picks a safe path based on the number of nodes to avoid a black hole attack.

One way to protect and safeguard the nodes in the MANETs is to procreate the full network intelligence. Artificial intelligence (AI) can be speculated as a mechanism to convert the nodes in the network to smart and intelligent. The embedded intelligence in the nodes allows them to take intelligent decisions autonomously similar to humans.

Artificial Intelligence techniques can be utilized in MANETs to increase security due to the following reasons:

(i) **To manage a huge volume of Data:** Complexity associated with data generation in MANET is huge and managing the security of such data files and packets is a challenge. To select relevant data from all the generated log files and system alerts AI could be used. The usage of AI could ease off the complexity in the data selection process.

(ii) **To effectively expose the threats:** A network such as MANET where nodes are dynamically adding and leaving is always prone to threats.AI could aid in exploring foe or attackers much faster with high precision.AI techniques employ self-learning strategies and studies behavior of both the users and the network. Based on the identified behaviors decision-making is done in the network.

(iii) **To increase the response time:** Threat analysis has to be carried out with high precision and accuracy and AI offers faster processing speed with much efficiency for detection of security threats.

## 4. PROPOSED METHODOLOGY

The Honeypot agent-based approach with deep learning technique will be utilized in this work to solve the problem of

detecting black hole attacks in MANETs. Before discussing detection strategies, we first provide a system design.

### 4.1 Detection system architecture

Figure 2 depicts the proposed honeypot detection scheme's system architecture, which includes the components listed below:

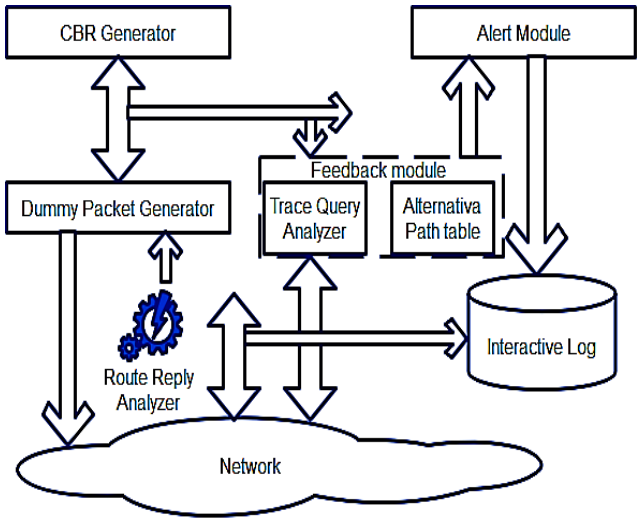


**Figure 2.** System architecture

**Route Module:** Dummy Packet Generator and Constant Bit Rate (CBR) Unit make up the Route module. As soon as the 'testee' enters the honeypot, an RREQ is generated to a known destination. A RREP packet is generated by the 'testee' when it receives an RREQ. Using the received reply packet, the Route Reply Analyzer module checks to see if the received RREP is genuine or a forgery. The RREP packet is analyzed by this module, which records the sequence sum and the hop count. The Dummy Packet Generator then generates dummy packets for the test subject to receive. The 'testee' under examination is either malevolent or trustworthy, therefore these phony packets are employed to test that. A 'testee' receives this communication and forwards it to a predetermined location. The Constant Bit Rate Unit used by the Dummy Packet Generator generates UDP packets at a fixed bit rate. It has been tweaked, however, so that the payload is overflowing with junk data.

**Feedback Module:** For the blackhole attack to be detected, it needs the feedback module to do its job well. A query packet is sent to the recognized destination to see if it has established any traffic from the testee since the alternate path was discovered. Any time the packet is received, it unicasts a trace reply back to the honeypot, indicating that it was received by the intended recipient. The feedback module determines whether or not the 'testee' is a trustworthy attacker based on his or her response.

**Alert Module:** If the feedback module finds evidence of malicious activity, it passes it along to the alarm module. Positive output is viewed as a sign of health, whereas negative output indicates an attack is underway. The alarm module sends out a message when it detects an attack so that the intruders know about it and can stop it. To prevent traffic from being forwarded through the malicious blackhole, the alert module exposes the malicious black hole's identity to all network nodes.

**Interactive log:** This provides insight into the honeypot's tactics for luring the malevolent MR. Additionally, it collects information on the route responses that the attacker is using to entice other nodes in the network. The Interactive log keeps track of everything that happened throughout the route exploration phase, including any alerts.

### 4.2 Honeypot agents in detection

Honeypots are used as software detection agents in our concept for detecting blackhole attacks. To detect a black hole attack, honeypots are placed on nodes to entice malicious attackers. Honeypots are also known as network cops because of their role in detecting attacks. The entire process is presented as a flow chart in Figure 3.

The suggested plan is broken down into the following phases, as follows:

**Step 1:** The 'testee' receives an RREQ packet from the Honeypot agent. The honeypot's node is the source address, while the endpoint address is a randomly selected, well-known location. This Honeypot is pre-configured to issue an exclusive RREQ to regulate the legitimacy of nodes in its immediate vicinity, so we believe it already knows the way there.

**Step 2:** The 'testee' sends an RREP packet to the LSTM technique and is used to verify whether a node is valid or spurious. This information is sent back to the honeypot. LSTM has been designed to resolve the problems and has been performed superiorly. Three gates and one cell memory state exist in the LSTM design. Figure 4 appearances the LSTM standard architecture.

$$X = \begin{bmatrix} h_{t-1} \\ x_t \end{bmatrix} \tag{1}$$

$$f_t = \sigma\left(W_f . X\right) + b_f \tag{2}$$

$$i_t = \sigma(W_i . X) + b_i \tag{3}$$

$$o_t = (W_o . X) + b_o \tag{4}$$

$$c_t = f_t \odot c_{t-1} + i_t \odot \tanh\left(W_c . X + b_c\right) \tag{5}$$

$$h_t = o_t \odot \tanh\left(c_t\right) \tag{6}$$

where, $W_i$ , $W_f$ , $W_o \in \mathbb{R}^{\times 2d}$ are the weighted matrices of RREP packet and $b_i, b_f, b_o \in \mathbb{R}^{d}$ are biases of LSTM, which is the short-term memory solution. They have inbuilt systems, which can control the flow of information, called gates. These gates can find out which data to keep or throw away in one sequence. This enables it over the extended chain of sequences to transmit relevant information to make forecasts of tasks. The main notion of LSTM is the cell condition and its diverse gates. The cell state serves as a transportation route throughout the flow of information. During the processing of the sequence, the cell state can contain useful data of RREP packets. Even early knowledge can thus lead to later temporal stages, which reduce the impact of short-term memory. The information will be added to or withdrawn by gates as the cell state moves on its trip. The gates can find out which knowledge is important in training to remember or forget. As a result, our honeypot detection approach using LSTM allows us to tell whether RREP packets are valid or not in later steps.

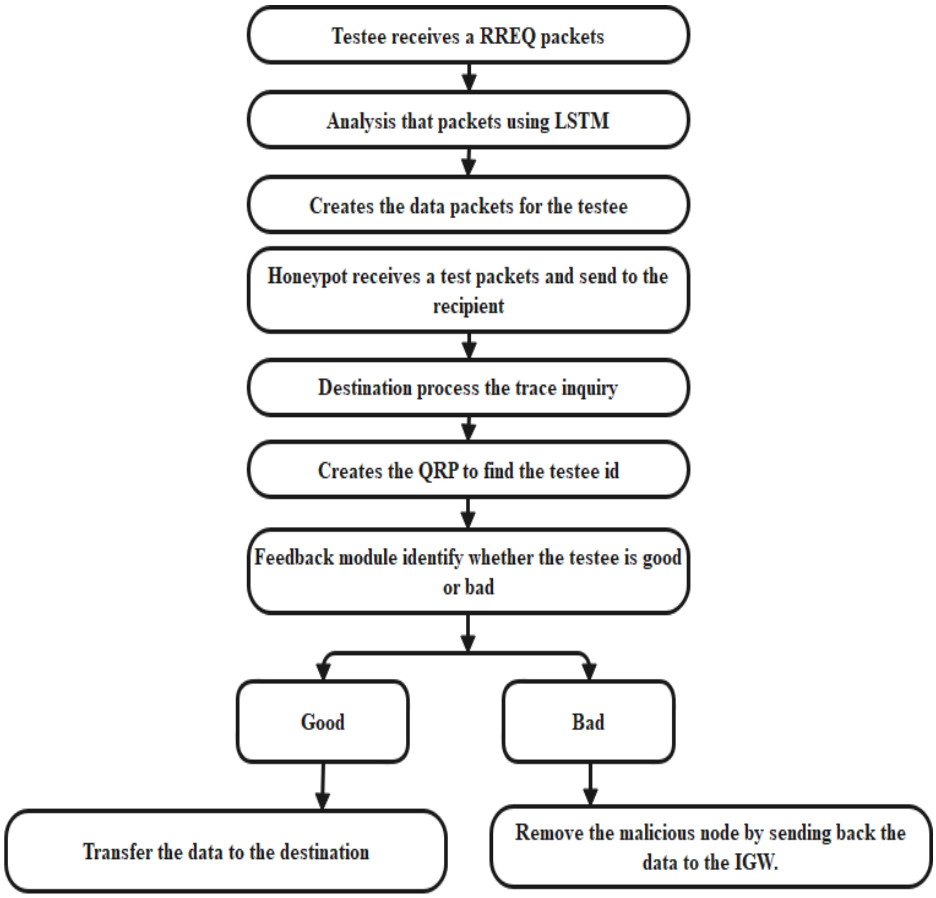


**Figure 3.** Steps involved in the process

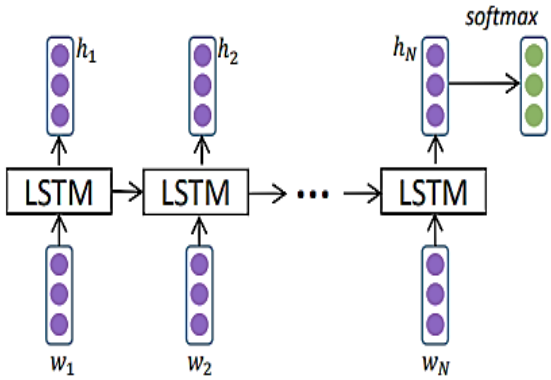


**Figure 4.** The standard LSTM architecture

**Step 3:** The honeypot then creates a data packet for the 'testee' and sends it to it. There is nothing special about the testee packet; it functions just like any other piece of ordinary data. There is a random data stream in the payload, making it impossible for the test subject to determine that the data is coming from the honeypot.

**Step 4:** When the honeypot receives the test packet, it sends a "Query packet" to the recipient, inquiring about it. The inquiry packet is then sent via this well-established path. The query packets have several different fields that include:

- Packet Sequence Number: This is the sequence numeral assigned to a particular packet once it has been produced.
- IP address of the honeypot's node. This is the IP address from which the honeypot receives its traffic.
- In the honeypot detection strategy, it's the IP address of the known location. c.) Source IP address.
- In the case of a testee, this is the source IP address.

**Step 5:** This trace inquiry is processed by the destination by looking at its Most Newly Received Traffic Cache, which includes the source ids, the timestamp of when it was received, and the number of packets established from this source.

**Step 6:** It creates a "Query reply packet (QRP)," whose destination address is equivalent to the basic address of the honeypot from which the query packet came if it discovers that the testee id has been stored in its traffic cache. The count of received packets and the date of the last received packet is also included in the query reply packet's information field. As a result, the honeypot receives the QRP through the same unicast path as the trace packet. The fields in the QRP are identical to those in the QRP and are described as follows:

- IP Sequence Number: This is the IP packet's sequence number as it arrives at the destination computer.
- IP Address of the Sender: This is the address of the node from which the packet is being transmitted.
- IP Address of the Honeypot Node: Address of the honeypot server.
- It keeps track of the number of packets the test subject sends and receives.
- A Time Stamp is a piece of information that tells you when it received the last packet.

**Step 7:** Query reply packets are handed out to feedback modules by the honeypot agent. The validity of a test depends on the information in the field. The 'testee' is a "Good Node" if the packet is received at the endpoint. The 'testee' is a

malicious attacker if the field is empty. The other path is used by the feedback module to retrieve the data.

**Step 8:** A malicious blackhole attacker is being considered as a "testee" by the honeypot's alert module. As a result, other nodes in the network do not relay the message through the malicious blackhole node in question.

**Step 9:** To remove a rogue node, this data is also sent to the Internet Gateway (IGW), which in turn sends it to the ISP. To put it another way, honeypots serve as network enforcers, checking to see if a node's routing module's integrity is intact using the LSTM model. You can program the mobile honeypot to follow a predetermined path through the network. When starting from the IGW node, Honeypot can perform a depth-first walk to the leaf nodes using random walks in the network.

## 5. RESULTS AND DISCUSSION

Initialization will be done by simulating the network; subsequent evaluation will focus on network parameters; and finally, the simulation output will be given. Then, the results of the proposed technique are compared with the outcomes of the existing deep learning techniques namely Bi-directional LSTM (Bi-LSTM), Recursive Neural Network (RNN), and Recurrent Neural Network (ReNN) to detect black hole attacks. These existing deep learning techniques are implemented with the proposed Honeypot Agent-based detection scheme (HPAS) for better evaluation. Finally, we'll talk about and analyze the findings. Table 1 shows the parameters for the proposed algorithm's simulated network.

**Table 1.** Simulation constraints

| Parameters | Value |
|---|---|
| Simulator | NS-3.31 |
| Pause Time | 5-20 s |
| Traffic Type | CBR |
| Antenna | Omni antenna. |
| Number of Nodes | 20, 40, 60, 80, 100. |
| Simulation time | 600s |
| MAC Type | IEEE 802.11 |
| Network Area | 300 m × 300 m |
| Mobility | 0.5-1.0 m/s |
| Packet Size | 512 bytes |
| Transmission Range | 250 m |

The following are the method's performance evaluation parameters:

**PLR:** During the data transmission process, Packet Loss Ratio (PLR) is described as the average number of packets loss. The PLR can be considered as in Eq. (7):

$$PLR(\%) = \frac{N^{tx} - N^{rx}}{N^{tx}} \times 100 \quad (7)$$

where, $N^{tx}$ and $N^{rx}$ are the total amount of transmitted and received packets, respectively.

**TH:** Throughput (TH) is defined as the total number of successful data received at the destination and it is defined as follows in Eq. (8):

$$TH = \frac{N^{rx}}{T} \quad (8)$$

where, $T$ is defined as the simulation time.

**PDR:** T Over the number of packets sent by the source, Packet Delivery Ratio (PDR) defined the proportion of a total number of packets that reached the destination, the PDR can be calculated as follows in Eq. (9):

$$PDR(\%) = \frac{N^{rx}}{N^{tx}} \times 100 \quad (9)$$

**TND:** In all circumstances, it's the whole network delay. This Total Network Delay (TND) is derived by subtracting the time it took for packets to arrive at their destinations from the total time it took.

### 5.1 Performance analysis of proposed HPAS-LSTM

Here, the validation of the proposed method is analyzed with malicious nodes and without malicious nodes in terms of various parameters. Table 2 offers the parameters of the proposed network without attack.

**Table 2.** Performance analysis of HPAS-LSTM without attacks

| Parameters | Number of Nodes | | | | |
|---|---|---|---|---|---|
| | 20 | 40 | 60 | 80 | 100 |
| PLR (%) | 8.78 | 7.30 | 9.70 | 7.34 | 8.21 |
| TH (kbps) | 178.82 | 151.87 | 193.91 | 165.32 | 175.18 |
| PDR (%) | 91.12 | 92.31 | 91.25 | 93.35 | 92.76 |
| TND (ms) | 7.25 | 13.44 | 12.30 | 11.08 | 14.07 |

For the TND analysis, the HPAS-LSTM achieved high delay, when the nodes increase. For instance, the TND is only 7.25ms, when the node is 20. But the proposed method achieved 14.07ms, when the node is 100. When the node is 40, the HPAS-LSTM achieved 7.30% of PLR, 151.87kbps of TH, 92.31% of PDR, and 13.44ms of TND. When the node is 80, the HPAS-LSTM achieved 7.34% of PLR, 165.32kbps of TH, 93.35% of PDR, and 11.08ms of TND. Finally, when the node is 100, the HPAS-LSTM achieved 8.21% of PLR, 175.18kbps of TH, 92.76% of PDR, and 14.07ms of TND. The next Table 3 shows the validated analysis of proposed HPAS-LSTM with blackhole attacks.

**Table 3.** Performance analysis of HPAS-LSTM with Blackhole attacks

| Parameters | Number of Nodes | | | | |
|---|---|---|---|---|---|
| | 20 | 40 | 60 | 80 | 100 |
| PLR (%) | 9.34 | 8.69 | 9.91 | 7.65 | 8.71 |
| TH (kbps) | 176.52 | 150.91 | 192.15 | 162.21 | 174.81 |
| PDR (%) | 90.21 | 91.70 | 90.08 | 92.36 | 91.26 |
| TND (ms) | 9.20 | 17.34 | 15.13 | 17.08 | 19.87 |

In the simulation network, when the attack is detected by the proposed HPAS-LSTM network, its performance will automatically be degraded. The clear tabulation analysis is given in Table 2 and Table 3. When the node is 20, the HPAS-LSTM achieved 9.34% of PLR, 176.52kbps of TH, 90.21% of PDR, and 9.20ms of TND. When the node is 40, the HPAS-LSTM achieved 8.69% of PLR, 150.91kbps of TH, 91.70% of PDR, and 17.34ms of TND. When the node is 60, the HPAS-LSTM achieved 9.91% of PLR, 192.15kbps of TH, 90.08% of PDR, and 15.13ms of TND. Finally, when the node is 100, the

HPAS-LSTM achieved 8.71% of PLR, 174.81kbps of TH, 91.26% of PDR, and 19.87ms of TND. For graphical representation between without attacks and with attacks using HPAS-LSTM, Figure 5 shows the sample comparison of PDR and TH.

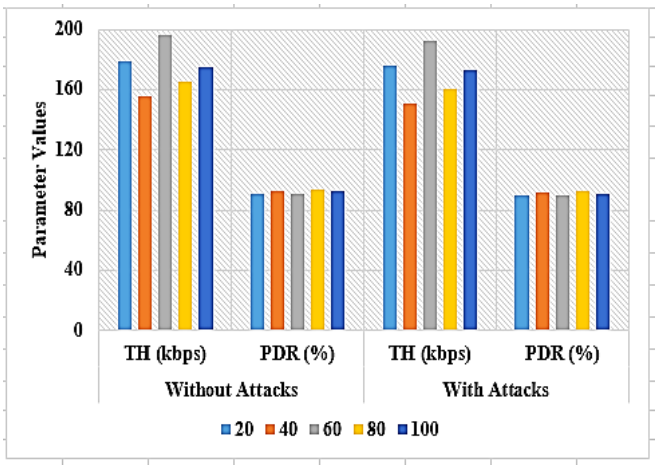


**Figure 5.** Graphical representation of HPAS-LSTM by considering with and without blackhole attacks

### 5.2 Performance analysis of proposed HPAS-LSTM with other existing techniques

In this section, the validation of the proposed method is compared with three pre-defined networks in terms of PDR, TH, TND, and PLR. Initially, Figure 6 shows the graphical representation of the proposed HPAS-LSTM with other techniques in terms of PDR.

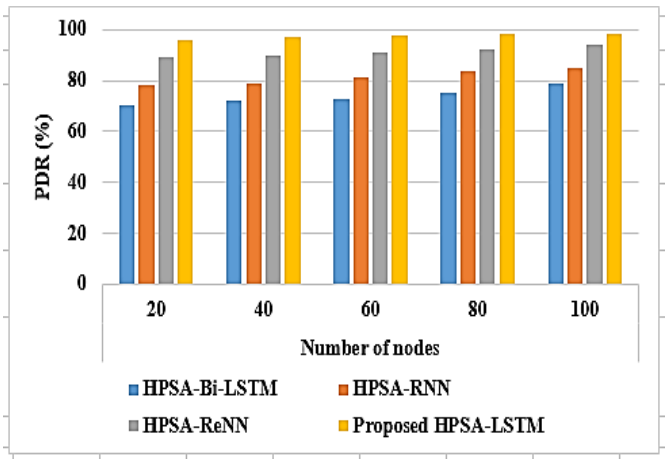


**Figure 6.** Graphical representation of proposed LSTM network in terms of PDR

When the node is 20, the existing techniques including Bi-LSTM, RNN, and ReNN achieved 70%, 78%, and 89% of PDR, but the proposed HPAS-LSTM achieved 96% of PDR. The reason is that existing techniques are insufficient to handle the process of HPAS for finding the integrity of malicious nodes and took a large training time than LSTM. When the node is 60, Bi-LSTM, RNN, ReNN and proposed LSTM achieved 73%, 81%, 91% and 97.50% of PDR. When the node increases, the analysis of PDR performance is also increased. For instance, RNN achieved 85.14% of PDR, and proposed LSTM achieved 98.16% of PDR. The training process is difficult in RNN and it can't handle the process of the long sequence, which automatically degrades the performance of RNN. Figure 7 shows the graphical representation of the proposed LSTM in terms of PLR.

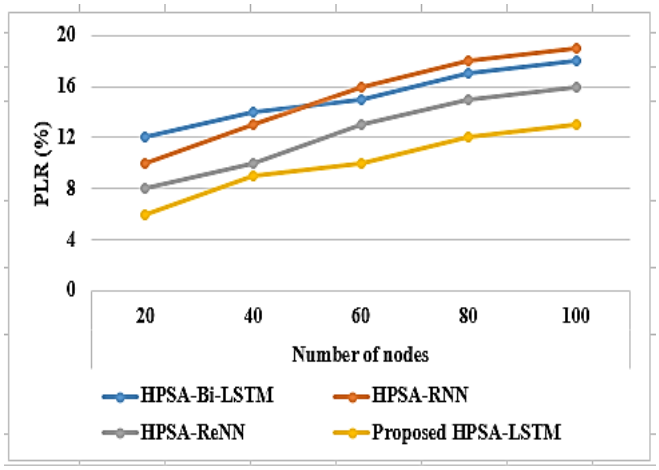


**Figure 7.** Graphical representation of proposed LSTM network in terms of PLR

When the node is 40, the existing techniques including Bi-LSTM, RNN, and ReNN achieved 14%, 13%, and 10% of PDR, but the proposed HPAS-LSTM achieved 9% of PLR. When the node is 80, Bi-LSTM, RNN, ReNN and proposed LSTM achieved 17%, 18%, 15% and 12% of PLR. When the node decreases, the analysis of PLR performance is also decreased. For instance, ReNN, RNN achieved 8%, 10% of PLR, but the proposed LSTM achieved 6% of PLR. The reason is that RNN training is a difficult process and it can't process the long sequences, since it uses ReLu as an activation function. Figure 8 presents the graphical analysis of the proposed LSTM in terms of TH.

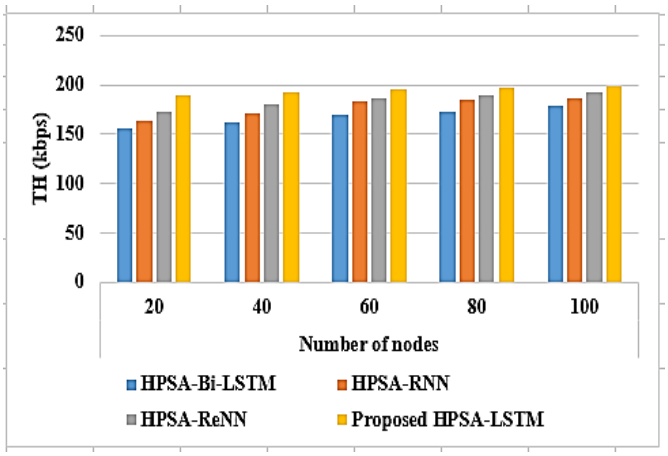


**Figure 8.** Graphical representation of proposed LSTM network in terms of TH

When the node is 20, the existing techniques including Bi-LSTM, RNN and ReNN achieved 156%, 163%, and 172% of TH, but the proposed HPAS-LSTM achieved 190% of TH. When the node is 40, Bi-LSTM, RNN, ReNN, and proposed LSTM achieved 162%, 171%, 180%, and 192% of TH. When the node is 60, Bi-LSTM, RNN, ReNN, and proposed LSTM achieved 169%, 183%, 186%, and 195% of TH. Finally, when the node is 80, the ReNN and RNN achieved nearly 185% to 189% of TH, but the proposed LSTM achieved 197% of TH. This shows that the proposed HPSA-LSTM achieved better

performance than existing techniques. The RNN relies on the hidden state, where LSTM is insensitive to the gap length and stores the information for future cell processing. For instance, instead of 10th intervals, the sequences must be predicted on 1000th intervals, RNN forgets the starting point, but LSTM remembers it and reduces the complexity for each weight update to O(1). The graphical representation of the proposed technique in terms of TND is given in Figure 9.

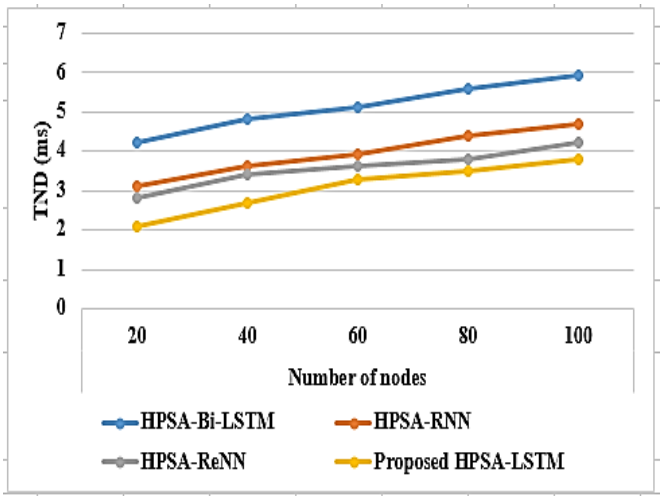


**Figure 9.** Graphical Representation of Proposed LSTM network in terms of TND

When the node is 20, the existing techniques including Bi-LSTM, RNN and ReNN achieved 4.2ms, 3.1ms, and 2.8ms of TND, but the proposed HPAS-LSTM achieved 2.1ms of TND. When the node is 40, Bi-LSTM, RNN, ReNN, and proposed LSTM achieved 4.8ms, 3.6ms, 3.4ms, and 2.7ms of TND. When the node is 60, Bi-LSTM, RNN, ReNN, and proposed LSTM achieved 5.1ms, 3.9ms, 3.6ms, and 3.3ms of TND. Finally, when the node is 80, the ReNN and RNN achieved nearly 4.2ms to 4.7ms of TND, but the proposed LSTM achieved only 3.8ms of TND. The following with attack, Table 4 shows the overall performance of the proposed method with existing techniques in terms of various parameters for node 100.

**Table 4.** Overall performance analysis of proposed HPSA-LSTM with existing techniques for node 100

| Methodology | Parameters | | | |
|---|---|---|---|---|
| | PDR (%) | PLR(%) | TH(kbps) | TND (ms) |
| HPSA-Bi-LSTM | 79 | 18 | 179 | 5.9 |
| HPSA-RNN | 85.14 | 19 | 187 | 4.7 |
| HPSA-ReNN | 94 | 16 | 193 | 4.2 |
| Proposed HPSA-LSTM | 98.16 | 13 | 199 | 3.8 |

Since the entire network's lower delay provides higher data transfer rates and better network performance, the proposed HPAS-LSTM should not exceed the expected network delay. If the number of nodes is small, the total network delays in all methods are almost close to each other. However, as the number of nodes increases to more than 20, the delay difference between the different methods slowly increases. However, the proposed HPAS-LSTM method is slightly better than other methods in terms of various parameter metrics.

## 6. CONCLUSION

Because of the MANET's unique properties, including its lack of infrastructure requirements, ease of setup, and lack of centralized management, this network has grown in popularity and found applications across a wide range of industries. MANETs must have security as a top priority. Using intrusion detection systems (IDSs) is one way to keep this network safe. An LSTM-based honeypot-based detection solution for MANET's black hole attackers is presented in this research. The LSTM network in a honeypot agent-based method detects the integrity of RREP packets. TH, TND, PDR, and PLR have all improved as a result of the black hole attack, according to the findings. The simulations show that our honeypot detection model helps boost the throughput in a MANET with blackhole nodes. We intend to deploy honeypot detection agents in the future to identify more types of threats. The cumulative transmission time with effective deep learning will be used as a routing approach to detect blackhole attackers in MANET.

## REFERENCES


[1] Kumar, S., Goyal, M., Goyal, D., Poonia, R.C. (2017). Routing protocols and security issues in MANET. In 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), pp. 818-824. https://doi.org/10.1109/ICTUS.2017.8286119

[2] Rath, M., Swain, J., Pati, B., Pattanayak, B.K. (2018). Network security: Attacks and control in MANET. In Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, 19-37. https://doi.org/10.4018/978-1-5225-4100-4.ch002

[3] Yu, F.R., Tang, H. (2010). Distributed node selection for threshold key management with intrusion detection in mobile ad hoc networks. Wireless Networks, 16(8): 2169-2178. http://dx.doi.org/10.1007/s11276-010-0250-6

[4] Arappali, N., Rajendran, G.B. (2021). MANET security routing protocols based on a machine learning technique (Raspberry PIs). Journal of Ambient Intelligence and Humanized Computing, 12(16): 6317-6331. https://doi.org/10.1007/s12652-020-02211-8

[5] Vyas, A., Satheesh, A. (2018). Implementing security features in MANET routing protocols. International Journal of Computer Network and Information Security, 8: 51-57. https://doi.org/10.5815/ijcnis.2018.08.06

[6] Elboukhari, M., Azizi, M., Azizi, A. (2014). Intrusion detection systems in mobile ad hoc networks: A survey. 2014 5th Workshop on Codes, Cryptography and Communication Systems (WCCCS), 2014, pp. 136-141. https://doi.org/10.1109/WCCCS.2014.7107930

[7] Sarbhukan, V.V., Ragha, L. (2020). Establishing secure routing path using trust to enhance security in MANET. Wireless Personal Communications, 110(6): 245-255. https://doi.org/10.1007/s11277-019-06724-0

[8] Vinayagam, J., Balaswamy, Ch., Soundararajan, K. (2019). Certain investigation on MANET security with routing and blackhole attacks detection. Procedia Computer Science, 165: 196-208. https://doi.org/10.1016/j.procs.2020.01.091

[9] Merlin, R.T., Ravi, R. (2019). Novel trust based energy aware routing mechanism for mitigation of black hole

attacks in MANET. Wireless Personal Communications, 104: 1599-1636. https://doi.org/10.1007/s11277-019-06120-8

[10] Patel, R., Kamboj, P. (2017). A survey on contemporary MANET security: Approaches for securing the MANET. International Journal of Engineering and Technology, 9(1): 98-112. http://dx.doi.org/10.21817/ijet/2017/v9i1/170901413

[11] The Honeynet Project. http://www.honeynet.org/.

[12] Khattab, S., Melhem, R., Mosse, D., Znati, T. (2006). Honeypot back-propagation for mitigating spoofing distributed Denial-of-service attacks. Proceedings 20th IEEE International Parallel & Distributed Processing Symposium, 2006, p. 8. https://doi.org/10.1109/IPDPS.2006.1639674

[13] Talukdar, M.I., Hassan, R., Hossen, M.S., Ahmad, K., Qamar, F., Ahmed, A.S. (2021). Performance improvements of AODV by black hole attack detection using IDS and digital signature. Wireless Communications and Mobile Computing. https://doi.org/10.1155/2021/6693316

[14] Elmahdi, E., Yoo, S.M., Sharshembiev, K., (2020). Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks. Journal of Information Security and Applications, 51: 102425. https://doi.org/10.1016/j.jisa.2019.102425

[15] Naveena, S., Senthilkumar, C., Manikandan, T. (2020). Analysis and countermeasures of black-hole attack in manet by employing trust-based routing. In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1222-1227. https://doi.org/10.1109/ICACCS48705.2020.9074282

[16] Kowsigan, M., Rajeshkumar, J., Baranidharan, B., Prasath, N., Nalini, S., Venkatachalam, K. (2021). A novel intrusion detection system to alleviate the black hole attacks to improve the security and performance of the MANET. Wireless Personal Communications, pp. 1-21. https://doi.org/10.1007/s11277-021-08530-z

[17] Verma, U.K., Kumar, S., Sinha, D. (2016). A secure and efficient certificate-based authentication protocol for MANET. In Proceedings of IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2016, pp. 1-7. https://doi.org/10.1109/ICCPCT.2016.7530346

[18] Jain, A.K., Tokekar, V. (2015). Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks. 2015 International Conference on Pervasive Computing (ICPC), pp. 1-6. https://doi.org/10.1109/PERVASIVE.2015.7087174

[19] Mapenduka, W. (2018). Methods for detecting attacks in mobile/wireless Ad-Hoc networks: A survey. International Journal of Scientific & Technology Research, 7(7): 168-174.

[20] Garg, M.K., Singh, N., Verma, P. (2018). Fuzzy rule-based approach for design and analysis of a Trust-based Secure Routing Protocol for MANETs. in Procedia Computer Science, 132: 653-658. https://doi.org/10.1016/j.procs.2018.05.064

[21] Yan, Z., Wang, M. (2014). Protect pervasive social networking based on two-dimensional trust levels. IEEE Systems Journal, 11(1): 207-218. https://doi.org/10.1109/JSYST.2014.2347259

[22] Jhaveri, R.H., Patel, N.M., Zhong, Y., Sangaiah, A.K. (2018). Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile Ad-Hoc networks in industrial IoT. IEEE Access, 6: 20085-20103. https://doi.org/10.1109/ACCESS.2018.2822945

[23] Cai, R.J., Li, X.J., Chong, P.H.J. (2019). An evolutionary self-cooperative trust scheme against routing disruptions in MANETs. IEEE Transactions on Mobile. Computing., 18(1): 42-55. https://doi.org/10.1109/TMC.2018.2828814

[24] Jim, L.E., Gregory, M.A. (2018). AIS Reputation Mechanism in MANET. 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), pp. 1-6. https://doi.org/10.1109/ATNAC.2018.8615267

[25] Dhanya, K., Jeyalakshmi, C., Balakumar, A. (2019). A secure autonomic mobile Ad-Hoc network based trusted routing proposal. International Conference on Computer Communication and Informatics (ICCCI), pp. 1-6. https://doi.org/10.1109/ICCCI.2019.8822012

[26] Riaz, M.K., Yangyu, F., Akhtar, I. (2019). A multidimensional trust inference model for the mobile Ad-Hoc networks. 28th Wireless and Optical Communications Conference (WOCC), pp. 1-5. https://doi.org/10.1109/WOCC.2019.8770587