Secure and Light Weight Aodv (Slw-Aodv) Routing Protocol for Resilience Against Blackhole Attack in Manets

M V D S Krishna Murty, Lakshmi Rajamani

Abstract**:** ***This paper aimed at the detection of blackhole attacks and proposed a new method called Secure and Light Weight Adhoc On Demand Distance Vector Routing (SLW-AODV). SLW-AODV is an extended version of the traditional AODV routing protocol. The proposed SLW-AODV ensures resilience for both blackhole and cooperative blackhole attacks. It employs a simple Challenge, Response, and Confirm (CRC) strategy, utilising chaotic maps, for the identification of both black hole and cooperative black hole attacks. SLW-AODV identifies the attacked nodes during both the route discovery and data forwarding processes. For experimental validation, we have conducted extensive simulations and the performance is validated through Packet Delivery Ratio, Throughput and Average end-to-end delay. The obtained performance metrics demonstrate outstanding performance compared to state-of-the-art methods.***

Keywords**:** ***Average End-To-End Delay, Chaotic Maps, Cooperative Blackhole, MANETs***

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are wireless networks formed with mobile devices as nodes. Due to the nature of decentralized communication, MANETs gained tremendous interest in different applications including emergency rescue operations, military operations, collaborative distributed computing, disaster management and some personal area network applications [1]. In MANETs, there exist mobile nodes which don't have any fixed infrastructure and can communicate with each other through multiple hops. Since MANET is characterised as a decentralised network, communication between any two nodes requires multi-hop relays to act as intermediate routers. Every node in MANET is permitted to move arbitrarily in the network. In a MANET, all nodes are treated equally, and so every node can transfer data between any source and destination pairs. However, the significant issues in MANETs are their varying mobility nature, which leads to serious link failures, network security and quality of services challenges for researchers [2-4]. Due to the dynamic nature of MANETs and their lack of fixed infrastructure, they are generally vulnerable to several types of attacks. These attacks include sinkhole, DoS (Denial of Service), DDoS (Distributed DoS), and blackhole attacks. For example, Kalita *et al.* [5] surveyed different types of attacks associated with ad hoc networks and provided countermeasures for these attacks. Nguyen and Nguyen [6] introduced the impact of different types of attacks associated with MANETs based on a simulation study. Among the several attacks, the blackhole attack is a major one that causes severe damage to the network. Panos *et al.* [7] presented a comprehensive analysis of the blackhole attack (BHA) related to MANETs. Additionally, they introduced the concept of black hole intensity as a new attack factor and evaluated its impact on network performance. Khanna and Sachdeva [8] presented different aspects of blackhole attack together with the weaknesses of the current literature. In addition, they introduced comprehensive classifications of mitigation and detection schemes, reviewing and incorporating several published works associated with those classifications. Although several methods have been proposed for identifying black hole attacks in MANETs, no technique has focused on determining cooperative black hole attacks, as well as on the nodes attacked by black hole attacks during the data forwarding process. Hence, this paper proposes a simple and effective mechanism called Secure and Lightweight AODV (SLW-AODV) for detecting both black hole and cooperative black hole attacks. SLW-AODV is an extended version of the traditional AODV routing protocol. SLW-AODV follows a three-phase mechanism called Challenge-Response-Confirm (CRC) to discover a route with no blackhole-attacked nodes. The SLW-AODV can detect malicious nodes that behave abnormally during the route discovery process, as well as those that behave normally during the routing process but maliciously during the forwarding process. The remaining paper is organised as follows: Section II explores the literature survey on black hole detection methods. Section III examines the details of the proposed SLW-AODV. Section IV discusses the details of simulation experiments, and the final section concludes the paper.

Manuscript received on 08 February 2023 | Revised Manuscript received on 13 February 2023 | Manuscript Accepted on 15 March 2023 | Manuscript published on 30 March 2023.

*Correspondence Author(s)

M V D S Krishna Murty*, Research Scholar, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University Hyderabad (Telangana), India. E-mail: mkrishnamurty@gmail.com, ORCID ID: https://orcid.org/0000-0002-4705-3818

Dr. Lakshmi Rajamani, Professor and Head (Retd), Department of Computer Science and Engineering, Osmania University, Hyderabad (Telangana), India. E-mail: drlakshmiraja@gmail.com

II. LITERATURE SURVEY

In this survey, we have explored various earlier methods primarily aimed at detecting black hole attacks in MANETs. S.

Sharma et al. [9] employed a new routing protocol called as secure zone routing protocol (SZRP) to provide resilience to MANETs against BHA. In this approach, the author assumed the BHA in both the inside and outside zones, i.e., internal and external BHAs. They used Qualnet for simulation purposes.

C. Jiwen et al. [10] adapted cross-layer design and aimed at the detection of BHA and Grey Hole Attacks (GHA). In the proposed method, an overhear-based path selection mechanism is proposed for the activity of the next-hop node. Moreover, they used internal HELLO packets and saved their energy resource upon detection of BHA. Furthermore, to reduce the false positive rate under larger network loads, this approach adapted a reporting system based on the collision rate in the Medium Access Control (MAC) layer. They referred to the standard Dynamic Source Routing (DSR) protocol and used NS-2 for simulation.

Y. F. Alem, Z. C. Xuan [11] proposed an anomaly detection-based intrusion detection (ADID) mechanism to identify BHA over both single and multiple mobile nodes in MANETs. Tamilarasan [12] proposed a new algorithm called the Prior Receive Reply (PRR) algorithm or counter algorithm to prevent nodes from being in the BHA in MANETs. Haas, Z. J [13] proposed a new routing protocol, Zone Routing Protocol (ZRP), for reconfigurable wireless networks. The novelty of the ZRP protocol lies in its applicability to large flat-routed networks, and its performance shows a reduction in the number of control messages compared to other reactive schemes. A. Tripathi and A. K. Mohapatra [14] proposed to measure hop count for BHA detection. The hop count is calculated based on packet confirmation. However, the significant disadvantage is that they didn't involve the destination sequence number at the detection of BHA.

T. N. D. Pham and C. K. Yeo [15] proposed a method called statistical-based BHA and GHA detection to detect two types of attacks in MANETs, which are collusion and individual attacks. Here, the nodes exchange their histories so that they can analyse the forwarding behaviour. To classify normal nodes from attacker nodes, they suggested a new metric called the Forwarding Ratio (FR). FR helps in BHA and GHA identification, as attackers are required to create a large number of fake encounter records to drop the message continuously. In such a case, the FR value will be very low for individual attacker nodes. Hence, a proposed mechanism involves the sent message count and an uneven pattern of appearance frequency in the routing algorithm to identify colluding attacks.

A. M. El-Semary and H. Diab [16] proposed BH-protected AODV (BP-AODV) routing to solve the BHA-related security issues in MANETs. This approach is an extended version of AODV, which involves randomly generated challenges during the route discovery process. Moreover, this approach also aimed to detect BHA and coordinate nodes that collectively launch BHA in MANETs. They employed secret maps generation to ensure resilience against BHA in MANETs.

S. Shrestha et al. [17] proposed a change in control packet sequence number, especially in RREP, to protect nodes of MANETs from BHA and reduce the loss of data packets. E. Elmahdi et al [18] proposed a homomorphic encryption scheme in the AOMDV protocol to ensure a reliable and secure data transmission in MANETs under BHA. They observed that their method has better detection performance than AOMDV when there are a large number of malicious nodes in the network.

N. G. Wakode [19] proposed a Cooperative Bait Detection (CBA) approach for malicious node identification using AODV. CBA is referred to as both a reactive and proactive approach and applies a simple mechanism called reverse tracing for the detection of BHA. S. Pandey and V. Singh [20] applied machine learning algorithms such as Artificial Neural Network (ANN) and Support Vector Machine (SVM) for BHA detection in MANETs. G. Li, Z. Yan and Y. Fu [21] used NS-3 simulator to study and analyze the impact of BHA in AV protocol. They analysed three performance metrics: packet loss rate, end-to-end delay, and throughput. Furthermore, they examined the effect of BHA on these metrics at various network parameters, including speed, the number of nodes, and the number of blackhole-attacked nodes in the network.

V. Sharma et al. [22] analyzed the TCP over BHA. They performed a detailed analysis of the reliability of the transport layer protocol under several conditions. The impact is measured through end-to-end delay, normalized routing load and throughput. S. Kaushik etal. [23] used SVM algorithm to analyze the performance of a AODV and SAODV for communication and packets transfer among nodes in Mobile Adhoc Networks. The analysis is conducted through several performance metrics, including end-to-end delay, packet delivery ratio, throughput, and average energy consumption. They designed a methodology with the help of lessons learned from the estimations and computations made during the transfer of packets between network nodes. S. Barai and P. Bhaumik [24] proposed an extended version of the conventional Spray and Wait Routing (SWR) protocol to reduce the impact of BHA on network performance. T. Terai et al [25] detected that Blackhole can predict the sequence numbers present in the control packets and can manipulate them to launch attacks in the network. To overcome this problem, they proposed a detection and prevention mechanism based on local data exchange between nodes in the network.

M. B. M. Kamel et al [26] proposed a secure and trust-based mechanism based on AODV (STAODV) to isolate malicious nodes in MANETs and to improve the security of the AODV protocol. They linked a trust value for each node to estimate the trust level of that node. They proposed to analyze each incoming packet to prevent BHA. I. Kaushik [27] developed an intrusion detection system using NS-2 after analysing various attacks at different layers. They concluded that BHA is one of the severe attacks and applied an intrusion detection system over it. F. Taranum et al. [28] applied Elliptical Key Cryptography (ECC) and reverse AODV (R-AODV) to detect BHA and to ensure a secure data transmission in MANETs. They mainly aimed to keep the packets secure. When compared to public key encryption algorithms, ECC is simpler as it provides keys with smaller sizes. Moreover, ECC eliminates the need for pre-key distribution and ensures secure paths against BHA in MANETs.

III. PROPOSED FRAMEWORK

3.1 Overview

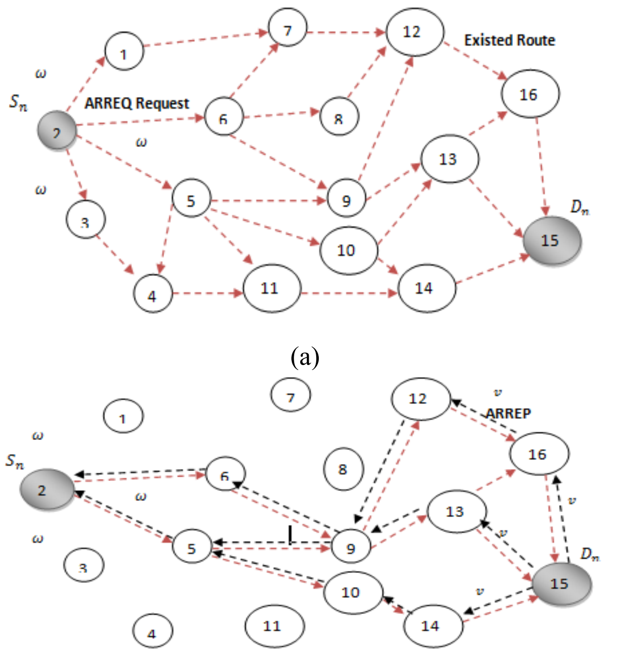
The main contribution of SLW-AODV is to address the cooperative blackhole attack associated with the AODV protocol, while also providing a routing protocol that is robust against blackhole and cooperative blackhole attacks during the routing process. SLW-AODV protocol uses a Challenge-Response-Confirm (CRC) pattern to establish trusted routes. Initially, the source node (S_n) generates a challenge value and then conveys it to a destination node during a route request process. When the destination receives the challenge, it computes the corresponding response as a function of the received challenge along with other secret values generated by the destination. The destination node propagates the response value to the source during the route reply process, while retaining the hidden values. Finally, the destination node confirms the route by conveying the secret values during the route confirmation process. The SLW-AODV accomplishes its task by incorporating a chaotic map into its design, along with using the Challenge-Response-Confirm pattern during the routing process.

3.2. Message Types

SLW-AODV uses five types of messages. They are - ARREQ (Altered Route REQuest), ARREP (Altered Route REPly), RERR (Route ERRor), HELLO (HELLO), and RC (Route Confirm). SLW-AODV modified the RREQ and RREP while retaining the HELLO and RERR of the AODV protocol as is. Alongside, SLW-AODV creates a new message called Route Confirm (RC). ARREQ is an extended version of RREQ, just by extending two fields to include two values; they are challenge (ω) and timestamp (τ). ω is a challenge value generated by the source node and τ Is the time at which ω Is generated. Next, ARREP is an extended form of RREP by extending one field to include a response value v generated by D_n. Finally, RC p, theacket has eight fields which convey several secret values generated by D_n At the time of the RC process.

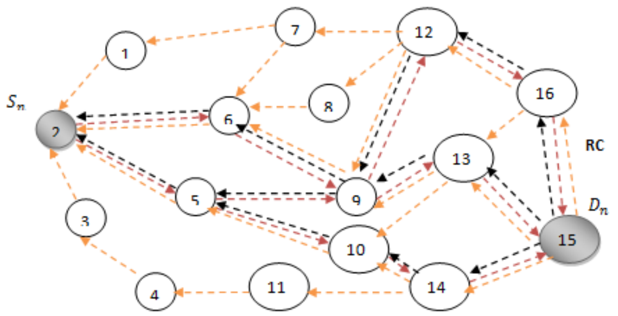
3.3 SLW-AODV Routing Process

SLW-AODV protects MANETs against BHA and CBHA. Additionally, SLW-AODV is capable of identifying BHA during the data forwarding process. The significant difference between AODV and SLW-AODV is that SLW-AODV extends the RD process of AODV to execute the RC mechanism. Moreover, unlike AODV, which creates only one route, the proposed SLW-AODV establishes three routes for a given source and destination node pair. The proposed SLW-AODV completes the route establishment process in three steps. They are- 1) Request, 2) Reply, and 3) Confirm. To explain the process of SLW-AODV, a network of 16 nodes is created, as shown in Figure 1. It is assumed that Node 2 is the source and Node 15 is the destination. Since SLW-AODV is a reactive protocol, S_nStarts RD when it wants to send data to D_n. At this stage S_n Generates a challenge value w and conveys it to the nodes. Further $S_n$creates ARREQ by putting w and hop count (h_c) and broadcast ID (b_{id}) in the respective fields of ARREQ. Then S_n Broadcasts ARREQ and receives at nodes 1, 3, 5 and 6. According to Figure 1(a), when an ARREQ is received at an intermediate node, it first checks whether the current ARREQ was previously received from the same node. Additionally, it checks the total ARREQ count to determine whether it exceeds three from different nodes. If the above situations have not happened, then it performs 4 steps. They are- 1) Increases the count of ARREQs received, 2) Establishes a reverse route to S_n Via a forwarding node. 3) The routing table is updated with the challenge value, 4) Increments the hop count, if the node at which the ARREQ was received is not a D_n And then rebroadcasts the ARREQ again to its neighbour nodes. The critical point to note is that SLW-AODV allows three routes through three different nodes to S_n. The above procedure is repeatedly performed by neighbour nodes until ARREQ reaches D_n. Upon receiving ARREQ, the D_n Starts the reply process.



(a)

(b)



(c)

Figure 1: SLW-AODV routing process

On the destination side, the reply process commences immediately after receiving the first ARREQ. At this phase, it generates a response value v and propagates to the neighbour nodes present on the routes through which the ARREQ is received. Furthermore, the SLW-AODV allows up to three ARREQs from three different nodes, and each neighbour node can receive up to three reply packets. While receiving ARREQ, D_n Performs four steps. They are, 1) If D_n Observed that the same ARREQ is received in the past, it skips the step and starts directly with the second step; otherwise, the destination node compares the response value according to Eq.(1).

$$v = \lfloor x(\zeta) \rfloor \tag{1}$$

Where $\lfloor . \rfloor$rounds the argument present in it and $x(\zeta)$ is a Logistic Chaotic map [87], [88]. Mathematically, it is calculated as

$$x(\zeta) = \mu x(\zeta - 1)[1 - x(\zeta - 1)] \tag{2}$$

Where ζ It is a secret value generated by D_nRandomly, and it represents the total number of iterations. μ Is the control parameter and $x(0)$ Is the initial value of the Logistic map. The mathematical representation of μ and $x(0)$ It is formulated through two random numbers generated by the destination nodes. They are r_{m1} and r_{m2}.

$$x(0) = \frac{\omega}{r_{m1}} \text{mod} 1 \tag{3}$$

$$\mu = \frac{\omega}{r_{m2}} \text{mod} 1 \tag{4}$$

Note that Eq.(3) and Eq.(4) generate $x(0)$ and μ Respectively, within their valid ranges, the calculated chaotic maps explore significant features of the applied map. Both equations include the challenge generated by S_nSuch that the source gets an awareness of the D_n . Moreover, the generation of these values is dynamic, and they are dependent on the nodes serving as S_n and D_n. Hence the corresponding $S_n$and D_n Will receive distinct, chaotic maps that provide more security.

The significant advantage of the Logistic map is that it is widely employed in general applications to provide security for multimedia content. Moreover, the Logistic map exhibits excellent features, including randomness, ergodicity, and sensitivity to control parameters and initial conditions. The dynamicity of control parameters adds a layer of security. Hence, the use of chaotic maps provides more protection to the proposed method. Next, the time is updated at D_n According to the following expression-

$$t = \sum_{i=1}^{n} (t_{ri} - \tau) / {2n} \tag{5},$$

where τ Denotes the time instance at which the chaotic map is generated, while t_{ri} Is the time instance of the i^{th} ARREQ received by D_n. n denotes the total ARREQ's account with a similar broadcast ID. Here, the maximum value of n is allowed up to 3 (i.e., $1 \leq n \leq 3$) Next, D_n generates an ARREP by including the response value along with the secret values used to produce the response value, such as r_{m1} , and r_{m2}. Then, ARREP is unicasted by D_n To its neighbour nodes, i.e., the node through which the ARREQ is obtained at D_n. In this case, as shown in Figure.1(b), the request that unicasted by D_nWill be received at nodes 13, 14, and 16.

Upon receiving the ARREP at any intermediate node, it executes mainly 4 steps. At first, it creates a reverse route to D_n Via the forwarding node. At this phase, every node is allowed to establish a maximum of 3 routes to D_n (for example, in Figure 1(b), node 9 can establish two reverse routes through node 12 and node 13 to D_n). Secondly, the intermediate nodes keep every route in the waiting state, i.e the route cannot be allowed to use until it gets confirmation from the D_n. A route will get into an operational state after being confirmed by the confirmation process initiated by the D_n. Thirdly, the intermediate node fetches the response value v from ARREP and updates it in its routing table.

Fourthly, if S_n receives ARREP, it simply

Retrieval Number: 100.1/ijsce.A35920313123
DOI: 10.35940/ijsce.A3592.0313123
Journal Website: www.ijsce.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

ignores it; otherwise, the intermediate node performs unicast of every obtained ARREPs with a similar response value to S_n Over different routes (as shown in Figure 1(b)), if node 9 receives replies with the same response value, it performs unicasting of one ARREP through node 12 and another through node 13. If the response values of ARREPs differ, then the node unicasts them via the same forwarding node. At last , D_n Starts the confirmation process when the time reaches zero. At the confirmation round, the proposed SLW-AODV performs three steps they are 1) The secret value generated by the destination node, such as ζ, r_{m1}, and r_{m2} 1) Revealed to neighbour nodes, 2) Malicious nodes that tend to compromise with BHA and CBHA are identified, 3) Routes with malicious nodes are discarded, and information is propagated to the entire network.

When D_n When the time reaches zero value, it creates a route confirmation message with eight fields and keeps the secret values such as ζ, r_{m1}, and r_{m2} Into it. Next, the route confirmation is broadcast by D_n As shown in Figure (b), it receives at nodes 13, 14, and 16. Upon receiving the route confirmation at any node which is not a part of the route within the specific time period, it performs a comparison between the corresponding values of ζ, r_{m1}, and r_{m2}. If most of the route confirmation messages have similar values, then the node rebroadcasts only a few RCs that have significant similarity. If the count of response values present in the RC message is neutral, then the intermediate nodes neglect those messages. On the other hand if the route confirmation messages that were received at a node which lies on the route (ex. 16, 14 13, 12, 10, 9, 6 and 5) from different nodes in the particular time period, then that node executes majorly five steps- 1) Calculate response value as per Eq.(1) for every RC with the help of secret values present in it such as ζ, r_{m1}, and r_{m2} And *w*. 2) Compare the response values with each other to find the most closely matched value. Let it be denoted as v_m, 3) v_m is compared with all v_i Values that were linked with different routes in the routing table, 4) If the node finds that v_m and v_i If they are the same, then it triggers the ith route into operational state. Otherwise, the node declares that the respective node linked with the route is not trustworthy and has a malicious nature. Further, the corresponding node is removed from the routing table of the i^{th} route. Finally, if the intermediate node is not S_n,It broadcasts the RC message to its following hop neighbour nodes to find the one with maximum mat.ch, otherwise S_nInitiates the transmission of data packets to D_n.

IV. EXPERIMENTAL ANALYSIS

This section presents a set of conducted experiments that compare the performance of the proposed SLW-AODV protocol against 4 methods, namely AODV, Modified Sequence Number AODV (MSN-AODV) [17], Cooperative Prevention Method AODV (CPM-AODV) [25], and Reverse AODV (RAODV) [28] protocols under cooperative blackhole attack.

4.1. Simulation set up

In the simulation setup, we have created a network, and the number of nodes chosen varies from 20 to 60. The area of the network is considered to be 1,000 m × 1,000 m. For every simulation, the mobile nodes are deployed randomly, and their positions are unrelated to those of the earlier simulation study. The transmission range varies from 10% to 25% of the network area, i.e., 100, 150, 200, and 250 meters, and the average speed of the mobile node is altered from 5 m/s to 25 m/s. On average, the source node generates 10 packets per second, with a packet size of 512 kilobytes. Table 1 shows the simulation setup details.

Table 1: Simulation set-up

Network parameter	Value
Number of nodes	20-60
Area of Network	1000*1000 m^2
Transmission Range	10% to 25% of the network area
Average Node Speed	5 m/s to 25 m/s
Traffic Type	Constant Bit Rate (CBR)
Data packets	10
Simulation Time	200 Seconds
Size of data packets	512 kilobytes

4.2 Performance Metrics

The performance is measured in terms of Throughput, Packet Delivery Ratio (PDR), and end-to-end delay (E2ED). The formal definitions of these metrics are given below;

Throughput: It is the amount of data received in a given period, typically measured in bits per second. The throughput metric measures the amount of productivity that reaches the destination node and is sent by the source node. Mathematically, the throughput is measured as

$$Throughput = \frac{Number\ of\ packets\ received \times 8}{(t-t_f)} \qquad (6)$$

Where t_f Is the time at which the first packet is received, and t Is the time at which the last packet was received or the simulation time when the session is not completed? Here, packets received are in kilobytes, and time is in seconds; hence, the unit of Throughput is Kilobytes per second (Kbps).

PDR: It is the ratio of the number of packets received to the number of packets sent by the destination and source nodes, respectively. PDR is measured for both links and paths. To determine the quality of a link, the PDR is measured at the link, which is a connection between only two nodes. In contrast, for a path, the PDR that occurs at individual links is summed and then divided by the total number of links on that path. Mathematically, PDR is measured as

$$PDR = \frac{P_r}{P_s} \times 100 \qquad (7)$$

Where P_s Is the total number of packets sent and the P_r It is the total number of packets received.

E2ED: It is the time that a packet takes from its source until it reaches its destination. Average E2ED (AE2ED) refers to the combination of delays, namely propagation, buffering, queuing, and retransmission. Mathematically, AE2ED is measured as

$$AE2ED = \frac{1}{P}\sum_{j=1}^{P} Delay\,(j) \quad (8)$$

Where P is the total packet count, $Delay\,(j)$ The propagation delay of packet j is measured as the difference between two successive time instants, specifically, the time the packet is received at the destination node and the time it is transmitted at the source node.

4.3 Result Analysis

The performance of the proposed SLW-AODV protocol is validated through several simulation experiments, considering Throughput (kbps), AE2ED (sec), and PDR (%) for both blackhole and cooperative blackhole attacks. The results of Throughput in Figure.2, AE2ED in Figure. Figure 3, PDR in Figure 4, shows the black hole attack for a malicious node for all methods with respect to simulation time.

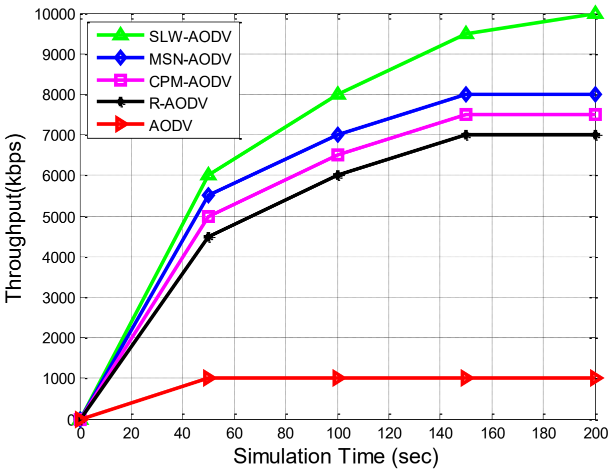


Figure 2: Throughput (kbps) for Varying Simulation Time (Sec) Under Blackhole Attack

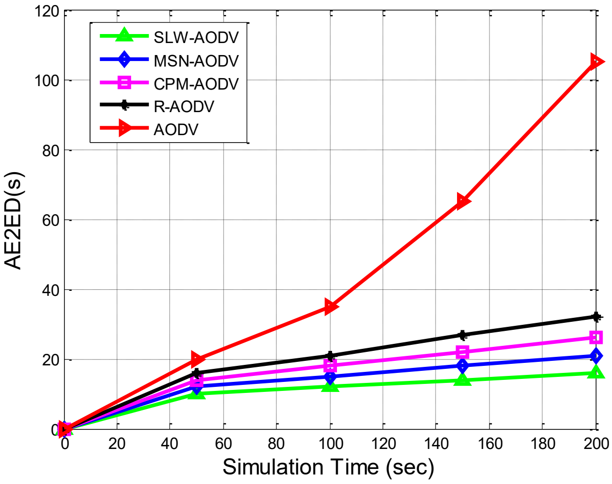


Figure. 3 AE2ED(s) for Varying Simulation Time (Sec) Under Blackhole Attack

As the simulation time increases, the throughput also increases gradually for the methods, as shown in Figure 2. There is no proper security mechanism for the AODV protocol to tackle the blackhole attack compared to the remaining methods. The throughput of the AODV protocol is very low. The throughput of the proposed SLW-AODV protocol is high because it efficiently identifies malicious nodes, employing a Challenge-Response-Confirmation strategy that is not available in conventional methods. Thus, the throughput of the proposed method is 6700 kbps, whereas it is 5700 kbps, 5300 kbps, 4900 kbps, and 800 kbps for MSN-AODV, CPM-AODV, R-AODV, and AODV, respectively.

Figure 3 shows the variation of AE2ED of the considered methods with respect to simulation time. As simulation time increases, AE2ED also increases. When the conventional AODV protocol is attacked with a blackhole attack, it drops packets due to the lack of security mechanism provisions. Hence, data transmission is delayed, and AE2ED is high in the conventional AODV protocol. When this type of attack occurs in the proposed method, it chooses three alternate ways to redirect data packets towards the destination. The proposed method reduces the delay compared to existing methods. The AE2ED of the proposed method is 10.4 seconds, whereas it is 13.2 seconds, 16.4 seconds, 19.2 seconds, and 45 seconds for MSN-AODV, CPM-AODV, R-AODV, and AODV, respectively.

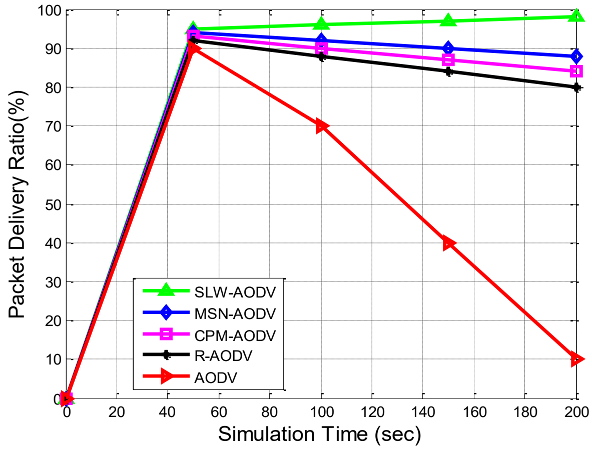


Figure 4 Packet Delivery Ratio (%) for Varying Simulation Time (Sec) Under Blackhole Attack

Figure 4 shows the variation of PDR of the considered methods with respect to simulation time. As simulation time increases, PDR also increases. To route data packets towards the destination, the proposed method utilises an efficient routing mechanism, such as the Challenge-Response-Confirmation strategy. The conventional methods are more vulnerable to black hole attacks and dropping packets in the middle. Initially, all packets are forwarded successfully towards the destination. However, when the attack occurs, conventional methods drop the packets in the middle, resulting in a decrease in PDR. Thus, the PDR of the proposed method, i.e., SLW-AODV, is 77.2%, whereas it is 72.8%, 70.8%, and 69% for MSN-AODV, CPM-AODV, and R-AODV, respectively. For AODV, the rate is 42%, as AODV lacks mechanisms to detect either black hole attacks or cooperative black hole attacks.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

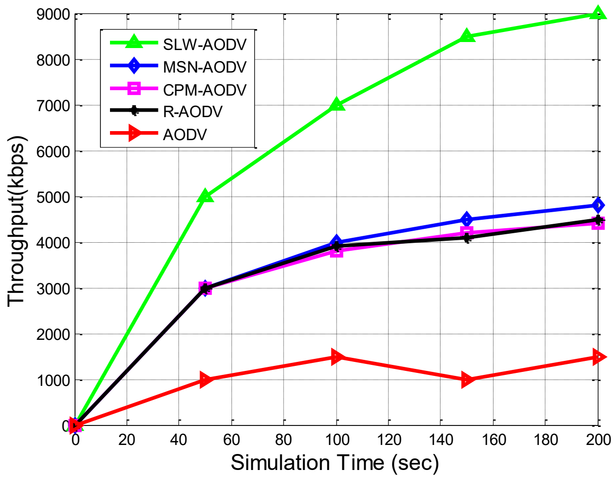


Figure 5 Throughput (kbps) for varying simulation time (sec) under cooperative blackhole attack

Figures 5, 6, and 7 show the performance of five protocols under the cooperative black hole attack. Figure 5 illustrates the throughput measurement over simulation time. As the simulation time increases, the network's throughput also increases. The data packets are forwarded through malicious nodes. The existing methods, such as R-AODV, CPM-AODV, and MSN-AODV, drop packets in the middle, whereas the proposed method can select alternate paths to forward data packets towards the destination. Hence, the throughput in the proposed method is higher than that of the existing methods. The conventional AODV method lacks security provisions, resulting in a rapid decrease in throughput as the simulation time increases. Thus, the throughput of the proposed method is 5900 kbps, whereas it is 3260 kbps, 3080 kbps, 3100 kbps, and 1000 kbps for MSN-AODV, CPM-AODV, R-AODV, and AODV, respectively.

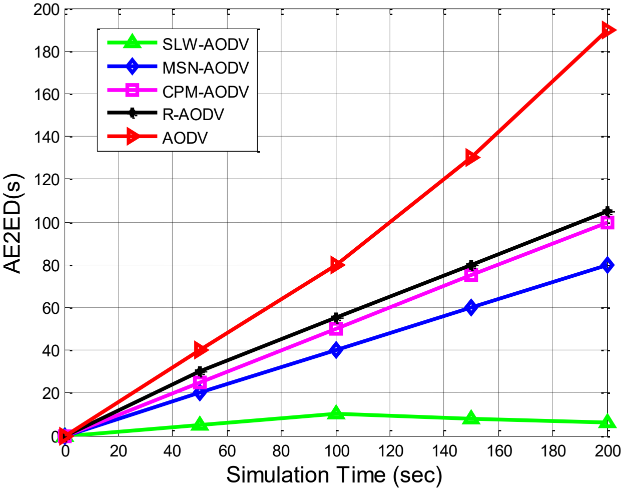


Figure 6 AE2ED (sec) for Varying Simulation Time (Sec) Under Cooperative Blackhole Attack

Figure 6 shows the measurement of AE2ED for five protocols with respect to simulation time. From Figure 6, it is known that as the simulation time increases, the AE2ED also increases. When the data packet is forwarded through the malicious nodes, the conventional AODV protocol immediately drops the packets and is unable to forward them to the destination. In such a case, the proposed method chooses an alternate path to forward the data packets towards the destination. As the simulation time increases, packet forwarding can be delayed in the conventional AODV protocol compared to the proposed method. Thus, the AE2ED of the proposed method is 5.8 seconds, whereas it is 40.3 seconds, 50.5 seconds, 54.5 seconds, and 88.3 seconds for MSN-AODV, CPM-AODV, R-AODV, and AODV, respectively.

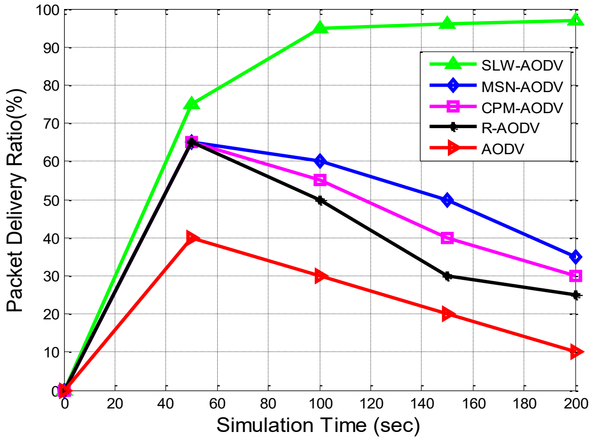


Figure 7. PDR (%) for Varying Simulation Time (Sec) Under Cooperative Blackhole Attack

Figure 7 illustrates the measurement of PDR for five protocols in terms of simulation time. From Figure 7, it can be observed that as the simulation time increases, the PDR decreases. The proposed method efficiently detects malicious nodes, and when an attack occurs, it chooses various alternate paths to forward data packets without dropping any packets. However, the conventional AODV protocol drops the packets in the middle of transmission and hence the PDR reduces. Thus, the PDR of the proposed method is 72.6%, whereas it is 42.3%, 48.5%, 44.3%, and 20.2% for MSN-AODV, CPM-AODV, R-AODV, and AODV, respectively.

V. CONCLUSION

This paper introduced a simple and effective SLW-AODV protocol to protect a MANET from blackhole and cooperative blackhole attacks. The SLW-AODV protocol employs a Challenge-Response-Confirm pattern to establish trusted routes, utilising five types of messages and an efficient routing process to transfer data packets. The performance of the proposed method is validated through the metrics, viz. Throughout AE2ED, PDR under black hole and cooperative black hole attack. When compared to the considered methods, viz. MSN-AODV, CPM-AODV, R-AODV, and AODV, the proposed method, i.e., SLW-AODV, has performed very well, with results for Throughput, AE2ED, and PDR showing its superiority.

ACKNOWLEDGEMENT

The authors acknowledge the immense help received from the scholars whose articles are cited and included in the references of this paper. The authors are obliged to the authors/editors/publishers of all those articles, journals and books from where the literature of this paper has been reviewed.

DECLARATION

Funding/ Grants/ Financial Support	No, I did not receive.
Conflicts of Interest/ Competing Interests	No conflict of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval or consent to participate, as it presents evidence that is not subject to interpretation.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	Conceptualization, software, methodology, validation, formal analysis, investigation, M V D S Krishna Murty; writing—original draft preparation, M V D S Krishna Murty; writing—review and editing, M V D S Krishna Murty, Lakshmi Rajamani;

REFERENCES

1. G. A. Walikar, R. C. Biradar, A survey on hybrid routing mechanisms in mobile ad hoc networks, *Journal of Network and Computer Applications*, 77 (2017) 48-63. [CrossRef]
2. M. K. Gulati, K. Kumar, A review of QoS routing protocols in MANETs, *in: 2013 International Conference on Computer Communication and Informatics,* 2013, pp. 1-6. [CrossRef]
3. M. M. Alani, "Manet security: A survey," in *2014 IEEE ICCSCE,* 2014, pp. 559-564. [CrossRef]
4. M. Amadeo, C. Campolo, A. Molinaro, Forwarding strategies in named data wireless ad hoc networks: Design and evaluation, *Journal of Network and Computer Applications,* 50 (2015) 148-158.587. [CrossRef]
5. S. Kalita, B. Sharma, and U. Sharma, ``Attacks and countermeasures in mobile ad hoc network - An analysis", *Int. J. Adv. Comput. Theory Eng.*, vol. 4, no. 3, pp. 16-21, 2015.
6. H. L. Nguyen and U. T. Nguyen, "A study of different types of attacks on multicast in mobile ad hoc networks", *Ad Hoc Netw.*, vol. 6, no. 1, pp. 32-46, 2008. [CrossRef]
7. C. Panos, C. Ntantogian, S. Malliaros, and C. Xenakis, ``Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks," *Comput. Netw.*, vol. 113, pp. 94-110, Feb. 2017. [CrossRef]
8. N. Khanna and M. Sachdeva, ``A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs," *Comput.Sci. Rev.*., vol. 32, pp. 24_44, May 2019. [CrossRef]
9. S. Sharma, Rajshree, R. P. Pandey, V. Shukla, "Bluff-Probe Based Black Hole Node Detection and Prevention", *IEEE International Advanced Computing Conference (IACC 2009), pp. 458-462, March* 2009. [CrossRef]
10. C. Jiwen, Y. Ping, C. Jialin, W. Zhiyang, L. Ning, "An Adaptive Approach to Detecting Black and Grey Hole Attacks in Ad Hoc Network",24th IEEE International Conference on Advanced Information Networking and Applications (AINA 2010), pp. 775-780, April 2010.
11. Y. F. Alem, Z. C. Xuan, "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection",*2nd International Conference on Future Computer and Communication (ICFCC 2010*), Vol. 3, pp. 672-676, May 2010.
12. Dr. S. Tamilarasan, "Securing and Preventing AODV Routing Protocol from Black Hole Attack using Counter Algorithm*", International Journal of Engineering Research & Technology (IJERT)* Vol. 1 Issue 5, July 2012, ISSN: 2278-018.
13. Haas, Z. J., 1997 (ps). A new routing protocol for the reconfigurable wireless networks. Retrieved 2011-05-06.
14. A. Tripathi and A. K. Mohapatra, "Mitigation of Blackhole attack in MANET," *2016 8th International Conference on Computational Intelligence and Communication Networks (CICN)*, pp. 437-441, 2016. [CrossRef]
15. T. N. D. Pham and C. K. Yeo, "Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks," in *IEEE Transactions on Mobile Computing*, vol. 15, no. 5, pp. 1116-1129, 1 May 2016. [CrossRef]
16. A. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," in *IEEE Access*, vol. 7, pp. 95197-95211, 2019. [CrossRef]
17. S. Shrestha, R. Baidya, B. Giri and A. Thapa, "Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol," *2020 8th International Electrical Engineering Congress (iEECON)*, 2020, pp. 1-4. [CrossRef]
18. E. Elmahdi, S. Yoo and K. Sharshembiev, "Securing data forwarding against blackhole attacks in mobile ad hoc networks", *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, 2018, pp. 463-467. [CrossRef]
19. N. G. Wakode, "Defending blackhole attack by using acknowledgement-based approach in MANETs," *2017 International Conference on IoT and Application (ICIOT)*, 2017, pp. 1-6. [CrossRef]
20. S. Pandey and V. Singh, "Blackhole Attack Detection Using Machine Learning Approach on MANET," *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 2020, pp. 797-802. [CrossRef]
21. G. Li, Z. Yan and Y. Fu, "A Study and Simulation Research of Blackhole Attack on Mobile AdHoc Network," *2018 IEEE Conference on Communications and Network Security (CNS)*, 2018, pp. 1-6.
22. V. Sharma, Renu and T. Shree, "An adaptive approach for Detecting Blackhole using TCP Analysis in MANETs," *2nd International Conference on Data, Engineering and Applications (IDEA)*, 2020, pp. 1-5. [CrossRef]
23. S. Kaushik, K. Tripathi, R. Gupta and P. Mahajan, "Performance Analysis of AODV and SAODV Routing Protocol using SVM against Black Hole Attack," *2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM)*, 2022, pp. 455-459. [CrossRef]
24. S. Barai and P. Bhaumik, "Detection and Mitigation of Blackhole Attack Effect in Opportunistic Networks," *2021 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 155-160. [CrossRef]
25. T. Terai, M. Yoshida, A. G. Ramonet and T. Noguchi, "Blackhole Attack Cooperative Prevention Method in MANETs," *2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW)*, 2020, pp. 60-66. [CrossRef]
26. M. B. M. Kamel, I. Alameri and A. N. Onaizah, "STAODV: A secure and trust-based approach to mitigate blackhole attack on AODV-based MANET," *2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 2017, pp. 1278-1282.
27. I. Kaushik, N. Sharma and N. Singh, "Intrusion Detection and Security System for Blackhole Attack," *2019 2nd International Conference on Signal Processing and Communication (ICSPC)*, 2019, pp. 320-324. [CrossRef]
28. F. Taranum, A. Sarvat, N. Ali and S. Siddiqui, "Detection and Prevention of Blackhole node," *2020 4th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech)*, 2020, pp. 1-7. [CrossRef]

AUTHORS PROFILE

M V D S Krishna Murty Completed B.E. in CSE from the University of Madras, Chennai and M. Tech in CS from JNTU, Hyderabad. Currently, he is a research scholar in the Department of CSE at JNTUH, Hyderabad. His areas of interest are MANETs and Machine Learning. He has 21 years of teaching experience and 5.5 years of industrial experience as a software professional. He has presented technical papers in the area of MANETs and Data Science at international conferences held in India. Additionally, he has published in reputable international journals.

Dr. Lakshmi Rajamani obtained a Ph.D. in Computer Science (CSE) from Jadavpur University, Kolkata, and worked as a Professor and Head in the Department of CSE at OUCE, Osmania University, Hyderabad. Her areas of interest are Fuzzy Logic and Network Security. She has published several papers in reputable international journals. Also, she has presented technical papers in international conferences held in India and abroad.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

Retrieval Number: 100.1/ijsce.A35920313123
DOI: 10.35940/ijsce.A3592.0313123
Journal Website: www.ijsce.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)