Computer Systems Science & Engineering
DOI:10.32604/csse.2023.024340
Article

Tech Science Press

Swarm Intelligence Based Routing with Black Hole Attack Detection in MANET

S. A. Arunmozhi*, S. Rajeswari and Y. Venkataramani

Department of Electronics and Communication Engineering, Saranathan College of Engineering, Thiruchirappalli, 620012, India
*Corresponding Author: S. A. Arunmozhi. Email: arunmozhi-ece@saranathan.ac.in
Received: 14 October 2021; Accepted: 17 January 2022

Abstract: Mobile Ad hoc Network (MANET) possesses unique characteristics which makes it vulnerable to security threats. In MANET, it is highly challenging to protect the nodes from cyberattacks. Power conservation improves both life time of nodes as well as the network. Computational capabilities and memory constraints are critical issues in the implementation of cryptographic techniques. Energy and security are two important factors that need to be considered for improving the performance of MANET. So, the incorporation of an energy efficient secure routing protocol becomes inevitable to ensure appropriate action upon the network. The nodes present in a network are limited due to energy constraints and secure communication protocols. Hence, the current study proposed an energy-efficient defense scheme using swarm intelligence approach. The functioning of the proposed method was validated under NS2 simulation. The experimental results confirmed that the proposed work outperformed existing methods in terms of packet delivery ratio, average end-to-end delay and throughput.

Keywords: Energy; security; swarm intelligence; optimization; routing

1 Introduction

Black Hole (BH) attack is a rapidly spreading dynamic attack that degrades the presentation and unwavering quality of networks. This is because such attacks relinquish all the approaching packets using noxious node. The node that experience BH attack tricks every other node in the network used for transmission with other nodes by portraying that it has the best route towards the end node. Here, Ad hoc On-demand Distance Vector (AODV) is a responsive directed convention that does not have any procedures for identification and prevention of BH attacks in Mobile Ad hoc Networks (MANETs). The aim of the BH attack is to bring the Wireless Sensor Network (WSN) traffic to a standstill and publicize that it has the most substantial and limited way to be considered for impeding information [1]. The source node starts its course of transmission by sending the route request message as broadcast for any end node. When this route request message is encountered by BH node, it promptly reacts with a fraudulent route reply by embedding 'high sequence number' [2]. This information is observed as if it has arrived from the correct destination or through the node with the most limited end destination node [3]. Subsequently, the source node is tricked by fraudulent routing path packet and disseminates the information along the path in network. In response to this, the BH node drops the packets instead of

disseminating the information [4]. Nodes are assessed through trust measures and its levels [5]. On the off chance, an adjoining node may have a trust level lesser than the pre-declared edge value of the route request. It is recognized as a misbehaving node and is not considered during route selection [6]. Secure AODV is the agent of several secure adaptations of AODV principle and is developed based on the exploitation of cryptographic methods. The aim of this agent is to protect the control management packets of AODV for strong attacks [7].

MANET lacks sophisticated structure to overcome cyberattacks. Since MANET utilizes wireless connections to associate with nodes, it is vulnerable to threats from unauthorized users who aim at leaking data privacy [8]. MANETs do not have focal framework for communication management among the nodes. As a result, the nodes depend on each other to transmit the information from one node to the other and finally the end node [9]. 'Denial of Service' (DoS) attack is viewed as a serious security threat to MANET. In such type of attacks, a misbehaving node consumes heavy battery power actually intended to be consumed by multiple nodes. This occurs as a result of camouflaging those nodes to advance an immense measure of information. MANET attacks are categorized into 'active' and 'passive' attacks [10].

Most of the times, nodes start disclosure stage to identify a path to reach the end node. The source node of MANET communicates the broadcasted message to find a path that reaches the destination node; any node that gets the broadcasted message informs the sender that it has a new way to destination node [11]. At this point, when BH gets the broadcasted information, it quickly transmits an answer to the sender, assuring that it has the freshest and the most limited path to the 'destination' node [12]. Based on this response, the source node accepts the answer assuming that there is no device to validate the authenticity of the broadcasted information. However, it is challenging to find whether it starts with an ordinary node or from a BH attack node [13]. The source node begins to send the data to BH node so that the data is transmitted to the end node. The BH opening node consequently begins to relinquish the sent packets [14]. BH attack is viewed as one of the famous attacks that hurt the network and many research works are conducted to resolve this attack that hurts the MANET [15]. BH attack over MANET has been discussed in the literature earlier too [16]. Proximity set-based BH detection in MANET is presented in the study conducted earlier [17]. It is fundamental to secure the MANET to protect the network, since it is vulnerable to different kinds of attacks [18]. Subsequently, in literature [19], the authors discussed about forward routing and the misbehaving node that can adjust the association between nodes or relinquish the sent information. Security-based BH analysis in routing path has been described earlier [20]. In literature, optimized BH attack detection is performed using Genetic Algorithm [21,22]. BH attack is a dynamic DoS assault as it disturbs the directing administrations in organization [23,24]. The reliability of AODV convention is undermined by specific kind of assaults, for instance, BH. Secure routing protocol with localized data transfer was validated in the study conducted earlier [25]. In literature [26], the researchers investigated about mitigating energy consumption in WSN using greedy algorithm. In MANET, Spider monkey optimization has been found as the best fit for star-based computation in BH identification [27]. MANET does not utilize any key dispersion measure and no progressions were made in terms of AODV routing algorithm. General spider monkey optimization procedures and fuzzy-based logics have been detailed in the studies conducted earlier [28,29]. In literature, dynamic routing AODV (DPRAODV) approach has been presented [30]. Optimized link state routing with MANET with AODV was analyzed earlier based on BH attacks [31].

BH attack is one of the commonly observed attacks and is generally focused on routing protocols like AODV and Dynamic Source Routing (DSR) in MANETs. AODV and DSR-based MANET utilize Network Simulator (NS) 2 and NS-3 to overcome the BH attacks at different situations. These entities aim at breaking down the conventional results. Various situations have been presented and handled to validate the versatility of nodes. Throughput and other few parameters were checked to check the proposed method's packet conveyance proportion.

The primary objective of current study is to improve the performance of MANETs by reducing BH attack from network traffic. The performance is evaluated by means of packet delivery ratio, delay, energy, and network lifetime. In the proposed work, swarm intelligence approach in route optimization is tested and the results were found to be promising compared to existing approaches. Such optimized routing path results in enhanced MANET outcomes. It also encourages the future researchers to shift their focus upon this domain. The proposed method was validated through simulation using NS-2 simulation tool.

2 Related Works

S A Arunmozhi, and Y Venkataramani, (2012) presented a BH attack detection approach for MANET since it is one of the major issues that affect the network traffic. Neighborhood node detection and route status monitoring are two primary entities that produce the result. Dynamic node updates and threshold value for every sequence help in improving the security of network. Here, the neighborhood route monitoring table reduces the traffic issue. Malicious node detection, by the proposed protocol, established a delay-efficient ad hoc network.

R Hemalatha and S A Arunmozhi, (2016) proposed a secure MANET model to overcome BH attacks using a collaborative defense scheme. The proposed model i.e., Bait detection scheme for route selection reduces the BH attack. While performing data transmission, encryption is done which uses elliptic curve-ElGamal cryptosystem with secure model. The model was validated under different parameters such as throughput, routing overhead, packet delivery ratio and end-to-end delay. This crypto-based encryption and bait detection approach enhanced the performance of MANET.

Avijit M, et al. (2016) presented a defense mechanism over BH attack in medical-based wireless sensor network with Internet of Things (IoT) applications. Forward routing is essential for medical-based networks, since it allows the transmission of data and information. Further, it supports a versatile network in a number of emergency clinics. Cryptographic hashes and threshold models are used in the identification of assaults. M.Rajesh Babu, et al. (2015) presented a proactive alleviation of BH attack in MANETs. In general, MANET is defenseless against network attacks, especially BH attack, while its variants can harm the whole MANET framework. So, an alleviation technique was proposed in this study which comprises of opportune command method, opening recognition calculation, and malicious behavior strategy identification to distinguish the sensitive nodes.

Adwan Y and Mahmoud Abu Zant, (2018) presented a defense method to identify BH attacks in MANETs using time-based bait technique. In this study, MANET is secured by using the most blazing point in network fields. BH node tricks each node in the network to communicate with other node by masquerading that it has the efficient way to end node. AODV is a responsive directing convention which does not follow any procedures to distinguish and kill the BH nodes in a network. In this study, AODV in combination with another strategy that utilizes clocks and teasing identified and confined the BH assaults. This unique geography changing procedure empowers MANET nodes to segregate nodes and also identify BH nodes in the network.

Pooja Vij, et al. (2012) proposed a broadcast-based detection method to improve the security by reducing the BH attack in MANETs. This is associated with routing processes that are utilized over AODV convention. In this attack, the noxious node portrays that it has the efficient way to end node. It is an approach that pauses and verifies the answers that arise out of every adjoining node to track down the BH-affected nodes. In this research, the authors identified BH attackers based on their transmission ID. The proposed directing approach recognizes and provides a method for the amendment of BH detection in AODV.

Zohaib H, et al. (2020) presented an intelligent defense approach to overcome BH attack in communication system so that it can be applied in autonomous vehicles and connected vehicles. Reduction of BH assaults is quite possibly the most difficult task and the basic security issue in Vehicular Adhoc Network (VANETs), self-governing & associated vehicles. In any case, rather than sending packets to adjoining node, malicious nodes avoid them and drop any information that may have crisis alerts. This study compared the existing methodologies against the proposed method under different network performance metrics. Ruo Jun Cai, et al. (2019) discussed a 'self-cooperative trust model' routing strategy in MANETs. The parameters that additionally devise the plan for routing conventions in MANETs turn out to be exhaustive. In this background, misbehaving nodes impersonate the intellectual interaction that focuses on trust level data to forestall different routing interruption attacks. Here, the portable nodes transfer the trust data based on its own intellectual property. Every node powerfully advances its insight to reject the traffic node. The approach plot is presented under different directing interruption attack instances and better outcomes were achieved. E O Ochola, et al. (2017) presented a reactive routing protocol strategy since MANETs undergo different security threats, because of its trademark highlights that include dedicated control unit, open communication platform, foundation less and dynamic geography.

3 Proposed Method

BH assault may lead to issues like packet dropping, misguiding of the route data between end nodes etc. The main strategy applied in the proposed method is based on swarm intelligence technique. Here, 'Spider Monkey Optimization' (SMO) is employed to change AODV routing convention. In this technique, the insect, spot at every node, computes an inherent pheromone value to send the proportion to node. AODV has the trust levels of adjoining nodes for the selection of routing path.

Fig. 1 shows the overall processing of the proposed work. After detecting BH attacks in routing protocol, SMO helps in stabilizing the path which in turn improves the packet delivery rate, packet conveyance proportion, start to finish deferral and throughput improvement. Delay and load conveyance proportion gets reduced, when the organization is assaulted by BH, on the grounds that noxious node retains or transmits a portion of packets. AODV routing is performed to detect the BH which is selected based on neighborhood detection of star BH. Then, it is routed by the shortest path of routing with objective function-verified state. Based on a user's request, transmission is performed which increases the security of the state.

3.1 AODV with Secure Analysis

BH attack is a result of massive sized star which possesses extreme gravitational power. In this regard, a malicious node gives false data while performing the shortest routing path to destination in order to get all information packets. In current research work, SMO is proposed to overcome BH attack in AODV directing protocol. Some of the major advantages in using swarm intelligence upon routing protocol are routing optimization, robustness, flexibility, implementation and cost-effectiveness. Here, the heuristic calculations are attempted to track down the ideal arrangement of a particular issue. This is done so without investigating the entire inquiry space and consuming the least possible execution time. Heuristic techniques are intended to achieve great outcomes for a particular malicious issue quickly, than the existing approaches with nearby hunting strategies. The principle drawback of these techniques is that it catches the neighborhood desired states of optimization.

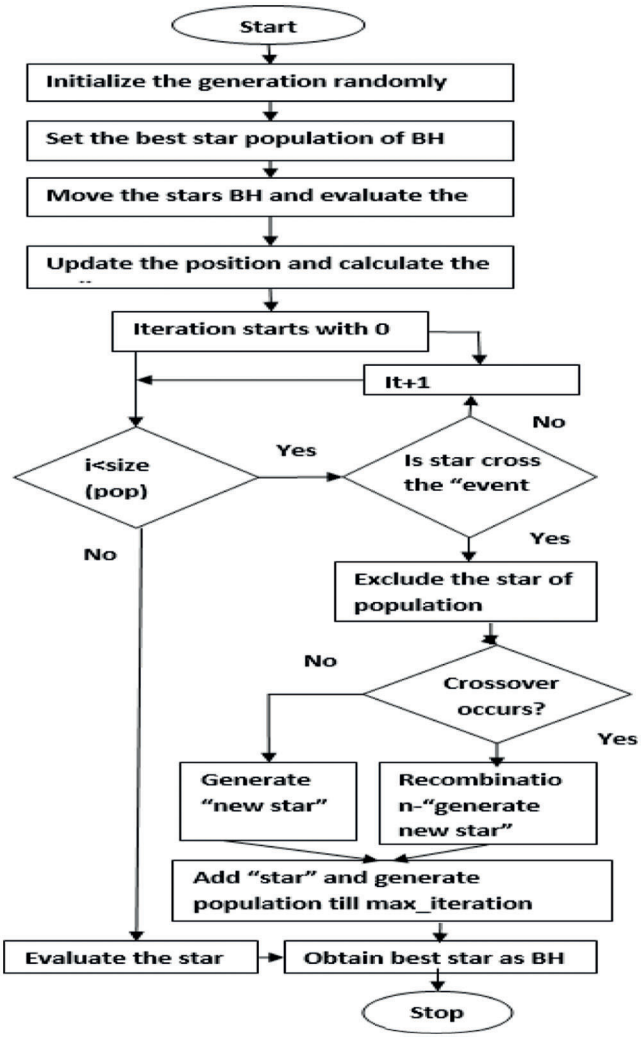

Figure 1: Flow diagram of overall system

3.2 Swarm Intelligence

Swarm intelligence technique on traffic path selection approach in MANET is performed with the help of spider monkey optimization. Since MANETs are increasingly used these days, security has become a fundamental prerequisite to ensure seamless communication between the versatile nodes. To overcome the difficulties, there is a need to assemble a multi-factorial security arrangement that accomplishes both wide assurance and attractive execution of the organization. Both recombination and re-evaluation strategy helps in the detection of whole network, by taking the maximum probability range of star BH. From this, crossover optimization function is used to select the optimal star. After finding the radius, the probability of star BH is changed to 0.5, 0.75 and 1. BH assault is one of the potential attacks identified by horizon and calculus radius; Calculus radius 'R_s' is expressed as follows,

$$R_s = (2GM_{bh})/L_s^2 \tag{1}$$

where 'G' represents the gravitational force and 'M' represents the mass value of BH attack. L_s represents the speed of light. By doing this, the malicious node can deny the traffic from source node. It is utilized as a disapproval of administration attack, where it can drop the packets later.

Optimal fitness, with star evaluation of radius in the detection of BH attack, is given as follows.

$$R_S = \frac{Fitness}{\sum_{star=1}^{population} CF_{star}} \tag{2}$$

Where, the radius of optimal value is calculated based on Cost Function (CF). Fitness value is determined by the number of populations at end iteration, which is identified through random analysis with star model.

Population optimization in SMO is given as follows.

$$X_i(star+1) = X_i(star) + Rand\ (X_{bh}(star) - X_i(star)) \tag{3}$$

where, X_i represents the star vector based on maximum iteration whereas random star population with BH identity is determined accordingly. Every molecule is considered as an answer for the issue at position X_i with speed, X_{bh}. Every molecule has a memory of its best-visited position with that of its neighborhood, G_{best}. The flow chart for spider monkey optimization is given in Fig. 2. Based on the attributes and clusters, star BH matrix is generated which determines the objective function of optimization. Star BH is performed till the iteration is stopped and fitness form is evaluated. However, it is selected from current BH population. The initialization probability of optimization, to select the star attributes, changes from 0.5, 0.75 and 1.

The portable impromptu organizations acquire its fame for different applications such as brisk and simple arrangement. There is no need for this organization to have any fixed framework for arrangement. Portable nodes in a network communicate with one another through remote communication medium. This phenomenon makes the network profoundly defenseless against a number of attacks. In this background, the level of optimization is estimated by wellness of the nodes and is motivated by whole number of insights that exist in social orders with coordinated populaces. In its application to advancement issues, this strategy depends on a bunch of people. At first, it arbitrarily disseminate the so-called particles that move in pursuit space. Packet drop attack is one of the notable attacks. The developmental procedure utilizes a group of competitor arrangements to develop an ideal answer for this issue. Overall, the proposed work is designed to achieve a better result than the existing works. The proposed work showed promising results in terms of star determination with reevaluation of the population.

4 Results and Discussion

Traffic management using MANET approach needs much efforts to be taken in its preparation of multi path routing protocol. Traffic control is used to reduce the transmission of information towards the sender at middle level. For this purpose, a procedure is used. Based on high packet delivery ratio, the traffic likely gets reduced. MANET routing productivity gets expanded with the usage of bio-inspired metaheuristic algorithms. Here, the mobile node takes the time speed of 10 m/s and the network is ranged at 1200 m × 1200 m. The transmission packet size takes 512 bytes of packets. Network Simulator 2 is used to implement the whole routing process.

4.1 Performance Metrics

The parameters mentioned below are primarily evaluated for its efficiency in the validation of the proposed model in routing network model.

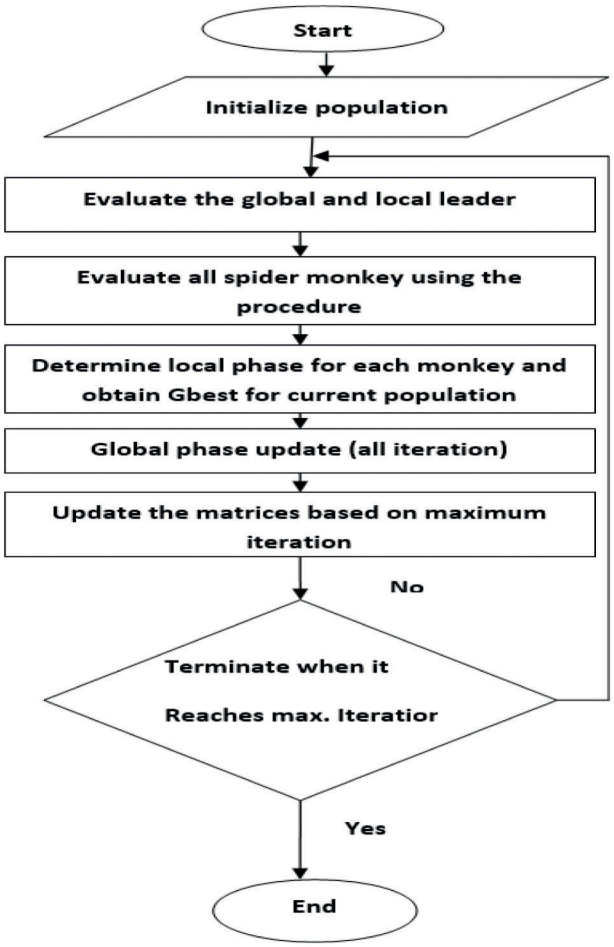

Figure 2: Flow chart for spider monkey optimization algorithm

Packet delivery ratio is obtained by,

$$Packet\ \ delivery\ \ ratio = \frac{1}{t}\sum_{n=1}^{t}\left(\frac{P_{receive}}{P_{sent}}\right)_n \tag{4}$$

Routing overhead is calculated as given herewith.

$$Overhead = \frac{1}{t}\sum_{n=1}^{t}\left(\frac{P_{control}}{P_{trans}}\right)_n \tag{5}$$

End-to end delay is obtained from,

$$Delay = \frac{1}{t}\sum_{n=1}^{t}\frac{Delay_n}{D_n} \tag{6}$$

4.1.1 Packet Delivery Rate

Packet Delivery Rate is calculated based on sender's and receivers' behavior, which improves the throughput by how much data is received without loss. The results for packet delivery ratio are portrayed in Fig. 3.

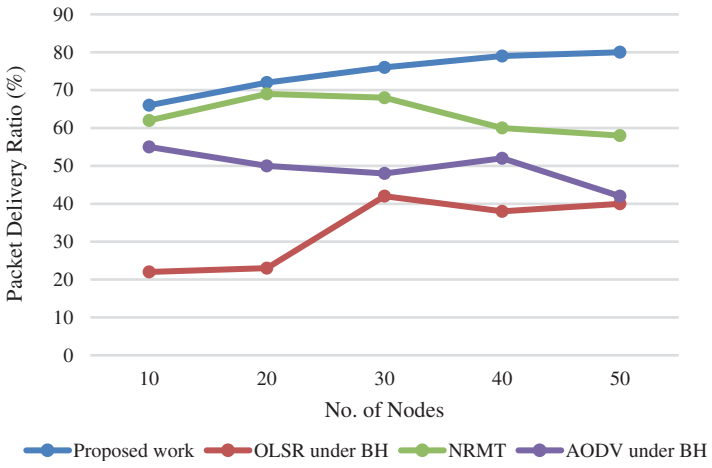

Figure 3: Packet delivery ratio results

Different variations of SMO are discussed in this section.

The section also provides a detailed outline of advantages and disadvantages of every variation in this research. The results for network throughput are given in Fig. 4.

4.1.2 Routing Overhead

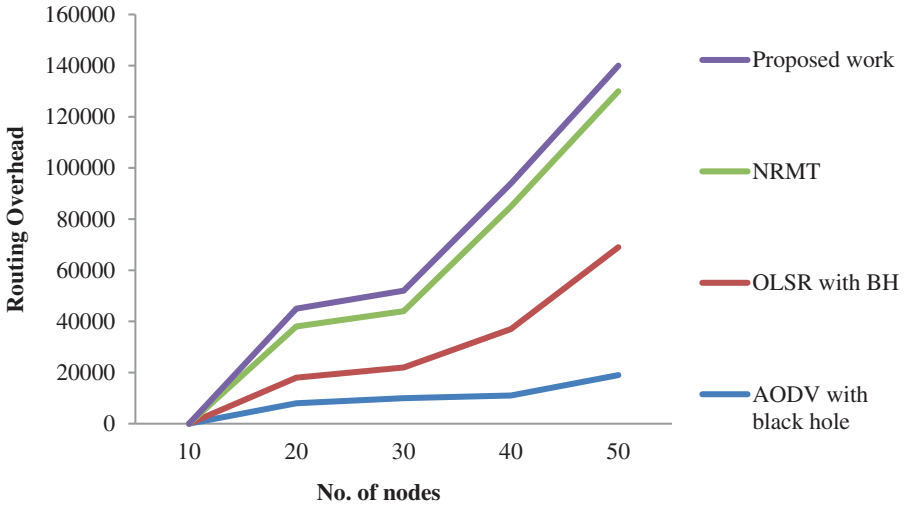

Figure 4: Routing overhead results

4.1.3 End-To-End Delay

In MANETs, the communication between devices occur simultaneously while energy utilization is a significant parameter to consider. The results for end-to end delay are shown in Fig. 5.

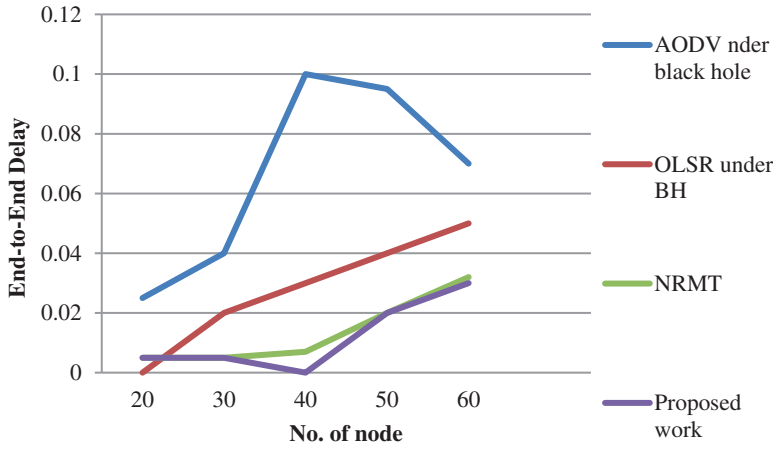

Figure 5: End to end delay performance results

The graphs plotted above shows the performance of MANET traffic management model. The model was validated for its impact on BH attack reduction in terms of packet delivery ratio, throughput and end-to-end delay. There is a significant increase observed in packet delivery ratio in the proposed work than other methods such as Neutral Remote Mapping Table (NRMT) [1], Optimized Link State Routing Protocol (OLSR) with BH [31], AODV with BH and [1]. Further, a slight reduction in delay was also obtained as shown in Fig. 5. In comparison with existing methods, the proposed method reduced the values extensively at end node. Here the comparative result shows that the proposed model achieved better outcomes than the existing models in terms of dynamic source performance. In this study, a point-by-point investigation was conducted for the normally-propelled meta-heuristic approach. The study also discussed about existing routing protocols and attack mechanisms, executives' strategies and related execution measurements. Further, various meta-heuristics approaches were also considered to improve the presentation issues experienced in MANET. The ultimate goal is to recognize the disadvantages of existing approaches and to overcome it in future examinations.

5 Conclusion and Future Scope

The proposed spider monkey approach optimizes the routing path in MANET under BH attack. It can be concluded that the study achieved efficient routing optimization in MANETs. Here, both source and destination of the routing protocol use AODV, whereas local and global phase systems improve packet delivery ratio. Both global phase and local phase of the SMO utilized routing path selection and identified BH attack. Here, spider monkey optimization with star analysis helped in obtaining a better result i.e., detection of BH attack with reevaluation procedure. This experiment was designed to achieve better performance in terms of packet delivery ratio, throughput and end-to-end delay. By comparing the proposed work against existing works, the proposed optimization design model has proved its supremacy by yielding an excellent performance. In future, the research can be extended to handle different types of attacks that are commonly encountered by MANETs and its performance can be improved in terms of security, stability and reliability.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. A. Arunmozhi and Y. Venkataramani, "BH attack detection and performance improvement in mobile Ad-hoc Network," *Information Security Journal a Global Perspective*, vol. 21, no. 3, pp. 150–158, 2012.

[2] R. Hemalatha and S. A. Aruunmmozhi, "A secured defense scheme against collaborative blackhole attacks in MANET," *Journal of Scientific Research*, vol. 24, no. 2, pp. 340–346, 2016.

[3] M. Avijit, N. Thomas and R. Muzaffar, "Defence against BH and selective forwarding attacks for medical WSN in the IoT," *Sensors*, vol. 16, no. 1, pp. 118–126, 2016.

[4] M. R. Babu, S. M. Dian, C. Siva and K. Mathiyalagan, "Proactive alleviation procedure to handle BH attack and its version," *Scientific World Journal*, vol. 12, no. 1, pp. 125–134, 2015.

[5] 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. 6, no. 8, pp. 116–135, 2018.

[6] P. Vij, V. K. Banga and T. P. Singh, "Broadcast ID based detection and correction of BH in MANET," *International Journal of Computer Applications*, vol. 56, no. 17, pp. 6–11, 2012.

[7] P. Rani, S. Kavita and V. Sahil, "Mitigation of BH and gray hole attack using swarm inspired algorithm with artificial neural network," *IEEE Access*, vol. 8, no. 4, pp. 121755–121764, 2020.

[8] S. L. Dhende and D. M. Bhalerao, "A mechanism for detection of BH attack in mobile ad hoc networks," *International Journal of Engineering Research & Technology*, vol. 1, no. 6, pp. 326–335, 2012.

[9] N. Simranjeet and A. Sandeep, "Analysis of BH gray hole attack on RP-AODV in MANET," *International Journal of Engineering Research & Technology*, vol. 2, no. 8, pp. 121–136, 2013.

[10] R. Cai, X. Li and J. C. P. Han, "An evolutionary self-cooperative trust scheme against routing disruptions in MANETs," *IEEE Transactions on Mobile Computing*, vol. 18, no. 1, pp. 42–55, 2018.

[11] M. A. Shurman, Y. S. Moo and P. Seunjin, "BH attack in mobile Ad Hoc Networks," in *Proc. of the Annual Southeast Regional Conf.*, Singapore, vol. 12, pp. 96–97, 2004.

[12] E. O. Ochola, L. F. Mejaele, M. M. Eloff and J. A. van der Poll, "MANET reactive routing protocols node mobility variation effect in analysing the impact of BH attack," *SAIEE Africa Research Journal*, vol. 108, no. 2, pp. 80–92, 2017.

[13] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan and A. Aldegheishem, "Intelligent detection of BH attacks for secure communication in autonomous and connected vehicles," *IEEE Access*, vol. 8, pp. 199618–199628, 2020.

[14] L. Teng, J. Ma, Q. Pei, H. Song, Y. Shen *et al.* "DAPV: Diagnosing anomalies in MANETS routing with provenance and verification," *IEEE Access*, vol. 7, pp. 35302–35316, 2019.

[15] A. Mathur and T. Newe, "Medical wsn: Power, routing and selective forwarding defense," in *Proc. of the 13th Int. Conf. on Telecommunications (ConTEL)*, Graz, Austria, vol. 13, pp. 1–6, 2015.

[16] M. A. Shurman, S. Yoo and S. Park, "BH attack in mobile ad hoc networks," in *Proc. of the 42nd Annual Southeast Regional Conf. on ACM-SE*, Huntsville, AL, USA, vol. 4, pp. 2–3, 2004.

[17] K. V. Kumar and K. Somasundaram, "Detection of BH attacks in MANETS by using proximity set method," *International Journal of Computer Science and Information Security*, vol. 14, no. 3, pp. 136–145, 2016.

[18] N. Khemariya and A. Khuntetha, "An efficient algorithm for detection of blackhole attack in AODV based manets," *International Journal of Computing Application*, vol. 66, no. 5, pp. 18–24, 2013.

[19] M. Tiwari, K. V. Arya, R. Choudhari and K. S. Choudhary, "Designing intrusion detection to detect BH and selective forwarding attack in WSN based on local information," in *Proc. of the Fourth Int. Conf. on Computer Sciences and Convergence Information Technology*, Seoul, Korea, vol. 24, no. pp. 26pp. 824–828, 2009.

[20] G. Gulhane, N. V. Mahajan, "Securing multipath routing protocol using authentication approach for wireless sensor network," in *Proc. of the Fourth Int. Conf. on Communication Systems and Network Technologies*, Bhopal, India, vol. 7, pp. 729–733, 2014.

[21] J. Jun and M. L. Sichitiu, "Wireless mesh networks routing protocol," *Computer Communication*, vol. 31, no. 12, pp. 1413–1435, 2008.

[22] T. P. Singh, R. K. Singh, J. Vats and M. Kaur, "Optimized BH detection and prevention algorithm (OBHDPA) for mobile ad hoc networks," in *Int. Conf. on Computer Science and Information Technology (ICCSIT'2011)*, Delhi, vol. 4, pp. 57–60, 2011.

[23] V. Gupta, S. Krishnamurthy and M. Faloutsos, "Denial of service attacks at the MAC layer in wireless ad hoc networks," in *Proc. IEEE Military Communications Conf.*, America, vol. 2, pp. 1118–1123, 2002.

[24] S. Kumari, M. Singhal and N. Yadav, "Blackhole attack implementation and its performance evaluation using AODV routing in MANET," in *Inventive Communication and Computational Technologies*, Springer, Singapore, vol. 12, pp. 431–438, 2020.

[25] T. Poongodi and M. Karthikeyan, "Localized secure routing architecture against cooperative BH attack in mobile ad hoc networks, " *Wireless Personal Communication*, vol. 90, no. 2, pp. 1039–1050, 2016.

[26] V. Srinath and S. A. Arunmozhi, "Minimizing energy consumption in wireless sensor network using energy remaining greedy algorithm," *Grenze International Journal of Engineering and Technology*, vol. 4, no. 6, pp. 33–39, 2019.

[27] J. C. Bansal, H. Sharma, S. S. Jadon and M. Clerc, "Spider monkey optimization algorithm for numerical optimization," *Memetic Computing*, vol. 6, vol. 1, pp. 31–47, 2014.

[28] A. Azza, A. A. A. Jodah and F. J. Harackiewicz, "Spider monkey optimization: A novel technique for antenna optimization," *IEEE Antennas Wireless. Propagation Letter*, vol. 15, pp. 1016–1019, 2016.

[29] J. Dhar and S. Arora, "Designing fuzzy rule base using spider monkey optimization algorithm in cooperative framework," *Future Computing and Informatics Journal*, vol. 2, no. 1, pp. 31–38, 2017.

[30] P. N. Raj and P. B. Swadas, "DPRAODV: A dynamic learning system against BH attack in AODV based MANET," *International Journal of Computer Science Issues*, vol. 4, no. 2, pp. 54–59, 2012.

[31] N. Abdellah, L. Ay Driss and S. Mohammed, "Evaluation of MANET routing protocols under BH attack using AODV and OLSR in NS3," in *Int. Conf. on Wireless Networks and Mobile Communications*, Marrakesh, Morocco, vol. 16, pp. 1–6, 2018.