Prevention of Attacks in Mobile Ad Hoc Network using African Buffalo Monitoring Zone Protocol

R.Srilakshmi[1]
Research Scholar
Koneru Lakshmaiah Education Foundation,
Vaddeswaram, 522502, Andhra pradesh, India

Dr. M.Jaya Bhaskar[2]
Professor
Koneru Lakshmaiah Education Foundation,
Vaddeswaram, 522502, Andhra Pradesh, India

***Abstract*—Mobile ad hoc networks (MANET) can be utilized for communicating wirelessly. However, MANET is affected by many attacks and malicious activities. In MANET, the prevention approach is necessary to secure communication. MANET is easily affected by numerous attacks such as wormhole (WH) attack, Grey-hole (GH) attack, and black-hole (BH) attack in which the sender hubs can't able to transmits the message to the target node due to the malicious behavior. To prevent the attacks in MANET, this research introduces a novel routing protocol as African Buffalo Monitoring Zone Protocol (ABMZP). This approach is utilized for preventing wormhole attack and other malicious activities in MANET. This mechanism monitors the communication channel continuously and identifies the attack detection. Sequentially, the ABMZP approach prevents the harmful nodes and finds the alternate path for communication. The simulation of this research is done with the use of Network Simulator 2 (NS-2) and finally, the efficiency of the projected ABMZP work outcomes are compared with the latest existing techniques and provides superior results.**

***Keywords*—Mobile ad hoc network; malicious nodes; routing protocol; wormhole attack; security**

I. Introduction

In general, MANET referred to the decentralized classification of a wireless network [1, 44]. Also, MANET has a routable associating situation on upper of a connection layer [2, 35]. Also, MANET has a collection of nodes, which are communicating wirelessly [3, 37]. Moreover, the nodes in the MANET are freely moving as the system topology transforms frequently [4,]. Generally, every hub acts as a router when it sends traffic to another specific node in the network. The MANET nature is very dynamic that is utilized for communicating between two nodes during business conferences, natural disasters, etc [5, 41]. In MANET, the routing procedure is utilized for communicating between the pair of nodes. These nodes are having the ability to transfer the message from the source hub to the target node [6, 40]. Generally, MANET has several groups of nodes, which is no permanent infrastructure to connect the nodes. So, these are very flexible & smoothly reconfigurable and these networks required a limited number of properties like memory of the network, bandwidth, and battery & computation power [7].The MANET nodes are in a particular network range and communicate directly to each other [8]. In general, several network actions are achieved using mobile nodes in MANET such as packet forwarding, packet detection, packet communication, and network organization [9].

Moreover, MANET is having the features of communicating in free space, broad sharing of packets, and nodes. However, MANET is vulnerable to several types of malicious activities so prevention is necessary to protect the channel [10, 39]. The packets should be controlled because when the sender node sends the message the neighboring nodes act maliciously to drop the data are passed through it [11, 38]. Several attacks are affecting the MANET network such as BH, denial of service (DoS), WH, distributed DoS(DDoS) and GH attacks. Moreover, the difficulties of misconduct routing are one of the disseminated protections terrorizations in the network like BH attacks. Therefore, several investigators are proposing many protected routing ideas to overcome these issues, but the safety problems of network are still an issue.

So, several prevention mechanisms are introduced to prevent malicious attacks but, it has attained numerous challenges. Several routing protocols like artificial intelligence [12], EMAODV [13, 45], and Ad-hoc On-demand Distance Vector (AODV) mechanism are introduced to secure communication. However, the malicious activities create trustful nodes so the sender transmits the message to it [14, 36]. But, it can't able to reach the destination because the hacker transmits the message into the third person [15, 46]. So, the proposed approach introduces a novel protocol for avoiding the occurrences in the MANET and provides secure communication. The proposed mechanism improves network performance and provides high security.

This research is categorized as various sections that are Section 2 demonstrates the recent literatures about the security, the problem definition is given in Section 3; the proposed methodology is detailed in Section 4, the attained results are explained in Section 5, and the conclusion part is mentioned in Section 6.

II. Related Work

Various authors have given different approaches to eliminate attacks in MANET and here are some:

A BH attack is one of the categories of MANET occurrence and here the malevolent hubs become part of the network. As a result, it absorbs everything that comes in, because it acts as a hole and the packets fall into it. Therefore, the desired target node does not attain the data packets; therefore, it disturbs the entire communication. Here, Gupta *et al* [16] established the methodology using reliability factors

for detecting and preventing the BH attacks in MANET. Also, the AODV protocol is modified to secure the channel that can act against the BH attack. Thus, the fake RREQ conception is utilized for detecting the malicious nodes in this method. Furthermore, this approach decreases the amount of dropped packets.

In MANET, several intrusions are detected to affect the nodes in the network. According to this reason, Su and Ming-Yang [17] introduced Anti-Blackhole Mechanism (ABM) for reducing the BH attack in the MANET. Thus, it detects and separates the malicious nodes in the MANET. Here, the utilized IDS nodes are arranged in the form of sniff for achieving the function of ABM that is utilized for evaluating the uncommon value of a node. Here, it considered the threshold value and when the particular node threshold is increased then IDS is blocking the message.

Moreover, WH attack is the rigorous activities in MANET, which is defeated using many prevention mechanisms. These prevention approaches are based on packet traversal time, round trip time, & hop-count but, these solutions are not successful. To avoid these issues, Vo *et al* [18] introduced a multi-level authentication method and procedure (MLAMAN). This method permitted the nodes to validate the packets based on 3 steps that are packet level, membership, and neighborhood level. Hence, the MLAMAN approach detects and prevents the wormhole attack in the network.

In MANET, the messages are not reaching the target node because of the malevolent activities of the node such as DoS and black-hole attacks. The packets are dropped because of the BH attacks that are eliminated by a new approach. Here, Gurung*et al* [19] introduced an approach that depends on a dynamic threshold algorithm that is named as MBDP-AODV protocol. This protocol moderates the collision of attacks based on various network densities and this mechanism improved network performance like throughput, PDR, overhead, and decreases the routing load.

MANET can be affected by many malicious attacks like DDoS attacks. A kind of DDoS attack is a Jellyfish attack that is quite hard and affects the complete performance of the network. To overcome this jellyfish attack, Doss *et al* [20] proposed an attack prevention APD-JFAD approach. This approach selects the trusted nodes for creating a path to overcome the attack. Moreover, it acts against the jellyfish attack accurately and provides better performance. Thus, the existing techniques presentation is summarized in the Table I.

The key contributions of the research are summarized below:

- In general, MANET is vulnerable to malicious activities. So, this approach develops the novel protocol for predicting malicious activities in the network.
- Here, African Buffalo Monitoring Zone Protocol (ABMZP) is developed to prevent the network from the WH, BH, and GH attacks.
- It secures the MANET communication channel against the malicious attacks.
- The implementation of the proposed approach is done using the NS-2 tool.
- Finally, the attained implementation results prove the efficacy of the projected approach.

TABLE I. RECENT LITERATURE BASED ON PREVENTING ATTACKS IN MANET

Author	Method	Merits	Demerits
Gupta *et al* [16]	Reliability Factor Based AODV Protocol (RF based AODV)	Packet drop ratio is reduced in this approach.	RF based AODV attained high simulation time and low accuracy.
Su and Ming-Yang [17]	Anti-Black hole Mechanism (ABM)	In this ABM method Packet loss rate is decreased.	It has high overhead.
Vo *et al* [18]	multi-level authentication model and protocol (MLAMAN)	It can detect the malicious activities as different tunnel lengths and node speeds.	This MLAMAN strategy attained high overhead during data transmission.
Gurung*et al* [19]	MBDP-AODV	MBDP-AODV manner attained high PDR, and throughput.	It attained high routing overhead during transmission.
Doss *et al* [20]	APD-JFAD	It attained high PDR, throughput, and low delay.	APD-JFAD method prevention accuracy is low.

III. PROBLEM STATEMENT

MANET has multiple nodes connected to multiple wireless connections. MANET is affected by various limitations such as limited bandwidth, connection failure, limited communication power, and power outage. Moreover, the wireless link and nodes are highly susceptible to attacks. The communication channel is affected by several malicious activities such as WH attacks [21], GH attacks [22], DDoS attacks [23], and BH attacks [24]. The most common attack in MANET is the WH attack, which can be dropped the packets and break the link. So, the information was not able to attain the destination of the network [25, 31]. Moreover, these attacks break the wireless links and pass the data into unwanted nodes. The destination node can't receive the packets because of the malicious activities [26, 32].

The source hubs transmit the data packs to the target through neighboring nodes. The attacker node receives the data packets from the sender. After that, the attacker node drops the data packets, which are detailed in fig.1. So, MANET security is necessary and that should be complete the security parameters such as network overload, processing time, and energy consumption. The proposed approach provides better network performance and high security between nodes.

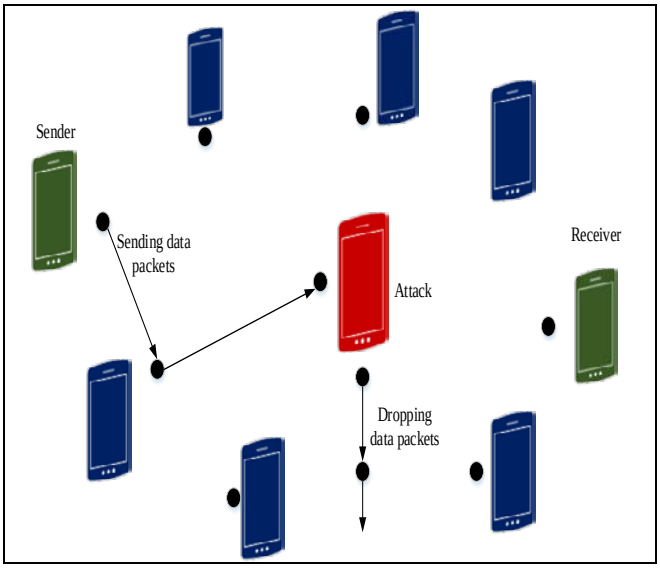

Fig. 1. System Framework for attack Intrusion in MANET.

IV. Proposed (ABMZP) Methodology

The proposed approach provides secure communication between the nodes in MANET. Initially, a communication channel is formed in MANET that can be easily affected by many attacks like WH, BH, and GH attacks. So, this methodology introduces an innovative African buffalo Monitoring zone protocol (ABMZP) to prevent communication channels from malicious activities. Finally, this approach acts as a prevention mechanism against the harmful nodes in the network. The proposed manner is aimed to secure the network before any type of malicious activity enters the node and make the malicious node not able to break the security of the network, which are shown in Fig. 2.

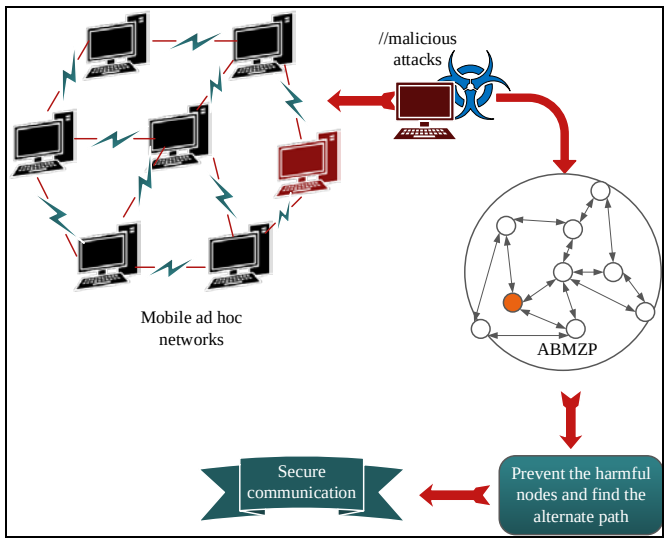

Fig. 2. Proposed Methodology.

A. African Buffalo Monitoring Zone Protocol (ABMZP)

African buffalo Monitoring Zone protocol (ABMZP) is the hybrid form of African buffalo optimization (ABO) [27,34] and Zone protocol (ZP) [28,43]. In this approach, the malicious nodes are predicted using the fitness function of ABO and it identifies another secure path for communication. Initially, the ABMZ protocol creates the routing zone for data transmission. This routing zone has several numbers of nodes (N) that all are in the communication network. Initially, the source hub conveys the data packets to the receiver through neighboring nodes that makes the path for packet transmission. MANET is vulnerable to malicious activities so the proposed approach identifies the attacked nodes and provides better transmission through alternate path [33,42]. The proposed ABMZP model identifies the attacks like WH attack, BH attack and GH attack. This approach initializes the network zone (N) that has several nodes. Primarily, the $R\,\mathrm{Re}\,q$ message is transmitted for all neighboring nodes by the sender node and that routers send the $RRply$ message to the sender node. Here, the proposed ABMZP monitors the network to identify the best path for better communication. Also, the proposed ABMZP categorizes the IP address for every nodes in the network. The finest path identification for better communication using eq. (1):

$$k'_w = P_k + N\left(\ln_1(bN - Q_k) + \left(\ln_2(bM.k. - Q_k)\right)\right) \quad (1)$$

Where, N specifies the whole communication network, k denotes the communication path, P_k represents all nodes in the network, Q_k is the malicious nodes, $\ln_1$ and $\ln_2$ is the learning parameters, bN mentioned the IP address of all nodes and bM denotes the IP address of malicious nodes.

Algorithm 1: ABMZP for attack prevention

begin
{
Initialize the communication network (N)
Develop the source (S) and destination (D) nodes;
Randomly initialize network path K_w *on the search space*

Let the attack nodes as (Q_k *)* // Q_k ***involves WH, BH, and GH attacks***

$P_k \rightarrow IP\_(N) = (bN)$ // ***set IP address for all nodes in the network***

If $S \xrightarrow{R\,\mathrm{Re}\,q} P_k$ ***then*** P_k & $Q_k \xrightarrow{RRply} S$

Analyze the network path using AB function by eqn.(1)

If $P_k(bN) \neq Q_k(bM)$ ***//bN and bM denotes the IP address of trusted node & Malicious node***
then
Calculate the energy levels of all nodes using eqn.(2)
If $E_T(N) > 1J$ ***// malicious activities are present***
then
calculate the energy threshold for all nodes
$1J < E_T(w) > 1.5J$ // $E_T(w)$ *denotes the energy threshold of wormhole attack*
$1.5J < E_T(b) > 2J$ // $E_T(b)$ *denotes the energy threshold of black hole attack*
$2J < E_T(g) > 2.5J$ // $E_T(g)$ *denotes the energy threshold of grey-hole attack*
end
*alert the source node;// **S node not transmits the message in this path***
*Identify the optimal path // **secure communication***
end-if
}
stop

Subsequently, if ABMZP detect the harmful nodes then it detects the attacks like WH, BH, and GH based on the energy levels of malicious nodes. Thus, the energy threshold of the nodes are identified using eq. (2).

$$E_T(N) = \frac{E_{R\,\mathrm{Re}\,q} + E_{RRply}}{Total\_energy} \tag{2}$$

Where, $E_{R\,\mathrm{Re}\,q}$ is represents the energy for $R\,\mathrm{Re}\,q$ message, E_{RRply} is denotes the energy for $RRply$ message and λ is the energy of attacks. The process of ABMZP is explained using algorithm 1.

In this approach, the ABMZP monitors the network continuously to detect the harmful nodes. If it is identifying the harmful nodes then it alerts the source node and provides secure communication through finest path that process is explained in Fig. 3.

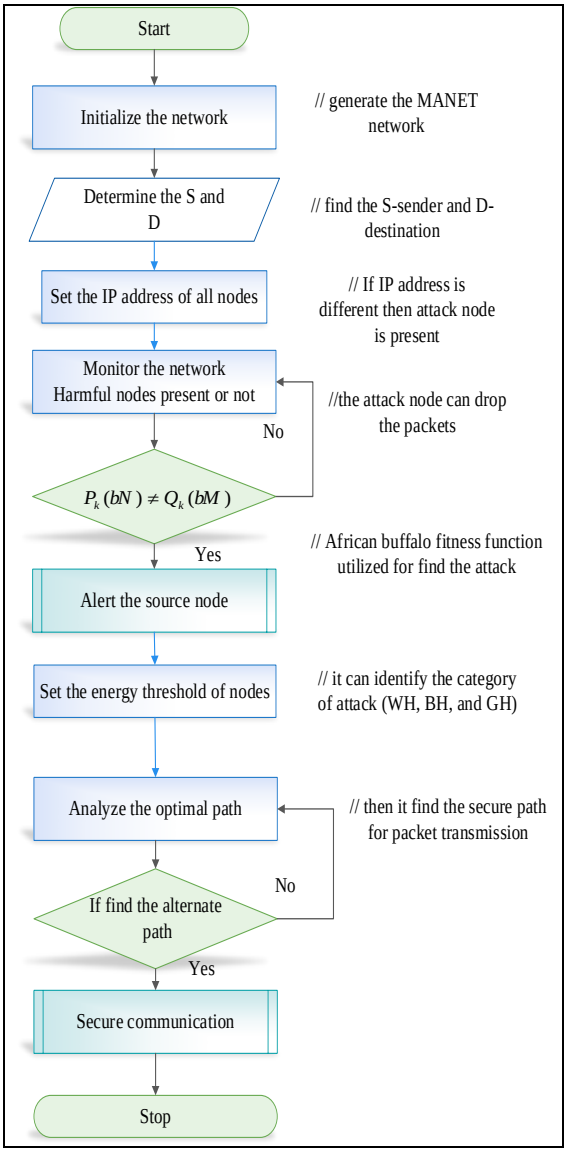

Fig. 3. Flow Chart for ABMZP.

V. Results and Discussion

The developed ABMZP model is simulated byNS-2 running on NAM console v1 15 in the Ubuntu 12.04.5 LTS platform. Generally, MANET is vulnerable to attacks so this proposed approach introduced novel prevention mechanism ABMZP. The projected ABMZP model is utilized to create the MANET nodes and transmit the messages through the routers in a secure way. This research focuses on the MANET nodes and identifies the malicious nodes. Also, ABMZP creates a better channel for communication, which is detailed in Fig. 4. Finally, the performance metrics are calculated using NS-2 and provide better network performance compared with existing approaches.

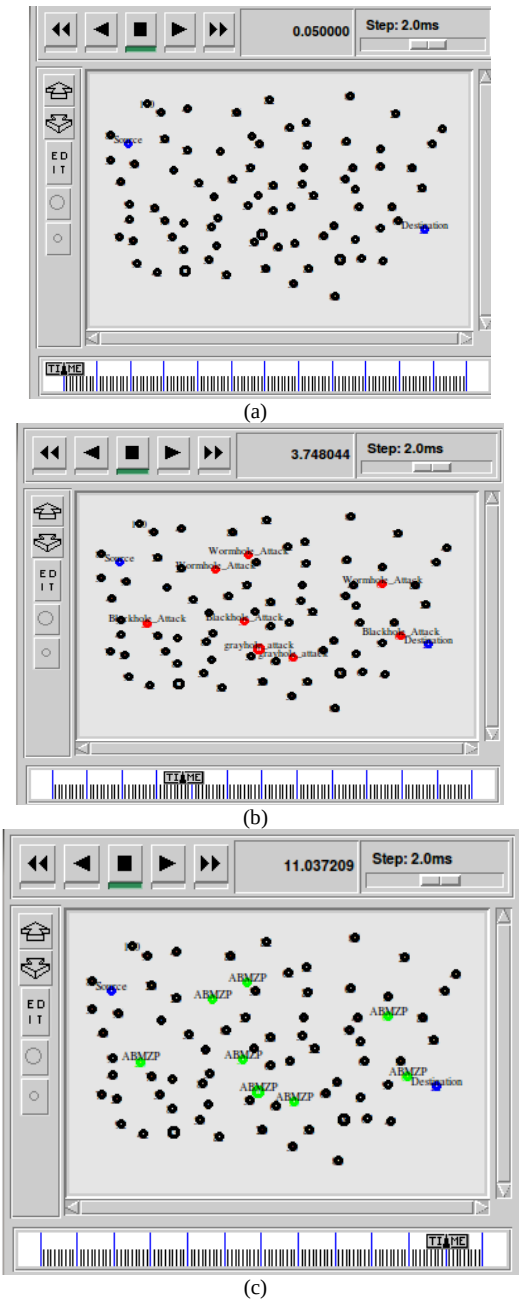

Fig. 4. (a) Node Formation in Network, (b) Detection of Attacks, (c) Communication through Best Path.

B. Case Study

Let the sender node S, destination node D, and A, B, C, D, E, F,G,H,I,J, and Kare taken as other neighboring nodes. Here, the data packets are transferred from S to D through neighboring nodes. Initially, the sender node wants to convey the information to the target. So, the sender node searches the IP address of every nearby node. Moreover, the sender node finds the IP address of each adjoining node in the zone. Subsequently, every node has a dissimilar IP address and that is stored in the sender node. Primarily, the sender node transmits the Route Request (RReq) to the routers in the zone before transmitting the packets. Consequently, the neighboring nodes are send Route Reply (RRply) message to the sender, if any node is attacked by malicious that is also sending the RRply message. The ABMZP is always monitoring the network and RRply messages. Also, it analyzes the IP address of the nodes which are forward the message to the sender. If it is same means there no malicious activity and it is different means the attack present in the network. The graphical illustration of these details is represented in Fig. 5.

Furthermore, malicious node forwards the RRply message through the sender, which is detected using ABMZP. Let us consider the total energy of the nodes as 0.4J and the energy for RReq message as 0.2J and the energy for RRply message as 0.18J, which are substitute in eqn.2. So, the attained energy threshold for all nodes as E(N)=0.875J. Also, let the energy threshold level for attacks as WH attack Ew= 1.2J, BH attack Eb=1.6J, and GH attack Eg=2.1J. Here, the proposed ABMZP utilizes lower energy to transmit the packets. If the energy threshold is high than the particular range then it is affected with malevolent activities. So, the ABMZP protocol alerts the sender node and transmits the message in another path to provide secure transmission, which is shown in Fig. 6.

Consequently, the proposed ABMZP develops best path to secure transmission. Finally, the data packets are sending through the secure path and reach the destination.

C. Performance Metrics

The introduced ABMZP mechanism compute the parameters like throughput, overhead, packet delivery ratio (PDR), packet delay, and end_to_end delay. This manner is compared with other strategies such as MBDP-AODV [19], OLSR [29], and CLPDM-SI [30]. The proposed method achieved better results in overhead, packet delay, PDR, and throughput.

1) Attack prevention rate: This is represented as a metrics for calculating the effectiveness of attack prevention rate in the network. It is the fraction of total quantity of sends messages and sum of data packets attained to the destination and the mathematical expression is represented in Eq. (3):

$$A = \frac{(Tn' + Tp')}{(Tn' + Tp' + Fn' + Fp')} \quad (3)$$

Where, Tn' is True negative, Tp' is denoted true positive, Fn' is represented the false negative value and Fp' is symbolized the false positive.

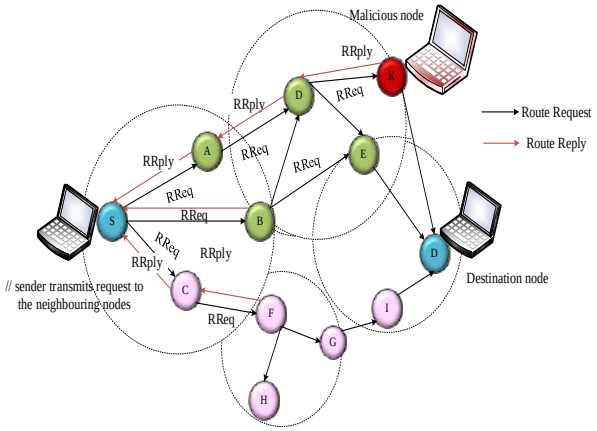

Fig. 5. Network Zone for Data Transmission.

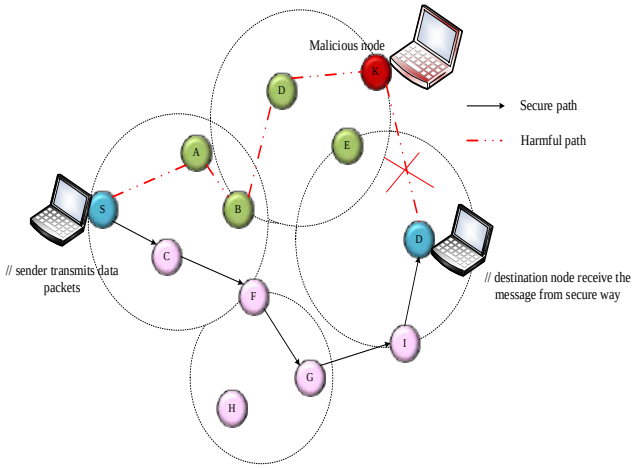

Fig. 6. Secure Packet Transmission.

TABLE II. CALCULATION OF ATTACK PREVENTION RATE

Method	Attack Prevention rate (%)
MBDP-AODV[19]	89
OLSR [29]	98.5
CLPDM-SI [30]	96
Proposed [ABMZP]	99. 96

The attack prevention rate is proves the efficiency of the proposed ABMZP method. This is campared with some techniques like MBDP-AODV, OLSR, and CLPDM-SI. Here, MBDP-AODV attains lower prevention rate as 89%, OLSR, and CLPDM-SI attains 98.5% & 96% prevention rates. But, the proposed ABMZP attains 99.96 % high rate for attack preventing rate, these values are given in Table II and it is represented in Fig. 7.

2) PDR calculation: It is the ratio between the entire amount of attained data packets and quantity of sent packets, which is calculated using eq. (4). The PDR ratio of the proposed ABMZP model is detailed in Fig. 8.

$$PDR = \frac{No.of\_received\_packets}{No.of\_sent\_packets} X100 \quad (4)$$

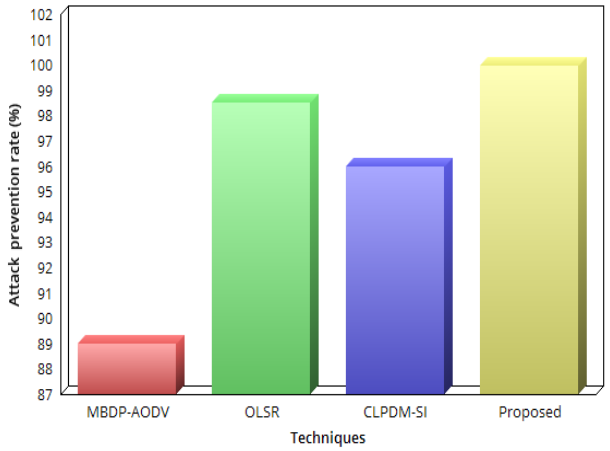

Fig. 7. Evaluation of Attack Prevention Rate.

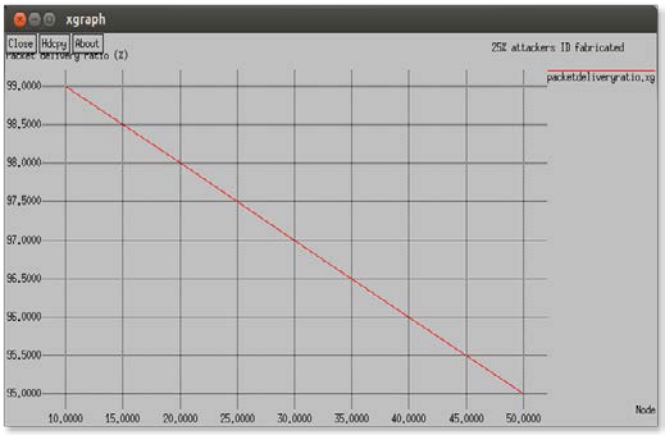

Fig. 8. PDR Rate.

Moreover, the PDR ratio is calculated and evaluated using prevailing approaches. Here, the PDR ratio is computed based on the number of transmitted nodes. While considering 50 numbers of nodes, MBDP- AODV achieved 92% PDR, OLSR attained 95% PDR and CLPDM-SI attained 99% PDR. Moreover, the proposed method ABMZP achieved 99.32% high PDR rate, which is given in Table III and represented in Fig. 9.

3) End-To-End delay calculation: It is a calculation of the regular time when the data take a time period to reach the target node from the sender and the delay time is calculated using eq. (5).

$$End\_to\_end-delay = \frac{received\_packets\_time}{sent\_packets\_time}$$

Generally, high packet delay increased the number of retransmitted RReq messages and data packets. Also, it can easily reduce the network resources and wastes the energy of nodes. In this approach, the delay is very low because of high attack prevention, which is mentioned in Fig. 10.

This ABMZP outcome is compared with MBDP-AODV, OLSR, and CLPDM-SI. Here, the MBDP-AODV method has a high delay for transmitting the packets. Therefore, the novel ABMZP method provides a low delay for receiving the packets in the destination that is given in Table IV and represented in Fig. 11.

TABLE III. EVALUATION OF PDR

Nodes	Packet Delivery ratio (%)			
	MBDP AODV[19]	**OLSR [29]**	**CLPDM-SI [30]**	**Proposed [ABMZP]**
10	94	48	85	99.98
20	93	78	98	99.86
30	92	82	99	99.65
40	90	88	98	99.55
50	92	95	99	99.32

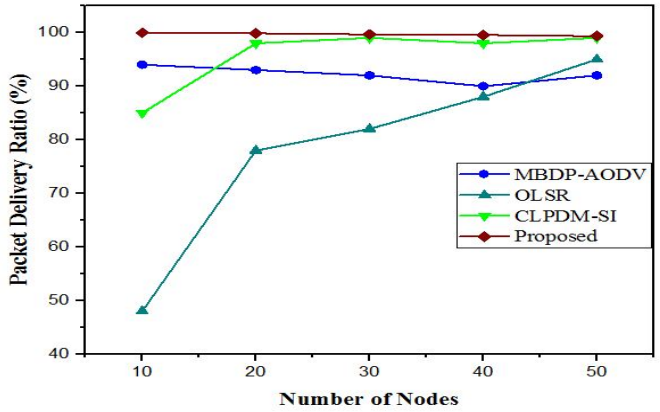

Fig. 9. Comparison of PDR Ratio.

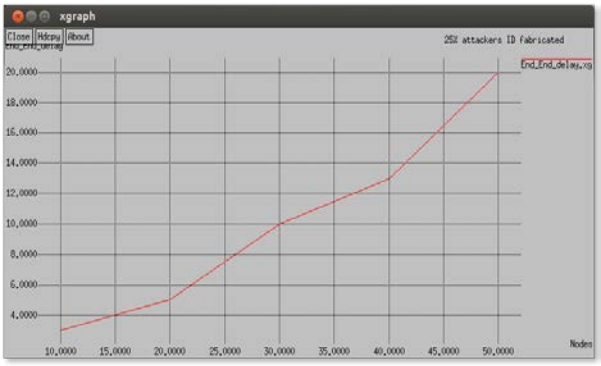

Fig. 10. End-End- Delay Calculation.

TABLE IV. EVALUATION OF END-TO-END DELAY

Nodes	End to end delay (s)			
	MBDP AODV[19]	**OLSR [29]**	**CLPDM-SI [30]**	**Proposed [ABMZP]**
10	40	18	8	3
20	80	28	10	5
30	110	38	14	10
40	160	58	28	13
50	180	64	30	20

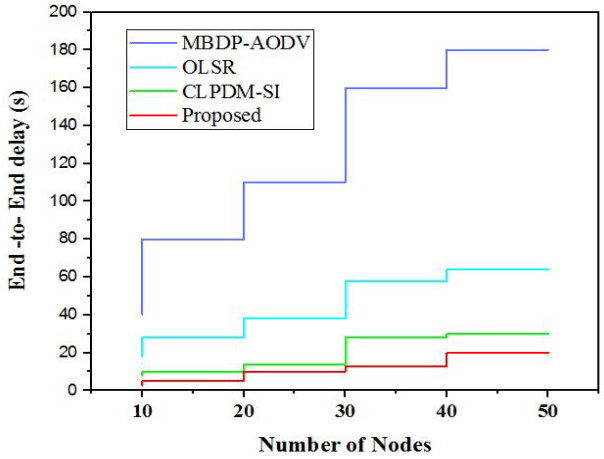

Fig. 11. Comparison of End-To-End Delay.

The security mechanism is taken at a particular time for detecting and eliminating the harmful nodes. Thus, the MANET security mechanisms should have very low processing time for packet transmission.

4) Packet drop ratio: This calculation measured using the fraction of total packet loss during transmission to the entire amount of received data packets. The sender hub transmits the packets to the neighboring nodes. If any attack present in the network then it is dropped or losses the packets, which is calculated and shown in Fig. 12.

During data transmission, some packets are lost due to the malicious activities and the packet drop ratio of the projected scheme and other techniques are given in Table V and it is represented in Fig. 13.

Here, when considered 50 numbers of packets transmitted then MBDP-AODV attained 23%, OLSR achieves 21% and CLPDM attained 22% Packet drop ratio. Moreover, the proposed ABMZP achieved a low packet drop as 18% validated with other procedures.

5) Throughput calculation: It denotes the rate of transmitting data packets through the network that is distributed through convinced physical or logical links. This value is denoted in bit/s or bps which is represented in Fig. 14.

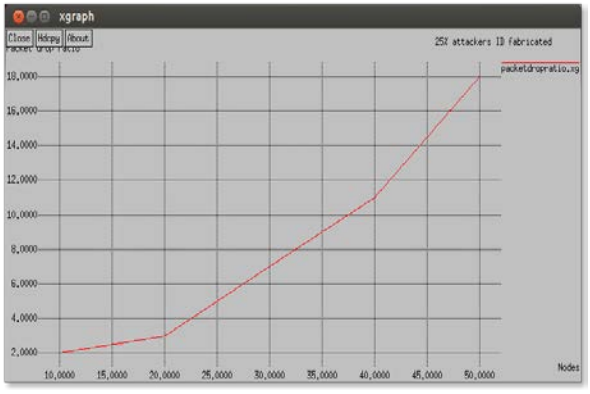

Fig. 12. Calculation of Packet Drop Ratio.

TABLE V. EVALUATION OF PACKET DROP RATIO

	Packet Drop ratio (%)			
No. of Nodes	**MBDP AODV[19]**	**OLSR [29]**	**CLPDM-SI [30]**	**Proposed [ABMZP]**
10	3.5	4	3	2
20	6	4.5	7	3
30	9.5	8	13	7
40	16	13.5	18	11
50	23	21	22	18

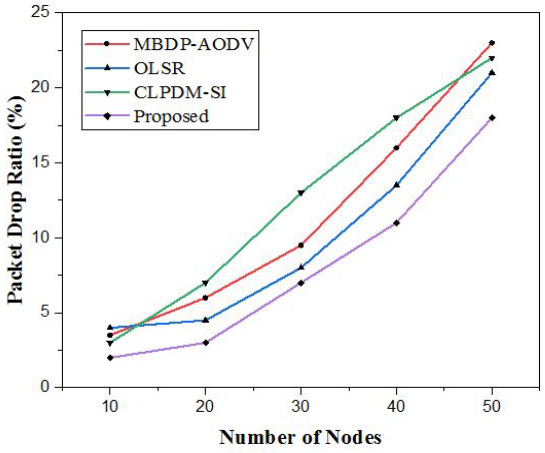

Fig. 13. Comparison of Packet Drop Ratio.

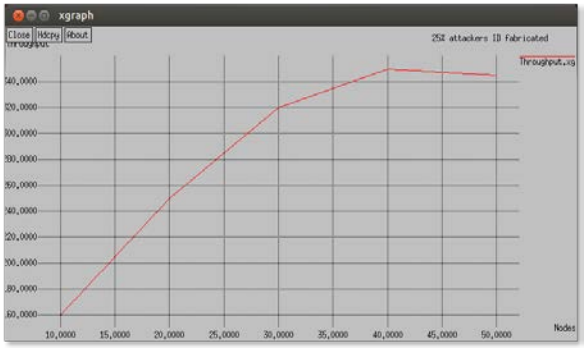

Fig. 14. Calculation of throughput.

The proposed manner achieves high throughput value validated with other prevailing approaches that are detailed in Table VI.

TABLE VI. EVALUATION OF THROUGHPUT

Throughput (kbps)				
Nodes	**MBDP AODV[19]**	**OLSR [29]**	**CLPDM-SI [30]**	**Proposed [ABMZP]**
10	20	36	145	160
20	18	48	198	250
30	17	54	201	320
40	15.5	88	198	350
50	18.63	95	201	345

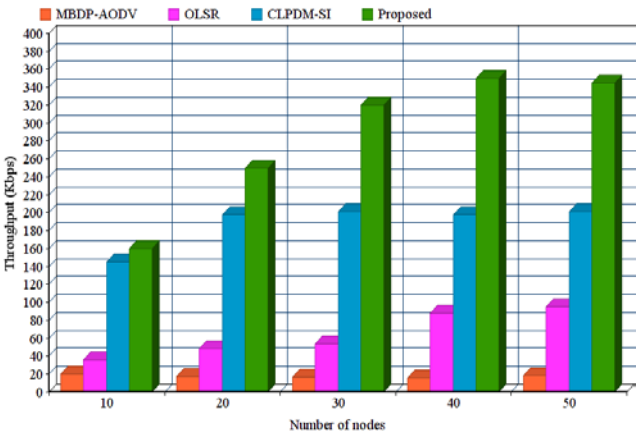

Fig. 15. Comparison of throughput.

Here, some recent methods like MBDP-AODV attained 18.63kbps, OLSR attained 95kbps, and the CLPDM-SI approach accomplished 201kbps for transmitting 50 numbers of nodes. But, the proposed ABMZP achieved 345 kbps high throughput value compared with other techniques, which is represented in the Fig. 15.

D. Discussion

The proposed ABMZP model provides secure communication in the MANET that is transferring the message from the sender hub to the target hub without any interruption. Therefore, the introduced novel ABMZP method provides better outcomes in terms of attack prevention rate, PDR, packet drop ratio, throughput, and delay validated with existing approaches like MBDP-AODV, OLSR, and CLPDM-SI.

VI. Conclusion

Generally, MANET is affected by various attacks such as wormhole attack, BH attack, and GH attack. To protect the information during data transmission the attack prevention is necessary. Hence, this paper introduced the novel prevention method as African Buffalo Monitoring Zone Protocol (ABMZP) for securing the communication. Thus, the ABMZP approach prevents the data from wormhole attacks and other malicious activities in the communication network. Consequently, if ABMZP detects the malicious activities then it alerts the source node. Also, it neglects the attack and provides secure transmission through an optimal path. Hence, it achieves a 99.96% high attack prevention ratio, 99.98% PDR, lower delay, and high throughput ratio.

References

[1] Das, Santosh Kumar, et al. Design Frameworks for Wireless Networks. Springer, 2020.

[2] Gowtham, M. S., and KamalrajSubramaniam. "Congestion control and packet recovery for cross layer approach in MANET." Cluster Computing 22.5 (2019): 12029-12036.

[3] Nehra, Deepa, Kanwalvir Singh Dhindsa, and Bharat Bhushan. "A Security Model to Make Communication Secure in Cluster-Based MANETs." Data Engineering and Communication Technology. Springer, Singapore, 2020. 183-193.

[4] Peng, Wei, and Xicheng Lu. "AHBP: An efficient broadcast protocol for mobile ad hoc networks." Journal of computer science and technology 16.2 (2001): 114-125.

[5] Erdelj, Milan, MichałKról, and Enrico Natalizio. "Wireless sensor networks and multi-UAV systems for natural disaster management." Computer Networks 124 (2017): 72-86.

[6] Yadav, Ajay Kumar, and SachinTripathi. "QMRPRNS: Design of QoS multicast routing protocol using reliable node selection scheme for MANETs." Peer-to-Peer Networking and Applications 10.4 (2017): 897-909.

[7] Lou, Wei, and Jie Wu. "A cluster-based backbone infrastructure for broadcasting in manets." Proceedings International Parallel and Distributed Processing Symposium. IEEE, 2003.

[8] Gautam, Divya, and VrindaTokekar. "A Comparative Study of DoS Attack Detection and Mitigation Techniques in MANET." Social Networking and Computational Intelligence. Springer, Singapore, 2020. 615-626.

[9] Vanitha, K., and AMJ ZubairRahaman. "Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol." Cluster Computing 22.6 (2019): 13453-13461.

[10] Jamal, Tauseef, and Shariq Aziz Butt. "Malicious node analysis in MANETS." International Journal of Information Technology 11.4 (2019): 859-867.

[11] Bisen, Dhananjay, and Sanjeev Sharma. "Fuzzy based detection of malicious activity for security assessment of MANET." National Academy Science Letters 41.1 (2018): 23-28.

[12] Ghathwan, Khalil I., and Abdul Razak B. Yaakub. "An Artificial Intelligence Technique for Prevent Black Hole Attacks in MANET." Recent Advances on Soft Computing and Data Mining. Springer, Cham, 2014. 121-131.

[13] Rana, Anuj, VinayRana, and Sandeep Gupta. "EMAODV: Technique to prevent collaborative attacks in MANETs." Procedia Computer Science 70 (2015): 137-145.

[14] Jamal, Tauseef, and Shariq Aziz Butt. "Malicious node analysis in MANETS." International Journal of Information Technology 11.4 (2019): 859-867.

[15] Hussain, Mohammed Ali, and D. Balaganesh. "Prevention of Packet Drop by System Fault in MANET Due to Buffer Overflow." Intelligent Computing and Innovation on Data Science. Springer, Singapore, 2020. 615-620.

[16] Gupta, Prakhar, et al. "Reliability factor based AODV protocol: Prevention of black hole attack in MANET." Smart Innovations in Communication and Computational Sciences. Springer, Singapore, 2019. 271-279.

[17] Su, Ming-Yang. "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems." Computer Communications 34.1 (2011): 107-117.

[18] Vo, Tu T., Ngoc T. Luong, and Doan Hoang. "MLAMAN: a novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network." Wireless Networks 25.7 (2019): 4115-4132.

[19] Gurung, Shashi, and Siddhartha Chauhan. "A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET." Wireless Networks 25.4 (2019): 1685-1695.

[20] Doss, Srinath, et al. "APD-JFAD: accurate prevention and detection of jelly fish attack in MANET." Ieee Access 6 (2018): 56954-56965.

[21] Gayathri, S., et al. "Wormhole Attack Detection using Energy Model in MANETs." 2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC). IEEE, 2019.

[22] Gurung, Shashi, and Siddhartha Chauhan. "A novel approach for mitigating gray hole attack in MANET." Wireless Networks 24.2 (2018): 565-579.

[23] Gautam, Divya, and VrindaTokekar. "Pattern Based Detection and Mitigation of DoS Attacks in MANET Using SVM-PSO." International Conference on Sustainable and Innovative Solutions for Current Challenges in Engineering & Technology. Springer, Cham, 2019.

[24] Gurung, Shashi, and Siddhartha Chauhan. "Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET." Wireless Networks 25.3 (2019): 975-988.

[25] Rajendran, N., P. K. Jawahar, and R. Priyadarshini. "Makespan of routing and security in Cross Centric Intrusion Detection System (CCIDS) over black hole attacks and rushing attacks in MANET." International Journal of Intelligent Unmanned Systems (2019).

[26] Chang, Jian-Ming, et al. "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach." IEEE systems journal 9.1 (2014): 65-75.

[27] Odili, Julius Beneoluchi, MohdNizamMohmadKahar, and Shahid Anwar. "African buffalo optimization: A swarm-intelligence technique." Procedia Computer Science 76 (2015): 443-448.

[28] Selvi, P. Tamil, and C. Suresh GhanaDhas. "A novel algorithm for enhancement of energy efficient zone based routing protocol for MANET." Mobile Networks and Applications 24.2 (2019): 307-317.

[29] Bhuvaneswari, R., and R. Ramachandran. "Denial of service attack solution in OLSR based manet by varying number of fictitious nodes." Cluster Computing 22.5 (2019): 12689-12699.

[30] Bhande, Premala, and M. D. Bakhar. "Cross layer packet drop attack detection in MANET using swarm intelligence." International Journal of Information Technology (2019): 1-10.

[31] Chaitanya, G.K.,Amarendra, K.,Aslam S.,Soundharya, U.L.,Saikushwanth V., "Prevention of data theft attacks in infrastructure as a service cloud through trusted computing" International Journal of Innovative Technology and Exploring Engineering, 2019, 8(6 Special Issue 4), pp. 1278-1283.

[32] Gogineni Krishna Chaitanya and Krovi Raja Sekhar, "GAIT based Behavioral Authentication using Hybrid Swarm based Feed Forward Neural Network" International Journal of Advanced Computer Science and Applications (IJACSA), 11(9), 2020. http://dx.doi.org/10.14569/IJACSA.2020.0110939.

[33] D Toradmalle, J Muthukuru, B Sathyanarayana "Cryptanalysis of an Improved ECDSA", International Journal of Engineering Research and Technology volume-11,issue-2,pg no:615-619.

[34] Gogineni Krishna Chaitanya and Krovi.Raja Sekhar(in press), "Knowledge-Based Gait Behavioural Authentication Through A Machine Learning Approach" International Journal of Biomedical Engineering and Technology(in press).

[35] Priyadarsini P., Sai M.S.S., Suneetha A., Santhi M.V.B.T."Robust feature selection technique for Intrusion Detection System". International Journal of Control and Automation 2018.

[36] Gummadi A, Rao K.R."EECLA: Clustering and localization techniques to improve energy efficient routing in wireless sensor networks", Indonesian Journal of Electrical Engineering and Computer Science 2018.

[37] B.Suresh Babu."Adaptive and Efficient Routing Model for MANET using TSCH Network" Jour of Adv Research in Dynamical & Control Systems" 2018.

[38] Kavitha M., Anvesh K., Arun Kumar P., Sravani P." IoT based home intrusion detection system", International Journal of Recent Technology and Engineering 2019.

[39] Sai Harika T., Madhusri N., Varaprasad P.V.V."Detection, prevention and mitigation of black hole attack for MANET".International Journal of Recent Technology and Engineering 2019.

[40] Swetha K., Sowmya V., Srihitha K., Adithya D," A novel technique for secure routing in wireless sensor networks", International Journal of Innovative Technology and Exploring Engineering 2019.

[41] Bhandari R.R., Rajasekhar K." Energy-efficient routing-based clustering approaches and sleep scheduling algorithm for network lifetime maximization in sensor network: A survey", Lecture Notes in Networks and Systems, 2020.

[42] Ananthakumaran. S, Sathishkumar. M, Bhavani. R, Ravinder Reddy. R, "Prevention Of Routing Attacks Using Trust-Based Multipath Protocol," International Journal Of Advanced Trends In Computer Science And Engineering, Vol. 9, No. 3, Pp. 4022-4029, May-June, 2020.

[43] Gogineni Krishna Chaitanya and Krovi.Raja Sekhar, "A Human Gait Recognition Against Information Theft in Smartphone using Residual Convolutional Neural Network" International Journal of Advanced Computer Science and Applications(IJACSA), 11(5), 2020.http://dx.doi.org/10.14569/IJACSA.2020.0110544.

[44] V Kavidha, S Ananthakumaran -,"Novel energy-efficient secure routing protocol for wireless sensor networks with Mobile sink" Peer-to-Peer networking and Applications 2019.

[45] D Toradmalle, J Muthukuru, B Sathyanarayana," Certificateless and provably-secure digital signature scheme based on elliptic curve."- International Journal of Electrical & Computer Engineering (2088-8708)- 2019.

[46] Ananthakumaran.S, Debrup Banerjee, P. G. Om Prakash, R. Bhavani, "Fuzzified Energy Efficient Mechanism (FEEM) in Wireless Sensor Network," International Journal of Emerging Trends in Engineering Research, Vol. 8, No. 9, pp. 6889-6396, September, 2020.