Trust Management Based Improved Mechanism to Prevent MANET from Security Threats Using Optimized SVM

Vishal Walia, Rahul Malhotra

Abstract: ***A temporal network creates various issues which are managed by nodes, communicating with the base station. The flow of packets with different routes usually attacked by malicious nodes, such an attack is also termed as black hole attack. A novel FSAODV mechanism is proposed in this paper to prevent the information from malicious nodes by following the Ad-hoc on demand distance vector (AODV) protocol. The detection of threats due to the black hole and route enhancement is implemented using the bio-inspired algorithms. Firefly algorithm and Support Vector Machine (SVM) algorithms are developed to determine the throughput, Packet Delivery Ratio (PDR), and TDR. A comparative analysis has been done to portray the success rate of proposed work. For the comparison, research works of Ashok Koujalagi and Rushdi A. Hamamreh are considered. 33.33% enhancement has been noted in throughput with Ashok Koujalagi and74.44% with Rushdi A. Hamamreh. 21.4% enhancement has been seen in PDR with Ashok Koujalagi and 91.71% with Rushdi A. Hamamreh.***

Keywords: Black hole attack, Route discovery, Ad hoc on demand distance vector, Firefly, Support vector machine, Detection rate, Throughput, Packet delivery ratio

INTRODUCTION

A significant role has been conducted by the wireless network in the field of communication. Presently, the wireless network finds applications in military, industrial and in PAN (Personal area networks). As we know that wired as well as wireless networks differ only in communication media. For wired communications, media like co-axial cable, optical fibres are used whereas for wireless communication no physical medium is required. Wireless communications increases day by day due to their advantages like ease of installation, reliability, cost, bandwidth, security, and efficiency of the network. Example of wireless networks is wacky tacky, cell phone, Wi-Fi, WiMAX, Satellite, and RADAR communication. Wireless communication in MANET communicates without any base station considers as forthcoming. In such type of networks, nodes communicate with each other, acting as source or destination for one and other nodes. The number of users and application are created by using these nodes and routing protocols. The routing paths for the transmission of information using the protocol over the channel are variable. Due to excessive use of wireless network and change in topology, routing in a wireless network is a challenge for the users.

Revised Manuscript Received on July 05, 2019.

Mr. Vishal Walia, scholar at IKG Punjab Technical University, Jalandhar.

Dr. Rahul Malhotra, Bachelor of Electronics and Telecommunication Engineering from Amravati University Amravati,

he rapid transformation of information over the nodes makes the network vulnerable to various issues. There is enough research in the literature and many routing protocols are developed such as AODV protocol, route discovery protocol etc. An AODV protocol, on-demand protocol, dynamic MANET, and temporarily ordered routing protocol was used for better communication. The performance of AODV protocol is considered as optimal among other protocols. The routing protocols can be reactive and proactive in nature [1]. More specifically, the communication in MANET in the remote medium is according to the access points. Each customer's basic station or access point is restricted to remote systems within a mobile-specific system, for example, MANET, the type of ad hoc network. Self-organizing system of portable routers associated with remote connections without any access point. In a system, each movable device manages itself; there is no middle power in MANET. Every device can move freely in all directions. The main aim of developing the network is to carry the device for the maintenance of information for routing the traffic appropriately. The routing structure of MANET follows two types of architecture namely reactive and proactive. These are also called as on-demand architecture. The proactive mechanism supports static routing in which the route elements are fixed. In the reactive protocol, the communication protocol is dynamic or in other words, it is Ad-Hoc. The discovery protocol aims to search the route when it is desired. This structure prevents a lot of bandwidth in the network as well as the memory of the network as the nodes do not carry enough memory with them. The reactive architecture has its own issues. The issues of the ad hoc network are due to the mobile architecture of nodes. An ad-hoc network has the following areas of work:

- Routing
- Load Management
- Reliability and Trust Modelling

Let $A(N, RS)$ be an ad-hoc network with N number of nodes and supports RS type of routing structure. $A(N, RS)$ Also supports a trust model T_m . The ordinals of an ad-hoc network are as follows.

A. Route Discovery

Definition 1: A route discovery mechanism is generally supported by reactive route architecture in ad-hoc networks. A route $R(N_l, Cov_{lim})$ covers N_l elements and Cov_{lim} threshold value for the selection of next node. The next node selection may be based on nearest node policy. Here the selection procedure does not ensure the load balancing mechanism for nodes. This gives the first area of work in this proposal.

Problem Definition 1: For(N_l, Cov_{lim}) , the selection of next the node in the R is only feasible if N_{next} has enough resources to process the incoming data packet and has a "μ" load utilization which must be lower than that of network load utilization. If the load utilization parameter is not satisfied then whether the structure should search a new node is dependent on the followinglemma:

Lemma 1: It has two elements namely true and false. True is represented by 1 and false is represented by 0.

Table .1.Fitness Criteria for Search and Wait for cost

1	**If** $\mathbf{f(Search_{Cost}) < f(Wait_{Cost})}$
0	**Otherwise**

A shown in Table 1, f is the fitness function for search and wait for cost evaluation.

B. Trust Management

Definition 2: A node N is labelled as trust worthy if, $N_{past_{Route_{Transfer}}} > 1$, that means the node has successfully participated in any data transfer through any route. As ad-hoc network is prone to intrusion due to its mobile nature, a trust table (TT) is maintained in the network which contains the information of nodes who ever actively participated in any data transfer or even has appeared in route discovery process detailed in Definition 1 .This framework of management is called trust management.

Problem Definition 2: N is termed as trusted only if it has participated in any route discovery or at-least has appeared in any discovery process. This architecture does not ensure that N cannot be intruded. The adaptive mechanism is required which analyses the behaviour of the nodes based on the Quality of Service (QoS) . Manual tracking is not always possible and hence utilization of Machine Learning is required.

Lemma 2: If a node is consuming more energy in the network, it is not necessarily due to the intrusion effect, it might be because of the overloading of the data packets. Hence integration of Lemma 1 will produce correct Lemma 2.

This paper focuses on the Black Hole Attack as the trust management issue and the proposed algorithm follows AODV as the routing protocol.

C. Black Hole Attack

A black hole is a network area or a number of region nodes. Node, resident in the region and joins the network. In a black hole attack, malicious nodes are presented for providing a shortcut to the destination node, therefore, mislead routing protocol. As a result, an attacker can intercept node packages or can keep it. At the forged root time, the forged routing successfully establishes. It depends on whether malicious nodes discard or send packets to each place when they want. Black hole attack in MANET and wireless network is ubiquitous. The nodes affecsted due to black hole does not identify the actual route, follows the shortest path. The network having such type of nodes, network protocol does not follow the routing protocol. Hence, packets are lost in such type of networks having a black hole. The commonly used protocols are insufficient to tackle the black hole issue. Hence AODV architecture is followed to determine and establish the route discovery mechanism to avoid the black hole affected nodes.

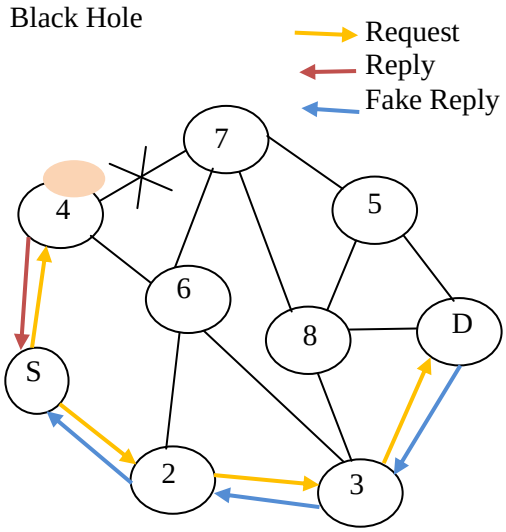

Fig.1 Black hole attack

The classification of black hole attack is defined below:

a) Internal Blackhole attack

In this black hole, the attack has malicious nodes, usually suitable for providing the source as well as destination paths. When it gets the chance, the vicious node marks itself as a dynamic data routing component. At this stage, it is now possible to start the outbreak through data transmission between several nodes. This is an internal attack as the nodes belong to packet routing. In several challenges of perceiving internal counterfeit nodes, internal attacks are very sensitive to protecting the opposite direction. Fig. 1 depicts the mechanism of black hole attack.

b) External Blackhole attack

An external attack substantially stays in the outer parts as well as denies entrance to network traffic otherwise producing overcrowding in the network or else by disturbing the complete network. The external attack could turn out to be a kind of internal attack the minute it takes control of interior malevolent node.

The rest of the paper is organized in the following manner. Section II is for the literature survey whereas Section III presents the proposed work architecture. Section IV demonstrates the results and Section V concludes the results.

LITERATURE SURVEY

Black hole attack is a serious concern. A trust factor is required to make the system reliable. A trust model is build up within the network for each node. The proposed model executes as IDS (Intrusion Detection System) for the detection and mitigation of black hole attack in MANET [2]. MANET is considered as a wireless medium which is deployed for a specific objective or some other utilization. As there is a shortage of central coordination, the network allocates an intrinsic trust relationship between the nodes that develop the network. Every node

usually trusts the neighbour for transferring the packets in the network when the packets will be the destination. Then, each network node may examine the neighbours by maintaining the track of the packets being passed via the neighbours. This characteristic of the network let to implement a trust model for co-relating with the innate trust being shared between the nodes. Energy-aware detection algorithms detect the black hole attack with enhanced security [3]. There is already enough research regarding black hole attack using AODV protocol [4, 5]. But still, preventing algorithms are developed using the defined protocol and different techniques were implemented to determine the black hole attack [6, 7]. Some researchers focussed on detecting and mitigating the wormhole attack while transmitting and propagating the data [8]. The algorithm is proposed has provided more safety towards network and has prevented it from that type of attacks. It facilitates to enhance the PDR and lessens the control overhead by enhancing the routing protocol performance. Future lies in enhancing the table entries in the destination node for detecting the wormhole nodes more precisely. It can also improve the network security with the deployment of effective techniques for preventing hybrid and DoS attacks with the assistance of the novel fresh algorithm [9]. The research regarding classification to network attacks in the network by differentiating each node in a formative manner is presented using the NS2 simulator. The aim of this research is to analyse the different attacks with distinctive measures for mitigation of attacks [10]. The networks are utilized in each field and the influence of the users has promised MANET development. MANET is known as a dynamic network that doesn't need some infrastructure network or some backbone because it deploys user to user connection among the nodes. A number of executions have been done in MANET that ranges via defense to the multi-user gaming that requires saving the network from different attacks and trespassers. ECBDS techniques have been utilized by the scholars to save the network from Byzantine attack and Resource Consumption [11]. The implementation has been taken place in MANET in which the mobile implements as a node and is known as infrastructure less and wireless network in which the nodes travel freely and may vary the positions as well. The consumption of resources has been detected by considering novel security checks for the algorithms. The usage of bandwidth and the battery for some node is not according to the proper utilization of the threshold setting. The Byzantine attacks are detected when the acknowledged is not taken by some source in the appropriate time [12]. In addition, trust-based mechanism integrates secure routing protocol in a wireless network to avoid black bole attacks [13]. Some researchers mitigate such attacks using the energy-aware routing protocol through which multiple routes were detected, which effectively share these routes with other nodes to detect a black hole in the network [14]. More specifically, scholars attempt to improve the efficiency of the developed system. Therefore, threshold-based novel trust mechanism is implemented to optimize the lifetime of the network and routes by avoiding attacks [15]. Considering alarm packer within the CBDS methods is ECBDS method. The proposed methods have shown improved results as contrasted towards CBDS method. ECBDS method is better as contrasted to 2 ACK, DSR and BFTR according to the varied metrics like PDR, Throughput, and E2ED [16]. The scenarios of MANET have been observed by considering the facts like; Presence and non-presence of attack with AODV [17]. The assessment of the routing protocol is by utilizing different loads and by considering simulation metrics. Consequently, the examination of the network is by QoS parameters, such as PDR, Throughput and an AE2ED in the network being deployed. The results obtained after the simulation has shown that the network performance in black hole attacks has decreased predominantly in PDR because the nodes have discarded each of the data packets being traversed the path. Additionally, the performance of throughput has decreased substantially in the existence of malicious nodes. This is because of the reason that the packets being transferred are not delivered towards the destination. There is some increment in the AE2ED when there is no black hole attack effect. It is accepted as malicious nodes have quickly transferred the reply without checking the routing table. The variations in the QoS parameters have depicted the network performance has decreased predominantly when there is a presence of black hole attack. [18] has given a solution for detecting black hole attack using AODV routing protocol, namely, Black hole detection system (bds)AODV The researchers has considered initial route reply as the feedback for malicious node and removed. The subsequent one is considered for the route reply saving method because it is taken as the destination node. bdsAODV has more PDR with 46.7% and Jitter as 5% and has an enhanced throughput. The system lacks in validating the attacker.

MANET is a structured network where the nodes vary their location with respect to time. The network aims to transfer the secure data from one end to another with a stable route. For the secure and stable transmission of data, routing protocols are there being designed by a number of researchers. As the nodes in the network are movable and that may lead to data loss, therefore, to design a stable and secure route is a big task. So, in this research, AODV routing protocol has been considered for the same, but, AODV routing protocol does not analyze the behaviour of intermediate nodes within the route that results in more data loss. Consequently, firefly algorithm and SVM has been used for this purpose with the fitness function. Firefly algorithm helps in analyzing the behaviour of intermediate nodes using their fitness function. If the behaviour of node fulfils the fitness criteria of Firefly than it would be considered in the route than it would be considered as black hole attack.

PROPOSED MODEL

The proposed work model is divided in three sections namely Route Discovery, route enhancement and attacker detection.

A. Route Discovery

The route discovery process follows the architecture of AODV and it also optimizes utilizing Firefly algorithm. Pseudo code 1 is for the placement of nodes and route discovery followed by its optimization. When after a certain time frame t , a node is not responding then, the alternative node search is done utilzing Firefly algorithm. The

basics of Firefly Algorithm are as follows:

i. Fly-Light: It is the intensity of the light which the fly demonstrates when it is in air. It is the light which decides the flying circle of the fly.
ii. Notation of Fly out of Circle: The fly groups send a notation to the fly going out from the group. The group flies raises their light intensity to notify the outgoing fly. The group flies wait for a certain time period and even after the certain time frame if the outgoing fly does not respond back, the group fly considers it gone and moves ahead.

Pseudocode 1: Route Discovery Mechanism

1. Input: Sourcs (S), Destination(D)
2. Output: Route From S to D
3. $\text{Broadcast}_{\text{Msg}} = \text{Broadcast}('\text{Hello}')$
4. For each respondent of BroadcastMsg
5. $\text{Check}_{\text{Route}_{\text{requirements}}}$ ()
6. $\text{Select}_{\text{Node}}(\text{Ping})$
7. If Pings Back
8. $\text{Add}_{\text{To}_{\text{Route}}}$
9. End If
10. Repeat Until Destination is not found
11. End For
12. Return: Route fro S to D
13. End

Pseudo Code 1 broadcasts a Hello message at the source end. For every respondent of the broadcast message, the transferring node checks the requirements of the transfer that is the memory, bandwidth utilization, associated power with the respondents and the consumption of the power in order to transfer the data. After checking all the requirements, the transferring node pings the selected node and if the selected node pings back, the respondent is added to the route list. The problem starts when the Broadcast respondent does not ping back. Why a node will reply to the broadcast and will not ping back after the selection. It might be due to the overload or any physical failure.

B. Route Enhancement

This section enhances the route which has been discovered previously. The proposed architecture utilizes Firefly algorithm in such a scenario. Here, a trust related an issue arises which is discussed in Lemma 2.

Pseudo Code 2*: *Optimization

Input: *Other Respondents (OR)*
Output: *Optimized Data*

1. $Fly_{Light} = [Power_{Consumtion}(\text{OR}), Activity_{Time}(\text{OR})]$
2. $Fly_{Threshold} = \sum_{i=1}^{n} Fly_{light}$
3. $Fly_{Flash_{time}} = Time_{to_{Respond}}$
4. ***If*** $Fly_{Threshold} * Fly_{Flash_{Time}} < Fly_{Light}$
5. $Ignore$
6. ***Else***
7. $Fly_{Light_{Diff}} = Fly_{Light} - Fly_{Threshold} * Fly_{Flash_{Time}}$
8. $Add\ Fly_{Light_{Diff}}\ to\ Possible\ List$
9. $Find\ Index.Minimum\ (Fly_{Light_{Diff}})$
10. $Selectd\ .Node = Index.Id$
11. ***End*** If
12. ***Return***: $Optimized\ data\ of\ nodes$
13. ***End***

The proposed model utilizes the power consumption of the respondents and their activity time in the network as the main light source. It creates the light threshold by considering the lighting time as well. Any respondent which satisfies the fly threshold opts and then the minimum difference value is selected as the respondent. Once the route is established, the node may fall under security threats as the attacker will obviously want to make the maximum damage in the network. Once the network is formed and data starts to transfer from one end to another, the process will attract intruders. The Black Hole attacker is one of the smart kind. It does not continuously drop the packets

C. Attacker detection

The proposed work model utilizes an adaptive learning mechanism by using Support Vector Machines (SVM). SVM is two classes or binary class classifier and it can only identify two classes at one time and that's all we want. It is a two-phase detection mechanism which identifies the affected path followed by node identifications. For both the phases, SVM uses "polynomial kernel". The algorithmic architecture is as follows.

Pseudo Code 3*: *SVM with polinomial kernel

Input: *Parameters of nodes*
Output: *Affected node*

1. $Classify_{path}\begin{pmatrix} All_{Paths}, Power_{Consumption_{path}}, \\ Delay_{path_{structure}} \end{pmatrix}$
2. $\boldsymbol{For}_{each} pth\ in\ Paths$
3. $Input_{SVM} = Concatinate(Power_{Consumption_{path}}, Delay_{pathstructure}$
4. $Target\_SVM[Pathid, 1000];$
5. $Train\ and\ Classify$
6. ***End*** *For*
7. ***Return***: Affected node
8. **End**

SVM takes each path and its associated power consumption combined with the produced delay in the path as the proposed structure keeps a record for every path and every node. Now it is a supervised learning mechanism, the classified with the classified element then it is termed as a suspected route.

For each route, the same structure is applied and classified. Route should be equal to the passed training route. In such a case, if the route element does not match, the only difference is the power consumption for the path will be replaced by the power consumption of the node and the delay produced by the path will be replaced by the delay produced by individual nodes.

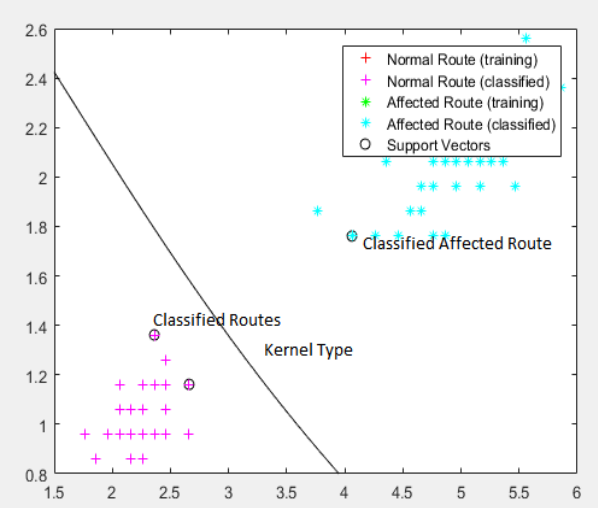

Fig.2 Classified Route

Fig 2 and Fig 3 depicts the classification process of the nodes.

The classification of the node architecture is similar to that of node route classification. The other ordinal measures of this classification are shown in Table 2.

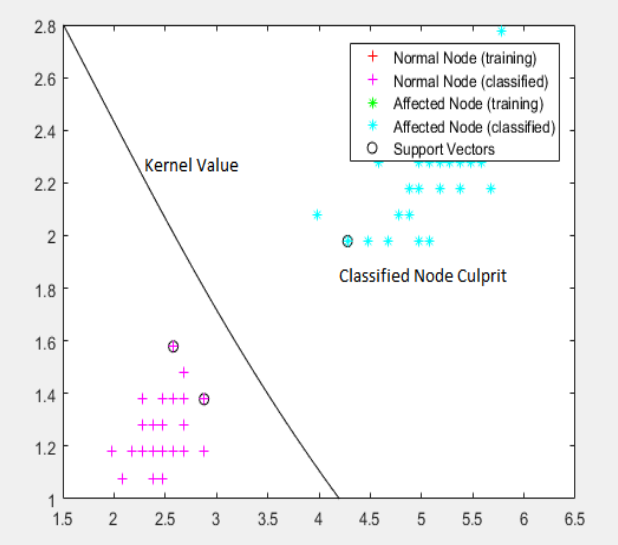

Fig.3 Classified Node

Table .2.Ordinal Measures of the Classification process

Parameters	Measure
Total Number of Simulations	1000
Total Number of Nodes	50-100
Area of Simulation	1000 * 1000
Kernel Type	Polynomial

RESULT AND DISCUSSION

Based on the classification structure, the following parameters are evaluated.

- Throughput : Total Received Packets per unit time
- True Detection Rate(TDR) : Total true detected intruders / Total Number of detections
- Packet Delivery Ratio(PDR) : Total number of received packets/ Total Transferred Packets

Table .3.True detection rate evaluation

Number of nodes	True detection rate (%)
20	88.29
25	81.26
30	79.45
35	76.89
40	76.05

Fig 4 and Table 3 represents the evaluation of TDR with respect to a number of nodes. X-axis is representing the number of nodes whereas Y-axis is representing the obtained values of TDR.

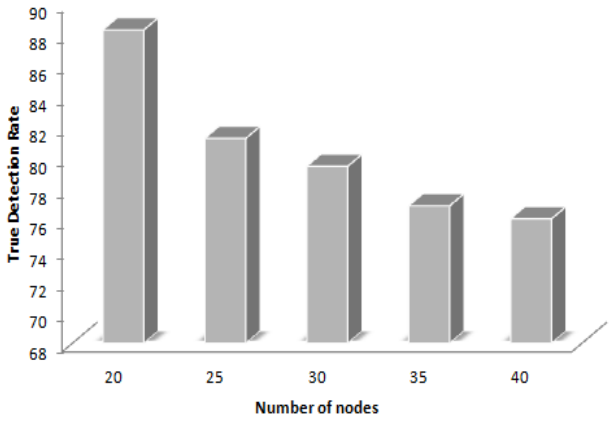

Fig.4 True Detection Rate

TDR helps in detecting the attacker nodes within the network using AODV with Firefly and SVM. With the less number of nodes, the detection of the attacker becomes an easy task. The average value of TDR is 80.38%.

Table .4.Comparison of throughput for proposed and bdsAODV [18]

Number of nodes	Throughput		
	bdsAODV [18]	RID-AODV [19]	FSAODV [Proposed]
20	4	4.3	6.1
25	6.5	1.5	7.2
30	2	1.3	6.9
35	4.8	1.1	7.5
40	6.7	1	8.3

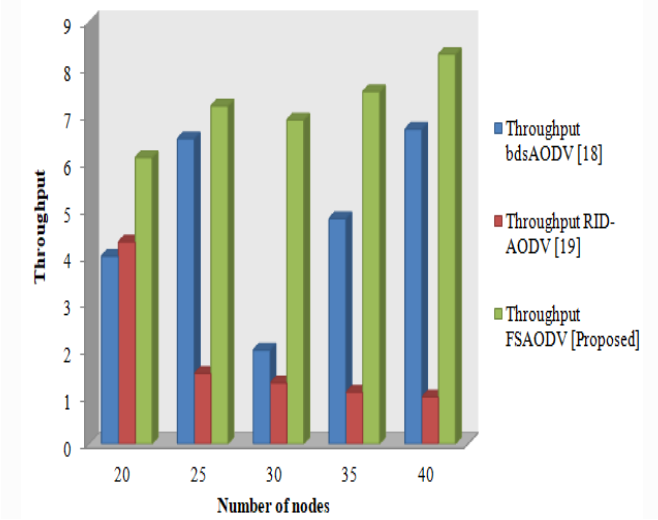

Fig.5 Throughput comparison

The comparison of throughput has been shown in Fig 5. The comparison has been drawn with bdsAODV [18], RID-AODV [19] and FSAODV [proposed]. Throughput represents the number of packets received at the destination with respect to simulation time. Here, Throughput has been calculated in kbps. The average value of bdsAODV [18] is 4.8 kbps; the average value of RIDAODV [19] is 1.84 kbps whereas the proposed FSAODV has an average value of 7.2 kbps. So, it is evident from the analysis that FSAODV [proposed] has better throughput as compared to a conventional methods. There is an enhancement of 33.33% in throughput with [18] and an enhancement of 74.44% with [19] of FSAODV [proposed].

Table .5.Comparison of PDR for proposed and bdsAODV [18]

Number of nodes	PDR (%)		
	bdsAODV [18]	RID-AODV [19]	FSAODV [Proposed]
20	38	12	54
25	62	7	68
30	24	5	72
35	44	3	63
40	63	1	81

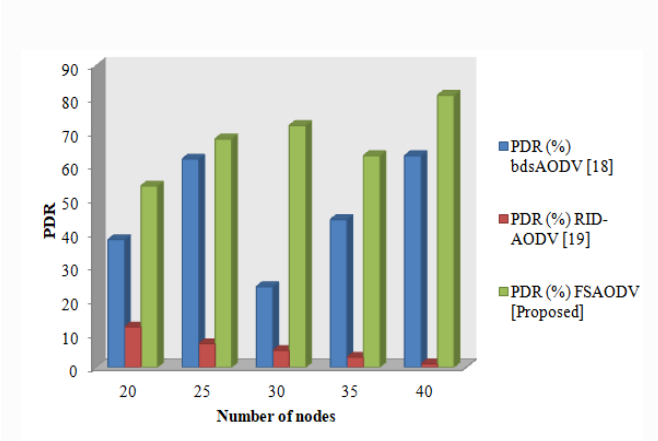

Fig.6 PDR comparison

PDR represents the packets transfer rate by intermediate nodes in a route. It is the sum of total data transfer rate which is generated by the source and received by the receiver by intermediate nodes. Fig 6 illustrates the comparison of PDR for bdsAODV [18], RID-AODV [19] and FSAODV [proposed]. The average value of bdsAODV [18] is 46.2%, the average value of RIDAODV [19] is 5.6% whereas the FSAODV [proposed] has an average value of 67.6%. The proposed FSAODV has shown an enhancement of 21.4% in terms of PDR than [18] and an enhancement of 91.71% with [19].

CONCLUSION

The main objective of the proposed FSAODV is to detect the route which is free from malicious attacks. More specifically, the architecture of the AODV protocol is utilized to detect the route. Robust firefly with SVM algorithms is used to optimize the developed algorithm and to discover the safe and stable data transmission. For the assessment, three scenarios have been considered, viz., route discovery, and route enhancement and attacker detection. Firefly has been considered in route enhancement process whereas; SVM has a job to detect the attackers. The proposed FFSVM has considered 40 nodes to execute the QoS parameters, such as TDR, Throughput and PDR. TDR has an average value of 80.38%. There is an enhancement of 33.33% in throughput with [18] and an enhancement of 74.44% with [19] of FSAODV [proposed]. The proposed FSAODV has shown an enhancement of 21.4% in terms of PDR than [18] and an enhancement of 91.71% with [19]. It is evident from the proposed system has shown fruitful results and has proved its reliability.

REFERENCES

1. S. Wali, S. I. Ullah, A. W. U. Khan, and A. Salam "A Comprehensive Study on Reactive and Proactive Routing Protocols under different performance Metric", Sukkur IBA Journal of Emerging Technologies, Vol. 1, No. 2, pp. 39-51, 2019.
2. . Sen, G. M. Moirangthem, K. Sharma, M. K. Ghose, and S. Sinha, "A Trust-Based Intrusion Detection System for Mitigating Blackhole Attacks in MANET", In Advanced Computational and Communication Paradigms, Springer, Singapore, pp. 765-775, 2018.
3. N. Panda, and B. Kumar Pattanayak, "Energy aware detection and prevention of black hole attack in MANET", International Journal of Engineering and Technology (UAE), Vol. 7, No. 2.6, pp.135-140, 2018.
4. S. Shahabi, G. Mahdieh, and B. Mehdi, "A modified algorithm to improve security and performance of AODV protocol against black hole attack", Wireless Networks, Vol. 22, No. 5, pp.1505-1511, 2016.
5. P. Gupta, G. Pratyaksh, P. Varshney, and N. Tyagi, "Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET", In Smart Innovations in Communication and Computational Sciences, Springer, Singapore, pp. 271-279, 2019.
6. R. N. Mohammad, R. P. Singh, A. Dey, and S.J. Ahmad, "ESMBCRT: Enhance Security to MANETs Against Black Hole Attack Using MCR Technique", In Innovations in Electronics and Communication Engineering, Springer, Singapore, pp. 319-326, 2019.
7. K.S. Arathy, and C.N. Sminesh, "A novel approach for detection of single and collaborative black hole attacks in MANET", Procedia Technology, Vol. 25, pp. 264-271, 2016.
8. R. Verma, R. Sharma, and U. Singh, "New approach through detection and prevention of wormhole attack in MANET", In 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), IEEE, Vol. 2, pp. 526-531, 2017.
9. N. Arya, U. Singh and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm", In 2015 International Conference on Computer, Communication

and Control (IC4) IEEE, pp. 1-5, 2015.
10. K.N. Chaturvedi, A. Kohli, A. Kamboj, S. Mendiratta, and N. Rakesh, "NS2 Based Structured Network Attack Scrutiny in MANET", In Networking Communication and Data Knowledge Engineering, Springer, Singapore, pp. 99-111, 2018.
11. P. Gupta, P. Goel, P. Varshney, and N. Tyagi, "Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET", In Smart Innovations in Communication and Computational Sciences, Springer, Singapore, pp. 271-279, 2019.
12. T. A. Kolade, "A Scheme for detecting and mitigating cooperative black hole attack in AODV-based MANET routing protocol", PhD dissertation, 2018.
13. A. Adnan, A. B. Kamalrulniza, M. I. Channa, and A.W. Khan, "A secure routing protocol with trust and energy awareness for wireless sensor network", Mobile Networks and Applications, Vol. 21, No. 2. pp 272-285, 2016.
14. R.T. Merlin, and R. Ravi, "Novel Trust Based Energy Aware Routing Mechanism for Mitigation of Black Hole Attacks in MANET", Wireless Personal Communications, pp.1-38, 2019.
15. B. Sen, M.G. Meitei, K. Sharma, M.K. Ghose, and S. Sinha, "Mitigating Black Hole Attacks in MANETs Using a Trust-Based Threshold Mechanism", International Journal of Applied Engineering Research, Vol. 13, No, 7, pp. 5458-5463, 2018.
16. M. G. Patil, A. Kumar, and A. D. Shaligram, "Performance Measurement and Analysis of MANET Routing Protocols on nodes Scalability", IJMSS-International Journal in Management and Social Science, Vol. 4, pp 443-451, 2016.
17. P. Rohal, R. Dahiya, P. Dahiya, "Study and analysis of throughput delay and packet delivery ratio in MANET for topology based routing protocols (AODV DSR and DSDV)", *International Journal for advance research in engineering and technology*, Vol. 1, No. 2, pp. 54-58, 2013.
18. Ashok Koujalagi, "Considerable detection of black hole attack and analysing its performance on AODV routing protocol in MANET (Mobile Ad hoc network)", American Journal of Computer Science and Information Technology, Vol. 6, No. 2, pp.1-6,2018.
19. Rushdi A. Hamamreh, "Protocol for Multiple Black Hole Attack Avoidance in Mobile Ad Hoc Networks", In Recent Advances in Cryptography and Network Security. IntechOpen, pp.25-41, 2018.

AUTHORS PROFILE

Mr. Vishal Walia did his Bachelor as well as Masters in Electronics and Telecommunication Engineering from IET, Bhaddal (Punjab Technical University, Jalandhar). He is currently a research scholar at IKG Punjab Technical University, Jalandhar.
His area of research are wireless and Mobile Communication, Fuzzy Logic, Neural Network and Optimization. He has published more than 30 research papers in National and International Journal of repute. He is a life member of ISTE.

Dr. Rahul Malhotra did his Bachelor of Electronics and Telecommunication Engineering from Amravati University Amravati, in year 2001. He did Masters of Technology in Electronics and Communication Engineering from Giani Zail Singh College of Engineering and Technology, Bathinda and Doctorate of Philosophy in the faculty of Engineering and Technology from Punjab Technical University in collaboration with Thapar University Patiala.
His area of research includes Evolutionary Computing Techniques, Wireless Communication systems. He started his professional career from HCL Technologies Bangalore and later he shifted to technical education industry, with elite educational groups of Punjab,
He specializes in Wireless Adhoc Networks, Fuzzy Logic, Neural Network and Optimization. He has published more than 110 research papers in National and International Journal of repute. He has guided more than 85 research thesis at Master's level and completed 04 Doctoral level of Research. He is a Fellow Member of Institution of Engineers, Calcutta, Institution of Electronics and Telecommunication Engineering, New Delhi and senior member of CSI and ISTE.
He served as faculty Head of Electronics and Communication engineering Guru Gobind Singh College of Engineering and Technology Talwandi Sabo, Adesh Institute of Engineering and Technology, Faridkot since 2001 to 2012 to teach Graduate and Postgraduate level of Engineering courses. In year 2011, he started groundwork to establish a new venture of Adesh Group at Chandigarh, Adesh Institute of Technology, Chandigarh Campus, Gharuan Tricity, and in year 2012, he joined as Founder Director-Principal of the campus.