Detecting Packet Dropping Misbehaving Nodes using Support Vector Machine (SVM) in MANET

Nirav J. Patel
Department of computer engineering-IT
Shri S'ad Vidya Mandal Institute of Technology
Bharuch 392-001, Gujarat, India

Rutvij H. Jhaveri
Department of computer engineering-IT
Shri S'ad Vidya Mandal Institute of Technology
Bharuch 392-001, Gujarat, India

ABSTRACT

Mobile ad-hoc network is suffering with various attacks due to the infrastructure-less network. Hence, MANET needs very specific security methods to detect false entrance of the misbehavior nodes. The networks work well if the nodes are trusty and act rightly cooperatively. In this paper, we are identifying and detecting packet dropping nodes using Support vector machine. Support vector machine is used reactively to classify nodes in two different classes either normal or malicious nodes. SVM takes as input the neighbor trust value, calculated with data packets and control packets. Our technique is implemented with AODV (Ad-hoc on demand vector routing) protocol. Our experimental results evaluated using packet delivery ratio (PDR), End-To-End delay, Average throughput, Normalized Routing Overhead, Average Energy Consumption.

Keywords

Mobile ad hoc network, machine learning techniques, packet dropping attacks, support vector machine (SVM)

1. INTRODUCTION

MANET is a wireless and decentralized network[13][19]. MANET routing depends on routing rules of conduct that divides into three categories: proactive, reactive and hybrid[17]. Mobile nodes establish communication with single hop and multi hop. In this proposed system we are using AODV(Ad-hoc on demand vector routing) protocol for routing[16][14].

Machine learning is basically distinguished in three phases: Data Gathering, Learning and classifying. The Machine learning way of doing things is divided in 3 categories: Supervised learning technique, Unsupervised learning technique, Reinforcement technique[18].

In our approach we are using support vector machine technique is part of supervised learning technique[13]. Trust based SVM used for classifying and mitigate packet drooping nodes. Trust management calculates the trust value of neighbour node with control packets and data packets and inserted into neighbour table. SVM have to train data through the neighbour trust value of neighbour node, then SVM classifies in two categories: normal and malicious.

In section 2, we present Related Work, Section 3 describes newly the Proposed method, Section 4,5 describes simulations results and experimental Results in section 6. Finally, the paper concluded and future scope in section 7.

2. RELATED WORK

Wenjia li. et al. [4][13] proposed a multidimensional trust management plan for calculating the trustworthiness value for particular a node. Support vector machine (SVM) based misbehavior detection way of doing things distinguish cruel and normal nodes. Outliner detection technique used to collect abnormal data of nodes and to describe edge-related limit of misbehavior. Three kinds of trust value are evaluated: collaboration trust (forwarding packets or not) calculates with logarithmic model. Behavioral trust (abnormal behavior, RTS flooding etc.) calculates with linear model. Reference trust (local view of them salves) calculates with exponential model. That identify different pattern by malicious node changing quickly as needed. SVM broadcast trustworthiness value of node to that neighbor's nodes and update trust value in trust table. Dempster shafer theory fused multiple behavioral data.

Meenakshi patel et al. [5][13] proposed as, detecting malicious attacks happing in AODV rule of conduct. Misbehavior as environmental factor, movement speed and communication range these types of misbehaving pattern detecting and classify them with SVM method of supervised learning method of machine learning. This way of doing things uses PMOR, PDER and PMIR behavioral numbers that measure things and compare with threshold value. SVM train with this behavioral metrics and that classify them in two class: normal and abnormal node. Disadvantage of this technique is predefining threshold value that may be updated by attacker node as changing in threshold value.

Fatemeh Barani et al. [6] [13] described a one-class SVM is kernel based approach for detecting anomaly based detection for statistical learning of nodes. It can detect black hole, worm hole, rushing, neighbor, flooding attacks. It uses kernel trick based function to classify nodes cruel and normal node. It is a mapping high dimensional feature space via kernel trick that work in three phases: initial training, updating, and detection.

Meenakshi patel et al. [7] [13] described a detecting and preventing flooding nodes in SVM. That classifies the nodes as par behavioral numbers that measure things of particular node cross the threshold limit which is predefined. If nodes cross threshold limit then that node detect as a evil node otherwise normal node. Packet delivery ratio (PDR), control overhead (CO), packet misroute rate (PMIR) behavioral metrics should be consider as that prevent the flooding attack with use of SVM classify them as train data.

Rehan akbani et al. [8] [13] proposed as, reputation system collecting in the past history of the transaction of the node and predicts the future of the node. That learns behavior of those nodes with reputation technique and distinguish normal and cruel node with SVM. Machine learning evaluate in the time series problem in RS. That collects the anomaly detected data with specified time slot and train in dataset. Total positive feedback divided with negative feedback and moves that value over secure medium.

Wenjia li et al. [9] [13] proposed as SAT-based misbehavior in automated trust management plan in MANE and SVM classify malicious and normal node. Predetermine weights define misbehavior contributes in overall measure of trustworthiness value of nodes. Packet drooping, packet modification and RTS flooding metrics used to calculate trust value of those nodes. Trust management observes direct and indirect behavior of node and dempster shafer theory fuse in one class and SVM classify them in evil and normal node.

Rahan akbani et al. [10] [13] described a reputation system to collect the past behavior of that node and predict the future of that node. SVM with RS apply in paper and prevents known and anomaly attacks. It detects dis-honest feedback by legitimate nodes. It predicts the behavior with time series predictions with fifteen time slots provide feedback of all neighbor nodes and SVM evaluate the value then distinguish normal and abnormal node.

3. PROPOSED SYSTEM

3.1 Flowchart of proposed system

Detect misbehaving nodes using machine learning techniques. In our approach we are using Support vector machine (SVM) technique for detecting and classifying malicious nodes according to the behavior of nodes. Our proposed technique overview is as below that describes in below Figure 1.

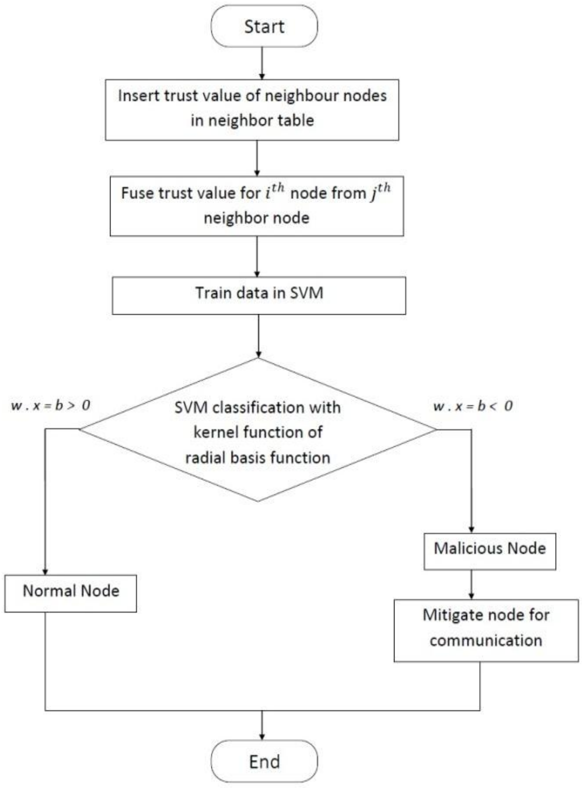
Start
Insert trust value of neighbour nodes in neighbor table
Fuse trust value for i^{th} node from j^{th} neighbor node
Train data in SVM
$w . x = b > 0$
SVM classification with kernel function of radial basis function
$w . x = b < 0$
Malicious Node
Normal Node
Mitigate node for communication
End

Fig 1: Proposed Framework of Detecting malicious nodes using support vector machine

3.2 Trust calculation algorithm for AODV [15]

Step 1

PR1= Count the number of packet received at each node.

PS2= Count the number of packet sent by each node.

RR1=Count the number of RREQ received at each node.

RS2=Count the number of RREP sent by each node.

Step 2

Calculate the P1 from neighbor node value:

$$P1 = \frac{Number\ of\ packet\ sent}{Number\ of\ packet\ received}$$

Calculate the P2 from neighbor node value:

$$P2 = \frac{Number\ of\ Route\ reply\ sent}{Number\ of\ Route\ request\ received}$$

Step 3

Calculate Trust Value = (P1*α) + (P2*β)

Where,

α and β = static weighting factor

Step 4

Insert Trust value into Neighbor Table.

3.3 SVM Misbehaviour classification algorithm:

Please We use SVM supervised technique for classification through trust value of that node.

STEP 1: Support vector machine based method is basically used for detection of malicious nodes and to restrict the data transmission through these nodes.

STEP 2: For each specified input SVM receives a set of input data. In this proposed technique, SVM collects all the behavior of each node in the network and then validate and classify those nodes according behavior of node. All of the nodes are classified either trusted or untrusted with the help of the SVM classifier integrating with MANET.

STEP 3: Classify in two class normal or abnormal nodes.

<u>Mathematical formulation in SVM[12].</u>

Give training data set (Xi,Yi):

X and Y is the input and output space vectors.

i = 1 to n

i-th dimension of trustworthiness for node Yi € {-1,+1}

Finds the hyper plane that have a maximum margin:

$$W * X = b$$

Where,

W = normal vector

b = threshold

Find the optimal hyper plane for convex optimization problem:

$$\min\{\frac{w^2}{2} + c \sum_{i=1}^{n} \varepsilon_i\}$$

$$yi(w * x_i + b) \geq 1 - \varepsilon_i, \qquad \varepsilon_i \geq 0$$

C = penalty constant for control

ε=Empirical error and margin

Following Lagrange equation:

$$Maximum\ L(\alpha_i) = \sum_{i=1}^{n} \alpha_i - \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \alpha_j y_i y_j K(x_j, x_i)$$

Subjected to

$\sum_{i=1}^{n} \alpha_i y_i = 0$ and $0 \le \alpha_i \le$ c for all $1 \le$ i $\le$ n

Where

$K(x_j, x_i) = \ kernel\ function$

$\alpha_i \ = Lagrange\ multipliers$

$Xi\ must\ correspond$

$0 \le \alpha_i \le$ c and $\sum_{i=1}^{n} \alpha_i y_i = 0$

It is called support vectors

With the help of equation (2) we can get (1)

$$w = \sum_{i=1}^{n} \alpha_i y_i x_i$$

Decision function can be represented as:

$$(X, \alpha, b) = \{\pm\} = \ Sign\ (\sum_{i=1}^{n} y_i \alpha_i K(x_i x_j) + b)$$

Training of SVM classification:

SVM classifier is trained with SVM train function

$$SVM_{struct} = \ SVMtrain(Data, Groups,' Kernel\ function', RBF)$$

Where,

Data: represent as matrix of points

Groups: column vector of each corresponding row

Kernel function: training data set to kernel space

Radial basis function

4. SIMULATION PARAMETER

The simulation parameter is explained as below which is used to produce the simulation suite for proposed solution.

Table I: Simulator Parameter

Parameter	Values
Simulator	NS 2.34
Routing Protocol	AODV, Packet dropper, SVM-AODV
Number of Nodes	10, 20, 30, 40, 50
Misbehaving Nodes	3, 6, 9, 12, 15(30% of number of nodes)
Simulation Time	150 s
Traffic Type	UDP
Packet Size	1000 bytes
Packet Rate	4 Packets/sec
Pause time	10 s
Number of connections	3,5,7,9
Scenario Size	800 X 800
Maximum Speed	20 m/sec

To overcome of problem of this paper, NS 2.34 simulator was used with 800 X 800 scenarios size. The routing protocol is used in the network for secure routing is called AODV. The packet size is taken 1000 bytes.

We have analyzed the performance parameter such as packet delivery ratio and end to end delay to evaluate the performance of the routing protocol.

(i) Packet Delivery Ratio: Total number of received packets divided by total number of packets transmitted by all nodes.

(ii) End to End Delay: First packet take times to transmission from source node subtracting by time to destination node receive those first packet.

(iii) Average Throughput: The Average number of packet deliver from source to destination is called throughput.

(iv) Normalized Routing Overhead: The ratio is measured between number of data packets and number of control packets over a communication channel it's called Routing overhead.

Attacker Model (Packet Dropper Attack): We create packet dropping attacker sends Even number packet and drop odd number packets with send (destination sequence number + 10(ten))

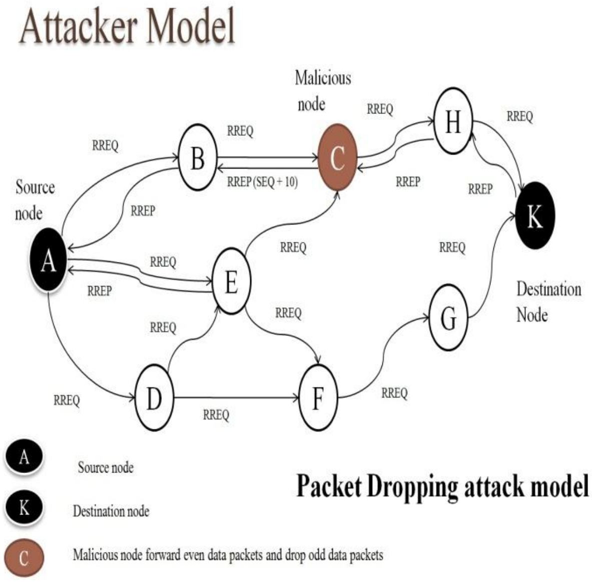

Fig 2: Packet Dropping Attack Model

5. EXPERIMENTAL RESULTS

A. Packet Delivery Ratio:

In this, the PDR of packet dropping attack is decreased with compare to the proposed scheme. To overcome of problem, we have taken 30% of malicious nodes in packet dropping attack to analyze the parameter. The below figure describes the comparison between the proposed scheme and packet dropping attack with respect to PDR.

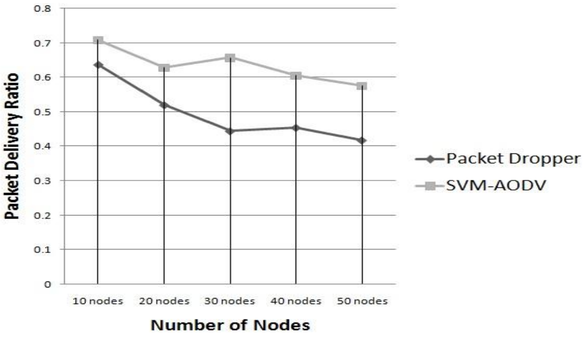

Fig 3: Packet Delivery Ratio (3 connection & 30% malicious node)

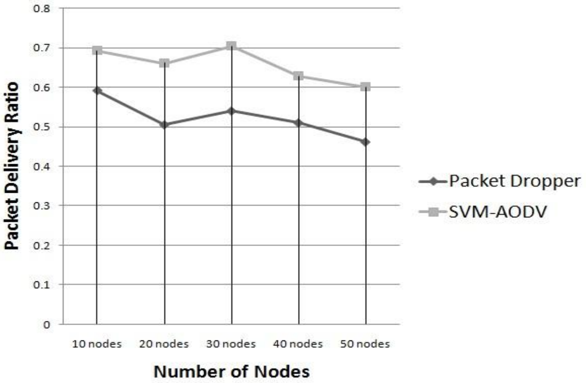

Fig 4: Packet Delivery Ratio (5 connection & 30% malicious node)

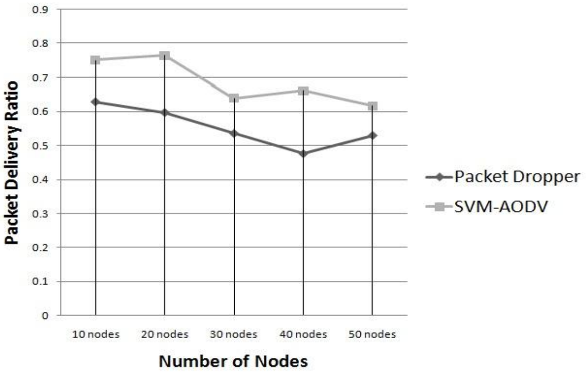

Fig 5: Packet Delivery Ratio (7 connection & 30% malicious node)

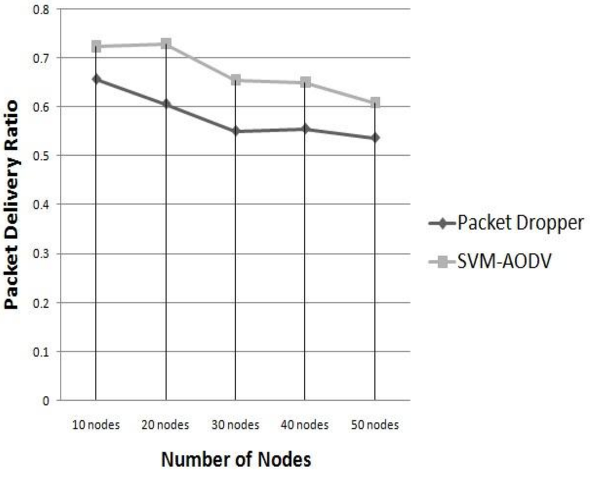

Fig 6: Packet Delivery Ratio (9 connection & 30% malicious node)

B. End to End Delay

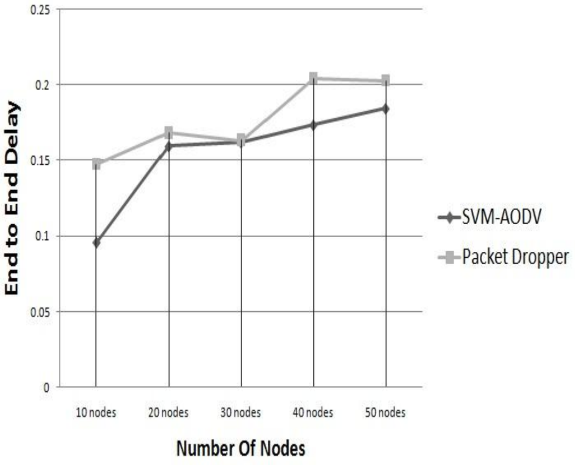

Fig 7: End to End Delay (3 connection & 30% malicious node)

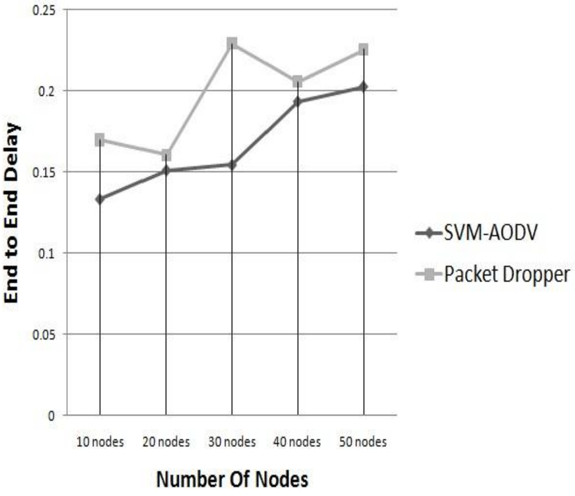

Fig 8: End to End Delay (5 connection & 30% malicious node)

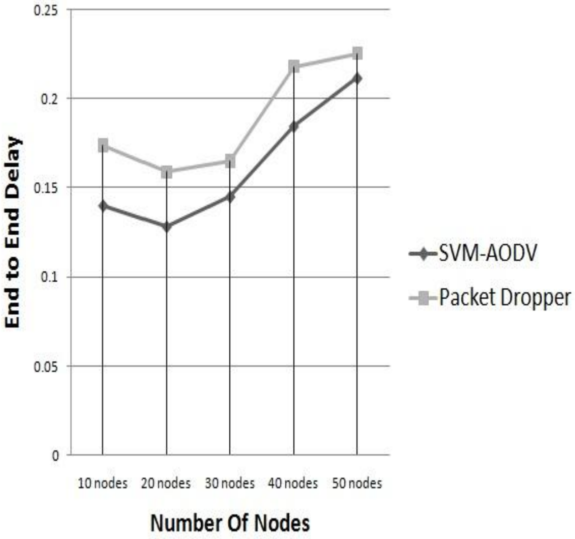

Fig 9: End to End Delay (7 connection & 30% malicious node)

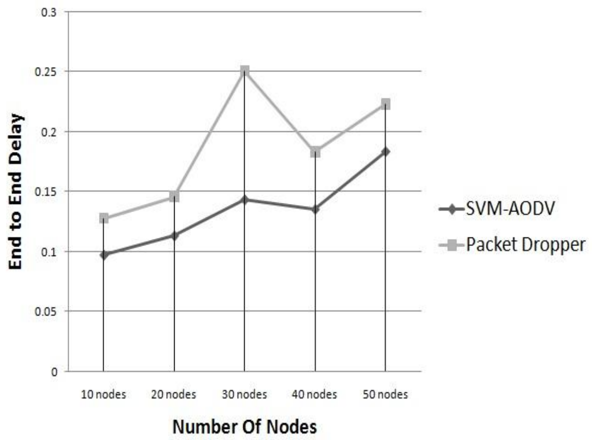

Fig 10: End to End Delay (9 connection & 30% malicious node)

It measure the average delay time that is taken by data packet between sources to destination. The below figure describes the comparison between the proposed scheme and packet dropping attack with respect to end to end delay. In this, the delay is increased in packet dropping attach with compare to proposed scheme.

C. Average Throughput

It measure the average of successful packet transmission from source to destination over a communication channel. In this, the performance of the network is increased in case of SVM-AODV.

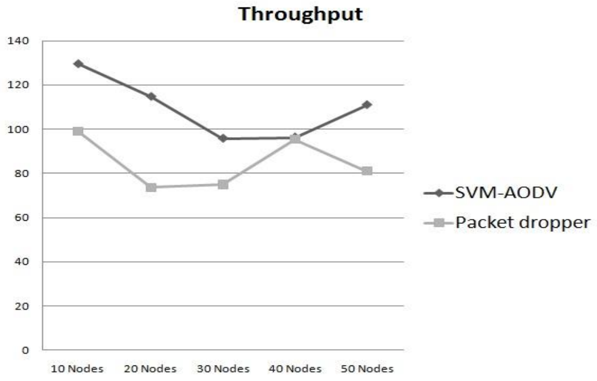

Fig 11: Average Throughput (3 connection & 30% malicious node)

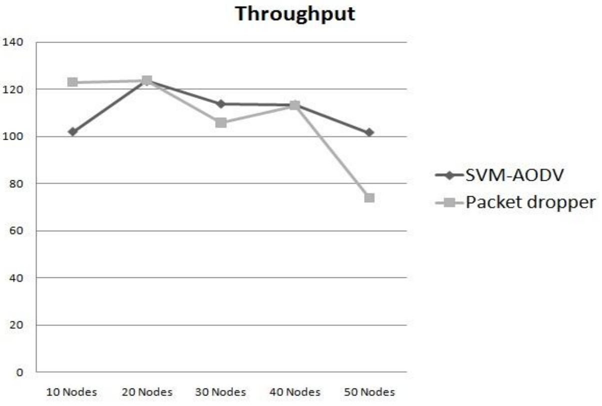

Fig 12: Average Throughput (5 connection & 30% malicious node)

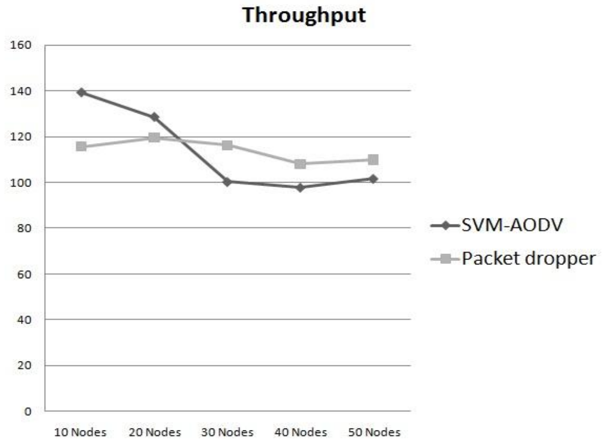

Fig 13: Average Throughput (7 connection & 30% malicious node)

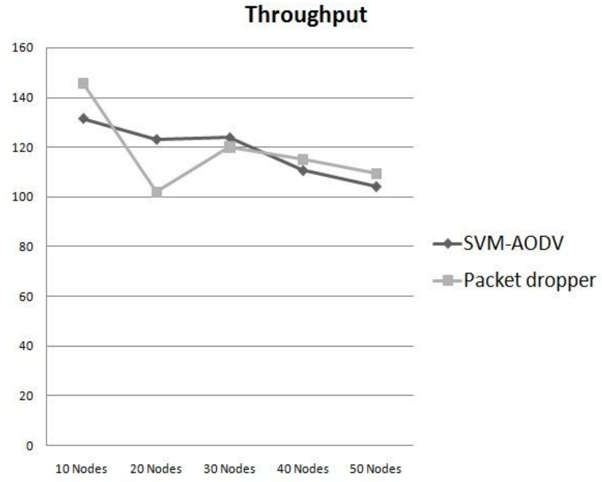

Fig 14: Average Throughput (9 connection & 30% malicious node)

D. Normalized Routing Overhead

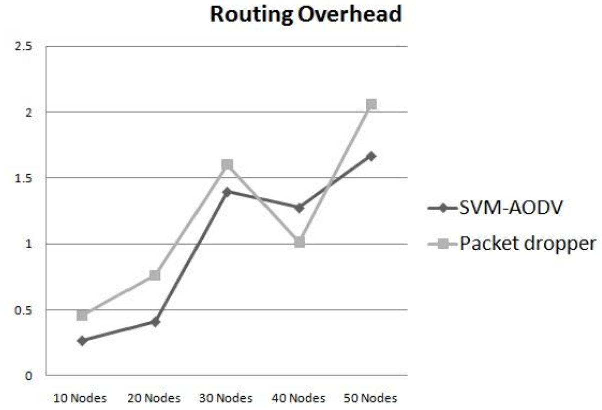

Fig 15: Routing Overhead (3 connection & 30% malicious node)

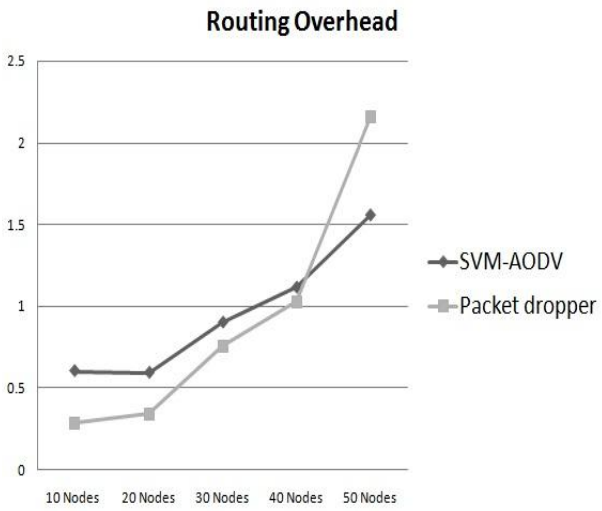

Fig 16: Routing Overhead (5 connection & 30% malicious node)

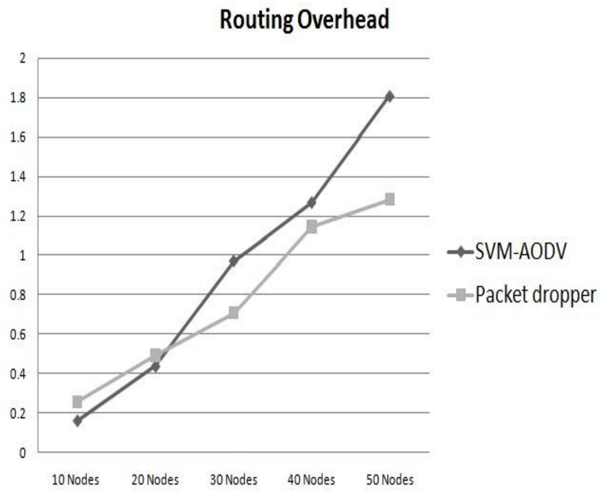

Fig 17: Routing Overhead (7 connection & 30% malicious node)

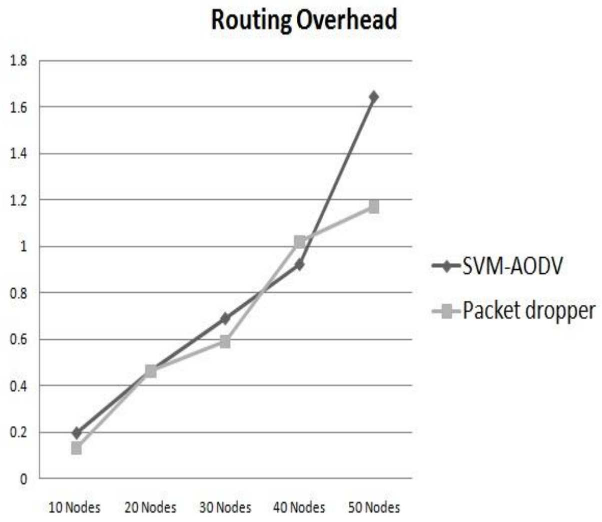

Fig 18: Routing Overhead (9 connection & 30% malicious node)

E. Average Energy Consumption

It measure the average energy that is consumed by mobile nodes during transmission process. In this, the consumption is increased in packet dropping attack with compare to proposed scheme.

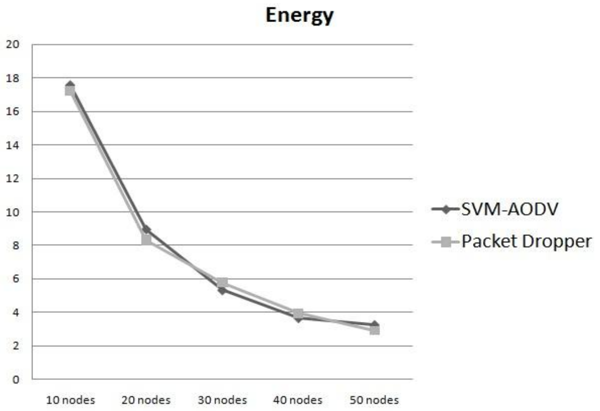

Fig 19: Energy consumption (3 connection & 30% malicious node)

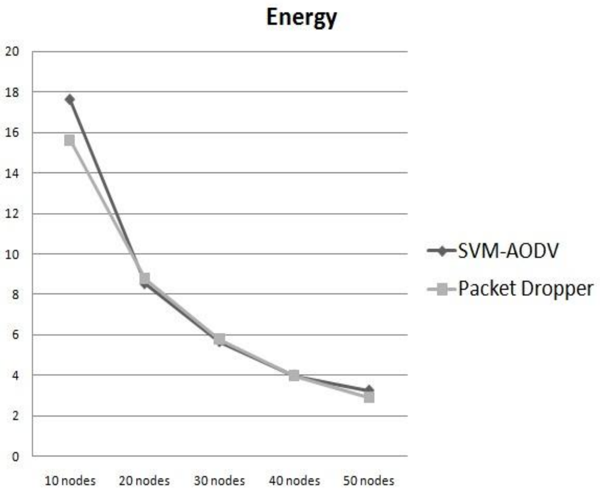

Fig 20: Energy consumption (5 connection & 30% malicious node)

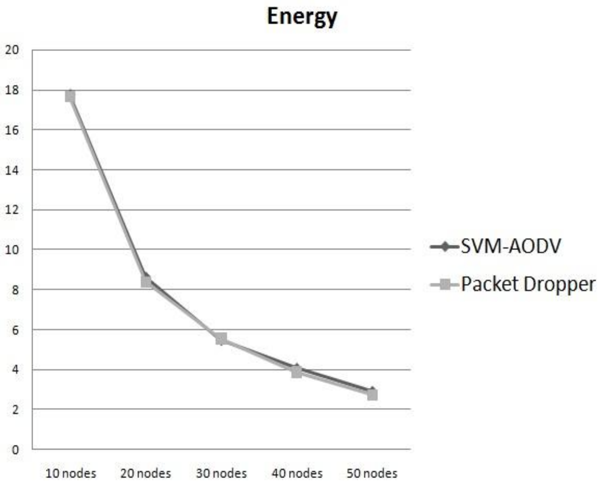

Fig 21: Energy consumption (7 connection & 30% malicious node)

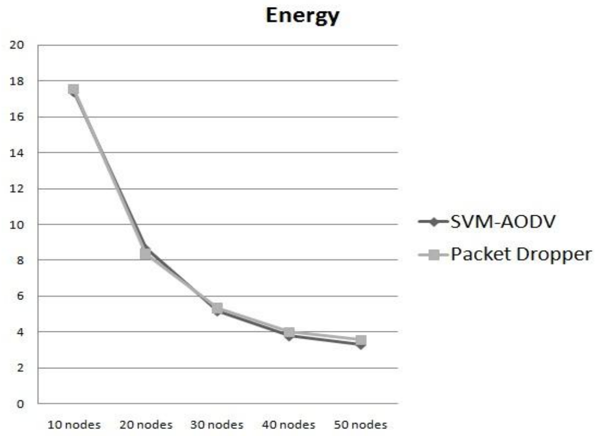

Fig 22: Energy consumption (9 connection & 30% malicious node)

6. CONCLUSION AND FUTURE SCOPE

Our Experimental results compared with the packet dropper attack that is implemented with AODV and SVM-AODV. SVM(Support Vector Machine) is used to mitigate the malicious nodes by classifying the nodes in malicious or non-malicious. SVM is a trust based approach in which train data are used. SVM used kernel function for classification as per behavior of node. We tested out the proposed solution using the NS-2.34 simulator and compared the performance in terms of Packet Delivery Ratio(PDR), End to End Delay(E2ED), Average Throughput and Normalized Routing Overhead. Energy of each node is big concern in wireless network. In future, we can applied different SVM model for more accuracy and decrease mathematical computation. we also have to concentrate on different types of attacks like selfish, worm hole, etc., then compare the SVM with other prevention techniques.

7. REFERENCES

[1] Basangi, S., Conti, M., Giordano, S. and Stojmenovic, I., “Mobile ad hoc networking” , IEEE Press, Wiley-Interscience, pp-282, IEEE, 2004.

[2] Abderrahmane Baadache and Ali Belmehdi, “Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks”, Elsevier Journal of Network and Computer Applications 35, pp-1130–1139. Availavle at SciVerse ScienceDirect, Elsevier, 2012.

[3] Michie, Donald, David J. Spiegelhalter, and Charles C. Taylor., "Machine learning, neural and statistical classification.", 1994.

[4] Li, Wenjia, Anupam Joshi, and Tim Finin., "SMART: An SVM-based Misbehavior Detection and Trust Management Framework for Mobile Ad hoc Networks.", In MIL· ITARY COMMUNICATIONS CONFERENCE, 20Il-MILCOM 20Il, pp- 1102-1107, IEEE,2011.

[5] Patel, Meenakshi, and Sanjay Sharma., "Detection of malicious attack in MANET a behavioral approach.", In Advance Computing Conference (IACC), 2013 IEEE 3rd International, pp-388-393, IEEE, 2013.

[6] Barani, Fatemeh, and Sajjad Gerami, "ManetSVM: Dynamic anomaly detection using one-class support vector machine in MANETs.", In Information Security and Cryptology (ISCISC), 2013 10th International ISC Conference on, pp- 1-6. IEEE, 2013.

[7] Patel, Meenakshi, Sanjay Sharma, and Divya Sharan., "Detection and Prevention of Flooding Attack Using SVM.", In Communication Systems and Network Technologies (CSNT), 2013 International Conference on, pp- 533-537, IEEE, 2013.

[8] Akbani, Rehan, Turgay Korkmaz, and G. V. S. Raju., "A Machine Learning Based Reputation System for Defending Against Malicious Node Behavior.", In Global Telecommunications Conference, 2008, IEEE GLOBECOM 2008, IEEE, pp- 1-5. IEEE, 2008.

[9] Li, Wenjia, Anupam Joshi, and Tim Finin., "Sat: an svm-based automated trust management system for mobile ad-hoc networks.", In MILITARY COMMUNICATIONS CONFERENCE, 2011-MILCOM 2011, pp- 1102-1107, IEEE, 2011.

[10] Akbani, Rehan, Turgay Korkmaz, and G. V. S. Raju., "Defending against malicious nodes using an SVM based reputation system.", In Military Communications Conference, 2008, MILCOM 2008, IEEE, pp- 1-7, IEEE, 2008.

[11] Forster, Anna., "Machine learning techniques applied to wireless ad-hoc networks: Guide and survey.", In Intelligent Sensors, Sensor Networks and Information, 2007,ISSNIP 2007, 3rd International Conference on, pp-365-370, IEEE, 2007.

[12] Kautoo, Priya, Piyush Kumar Shukla, and Sanjay Silakari., "Trust Formulization in Dynamic Source Routing Protocol Using SVM.", International Journal of Information Technology and Computer Science (IJITCS) 6, no- 8,2014

[13] Patel, Nirav J., and Rutvij H. Jhaveri. "Detecting packet dropping nodes using machine learning techniques in Mobile ad-hoc network: A survey." In Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on, pp. 468-472. IEEE, 2015.

[14] Patel, Nirav J., and Rutvij H. Jhaveri. "Trust Based Approaches for Secure Routing in VANET: A Survey." Procedia Computer Science 45 (2015): 592-601.

[15] Bar, Radha Krishna, Jyotsna Kumar Mandal, and Moirangthem Marjit Singh. "QoS of MANet Through Trust based AODV Routing Protocol by Exclusion of Black Hole Attack." Procedia Technology 10 (2013): 530-537.

[16] Basangi, S., Conti, M., Giordano, S. and Stojmenovic, I., “Mobile ad hoc networking” , IEEE Press, Wiley-Interscience, pp-282, IEEE, 2004

[17] Alsheikh, Mohammad Abu, Shaowei Lin, Dusit Niyato, and Hwee-Pink Tan., "Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications.", 2014.

[18] Michie, Donald, David J. Spiegelhalter, and Charles C. Taylor., "Machine learning, neural and statistical classification.", 1994.

[19] Kannhavong, Bounpadith, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, and Abbas Jamalipour., "A survey of routing attacks in mobile ad hoc networks.", Wireless communications, IEEE 14, no. 5, pp-85-91, 2007.