SVM BASED APPROACH FOR INTRUSION DETECTION IN MANET

G. K.Wadhwani*[1],S. K.Khatri**, S K Muttoo***
*Deptt. Of Computer Science, IITM, GGSIPU,New Delhi, India,
**Amity University Tashkent, Tashkent, Uzbekistan,
***Deptt. Of Computer Science, University of Delhi, New Delhi, India.

ABSTRACT
A mobile ad-hoc network (MANET) is a collection of mobile devices having routing capabilities to reach to the destination. Co-operation of all the nodes in the network is essential for efficient performance of the network. But cooperation of all the nodes cannot be assumed in such a dynamic network in which nodes are joining and leaving very frequently and topology changes randomly. Some of the nodes can be compromised that adversely affects the performance of the network. Different types of attacks can be performed at various layers of the protocol suite An Intrusion detection system is required to accurately detect attacks and isolates compromised nodes in the network. In this work black hole attack has been introduced using Ad-hoc On Demand Distance Vector (AODV) as Routing MANET protocol and the system is trained and tested using Support Vector Machine (SVM) to detect the malicious nodes in the network. The simulation was done in NS-2 to carry out black hole attack and trace file obtained is used as dataset for training and testing purpose using R.

KEYWORDS:MANET, SVM, Blackhole Attack, Intrusion Detection System.

MSC: 90B25

RESUMEN
Una red ad-hoc de móviles(MANET) es una colección de aparatosmóviles que tiene capacidades para llegar a su destinación. Co-operación entre todos los nodos en la red es esencial para un desempeño eficiente de esta. Pero la cooperaciónde todos los nodos no puede ser asumida en tal red dinámicacuyos nodos se unen y separan muyfrecuentemente y la topologíacambia aleatoriamente. Algunos nodos pueden verse comprometidos, lo que afecta adversamente el desempeño dela red y la afecta . Diferentestipos de ataques pueden ser desarrollados en varias capas del protocolo. Unsistema de detección de intrusiones es requerido paradetectar con exactitud ataques y aislar los nodos comprometidos de la red. En este trabajo ha sido introducido un ataque de hueco negro usando un ruteo del protocolo MANET: Ad-hoc OnDemandDistance Vector (AODV) y el sistema es entrenado y probado usando “Support Vector Machine” (SVM) para detectar los nodos maliciososen la red. La simulaciónse desarrolló en NS-2 para llevar a cabo el “ ataque hueco negro” y el fichero-traza es obtenido y usando la data con el propósito de entrenar y probar utilizando R.

KEYWORDS:MANET, SVM, Ataque Hueco Negro, Sistema de Deteccion de Intrusion

1. INTRODUCTION

MANET is an infrastructure less network in which devices organize themselves to communicate with each other. These devices are able to recognize the presence of any other device in the close proximity and are responsible for discovering the route through their neighboring nodes if the receiver node is not reachable directly by the sending node (Wang et al. (2017), Kuo et al. (2016), Ejmaa et al. (2016), Mehmood et al. (2018), Taha et al. (2017),Liu et al. (2017)).The nodes move arbitrarily in the network which changes the underlying topology in an unpredictable manner which also changes the routing information available at the nodes during route discovery and data forwarding. This arbitrary movement of nodes causes link breakages in the network which makes it difficult to design a protocol which deals with all such issues. Node energy and reliability are the other issues which have not been addressed efficiently in any MANET routing protocol (Pati et al. (2018)). MANET can be of two types’ single hop and multi-hop. Single hop MANET allows data transmission with directly connected nodes and in multi-hop network a node can forward packets to other intermediary node to reach to the intended destination (Shakshuki et al. (2013)).

[1]gkwadhwani@gmail.com, skmuttoo@cs.du.ac.in, skkhatri@amity.edu,sunilkkhatri@gmail.com

These intermediary nodes are assumed to be trustworthy at all layers to perform data transmission. This assumption of trustworthiness is the most critical issue in the constantly changing environment of MANET due to mobility of nodes (Pathan et al. (2018)). In such an environment it is very easy for any node to eavesdrop the packet transmission and even enter into the network and compromise other nodes in the network. In MANET, User Datagram Protocol (UDP) is used by most of the applications which is unreliable and main reason for errors because of mobility of nodes and radio interference among the nodes at the medium access control layer. Some applications like HTTP and FTP need reliable transmission and it depend on TCP at the transport layer for end to end reliable delivery (Ahmed and Khalifa (2017)).But TCP performance degrades gradually as the mobility of the nodes increases because it does not have any mechanism to detect whether packets are dropped due to network property or due to congestion in the network. This type of network completely relies on such intermediary to transmit data. MANET can be used in military applications, disasters, and medical emergencies due to its minimal requirement for configuration and deployment (Naseer and Chen (2007)). The dynamic topology, reliance on intermediary node, frequently changing routing information make it susceptible to different type of attack which raises the requirement of stringent security measures at all layers of the protocol suite for such network. The first layer of defense is to ensure that no intrusion takes place, but it would be irrational to make such assumption. The second layer of defense is to detect the intrusion and try to recover from it within quick time. SVM based detection mechanism is proposed in this paper to identify black hole attack at the network layer. In this technique all the nodes' packet forwarding behavior is examined through machine learning method to detect this attack and to identify nodes that are carrying this attack. The reason for using machine learning algorithm is to get more accurate results. SVM is used because it scales well with high dimensional data and it can easily works with semi structured or unstructured data also. Black hole attack is very critical and it badly affects Average Throughput, Packet Delivery Ratio, and Residual Energy in the network. Therefore it is very important to identify this attack and isolate those nodes to participate in the route discovery process and packet transmission. This work can be utilized by researchers working on proposing security solutions for wireless ad-hoc communication and it can also be used for industries which are developing critical applications where confidentiality is very high. Intrusion detection system with high accuracy as proposed in this paper can be used in military application but it is very difficult to get real time data for such critical and confidential applications. Section-II presents the work done in this area, section-III gives overview of Black hole attack in MANET, Section-IV presents impact of black hole attack on the performance of AODV, Section-V is about classification of nodes using support vector machine and Section VI concludes the paper with scope for future.

2. RELATED WORK

Zone Sampling based algorithm is based on tracing in which a node writes it zone-id with certain probability prior to forwarding it to the next node. If under attack, the victim traces back the path to reach the attacker node with the help of zone-id provided in the packet (Jin et al. (2006)). This algorithm is not scalable and is not able to classify malicious nodes accurately as the node density increases in the zone.

A secure protocol is designed to deal with jellyfish attack and buffer overflow. In this protocol a compromised node carries out attack by flooding the hello packets which modifies the buffer values at the benign nodes. This technique was applied on On Demand Multicast Routing Protocol (ODMRP) and AODV protocols. Simulation results show that it is able to efficiently deal with jellyfish attack & buffer overflow problem and it improves the packet delivery ratio, throughput in the network (Aburumman et al. (2017)).

Sujatha et al. (2012) have used genetic algorithms for detection of black hole attack in the network. Genetic Algorithm Control method is used to analyze the behavior of every node. Several parameters like no. of request forwarded, request reply rate, no. of data packets received, forwarded and dropped are calculated and passed to the algorithm as an input. The performance of this method deteriorates as the node density increases in the network.

Fuzzy logic based distributed approach is proposed to determine the degree of maliciousness of a given node by examining the attack symptoms. In this approach all the participating nodes are required to remain in promiscuous mode and give the collected information to the fuzzy system. The fuzzy system assigns some fidelity level to each node on the basis of information received by all the nodes. If this value for a given node is less than the predetermined value defined for the network, it is treated as malicious node and isolated from other nodes (Singh (2011)). This approach is computation intensive and consumes lots of energy of every node.

Another distributed method for black hole detection in which some trustworthy base stations are installed along with mobile agents at different locations in the communication system. These mobile agents detect an attack by calculating frequency of packets forwarded and received by a neighboring node. If a malicious activity is detected then all the transmissions are done through base stations only (Kachirski and Guha (2002)). This method cannot deal with existence of more than one black hole node in the network.
Su (2011) has proposed an approach for detecting and separating malicious nodes which carry out black hole attack by configuring intrusion detection system (IDS). This system calculates the suspicious value of a node by determining the ratio of route replies and route request packets generated by a node. If any intermediate node does not transmit a route request for a specific route but generates route reply then the neighboring node will increase its suspicious value by 1 in its table. If this value exceeds beyond a predetermined threshold value, this is intimated to all the nodes to cooperatively separate the node from the network.
A simple approach for black hole attack detection and mitigation is proposed by Liu and Deng (2007) called 2-ACK technique. In this method the next hop link of the receiving node send the acknowledgment of the received packet. In this environment cannot drop packets otherwise it can easily be detected by the next hop node. This technique also solves the problem of receiver collision and limited energy power on a node. This technique can easily be supplemented to the existing routing protocol such as Dynamic Source Routing (DSR) that can significantly reduce the attacks.
A distributed algorithm to detect packet dropping attack by joint participation of all the nodes at the time of network initiation and identification of malicious nodes as these nodes participate in packet receiving, packet forwarding etc. activities of the network. It efficiently uses routing information redundancies to make the detection process secure and robust. This algorithm uses controlled flooding which reduces the transmission overhead on the network. These identified malicious nodes can be isolated from the network easily (Sen et al. (2007)).
The trust value along with trusted list determines how many times a node has participated in the packet transmission and residual energy on a given node is used to determine whether denial of packet forwarding is malicious or non-malicious (Kshirsagar et al. (2018)). Secure communication can be achieved using benign nodes having sufficient energy to carry out data transmission. This method can be supplemented with the existing protocols for MANET.
The algorithm capable of detecting packet forwarding misbehavior that can also work in sparsely dense network and does not require overhearing by all the nodes in the network. It uses statistics obtained from all the nodes as it receives and transmits packets to its neighboring nodes. This mechanism is able to detect attack in the presence of packet losses due to noisy links, mobility and routing protocol misbehavior. In this approach accusation is made on the basis of predefined number of detection to avoid falsely accusing a legitimate node (Gonzalez-Duque (2008)). This scheme does not interfere with the existing routing method for data transmission and can be added for intrusion detection.
An IDS based on watchdog and pathrater is proposed and its performance is evaluated using dynamic source routing (DSR) and AODV in the presence of sinkhole attack. Performance of both the protocols has been measured considering packet transfer capability, throughput and delay (Saifuddin et al. (2018)).
A distributed trust-based security scheme is proposed to deal with multiple attacks such as Vampire, Denial of Service, Probe and User to root (Vaseer et al. (2018)).
A combination of elliptic curve cryptography and modified Advanced Encryption Standard Algorithm is used to deal with different types of attack. System performance is analyzed using Delay, PDR and life cycle (Vegda and Modi (2018)).
All the approaches talks about detecting attacks but none of the approach extensively emphasize the accuracy of intrusion detection. In this paper SVM based approach has been used to maximize the accuracy and make it scalable to be used for any size of network.

3. OVERVIEW OF BLACK HOLE ATTACK

The responsibility of the network is to offer a secure mechanism for forwarding packets so that they reach to the intended destination in an optimal time. In the presence of an untrustworthy node in the network, it will lead to unexpected network operations which can impact the performance of the network. A network shows the following symptoms if it is under attack

- Unnecessary delay in transmitting the packets which in turn affects the throughput of the system
- Unexpected increase in the volume of junk packets in the network which prevents benign nodes to carry their operations

- Circulation of fake routing table information packets which badly impacts the legitimacy of routing information in the network.

Table 1 summarizes various attacks that may happen at different layers of the protocol suite (Wang and Yan (2017), Singh et al. (2017) and Wadhwani et al. (2017)).

Table 1 Various Attack on MANET

Layer	Type of Attack
Application Layer	Data Corruption
Transport Layer	Sync flooding, Session Hijacking
Network Layer	Black hole Attack, Grayhole, Sinkhole, Byzantine Attack, Rushing, Table Poisoning Attack, Replay Attack, Cache Poisoning
Data Link Layer	Denial of service, Traffic Analysis, MAC Targeted Attack
Physical Layer	Eavesdropping, Device Tampering and Jamming

Black hole is a network layer attack in which a malicious node advertises to have the shortest path to reach to the intended receiver (Kaur & Kaur (2014) and Yadav et al. (2012)). The compromised node sends this advertisement to the source node without processing the route request to get on the route to reach the destination. As shown in Fig. 1 source node forwards the route request to all its neighboring nodes N2, N5 and malicious node.N2 and N5 will process the request and forwards it to their neighboring nodes whereas malicious node will simply advertise to have a route to the destination node and becomes the part of the route. Once it becomes the part of the route it can stop forwarding packets for this destination or it can insert false route information to create routing loops in the network.

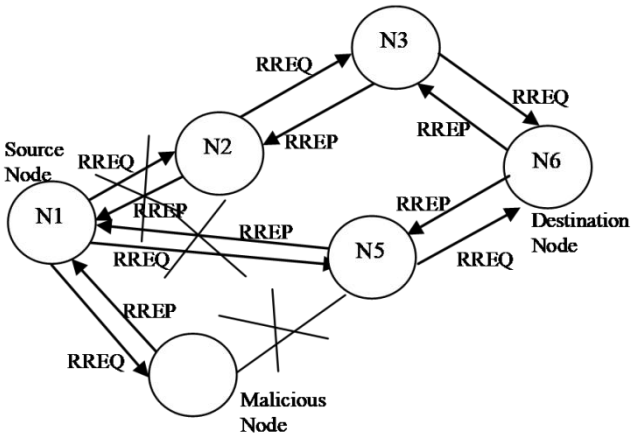

Fig. 1 Black hole Attack

A variation of black hole attack is cooperative black hole attack in which more than one malicious node collude with each other to avoid detection of its presence by getting the acknowledgment from the next hop (Wahane and Lonare (2013)) as shown in fig.2

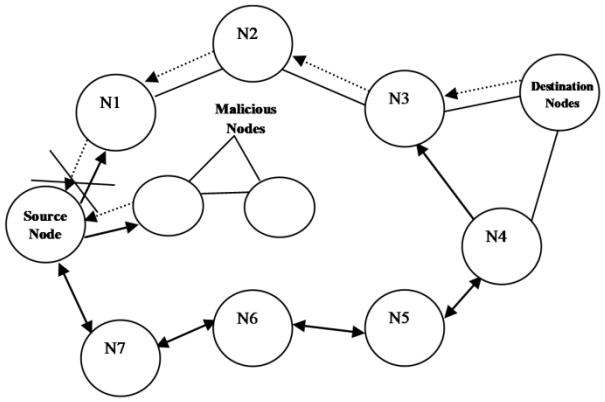

Fig. 2 Co-operative Black hole Attack

Black hole attack significantly deteriorates performance, reliability and security of the network.

4. IMPACT OF BLACK HOLE ATTACK ON THE PERFORMANCE OF AODV

Three critical parameters were considered to show how black hole attack is negatively affecting the overall performance of MANET. AODV is used as routing protocol in MANET to compare its performance under normal system environment and with black hole attack on the basis of following parameters:

a) *Average Throughput*: It is the total number of bytes transmitted per unit time and is generally represented in bits per second. Average throughput can be calculated as follows
Average Throughput (bits per second) = (Total No. of Packets delivered * Packet Size *8)/End Time-Start Time

b) Packet Delivery Ratio: It is the fraction of numbers of packets delivered to the destination, sent by the source can be calculated as
Packet delivery ratio= Number of packets received/ Number of packets sent

c) Residual Energy: Nodes performs various network operations and they losses its energy to carry out these task. Residual energy is the remaining energy on all the nodes in the network at the end of the simulation.

Ns2.35 is used to compare the performance and the simulation environment is shown in Table 2.The simulation results are shown in Fig. 3 (a), (b) & (c) with respect to Average throughput, Packet Delivery Ratio and Residual Energy respectively.

Table 2 Simulation Environment

Parameter	**Value**
Simulator	Ns-2.35
Simulation Time	100 Sec
Area	1000*1000 m
Node Energy	70 Jules
No. Of Nodes	50
No. Of Malicious Nodes	3,5,7,9
MAC Specification	802.11
Packet Size	1000
Routing Protocol	AODV

As shown in Fig. 3(a) & b as the number of malicious nodes are increasing in the network the average throughout and packet delivery ratio plunging significantly.

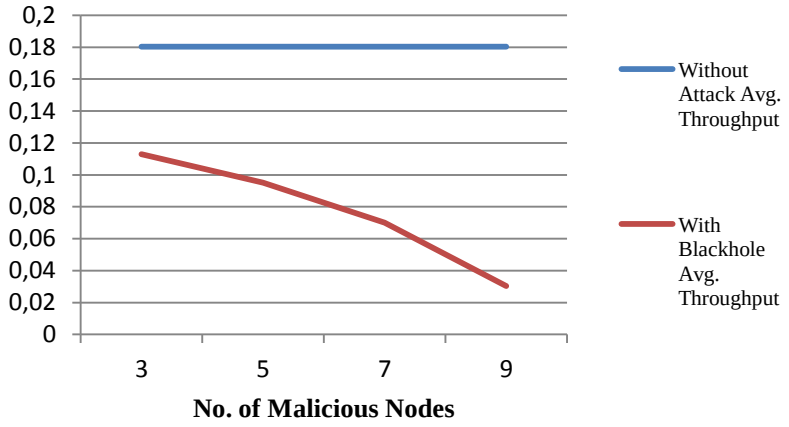

Fig. 3(a) Average Throughput

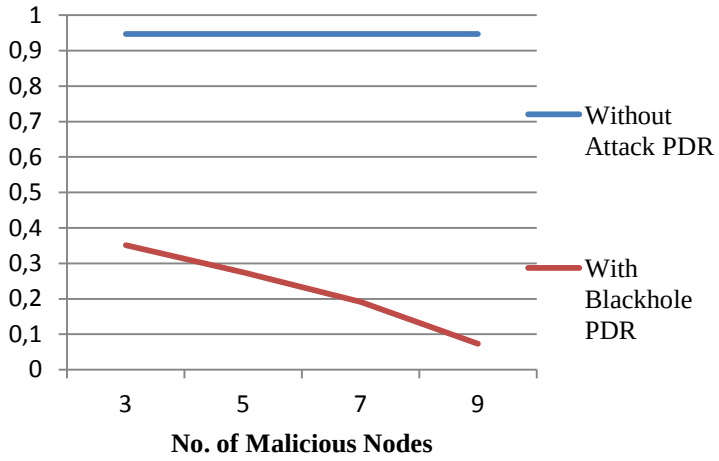

Fig. 3(b) Packet Delivery Ratio

The residual energy of the whole network increases with increase in number of malicious nodes because these malicious nodes are sending reply without processing the request and later on once these nodes are part of the forwarding process, they are either dropping the packets or changing the routing information in the packet while forwarding the packets to the neighboring nodes. Therefore the amount of energy spent by these nodes gets minimize. In addition less number of packets is received by the benign nodes because malicious nodes are not forwarding it to them. Therefore less amount of energy is spent by both malicious and benign node which is clearly gets reflected in the simulation result.

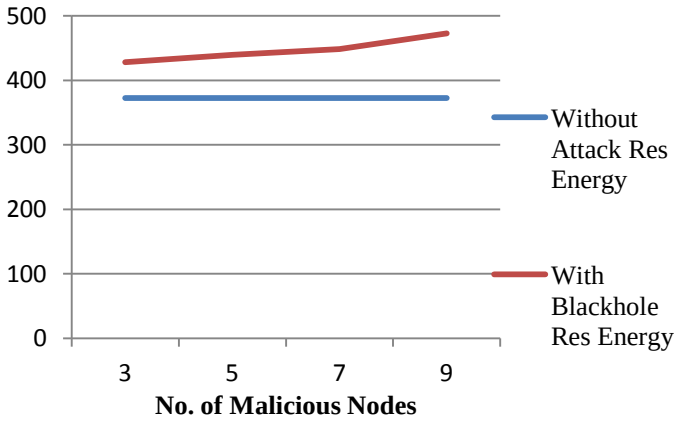

Fig. 3(c) Residual Energy

5. NODE CLASSIFICATION USING SUPPORT VECTOR MACHINE

SVM is binary classifier and in the proposed method it is used to identify black hole attack in the network. It is a supervised learning technique and can be used on any type of dataset to classify nodes as malicious or normal. In SVM based intrusion detection system, nodes cannot change their behavior and if they change it can easily be detected & isolated by the IDS to participate in the routing process. The first step in SVM is to convert the input variables or features of the dataset to multidimensional feature space (Burges (1999)). This is done with the help of pre decided nonlinear function. After mapping to new feature space SVM builds a linear decision function to classify activities as normal and malicious. It is different from linear machine in which decision function get trained for this classification. In SVM it looks for a decision function which tries to maximize the margin between the two boundaries. Margin can be defined as the void space around the decision function in the feature space so that the events can be best classified. The margin width can be

represented as 2/ ||w||.SVM uses Lagrange Multiplier (Nello and John (2000)) to maximize the width by minimizing the value of ||w||.
The decision function build is a nonlinear function which separates the activities in the input unmapped space. This is because of the mapping from input space to high dimensional feature space. The data points which lie within the margin area are called support vector and these vector defines the boundaries of the classification done by SVM. The major advantage of SVM is its nonlinearity and it is proved that nonlinear classification model gives better accuracy as compared to linear classification (Duda et al. (2000)).The mathematical model of SVM is presented below
The training dataset (D) has x_i (data points) and y_i (class of x_i). Classification function can be stated as

$$f(x) = \text{sign}\,(w^T x^i + b) \quad (1)$$

where w is normal on hyperplane and b is length of intercept
Function Margin can be calculated as

$$y^i(w^T x^i + b) \quad (2)$$

For reducing errors, the following equation is used:

$$(w) = \frac{1}{2}\|w\|^2 \quad (3)$$

The margin width between two classes can be calculated as

$$\frac{1}{2}\|w\| \quad (4)$$

Algorithm 1 demonstrates the SVM algorithm to solve the above problem.

Algorithm 1 SVM algorithm
Initialize Vector v and b to 0
Dataset $D = (x_1, y_1), \ldots, (x_n, y_n)$
Where *x*, *y* are labeled samples
Train SVM to learn decision function
For each sample of D do
Classify x_i using decision function $f(x_i)$
If (function margin < 1) then
Calculate w', b' for given data
Add sample example to known data
Use Eq. (3) for reducing errors
Use Eq. (1) to predict.
If (prediction is correct) then
Do it Again
Else
Train SVM Again
Endif
Endif
Classify x_i as benign or malicious

The SVM framework is shown in Fig. 4.

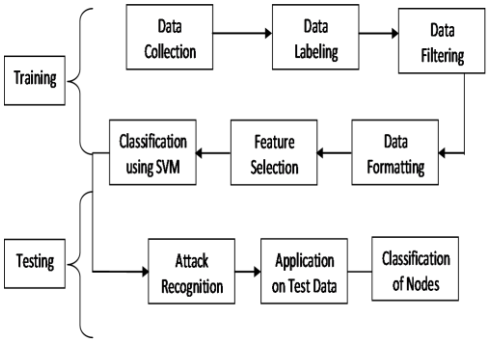

Fig. 4 SVM Framework

To design the mechanism, following steps are taken

- Data Collection
- SVM Modeling
- Result Analysis

Data Collection Black hole attack is carried out using Ns-2.35 and the trace file was generated to get the data. The trace data was then formatted and the data was captured to train and test SVM.
SVM Modeling Data is filtered using linear discriminant analysis and data labeling is done using R Package. Preprocessing is done using Linear Discriminant analysis to minimize the resource use and complexity of the system. The incorporation of distributed parallelism will certainly manage the complexity but its implementation will add an additional overhead on the system which will compromise the objective of proposing a light weight solution. The whole dataset is divided into two parts, 70% of data is used for training purpose and remaining is used for testing. Once the machine gets trained and attack recognition pattern has been learnt, then the testing data was passed to it to check whether it is able to recognize the attack and able to classify the nodes as malicious and normal node.
Result Analysis Following is the reflection table to calculate the accuracy of the algorithm. As shown in Table2, this classification is giving 100% accurate results.

Table 2 Predicted Values

	Malicious	Normal
Malicious	296	0
Normal	0	9231

6. CONCLUSION

In MANET cooperation is required from intermediary nodes for data transmission from source to destination. But the presence of malicious nodes cannot be ignored and these nodes can carry different types of attack at various layers of protocol suite. These attacks can significantly deteriorate the performance of the entire system. The objective of this paper is to classify nodes accurately and isolate the compromised nodes in the network. In this paper the effect of Black hole attack on Packet Delivery ratio, Average Throughput and Residual energy is shown. These results clearly demonstrate that such an attack can considerably dampen the performance of the system. Therefore it is very important to identify malicious nodes in the network accurately and these nodes should be isolated from the process of route discovery and data forwarding. In this paper for classification of nodes a machine learning method SVM is used which is giving 100% accurate results when applied to the simulated data produced while carrying out the black hole attack in the network. Though SVM requires more system resources but after data filtering it can produce the result in quick time. Once the machine is trained on the datasets having records of all types of nodes in the network, it can accurately predict malicious nodes in the network later on. Grid search can be used to get the optimal number of parameters to be used for a given model which can further increase the efficiency of the system. This can be taken up as future work.

RECEIVED: MAY, 2019
REVISED: DECEMBER, 2019

REFERENCES

[1] ABURUMMAN, A., SEO, W.J., ESPOSITO, C., CASTIGLIONE, A., ISLAM, R. and CHOO, K.K.R. (2017): A secure and resilient cross-domain SIP solution for MANETs using dynamic clustering and joint spatial and temporal redundancy. **Concurrency Comput., Pract. Exper. ,** 29(23), e3978.
[2] AHMED, D. and KHALIFA, O.(2017) : An overview of MANETs: Applications, characteristics, challenges and recent issues. **Int. J. Eng. Adv. Technol.,** 6(4),128.
[3] BURGES, C.J.C.(1998) : A Tutorial on Support Vector Machines for Pattern Recognition. **Data Mining and Knowledge Discovery**,*2*, 121-167.
[4] DUDA, R.O., HART, P.E. and STORK, D.G.(2000) : **Pattern Classification**. Wiley Inter-Science Publication,New York.
[5] EJMAA, A.M.E,SUBRAMANIAM, S., ZUKARNAIN, Z.A., and HANAPI, Z.M.(2016) : Neighbor-based dynamic connectivity factor routing protocol for mobile ad hoc network. **IEEE Access**, 4, 8053-8064.

[6] GONZALEZ-DUQUE, O.P., ANSA, G., HOWARTH, M. and PAVLOU, G.(2008) : Detection and Accusation of Packet Forwarding Misbehaviour in Mobile Ad hoc Network. **Journal of Internet Engineering**,2(8),181-192.
[7] JIN, X., ZHANG, Y., PAN, Y.and ZHOU, Y.(2006) : ZSBT: A novel algorithm for tracing DoS attackers in MANETs. **EURASIP Journal on Wireless Communications and Networking**, 1(2),1–9.
[8] KACHIRSKI, O. and GUHA, R.(2002) : Intrusion Detection using Mobile Agents in Wireless Ad Hoc Networks.**Knowledge Media Network,Proceeding IEEE Workshop,Kyoto,** 153-158.
[9] KAUR, R. and KAUR, A.(2014) : Blackhole Detection In Manets Using Artificial Neural Network. **International Journal For Technological Research In Engineering**, 1, 959-962.
[10] KSHIRSAGAR, V. H., KANTHE, A. M. and SIMUNIC, D.(2018) : Trust based detection and elimination of packet drop attack in the mobile ad-hoc networks. **Wireless Personal Communications,** 100,311–320.
[11] KUO, W.K. AND CHU, S.H. (2016): Energy efficiency optimization for mobile ad-hoc networks. **IEEE Access**, 4, 928-940.
[12] LIU, K. and DENG, J.(2007) : An Acknowledgment Based Approach for the Detection of Routing Misbehavior in MANETS.**IEEETransaction in Mobile Computing**,6(5), 536-550.
[13] LIU, Y., FIELDSEND, J.E. and MIN, G.(2017) : A framework of fog computing: Architecture, challenges, and optimization. **IEEE Access**, 5,25445-25454.
[14] MEHMOOD, A., KHANAN, A., MOHAMED, A.H.H., MAHFOOZ, S., SONG, H.,and ABDULLAH, S.(2018) : ANTSC: An intelligent Naïve Bayesian probabilistic estimation practice for traffic flow to form stable clustering in VANET. **IEEE Access**, 6,4452-4461.
[15] NASSER, N. and CHEN, Y.(2007) : Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network. In **Proc. IEEE Int.Conf. Commun., Glasgow, Scotland**,1154-1159.
[16] NELLO, C. and JOHN, S.T. (2000): **An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods.** Cambridge Univ. Press, Cambridge.
[17] PATHAN, M.S., ZHU, N., HE, J., ZARDARI, Z.A., MEMON, M.Q. and HUSSAIN, M.I. (2018): An efficient trust-based scheme for secure and quality of service routing in MANETs. **Future Internet**,10(2), 16.
[18] PATI, B., PATTANAYAK, B.K. and SWAIN, J.(2018) : A systematic study and analysis of security issues in mobile ad-hoc networks. **Int. J. Inf. Secur. Privacy**, 12(2),38-45.
[19] SAIFUDDIN,K.M, ALI,A.J.B, AHMED,A.S, ALAM,S.K.S,AHMAD,A.S.(2018) : Watchdog and Pathrater based Intrusion Detection System for MANET. **4th International conference on Electrical Engineering and Information & Communication Technology**,**Mirpur.**
[20] SEN, J., CHANDRA, M.G., BALAMURALIDHAR, P., HARIHARA, S.G. and REDDY, H.(2007) : A Distributed Protocol for Detection of packet Dropping Attack in Mobile Ad Hoc Network. **2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications**,**Penang**.
[21] SHAKSHUKI, E., KANG, N. and SHELTAMI, T.(2013) : EAACK-A Secure Intrusion Detection System for MANETs. **IEEE Trans. Ind. Electron.,** 60(3),1089-1098.
[22] SINGH, J.(2011) : Fuzzy logic based intrusion detection system against blackhole attack on aodv in manet, **Computing**,28-35.
[23] SINGH, T.,SINGH, J. and SHARMA, S.(2017) : Energy efficient secured routing protocol for MANETs. **Wireless Network.**, 23, 1001-1009.
[24] SU, M.Y.(2011) : Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems.**Computer Communication**, 34(1),107-117.
[25] SUJATHA, K. S., DHARMAR, V. and BHUVANESWARAN, R. S.(2012) : Design of Genetic Algorithm Based IDS for MANET. **IEEE International Conference on Recent Trends in Information Technology (ICRTIT)**,**Chennai,**28-33.
[26] TAHA, A., ALSAQOUR, R., UDDIN, M., ABDELHAQ, M., and SABA, T.(2017) : Energy efficient multipath routing protocol for mobile ad-hoc network using the fitness function. **IEEE Access**, 5,10369-10381.
[27] VASEER, G, Ghai, G.,Ghai, D.(2018) : Distributed Trust-Based Multiple Attack Prevention for Secure MANETs. **2018 IEEE International Symposium on Smart Electronic System (iSES),Hyderabad,India.**
[28] VEGDA,H. and MODI,N.(2018) : Secure and Efficient Approach to Prevent Ad-hoc Network Attacks using Intrusion Detection System. **Proceedings of the Second International Conference on Intelligent Computing and Control Systems,Madurai.**

[29] WADHWANI,G.K., KHATRI,S.K. and MUTTOO,S.K.(2017) : Trust Modeling for Secure Route Discovery in mobile ad-hoc networks.**In International Conference on Reliability,Infocom Technologies and Optimization(ICRITO), Noida,** 391-395.
[30] WAHANE, G. and LONARE, S.(2013) : Technique for Detection of Cooperative Black Hole Attack in MANET. **2013 Fourth International Conference on Computing,Communication and Networking Technologies(ICCCNT), Tiruchengode,** 357-362.
[31] WANG, M. and YAN, Z.(2017) : A survey on security in D2D communications. **Mobile Network Appl.**, 22, 195-208.
[32] WANG, Y., CHEN, I.R., CHO, J.H., SWAMI, A., and CHAN, K. S.(2017) : Trust-based service composition and binding with multiple objective optimization in service oriented mobile ad hoc networks. **IEEE Trans. Services Comput.**, 10(4), 660-672.
[33] YADAV, P., KUMAR, N. and GILL, R.K.(2012) : A Fuzzy Based Approach to Detect Black Hole Attack. **International Journal of Soft Computing And Engineering**, 2,2231-2306.