An Optimized Algorithm For Blackhole Attack Detection inMANET

Girijesh Tiwari[1], Dr. Taruna Jain[2], Prof. Mayank Namdev[3]

[1]*PG Scholar*, [2]*Head (MS-CLIS)*, [3]*Assistant Professor(Dept. of IT)*

UIT, BU, Bhopal

Abstract- The improving reputation and custom of wireless expertise is creating a call for more safe and sound wireless networks. In MANET, data communication is performed within an un-trusted wireless background.A many types of attack have been recognized and comparable solutions have been considered. In wormhole attack, an aggressor record package at one site into the network, sequence them to another site and retransmits them there into the set of connections. Existing works on wormhole attacks have listening carefully only on recognition and used particular hardware such as directional antennas or tremendously precise clocks.More fresh task has dissimilarity of jump distance at station,generate information with two areas handing out bit, count to arrive at next hop and AODV for path establishment, public key encryption technique are also used.In this paper, explain a normal system, without use of hardware, site information and time harmonization called detection packet for detecting infected system in network. Detection Packet has three areas: dispensation bit, count to reach next hop and time stamp. Timestamp is used for powerfully finding with conformance at wormhole harass. Here finding packet can easily be included in the wide variety of ad hoc routing strategy with only considerable alter in the previous protocol to protect against wormhole attack.Here DSR technique is use for path establishment and NS2 for simulations.

Keywords: Mobile Ad-Hoc Network, Blackhole Attack, Tunnel, Performance Analysis, Routing Protocol, MANET Security.

I. INTRODUCTION

The scale development of the computer technology and information sector raise the need of digitalization of transfer of information, it becomes a very important key in the direction of development of data processing sector. Modern techniques of scientific management and advanced information approach can be used for the intelligent transportation information management. However at present the data transportation industries have made some approach in this area. The security of data in information system is an integral part whose main tasks are to maintaineffective safety protections on thatsystem development plan, and establish security system from perspective of network security and also for the application security.

Since network security is important for the information system and forestablishing the effective operation ofnetwork defense system for network become integral part and effective intrusion detection technology is accurate for this measures. Numbers of techniques like advanced machine learning algorithm including genetic evolution algorithm or adaptive algorithms and intelligence algorithm and also learning algorithms aregenerally used in the field of security. Between them support vector machine technique is one of the most promising technique in mining for small sample data.

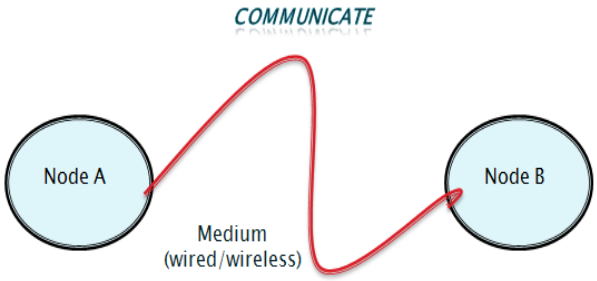

Fig 1 Basic Function of Network

However, detection accuracy of this approach is largely affected by its structural parameters. One thing is that thedata or information has too large dimensions and only some of thecharacteristics are useless and for the other features the SVM structure is always not optimized whichcauses an inefficient detection performance. Although PCA is employed to dodimension reduction butthey did not consider the optimization of FSVM parameters. PCA is accurate forlinear method and does not competent with the nonlinear scenarios. Therefore the accuracy of detection mechanism for the information security of system could be improved when the feature reduction is integrated withparameter optimization. Solution of the above discussed problems and for the protection information security system here proposed new intrusion detection method which is based on GA for optimization and FSVM for classification.

II. LITRAURE SURVEY

In wireless network nodes are not connected by any of the physical links. For route finding routing is a necessary factor in wireless network between nodes. In wireless sensor networks AODV is one of the most widely known routing protocols for route formation. AODV is a protocol which is stateless and use to establish and maintain a single route between the source and the destination [1]. If the path obtained is disrupted by any event then another alternate path is to be found. An alternative approach as of AODV is multi path AODV that proposes to establish multiple routes between any source and destination node in a single route discovery.

Michael Beham present work-in-progress that studies the feasibility of combining virtualization-based intrusion detection and virtualization-based honey pots with nested virtualization. They have perform research have exposed that in practice such a combination is not simple and straightforward to set up with obtainable components. They have illustrated the results of research that evaluate the performance of existing nested virtualization approaches.

Sriparna Saha shows the development of IDS with the use ofmachine learning technique. Then intrusion detection was tested on KDD CUP dataset and was establish to be accurate than any other obtainable IDS using machine learning.

Jun Wang shows a inclusive optimal search presentation of Artificial Bee Colony (ABC) is used to optimize the SVM parameters and also the feature selection for IDS from the KDD Cup 99 data sets. The technique is extremely simple to implement and discover the true global minimum of a multi-modal search space regardless of the initial parameter values or rapid convergence than being easy and flexible and using extremely few control parameters to adjust.

Mrutyunjaya Panda shows the purpose of their work is to address some of the issues in nearly all usually used KDDCup 1999 dataset. The NSL-KDD dataset have used as a benchmark dataset for this experimentation is modified KDDCup 1999. The work that combines DMNB classifier with PCA as a filtering approach produce improved classification accuracy with other existing approach.

Machine learning approach is becoming more usable technique in many problem domains. Similarly, Zhang in his work on IDS consist of global system. However, instead of using single global IDS the architecture uses number of local IDSsin hierarchal manner. This type of architecture increases the reliability of global IDS.

The research has been divided on two different perspectives for solving the intrusion detection problem.

• Conversion of the problem into the classification problem by modeling normal traffic as well as attack traffic and for classification of the initialstate of the network as their nature by detecting attacks.

• Cryptographic solutions which discourage attempts of attack. Numerous approaches have been proposed for the security of system. This includes statistical approaches which suggest a Chi-Square-Test. Multivariate correlation analysis effects is detected on the distributed DoSdetection and presented by example related to SYN flooding. The matrix of co variance is used for presentation of the relationship among every pair of network feature and to identify attacks.

III. PROBLEM DEFINITIONS

Internet is continuously expanding and with its high-speed development there is a need for network security as it is becoming very essential in day to day life. Cyber attack detection process has been defined as the problem of identifying individuals who have legitimate access to the system but are abusing their privileges like insider threat added to this the identification of attempts to use a computer system without authorization or to abuse existing privileges. The deployment of sophisticated firewalls and authentication systems is no longer enough for building a secure information system. An important component for any of the strong security solution is represented by intrusion detection systems, able to deal with the violations from external network, and more importantly, to resist the attacks of internal network.

Recent year's research on intrusion detection is gradually inclined to artificial intelligence technology to improve the detection accuracy. It is generally considered that intrusions illustrate that something which differs from normal pattern of operation and that any unknown intrusion will present patterns more similar to known intrusion than to normal data. Additionally by gathering network traffic and using the right classification algorithm the system should be able to detect known intrusion as well as also the new intrusions. The solution of above discussed problems and for protection the data a new intrusion detection technique based on optimization of GA & classification of fuzzy svm is proposed. The analysis suggests that this technique could detect the network attack efficiently.

IV. OBJECTIVE

• To improve IDS using multi objective optimization GA base FSVM.

• Improve rate of error finding in IDS. However, fuzzy support vector machine parameters could be used in place of the other objective functions.

• Propose the approach to improve the performance of IDS in two aspects. Feature subset selection and parameter of FSVM optimization.

V. THE PROPOSED MODEL BASED ON SVM FOR IDS

Above methods requires a large number or a complete samples set to achieve the desired performance and need a longer training time. The support vector machine is an effective tool to solve the problem with small samples set, and it's been widely applied to various fields of pattern recognition. In the literature, SVM was used in intrusion detection system, and made a very good experiment results. Intrusion detection system which is based on SVMgenerally compose of three parts data-preprocessor, trainer and decision-making system.

As shown in Fig 2 the pre-data processor mainly extracts the network data from the large network data stream, and converts the data format. Support vector machines only identify the data of digital type and the data must be the same dimension, therefore, it must extract effective information of network connection and at the same time transform the original network data into the digital vectors. Trainer trains SVM with the data that was preprocessed with above method and stores the training results to support vector library. Decision-making system classifies the network connection behavior according to information of support vector database, and then makes the appropriate decision.

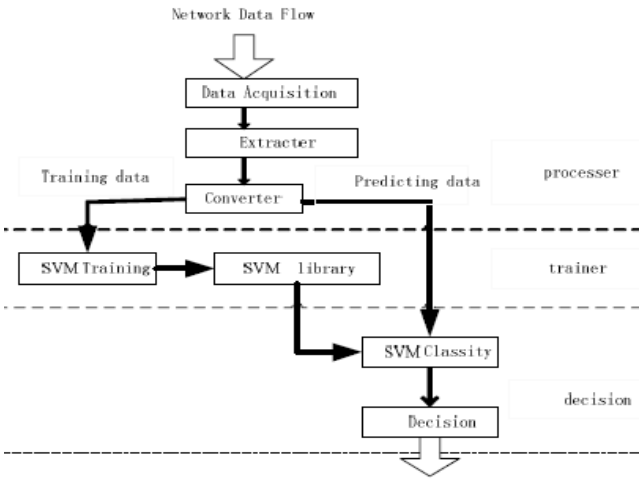

Fig 2. SVM Decision Training

The whole system can be divided into two processes: training and predicting. In the training stage, the support vector machine uses the samples of known types and according to train. We can obtain support vectors parameters and the others parameters. Predicting stage is a process that use support vector machines to classify the network data by this method. The discriminate function can get the sort of networks behavior, and then submit the results to the decision making system can make the appropriate decision.

The work here proposed methods for improving the performance of IDS in two aspects first is feature subset selection and other is parameter of SVM optimization.

a. Optimizing the feature subset
b. Optimizing the parameters of SVM

The proposed algorithm is as follows

START:

STEP 1: for each node

STEP 2: build the relationship between the mobile nodes in the MANET

STEP 3: calculate the trust value of each neighboring node.

STEP 4: for each neighboring nodes &&calculate neighbor_node_trust from svm classifier

STEP 5: if (neighbor_node_trust== NULL)

STEP 6: collect nodes information as raw feature subset

STEP 7: process raw feature subset using svm based classifier

STEP 8: create svm trust value

STEP 9: else

STEP 10: go to step 11

STEP 11: if (node_trust)

STEP 12: select next_hop

STEP 13: else

STEP 14: go to step 4

STEP 15: for each nodes trust value

STEP 16: if (max_trust)

STEP 17: select nodes as nearest node in routes based on the trust.

STEP 18: else

STEP 19: go to step 1

END

The shortage in Support Vector machines is solved by proposes new memory Genetic Algorithm optimization technique. In this algorithm SVM used since the modeling of the classification and Genetic Algorithms are adopted in solving the problems of a hyper plane optimization. The choice of penalty factor c parameter for SVM and Kernel function parameter made influence on the classification accuracy and generalization ability for support vector machine. But there is now no effective way to rationally choose the parameters for SVM and the general way is to solve the problems through adopting method or cross-

validation trial calculation which may lead the problems of partial optimization and that may seriously affect the practical application of Support Vector Machines. The procedures taken by SVM based on Genetic Algorithm parameter optimization is shown as follows:

(1) System initialization, including SVM parameters and the initial antibody groups,

(2) The target parameter optimization for SVM functions as an Antigen,

(3) To calculate each Antigen and antibody for their avidity by using the target function.

(4) For making log of appearance of the cells and record the excellent antibody in the process of evolution. Given the optimal parameters are obtained then the evolution process ends and optimal parameters output. Then skip to procedure 5.

(5) To calculate each antibody of its concentration and survival rate, and to appropriately supply antibody selection and its immune system.

(6) The new group updates. New groups can be generated by way of selecting, recovering and mutating, and then remove the rookie individual from the memory base to constitute a new generation, and then repeat from step 3.

VI RESULTS AND ANALYSIS

Table 1 Detection Accuracy Result

Protocol	Normal Nodes	Attack Nodes (20%)	Packet Drop Rate(in mbps)
MOIP	50	10	38.5405
	60	12	45.8007
	80	16	74.042
	100	20	4.5942

In the above table the protocol used is MOIP which uses SVM & GA in this current scenario the attacking nodes is 20% of the normal node in network environment. The output obtained is the amount of data dropped during transmission.

Table 2 Scenario result AODV

Protocol	Normal Node	Attack Nodes (20%)	Packet Drop Rate(in mbps)
AODV	50	10	4.8613
	60	12	4.5246
	80	16	26.1783
	100	20	0.1293

In the above table the protocol used is AODV which uses queue based process in this current scenario the attacking nodes is 20% of the normal node in network environment. The output obtained is the amount of data dropped during transmission.

Table 3 Scenario result DSDV

Protocol	Normal Nodes	Attack Nodes (20%)	Packet Drop Rate(in mbps)
DSDV	50	10	4.9237
	60	12	7.9006
	80	16	11.9472
	100	20	0.118

In the above table the protocol used is DSDV which uses queue based process in this current scenario the attacking nodes is 20% of the normal node in network environment. The output obtained is the amount of data dropped during transmission.

Table 4 Scenario result MOIP

Protocol	Normal Nodes	Attack Nodes (20%)	Packet Drop Rate(in mbps)
MOIP	50	10	38.5405
	60	12	45.8007
	80	16	74.042
	100	20	4.5942

In the above table the protocol used is MOIP which uses SVM & GA in this current scenario the attacking nodes is 20% of the normal node in network environment. The output obtained is the amount of data dropped during transmission.

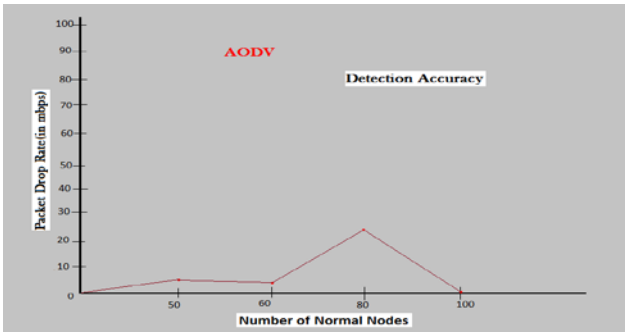

Fig 3. AODV Observation Chart

In the above chart the protocol used is AODV which uses queue based process in this current scenario the attacking nodes is 20% of the normal node in network environment. The output obtained is the amount of data dropped during transmission. In this chart it is observed that when the numbers of normal nodes are exposed to 20% of the attacking nodes then the observed output packet drop ratio is used to specify the detection accuracy of the AODV protocol on that current scenario. In the current environment different scenarios is considered by varying the number of normal nodes in the network so that more accurate results can be obtained.

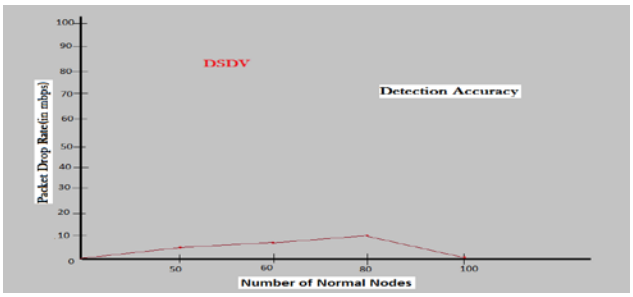

Fig 4. DSDV Observation Chart

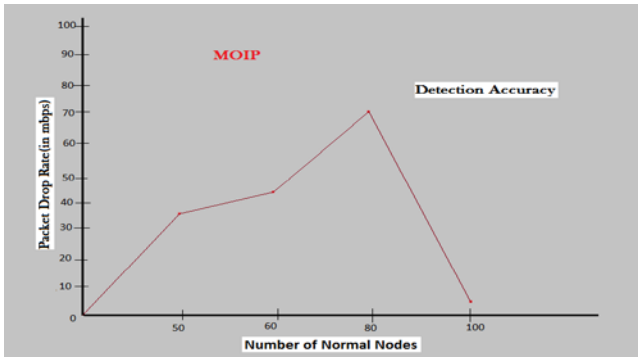

Fig 5 MOIP Observation Chart

In the above chart the protocol used is DSDV which uses queue based process in this current scenario the attacking nodes is 20% of the normal node in network environment. The output obtained is the amount of data dropped during transmission. In this chart it is observed that when the numbers of normal nodes are exposed to 20% of the attacking nodes then the observed output packet drop ratio is used to specify the detection accuracy of the DSDV protocol on that current scenario. In the current environment different scenarios is considered by varying the number of normal nodes in the network so that more accurate results can be obtained.

In the above chart the protocol used is MOIP which uses SVM & GA in this current scenario the attacking nodes is 20% of the normal node in network environment. The output obtained is the amount of data dropped during transmission. In this chart it is observed that when the numbers of normal nodes are exposed to 20% of the attacking nodes then the observed output packet drop ratio is used to specify the detection accuracy of the MOIP protocol on that current scenario. In the current environment different scenarios is considered by varying the number of normal nodes in the network so that more accurate results can be obtained.

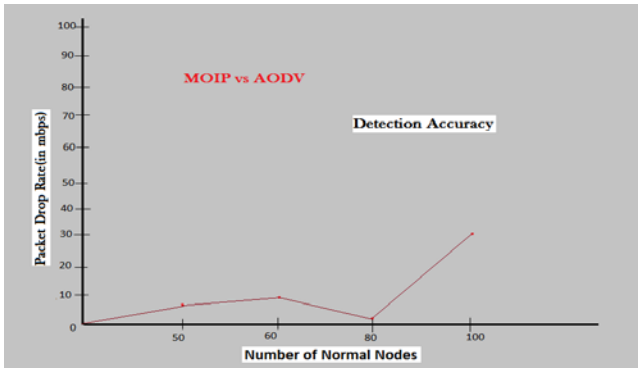

Fig 6. AODV vs MOIP Observation Chart

In the above chart the protocol used is AODV which uses queue based process & MOIP uses SVM & GA are simulate in this current scenario the attacking nodes is 20% of the normal node in network environment. The output obtained is the amount of data dropped during transmission & it is a comparative result.In this chart it is observed that when the numbers of normal nodes are exposed to 20% of the attacking nodes then the observed output packet drop ratio is used to specify the detection accuracy of the AODV protocol on that current scenario. In the current environment different scenarios is considered by varying the number of normal nodes in the network so that more accurate results can be obtained.

VII CONCLUSION

Mobile Ad-Hoc network is becoming more challenging day by day and facing new type of vulnerabilities compared to wire network technology. Widely popularization of

MANET also makes it to more attract towards the sophisticated attack, Since it can be deployed anywhere and does not need any pre infrastructure also dynamic topology and no centralized control and mainly open to all devices so it is highly vulnerable to attacks. Now it is required to make it more advance and secure from unknown threats. In proposed work use of Support vector machine classification to detect such type of attack. In order to solve the problems raised and protect the information need to propose a new intrusion detection technique base on multi objective optimization GA base fuzzy svm(fuzzy support vector machine) propose. The observed results in AODV and DSDV protocols the intrusion detection is performed on the basis of some predefined constraints so it need to cross that limit in order to gain some efficient output. So for this problem here use SVM. It is also not the 100% efficient techniques because it can take all the constraints to produce output values. Here also solved this limitation for SVM parameters optimization by using genetic algorithm which gives optimal solution. So here say that our protocol MOIP is the machine learning protocol which gives optimal solutions.

VIIIFUTURE WORK

The next step forward for the research would be reutilizing and standardizing the implementation, which is the preparation of the product development.In suggested work try to use support vector machine as a machine learning technique which is a self learning technique so that efficient detection of intrusion is done.But due to its nature SVM uses all the parameters for subset selection. So, use genetic algorithm so that only optimized parameters can be selected.By using such technique here make new protocol to efficiently detect intrusion. In future it can be extended to prevent intrusion and also to take some action against intrusion.

IX REFERENCES

[1] ff Macro Conti, Silvia Giordano and Ivan Stojmenovi “Mobile Ad Hoc Networks”, Stefano Basagni, IEEE press, A john Wily & Sons, INC. publication, 2003

[2] A.K. Rai, R. R. Tewari and S. K. Upadhyay, “Different Types of Attacks on Integrated MANET-Internet Communication,” International Journal of Computer Science and Security, Vol. 4, No. 3, pp. 265-274, 2010.

[3] Sunil Taneja and Ashwani Kush “A Survey of Routing Protocols in Mobile Ad Hoc Networks”, International Journal of Innovation, Management and Technology, Vol. 1, No. 3, pp. 279-285, August 2010.

[4] Ipsita Panda “A Survey on Routing Protocols of MANETs by Using QoS Metrics” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, pp. 121129, 2012

[5] W. Stallings, "Cryptography and Network Security", Principles and Practices, 3rd edition, Prentice Hall, 2003.

[6] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat “Lightweight Blackhole Attack Detection In Manets” Ieee Systems Journal, Vol. 7, No. 2, June 2013.

[7] Nitish Balachandran “A Review of Techniques to Mitigate Blackhole Attacks” Int. J. Advanced Networking and Applications 11 July 2012. [8] Chris Piro Clay Shields Brian Neil Levine “Detecting the Blackhole Attack in Mobile Ad hoc Networks” NSF grants CNS-0133055, CNS-0534618, and CNS0087639.

[8] Issa Khalil, Saurabh Bagchi, Ness B. Shroff. “LITEWORP: a Lightweight countermeasure for the wormhole attack in multihop wireless networks” In the proceedings of the 2005 international conference on dependable systems and networks (DSN’05); 2005.

[9] Issa Khalil, Saurabh Bagchi,and Ness B. Shroff. “MOBIWORP: mitigation of the wormhole attack in mobile multihop wireless networks” In the IEEE securecomm and workshops; 2006.

[10] Xia Wang and Johnny Wong, “An end-to-end detection of wormhole attack in wireless ad-hoc networks” In the proceedings of the 31st annual international computer software and applications conference (COMPSAC); 2007.

[11] Hu Yih-Chnu, Perrig Adrian, Jonhson David B. “Wormhole attacks in wireless networks” IEEE Journal on Selected Areas in Communication 2006.

[12] Lazos L, Poovendran R, Meadows C, Syverson P, Chang LW. “Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach” In the proceedings of the IEEE conference on wireless communications and networking; 2005.