IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 4 Issue 2 February, 2016

AN OPTIMIZED APPROACH FOR BLACKHOLE ATTACK DETECTION IN MANET

SACHIN MALVIYA
Assistant Professor, Department of Computer Science & Engineering,
Shri Balaji Institute of Technology & Science,
BETUL (M.P.)
Sachinm.research@gmail.com

ABSTRACT

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

The research in recent years on intrusion detection is gradually inclined to artificial intelligence technology to improve the detection accuracy. Generally it is believed that intrusions illustrate something which differs from the normal pattern, and that any unknown intrusion will present patterns more similar to known intrusion than to normal data. Additionally, by gathering network traffic, using the right classification algorithm, the system should be able to detect known intrusion as well as new intrusions.

The solution for above mentioned problems and for the protection of information system, a new detection technique is needed which is able to detect Intrusion. Proposed work introduces combination of support vector machine & genetic algorithm to give optimized algorithm for intrusion detection. The analysis suggests that the new technique can detect the network attack efficiently. For communication over the wireless network nodes use data as packets to send it over the network and it has to be sent via some medium on some routes. Attackers make some moves on these routes to make an attack here, so there is a need to place an effective detection system to detect this intrusion attack i.e. blackhole attack. Routing protocols are needed which are used to find route which is then use to send a packets over the networks. Some of the protocols such as adhoc on demand distance vector routing protocol(AODV) & destination-sequenced distance vector(DSDV) are used which has queue based packet processing.

AODV uses destination sequence numbers to ensure loop freedom at all times avoiding problems (such as "counting to infinity") associated with classical distance vector protocols. DSDV Routing is a table-driven routing scheme for ad hoc mobile networks based on the Bellman–Ford algorithm.

AODV & DSDV protocol has a queue based processing so they are vulnerable to denial of service (DoS) attack in which multiple packet are sent to the destination in order to take over the resources. Proposed approach blackhole detection algorithm (BDA) is improved protocol in which SVM techniques is used to make the decision about which packet needs to be accepted or rejected. SVM is a machine learning algorithm which uses previous patterns to make classifications. But one problem associate with SVM is that it can create hyperplane in an infinite dimension. SVM use parameters as raw features for creating a hyperplane. Optimization of number of parameters used in SVM can be done by genetic algorithm which gives optimal solution so that more efficient result for detection of blackhole attack should be obtained.

Keywords: Intrusion Detection, Mobile Ad-hoc network, Routing protocols, Support Vector

Machine, Genetic Algorithm, Machine classifier, Denial of Services, Blackhole Attack

1. 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 and its main tasks are to maintain effective safety protections on that system development plan, and establish security system from perspective of network security and also for the application security [1].

Since network security is important for the information system and for establishing the effective operation of network 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 are generally 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.

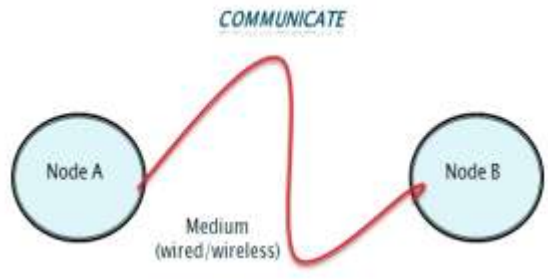

Fig 1.1 Basic Function of Network [4]

However, detection accuracy of this approach is largely affected by its structural parameters. One thing is that the data or information has too large dimensions and only some of the characteristics are useless and for the other features the SVM structure is always not optimized which causes an inefficient detection performance. Although PCA is employed to do dimension reduction but they did not consider the optimization of FSVM parameters. PCA is accurate for linear 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 with parameter optimization. Solution of the above discussed problems and for the protection information security system from blackhole attack new detection approach is proposed which is based on GA for optimization and FSVM for classification.

1.1.1 IDS Techniques

Some of the techniques for intrusion detection are specified below [3].

1.1.1.1 Statistical Models

Several statistical techniques have been implemented in anomaly detection mechanism for events and event counters more. Threshold measures, mean and standard deviation are used in these techniques include multivariate models.

1.1.1.2 Markov Process Model

In this model the state transitions for each system call is analyze and does not use system call sequences.

1.1.1.3 Rule-Based Algorithm

In the intrusion detection field is RIPPER is one of the commonly used rule-based algorithms, which performs classifications by creating a list of rules from a set of training set examples.

1.1.1.4 Data Mining Techniques

In this technique intrusion detection mechanism build detection models by applying data mining techniques to large data sets collected by a system.

1.1.1.5 Immune System Approach

This approach includes process in which applications and procedures are modeled as a system call sequences.

2. PROBLEM DEFINITION & OBJECTIVE

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 [6]. 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 threats and more importantly to resist the attacks of internal threats.

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 [4]. The solution of above discussed problems and for protection the data a new intrusion detection technique for blackhole attack detection based on optimization of GA & classification of fuzzy SVM have been proposed. The analysis suggests that this technique could detect the blackhole attack efficiently.

The main objectives related to work is:

• Improve IDS using FSVM by classification analysis and learning mechanism & also GA for optimized solution.

• 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, so that blackhole detection should be more efficient.

3. WIRELESS TECHNOLOGY

Wireless networks as medium uses open air for communication as transfer medium and information travels as electromagnetic signals to send information from one node to another. In wireless network nodes can communicate with other node of that network situated in a specified range from each other called transmission range. If one node want to send a data packet to other node in network that is not in neighborhood then, it has to rely in nodes in between for forwarding the packets to its destination address where data is received, thus an efficient routing protocol is required for finding the optimize path for communication.

Sharing on an insecure network has a major problem in the area of security over the recent years. Intruders always try to break through the system to gain access to the resources to which they are not permitted to access. The unauthorized attempt to access over the unsecured network & creates a potential threat to the integrity of the system is the task performed by hackers. As the network become wider day by day & the information are circulated over the network this problem is even getting worse day after day. This problem is generally given a name intrusion.

3.1 SECURITY IN MANETS

Dynamic nature of adhoc network results in issue arises in security risks while some existing vulnerabilities in wired networks still needs to be solved. Use of technologies related with security required in development of wired networks for securing wireless networks. Also when wired medium connect the nodes is absent so any node which is either normal or malicious may penetrates the network without restrictions. It prevents outsiders entering in the network by using cryptographic techniques are likely be used for authentication of the nodes in network [8].

Since the general function of the network is typically related on a trust between the two participating nodes. Generally most of these attacks in mobile environments are considered to focus on protocols for routing. They were initially designed to be efficient rather than taking security issues into account. All of them usually need to build the confidence between participating nodes [11]. But a node with malicious features may modify functionality and disturb the functional behavior of

this protocol. This creates illustration of attacks that needs to take into consideration to evaluate the effectiveness of the used algorithms for intrusion detection.

3.1 Packet Dropping Attack

The Route Error packets are rejected by attacker results in authorized nodes forward packets to the broken links [4].

3.2 Flooding Attack

Forged Route Request packets are broadcasts randomly to all nodes by the malicious node in some time interval to overload the network.

3.3 Black Hole Attack

Black hole attack is an attack in which an attack node advertises itself as the route to shortest path in the network. Also it receives packets which is destined for other nodes and simply drops them rather than forwarding to its destination.

3.4 Forging Attack

A node with malicious behavior modifies and broadcasts Route Error packets to the victim node leading to repeated link features.

4. INTRUSION DETECTION IN MANETS

This is a system which is either software or hardware or combination of both of two that scan and monitors the computer network event for intrusive evidence. When designing IDS to be used in ad hoc environment some issues may be taken into account because of its nature. There are numbers of aspects the detection engine must behave properly to a wired network based intrusion detection system.

In general the anomaly based IDS uses predefine model of normality to detect anomalies in the wireless network. This approach not be simply used in adhoc environment because of dynamic and flexible behavior of MANET nodes makes hard the definition of normal and malicious behavior. Furthermore a dynamic feature of node leads to dynamic nature of the network topology and increases the complexity of the process mechanism for detection. Additionally since the dynamic nodes does not have any fixed location and so no central management and monitoring point is in IDS that could be placed anywhere in the network stores information. That result in detection process may be distributed different nodes and also the collection and analysis of data in the network. Usually IDS are categorized into collaborative and independent or non-collaborative.

5. PROPOSED APPROACH

IDS can be improved using optimization GA and FSVM. IDS are a software or hardware which can detect possible intrusion so that it can be prevented. But in order to do so IDS uses different approaches for it processing. Suggested work uses FSVM for decision making; SVM is a machine learning algorithm which can uses previous patterns for regression and classification analysis. But a problem associated with SVM is that it can take all the parameter in its decision making due to this optimized result could not be obtained. To optimize Parameters GA is used which is an algorithm gives optimal solution.

The amount of error find with respect to time can be improved in proposed IDS. However some mechanism needs to be put into fuzzy support vector machine so that parameters can be used as the other objective functions.

Hence proposes the methods to improve the performance of IDS in two ways feature subset selection and other one is optimization of parameter.

5.1 SUPPORT VECTOR MACHINE

SVM is a machine learning approach and can be applied to solve the problems of classification and also regression analysis in an efficient manner. SVM is capable of reducing errors in training and testing and has efficient prediction result based on the trained models. For classification using a linear classifier, SVM tries to find a hyper plane based a training data set so that this hyper plane [10].

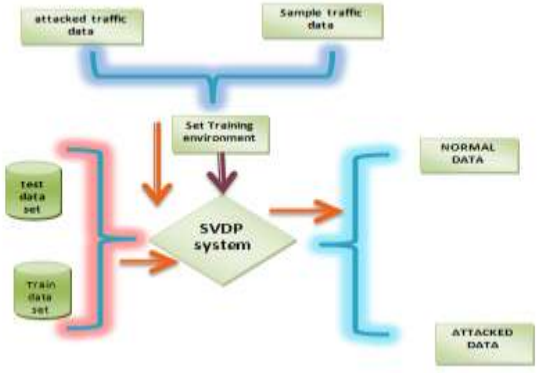

Fig 3.2 SVM Implementation

The AODV and DSDV protocol has a queue based processing so they are vulnerable to DoS attack in which multiple packet are sent to the destination in order to take over the resources. So here proposed new improved protocol in which use of SVM techniques to make the decision that which packet needs to be accepted or rejected. SVM is a machine learning algorithm which uses previous patterns to make classifications. But one problem associate with SVM is that it can create hyperplane in an infinite dimension. For creating a hyperplane SVM use parameters as raw features.

5.2 USE OF GENETIC ALGORITHM

Proposed approach use GA to select the support vector which is optimized so that efficient results are obtained. Support vector machine uses parameter to make hyperplanes in an infinite dimensions so it can take as much as parameters available. Due to this reason SVM is highly inefficient. To overcome this problem here use genetic algorithm so that only optimized values should be used for parameters of SVM & highly optimized result can be obtained.

6. PROPOSED ALGORITHM

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

7. DESIGN OF THE IDS

- Creation of network with nodes
- Selection of Parameter (by GA)
- Training by FSVM
- Execution of Scenario
- Obtained Result

8. Result Analysis

Table 8.1 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 8.2 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 8.3 Scenario result BDA

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

In the above table the protocol used is BDA 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.

9. Result Comparison

Table 9.1 Scenario result AODV vs DSDV vs BDA

Normal Nodes	Attack Nodes (20%)	AODV	DSDV	BDA
		Packet Drop Rate(in mbps)		
50	10	4.8613	4.9237	38.5405
60	12	4.5246	7.9006	45.8007
80	16	26.1783	11.9472	74.042
100	20	0.1293	0.118	4.5942

In the above table the protocol used is AODV which uses queue based process, DSDV which also uses queue based process & BDA 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.

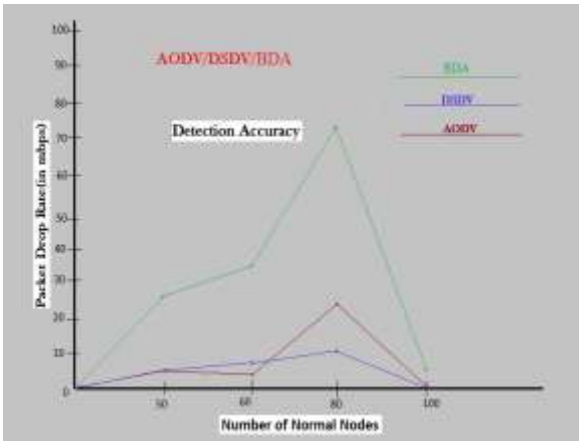

Fig 9.1 AODV vs DSDV vs BDA Observation Chart

In the above chart the protocol used is AODV which uses queue based process, DSDV which also uses queue based process and BDA uses SVM and 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 and 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 used 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.

10. 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 more attracted 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 attack. 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) has been proposed. The new analysis suggested that the proposed technique could detect the network attack more efficiently. Wireless networks use the open medium as communication to send messages among node to node. Wireless networks nodes can communicate inside their transmission range and in mobile ad-hoc network rely on intermediate nodes while transmitting the data to a node that is more than one hop away from node. The Routing protocol is needed to be more efficient in order to find the most reliable and optimized communication path is needed. Now a day several application and architecture are using wireless channel & this would lead to critical security issues in mobile ad-hoc network. It is required that all nodes must be situated into the area of fixed access point otherwise there will be no communication at all.

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 SVM is used. It is also not 100% efficient techniques because it can take all the constraints to produce output values. Here the limitation was solved for SVM parameters optimization by using genetic algorithm which gives optimal solution. So here say that proposed algorithm BDA is the machine learning protocol which gives optimal solutions.

11. Future Work

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 but only blackhole attack. In future it can be extended to detect more intrusive activity & to prevent intrusion and also to take some action against intrusion

12. Acknowledgement

This work is the result of guidance of Dr. C S Satsangi (Professor IT Dept, MITM, Indore) & Mr. Suneet Joshi (Assistant Professor IT Dept,MIST, Indore). Also I like to thank all my faculties which directly or indirectly guide me for the same.

REFERENCE

[1] Dutta, C.B., Biswas, U., "A novel blackhole attack for multipath AODV and its mitigation", Recent Advances and Innovations in Engineering (ICRAIE), 2014.

[2] Michael Beham, Marius Vlad, Hans P. Reiser, "Intrusion Detection and Honeypots in Nested Virtualization Environments" 978-1-4799-0181-4/13/-2013 IEEE, 2013.

[3] Suneet Joshi, Sachin Malviya, "Intrusion Detection by Intrusion Detection System (IDS)",International Journal of software & Hardware Research in Engineering Volume 1 Issue 2, October 2013.

[4] Suneet Joshi, Sachin Malviya, "Study Of Implementation Of Intrusion Detection System (IDS) Via Different Approaches", International Journal of software & Hardware Research in Engineering Volume 1 Issue 4, December 2013.

[5] Sriparna Saha, Ashok Singh Sairam, Asif Ekbal, "Genetic Algorithm Combined with Support

Vector Machine for Building an Intrusion Detection System", ACM 978-1-4503-1196-0/12/08, ICACCI, 2012.

[6] K.Kiruthika Devi, M.Ravichandran, "Detecting Sinking Behavior at MAC and Network Layer Using SVM in Wireless Ad hoc Networks", (IJCSN) Volume 1, Issue 3, June 2012 ISSN 2277-5420, 2012.

[7] Ashish jain, Sachin Malviya, Sohil jain, Sourabh Joshi "Cryptosystem using Genetic Algorithm" ICCMS 2011.

[8] Mrutyunjaya Panda, Ajith Abraham, Manas Ranjan Patra, "Discriminative Multinomial Naïve Bayes for Network Intrusion Detection", Information Assurance and Security (IAS) IEEE, 2010.

[9] D. M. Farid, N. Harbi, and M. Z. Rahman, "Combining naive bayes and decision tree for adaptive intrusion detection", CoRR, vol. abs/1005.4496, Apr. 2010.

[10] Yin-Wen Chang Cho-Jui Hsieh Kai-Wei Chang, "Training and Testing Low-degree Polynomial Data Mappings via Linear SVM", Journal of Machine Learning Research 11 (2010) 1471-1490, 2010.

[11] Huei-Wen Ferng and Chien-Liang Liu, "Design of a Joint Defense System for Mobile Ad Hoc Networks", IEEE 0-7803-9392-9/06, 2006.

