ijesm
Consulting, help, relaxation
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES
&
MANAGEMENT

DCA BASED RANDOM FOREST APPROACH FOR SECURE IDS OVER MANET

Sachin Khasdev[1], Varsha Namdeo[2] and Mohit Gangwar[3]
1, Research Scholar, Department of Computer Science, BERI Bhopal, (MP) - India
2, Department of Computer Science, BERI Bhopal, (MP) - India
3, Principal, BERI Bhopal, (MP) – India
Email: khasdev.sachin@gmail.com, varsha_namdeo@gmail.com, mohitgangwar@gmail.com

Abstract

The mobile ad-hoc network (MANET) is a new wireless technology, having features like dynamic topology and self-configuring ability of nodes. The self configuring ability of nodes in MANET made it popular among the critical situation such as military use and emergency recovery. But due to open medium and broad distribution of nodes make MANET vulnerable to different attacks. So to protect MANET from various attacks, it is important to develop an efficient and secure system for MANET. Intrusion means any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. Intrusion Prevention is the primary defense because it is the first step to make the systems secure from attacks by using passwords, biometrics etc. Even if intrusion prevention methods are used, the system may be subjected to some vulnerability. So we need a second wall of defense known as Intrusion Detection Systems (IDSs), to detect and produce responses whenever necessary. In this article we present a survey of various intrusion detection schemes available for ad hoc networks. We have also described some of the basic attacks present in ad hoc network and discussed their available solution.

Key-Words: Mobile Ad hoc Network; Intrusion Detection System (IDS) ; IDS in MANET; Security Issues in MANET.

INTRODUCTION

MANET consists of wireless mobile nodes that form a temporary network without the aid fixed infrastructure or central administration. Nodes can communicates directly to other nodes if they are under the transmission range. For communicating to nodes outside the transmission range, nodes have to depend on intermediate nodes, which form a multihop scenario. In multi-hop transmission, a packet is forwarded from one node to another, until it reaches the destination. Routing protocols are generally necessary and plays very crucial role for effective communication between distinct nodes in MANET. Routing protocol not only discovers network topology but also built the route for forwarding data packets. Routing protocols are designed to adapt frequent changes in the network topology because of node mobility and dynamically maintains routes between any pair of communicating nodes. Several ad hoc routing protocols have been proposed in literature for communicating between mobile nodes. These routing protocols can be roughly classified [1] into proactive, reactive and hybrids protocols. MANET is vulnerable to various types of attacks because of open infrastructure and limited battery-based energy of mobile nodes. These attacks may be classified as external (outside) and internal (inside). Many schemes had been proposed previously that solely aimed on detection and prevention of outside attacks. But most of these schemes become worthless when the malicious nodes have already entered the network, or some nodes in the network have been compromised by attacker. Such attacks are more vulnerable and serious threat as these are initiated from inside the network and because of this the first defence lines of network become ineffective. Since inside attacks are performed by participating malicious nodes which behave well before they are compromised therefore it becomes very difficult to detect.

The basic problem with most of the routing protocols is that they trust all nodes of network and assume that all nodes behave properly which is not

true in all cases. Most ad hoc network routing protocols are inefficient and shows dropped performance while dealing with large number of misbehaving nodes. Such misbehaving nodes support the flow of route discovery traffic but interrupt the data flow, causing the routing protocol to restart the route-discovery process or to select an alternative route if one is available. The newly selected routes may still include some of misbehaving nodes, and hence the new route will also fail. This process will continue until the source concludes that data cannot be further transferred.

II)NODE MISBEHAVIOR MODEL

Routing protocols basically performs two important functions: Routing function and Data forwarding function. Routing function performs routes discovery and routes maintenance activity. Data forwarding function is concerned with forwarding data packets toward the destination through the established route. In order to work properly, the routing protocols need trusted working environments, which are not always available. There might be a situation where some nodes i.e. selfish, malicious or node compromised by attackers are not behaving properly. Thus network will be vulnerable to attacks launched by misbehaving nodes. Both routing and data forwarding function of routing protocol would be affected with the presence of misbehaving nodes in network. Such node misbehavior can be classified [2] into following:

1)Malfunctioning: These nodes suffer from hardware failures or software errors.

2) Selfish: These nodes agree to forward data packet but silently drop packet in order to save its energy and can be defined into three types [3] (i.e. SN1, SN2 and SN3) related to routing. SN1 nodes participate in the route discovery and route maintenance phases, but refuse to forward data packets to save its resources. SN2 nodes neither participate in the route discovery phase, nor in forwarding data packets. Instead they use their resource only for transmissions of their own packets. SN3 nodes behave properly if its energy level lies between full energy level E and certain threshold T1. They behave like node of type SN2 if energy level lies between threshold T1 and another threshold T2. And if energy level falls below T2 they behave like node of type SN1.

3) Malicious: These nodes use their resource and aims to weaken other nodes or whole network by trying to take participation in all established routes thereby forcing other nodes to use a malicious route which is under their control. After being selected in the requested route, they cause serious attacks either by dropping all received packets as in case of Black Hole attack [4], or selectively dropping packets in case of Gray Hole attack [5]. We refer such nodes as MN nodes.

SN2 type nodes do not pose significant threat therefore can simply be ignored by the routing protocol. On the other hand SN1, SN3 and MN nodes (defined in section II) are much more dangerous to routing protocols. These nodes take part in route discovery phase and interrupt the data flow by dropping or refusing to forward the data packets thus forcing routing protocol to restart the route-discovery phase or to select an alternative route if it is available. The newly selected routes may again include some of these type nodes, therefore the new route will also fail. This process will continue again and again until the source reaches a decision that data cannot be further transferred. In our work, we aimed on the detection and mitigation of such SN1 type selfish nodes and MN type malicious nodes. SN3 type selfish nodes will be detected only when they are behaving similar to SN1 type nodes.

III) SECURITY ISSUES IN MANET

Security always plays a vital role to identify various types of attacks, security threats and different vulnerabilities present in a system. Vulnerability could be a weakness in security system of any network. A particular system may be prone to unauthorized access to manipulate data because the system does not verifies a user's authenticity before permitting it to access into the network. Wireless ad hoc network like MANET is more vulnerable than wired network. Some of the major issues [7] regarding vulnerabilities in mobile ad hoc network are as follows:-

A. Lack of Centralized Management:

There is not any concept of centralized coordinating system in the mobile ad hoc network. Because of the absence of central management system it is very tough task to detect attacks present in the network, since it is not easy to observe the traffic in a movable and very big ad hoc network. Lack of centralized coordinating system may break trust among nodes in the network.

B. Resource Availability:

Availability of resources is a big issue in MANET. Establishing secure communication path in such dynamic network and protect the network from various attacks, ends up to the development of different security approaches and systems. Cooperative ad hoc network always permit development of self organized security systems.

C. Scalability:

Because of the moving nature of nodes, era of ad hoc network changes all the time. Therefore scalability is an important issue regarding security of ad hoc network. Hence security system should be able to manage a large scale network as well as small ones.

D. Cooperativeness:

Some routing algorithm for MANET like AODV normally assumes that nodes are cooperative in nature and non- attacker. As a result an attacker node may become main routing agent very easily and manipulate network functions as not following the protocol rules.

E. Dynamic Topology:

Dynamic nature and movable nodes relationship can break the trust between nodes. The trust of a node can also bedisturbed if few nodes are detected as agreed. This dynamic or changeable nature can be better protected with distributed and cooperative security systems.

F. Limited Power Supply:

The power supply for any node in mobile ad hoc network is limited, which causes many problems.

IV) RELATED WORK

In the intrusion hand side, the attacker must realize the routing protocol mechanism to fake the network, while in the security hand side; the researcher must understand the routing protocol mechanism to protect the network as well. This means that the attacker applies the same type of attack on different protocols using different ways; and hence the researchers use different types of intrusion detection mechanisms on different routing protocols to defend against same attack and/or different types of attacks. In 1980, the concept of intrusion detection began with Anderson's seminar paper [11], in which the author introduced a threat classification model that develops a security monitoring surveillance system based on detecting anomalies in user behaviour. **In 2014**, **Sumit et al** [12] introduced a new technique for intrusion detection. In the proposed IDS, the authors used the Effective K-means algorithm. The centroids of the clusters are constructed using this algorithm. It takes the input as the features of the nodes like total number of RREQ sent by each node or total number of RREP received by each node etc. The desired node features can be picked from the trace file which is obtained on running the simulation in Network Simulator-2. Authors assumed the value of K=2 because, they want to obtain two centroids of highly dense segments. One of these dense segments consists of nodes with normal behaviour and the other consists of abnormal or intrusive behaving nodes. The Effective K-means algorithm runs on a data set which is represented by two centroids of highly dense segments. The IDS is host based and monitors every node in the MANET. If any event is generated by a node, then the selected features of that particular node is fetched. Then the meansquare error is calculated and Euclidean distance from the previously constructed centroids is checked. If the result is close to the normal segment centroid, then IDS assumes the node to be normal and allows it to proceed with its normal events. Else, it will not allow the node to proceed with its events. The IDS will simply drop the activity from the queue, which is generated by the node which has been detected as a malicious node [13]. The above process is continued till all the nodes showing intrusive behaviour are detected and separated from the normal nodes. Thus malicious nodes can be separated from the nodes working properly and as a result, our MANET can again get back to its normal functioning i.e. routing packets properly. **Again in 2014, Indirani and Selvakumar** [14] proposed swarm- based efficient distributed IDS for MANET. An artificial intelligence technique that represents the clever activities witnessed in swarms with the help of multi-agent systems (MAS) is termed as swarm intelligence. A MAS is a system that consist multiple interacting intelligent agents. It can be used for solving those problems which are very complex or impracticable for a particular user or a system to solve. In this approach, the swarm

intelligence-based ant colony optimization (ACO [15]) is used for selecting the active nodes. In selected route, the parameter to select any node as active node are- maximum trust value, residual bandwidth and energy. This is accomplished to perform the process for detecting intrusion. Every active node checks its neighbour node within its communication range and stores the trust values of all checked nodes. Each active node changes in a timely manner as per the trust parameter. After that active nodes interchange the trust values with its corresponding neighbour active nodes. Once the exchange process done, if any specific node's trust value is less than the minimum threshold, then the node is declared as attacker. After successfully detecting all attacker nodes, the active node informs to the source node. The source then established a protective mechanism to remove the attacker nodes from the networks. The author used some well defined parameter to select active nodes in the network are- residual energy, bandwidth, coverage and connectivity and trust. **In 2013, Bhavsar and Waghmare** [15] proposed a system, in which the author constructed a SVM model for classification. Whenever any intrusive activity happens, SVM detects the intrusion. A classification task involves training set and testing set which consist of objects. Each object in the training set contains one "target value" (class labels: Normal or Attack) and several "attributes" (features).The goal of SVM is to produce a model which predicts target value of data object in the testing set which gives only attributes. To achieve this goal, the author used kernel functions available with SVM. There are 3 major SVM kernel functions [16]:

(I) Gaussian Kernel Function
(II) Polynomial Kernel Function
(III) Sigmoid Kernel Function

In the same year 2013, Abirami et al [17] proposed anDS which is based on Sentinel Protocol. Sentinel Protocol. It is an efficient approach to detect replica nodes when the IDS inform it by an alert value. Replica detection is based on an interactive time and global information about the node. Whenever two nodes communicate during the packet transmission, each node will exchange some information such as time and global information with another node. This confidential information exchange process should do with all nodes in the network during the transmission. If any node fails to perform this activity, then from the knowledge of the neighbourhood node, it can easily detect the abnormal silence of the replica node. Nodes also exchange the challenge key which contains least and unused index of the node. With this detection scheme the geographical range of replica nodes are detected easily. The author used five simple steps to form the proposed IDS, are- Network formation, Route discovery, Protocol implementation, Route maintenance and Analysis. In the protocol implementation phase, the author believed that the attacker has the potential to agree a few number of nodes, control on the agreed nodes, and build many copies of agreed nodes to enlarge the possibility of attack. The assumption is that the attacker can't compromise enough number of nodes to have a remarkable effect on the network, but it can take full control on the network by inserting many copies of replica node. Hence the motivation of the Sentinel Protocol is to discover and reject all alias nodes with the same identity to make sure the security of the network. If the alias is constructed in an area where the distance between any two alias node exceeds some predefined value and if they do not interchange information with other node during the data transmission process then it's the responsibility of neighbour node to detect Attacker Node (AN) present in the network. The neighbour node implements the Sentinel Protocol. **In 2011, Abdelhaq et al** [18] approached a new technique for detecting intrusion in MANET, known as Local Intrusion Detection (LID). The LID secure routing technique allows the diagnosis of the attacker node to be locally; it means that when the suspected intermediate node unicast the RREP message towards the source node, the preceding node to the intermediate node performs the process of detection and not the source node. The detection process is as follow- First, the previous node buffers the RREP packet. Second, it uses a new route to the next hop node and sends FRREQ packet to it. When the previous node receives the FRREP packet from the next hop node, it extracts the information from the FRREP packet and behaves according to following rules:

(i) If the next node has a route to intermediate node and destination node, the previous hop node discard the FRREP, and unicast the RREP to the source node.

(ii) If the next hop has no route to the destination node or the intermediate node or both of them, the previous node discards the buffered RREP and the FRREP as well, at the same time broadcasts the alarm message to announce there is no secured enough route available to the destination node. The last case includes another scenario such as; the case inwhich the previous hop node does not receive any FRREP from the next hop node. So, here the source node will discover a new route to the destination. This will decrease both routing overhead packets and end to end delay,and increase the network throughput at the same time.

V)PROPOSED METHODOLOGY

The central challenge with computer security is developing systems which have the ability to differentiate between the normal and an intrusion which represents potentially harmful activity. A promising solution is emerging in the form of biologically inspired computing, and in particular artificial immune systems (AIS).

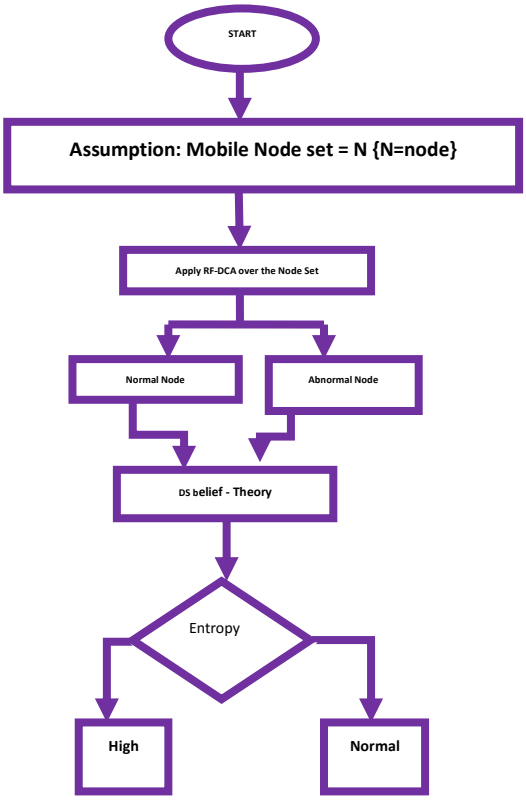
We modified Random Forest with the of the concept of Dempster–Belief Theory and along with the concept of entropy for data authentication in Host based Network. Random Forest provide facility for the Feature for normal and abnormal data and Dempster-Belief theory is used to compute the probability of evidences that indicate support the attack or normal class .The use of Dempster Belief theory steadily spreads out, mostly because it is used to cope with large amounts of uncertainties that are inherent of natural environment Different author proposed a different scheme for intrusion detection for providing computer security. All existing methods having lower true positive rates and high false negative rates that's lead to compromise security of IDS system. In order to overcome this problem proposed methodology modified the existing Random Forest for controlling a generation of false alarm generation and also improve performance of classification of data.

We introduced a novel intrusion detection system to identify all intrusion correctly and minimized the false alarm generation. Proposed introduced a novel intrusion detection system to identify all intrusion correctly and minimized the false alarm generation. Proposed methodology encapsulate Random Forest and Dempster–Belief theory (DBT) along with the concept of entropy is used to designed and increase the performance of the system. Dempster–Belief Theory scale the uncertainty in feature selected by random forest and on the basis of entropy refine the feature. If feature set have higher entropy it's again send for decision otherwise consider.

The Dendritic Cell Algorithm (DCA) and Dempster–Belief theory (DBT) along with the concept of entropy is used to designed and increase the performance of the system. Dempster–Belief Theory calculated the degree of uncertainty and again on the basis of entropy calculated we find the intruder, having higher entropy, is regarded as the "intruder", and generate the alarm.

VI) PROPOSED FRAMEWORK

In proposed framework initially intruder data set initialized with random partition. Then random forest approach tends to generate random feature for intruder. This Random feature is recertifying through Dempester Shafer theorem. If entropy of Random feature is low then it's acceptable otherwise feature is not to be consider. Acceptable Feature is denoted as relevant feature and apply for classify intruder. If intruder detection have high false negative rate then whole process is initialed by random partition and if intruder detection have low true positive rate then new feature is generated on same partition.



This chapter conclude the proposed technique for intrusion detection that is based on one of the algorithm of Artificial immune system called The Random Forest and Dempster–Belief theory (DST) .With the help of Dempster–Belief theory we calculate the degree of uncertainty and again on the basis of entropy with the classify the end user, end user having higher entropy, is regarded as the "intruder", and generate the alarm. Proposed System can not only reduce the false positive and false negative rate but also improved the correlation technique and decrease the intrusion rate in the system.

VII)CONCLUSION

RESULT ANALYSIS

Proposed methodology show better result in term of packet delivery ratio, battery power consumption and control packet overhead.

- **True Positive Rate: -** Proposed methodology use Random Forest DCT which return high TPR Rate as compare with existing approach by using Machine Learning Technique.
- The performance of an intrusion detection system may be evaluated in terms of TP (True Positive) rate and FP (False positive rate) rate. TP rate is calculated as the number of abnormal patterns detected by the system, divided by the total number of abnormal patterns.
- Here A represent attack and I represent Intrusion TPR= =P (A| I) ……. (1)
- Similarly TN (True negative) rate can be calculated as,**TNR= =P (-A|I)**

Figure-True Positive Rate Comparison

FP (False Positive) rate occurs when the system wrongfully classifies normal patterns as abnormal patterns. In this experiment, FP rate is calculated as the number of false positives created by the system, divided by

FNR= =P ( ) …….. (3)

Similarly FN (False negative) rate can be calculated as,

FNR= =P ( ) …….(4)

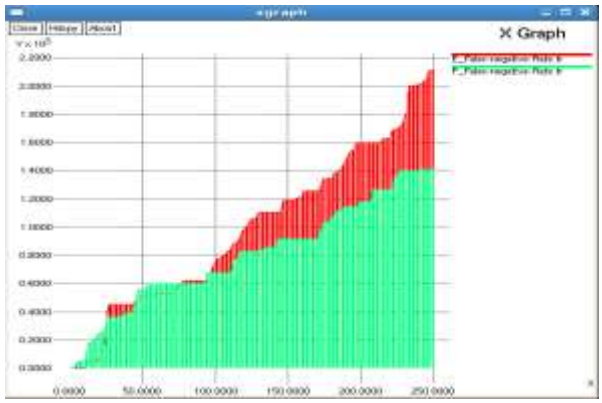


Figure-False Negative rate of Proposed Protocol and Existing Protocol

- **Routing overhead: -** For any ideal routing protocol it is required that it has lower Routing overhead, whereas existing approach by using ML have required higher Routing as compare to proposed methodology by using RF-DCT .

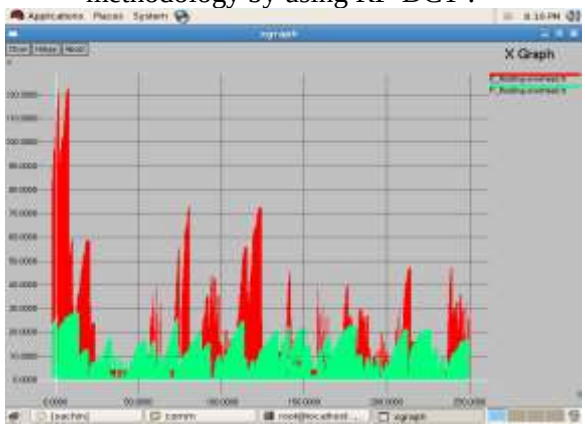


Figure-Routing Load of Proposed Protocol and Existing Protocol

- **Battery Power Consumption:-** Towards Energy saving routing protocol proposed protocol try to move lower energy node towards less traffic and higher energy node towards high traffic and reduce retransmission whereas existing approach only minimized redundant path.

Figure -Resident Energy of network in Proposed Protocol and Existing Protocol

VIII) REFERENCES

1. Pooja Jaiswal and D.Rakesh Kumar. Prevention of Black Hole Attack in MANET. IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC); ISSN; 2012; p. 2250-3501I.
2. Neethu B. Classification of intrusion detection dataset using machine learning approaches. International Journal of Electronics and Computer Science Engineering; 2012; p.1044-1051.
3. Shailesh Kumar Gaikwad, Prof. Vijay Shah, Yogendra Kumar Jain. A Secure Network Detection System against Noisy Unlabeled Data. International Journal of Computer Applications, 2010. 9(9).
4. Mishra A., K. Nadkarni and A. Patcha. Intrusion detection in wireless ad hoc networks. Wireless Communications; IEEE;2004. 11(1): p. 48-60 %@ 1536-1284.
5. BalaGanesh M. and M.M. Faisal. Enhance the Security Level of MANET's Using Digital Signature. IEEE Transactions on Networking, 2004.Electronic Publication: Digital Object Identifiers (DOIs):
6. Tiranuch Anantvalee, Jie Wu A survey on intrusion detection in mobile ad hoc networks, in Wireless Network Security.2007; Springer; p. 159-180 %@ 0387280405.
7. Priyanka Goyal., Sahil Batra, and Ajit Singh. A literature review of security attack in mobile ad-hoc networks. International Journal of Computer Applications; 2010; 9(12): p. 11-15.
8. Vesa Kärpijoki. Security in ad hoc networks. 2000.
9. Janne Lundberg. Routing security in ad hoc networks.Helsinki University of Technology, http://citeseer.nj.nec.com /400961. html, 2000.
10. Wenjia Li and Anupam Joshi, Security issues in mobile ad hoc networks-a survey. Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, 2008: p. 1-23.
11. Anderson, J.P., Computer security threat monitoring and surveillance. 1980, Technical report, James P. Anderson Company, Fort Washington, Pennsylvania.
12. Sumit, S., D. Mitra, and D. Gupta. Proposed Intrusion Detection on ZRP based MANET by effective k-means clustering method of data mining. 2014. IEEE.
13. Preetee K. Karmore , Smita M. Nirkhi, Detecting Intrusion on AODV based Mobile Ad Hoc Networks by k-means Clustering method of Data Mining. International Journal of Computer Science and Information Technologies, 2011. 2(4): p. 1774-1779.
14. Indirani, G. and K. Selvakumar, A swarm-based efficient distributed intrusion detection system for mobile ad hoc networks (MANET). International Journal of Parallel, Emergent and Distributed Systems, 2014. 29(1): p. 90-103%@ 1744-5760.
15. Yogita B. Bhavsar , Kalyani C.Waghmare, Intrusion Detection System Using Data Mining Technique: Support Vector Machine. International Journal of Emerging Technology and Advanced Engineering, 2013. 3(3): p. 581-586.
16. Panwar, S.S. and Y.P. Raiwani, Data Reduction Technique to analyze NSL-KDD set .Journal Impact Factor, 2014. 5(10): p.21-31
17. Abirami, K.R., M.G. Sumithra, and J. Rajasekaran. An enhanced intrusion detection system for routing attacks in MANET. 2013. IEEE.
18. Abdelhaq, M., et al. A local intrusion detection routing security over MANET network. 2011. IEEE.