Engineering Universe for Scientific Research and Management
(International Journal)

EUSRM
A Universe of Research
ISSN(ONLINE) : 2319-3069

Vol. 8 Issue 12
December 2016

Energy efficient Intrusion Detection System in Mobile Ad Hoc Networks

Sarita[1], Shubha Dubey[2]
Department of Computer Science & Engineering
Radharaman Institute of Technology and Science, Bhopal[1, 2]
sarita.narwaria93@gmail.com[1]

Abstract

In network security various techniques have proposed to detect unauthorized use, misuse and abuse of computer systems by both system insiders and external intruders. Due to the rapidly increasing unauthorized activities In order to increase network security various technique has been proposed but having a deficiency over IDS system in some of the situation i.e. if correlation alarm is not precise, reduction and prevention of false positive and false negative is high , at last having insufficient measurement of pattern recognition. In order to overcome all these deficiency from IDS, system over network, we propose a novel dual detection of IDS based on supervised clustering that integrating the Game theory and K-means .The Game Theory helps for calculating reliability score and K-means resolves the problem of clustering and cluster head.

Keywords: MANET, IDS, K-Means, Clustering, Game Theory.

1. Introduction

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 [1-5]. So we need a second wall of defense known as Intrusion Detection Systems (IDSs), to detect and produce responses whenever necessary.

The enormous growth of computer network increasing the importance of network security. The central challenge with computer security is to develop systems which have the ability to correctly identify an intrusion which represents potentially harmful activity. Therefore, the role of IDS is as special-purpose devices to detect and prevent the anomalies and illegal access of data. In current scenario, users look for the complete security of data at any cost, since security of data become prime requirement for everyone. The new challenge requires several changes in existing IDS system in order to improve the correlation of alarm; the detection and prediction of false positive and false negative rate must be low. Recently, using biological models such as neural networks and genetic algorithms in modelling and solving computational problems has been spectacularly successful. Lots of traditional IDS techniques are only able to detect and prevent [6, 7].

In network security various techniques have proposed to detect unauthorized use, misuse and abuse of computer systems by both system insiders and external intruders. Due to the rapidly increasing unauthorized activities, Intrusion Detection System (IDS) as a component of defence-in- depth is very necessary because traditional techniques cannot provide complete protection against intrusion. Along with that mobile nodes operate on the limited power of battery therefore it becomes very necessary to develop techniques which can successfully maintaining lesser complexity [8-10]. The objective of this paper is to develop a new approach which can successfully maintain security with lesser battery power in order to long survival of Sensor network.

2. Related Work

This Section throws some light on previous work which has been done in past years. The large number of paper has been studied but some of them are presented here. This chapter hasn't described the whole paper but the part of paper and its proposed work with the author name and paper title.

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 [17-20]. 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 [16]. 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

In network security various techniques have proposed to detect unauthorized use, misuse and abuse of computer systems by both system insiders and external intruders. Due to the rapidly increasing unauthorized activities, Intrusion Detection System (IDS) as a component of defense-in- depth is very necessary because traditional techniques cannot provide complete protection against intrusion.

3. 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).

IDS focus on exploiting attacks, or attempted attacks, on networks and systems, in order to take effective measures based on the system security policies, if abnormal patterns or unauthorized access is being suspected. A lot of methods and techniques have been proposed for the effective designing of IDS. But all technique suffered common problem that problem is detection and prediction of false positive and false negative rate is high.

In proposed work cluster based IDS over mobile node in MANET has been carried out. The main objective of desire work is to monitor the nodes in its cluster at the desired security level in order to detect any malicious activity. Another objective is to conserve its energy. In this work cluster is form on the basis of communication demand. As shown in figure 1(a) initially all nodes are independently as cluster. But if any node wants to communicate with their neighbor node ie if node A want to communicate with node B then node A first authenticate node B by using n-player cooperative game and if success then node A become the cluster head and node B become the member of cluster 1 as shown in figure 1(b). Subsequently if node C wants to communicate with any node of cluster 1 then there is only requirement that node C first follows n-player cooperative game authentication and become the member of cluster 1.

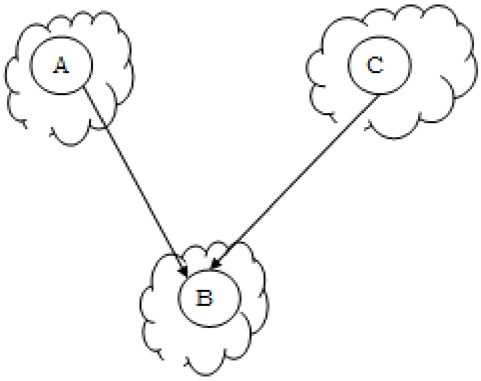

Figure 1(a) Network Scenario

The whole above process has been carried out over the network for every communication subgroup.

In this process it is possible that one node become the member of one or more cluster and their communication system over respective cluster has been control by their luster head. In proposed work both inter cluster and intra cluster authentication is carried out with the help of cluster head.

RESPONSIBILITY OF CLUSTER HEAD

1. Cluster head manages a group of nodes so that the communication can securely execute over the network.
2. Cluster head is called trusted nodes. To be trusted, a node should be set in a secure environment and also run trusted MANET.

Cluster head checks the background of embedded nodes in secure environment and if the records were verification a certification is sent to the node platform according to run the trusted MANET.

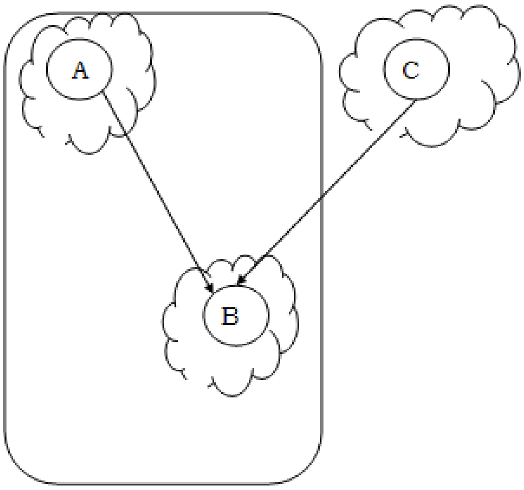

Figure 1(b) Network Scenario With Cluster

3. After events such as add/remove nodes to/from a cluster, or permanent closing for protection or optimizing a user, cluster head can verify whether or not authentication service secures its computing by cluster head verification.

4. Searching of New cluster head before their time out on the basis of following parameter

   a. New node should have minimum work load responsibility

   b. New node should be easily reachable over cluster area.

   c. Existing cluster head hand over their responsibly and remain the cluster head during Swaping.

4. Result Analysis

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

True Detection Rate: - Proposed methodology use K-Means which return high TDR Rate as compare with existing approach by using Machine Learning Technique.

The performance of an intrusion detection system may be evaluated in terms of TD (True Detection) rate and FD (False Detection rate) rate. TD 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

TDR= P (A| I) …………. (1)

Similarly TD (True negative) rate can be calculated as,

TDR= =P (-A|I) …………. (2)

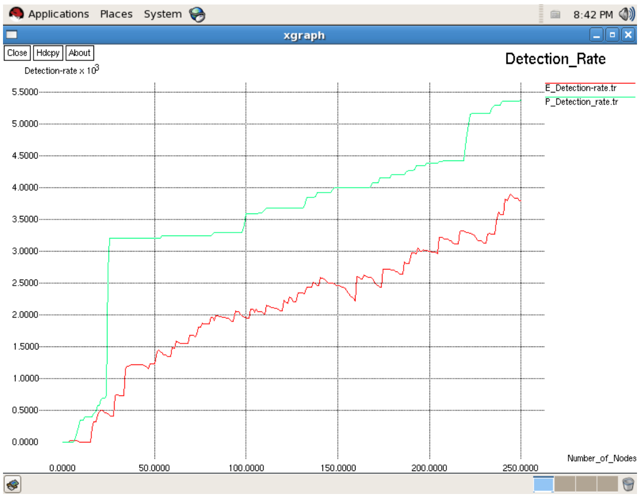

Figure 2 True Detection Rate Comparison

FD (False detection) rate occurs when the system wrongfully classifies normal patterns as abnormal patterns. In this experiment, FD rate is calculated as the number of false Detection created by the system, divided by the total number of self-antigens.

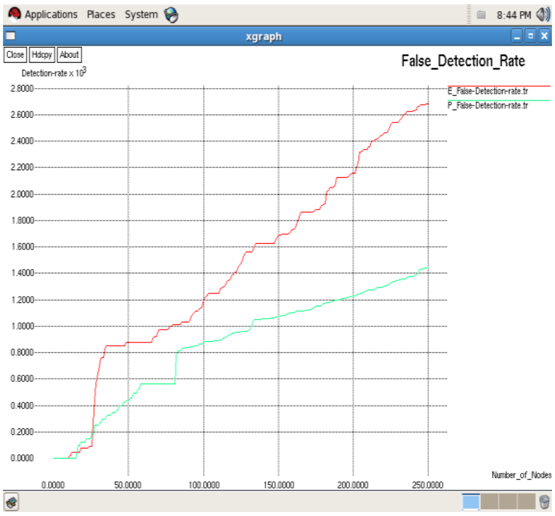

Figure 3 False Detection rate of Proposed Protocol and Existing Protocol

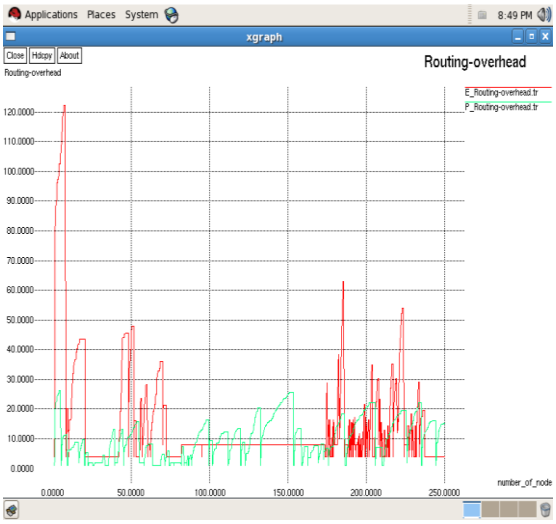

Figure 4 Routing Load of Proposed Protocol and Existing Protocol

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 .

Resident Energy:- 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 and increase Resident energy.

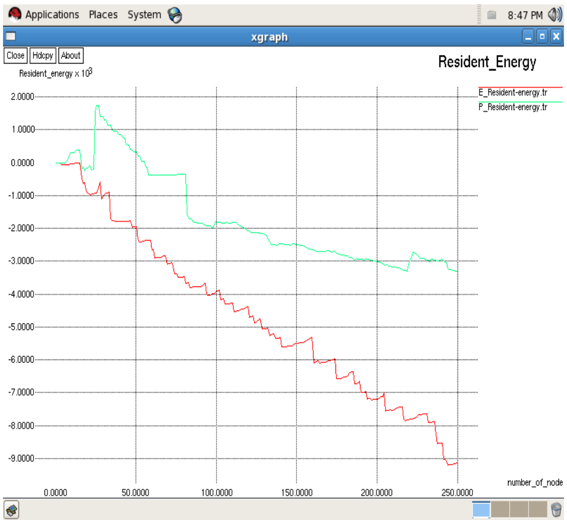

Figure 5 Resident Energy of network in Proposed Protocol and Existing Protocol

5. Conclusion

As rapid increase in unauthorized activities and abuse of computer system by both system insider and external intruder trends to increase the degree of network security. In order to increase network security various technique has been proposed but having a deficiency over IDS system in some of the situation i.e. if correlation alarm is not precise, reduction and prevention of false positive and false negative is high , at last having insufficient measurement of pattern recognition. In order to overcome all these deficiency from IDS, system over network, we propose a novel dual detection of IDS based on supervised clustering that integrating the Game theory and K-means .The Game Theory helps for calculating reliability score and K-means resolves the problem of clustering and cluster head. The simulation results shows that the proposed method has improved the correlation factor, minimizing false +ve and false –ve alarm generation and to increase the efficiency and accuracy of the IDS system. Methodology by using bi-partite graph achieves substantial energy efficiency, as shown through simulation tests, which indicates that methodology by using bi-partite graph outperforms several previously proposed protocols, namely leach. In future work, methodology by using bi-partite graph can be further enhanced by taking into consideration metrics related to QOS and time constraints.

Reference

[1] Zunnun Narmawala, Sanjay Srivastava, "Survey of Applications of Network Coding in Wired and Wireless Networks", in Proceedings of the 14th National Conference on Communications, pp. 153-157, February 2008.

[2] Sheikh, R., Singh Chande, M. and Mishra, D.K., "Security issues in MANET: A review", IEEE 2010, pp 1-4.

[3] Kannhavong, B., Nakayama, H., Nemoto, Y. and Kato, N., "A survey of routing attacks in mobile ad hoc networks", IEEE 2007, pp 85-91.

[4] Verma, M.K. and Joshi, S. Doohan, N. V. "A survey on: An analysis of secure routing of volatile nodes in MANET", IEEE 2012, pp 1-3.

[5] Mariannne. A. Azer, "Wormhole Attacks Mitigation in Ad Hoc Networks", IEEE 2011, pp 561-568.

[6] R. Maheshwari, J. Gao, and S. R. Das, "Detecting Wormhole Attacks In Wireless Networks Using Connectivity Information", in Proc. of IEEE INFOCOM, 2007.

[7] Ali Modirkhazeni, Saeedeh Aghamahmoodi, Arsalan Modirkhazeni and Naghmeh Niknejad, "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks", IEEE 2011, pp 122-128.

[8] Ronggong Song, Peter C. Mason and Ming Li, "Enhancement of Frequency-based Wormhole Attack Detection", IEEE 2011, pp 1139-1145

[9] S. A. Razak, S. M. Furnell and P. J. Brooke, "Attacks against Mobile Ad Hoc Networks Routing Protocols", School of Computing 2004.

[10] Xiangyang Li "Wireless Ad Hoc and Sensor Networks: Theory and Applications", Cambridge University Press 978-0-521-86523-4

[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.

[19] Xu Su and Rajendra V. Boppana, "On Mitigating In-band Wormhole Attacks in Mobile Ad Hoc Networks", IEEE 2007, pp 1136-1141.

[20] Dang Quan Nguyen and Louise Lamont "A Simple and Efficient Detection of Wormhole Attacks", IEEE 2008, pp 1-5.