A SURVEY ON INTRUSION DETECTION IN MANETs.

P.BakeyaLakshmi,
Research Scholar,
Dept Of Computer Science,
Sri Ramakrishna College Of Arts
And Science For Women,
Coimbatore, India.
harunya17@gmail.com

Mrs.K.Santhi
Assistant Professor,
Dept Of Computer Science,
Sri Ramakrishna College Of Arts
And Science For Women,
Coimbatore, India.
santhi_visu@yahoo.com

ABSTRACT:

A mobile ad hoc network is an infrastructureless network that changes its links dynamically, which makes routing in MANET a difficult process. As Mobile Ad-Hoc Network (MANET) has become a very important technology, research concerning its security problem, especially, in intrusion detection has attracted many researchers. Feature selection methodology plays a vital role in the data analysis process. PCA is used to analyze the selected features. This is because, redundant and irrelevant features often reduce performance of the intrusion detection system. It performs better in increasing speed and predictive accuracy. This survey aims to select and analyze the network features using principal component analysis. While performing various experiments, normal and attack states are simulated and the results for the selected features are analyzed.

Keywords: Feature Selection, Intrusion Detection, MANET, PCA.

1. INTRODUCTION:

Mobile Ad-hoc network (MANET) is an unstructured wireless network that can be established temporarily. In MANET, node can add-in to the network are detach from it any time. Thus, there is no central control on the network from the nodes to follow. This paper proposes a neighbor monitoring intrusion detection based on the traffic profile of the node, where feature selection is used to improve its performance. This survey approach uses with various intrusion detection method. In ad-hoc networks, packets that are sent from each node can be used for network condition monitoring.

Intrusion detection can be defined as a process of monitoring activities in a system. The mechanism by which this is achieved is called an intrusion detection system (IDS). An IDS collects activity information and then analyzes it to determine whether there are any activities that violate the security rules. Once an IDS determines that an unusual activity or an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator. In addition, IDS can also initiate a proper response to the malicious activity.

The following section provides a brief summary of the most relevant mechanisms for intrusion detection on PCA in MANET. Then the final section is concluded.

BACKGROUND STUDY:

[AMC, 04] [1] This paper propose a general method to diagnose anomalies. This method is based on a separation of the high-dimensional space occupied by a set of network traffic measurements into disjoint subspaces corresponding to normal and anomalous network conditions. They show that this separation can be performed effectively by Principal Component Analysis. Using only simple traffic measurements from links, They study volume anomalies and show that the method can: (1) accurately detect when a volume anomaly is occurring; (2) correctly identify the underlying origin-destination (OD) flow which is the source of the anomaly; and (3) accurately estimate the amount of traffic involved in the anomalous OD flow.

[ASS, 03] [2] The intrusion detection community has been concentrating mainly on wired networks. Techniques geared towards wireline networks would not suffice for an environment consisting of multihop wireless links because of the various differences such as lack of fixed infrastructure, mobility, the ease of listening to wireless transmissions, lack of clear separation between normal and abnormal behavior in ad hoc networks, and consider the signature detection technique and investigate the ability of various routing protocols to facilitate intrusion detection when the attack signatures are completely known. Show that reactive ad-hoc routing protocols suffer from a serious problem due to which it might be difficult to detect intrusions even in the absence of mobility. Mobility makes the problem of detecting intruders harder. Also investigate a relationship between the probability of detecting an intrusion and the number of nodes that must participate in the process of detecting intrusions.

[CP, 07] [3] In this paper, an anomaly detection approach that fuses data gathered from different nodes in a distributed sensor network is proposed and evaluated. The emphasis of this work is placed on the data integrity and accuracy problem caused by compromised or malfunctioning nodes. The proposed approach utilizes and applies Principal Component Analysis simultaneously on multiple metrics received from various sensors. One of the key features of the proposed approach is that it provides an integrated methodology of taking into consideration and combining effectively correlated sensor data, in a distributed fashion, in order to reveal anomalies that span through a number of neighboring sensors. The efficiency and effectiveness of the proposed approach is demonstrated for a real use case that utilizes meteorological data collected from a distributed set of sensor nodes.

[CMCM, 06] [4] Security is a critical challenge for creating robust and reliable sensor networks. For example, routing attacks have the ability to disconnect a sensor network from its central base station. In this paper, they present a method for intrusion detection in wireless sensor networks. This intrusion detection scheme uses a clustering algorithm to build a model of normal traffic behavior, and then uses this model of normal traffic to detect abnormal traffic patterns.

[FR, 08] [5] This paper presents, theoretical overview of intrusion detection and a new approach for intrusion detection based on adaptive Bayesian algorithm. This algorithm correctly classify different types of attack of KDD99 benchmark intrusion detection dataset with high detection accuracy in short response time. The experimental result also shows that, this algorithm maximize the detection rate (DR) and minimized the false positive rate (FPR) for intrusion detection.

[FSGSTYZ, 02] [6] This paper presents a new approach that combines specification-based and anomaly-based intrusion detection, mitigating the weaknesses of the two approaches while magnifying their strengths. The approach begins with state-machine specifications of network protocols, and augments these state machines with information about statistics that need to be maintained to detect anomalies. They present a specification language in which all of this information can be captured in a succinct manner. Feature selection was a crucial step that required a great deal of expertise and insight in the case of previous anomaly detection approaches.

[HFSL, 04] [7] In this paper they present a Statistical En-route Filtering (SEF) mechanism that can detect and drop such false reports. SEF requires that each sensing report be validated by multiple keyed message authentication des (MACS), each generated by a node that detects the same event. As the report is forwarded, each node along the way verifies the correctness of the MACS probabilistically and drops those with invalid MACs at earliest points. The sink further filters out remaining false reports that escape the en-route filtering. SEF exploits the network scale to determine the truthfulness of each report through collective decision-making by multiple detecting nodes and collective false-report detection by multiple forwarding nodes.

[HK, 99] [8] In this n length subsequences are extracted from the training set and the are assigned a probability given, P(subsequence) = Frequency (subsequence) / total number of subsequences During prediction the test sequence windows are looked up in stored model and assigned corresponding probabilities. If the window had never occurred in the training data then it is given a zero probability score. Now the sequence of symbols gets converted to a sequence of probabilities. These probabilities need to be combined to get an anomaly score. Different combining methodologies were checked but log average was found to be superior.

[JJ, 2000] **[9]** This paper discuss various generalizations of neural PCA (Principal Component Analysis)-type learning algorithms containing nonlinearities using optimization-based approach. Standard PCA arises as an optimal solution to several different information representation problems, and justify that this is essentially due to the fact that the solution is based on the second-order statistics only. If the respective optimization problems are generalized for nonquadratic criteria so that higher-order statistics are taken into account, their solutions will in general be different. The solutions define in a natural way several meaningful extensions of PCA and give a solid foundation for them.In this framework, the study more closely generalizations of the problems of variance maximization and mean-square error minimization. For these problems, the derive gradient-type neural learning algorithms both for symmetric and hierarchic PCA-type networks. As an important special case, the well-known Sanger's generalized Hebbian algorithm (GHA) is shown to emerge from natural optimization problems.

[KW, 97] **[10]** In this n+1 length windows are extracted from the entire training data. The first n length subsequences are used to form states and the transition probability is attached to each symbol (using the last symbol). Thus while evaluating new test sequences every event is the sequence is assigned a probability by looking at its history and looking up for the corresponding transition probability in the FSA table. Now the sequence of symbols gets converted to a sequence of probabilities. These probabilities need to be combined to get an anomaly score. Different combining methodologies were checked but log average was found to be superior.

[ML, 96] **[11]** This paper introduces ADHOC, a tool that integrates statistical methods and machine learning techniques to perform effective feature selection. Feature selection plays a central role in the data analysis process since redundant and irrelevant features often degrade the performance of induction algorithms, both in speed and predictive accuracy. ADHOC combines the advantages of both Jilter and feedback approaches to feature selection to enhance the understanding of the given data and increase the efficiency of the feature selection process and report results of extensive experiments on real world data which demonstrate the effectiveness of ADHOC as data reduction technique as well as feature selection method. ADHOC has been employed in the analysis of several corporate databases. In particular, it is currently used to support the difficult task of early estimating the cost of software projects.

[MHRJ, 2000] [12] In this approach each point computes the density of its local neighborhood. Compute local outlier factor (LOF) of a sample *p* as the average of the ratios of the density of sample *p* and the density of its nearest neighbors Outliers are points with largest LOF value. Outliers are points with largest LOF value.

[PM, 09] [13] The goal of PCA is to reduce the dimensionality of a data set in which there are a large number of interrelated variables, while retaining as much as possible of the variation present in the data set .The extracted non correlated components are estimated from the eigenvectors of the covariance matrix of the original variables. The objective of the anomaly detection algorithm is to provide an efficient and effective methodology of fusing and combining data of heterogeneous monitors that spread throughout the network, in order to provide a generalized framework, capable of detecting a wide range of classes of anomalies, such as the ones created randomly by faulty nodes or others that result from coordinated compromised nodes. In this work, this is achieved by applying a PCA-based approach simultaneously on one or more monitored metrics.

[SA, 05] [14] This paper introduces a new approach that addresses data contamination problems from attacks in unattended wireless sensor networks. They propose a sliding-window based spatio-temporal correlation analysis called Abnormal Relationships Test (ART)" to effectively detect, respond and immune to inserted spoofed data from both various-ID impersonators and compromised nodes. Also a systematic approach is given to identify the appropriate sliding window size and correlation coefficient threshold. The study shows that correlation property of observed phenomenon is not always transitive, different phenomenon from same set of nodes at the same or different period of time can have different correlation coefficients.

[SNKJN, 07] [15] This paper analyzes the blackhole attack which is one of the possible attacks in ad hoc networks. In a blackhole attack, a malicious node impersonates a destination node by sending a spoofed route reply packet to a source node that initiates a route discovery. By doing this, the malicious node can deprive the traffic from the source node. In order to prevent this kind of attack, it is crucial to detect the abnormality occurs during the attack. In conventional schemes, anomaly detection is achieved by defining the normal state from static training data. However, in mobile ad hoc networks where the network topology dynamically changes, such static training method could not be used efficiently. This paper, propose an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals. The simulation results show the effectiveness of our scheme compared with conventional scheme.

[ST, 07] [16] Recently data mining methods have gained importance in addressing network security issues, including network intrusion detection — a challenging task in network security. Intrusion detection systems aim to identify attacks with a high detection rate and a low false alarm rate. Classification-based data mining models for intrusion detection are often ineffective in dealing with dynamic changes in intrusion patterns and characteristics. Consequently, unsupervised learning methods have been given a closer look for network intrusion detection. While investigate multiple centroid-based unsupervised clustering algorithms for intrusion detection, and propose a simple yet effective self-labeling heuristic for detecting attack and normal clusters of network traffic audit data. The clustering algorithms investigated include, k-means, Mixture-Of-Spherical Gaussians, Self-Organizing Map, and Neural-Gas. The network traffic datasets provided by the DARPA 1998 offline intrusion detection project are used in our empirical investigation, which demonstrates the feasibility and promise of unsupervised learning methods for network intrusion detection. In addition, a comparative analysis shows the advantage of clustering-based methods over supervised classification techniques in identifying new or unseen attack types.

[SCMJ, 06] [17] Identifying misbehaviors is an important challenge for monitoring, fault diagnosis and intrusion detection in wireless sensor networks. A key problem is how to minimize the communication overhead and energy consumption in the network when identifying misbehaviors. The approach to this problem is based on a distributed, cluster-based anomaly detection algorithm. While minimize the communication overhead by clustering the sensor measurements and merging clusters before sending a description of the clusters to the other nodes.

[TDVD, 03] [18] In this work, they propose a technique for online deviation detection in streaming data. They discuss how these techniques can operate efficiently in the distributed environment of a sensor network, and discuss the tradeoffs that arise in this setting.

The techniques process as much of the data as possible in a decentralized fashion, so as to avoid unnecessary communication and computational effort. An interesting problem which has not been adequately addressed so far is that of distributed online deviation detection in streaming data. The identification of deviating values provides an efficient way to focus on the interesting events in the sensor network.

[TW, 05] [19] As Mobile ad-hoc network (MANET) has become a very important technology the security problem, especially, intrusion detection technique research has attracted many people’s effort. MANET is more vulnerable than wired network and suffers intrusion like wired network. This paper investigated some intrusion detection techniques using machine learning and proposed a profile based neighbor monitoring intrusion detection method. Further analysis shows that the features collected by each node are too many for wireless devices with limited capacity, and can apply Markov Blanket algorithm to the feature selection of the intrusion detection method. Experimental studies have shown that Markov Blanket algorithm can decrease the number of features dramatically with very similar detection rate.

[WH, 03] [20] Mobile ad hoc networking (MANET) has become an exciting and important technology in recent years because of the rapid proliferation of wireless devices. MANETs are highly vulnerable to attacks due to the open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. In this paper, report our progress in developing intrusion detection (ID) capabilities for MANET. Building on our prior work on anomaly detection, and investigate how to improve the anomaly detection approach to provide more details on attack types and sources. For several well-known attacks, can apply a simple rule to identify the attack type when an anomaly is reported. In some cases, these rules can also help identify the attackers. Address the run-time resource constraint problem using a cluster-based detection scheme where periodically a node is elected as the ID agent for a cluster. Compared with the scheme where each node is its own ID agent, this scheme is much more efficient while maintaining the same level of effectiveness.

[XW, 05] [21] The underlying hypothesis of this class of technique is that the next event can be predicted by looking at a short history of past events. They use the short memory property of sequences which has been shown to exist across domains. The history window can be fixed or variable. Length of the window is n.

[YFLY, 03] [22] With the proliferation of wireless devices, mobile ad hoc networking (MANET) has become a very exciting and important technology due to its characteristics of open medium and dynamic topology among others. However, MANETs are more vulnerable than wired networks. Existing security mechanisms developed for wired networks need be redesigned for MANET. In this paper, discuss the problem of intrusion detection in MANET. The focus of our research is on techniques for automatically constructing anomaly detection models that are capable of detecting new (or unknown) attacks. Introduce a new data mining method that uses “cross-feature analysis” to capture the inter-feature correlation patterns in normal traffic. These patterns can be used as normal profiles to detect deviation (or anomalies) caused by attacks, and implemented method with two well known ad-hoc routing protocols, namely, Dynamic Source Routing (DSR) and Ad-hoc On-Demand Distance Vector (AODV), and have conducted extensive experiments using the ns-2 simulator. The results show that the anomaly detection models automatically computed using our data mining method can effectively detect the anomalies caused by representative intrusions.

[YR, 02] [23] A new approach, based on the k-NearestNeighbor (kNN) classifier, is used to classify program behavior as normal or intrusive. Program behavior, in turn, is represented by frequencies of system calls. Each system call is treated as a word and the collection of system calls over each program execution as a document, then classified using kNN classifier, a popular method in text categorization. This method seems to offer some computational advantages over those that seek to characterize program behavior with short sequences of system calls and generate individual program profiles. Preliminary experiments show that the kNN classifier can effectively detect intrusive attacks and achieve a low false positive rate.

[YWY, 03] [24] has examine the vulnerabilities of wireless networks and argue that must include intrusion detection in the security architecture for mobile computing environment, and developed an architecture and evaluated a key mechanism in this architecture, anomaly detection for mobile ad-hoc network, through simulation experiments. To build anomaly detection models for mobile wireless networks. Detection based on activities in different network layers may differ in the format and the amount of available audit data as well as the modeling algorithms.

[YZX, 05] [25] The research on distributed intrusion detection system (DIDS) is a rapidly growing area of interest because the existence of centralized intrusion detection system (IDS) techniques is increasingly unable to protect the global distributed information infrastructure. Distributed analysis employed by Agent-based DIDS is an accepted fabulous method. Clustering-based intrusion detection technique overcomes the drawbacks of relying on labeled training data which most current anomaly-based intrusion detection depend on. Clustering-based DIDS technique according to the advantages of two techniques is presented. For effectively choosing the attacks, twice clustering is employed: the first clustering is to choose the candidate anomalies at Agent IDS and the second clustering is to choose the true attack at central IDS. At last, through experiment on the KDD CUP 1999 data records of network connections verified that the methods put forward is better.

CONCLUSION:

In this survey, we focused on Intrusion detection in MANETs and also the various way to find the Intrusion. And also PCA techniques to find Intrusion detection. And provide the various techniques to find Intrusion Detection.

REFERENCES:

[1]. [**AMC, 04**] Anukool Lakhina, Mark Crovella, and Christophe Diot, “Diagnosing Network wide Traffic Anomalies,” International Journal of Networks Security, Vol.12, No.1, PP.42-49, Feb 2004.

[2]. [**ASS, 03**] Anjum, D.Subhadrabandhu, and S.Sarkar, “ Signature-based intrusion detection for wireless Ad-hoc networks," Proceedings of Vehicular Technology Conference, vol. 3, pp. 2152-2156, USA, Oct. 2003.

[3]. [**CP, 07**] Chatzigiannakis,V and Papavassiliou, S,“Diagnosing Anomalies and Identifying Faulty Nodes in Sensor Networks”, Sensor Journal, IEEE,Vol.7, Issue.5,PP.637 – 645, May 2007.

[4]. [**CMCM, 06**] Chong Eik Loo, Mun Yong Ng, Christopher Leckie, and Marimuthu Palaniswami, “Intrusion Detection for Routing Attacks in Sensor Networks,” International Journal of Distributed Sensor Networks, V.2, PP. 313–332, 2006.

[5]. [**FR, 08**] D.M.Farid, and M.Z Rahman, “Learning intrusion detection based on adaptive Bayesian algorithm," 11th International Conference on Computer and Information Technology (ICCIT2008), pp. 652-656, 2008.

[6]. [**FSGSTYZ, 02**] J.Frullo, R.Sekar, A.Gupta, T.Shanbhag, A.Tiwary, H.Yang, and S.Zhou, “Specifcation-based anomaly detection: A new approach for detecting network intrusions," Proceedings of the 9th ACM Conference on Computer and Communication Security, pp. 265-274, USA, 2002.

[7]. [**HFSL, 04**] Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang, "Statistical En-route Detection and Filtering of Injected False Data in Sensor Networks", UCLA Computer Science Department, Los Angeles,2004.

[8]. [**HK, 99**] Hyeon-Kyn Lee, and Kim,J.H, "An HMM-Based Threshold Model Approach For Gesture Recognition," Pattern Analysis and Machine Intelligence, IEEE Transaction, Vol.21, Issue.10, PP.961-973, Oct 1999.

[9]. [**JJ, 2000**] Juha Karhunen and Jyrki Joutsensalo, "Generalizations of Principal Component analysis, Optimization problems, and Neural Networks," Helsinki University Of Technology, Finland, Vol.8, Issue.4, PP. 549-562, April 2000.

[10]. [**KW, 97**] Kondacs.A and Watrous.J, "Power Of Quantum Finite State Automata," Foundations of Computer Science, Proceedings, PP. 66-75, Oct 1997.

[11]. [**ML, 96**] M.Marco Richeldi, and P. L. Lanzit, "ADHOC: A tool for performing effective feature selection," Proceedings eighth IEEE international conference on tools with Artificial Intelligence, pp. 102-105, 1996.

[12]. [**MHRJ, 2000**] Markus M. Breunig, Hans-Peter Kriegel, Raymond T. Ng, and Jörg Sander, "LOF:Identifying Density-Based Local Outliers," MOD 2000, Dallas, TX USA, ACM 2000.

[13]. [**PM, 09**] Peyman Kabiri and Mehran Aghaei, "Feature Analysis for Intrusion Detection in Mobile Ad-hoc Networks," International Journal of Network Security, Vol.12, No.1, PP.4249, Jan. 2011.

[14]. [**SA, 05**] Sapon Tanachaiwiwat and Ahmed Helmy, "Correlation Analysis for Alleviating Effects of Inserted Data in Wireless Sensor Networks," Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services,2005.

[15]. [**SNKJN, 07**] S.Satoshi Kurosawa, H.Nakayama, N.Kato, A.Jamalipour,and Y.Nemoto, "Detecting blackhole attack on AODV-based mobile ad-hoc networks by dynamic learning," International Journal of Network Security, vol. 5, no. 3, pp. 338-346, 2007.

[16]. [**ST, 07**] Shi Zhong And Taghi M. Khoshgoftaar, "Clustering-Based Network Intrusion Detection", International Journal Of Reliability, Quality And Safety Engineering, Vol. 14, No. 2, PP.169–187, 2007.

[17]. [**SCMJ, 06**] Sutharshan Rajasegara1, Christopher Leckie, Marimuthu Palaniswami, and James C. Bezdek "Distributed Anomaly Detection In Wireless Sensor Networks," Computer Science Department University of West Florida USA, 2006.

[18]. [**TDVD, 03**] Themistoklis Palpanas, Dimitris Papadopoulos, Vana Kalogeraki, and Dimitrios Gunopulos, "Distributed Deviation Detection in Sensor Networks," SIGMOD Record, Vol. 32, No. 4, December 2003.

[19]. [**TW, 05**] T.Tu-Liang Lin, and J. Wong, "Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network," Technical Report, Computer Science, Iowa State University, USA, 2005.

[20]. [**WH, 03**] Wenke Lee, Y.A.Huang, and "A Cooperative Intrusion Detection System for Ad Hoc Networks," Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN' 03), pp. 135-147, USA, 2003.

[21]. [**XW, 05**] Xia Wang, and J. Wong, "Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network," Technical Report, Computer Science, Iowa State University, USA, 2005.

[22]. [**YFLY, 03**] Yi-An Huang, W. Fan, W. Lee, and P. S. Yu, " Cross-feature analysis for detecting ad-hoc routing anomalies," Proceedings of The 23rd International

Conference on Distributed Computing Systems (ICDCS), pp. 478-487, USA, 2003.

[23]. [**YR, 02**] Yihua Liao, and V.Rao Vemuri, "Use Of K-Nearest Neighbor Classifier For Intrusion Detection," Department of Computer Science University of California, Davis One Shields Avenue, Davis, CA 95616, USA, July 2002.

[24]. [**YWY, 03**] Yongguang Zhang, Wenke Lee And Yi-An Huang, "Intrusion Detection Techniques For Mobile Wireless Networks," Wireless Networks,Vol. 9, Pp.545–556, 2003.

[25]. [**YZX, 05**] Yu-Fang Zhang, Zhong-Yang Xiong, and Xiu-Qiong Wang, " Distributed Intrusion Detection Based On Clustering," Proceedings OF THE Fourth International Conference ON Machine Learning AND Cybernetics, Guangzhou, Pp.18-21 August 2005.

BAKEYALAKSHMI.P received the B.Sc (Computer Science) degree from the Department of Computer Science at Bharathiar University, Coimbatore, India, the M.Sc (Information Technology) degree from the Department of Computer Science at the Anna University, Erode, India, and she perusing her Master of philosophy in Computer Science at Bharathiar University, Coimbatore, India.