Srikanth.Gangadhara,Anup Kumar.M/ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 1, Issue 3, pp.874-878

Implementation of Intrusion Recognition System In Distributed Systems.

[1]Srikanth.Gangadhara, [2]Anup Kumar.M
[1]Department of Computer Science & Information Technology, Jyothishmathi Institute of Tech & Sciences, JNTU, Hyderabad, AP, INDIA.
[2]Department of Computer Science & Information Technology, Jyothishmathi Institute of Tech & Sciences, JNTU, Hyderabad, AP, INDIA.

ABSTRACT
Modern networks routinely drop packets when the load temporarily exceeds their buffering capacities. It is quite challenging to attribute a missing packet to a malevolent action because normal network congestion cannot produce the same effect. One of the primary challenges in intrusion recognition is modeling typical application behavior, so that we can recognize attacks by their atypical effects without raising too many false alarms. IDS implemented using mobile agents is one of the new paradigms for intrusion recognition. In this paper, we have proposed an effective intrusion identification system in which local agent collects data from its own system and it classifies anomaly behaviors using SVM classifier. Each local agent is capable of removing the host system from the network on successful recognition of attacks. The mobile agent gathers information from the local agent before it allows the system to send data. Our system identifies successful attacks from the anomaly behaviors.

Keywords-Distributed Systems, Mobile Agents, Intrusion recognition system, Network security, multiple packet losses.

I. INTRODUCTION
Intrusion recognition is used to secure the systems in the networks by comparing the set of baselines of the system with the present behavior of the system Therefore; we can characterize normal and abnormal behavior of the system. Researchers have developed distributed protocols to detect such manipulations by validating that the traffic transmitted by one router is received unmodified by another router.

Puttinietal(2006) propose a parametrical mixture model used for behavior modeling from reference data. Cabreraetal (2008) proposed the solution for intrusion recognition in MANET's utilizing ensemble methods. .

Subhadrabandhu and Sarkar (2008) proposed the signature recognition technique which investigates the ability of various routing protocols to facilitate intrusion recognition when the attack signatures are completely known.

Bhuse and Gupta(2006) proposed light weight methods to detect anomaly intrusions inwirelesssensors.

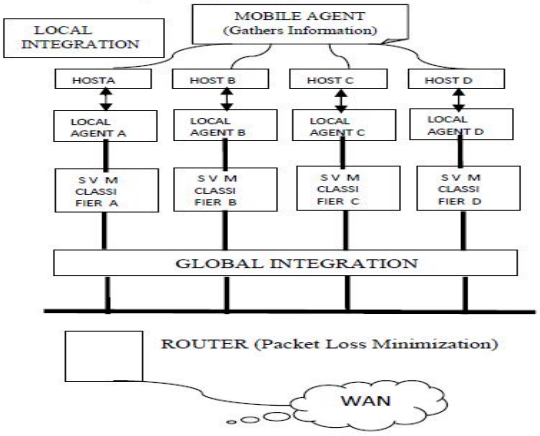
Dengetal(2008) proposed the underlying distributed and cooperative nature of wireless ad hoc networks and adds one more dimensions to the intrusion recognition process. Bo Sun et al. (2006) proposed an adaptive Scheme in which suitable normal profiles and corresponding proper thresholds can be selected adaptively by each local ID by periodically measuring its local link change rate. Cheneta (2007) proposed light weight anomaly intrusions recognition in which investigates different key features for wsn's and define some rules for building efficient and accurate intrusion recognition system.

Liuet al (2006) proposed game theoretic framework to analyze the interactions between pairs of attacking or defending nodes using a Bayesian formulation. In this paper, a new attempt has been worked out effectively against attacks in wireless networks. With the help of local agents and mobile agents, it gathers information from its own systems and also neighboring system to identify any attacks that has been made in that network.

Fault-tolerant forwarding has been proposed by Perlman (1988) who developed a routing system

based on source routing which uses digitally signed route setup Packets and reserved buffers. When packet loss due to congestion can be inferred then remaining packet loss may be due to malicious actions. Our system also removes the ambiguity in packet losses due to congestion and therefore the subsequent packet losses can by safely inferred as packet loss due to malicious actions.

Fig. 1. Proposed system architecture.



II.CONCEPT

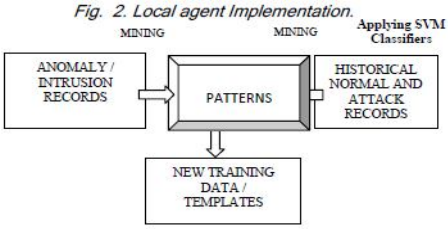
The concept is implemented on anomaly based method. The architecture of the system to prevent the attacks in networks is shown in Fig1.

Mobile agent: In order to use mobile agents, all the hosts in the networks must have an agent platform installed, where the agents are going to be executed.

Local agent: Local agent is implemented in every system in the network which gathers information about its system in (Fig. 2). The main functions of local agent are

1. It monitors its own system and its environment dynamically. It uses SVM classifier to find out the local anomaly.
2. Whenever a node wants to transfer information to another node, it broadcasts the message to its neighboring nodes.
3. It gathers neighboring nodes information using mobile agents. It then calls the SVM classifier to find out the attacks with the help of trained test data.
4. It provides same type of security solution throughout the network.

Fig. 2. Local agent Implementation.



III.FUNCTIONALITY

Classification in current node: Local agent is present in this system and it continuously monitors its own system if an attacker packet arrives at this system to gather Information, it calls SVM classifier to find out attacks.

Gathering Information from

Neighboring node: Whenever any system transfers information to some other system in the network, it broadcast through intermediate systems. Before transferring message, it sends the mobile agent to the neighboring node gathers information from that node and it return back to the system.

Data collection: Data collection module is included for each intrusion recognition subsystem to collect the values of features, and then normal profile is created using the normal scenario and attack profile is created during the attack scenario.

Data Preprocess: Data preprocess is a technique to process the information with the test train data. The audit data is stored in a file and it is smoothed so that it can be used for anomaly recognition.

Local Integration**:** Local Integration module concentrates on self system to find out the local anomaly attacks. Every system under that network follows the same methodology to provide secure global networks.

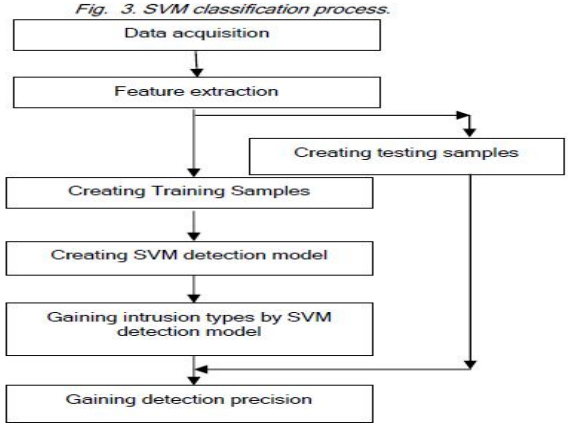
Global Integration: Global Integration module is used to find the intrusion result for entire network. It is used to find the status of neighboring nodes before taking decisions towards forwarding messages.

Packet loss minimization mechanism: The necessary traffic information has to be distributed among the routers and a distributed recognition protocol has to be implemented. Every outbound interface queue Q is monitored by the neighboring routers.

IV.IMPLEMENTATION

Qdir is either Qin, meaning traffic into Q, or Qout, meaning traffic out of Q as Tinfo (rs, Qdir,π,τ).
Assume that for a given Q, the routers involved in detecting compromised routers are shown below.
• rs – Which sends traffic into Q and which collects the traffic information Tinfo (rs, Qin, < rs , r , rd>, τ)
• r – which hosts Q and which collects the traffic information info (r, Qin, < rs , r , rd>, τ)
Qout, < r , rd>, τ)
Recognition at r: Let α be the upper bound on the time to forward traffic information
• If r does not receive traffic information from rs, withinα, then r detects < rs,r> as traffic faulty.•On receiving traffic information from rs, router r verifies the signature and then it forwards the information Tinfo (rs, Qin, < rs, r, rd>,τ) router rd. If not then r detects < rs, r> segment as traffic faulty. In this case it forwards its own copy of traffic information Tinfo (r, Qin, < rs, r, rd>,τ) to router rd.
Recognition at rd :
• If rd does not receive traffic information from r, originated by rs , it expects r to broadcast the recognition <rs , r>. If not then router rd detects <r,rd >as traffic
faulty. On receiving the traffic information forwarded from r, rd checks the signature for integrity and authenticity and then evaluates the information received.
SVM classifiers: Support vector machines (SVM) are a set of related supervised learning methods that analyze data and recognize patterns, used for classification and regression analysis.SVM delivers a unique solution, since the optimality problem is convex. This is an advantage compared to Neural Networks, which have multiple solutions associated with local minima and for this reason may not be robust over different samples.SVM are a set of related supervised learning methods that analyze data and recognize patterns, used for classification and regression analysis. Since SVM is a classifier, then given a set of training examples, each marked as belonging to one of two categories, an SVM training algorithm builds a model that predicts whether a new example falls into one category or the other. The working of SVM classifier is given in Fig. 3. An SVM model is a representation of the
examples as points in space, mapped so that the examples of the separate categories are divided by a Clear gap that is as wide as possible. Fig. 4 shows supervised and unsupervised model generation

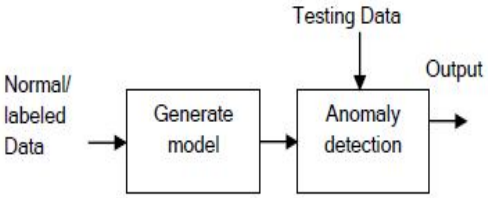
Fig. 3. SVM classification process.



Conventional pattern recognition systems have 2 components: Feature analysis and pattern classification.
Feature analysis is achieved in 2 steps: parameter extraction step and feature extraction step. In the parameter extraction step, information relevant for pattern
Classification is extracted from the input data in the form of parameter vector. In the feature extraction step, the parameter vector is transformed to a feature vector.
Feature extraction can be conducted independently or jointly with either parameter extraction or classification.
Linear discriminant analysis (LDA) and principal component analysis (PCA) are the two popular independent feature extraction algorithms. Both of them extract features by projecting the parameter vectors into a new feature space through a linear transformation matrix. But they optimize the transformation matrix with different intentions.PCA optimizes the transformation matrix by finding the largest variations in the original feature space.LDA pursues the largest ratio of between-class variation and within-class variation when projecting the original feature space to a subspace. SVM is a recently developed integrated pattern classification algorithm with non-linear formulation.
Because of this, SVM has the advantage that it can handle the classes with complex nonlinear decision

boundaries. However, SVM is a highly integrated and closed pattern classification system.

Fig. 4. Supervised & unsupervised generation in anomaly detection system.



Training mode

Input: The file containing the features values logged during the learning phase
Output: files containing the mean, standard deviations and inverse matrices of feature set.
Begin
for i =1 to Num.of week days do
for j =1 to Num. of hours in a day do
Read the feature values logged during learning phase;
For k =1 to Num. of network features do
Find sum of the values corresponding to the same hour and day of the week;
Compute Average values and standard deviation for each feature;
Compute where n is the total number of features
Compute the Determinant of above covariance matrices
If Determinant ≤ 0
Consider the neighboring covariance matrix having positive Determinant.
Compute inverse matrix corresponding to each covariance matrix
End
Recognition mode:
Input: The file containing the network profile
Output: Sends alert in case an event is detected as intrusion.
Begin
for i =1 to Num .of week days do
for j =1 to Num. of hours in a day do
for k =1 to Num. of network features do
Read Average values and standard deviation for each feature;
Read the inverse matrices
Read the determinant matrix corresponding to each inverse matrix
Compute ($\mu \pm \sigma$) for each parameter
If($\mu - \sigma > x > \mu - \sigma$) then
x is intrusive
Compute T2= $(X - \mu)$ S-1 $(X - \mu)$ T
If T2 exceeds, the threshold flag alerts
Compute gI (X) = - ½ ln |S| - ½ $(X-\mu)$T S-1 $(X-\mu)$ + ln p(l)
If gi (X) exceeds the threshold flag alerts.

End Results. Our results are compared with other recently published results in Table 1. Which shows the proposed system is greatly competitive with others. The recognition rate of anomaly in our proposed system is high and it encourages the system. The percentage of anomaly recognition is calculated as follows:
No. of Predicted abnormal class
% of anomaly recognition = X 100
Total No. of traces
This system can act as Intrusion prevention system to detect and prevent the attacks. This system can be able to stop a number of attacks as well as the false positive rate of the proposed system is low.

V.CONCLUSION

This paper provides a strong platform to detect anomalies. The proposed system is cooperative and distributive; it considers the anomaly recognition result from the neighbor nodes and sends the current nodes result to its neighbor nodes. This system can be able to stop a number of attacks as well as the false positive rate of the proposed system is low. We also met One of the primary challenges in intrusion recognition is modeling typical application behavior, so that we can recognize attacks by their atypical effects without raising too many false alarms**.** we have determined
The necessary traffic information has to be distributed among the routers and a distributed recognition protocol has to be implemented. When packet loss due to congestion can be inferred then remaining packet loss may be due to malicious actions. Our system also removes the ambiguity in packet losses due to congestion and therefore the subsequent packet losses can by safely inferred as packet loss due to malicious actions.

REFERENCES

[1]. Bhuse V and Gupta A (2006) Anomaly intrusion recognition in wireless sensor networks. High Speed Networks. 15(1), 33–51.
[2]. Bo Sun, Wu K, Xiao Y and Wang R (2006) Integration of mobility and intrusion recognition for wireless ad hoc Networks DOI: 10.1002/dac.853.
[3]. Cabrera D and Gutiérrez C and Raman K. Mehra (2008) Ensemble methods for anomaly recognition and distributed intrusion recognition in mobile Ad-Hoc networks.Elsevier Sci. Publishers.
[4]. Chen H, Han P, Zhou X and Gao C (2007)Lightweight anomaly intrusion recognition in wireless sensor networks. IntelligenceSecurity Informatics.Springerlink.
[5]. Deng H, Xu, R, Li, J, Zhang, F, Levy, R and Lee W (2008) Agent-based cooperative anomaly recognition for wireless ad hoc networks. Parallel Distributed Sys.1, 8.
[6]. Liu Y Comaniciu C and Man H (2006) A Bayesian game approach personal wirelessCommunications.ACM 159593507X.
[7]. Mishra A and Nadkarni K (2003) Security in wireless Ad Hoc networks. CRC press LLC.
[8].Mishra A, Nadkarni K and Animesh Patcha (2004) Intrusion recognition in wireless Ad Hoc networks. IEEE Wireless Commun. pp: 48-60.
[9].Mizrak AT, Cheng YC, Marzullo K and Savage S (2006) Detecting and isolating malicious routers.IEEE Trans. Dependable Secure Computing. 3(3),230-244.
[10].Perlman R (1988) Network layer protocols with byzantine robustness, MIT LCS TR-429.
[11].Puttini R, Hanashiro M, García-Villalba J and Barenco CJ (2006) On the anomaly intrusion-recognition in mobile Ad Hoc network environments. Personal Wireless Commun. Vol. 4217/2006, Springerlink.
[12].Subhadrabandhu FAD and Sarkar S (2008) Signature based intrusion recognition for wireless Ad-Hoc networks: A comparative study of various routing protocols. Seas.
[13].Y.G. Liu, K.F. Chen, X.F. Liao, and W.Zhang (2004) A genetic clustering method for intrusion recognition.Pattern Recognition, 37(5), 927-942.