Indian Journal of Science and Technology Vol.3 No.10 (Oct 2010) ISSN: 0974- 6846

# Distributed and cooperative multi-agent based intrusion detection system

J. Arokia Renjit[1] and K. L. Shunmuganathan[2]

[1]*Department of CSE, Jeppiaar Engineering College, Tamil Nadu, India-600119*
[2]*Department of CSE, RMK Engineering College, Tamil Nadu, India-601 206*
arokiarenjith@gmail.com, Kls_nathan@gmail.com

## Abstract

One of the primary challenges in intrusion detection 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 detection. In this paper, we have proposed an effective intrusion detection 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 detection 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. Experimental results show that the proposed system has high detection rate and low false alarm rate which encourages the proposed system.

**Keywords:**Mobile agents, classification, Intrusion detection system, packet loss, network security

## Introduction

Internet has become an essential tool useful for professionals and private individuals providing a large range of services like entailing, management of bank accounts, reservation of hotels, train time schedules, real time traffic information and internet search. Intrusion detection is used to secure the systems in the networks by comparing the set of baselines of the system with the present behaviorof the system (Mishra *et al.,* 2004). Therefore, we can characterize normal and abnormal behaviorof the system. It is a very difficult to secure routers from attacker. Using a compromised router an attacker may interpose on the traffic stream and manipulate it maliciously to impose attacks like selectively dropping, modifying or rerouting packets. Researchers have developed distributed protocols to detect such manipulations by validating that the traffic transmitted by one router is received unmodified by another router (Mizrak,2006). Intrusion detection is the means of identifying any set of actions that attempt to compromise the integrity, confidentiality or availability of resource(Bradley, 1998). Puttini *et al.*(2006) propose a parametrical mixture model used for behaviormodeling from reference data. Cabrera *et al.* (2008) proposed the solution for intrusion detection in MANET's utilizing ensemble methods. Subhadrabandhu and Sarkar(2008) proposed the signature detection technique which investigates the ability of various routing protocols to facilitate intrusion detection when the attack signatures are completely known. Bhuse and Gupta (2006) proposed light weight methods to detect anomaly intrusions in wireless sensor networks.

Deng *et al.* (2008) proposed the underlying distributed and cooperative nature of wireless ad hoc networks and adds one more dimensions to the intrusion detection process. Cooperative way of intrusion detection is performed which involves the participation of multiple mobile nodes.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. Chen *et al.* (2007) proposed light weight anomaly intrusions detection in which investigates different key features for wsn's and define some rules for building an efficient and accurate intrusion detection system.

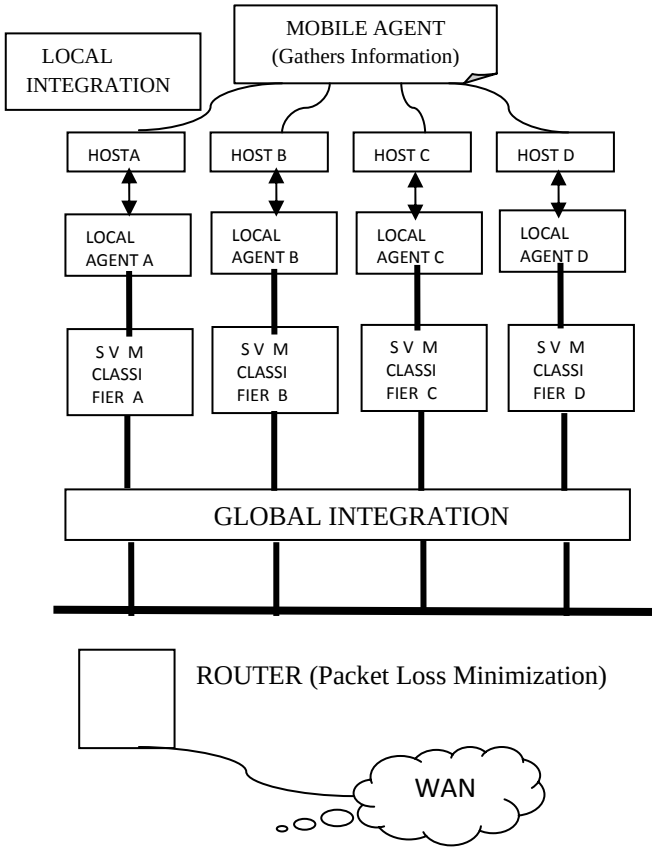
Liu *et al.* (2006) proposed game theoretic framework to analyze the interactions between pairs of attacking or defending nodes using a Bayesian formulation. The dynamic Bayesian game is a more realistic model as it allows the defender to consistently update his belief on his opponent's maliciousness as the game evolves. 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 thatnetwork.

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. Perlman's work required significant commitments of router resources and high levels of network participation to detect anomalies. A router can be traffic faulty by maliciously dropping the packets and protocol faulty by not allowing the rules of the detection protocol. When packet loss due to congestion can be inferred then remaining packet loss may be due to malicious actions. In this paper, we develop an intrusion detection system which could characterize the packets and identify the attacked system

Indian Journal of Science and Technology Vol.3 No.10 (Oct 2010) ISSN: 0974- 6846

from the system behavior. 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.*



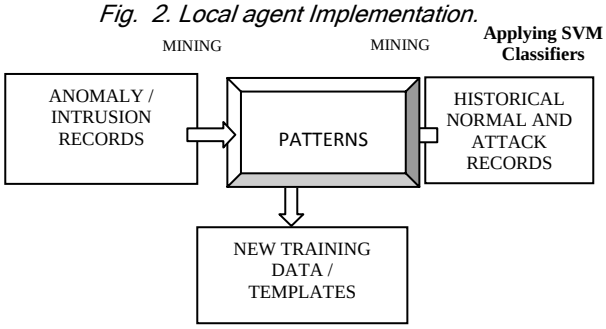

## Proposed system

Our approach is based on anomaly based method. The architecture of the system to prevent the attacks in networks is shown in Fig. 1.

*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.The mobile agent based systems has the advantages of overcoming network latency, reducing network load, autonomous execution, platform independence, dynamic adaption, static adaption, scalability.

*Local agent:* Local agent is implemented in every system in the network which gathers information about its system (Fig. 2). The 3 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. It gathers neighboringnodes information using mobile agents. It then calls the SVM classifier to find out the attacks with the help of trained test data. 3. It provides same type of security solution throughout the network.

*Fig. 2. Local agent Implementation.*




*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. If an attack has been made, local agent will filter the respective system from the global networks.

*Gathering Information from neighboringnode*: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 neighboringnode gathers information from that node and it return back to the system. It then calls the SVM classifier to find out the attacks. If there is no suspicious activity, then it will forward the message to the neighboringnode.

*Data collection:* Data collection module is included for each intrusion detection 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 detection.

*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 neighboringnodes before taking decisions towards forwarding messages.

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

Indian Journal of Science and Technology Vol.3 No.10 (Oct 2010) ISSN: 0974- 6846

We denote traffic information collected by router r that traversed path segment $\pi$ over time interval $\tau$.
$Q_{dir}$ is either $Q_{in}$ ,meaning traffic into Q, or $Q_{out}$ ,meaning traffic out of Q as $T_{info}$ ($r_s$, $Q_{dir}$,$\pi$,$\tau$).
Assume that for a given Q, the routers involved in detecting compromised routers are shown below.

- $r_s$ – which sends traffic into Q and which collects the traffic information $T_{info}$ ($r_s$, $Q_{in}$, < $r_s$ , r , $r_d$>, $\tau$)
- r - which hosts Q and which collects the traffic information$T_{info}$ ($r$, $Q_{in}$, < $r_s$ , r , $r_d$>, $\tau$)
- $r_d$ – which is the router to which Q's outgoing traffic is forwarded and it collects the traffic information $T_{info}$ ($r_d$, $Q_{out}$, < r , $r_d$>, $\tau$)

*Detection at r*:Let $\alpha$ be the upper bound on the time to forward traffic information

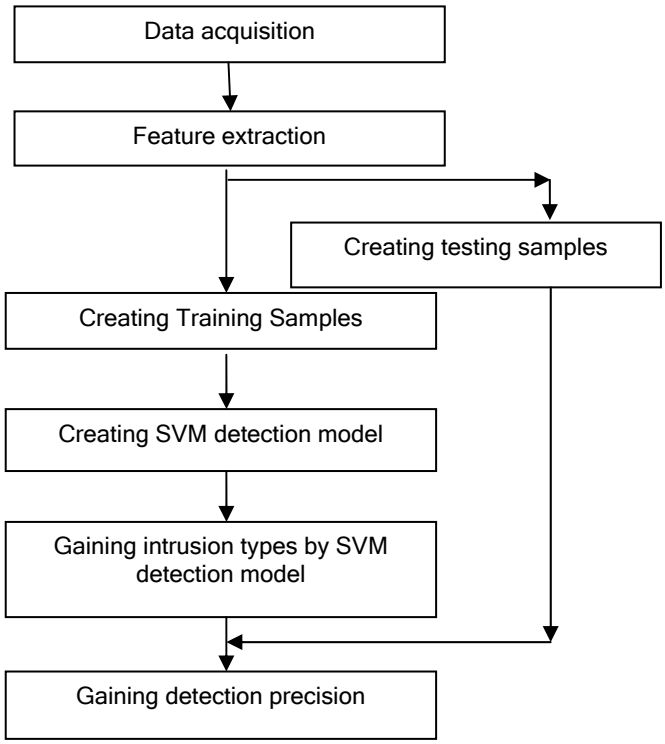
- If r does not receive traffic information from $r_s$, within$\alpha$, then r detects < $r_s$,r> as traffic faulty.
- On receiving traffic information from $r_s$, router r verifies the signature and then it forwards the information $T_{info}$ ($r_s$, $Q_{in}$, < $r_s$, r, $r_d$>,$\tau$) router $r_d$. If not then r detects < $r_s$, r> segment as traffic faulty. In this case it forwards its own copy of traffic information $T_{info}$ ($r$, $Q_{in}$, < $r_s$, r, $r_d$>,$\tau$) to router $r_d$.

*Detection at $r_d$ :*

- If $r_d$ does not receive traffic information from r, originated by $r_s$ , it expects r to broadcast the detection <$r_s$ , r>. If not then router $r_d$ detects <r,$r_d$ >as traffic faulty.
- On receiving the traffic information forwarded from r, $r_d$ 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. New examples are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall on. Fig. 4 shows supervised and unsupervised model generation.

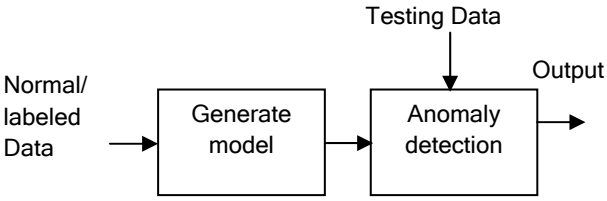
*Fig. 3. SVM classification process.*




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. It is based on the idea that the classification that accords dot-products can be computed efficiently in higher dimensional feature spaces. The classes which are not linearly separable in the original parametric space can be linearly separated in the higher dimensional feature space. 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.

Indian Journal of Science and Technology Vol.3 No.10 (Oct 2010) ISSN: 0974- 6846

*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

$$\sum_{l,m=1}^{n}(x_l-\mu)(x_m-\mu)^T$$

Where n is the total number of features
Compute the Determinant of above covariance matrices
if Determinant ≤ 0
Consider the neighboringcovariance matrix having positive Determinant
Compute inverse matrix corresponding to each covariance matrix
End

*Detection 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 $T^2 = (X - \mu) S^{-1} (X - \mu)^T$*
If $T^2$ exceeds, the threshold flag alerts

*Compute $g_l(X) = - ½ \ln |S| - ½ (X-\mu)^T S^{-1} (X-\mu) + \ln p(l)$*
If $g_i(X)$ exceeds the threshold flag alerts.
End

## Results

This system not only blocks the security threats at the application level, but also stops some of the threats at the network level. Our results are compared with other recently published results in Table 1. Which shows the proposed system is greatly competitive with others.The detection rate of anomaly in our proposed system is high and it encourages the system. The percentage of anomaly detection is calculated as follows:

$$\% \text{ of anomaly detection} = \frac{\text{No. of Predicted abnormal class}}{\text{Total No. of traces}} X\ 100$$

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. The proposed system is compared with existing system which uses Bayesian classifier program for training the classifier for anomaly detection. The information's required to classify anomalies are shared among the neighboringnodes beforesending packets and thereby ensuring safety during communication between the network systems and therefore our intrusion detection system proves strong.

*Table 1. Results comparison.*

| Methods | FPR (%) | DR (%) |
|---|---|---|
| Genetic clustering(Y.G. Liu *et al.* 2004) | 0.3 | 79 |
| Hierarchal SOM (Q.A. Zhu *et al.* 2005) | 2.19 - 3.99 | 90.94 - 93.46 |
| Proposed system | 5-9 | 89 - 98 |

## Conclusion

This paper provides a strong platform to detect anomalies. The proposed system is cooperative and distributive; it considers the anomaly detection result from the neighbor nodes and sends the current nodes result to its neighbor nodes. Our system also could differentiate congestive packet loss from malicious packet loss using a packet loss minimization algorithm implemented in routers by accessing the traffic rates and buffer sizes. Experimental results show that anomaly detection rate is higher when compared to existing mechanism. This mechanism proves strong in places where traditional security mechanisms like IDS and firewall have not been sufficient to provide security of networks.

## Acknowledgement

We take immense pleasure in thanking Dr. Jeppiaar, Mr. Marie Wilson, Mrs. Regeena Wilson and Dr. Sushil Lal Das for their continual support and guidance.

Indian Journal of Science and Technology Vol.3 No.10 (Oct 2010) ISSN: 0974- 6846

## References


1. Bhuse V and Gupta A (2006) Anomaly intrusion detection in wireless sensor networks.*J. High Speed Networks*. 15(1), 33–51.
2. Bo Sun, Wu K, Xiao Y and Wang R (2006) Integration of mobility and intrusion detection for wireless ad hoc networks DOI: 10.1002/dac.853.
3. Bradley KA, Cheung S, Puketza N, Mukherjee B and Olsson RA (1998) Detecting disruptive routers: A distributed network monitoring approach. *Proc. IEEE Symp. Security Privacy.* pp:115-124.
4. Cabrera D and Gutiérrez C and Raman K. Mehra (2008) Ensemble methods for anomaly detection and distributed intrusion detection in mobile Ad-Hoc networks.*Elsevier Sci. Publishers.* 9(1), 96-119.
5. Chen H, Han P, Zhou X and Gao C (2007) Lightweight anomaly intrusion detection in wireless sensor networks. *Intelligence Security Informatics. Springerlink.*
6. Deng H, Xu, R, Li, J, Zhang, F, Levy, R and Lee W (2008) Agent-based cooperative anomaly detection for wireless ad hoc networks. *Parallel Distributed Sys*. 1, 8.
7. Liu Y, Comaniciu C and Man H (2006) A Bayesian game approach personal wireless communications. ACM 159593507X.
8. Liu Y, Li Y and Man H (2005) MAC layer anomaly detection in Ad Hoc networks. *Proc. of the 6th IEEE Information Assurance Workshop.* pp: 402-409.
9. Mishra A and Nadkarni K (2003) Security in wireless Ad Hoc networks. *CRC press* LLC.
10. Mishra A, Nadkarni K and Animesh Patcha (2004) Intrusion detection in wireless Ad Hoc networks. *IEEE Wireless Commun*. pp: 48-60.
11. Mizrak AT, Cheng YC, Marzullo K and Savage S (2006) Detecting and isolating malicious routers. *IEEE Trans. Dependable Secure Computing*. 3(3), 230-244.
12. Perlman R (1988) Network layer protocols with byzantine robustness, MIT LCS TR-429.
13. Puttini R, Hanashiro M, García-Villalba J and Barenco CJ (2006) On the anomaly intrusion-detection in mobile Ad Hoc network environments. *Personal Wireless Commun*. Vol. 4217/2006, Springerlink.
14. Subhadrabandhu FAD and Sarkar S (2008) Signature based intrusion detection for wireless Ad-Hoc networks: A comparative study of various routing protocols. *Seas*.
15. Y.G. Liu, K.F. Chen, X.F. Liao, and W.Zhang (2004) A genetic clustering method for intrusion detection. *Pattern Recognition,* 37(5), 927-942.
16. S.T. Sarasamma, Q.A. Zhu and J. Huff (2005) Hierarchial kohonenen net for anomaly detection in network security. *IEEE Transactions on Systems, Man & Cybernetics.* 32(2), 302-312.