# Artificial Immune System based Intrusion Detection with Fisher Score Feature Selection

R. Sridevi
Associate Professor
Department of Information Technology,
Shri Angalamman College of Engineering & Technology,
Tiruchirappalli Tamilnadu India.

G. Jagajothi, Ph.D
Professor
Department of Information Technology,
PeriyarManiammaiUniversity,
Tanjore Tamilnadu India.

Rajan Chattemvelli, Ph.D
Professor
Department of Information Technology,
PeriyarManiammaiUniversity,
Tanjore Tamilnadu India.

## ABSTRACT
Intrusion-detection systems (IDS) which were essential in computer security because of difficulties in ensuring the information systems are security free. Literature has numerous intrusion detection approaches for network security. IDS efficiency was based on the ability to differentiate between normal and harmful activity. Hence, it becomes crucial to achieve better detection rates and lower false alarm rates in IDS. Automated/adaptive detection systems should secure the system handling present and possible threats in the future. Features extracted from network traffic by the IDS, classify the record/connection as either an attack or normal traffic. So, feature selection has a major role in IDS performance. This paper adopts a feature selection using the Fisher Score. Artificial Immune Systems (AIS) based IDS to detect and defend against harmful, unknown invaders is proposed. Evaluation of security detection mechanisms is done through the KDD-cup dataset.

## Keywords
Intrusion Detection System (IDS), KDD Cup 99 dataset, Fisher Score for feature selection, Artificial Immune Systems (AIS).

## 1. INTRODUCTION
Intrusion detection system (IDS) is essential in computer security due to problems in ensuring that information systems are free of attacks. Computer systems are susceptible to breaches in security irrespective of their purpose, manufacturer, or origin. Also technically difficult and costly to ensure attack free networks. An IDS diagnose the security status of a system [1], aims to uncover security breaches, breaching attempts, or vulnerabilities which are harmful in the future. A typical IDS is seen in Figure 1.

IDS play as a detector to process information from a system requiring protection. The detector launches probes to audit process like version application numbers. It uses three types of information: long-term information that relates to techniques to detect intrusions using knowledge of attacks, configuration information relating to the existing system conditions and audit information describing events happening within a system [2]. The detector's role is to eliminate unnecessary information from the audit. It then reveals synthetic views of security-related action in normal system usage, or of the system's present security level. A decision evaluates whether such actions and/or this state are intrusion symptoms or vulnerabilities. Then a countermeasure component opts for corrective measures, to prevent execution of action or to get back to a secure state.

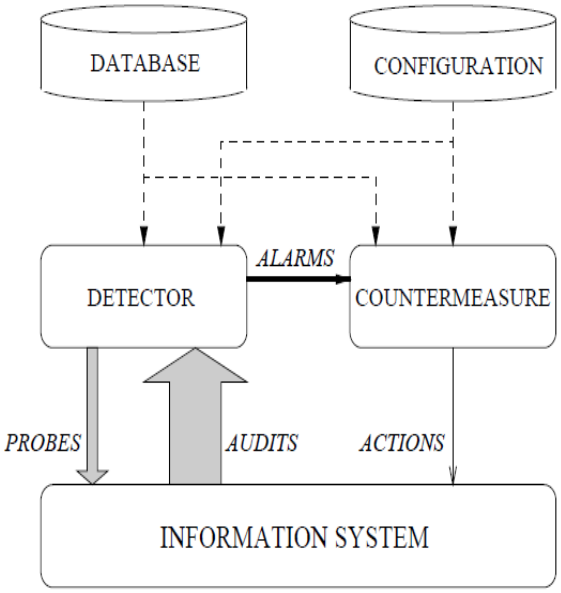


**Fig.1: A simple intrusion-detection system.**

The following parameters are proposed to evaluate an intrusion detection system's efficiency [3].

### 1.1 Accuracy
This relates to attack detection and false alarms absence. An inaccuracy occurs when an IDS considers legitimate action as either anomalous or intrusive.

### 1.2 Performance
IDS performance depends on the rate in which audit events are processed. Real time detections are impossible when performance is poor.

### 1.3 Completeness
Completeness in IDS is the characteristic of detecting attacks. Incompleteness arises when attacks are undetected, and this was harder to evaluate as it not possible to get prior knowledge of attacks/abuses/privileges.

Two additional properties include:

## 1.4 Fault Tolerance

An IDS must be attack-free and resistant to attacks including denial-of-service attacks and should be designed with this aim as IDS operate above commercially available operating systems/hardware vulnerable to such attacks.

## 1.5 Timeliness

An IDS acts and gives out its analysis early to ensure that security personnel react before damage was large and to prevent attackers from tampering with audit sources or IDS itself, thereby implying the importance of IDS processing speed, information forwarding time and its reaction.

Various intrusion types of attacks are discussed [4]:

## 1.6 Denial of Service (DOS)

An attack where attackers manipulate so that memory resource has no time or too full to cater to legitimate requests or denies legitimate users access to a machine. Attacks like neptune, or smurf abuse legitimate features while others like teardrop, Ping of Death etc; lead to malformed packets confusing machine TCP/IP stack which tries to reconstruct the packet. Also, others like apache2, back, syslogd use network daemons advantageously.

## 1.7 User to Root Attacks (U2R)

An attack starts with access to a normal user account exploiting existing vulnerability to get system root access. There are different types of U2R attacks, the buffer overflow attack being the commonest. A Buffer overflow happens when a program copies excess data into a static buffer without seeing whether it will fit. Some U2R attack examples are Perl, Rootkit and Bufferflow.

## 1.8 Probe

The attacker collects information/services provided by network machines to develop ordinary information. Probes generally used by attackers include Satan, nmap, insweep and Portssweep.

IDS efficiency depends purely on how it differentiates normal and harmful activity. Automated and adaptive detection systems are needed to secure the system so that it can handle present and future threats. The IDS also used in tandem with protection techniques like encryption and firewalls to secure computer systems. The objective of IDS is detection of unauthorized use/misuse/abuse of computer systems from intruders who are possibly system insiders or external intruders. An IDS depends on knowledge of signatures of known intrusions and probes to detect suspicious signatures [4], which forms as a major disadvantage as unknown intrusions harm system security. To overcome this, Artificial Immune System (AIS) based on the principle of the human immune system, which adapts or creates new immune cells to detect earlier unknown and quickly evolving harmful antigens [5] was focused.

This paper proposes an adaptive intrusion system based on the Artificial Immune Systems (AIS) to detect/defend against harmful and unknown invaders. The proposed IDS are based on this principle. It checks traffic connection records and traffic control packets to identify intrusions/attacks. Network generated records are huge in quantity. The IDS extracts features from such records, classifying them as either an attack or normal traffic. Feature selection facilitates machine learning methods in classification. Feature extraction includes feature selection and space dimension reduction and these techniques are used to pre-process data before using inputs in machine learning and statistics tasks. Efficient feature extraction leads to better classification and reduced pre-processing costs. This in turn, leads to better overall performance of classifier based IDS.

In our earlier investigations [6], we had used Principal Component Analysis for feature selection. Though satisfactory results were obtained, the computation of finding the transformation matrix is high. Fisher Score used for feature extraction in this paper, the method being based on discriminative methods, and a generative statistical model. It is simple and effective method to measure the discrimination between a label and a feature.

# 2. RELATED WORKS

Aickelin, et al., [7] presented an IDS based on theimmunological theories. The immunological algorithmsdepend on self and nonself discrimination. But the selfnonselfthinking has faults which are addressed by Danger Theory' (DT). The DT expounds that immune system responds to threats based danger signals and links it directly to the attacker. It was proposed to correlate and translate the DT in such a way that AIS will not belimited by self-nonself discrimination. The proposed method was based on the two effects of danger signals. In the IDS framework, the danger signals should identify attack early so as to minimise damage. On transmissionof danger signal, the proposed AIS respond to antigens near the danger signal. The proposed system has the advantage of detecting the intrusions at an early stage beforeit creates serious damage.

Powers [8] presented a hybrid system to detect anomalous network connections using combined techniques of artificial immune system and Kohonen Self Organising Map (SOM). The proposed system takes advantage of both approaches where AIS used for detection and SOM used for classification. AIS detects the anomalous network connections initially and anomalous connections are categorised using SOM. The proposed method creates clusters of attacks having similar properties thus higher-level abstraction of the attacks were identified. This allows the proposed system to identify other attacks belonging to the cluster. Experiments were conducted using KDD 1999 Cup dataset. Experimental results show that the proposed method achieves low false positive rate and high detection and classification rate.

Dal, et al., [9] described an IDS system based on AIS with Genetic algorithm. The proposed method incorporates Secondary Immune Response using the idea of memory cells. The memory cells depend on GeneticAlgorithm operators for evolution of the detectors. This leads to early detection of encountered attacks by the memory cells. The proposed method achieves better immunity from anomalies and attacks due to the random nature of the memory cells and adaptability of AIS. Experimental results demonstrate the efficiency of the anomaly detection rate of the proposed system.

# 3. MATERIALS & METHODS

## 3.1 Fisher Score for Feature Selection

The Fisher score is used for determining the most relevant features for classification which based on discriminative methods, and generative statistical model. The Fisher score is a supervised method with class labels and features with best discriminant ability found [10]. If $n_i$ is the number of samples in class $i$, $\mu_r^i$ and $\left(\sigma_r^i\right)^2$ is the mean and variance of class $i$, (i=1,…,c) for feature $r$. The Fisher score can be computed as follows:

$$F_r = \frac{\sum_{i=1}^{c} n_i \left( \mu_r^i - \mu_r \right)^2}{\sum_{i=1}^{c} n_i \left( \sigma_r^i \right)^2}$$

Higher the Fisher score, more discriminative is the feature.

## 3.2 Artificial Immune System (AIS)

Artificial Immune Systems (AIS) [11] is a diverse research area, attempting to bridge the chasm between immunology and engineering, developed through mathematical and computational modeling of immunology, abstraction into an algorithm (and system) design and implementation in the context of engineering from them. The immune system may be considered a multilayer system with several layers of defense mechanisms, the three main being anatomic barrier, innate immunity and adaptive immunity as described below:

### *3.2.1 The Anatomic Barrier*

The first layer formed of skin and a surface of mucous membranes. Skin prevents pathogen penetration and lowers bacterial growth due to low pH. But pathogens penetrate the body through mucous membranes which have many nonspecific mechanisms to prevent entry [12, 13].

### *3.2.2 Innate Immunity*

Immunity transferred from mother to baby when the latter born. It has a nonspecific response to foreign entities and consists of the following mechanisms.

### *3.2.3 Physiologic Barriers*

This includes temperature, pH, oxygen, tension and various soluble chemicals whose aim is to the provision of detrimental living conditions to foreign pathogens.

### *3.2.4 Phagocytic Barriers*

Specialized cells like macrophages, neutrophils and natural killer cells ingest specific material, including whole pathogenic microorganisms [11]. This ingestion kills antigens and presents protein fragments to other immune cells/molecules.

### *3.2.5 Inflammatory Response*

Active macrophages produce cytokines, hormone-like messengers which have an inflammatory response, characterized by vasodilation and increase in capillary permeability, all of which permit circulation of immune cells to the infected area.

### *3.2.6 Adaptive Immunity*

Adaptive immunity also called acquired or specific immunity represents the part of an immune system which specially recognizes and selectively eradicates foreign microorganism/molecules. Such adaptive immunity characteristics are as follows:

### *3.2.7 Antigenetic Specificity*

It enables the immune system to differentiate the subtle differences between antigens.

### *3.2.8 Diversity*

The adaptive immune system generates billions of different recognition molecules that recognize foreign antigens varied structures.

### *3.2.9 Immunologic Memory*

The adaptive immune system remembers an earlier antigen encounter thereby able to provide an immediate response in future encounters.

### *3.2.10 Self/Non-Self Recognition*

As immune cells can differentiate own cells from those of foreign antigens it responds only to non-self molecules.

Table 1 tabulates the mapping between the immune system and artificial immune recognition system [14].

**Table 1. Mapping Between the Immune System and Airs**

| IMMUNE SYSTEM | AIRS |
|---|---|
| Antibody | Feature vector |
| Recognition Ball | Combination of feature vector and vector class |
| Shape-Space | Possible values of the data vector |
| Clonal Expansion | Reproduction of ARBs that match antigens |
| Antigens | Training data |
| Affinity Maturation | Random mutation of ARB and removal of lowest stimulated ARBs |
| Immune Memory | Memory set of mutated ARBs |
| Meta dynamics | Continued removal/ creation of ARBs/ Memory Cells |

## 4. RESULTS

The experiments were conducted using KDD 99 dataset on WEKA platform. A subset of 36496 instances was used with 18 attributes for the evaluation purpose. 66% of the dataset was used for training the classifier and the remaining for testing. Initial experiments were conducted without any dimension reduction of the feature set. Second set of experiments were conducted based of feature selection using Fisher Score. Table 2 tabulates the training summary of Artificial Immune Recognition System without and with feature selection and Table 3 and Figure 2 gives the summary of results.

Table 4 gives the detailed Accuracy by Class for proposed IDS with AIS and Fisher Score feature selection. Figure 3 shows the precision and recall by class for proposed IDS with AIS and Fisher Score feature selection, Figure 4 gives the f Measure of the same. Table 5 tabulates the confusion matrix.

**Table 2. The Training Summary of Artificial Immune System without and with Fisher Score Feature Selection**

| | AIS | AIS + Fisher score feature selection |
|---|---|---|
| Affinity Threshold | 0.227 | 0.229 |
| Total training instances | 36,496 | 36,496 |
| Total memory cell replacements | 36,049 | 35,946 |
| Mean ARB clones per refinement iteration | 51.313 | 51.533 |
| Mean total resources per refinement iteration | 126.285 | 126.445 |
| Mean pool size per refinement iteration | 69.617 | 69.93 |
| Mean memory cell clones per antigen | 19.606 | 19.79 |
| Mean ARB refinement iterations per antigen | 2 | 2.002 |
| Mean ARB prunings per refinement iteration | 53.616 | 53.924 |

**Table 3. Summary of Results**

| AIS | AIS + Fisher score feature selection | AIS |
|---|---|---|
| Correctly Classified Instances | 12149 (97.9047 %) | **12328 (99.3472 %)** |
| Incorrectly Classified Instances | 260 (2.0953 %) | 81 (0.6528 %) |
| Kappa statistic | 0.6848 | 0.8518 |
| Mean absolute error | 0.0105 | 0.0033 |
| Root mean squared error | 0.1024 | 0.0571 |
| Relative absolute error | 44.53% | 13.87% |
| Root relative squared error | 93.72% | 52.31% |
| Total Number of Instances | 12409 | 12409 |

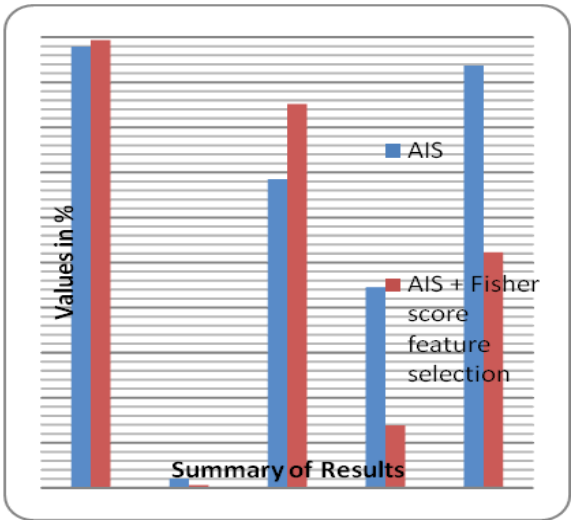


**Fig 2. Summary of Results**

**Table 4. Detailed Accuracy by Class for Proposed Ids with Ais and Fisher Score Feature Selection**

| Precision | Recall | F-Measure | ROC Area | Class |
|---|---|---|---|---|
| 0.999 | 0.979 | 0.989 | 0.973 | normal. |
| 0.217 | 0.932 | 0.352 | 0.956 | teardrop. |
| 1 | 0.987 | 0.993 | 0.993 | satan. |
| 0.938 | 0.962 | 0.949 | 0.981 | nmap. |
| 0.994 | 0.979 | 0.985 | 0.973 | Weighted Avg. |

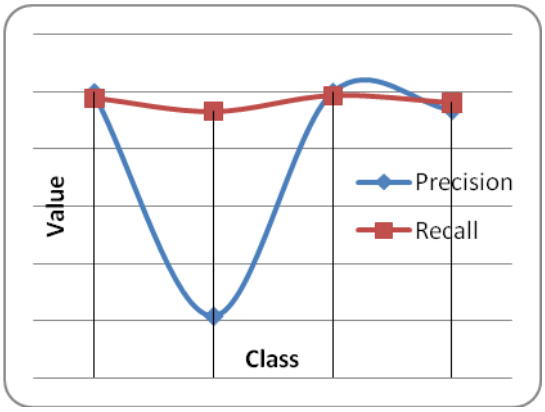


**Fig 3. Precision and Recall by Class for proposed IDS with AIS and Fisher Score feature selection**

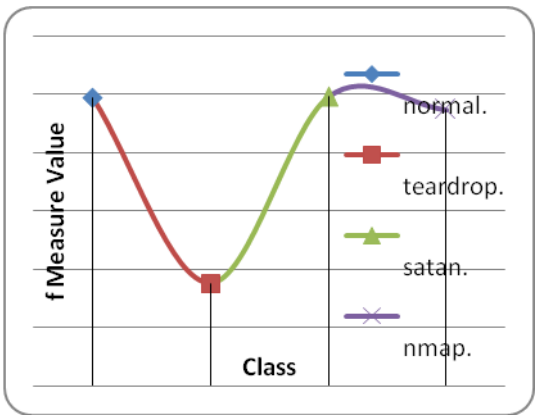


**Table 5. Confusion Matrix**

| a | b | c | d | classified as |
|---|---|---|---|---|
| 12091 | 13 | 2 | 2 | a = normal. |
| 53 | 20 | 0 | 0 | b = teardrop. |
| 2 | 0 | 148 | 0 | c = satan. |
| 9 | 0 | 0 | 69 | D=nmap |

## 5. CONCLUSION

In this paper, it was proposed to investigate feature reduction technique using fisher score on the KDD 99 dataset. Matlab was used to program the ranking of the attributes using Fisher score. The top 10 attributes were selected for classification using Artificial Immune System classifier. Results show that the classification and recall of the proposed system was better than system without feature reduction technique.

## 6. REFERENCES

[1] R. Bace and P. Mell. "Intrusion Detection Systems", NIST Special Publication 800-31. 2001.

[2] S. Northcutt & J. Novak, "Network Intrusion Detection: An Analyst's Handbook," 2nd Edition, New Riders Publishing, Berkeley, 2000.

[3] Debar, H. (2002). An Introduction to Intrusion-Detection Systems. In Proceedings of Connect'2000.

[4] Vera Marinova-Boncheva, 2007, "A Short Survey of Intrusion Detection Systems", Problems Of Engineering Cybernetics And Robotics, pp. 23 – 30.

[5] Kim J, Bentley P (1999), The Artificial Immune Model for Network Intrusion Detection, 7th European Congress on Intelligent Techniques and Soft Computing (EUFIT'99).

[6] R. Sridevi, G. Jagajothi and RajanChattemvelli, A PCA-AIS Approach for Intrusion Detection, International Journal of Computer Science and Telecommunications, Volume 3, Issue 7, July 2012], pp:104-108.

[7] U Aickelin, P Bentley, S Cayzer, J Kim, J McLeod, Danger Theory: The Link between AIS and IDS?, Proceedings ICARIS-2003, 2nd International Conference on Artificial Immune Systems, pp 147-155, 2003.

[8] Simon T. Powers, A Hybrid Artificial Immune System and Self Organising Map for Network Intrusion Detection, Information Sciences 178(15), pp. 3024-3042, August 2008.

[9] Divyata Dal, Siby Abraham, Ajith Abraham,and MukundSanglikar, Evolution Induced Secondary Immunity: An Artificial Immune System based Intrusion Detection System, in: the 2008 7th Computer Information systems and Industrial Management Applications (IEEE Computer Society Washington, DC, USA, 2008) 65-70.

[10] Gu, Q., & Han, J. (2011, October). Towards feature selection in network. In Proceedings of the 20th ACM international conference on Information and knowledge management (pp. 1175-1184). ACM.

[11] Kuby J (2002), Immunology, Fifth Edition WH Freeman by RA Goldsby, TJ Kindt, BA Osborne.

[12] Tarakanov, A. O., Skormin, V. A., Sokolova, S. P., & Sokolova, S. S. (2003). Immunocomputing: principles and applications. Springer-Verlag.

[13] Aickelin, U., Greensmith, J. and Twycross, J., 2004, Immune system approaches to intrusion detection—a review, in: Proc. ICARIS-04, 3rd Int. Conf. on Artificial Immune Systems (Catania, Italy), pp.316–329, Springer, Berlin. Amazon, 2003

[14] Simon M. Garrett, "How Do We Evaluate Artificial Immune Systems?", Evolutionary Computation 13(2):, 2005, Massachusetts Institute of Technology, pp. 145-178.