



## Stratified Path Using Fortuitous Enclosure Field For Incursion Revelation

G. Ramesh Kumar <sup>1</sup>

Assistant Professor

Department of Computer Science  
Adhiparasakthi College of Arts and Science,  
Kalavai. – 632 506, Vellore District  
Tamilnadu, India

K.Nadhiya, <sup>2</sup>

Research scholar

Department of Computer Science  
Adhiparasakthi College of Arts and Science,  
Kalavai.- – 632 506, Vellore District  
Tamilnadu, India

---

**Abstract-** Incursion revelation faces a number of problems; model of a real-time incursion revelation expert system capable of detecting break-ins, penetrations, and other forms of computer abuse is described. An incursion revelation system must reliably detect malicious activities in a network and must perform efficiently to cope with the large amount of network traffic. In this project, we address these two issues of Accuracy and Efficiency using Fortuitous Enclosure Fields and Stratified Path. We demonstrate that high attack revelation accuracy can be achieved by using Fortuitous Enclosure Fields and high efficiency by implementing the Stratified path. Finally, we show that our system is robust and is able to handle noisy data without compromising performance.

**Keywords-** Incursion Revelation, Fortuitous Enclosure Field, Methodology, Experimental Result.

---

### I. Introduction

An Incursion Revelation System (IRS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IRS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network.

This is concerned with accurate and efficient hybrid incursion revelation system. In this paper we combine both the signature based system and anomaly based incursion revelation system. Here we address the two issues of Accuracy and Efficiency using Enclosure fortuitous fields and Encrusted Approach for signature based system and acquiring volatile data once system is turn off For anomaly based system. We demonstrate that high attack detection accuracy can be achieved by using Enclosure fortuitous fields and high efficiency by implementing the Encrusted Approach in signature based system.

Incursion revelation is a necessary part of the management cycle. It is part of knowing what is happening on your network, Intruders can cause harm to the general health of the network. The obvious reason for doing incursion revelation is to detect suspicious activity on your systems. Incursion revelation as defined by the SysAdmin, Audit, Networking, and Security (SANS) Institute is the art of detecting inappropriate, inaccurate, or anomalous activity. Today, incursion revelation is one of the high priority and challenging tasks for network administrators and security professionals. More sophisticated security tools mean that the attackers come up with newer and more advanced penetration methods to defeat the installed security systems.

**Fortuitous Enclosure Field-** The FEFs have proven to be very successful in such tasks, as they do not make any unwarranted assumptions about the data. Hence, we explore the suitability of FEFs for incursion revelation. System may consider features such as “logged in” and “number of file creations.” When these features are analyzed individually, they do not provide any information that can aid in detecting attacks.

### II. Methodology

**Preprocessing and Cleansing of Weblogs-** This method concentrates on preprocessing of a system for storing and delivering massive quantities of data. The Cleansing process is to ensure that all values in a dataset are consistent and correctly recorded. In general, the duplicates elimination problem is difficult to handle both in scale and accuracy. This project proposed approach aims to increase the accuracy by pre-processing the records so that subsequent sorting will bring potentially matching records to a close neighbourhood. In this way, the window size can be reduced which improves processing time.

**Temporal Navigational Pattern Discovery-** This method implements the pattern discovery using the popular FEF model which can discover user navigation patterns that hold the order, adjacency and regency information.

**Temporal Navigational Pattern Prediction and Statistical Analysis-** Once user transactions or sessions have been identified as there are several kinds of access pattern mining that can be performed depending on the needs of the analyst. In this project mainly concentrates on

- ✓ Path Analysis
- ✓ Association Rules
- ✓ Clustering and Classification

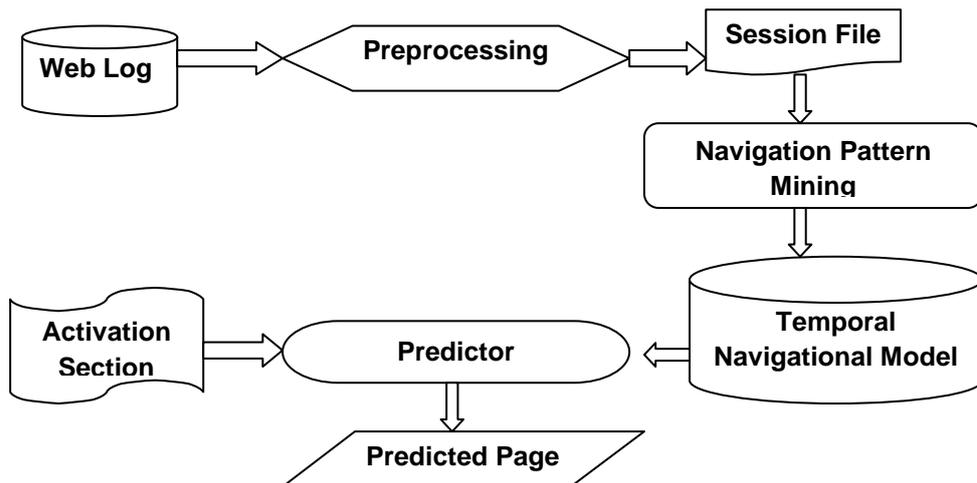


Fig.1 A Temporal Navigational Pattern Prediction and Statistical Analysis

### III. Experimental result:



Fig 2: Log files

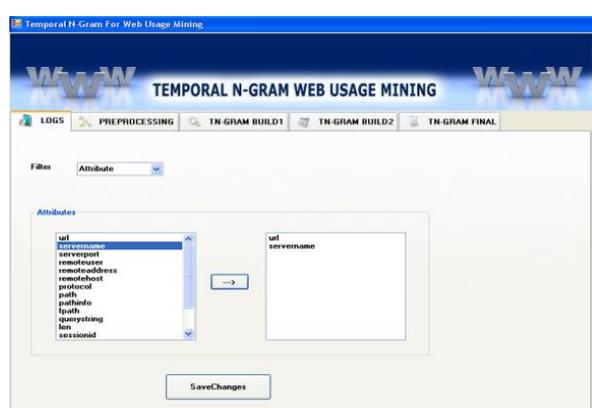


Fig 3: Filter attributes

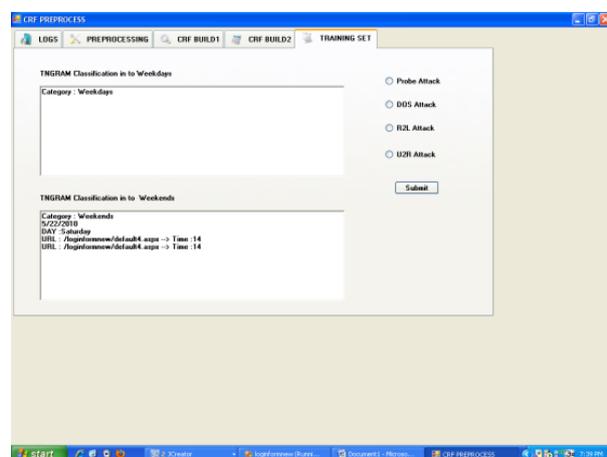


Fig 4: Types of attacks

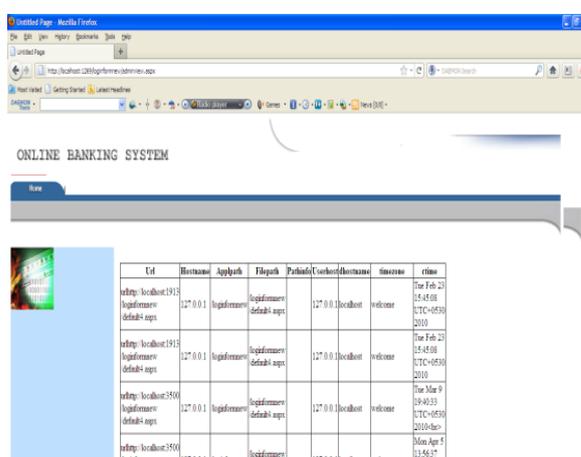


Fig5: Attack details

### IV. Conclusion and Future Enhancement

The Stratified path using Fortuitous Enclosure Field for Incursion revelation System reduces the Attacks of Intruders and Protects the Network from Malicious Activities or Policy Violations and provides reports to manage Critical situation. A new Technique called Nectar is used to detect other new Attacks and new methods could be enhanced to avoid future attacks. Thus, the Attacks are reduced by Fortuitous Enclosure Field Approach and Pyramidal Time Frame Approach.

Based on the incursions, techniques can be developed and implemented to detect and prevent from intruders.

### **Acknowledgment**

First we thank God Almighty for his blessings for this paper. We thank this opportunity to express my hearty thanks to my parents and friends for the moral support, encouragement to make this as a success.

### **Reference:**

- [1]. T. Abraham, "IDDM: Intrusion Detection Using Data Mining Techniques", <http://www.dsto.defence.gov.au/publications/2345/DSTO-GD-0286.pdf>, 2008.
- [2]. R. Agrawal, T. Imielinski, and A. Swami, "Mining Association Rules between Sets of Items in Large Databases", Proc. ACM SIGMOD, vol. 22, no. 2, pp. 207-216, 1993.
- [3]. N.B. Amor, S. Benferhat, and Z. Elouedi, "Naive Bayes vs Decision Trees in Intrusion Detection Systems", Proc. ACM Symp. Applied Computing (SAC '04), pp. 420-424, 2004.
- [4]. J.P. Anderson, "Computer Security Threat Monitoring and Surveillance", Proc. ACM SIGMOD, vol. 22, no. 2, pp. 207-216, 1993.

### **Websites:**

<http://csrc.nist.gov/publications/history>.  
<http://www.cerias.purdue.edu/research/aafid>.  
[http://www.cert.org/archive/pdf/attack\\_trends.pdf](http://www.cert.org/archive/pdf/attack_trends.pdf).  
<http://www.sans.org/resources/idfaq>.