# A Normal Profile Updating Method for False Positives Reduction in Anomaly Detection Systems

Walid Mohamed Alsharafi and Mohd Nizam Omar
InterNetworks Research Laboratory, School of Computing, College of Arts and Sciences,
06010 UUM Sintok, Universiti Utara Malaysia, Malaysia
sharafi12@yahoo.com , niezam@uum.edu.my

## ABSTRACT

The contribution of this paper is to investigate whether there is a possibility of further processing of both the normal and abnormal data identified by any anomaly detector with the intent of reducing the false positive alerts. For this end, we use an existing anomaly detector model which is called as Protocol based Packet Header Anomaly Detector (PbPHAD). This model has been demonstrated as a very promising model to be used for anomaly based Intrusion Detection Systems (IDSs). However, the percentage of false positives is quite big for the detected anomalous packets based on PbPHAD model alone. Thus, the purpose of this paper is to investigate a proposed method of normal profile updating in anomaly detection systems with the intent of reducing the false positive alerts. The proposed method was applied and tested using the PbPHAD model. The evaluation data set were downloaded from MIT Lincoln Laboratory. The experimental results on one selected host show that the proposed method has a good ability to solve the shortcoming of the PbPHAD model regarding the high false positives rate for the detected anomalous packets.

## KEYWORDS

Normal Profile, False Positive, Anomaly, Intrusion Detection System, Dataset

## 1 INTRODUCTION

The high false positive alerts rate is considered as one of the main disadvantages of anomaly detection since the advent of IDS technologies. At present various intrusions detection systems are available using different methodology but the main problem with them is the false positives [1]. So many works was done to reduce these false positives and increase the accuracy of an IDS. Thus, in this paper, we are exploiting an existing IDS model, that is PbPHAD model proposed in [2], to investigate the ability extent of our proposed method of normal profile updating to reduce the false positives in anomaly detection systems.

In this work, we firstly redevelop the PbPHAD model and apply it on one selected host, from the MIT Lincoln Lab. 1999 off-line intrusion detection evaluation dataset [3], to get the false positives packets from the detected anomalous packets. We then reapply the PbPHAD model on the same selected host using, however, the proposed method of normal profile updating. Finally, we compare the results of applying the PbPHAD model before and after using the proposed method to evaluate the efficiency of our method in reducing the false positives.

The paper is organized as follows. Section 2 overviews the related works. Section 3 provides an overview of the PbPHAD model and the dataset used in the simulation and describes the implementation of the PbPHAD model on the selected host. The proposed normal profile updating method for reducing the false positives is introduced in Section 4. We describe the simulation framework in Section 5. Section 6 compares and discusses the results of the experiments. Section 7 offers conclusions.

## 2 RELATED WORKS

PbPHAD model, proposed in [2], has been demonstrated as a very promising model to be used for an anomaly based IDS model, however the percentage of false positives is quite big for the detected anomalous packets based on the PbPHAD model alone [2]. The idea of PbPHAD IDS model

was drawn from a Technical Report written by [4] that learns the normal range of values for 33 fields of the Ethernet, IP, TCP, UDP and ICMP protocols using a generic statistical model for all values in the packet headers for all protocols.
In this paper, we examine our proposed method for reducing false positives on the PbPHAD anomaly statistical model.

### 2.1 False Positives and Normal Profiles

Simply stated, a false positive is any normal or expected behavior that is identified by IDS as anomalous or malicious. The high false positive alerts rate is considered as one of the main disadvantages of anomaly-based IDSs. The most commonly used tuning procedure for anomaly-based IDSs is finding an optimal threshold value, i.e., the best compromise between a high number of detected attacks and a low (or acceptable) number of false positives. This is typically carried out manually by trained IT personnel: different improving steps can be necessary to obtain a good balance between detection and false positive rates [5]. A number of techniques, however, have been proposed to the problem of high false positives rate resulted by anomaly IDSs. Some of them attempt to address the fundamental issue related with this problem, which is the *normal profile updating* issue. In anomaly IDSs, the normal profiles have to characterize the current behaviors, i.e. current patterns, of all IDS's subjects. Lee et al. assert that "if the training data cannot be nearly complete with regard to all possible normal behavior of a program/user, then the learned detection model cannot confidently classify or label an unmatched data as abnormal since it can just be an unseen normal data" [6]. Thus, anomaly-based IDS products often produce many false positives because of benign activity that deviates significantly from profiles, especially in more diverse or dynamic environments [7]. So, if normal profile fail to reflect a current behavior, then an unusual behavior (i.e. non-malicious pattern), even a safe one, tends to be flagged as an anomaly and raise a false alert [8].

### 2.2 Updating Normal Profiles

For anomaly detection accuracy it is very important to answer a key question: How to effectively update normal profiles so they constantly maintain current behaviors, i.e. latest patterns? Consequently, the way to handle this question directly affects the overall performance of anomaly detection systems including handling the problem of the high false positive alerts rate. Some research show limitations of existing normal profiles updating approaches for the anomaly detection systems. Schemes, based on waiting until sufficiently large patterns are collected, are generally time-consuming, suffer from high data dimensionality and profiles can become outdated as users utilize new patterns [9]. Other approaches, that attempted to update the normal profile periodically, suffered because keeping only the relevant data could be not done effectively [8]. The main idea of our work is to update normal profiles constantly by re-processing the normal data resulted from anomaly detection system. Further, the updated normal profiles will be used for re-processing, on other hand, the resulted abnormal data in order to refine them from normal one. As a result the false positives will be reduced. In the section 4, we describe the proposed method that addresses the problem of reducing false positives which rely on the proposed normal profiles updating technique. We use the PbPHAD IDS model, which we overview in the next section, to examine and test the efficiency of our proposed approach.

## 3 OVERVIEW of THE PbPHAD MODEL

Authors of the PbPHAD model designed it based on 3 specific protocols, which are TCP, UDP and ICMP, because of their unique behavior when communicating among hosts, client and servers depending on the purpose and application used for a particular session. With this in mind, a more accurate statistical model with finer granularity, which represents the 3 chosen protocols, can be built for detecting the anomalous behavior of the testing data [2]. For each protocol, if each field is indexed as $i$, $i = 1,2,\ldots,n$, the model is built based on the ratio of the normal number of distinct field

values in the training data, R*i*, against the total number of packets associated with each protocol, N*i*. The ratio, P*i* = R*i*/N*i* represents the probability of the network seeing normal field values in a packet [2]. Thus, the probability of anomalies will be 1-P*i* for each corresponding field. Each packet header field containing values not found in the normal profile will be assigned a score of 1-$P_i$ and will be summed up to give the total value for that particular packet [2].

$$\text{Score packet} = \sum_{i=1}^{n} (1 - pi), \quad i = 1,2,\ldots n \qquad (1)$$

As the value of R*i* varies greatly, authors of PbPHAD model use log ratio in the PbPHAD model. The value of column TCP, UDP and ICMP in Table 1 is calculated based on:

*Relative percentage ratio of 1-log(Ri/Ni)*

to give the total probability of 1 for each protocol. Table 1 shows the formed PbPHAD statistical model for the selected host with IP address 172.016.114.050. The anomaly score of 0.000 shows that particular field is not related to that particular protocol.

**Table 1.** PbPHAD Statistical Model for Host 172.016.114.050 Incoming Packets

| Field_Name | R | N | ANOMALY SCORE | | |
|---|---|---|---|---|---|
| | | | TCP | UDP | ICMP |
| icmpchecksum | 2 | 72 | 0 | 0 | 0.039777586 |
| Icmpcode | 1 | 72 | 0 | 0 | 0.044461791 |
| Icmptype | 2 | 72 | 0 | 0 | 0.039777586 |
| udpchecksum | 2 | 23475 | 0 | 0.070056198 | 0 |
| Udplen | 42 | 23475 | 0 | 0.051784519 | 0 |
| udpdestport | 1027 | 23475 | 0 | 0.032599383 | 0 |
| Udpsrcport | 3 | 23475 | 0 | 0.067622802 | 0 |
| Tcpoption | 2 | 439879 | 0.063107164 | 0 | 0 |
| Tcpurgptr | 1 | 439879 | 0.066102472 | 0 | 0 |
| tcpchecksum | 2 | 439879 | 0.063107164 | 0 | 0 |
| tcpwindowsize | 1098 | 439879 | 0.035847881 | 0 | 0 |
| tcpflag | 9 | 439879 | 0.056607571 | 0 | 0 |
| tcpheaderlen | 3 | 439879 | 0.061355022 | 0 | 0 |
| tcpack | 235828 | 439879 | 0.012644092 | 0 | 0 |
| tcpseq | 232808 | 439879 | 0.012699788 | 0 | 0 |
| tcpdestport | 468 | 439879 | 0.039533001 | 0 | 0 |
| tcpsrcport | 5545 | 439879 | 0.028849915 | 0 | 0 |
| ipdest | 1 | 439879 | 0.066327816 | 0.092116832 | 0.103726615 |
| ipsrc | 28 | 439879 | 0.051928309 | 0.072118631 | 0.081207977 |
| ipchecksum | 1 | 439879 | 0.066327816 | 0.092116832 | 0.103726615 |
| ipprotocol | 3 | 439879 | 0.061580365 | 0.085523518 | 0.096302325 |
| ipttl | 1 | 439879 | 0.066327816 | 0.092116832 | 0.103726615 |
| ipfragptr | 2 | 439879 | 0.063332508 | 0.087956914 | 0.09904241 |
| ipfragpid | 65475 | 439879 | 0.018406917 | 0.025563738 | 0.028785619 |
| iplength | 702 | 439879 | 0.038006202 | 0.052783449 | 0.059435919 |
| iptos | 3 | 439879 | 0.061580365 | 0.085523518 | 0.096302325 |
| ipheaderlength | 1 | 439879 | 0.066327816 | 0.092116832 | 0.103726615 |
| **Total** | **543060** | | **1** | **1** | **1** |

### 3.1 Data Collection

The MIT Lincoln Lab. 1999 off-line intrusion detection evaluation data set [3] was downloaded and used to rebuild the PbPHAD model and run the experiment for the selected host 172.016.114.050. This dataset includes 2 weeks of testing data and one week of training data. Attack identification file is also available in the text format from the MIT Lincoln Lab. This dataset has become one of the *de facto* standards for test dataset among the IDS' researcher community.

### 3.2 Implementation the PbPHAD Model on the Selected Host

Figure 1 shows the PbPHAD IDS model that operates as the anomaly detector component within simple anomaly detection architecture. This architecture is used, in our work, to detect the anomalous packets, and thus to identify the false positives for the selected host 172.016.114.

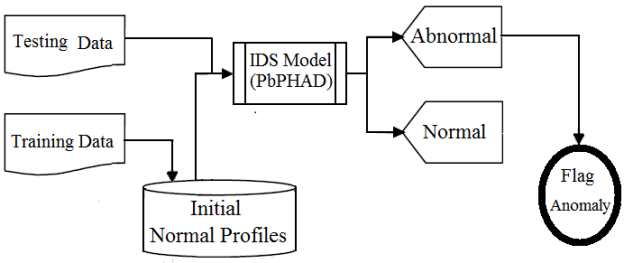



**Figure 1.** Anomaly Detection Architecture

Figure 2 shows the packet statistics of all testing incoming packets into the selected host 172.016.114 processed by PbPHAD model within the architecture shown in Figure 1. So, from Figure 2, it is seen that the size of anomalous data is high comparing with the size of the testing data. For this reason, the percentage of false positives is also high comparing with the size of the anomalous packets itself.

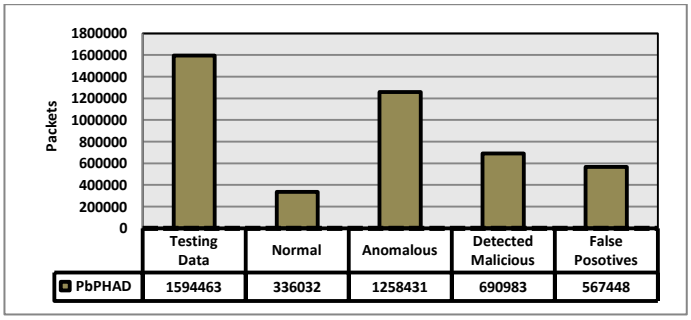



**Figure 2.** Statistics at The Packet Level Processed by PbPHAD Model for Host 172.016.114. Incoming Packets

## 4 NORMAL PROFILE UPDATING METHOD for FALSE POSITIVES REDUCTION

As we mentioned above, the percentage of false positives is high for the detected anomalous packets based on the PbPHAD statistical model alone. It is the shortcoming of this model.

In this paper a method for reducing the false positives is proposed. The main idea of our work is to investigate the ability of any anomaly detector to *re-process* the abnormal data (i.e. anomalous data) identified by that anomaly detector itself for *refining* these abnormal data from normal one before flag them as the end anomalous detected data. The whole idea of the proposed method is shown in the architecture in Figure 3.

Figure 3 shows a composition of two distinguished modules, the *anomaly detection module* and the *anomalous refining module*. For this architecture, we assume that one same anomaly detector should be applied in both modules. In this paper, we used the PbPHAD model as the anomaly detector applied in the both modules of the fore mentioned architecture. Next, we describe the operation of the aforesaid two modules.

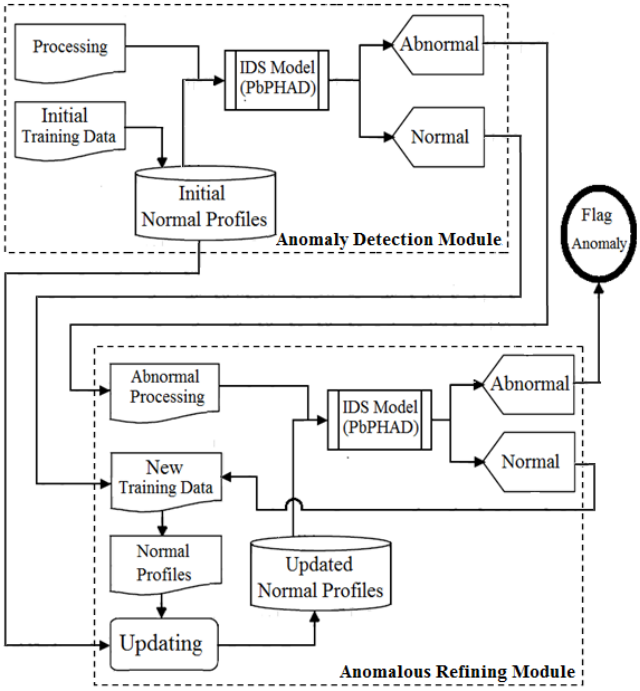



**Figure 3.** Normal Profile Updating Method for False Positives Reduction in Anomaly Detection

### 4.1 Anomaly Detection Module

This module operates as simple anomaly detection system. Firstly, using training data, static unchanged normal profiles are established by an anomaly detector component (i.e. the PbPHAD model in our experiment). Then, the anomaly detector uses the established normal profiles for processing data to identify which are normal and which are abnormal. Each of the normal data, the abnormal data, and the established normal profiles will be dealt as output data from this module and as input data for the next module, i.e. the *Anomalous Refining Module*.

### 4.2 Anomalous Refining Module

The main idea of operation of this module can be divided into two main steps: (1) creating the updated normal profiles using the normal data that output by the previous module, (2) the abnormal data, that output by the previous module too, will be refined from normal data.

Thus, in the first step the normal data will be re-used for creating new training data which used in creating respective normal profiles that in turn will enter, along with the initial normal profiles, in the

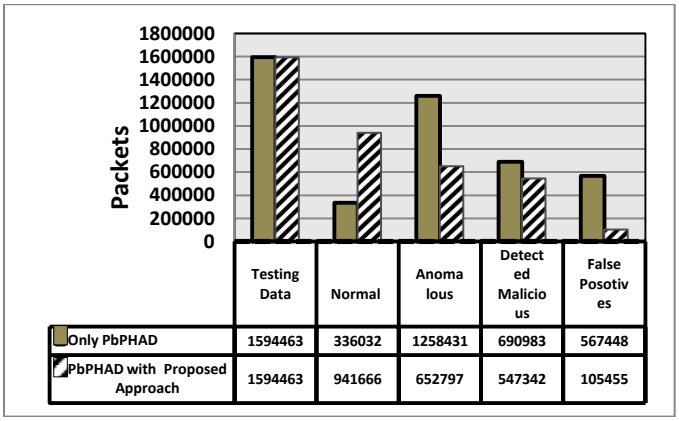
process of creating the updated normal profiles. In the second step the updated normal profiles will be used for further re-processing the abnormal data to refine them from the normal one. So, only the refined abnormal data will be flagged as the end anomaly detection. As a result, the false positives will be reduced.

## 5 SIMULATION DESIGN

Firstly, the PbPHAD model was redeveloped using the Structured Query Language (SQL Server 2008), which also was used as a database management system (DBMS) because it has the adequate power to be utilized to deal with huge number of packet records in the dataset. Then, we followed the designs in Figure 1 and Figure 3 as the flows for the simulations.

## 6 RESULT COMPARISION

Figure 4 shows packet statistics of testing data processed by the PbPHAD model for the selected host before and after applying the above described proposed method. The "False Positives" values shown in Figure 4 represent the final number of detected anomalous packets before and after applying the proposed method.
Seeing the Figure 4, if the size of "Anomalous" packets after applying the proposed method is compared with the size of "Anomalous" packets before using it, then it is clear that the proposed method could reduce the number of detected anomalous packets (approximately into 50%). This leads to reducing the number of false positives packets, however, into greater percentage (about 80% fewer false positives packets) as depicted in the Figure 4.




| | Testing Data | Normal | Anomalous | Detected Malicious | False Posotives |
|---|---|---|---|---|---|
| Only PbPHAD | 1594463 | 336032 | 1258431 | 690983 | 567448 |
| PbPHAD with Proposed Approach | 1594463 | 941666 | 652797 | 547342 | 105455 |

**Figure 4.** Statistics of Testing Data Processed for Host 172.016.114. Incoming Packets Before and After Reducing the False Positives

## 7 CONCLUSIONS

In this paper, we investigated a proposed method of normal profile updating in anomaly detection systems with the intent of reducing the false positive alerts. For this end, we tested the proposed method by applying it for reducing the false positives rate resulted in an existing anomaly detector, that is the PbPHAD model. The dataset, which was used for evaluation, were downloaded from MIT Lincoln Laboratory. One host was selected in our experiments. We created the simulations to study the ability of the proposed method to reduce the false positives rate. The results demonstrate that the proposed method was managed to get around 80% of false positive reducing percentage but with about 15% of reducing the true positives too. In this regard, a preliminary result can be concluded, that is the ability of reusing the refined testing data (i.e. the detected normal data which dealt as new training data) resulted after applying any anomaly detector in updating the normal profiles that in turn can be used in refining the abnormal data and thus in reducing the false positives. Therefore, our future works is to investigate the degree to which our proposed method is generalizable to a wide class of representative of anomaly detection techniques instead of the PbPHAD anomaly detector which was used in this work.

## 8 REFERENCES


[1] U. Singh, and S. Gupta. (2012). Incorporation of IDS in Real World Applications. Journal of Emerging Trends in Computing and Information Sciences, 3(1).

[2] S. B. Shamsuddin, and M. E. Woodward. (2007). Modeling protocol based packet header anomaly detector for network and host intrusion detection systems. In Cryptology and Network Security (pp. 209-227). Springer Berlin Heidelberg

[3] MIT Lincoln Laboratory 1999 DARPA Intrusion Detection Data Sets (1999), http://www.ll.mit.edu/IST/ideval/data/1999/1999_data_index.html

[4] M. Mahoney, and P. K. Chan. (2001). PHAD: Packet header anomaly detection for identifying hostile network traffic. Florida Institute of Technology technical report CS-2001-04, 1-17.

[5] D. Bolzoni. (2009). Revisiting anomaly-based network intrusion detection systems. University of Twente.

[6] W. Lee, and S. Stolfo, S. (1998). Data mining approaches for intrusion detection. In Proceedings of the 7th USENIX Security Symposium. San Antonio, TX.

[7] K. Scarfone, and P. Mell. (2007). Guide to intrusion detection and prevention systems (idps). NIST Special Publication, 800(2007), 94.

[8] J. Y. Kim, and R. E. Adviser-Gantenbein. (2008). Time-variant normal profiling for anomaly detection systems. University of Wyoming.

[9] S. Zuo. (2009). A dynamic normal profiling for anomaly detection. InWireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on (pp. 1-4). IEEE.