Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 6, June 2013, pg.339 – 349

RESEARCH ARTICLE

A Combined Protection for Entire Network Based On Immune Inspired Theories

P.S. ThumilVannan[1], S. Hirutiha[2]

[1]Assistant Professor/CSE, Arulmigu Meenakshi Amman College of Engineering, Kanchipuram, India

[2]M.E/CSE, Arulmigu Meenakshi Amman College of Engineering, Kanchipuram, India

Abstract— The combined protection for entire network identifies the traffic anomalies by monitoring the header information. Some attacks like denial of service led to develop the techniques for identifying the network traffic. The possibilities of traffic-analysis based mechanisms for attack and anomaly detection is also being studied. The motivation for this work came from a need to reduce the likelihood that an attacker may hijack the position machines to stage an attack on a third party. A position may want to prevent or limit misuse of its machines in staging attacks, and possibly limit the liability from such attacks. In particular, the utility of observing packet header data of outgoing traffic, such as destination addresses, port numbers and the number of flows, in order to detect attacks/anomalies originating from the position at the edge of a position is also dealt with. Detecting anomalies/attacks close to the source allows us to limit the potential damage close to the attacking machines. Project approach passively monitors network traffic at regular intervals and analyzes it to find any abnormalities in the aggregated traffic.

Key Terms: - Network Traffic; Traffic anomalies; anomaly Detection

I. INTRODUCTION

With the explosive growth of the network systems, information exchange became routine between computers around the world, thus the need for network security has become even more critical with the rise of information technology in everyday life. Meanwhile, the complexity of attacks is on the rise regardless of the beefed up security measures. Intrusion Prevention Systems provide an in-line mechanism focus on identifying and blocking malicious network activity in real time.

Along with the rapid development of network technology and fast upgrade of network attack technologies network security has become the focus of the age. However, current intrusion detection technologies, like statistical analysis, characteristics analysis and expert system etc, cannot meet well all the needs. Firstly, the lack of adaptability makes it difficult to detect unknown attacks; Secondly, the lack of robustness leaves each part isolated without communication. Therefore, the building of a detection system with adaptability and robustness is in pressing needs.

II. INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) is an automated system for the detection of computer system intrusions. The main goal of IDS is to detect unauthorized use, misuse and abuse of computer systems by both system insiders and external intruders. In parallel to rigorous investigation into intrusion prevention such as firewall and cryptography, the significance of research into IDS has been growing and various approaches have been suggested and developed. As one novel approach, a few computer scientists have proposed simple computer immune models for intrusion and computer virus detection. The promising initial results from these models motivate computer scientists to understand human immune systems more fully.

© 2013, IJCSMC All Rights Reserved

Early IDS's operated at the host level, whereas contemporary systems tend to be network-based. Host-based IDS's monitor a single host machine using the audit trails of a host operating system and network-based IDS's monitor any number of hosts on a network by scrutinizing the audit trails of multiple hosts and network traffic. Both host-based IDS's and network-based IDS's mainly employ two techniques: anomaly detection and misuse Detection. The anomaly detection approach establishes the profiles of normal activities of users, systems, system resources, network traffic and/or services and detects intrusions by identifying significant deviations from the normal behavior patterns observed from profiles. The misuse detection approach defines suspicious misuse signatures based on known system vulnerabilities and a security policy. The approach probes whether these misuse signatures are present or not in the auditing trails. These two techniques have different strengths and weaknesses and should be reciprocal in complete IDS.

IDS focus on presenting the analogy between human immune systems and network-based IDS's. Somayaji et al. present more general principles and suggest various possibilities for a computer immune system. In contrast, IDS concentrates on the design of competent network-based IDS's, and analyses the several outstanding features of the human immune system with the specific problem in mind.

A. Requirements of IDS

Before presenting the human immune system features, it is necessary to comprehend which functions are required to design a competent network-based IDS's. A careful examination of the literature allows the significant functions to be distilled into seven points:

- **Robustness:** it should have multiple detection points, which are robust enough against the attack and any system faults on IDS's. The critical weak point of IDS is its failure and subversion by intruders. If intruders already know the existence of IDS and can subvert it, then the effort to develop the IDS was futile.
- **Configurability:** it should be able to configure itself easily to the local requirements of each host or each network component. Individual hosts in a network environment are heterogeneous. They may have different security requirements. In addition to hosts, different network components such as routers, filters, DNS, firewalls, or various network services may have various security requirements.
- **Extendibility:** it should be easy to extend the scope of IDS monitoring by and for new hosts easily and simply regardless of operating systems. When a new host is added to an existing network environment and especially when the new host runs a different operating system that has a different format of audit data, it is not simple to monitor it in a consistent manner with existing IDS's.
- **Scalability:** it is necessary to achieve reliable scalability to gather and analyses the high-volume of audit data correctly from distributed hosts. In the case of the monolithic IDS's, the audit trail collection procedure is distributed and its analysis is centralized. However, it is very difficult to forward all audit data to a single IDS for analysis without losing the data. Even if it scales for all audit data correctly, it may cause severe network performance degradation.
- **Adaptability:** it should be dynamically adjusted in order to detect dynamically changing network intrusions. Computer system environments are not static. The normal activities of networks and intrusions are also continuously changing according to the environment.
- **Global Analysis:** in order to detect network intrusions, it should collectively monitor multiple events generated on various hosts to integrate sufficient evidence and to identify the correlation between multiple events. Many network intrusions often exploit the multiple points of a network. Thus, from a single host, they might appear to be just a normal mistake. But if they are collectively monitored from multiple points, they clearly can be identified as a single attack attempt.
- **Efficiency:** it should be simple and lightweight enough to impose a low overhead on the monitored host systems and network. A single IDS is expected to perform monitoring, data gathering, data manipulation and decision making. It may impose a large overhead on a system and could place a particularly heavy burden on CPU and I/O,resulting in severe system and network performance degradation.

Even though various approaches have been developed and proposed until now, no existing network-based model satisfies these requirements completely.

B. Human Immune System

The human immune system presents a valuable metaphor for computer network security systems and it is an appealing mechanism because the human immune system defends the body with high levels of protection features from pathogens, in a self-organized, robust and diverse manner.

The human immune system has two levels: innate and adaptive immune systems. The innate immune system has dendrite cells (DCs) which interact with antigens derived from the host tissue. DCs are critical in the initiation and activation of an immune response. Dendrite cells monitor the host tissue for evidence of damage. The second level of the HIS, the adaptive immune system mainly consists of T and B lymphatic cells. T cells

© 2013, IJCSMC All Rights Reserved

come in two different types, helper and killer cells. B cells look for antigens which match their receptors to bind with them. The connection triggers a signal for proteins from T helper cells to become fully activated. T helpers are also needed for the activation of T-killer cells which destroy cells infected by viruses and sometimes bacteria. The matching between receptors and antigens explains the core of HIS and most AIS implementations.

There are two major approaches to artificial immune systems, each presenting a different view point: the Negative Selection paradigm and Danger Theory.

i) The Negative Selection paradigm

The Negative Selection paradigm approach is based on the notion of a distinction between "self" from "non-self", which is mapped to normal behavior and abnormal behavior in network traffic. It follows the idea of immunology that the body is able to discriminate between self and non-self i.e. foreign protein molecules or antigens.

The negative selection algorithm consists of three phases: defining the self, generating detectors and monitoring any anomalies. In the first phase, self-patterns i.e. normal activities are defined and normal behavior patterns of a monitored system established. In the second phase, a number of random patterns are generated which are compared to each self- pattern defined in the first phase. If a detector pattern matches any newly profiled pattern during the monitoring stage, it is detected as a new anomaly which occurred in the monitored system.

An NS inspired architecture to identify anomalies (e.g., viruses) in computer systems. Since then, there has been a significant amount of effort from the research community to develop computational models inspired by the NS theory. Most of the existing studies have employed the "learning" mechanisms of the NS model to create a pattern-matching rule that can identify self-nonself features in the targeted system. For example, in NS inspired detection the normal behavior is regarded as self and the intrusive behavior as non-self. The detectors (e.g., patterns of the network traffic, host activities) are then randomly generated to emulate the generation of T cells in HIS. In the training stage these detectors are exposed to the normal events and any matching detectors are removed from the detector sets (i.e., the NS process). The remaining detectors are then used to detect the abnormal behavior. The detectors, which correctly match the anomalous behavior, are kept for future use. However, recent Tang et al. has proposed a new breed of NS called avidity based model for constructing detector set in IDS

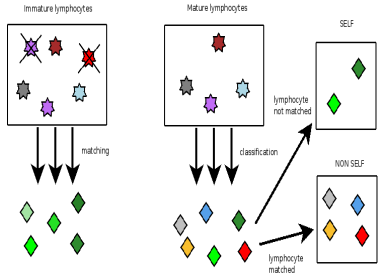

Fig.1.1. Negative selection paradigm.

ii) Danger Theory

Since 1959, the central dogma of immunology has stated that the human immune system reacts to entities that are not part of the organism. Therefore the decision to react is a result of the HIS classifying its own cells as self and everything else as non-self. The HIS performs the classification by recognizing proteins found on the surface of foreign cells (known as antigens). Foreign cells are different to cells present in the host (known as self-antigens) in structure and shape. For example, the intestinal tract is exposed to many different bacteria and food, neither of which is classically defined as `self', but neither of which produce an immune response. In addition, the model of self-nonself discrimination cannot explain the phenomena of auto-immune diseases. In the example of multiple sclerosis, the HIS attacks certain cells that it classifies as `self'.

In 1994, Polly Matzinger postulated that in the instance, the HIS was not reacting to self or nonself but was due to a protection mechanism of sensing danger. The manner in which danger is detected forms the basis of the Danger Theory. The Danger Theory does not deny the existence of self-nonself discrimination but rather states there are other contributory factors involved in the initiation of an immune response. It is now believed that the HIS responds to certain danger signals produced as a result of cellular necrosis; the unexpected stress and/or death of a cell.

Cell death is a natural process that occurs within the body as a result of homeostatic regulation. The process however comes from a pre-programmed and highly controlled mechanism, known as apoptosis. The Danger Theory proposes that the mechanisms behind cell death can cause different biochemical reactions that in turn can cause different danger signals. It is believed that these signals may facilitate an immune response.

Initialise the value of AIS parameters [antibody size (p), iterations (I_{max}), and percentage of antibody elimination (%B)]

© 2013, IJCSMC All Rights Reserved

Generate a population of P antibodies
For each antibody (iεP), calculate affinity (i)
Set current iteration of (I) =1
Do
For each antibody(i)
Calculate the number of clones (N_c) and clone antibody(i)
For each clone, apply inverse mutation to create a new antibody
Calculate the affinity of the new antibody
If affinity (new antibody) is better than the clone **then** clone= new antibody
Else perform pairwise interchange mutation to create a new antibody
Calculate the affinity of new the antibody
If affinity (new antibody) is better than the clone **then** clone = new antibody
antibody (i) = clone
Eliminate the worst antibody from the population based on %B
Create new antibodies to replace the eliminated antibodies
I=I+1
While $I \leq I_{min}$

Fig.1.2. Danger theory algorithm.

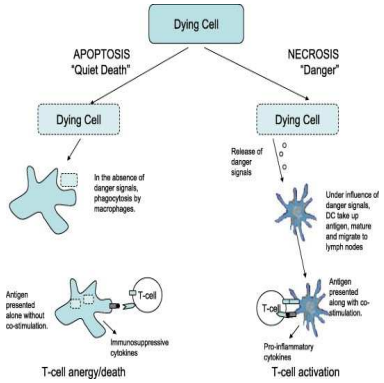

Fig. 1.3. Danger Theory Model.

C. Application of HIS in IDS

An intrusion detection system (IDS) is an automated system for the detection of computer system intrusions. The main goal of IDS is to detect unauthorized use, misuse and abuse of computer systems by both system insiders and external intruders. In parallel to rigorous investigation into intrusion prevention such as firewall and cryptography, the significance of research into IDS has been growing and various approaches have been suggested and developed. As one novel approach, a few computer scientists have proposed simple computer immune models for intrusion and computer virus detection. The promising initial results from these models motivate computer scientists to understand human immune systems more fully.

IDS aims to unravel the significant features of the human immune system, which would be successfully employed for a novel network intrusion detection model. Several salient features of the human immune system, which detects intruding pathogens, are carefully studied and the possibility and the advantages of adopting these features for network intrusion detection are reviewed and assessed.

i) The Danger Theory and anomaly detection

An intriguing area for the application of Artificial Immune Systems is the detection of anomalies such as computer viruses, fraudulent transactions or hardware faults. The underlying metaphor seems to fit particularly nicely here, as there is a system (self) that has to be protected against intruders (non-self). Thus if natural immune systems have enabled biological species to survive, Artificial Immune Systems cannot do the same to the computers, machines etc. Presumably those systems would then have the same beneficial properties as natural immune systems like error tolerance, distribution, adaptation and self-monitoring. A recent overview of biologically inspired approaches to the area can be found in Williamson. In the section The study will present indicative examples of such artificial systems, explain their current shortcomings and show how the Danger Theory might help overcome some of these.

© 2013, IJCSMC All Rights Reserved

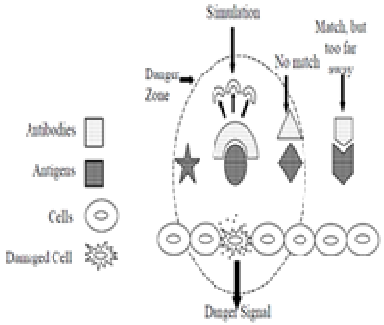

Fig.1.4. Danger theory based IDS

One of the first such approaches is presented by Forrest et al and extended by Hofmeyr and Forrest. The work is concerned with building an Artificial Immune System that is able to detect non-self in the area of network security where non-self is defined as an undesired connection. All connections are modeled as binary strings and there is a set of known good and bad connections, which is used to train and evaluate the algorithm. To build the Artificial Immune System, random binary strings are created called detectors. These detectors then undergo a maturation phase where they are presented with good, i.e. self, connections. If they match any of these they are eliminated otherwise they become mature, but not activated. If during their further lifetime these mature detectors match anything else, exceeding a certain threshold value, they become activated. It is then reported to a human operator who decides whether there is a true anomaly. If so the detectors are promoted to memory detectors with an indefinite life span and minimum activation threshold. Thus, It is similar to the secondary response in the natural immune system, for instance after immunization. An approach such as the above is known in Artificial Immune Systems as negative selection as only those detectors (antibodies) that do not match live on. It is thought that T cells mature in similar fashion in the thymus such that only those survive and mature that does not match any self-cells after a certain amount of time.

The network traffic behaviors can be observed in form of system call sequences, network protocols headers, port and socket as good categories with parameters in mapping the danger theory to IPS model. For example in "system processes" category, each system process has life span like biological cells. Also may be for example, the disconnection in network is normal (like apoptosis the normal death of cells) or abnormal (necrosis processes). Another example, TCP sessions can also die abnormally and feel distress such as receiving segment for the inappropriate ports. Thus, the cells in the model can be defined as category with parameters and processes, whilst any external input to the cell as antigen. It could be network traffic, command line argument or environment variables. A link between network signatures, IPC (inter process communication), protocol headers, port and socket, etc, and entities of danger theory can be created. For example, signal zero can be defined from sensing the deviation from the trained rules or, mapping the link between T-helper with process behavior analyzing module, or scanning the port or socket. As a result, the module can generate an activation signals to prevent the intrusion that can stop access by blocking the network traffic. The study assimilates the activation signal to T-killer to kill the pathogens cell.

The sensitivity of each category process in the system is determined during the learning and training period. It is possible to increase the accuracy of intrusion detection and prevention by associating received network with categories behavior. Likewise, false negative alert can be avoided by adding a direct call or categories flag for any unspecified program to the legitimate user signature. Meanwhile in many cases, false negative alerts can be avoided if rules for accessing any system or connection to the signature are added.. (Consider rephrasing) When there is any activation of danger signal i.e. detection of intrusion like T-killer, the intrusion will be prevented immediately by the network traffic either by blocking or by disconnecting the network connection. A relationship between the categories behavior with network traffic makes dynamic generation of network signatures possible by a clonal selection mechanism. For the purpose, a danger zone is classified as a combination of network received by observed categories, and time during which traffic was monitored.

ii) Artificial Immune Systems and Negative Selection

The negative selection algorithm was first used by Forrest et al as a means of detecting unknown or illegal strings for virus detection in computer systems. A population of detectors is created to perform the job of T-cells. These detectors are simple, fixed length binary strings. A simple rule is used to compare bits in two such strings and decide whether a match has occurred. Such a match is equivalent to a match between lymphocyte and antigen. Every randomly generated candidate detector is compared to every pattern in the self-set. The self-set is analogous to the self-proteins stored in the thymus in that it contains examples of self, against which detectors are tested. Any detector which matches any pattern in the self-set is not included in the detector set. New patterns can then be gathered from the system detector set then it can be guaranteed that that pattern is non-self and action can be taken accordingly. If an exact match were required by the matching rule, the detector set

© 2013, IJCSMC All Rights Reserved

would need to contain detectors for every possible illegal string which could occur. The study would lead to a huge computational overhead and an impractical algorithm. Instead, detection is probabilistic. Only r contiguous bits are required to be identical for a match to occur. The value of r is known as the matching threshold. Figure1.4 shows two 8 bit binary strings which match when the matching threshold is less than 5.

Two binary strings which match when $r \leq 4$ but do not match if $r > 4$. Matching bits are shown in bold. Much other work has concentrated on the use of artificial immune systems and the negative selection algorithm for virus detection and computer security. Work has also been done to use self/non-self discrimination to detect anomalies in time series data. The study is of particular interest and relevance to us. Time series data, in order to be used by negative selection based algorithms, must be transformed into a series of short binary strings. The study is done by sequentially sampling the data in blocks of a given size. For example, for a time series T= {t0, t1, …tn} and a pattern length of 4, the first pattern would contain P0={t0, t1, t2, t3}, the second would contain P1={t4, t5, t6, t7} and so on. Each value is converted and stored sequentially in a binary string which forms the final representation of the pattern.

The self-set is constructed using data patterns which represent the normal operation of the system. Patterns should be long enough to capture any important system behaviors. The detector set is then generated and negative selection is used to ensure that no detector matches any self-pattern. New data from the system can then be matched against these detectors to find anomalies. Work in the area has, to date, generally focused on the use of simulated datasets such as Mackey-Glass time series and simulated cutting tool data.

0 1 1 **1 1 0 1** 0
0 1 0 **1 1 0 1** 1

Fig.1.5 Two binary strings which match when $r \leq 4$ but do not match if $r > 4$. Matching bits are shown in bold.

In the anomaly detection systems created by Dasgupta, Forrest et al the binary encoding detailed above is used. However, by encoding self and detector sets as binary strings the study run the risk of destroying the semantic value of relationships between data items, as the r contiguous bits required to match can lie across word boundaries.

It has been shown, however, that increasing the number of symbols used to represent patterns (i.e. using a decimal rather than binary encoding greatly increases the required size of the detector set and, thus, increases the computational complexity of the algorithm. Another, simpler, matching rule can be applied in situations where a greater number of symbols is required, for whatever reason. The matching rule is based on the Euclidean distance between the patterns in p dimensional space, where p is the number of data items in each pattern. A threshold, D, is chosen for the matching rule and patterns are said to match if the distance between them is less than the threshold value. Patterns then cover an area of problem space with radius D.

Algorithm Negative-Selection

```
Input: A S⊂U ("self-set"); a set M⊂U ("monitor set"); an integer n
Output: For each element m∈M, either "self" or "non-self".
// training phase
1 d ← empty set
2 while |D|<ndo
3   d ← random detector
4   ifd does not match any element of Sthen
5     insert d into D
// classification phase
6 for eachm∈mdo
7   ifm matches any detector d∈D then
8     output "m is non-self" (an anomaly)
9   else
10     output "m is self"
```

III. ANOMOLY SYSTEM

The promising results of the DT inspired approach, intend to explore the combination of the working principles of both NS and DT in a single NIDS. As both theories can complement to each other.

A. Detection System

Performance evaluation of Negative selection and Dangerous theory has been compared by means of "True and False positive" ranking method. Hence by proving Dangerous theory express better performance analysis than Negative selection**.**

i) Failure of Detection System.

The attacker finds it easy to attack the system with fake signals. And also in the emerging network many are used for some good purpose. And in those there is a lot of chance for the attacker to send unwanted

© 2013, IJCSMC All Rights Reserved

information. In case of the fire alarm, if all the system are considered as trusted they could send false alarm where it lead to a heavy loss. And so the study needs a system to protect it. Hence the study develop a new system

B. Combined Detection System

The essence of Human Immune inspired (HIS) Negative selection Theory can be used for classification and the revelations of Dangerous theory can be used for Decision making. Which might be an better result yielding combination than DT and NS alone. Focus on analyzing the traffic at an egress router, Monitoring traffic at a source network enables early detection of attacks, to control hijacking of AD (administrative domain, e.g., position) machines, and to limit the squandering of resources.

There are two kinds of filtering based on traffic controlling point as shown in. Ingress filtering protects the flow of traffic entering into an internal network under administrative control. Ingress filtering is typically performed through firewall or IDS rules to control inbound traffic originated from the public Internet. On the other hand, egress filtering controls the flow of traffic leaving the administered network. Thus, internal machines are typically the origin of the outbound traffic in view of an egress filter. As a result, the filtering is performed at the position edge. Outbound filtering has been advocated for limiting the possibility of address spoofing, i.e., to make sure that source addresses correspond to the designated addresses for the position. With such filtering in place, the study can focus on destination addresses and port numbers of the outgoing traffic for analysis purposes.

Fields in the packet header, such as destination addresses and port numbers, and traffic volume depending on the nature of the traffic, can be used as a signal. By the way the study generates the signal.

Second step is to transform the signal using the Negative Selection (NS). Analyzing discrete domains such as address spaces and port Numbers poses interesting problems for wavelet analysis. The study employs the correlation in different domains to generate the suitable signal for analysis.

Finally the study uses the technique of finding the attack or the anomalies. This is done with the help of setting the threshold . And the study are comparing the result with the historical data .and the anomalies are detected using the statically analysis. The study report on the results employing correlation of destination addresses, port numbers and the distribution of the number of flows as monitored traffic signals.

i) Application:

Detecting anomalies through multiple levels will have a number of advantages:

- By setting a high threshold at each level, anomalies can be detected with high confidence;
- Depending on operator's filtering criteria, he/she can adjust the threshold between accuracy and flexibility.
- The attributes of attacks, such as the frequency and pattern, can be determined.

IV. TECHNIQUES USED

In the project the study is going to detect the anomalies using the following three techniques.

- Traffic Analysis at the Source
- General mechanism of detector.
- Trace.

A. Traffic Analysis at the Source.

The study focus on analysing the traffic at an egress router. Monitoring traffic at a source network enables early detection of attacks, to control hijacking of AD (administrative domain, e.g., position) machines, and to limit the squandering of resources.

There are two kinds of filtering based on traffic controlling point as shown in. Ingress filtering protects the flow of traffic entering into an internal network under administrative control. Ingress filtering is typically performed through firewall or IDS rules to control inbound traffic originated from the public Internet. On the other hand, egress filtering controls the flow of traffic leaving the administered network. Thus, internal machines are typically the origin of the outbound traffic in view of an egress filter. As a result, the filtering is performed at the position edge. Outbound filtering has been advocated for limiting the possibility of address spoofing, i.e., to make sure that source addresses correspond to the designated addresses for the position. With such filtering in place, the study can focus on destination addresses and port numbers of the outgoing traffic for analysis purposes.

B. General mechanism of detector.

Fields in the packet header, such as destination addresses and port numbers, and traffic volume depending on the nature of the traffic, can be used as a signal. By the way the study generates the signal.

© 2013, IJCSMC All Rights Reserved

Second step is to transform the signal using the Negative Selection (NS). Analyzing discrete domains such as address spaces and port Numbers poses interesting problems for wavelet analysis. The study employs the correlation in different domains to generate the suitable signal for analysis.

Finally the study uses the technique of finding the attack or the anomalies. The study is done with the help of setting the threshold. And the study are comparing the result with the historical data .and the anomalies are detected using the statically analysis. The study report on the results employing correlation of destination addresses, port numbers and the distribution of the number of flows as monitored traffic signals.

C. Trace:

To verify the validity of the approach, the study runs the algorithm on four traces of network traffic. First, the study examines the method on traces from the University of Southern California that contain real network attacks. Second, to inspect the performance of the detector on backbone links, the study examine the mechanism on Danger Theory.

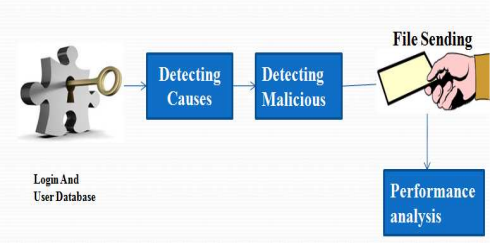

Fig. 1.6. Modules Involved.

V. DETECTING CAUSES

Wireless Sensor Networks (WSNs) represent an emerging system paradigm that tightly couples the network with its deployment environment. Relying on resource constrained embedded devices for communication, processing, and sensing, WSNs can experience unexpected problems during deployment, due to hardware, software, or environmental anomalies. The volatility of WSNs is always in tension with ambitious application goals, including long term deployments of several years, large scale networks of thousands of nodes, and highly reliable data delivery. As the WSN field matures, strategies for detecting (and possibly correcting) the anomalies that are inherent to their physically coupled low-end system design will only grow in importance. In fact, providing appropriate tools that can effectively detect and respond to anomalies can greatly increase uptake of the technology by stakeholders.

While significant work on conventional network management tools exists, WSN counterparts have been slow to gain traction within the community. One of the main challenges for WSN anomaly detection is determining where to embed the intelligence for detecting and localizing anomalies. While centralized approaches rely on more comprehensive network state information available at the back-end and are thus simpler to implement, distributed approaches provide more scalable and responsive anomaly detection, as nodes can detect network problems in their vicinity immediately. A challenge for distributed anomaly detection is its implementation complexity and the limited state information available at resource-constrained sensor nodes.

Another key requirement for any anomaly detection strategy is catering to the needs and to the feedback of the human operator. A user-friendly detection strategy should provide several modes of notification, such as email and SMS alerts, and adapt its frequency of alerts to user feedback, in order to avoid “crying wolf” too many times and risking user apathy to more significant alerts. An effective anomaly detection strategy should also provide the versatility to cater to diverse user requirements, supporting both network managers who require detailed diagnostic information, and end users who are only interested in data quality.

One shortfall of existing strategies is that none of them comprehensively addresses network, node and data level anomalies in WSNs. A common reason for the application-specific design choices in sensor networks that tend to tailor anomalies detection strategies to a family of applications with a given set of constraints and assumptions. The lack of comprehensive anomaly detection strategies for WSNs contributes to slower adoption and more frustration in deploying and maintaining these networks. From a WSN user or operator perspective, it is crucial that a network management tool embeds the required intelligence to detect all possible anomaly types, as the network is perceived holistically as an intelligent data delivery system.

To design such system-level tools demands a comprehensive understanding of all types of WSN anomalies, their likely causes, and their potential solutions. The chapter examines WSN anomalies from a systems perspective, covering anomalies that arise at the network, node and data levels. It introduces a simple process for diagnosing anomalies in WSNs for detection, localization, and root cause determination. A survey of existing anomaly detection strategies also reveals their major design choices, including architecture and user

© 2013, IJCSMC All Rights Reserved

support, and yields guidelines for tailoring new anomaly detection strategies to specific WSN application requirements.

A. Types of WSN Anomalies

The study begins by defining the scope of the term anomalies in the chapter. Anomalies can range from faults, such as complete hardware failures, to unexpected system performance, such as gradual degradation. Note that certain outliers in spatial or temporal sensor data can signify events of interest in the monitored area, and should not be reported as anomalies to the network operator unless explicitly specified. Otherwise, separate data analysis tools can handle these outliers.

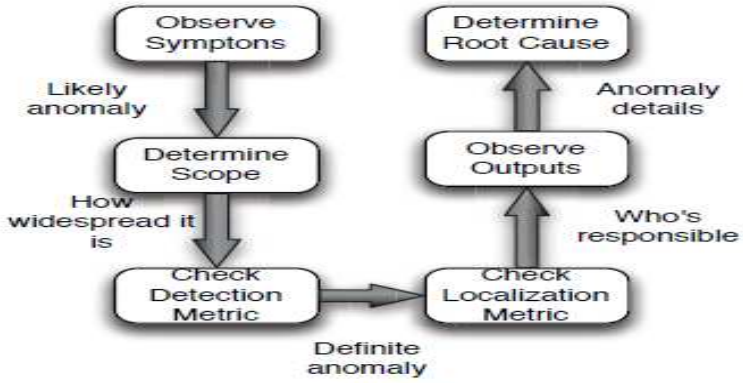

Fig. 1.7. Anomaly diagnosis process

The conditions that signal an anomaly relate to user policy for a particular application. For instance, an operator sets the frequency and timeout period for data delivery by the sensor nodes. These determine thresholds for detecting and reporting anomalies to operators. Whenever data from a sensor node is not received according to the expected schedule, the operator can be notified. The frequency, urgency and level of detail within the notification can also be user-defined.

Anomaly diagnosis is established in conventional network management tools; however, the study revisit it here from a WSN perspective to expose how it can apply to the different types of WSN anomalies. The main goal of WSN anomaly diagnosis is mapping the symptoms to possible root causes, in order to possibly suggest remedial actions. The process for characterizing a sensor network fault or anomaly is very similar to diagnosing an illness. The symptoms must first be examined, followed by a specification of the scope of the affected region. The process then involves some testing on the affected region (detection), where the operator must localize the anomaly causing node and expect some diagnostic information on the nature of the problem. The feedback yields a hypothesis on the most likely root cause of the problem.

Based on the above process, the study now examines how to detect common WSN anomalies, which fall into three broad categories: (1) network anomalies; (2) node anomalies; (3) data anomalies.

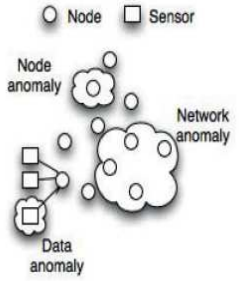

Fig. 1.8. Scope of each anomaly types

B. Complete Ids Based On His

The frequent attacks on network infrastructure, using various forms of denial of service (DoS) attacks and worms, have led to an increased need for developing techniques for analyzing and monitoring network traffic. If efficient analysis tools were available, it could become possible to detect the attacks, anomalies and take action to suppress them before they have had much time to propagate across the network.

© 2013, IJCSMC All Rights Reserved

VI. INTRUSION DETECTION MECHANISM- MODULE DESCRIPTION

A. Login:

In this module the user are allowed to sign up as a new user. Once the user signs in there is a separate log maintained for the particular user. The existing user can sign in to perform the operation.

B. Client:

The user who wants to send a file is treated as client. Before selecting a file to send, the client has to provide his details to the server. The client is restricted to choose the file which creates traffic in the network.

C. Detecting Causes:

Appropriate parameters such as number of packet loss, jitter, delay, etc. However, as the anomaly detection process is sensitive and dependent to this initial step protects the flow of traffic entering into an internal network under administrative control. Once the user signs in to the application his details are stored in the server. After choosing a particular file the details of file is gathered in order to prevent traffic.

D. Detecting Malicious:

In this module the activities of user after choosing a file is checked. An separate log is created for the user. Here all the details including size and type of the file he chooses is stored. If he chooses the file which may create traffic (Size above 800KB and Executable file) the error count in his account gets added.

E. File Sending:

Server checks the size and type of the file chosen by the client. If the server finds that it may create traffic then server provide request to the client to choose another file.

F. Performance analysis.

The performance of the NIDS could be explained as

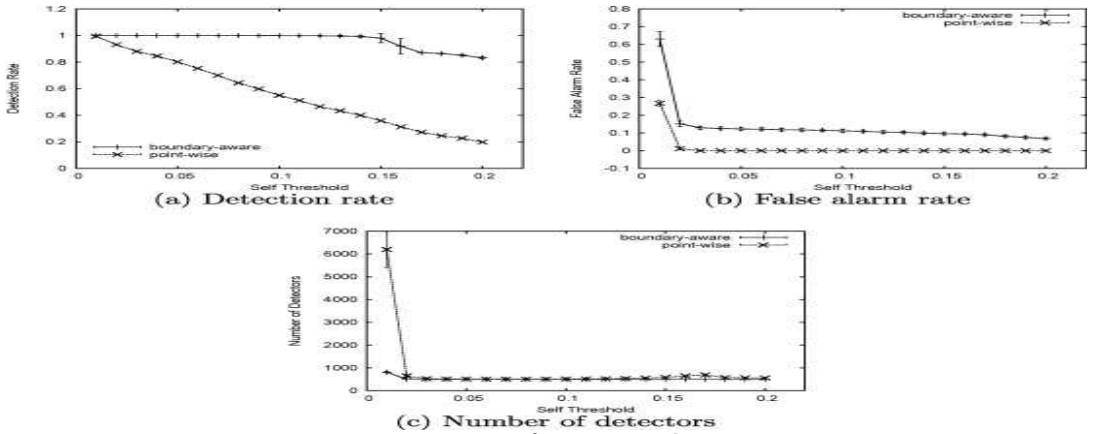

Fig. 1.9. Performance graph

VII. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Implementation is the process of converting a new system design into operation. It is the phase that focuses on user training, site preparation and file conversion for installing a candidate system. The important factor that should be considered here is that the conversion should not disrupt the functioning of the organization.

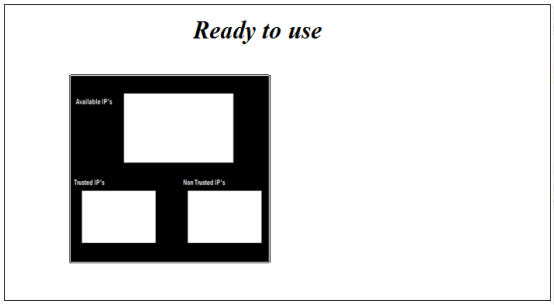

Fig. 1.10. Detecting IP's

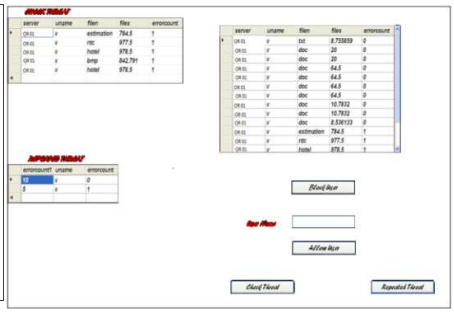

Fig. 1.11. Sending File

© 2013, IJCSMC All Rights Reserved

VIII. FUTURE PLAN

The results show that statistical analysis of aggregate traffic header data may provide an effective mechanism for the detection of anomalies within a campus or edge network. The effectiveness of the approach in post-mortem and real-time analysis of network traffic is studied. The results of the analysis are encouraging and point to a number of interesting directions for future research.

IX. CONCLUSION

The project has covered almost all the requirements. Further requirements and improvements can easily be done since the coding is mainly structured or modular in nature. Improvements can be appended by changing the existing modules or adding new modules. The feasibility of analyzing packet header data through wavelet analysis for detecting traffic anomalies is studied. Specifically, the study proposed the use of correlation of destination IP addresses, port numbers and the number of flows in the outgoing traffic at a Detecting Malicious.

REFERENCES

[1] Hofmeyr and S. Forrest, "Architecture for an Artificial Immune System," Evolutionary Computation, vol. 8, no. 4, Dec. 2000, pp. 443–73.
[2] S. Forrestl., "Self-Nonself Discrimination in A Computer," Proc. IEEE Symp. Security and Privacy, Oakland, USA, May 1994, pp. 202–12.
[3] H. Wang, D. Zhang, and K. G. Shin, "Change-Point Monitoring for the Detection of DoS Attacks," IEEETrans. on Dependable and Secure Computing, vol. 1, no. 4, Oct. 2004, pp. 193–208.
[4] M. Burgess, "Probabilistic Anomaly Detection in Distributed Computer Networks," Science of ComputerProgramming, vol. 60, no. 1, Mar. 2006, pp. 1–26.
[5] Ada, G. L. & Nossal, G. J. V. (1987), "The Clonal Selection Theory", Scientific American, 257(2), pp. 50-57.
[6] Aisu, H. & Mizutani H. (1996), "Immunity-Based Learning – Integration of Distributed Search and Constraint Relaxation", Proc. of the IMBS'96
[7] Bradly, D. W. & Tyrrell, A. M. (2000), "Immunotronics: Hardware Fault Tolerance Inspired by the Immune System", Lecture Notes in Computer Science , 1801, pp. 11-20.
[8] Carter, J. H. (2000), "The Immune System as a Model for Pattern Recognition and Classification", Journal of the American Medical Informatics Association, 7(3), pp. 28-41.
[9] Dasgupta, D. & Forrest, S. (1996), "Novelty Detection in Time Series Data Using Ideas From Immunology", Proc. of the ISCA'96.
[10] Dasgupta, D., Cao, Y. & Yang, C. (1999), "An Immunogenetic Approach to Spectra Recognition", Proc. of GECCO'99, pp. 149-155.
[11] Dasgupta, D. (2000), "An Immune Agent Architecture for Intrusion Detection", Proc. of GECCO'00–Workshop Proceedings, pp. 42-44.
[12] De Castro, L. N., & Von Zuben, F. J., (2001), "The Construction of a Boolean Competitive Neural Network Using Ideas From Immunology", International Journal of Neurocomputing(in print).

© 2013, IJCSMC All Rights Reserved