IMPROVED IDS USING LAYERED CRFS WITH LOGON RESTRICTIONS AND MOBILE ALERTS BASED ON DEVIANT SYSTEM BEHAVIOUR

Arpitha M[1], Geetha V[1],

Gowranga K H[2] and Bhakthavathsalam R[2]

[1]Department of Information Science and Engineering
Alpha College Of Engineering, Bangalore, India
arpitha119@gmail.com, geethaanjali78@gmail.com

[2]Supercomputer Education and Research Center
Indian Institute of Science, Bangalore, India
gowranga@serc.iisc.ernet.in, bhaktha@serc.iisc.ernet.in

ABSTRACT

With the ever increasing numberand diverse type of attacks, including new and previouslyunseen attacks, the effectiveness of an Intrusion DetectionSystem is very important. Hence there is high demand to reduce the threat level in networks to ensure the data and services offered by them to be more secure. In this paper we developed an effective test suite for improving the efficiency and accuracy of an intrusion detection system using the layered CRFs. We set up different types of checks at multiple levels in each layer.Our framework examines various attributes at every layer in order to effectively identify any breach of security. Once the attack is detected, it is intimated throughmobile phone to the system administrator for safeguarding the server system. We established experimentally that the layered CRFs can thus be more effectivein detecting intrusions when compared with the other previouslyknown techniques.

KEYWORDS

Network Security, Intrusion Detection, Layered Approach, Conditional Random Fields, Mobile Phones

1. INTRODUCTION

The current state of network is vulnerable they are prone to increasing number of attacks. Thus securing a network from unwanted malicious traffic is of prime concern. A computer network needs to provide continuous services, such as e-mail to users, while on the other it stores huge amount of data which is of vital significance. Recently, there has been increasing concern over safeguarding the vast amount of data stored in a network from malicious modifications and disclosure to unauthorized individuals. Intrusion Detection Systems (IDS) [1] are based on two concepts; matching of the previously seen and hence known anomalous patterns from an internal

database of signatures or building profiles based on normal data and detecting deviations from the expected behaviour[2].Based on the mode of deployment, the Intrusion Detection Systems are classifiedas Network based [3] andHost based [4]. Network based systems make a decision by analysing the network logs and packet headers from the incoming and outgoing packets. Host based systems monitor's individual systems and uses system logs extensively to make any decision. Intrusion Detection Systems are either Signature based or Behaviour based [5]. The Signature based systems build a model based on the available knowledge of the attacks. The Behaviour based systems which build a model based on the available knowledge of the normal use of the system.We propose and evaluate the use of the CRFs [6] also which is a novel technique for the task of Intrusion Detection along with Layered Approach. Further, our system can be used as a standalone system monitoring an entire Network or a single Host or even a single Application running on a particular host.

1.1 Intrusion Detection

Intrusion detection [7] is the process of monitoring computers or networks for unauthorized entrance, activity, or file modification. An IDS (Intrusion Detection System) is a device or application used to inspect all network traffic, thereby detecting if a system is being targeted by a network attack such as a denial of service attack. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. IDS protect a network and attempt to prevent intrusions. They don't fully guarantee security, but when used with security policy, vulnerability assessments, data encryption, user authentication, access control, and firewalls, they can greatly enhance network safety [8].

Intrusion detection systems serve three essential security functions: they monitor, detect, and respond to unauthorized activity by company insiders and outsiders. Intrusion detection systems use policies to define certain events that, if detected will issue an alert. Certain intrusion detection systems have the capability of sending out alerts, so that the administrator of the IDS will receive a notification of a possible security incident. Many intrusion detection systems not only recognize a particular incident and issue an appropriate alert, they also respond automatically to the event. Such a response might include logging off a user, disabling a user account, and launching of scripts.

2. NEW SCHEME FOR ROBUST IDS

Intrusion detection as a discipline is fairly immature. Commercially available examples of successful intrusion detection systems are limited, although the state of the art is progressing rapidly. The whole concept of our paper is to build an intrusion detection system which is very accurate in detection of request from unknown computers and which is very fast to respond to such intrusions taking place in system which gives efficiency [9] to the system and intimating the administrator about the intrusions through the mobile phone. To achieve this system, we have integrated the properties of conditional random fields and the layered approach.

2.1 Existing System

There are a number of methods and frameworks been proposed and many systems have been built to detect intrusions. Various techniques such as association rules [10], clustering, naive Bayes classifier, support vector machines, genetic algorithms, artificial neural networks, and others have been applied to detect intrusions. These existing systems suffer from a wide range of problems.

a. The features are limited to the entry level of the packets and require the no. of records to be large. They tend to produce a large number of rules that increases the system's complexity.
b. Some methods consider the features independently and are unable to capture the relationship between different features of a single record. This further degrades the attack detection strength of the system.
c. Some existing systems are attack specific and hence they would build networks which rapidly increases as the detection load increases.

2.2 Proposed System

In our proposed system we describe the Layer-based Intrusion Detection System (LIDS) [11] [12]. The LIDS draws its motivation from what we call as the Airport Security model, where a number of security checks are performed one after the other in a sequence. Similar to this model, the LIDS represents a sequential Layered Approach [13] and is based on ensuring availability, confidentiality, and integrity of data and (or) services over a network.

The goal of using a layered model is to reduce computation and the overall time required to detect anomalous events. The time required to detect an intrusive event is significant and can be reduced by eliminating the communication overhead among different layers. We define four layers they are Probe layer, DoS layer, R2L layer, and U2R layer. Each layer is separately trained with a small set of features. The layers essentially act as filters that block any anomalous connection, thereby eliminating the need of further processing at subsequent layers enabling quick response to intrusion.

The effect of such a sequence of layers is that the anomalous events are identified and blocked as soon as they are detected. Once the attack is detected, it is intimated through mobile phone to the system administrator for safe guarding the server system.

We implement the LIDS and select four set of features which reduces the computational time. Methods such as naive Bayes [14] assume independence among the observed data. To balance this trade-off, we use the CRFs that are more accurate, though expensive, but we implement the Layered Approach to improve overall system performance.

Our proposed system, Layered CRFs, performs significantly better than other systems.

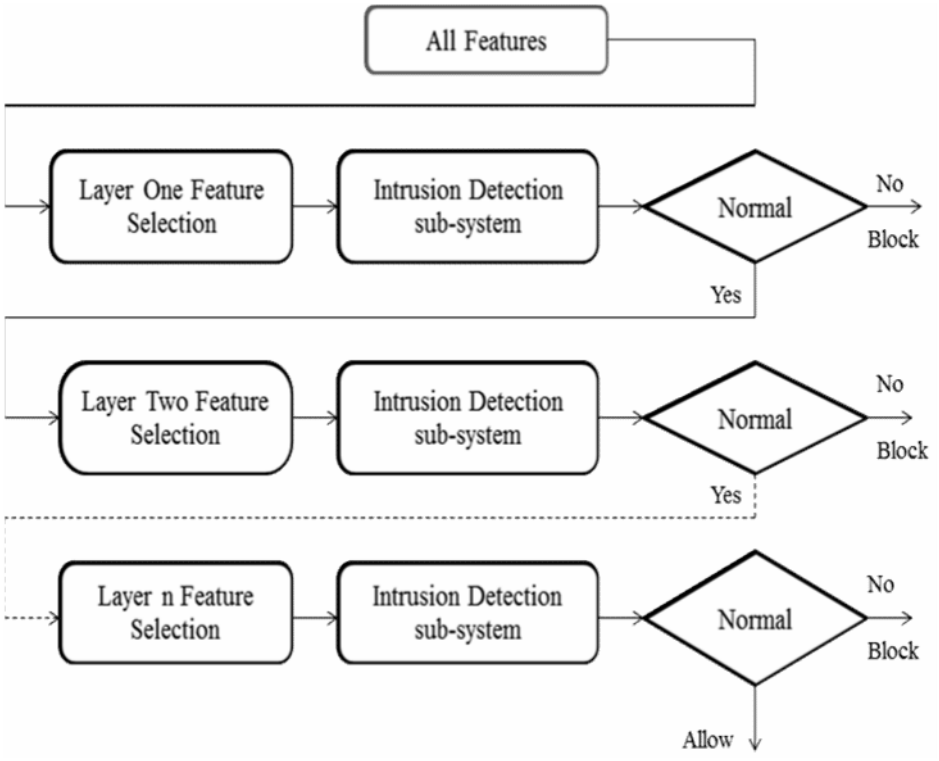

Figure 1. Proposed System

3. IMPLEMENTATION

Implementation is the stage 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.

3.1 Layered Approach for Intrusion Detection

Layer-based Intrusion Detection System (LIDS) draws its motivation from what we call as the Airport Security model, where a number of security checks are performed one after the other in a sequence. Similar to this model, the LIDS represents a sequential Layered Approach and is based on ensuring availability, confidentiality, and integrity of data and (or) services over a network. Figure 2 gives a generic representation of the framework. The goal of using a layered model is to reduce computation and the overall time required to detect anomalous events. The time required to detect an intrusive event is significant and can be reduced by eliminating the communication

overhead among different layers. Every layer in the LIDS framework is trained separately and then deployed sequentially.

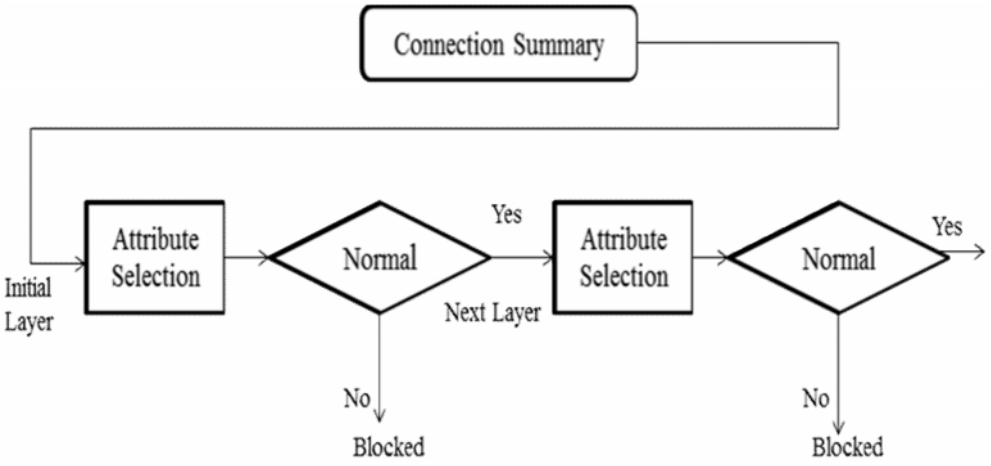

Figure 2. Layered Approach for Intrusion Detection

We define four layers that correspond to the four attack groups [15]. They are Probe layer, DoS layer, R2L layer, and U2R layer. Each layer is then separately trained with features. Feature selection is significant for Layered Approach. The layers essentially act as filters that block any anomalous connection, thereby eliminating the need of further processing at subsequent layers enabling quick response to intrusion. The effect of such a sequence of layers is that the anomalous events are identified and blocked as soon as they are detected. Hence, we implement the LIDS and select four set of features for every layer. In many situations, there is a trade-off between efficiency and accuracy of the system and there can be various avenues to improve system performance. To balance this trade-off, we use the CRFs that are more accurate, though expensive, but we implement the Layered Approach to improve overall system performance. The performance of our proposed system, Layered CRFs is comparable to that of the decision trees and the naive Bayes, and our system has higher attack detection accuracy.

3.2 Conditional Random Fields for Intrusion Detection

Conditional models are systems that are used to model the conditional distribution [16] over a set of random variables. Such models have been extensively used in the natural language processing tasks. Conditional models offer a better framework and can be used to model rich overlapping features among the visible observations. CRFs are undirected graphical models used for sequence tagging.

The CRFs 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 CRFs for intrusion detection. 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. However, when these features are analyzed together, they can provide meaningful information.

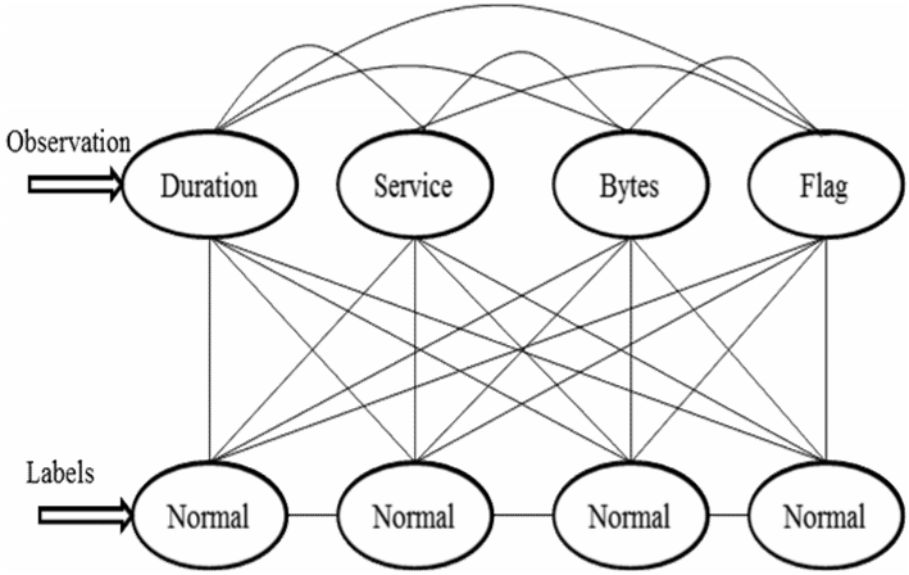

Figure 3. Conditional Random Field

3.3 Integrating Layered Approach with Conditional Random Fields

A natural choice is to integrate them to build a single system that is accurate in detecting attacks and efficient in operation.

Probe layer

The probe attacks are aimed at acquiring information about the target network from a source that is often external to the network. Hence, basic connection level features such as the "duration of connection" and "source bytes" are significant while features like "number of files creations" and "number of files accessed" are not expected to provide information for detecting probes.

DoS layer

For the DoS layer, traffic features such as the "percentage of connections having same destination host and same service" and packet level features such as the "source bytes" and "percentage of packets with errors" is significant.

R2L layer

The R2L attacks are one of the most difficult to detect as they involve the network level and the host level features. We therefore select both the network level features such as the "duration of

connection" and "service requested" and the host level features such as the "number of failed login attempts" among others for detecting R2L attack.

U2R layer (User to Root attacks)

The U2R attacks involve the semantic details that are very difficult to capture at an early stage. Such attacks are often content based and target an application. Hence, for U2R attacks, we select features such as "number of file creations" and "number of shell prompts invoked," while we ignored features such as "protocol" and "source bytes."

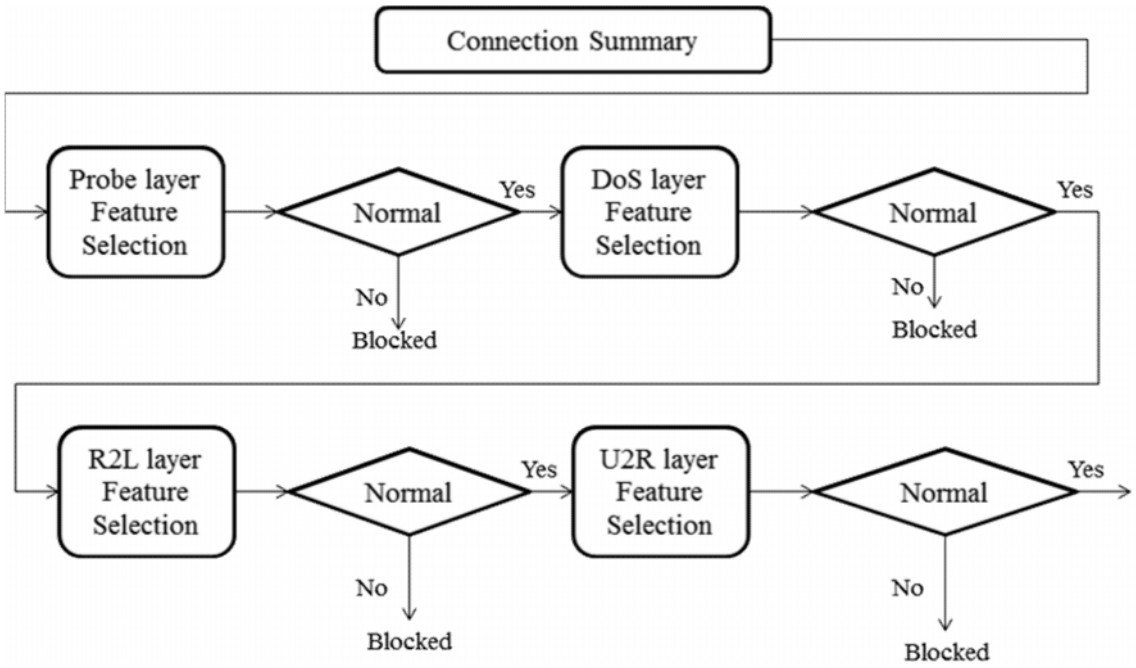

Figure 4. Integrating Layered Approach with Conditional Random Fields

3.4 Time Scheduling of Users

With the increasing number of user's everyday on the internet, networks are getting burdened with a huge amount of requests, processes, services etc. Every user performs some or the other function when they are using the internet this increases the load on the network. In our system we have scheduled a particular day and time for the users who are a part of an organisation, restricting their usage to prevent intrusions and wastage of bandwidth in the network. In simple words they are assigned a particular day and time to login to their accounts and work on their requirements.

We have symbolised the days of a week as 0-6 depicting Sunday-Saturday and time on a 24 hour clock. This feature is added in the database and access will be given only to those users who login

at the right schedule. Users who do not login at the right schedule are denied access and will be treated as intruders.

3.5 Intrusion Detected Message Sent to System Administrators Mobile

The mobile device can be used to keep oneself informed about the attacks. The corresponding error messages are generated and are intimated to the server which schedules the appropriate actions. Mobile alerts are sent to the server administrator's mobile through usage of a GSM modem connected to the COM port of your computer and making sure that the Java communication API is installed in your system. We also carefully consider several parameters such as text message centre number found in your mobile in the SMS settings menu and the baud rate and type of flow control for receiving, type of flow control for sending, the number of data bits, the number of stop bits, and the type of parity.

In a nutshell, intrusion detection systems do exactly as the name suggests: they detect possible intrusions. More specifically, IDS tools aim to detect computer attacks and/or computer misuse, and to alert the proper individuals upon detection.

Through various methods, both detect when an intruder/attacker/burglar is present, and both subsequently issue some type of warning or alert. Using the previous example, firewalls can be thought of as a fence or a security guard placed in front of a house. They protect a network and attempt to prevent intrusions, while IDS tools detect whether or not the network is under attack or has, in fact, been breached. IDS tools thus form an integral part of a thorough and complete security system.

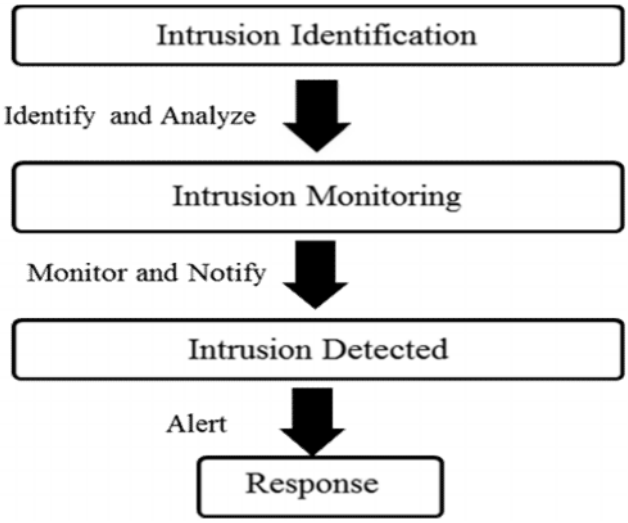

Figure 5. Proposed IDS system Activities

Intrusion detection systems [17] serve three essential security functions: they monitor, detect, and respond to unauthorized activity by company insiders and outsider intrusion. An IDS installed on

a network provides much the same purpose as a burglar alarm system installed in a house. Intrusion detection systems use policies to define certain events that, if detected will issue an alert. In other words, if a particular event is considered to constitute a security incident, an alert will be issued if that event is detected. Many intrusion detection systems not only recognize a particular incident and issue an appropriate alert, they also respond automatically to the event. Such a response might include logging off a user, disabling a user account, and launching of scripts. Our system has the capability of sending out alerts, so that the administrator of the IDS will receive a notification of a possible security incident in the form of a page, email, or SNMP trap [18].

3.6 Proposed Algorithm

Step 1: Select the number of layers, n, for the complete system.
Step 2: Separately perform features selection for each layer.
Step 3: Plug in the layers sequentially such that only the connections labelled as normal are passed to the next layer
Step 4: For each (next) test instance perform Steps 5 through 8.
Step 5: Test the instance and label it either as attack or normal.
Step 6: If the instance is labelled as an attack, block it and then identify it as an attack with the corresponding layer name at which it is detected and go to step 4. Pass the sequence to next layer.
Step 7:If the current layer is not the last layer in the system, test the instance and go to step 6. Else go to step 8.
Step 8: Test the instance and label it either as normal or as an attack. If the instance is labelled as an attack, block it and identify it as an attack corresponding to the layer name.
Step 9: If the instance is labelled as an attack at any layer then intimate it to system admin's mobile with a corresponding appropriate message of attack.

4. RESULTS

We have represented the results for every operation that is performed as per the proposed algorithm. Our results confirm that the implementations that are carried out are effectively displaying the outcomes accurately.

We have produced results for eight possible conditions on the use of four CRFs. type of a system is very much suited in an organizational network. Finally, our system has the advantage that the number of layers can be increased or decreased depending upon the environment in which the system is deployed, giving flexibility to the network administrator.

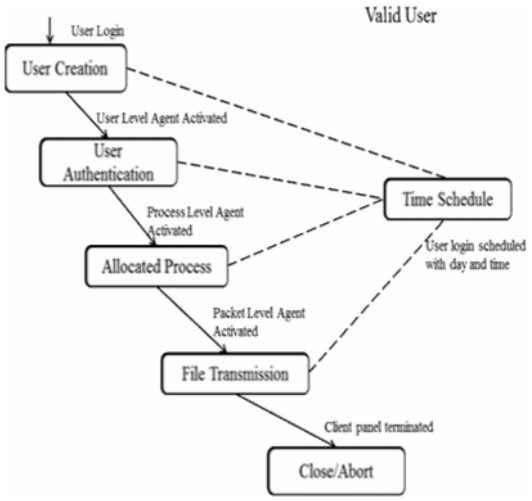

Figure 6. Sequence of checks for Valid User.

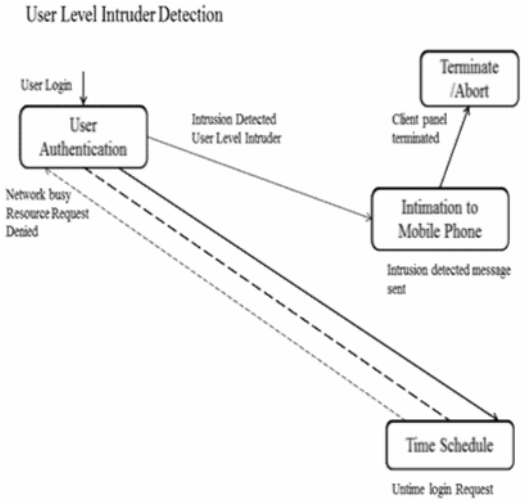

Figure 7. Intrusion detected at User Level

For every valid user the security checks are followed in sequence in the given time schedule and the necessary action is taken. At the first level the user level agent gets activated and authenticates the user. At the second level the process level agent gets activated and the user can use the process allocated. At the next level the packet level agent gets activated and the user is allowed to transmit files. Once all the necessary operations of the user is fulfilled the client panel sucessfully terminates.

At the first level user is checked for authentication and if he is not authenticated he is treated as an intruder. Next he is checked for the use of processes and if he is violating the allocated process uasage he is treated as a process level intruder. At the third level if the file transmissions are

crossing the fixed bytes of data he is treated as a packet level intruder.Adding to al these even when the user tries to access at a time which is not scheduled he will be treated as an intuder [19].

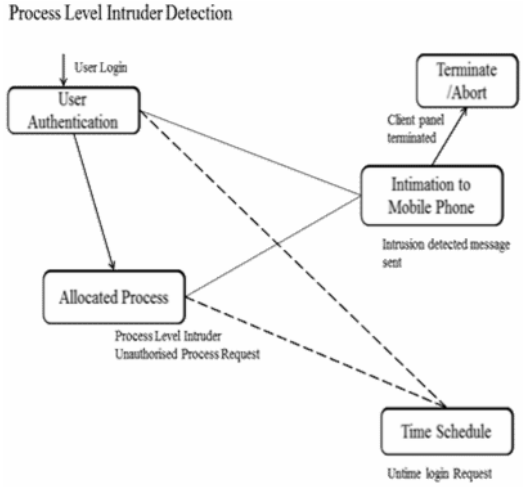

Figure 8. Intrusion detected at Process Level.

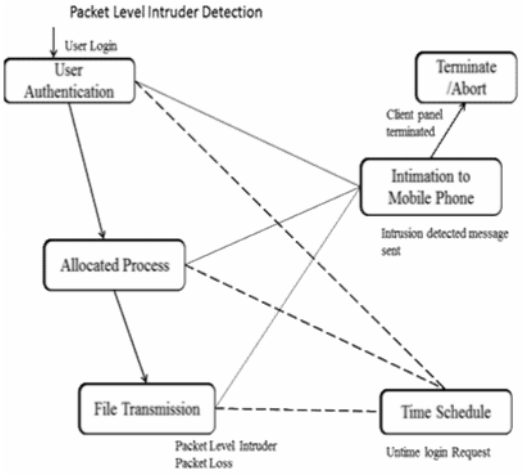

Figure 9. Intrusion detected at Packet Level.

The results represent the intrusions detected at various levels of the security checks. For an invalid user or intruder the security checks are explicit. All the events of intrusions are alerted to the sytem administrator to his mobile phone to ensure that the intuder is blocked at the level at which he is detected ensuring security to the IDS.

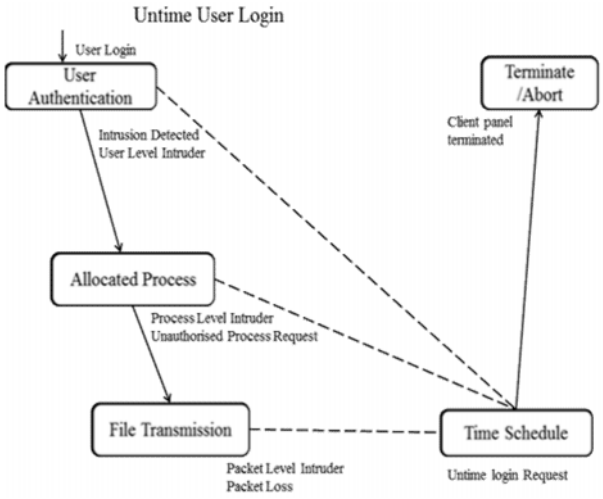

Figure 10. Intrusion detection at Untime Login of user.

From the above results it can be concluded that our proposed system is capable of detecting intrusions at various layers by using layered conditional random fields and when detected they will be first intimated to the system administrator at the server side so that necessary actions can be taken. The particular intruder will be denied of access thereby indicating that the intruder is blocked at a particular level.

5. CONCLUSIONS

As security incidents become more numerous, IDS tools are becoming increasingly necessary. They round out the security factor, working in conjunction with other information security tools, such as firewalls, and allow for the complete supervision of all network activity. In our project we have implemented a system for building robust and efficient intrusion detection systems by implementing the layered conditional random fields using mobile phones.

Ideally, the best IDS tools combine both approaches. That way, the user gets comprehensive coverage, making sure to guard against as many threats as possible. It is clear that using intrusion detection systems is an important and necessary tool in the security manager's arsenal.

Our system addresses the problem of finding intruders effectively and blocking them as soon as they are detected. The Layered Approach is a signature based system and the Conditional Random Fields is an anomaly based system thus combining these both systems would result in a hybrid system. Taking a thread from the integrated approach we have established scheduled user login and successful communication with the system administrator through the mobile phones.
Our system can help in identifying an attack once it is detected at a particular layer, which expedites the intrusion mechanism, thus minimizing the impact of an attack. Once the attack is detected, it is intimated through mobile phone to the system administrator for safe guarding the server system. This type of a system is very much suited in an organizational network. Finally,

our system has the advantage that the number of layers can be increased or decreased depending upon the environment in which the system is deployed, giving flexibility to the network administrator.

ACKNOWLEDGEMENT

The authors sincerely thank the authorities of Supercomputer Education and Research Center, Indian Institute of Science for the encouragement and support.

REFERENCES

[1] Intrusion Detection Systems Basics. http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[2] PengNing and SushilJajodia,(2003) "Intrusion Detection Techniques", in H. Bidgoli (Ed.), The Internet Encyclopedia, John Wiley & Sons.

[3] Harley Kozushko, (2003) Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems. http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/IntrusionDetectionPaper.pdf

[4] SANS Institute, (2012) Intrusion Detection FAQ.http://www.sans.org/resources/idfaq/

[5] E. Tombini, H. Debar, L. Me, and M. Ducasse, (2003) "A Serial Combination of Anomaly and Misuse IDSes Applied to HTTP Traffic", Proc. 20th Annual Computer Security Applications Conference (ACSAC'04), pp. 428-437.

[6] Kapil Kumar Gupta, BaikunthNath, KotagiriRamamohanarao, (2010)"Conditional Random Fields for IntrusionDetection",Proc. IEEE dependable and secure computing.

[7] McHugh, John, (2001) "Intrusion and Intrusion Detection", Technical Report, CERT Coordination Center,Software Engineering Institute, Carnegie Mellon University.

[8] J. P. Anderson, (2010) "Computer Security Threat Monitoring and Surveillance",http://csrc.nist.gov/ publications/history/ande80.pdf

[9] Y.-S. Wu, B. Foo, Y. Mei, and S. Bagchi, (2003)"Collaborative Intrusion Detection System (CIDS): AFramework for Accurate and Efficient IDS", Proc. 19th Ann. Computer Security Applications Conf. (ACSAC '03), pp. 234-244.

[10] R. Agrawal, T. Imielinski, and A. Swami, (1993)"Mining Association Rules between Sets of Items in Large Databases", Proc. ACM SIGMOD, vol. 22, no. 2, pp. 207-216.

[11] K.K. Gupta, B. Nath, and R. Kotagiri, (2006)"Network Security Framework", Int'l J. Computer Science and Network Security, vol. 6, no. 7B,pp. 151-157.

[12] K.K.Gupta, (2009)"Robust and Efficient Intrusion Detection Systems", ww2.cs.mu.oz.au/~kgupta/files/phd-completion.pdf

[13] Kapil Kumar Gupta, BaikunthNath, RamamohanaraoKotagiri, (2010) "Layered Approach Using Conditional Random Fields for Intrusion Detection", Proc. IEEE dependable and secure computing.

[14] N.B. Amor, S. Benferhat, and Z. Elouedi, (2004)"Naive Bayes vs.Decision Trees in Intrusion Detection Systems", Proc. ACM Symp.Applied Computing (SAC '04), pp. 420-424.

[15] T. Abraham, (2008)"IDDM: Intrusion Detection Using Data Mining Techniques". http://www.dsto.defence./gov.au/publications/2345/DSTO-GD-0286.pdf

[16] C. Sutton and A. McCallum, (2006) "An Introduction to Conditional Random Fields for RelationalLearning", Introduction to Statistical Relational Learning, Edited by LiseGetoor and Ben Taskar,Published by The MIT Press.

[17] SANS Institute, (2001) "Understanding Intrusion Detection Systems", SANS Institute. http://www.sans.org/reading_room/whitepapers/detection/understanding-intrusiondetectionsystems

[18] Rebecca Bace, "An Introduction to Intrusion Detection and Assessment for System and Network Security Management", ICSA, Inc.
http://www.icsalabs.com/icsa/docs/html/communities/ids/whitepaper/Intrusion1.pdf

[19] Arpitha M, Geetha V, Gowranga K H and Bhakthavathsalam R, (2013) "Test Suite for Intrusion Detection by Layered Conditional Random Fields Using Mobile Phones",Lecture Notes in Electrical Engineering 131, Springer Science,NY, pp 537-549.
http://www.springer.com/engineering/signals/book/978-1-4614-6153-1

AUTHORS

Arpitha M has obtained her B.E. degree from the Dept of Information Science and Engineering, Alpha College of Engineering affiliated to Visvesvaraya Technological University. She has successfully completed her final semester project at IISc. She has presented a paper at the NetCom2012 conference. Her interests are Wireless Technology and Network Security.

Geetha V has obtained her B.E. degree from the Dept of Information Science and Engineering, Alpha College of Engineering, Bangalore affiliated to Visvesvaraya Technological University. She has successfully completed her final semester project at IISc. She has published a paper in the NCS-2012 conference. Her interests are Network Security & Mobile Communication.

Mr.Gowranga K H is currently working as a Scientific Assistant in Supercomputer Education and Research Center, IISc, Bangalore. His research interests include Wireless Networks, Webmail Systems, and Digital Communication.

Dr.Bhakthavathsalam R is presently working as a Senior Scientific Officer in SERC, IISc, Bangalore. His areas of interests are Electromagnetics, Wireless Networks and Pervasive Computing and Communication. He is a Member of ACM and CSI.