A NEW LAYERED APPROACH FOR INTRUSION DETECTION

1Ramana Rao H. C and 2Janardhana Reddy Y. R
1PRRM Engineering College, Hyderabad
2AVR&SVR Engg College, Nandyal,

Abstract:
In this paper, we have addressed the dual problem of Accuracy and Efficiency for building robust and efficient intrusion detection systems. Our experimental results show that CRFs are very effective in improving the attack detection rate and decreasing the FAR. Having a low FAR is very important for any intrusion detection system. Further, feature selection and implementing the Layered Approach significantly reduce the time required to train and test the model. Even though we used a relational data set for our experiments

INDEXING TERMS : Layered Approach, Random Fields

Existing System:-
The field of intrusion detection and network security has been around since late 1980s. Since then, a number of methods and frameworks have been proposed and many systems have been built to detect intrusions. Various techniques such as association rules, clustering, naive Bayes classifier, support vector machines, genetic algorithms, artificial neural networks, and others have been applied to detect intrusions. In this section, we briefly discuss these techniques and frameworks. Experimental results on the benchmark KDD ’99 intrusion data set show that our proposed system based on Layered Conditional Random Fields outperforms other well-known methods such as the decision trees and the naive Bayes. The improvement in attack detection accuracy is very high, particularly, for the U2R attacks (34.8 percent improvement) and the R2L attacks (34.5 percent improvement). Statistical Tests also demonstrate higher confidence in detection accuracy for our method.

Proposed System:-
Other approaches for detecting intrusion include the use of autonomous and probabilistic agents for intrusion detection. These methods are generally aimed at developing a distributed intrusion detection system. To overcome the weakness of a single intrusion detection system, a number of frameworks have been proposed, which describe the collaborative use of network-based and host-based systems. Systems that employ both signature based and behavior-based techniques are discussed in the authors describe a data mining framework for building adaptive intrusion detection models.

Two Approach

INTEGRATING LAYERED APPROACH WITH CONDITIONAL RANDOM FIELD
The LIDS represents a sequential Layered Approach 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. This can be achieved by making the layers autonomous and self-sufficient to block an attack without the need of a central decision-maker.

Each layer is then separately trained with a small set of relevant features. Feature selection is significant for Layered Approach and discussed in the next section.

In order to make the layers independent, some features may be present in more than one layer. 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.

**Main Modules:**

**CONDITIONAL RANDOM FIELD**

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.

**Probe layer**

The probe attacks are expected at acquiring information about the target network from a source that is often external to the network.

**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” are significant. To detect DoS attacks, it may not be important to know whether a user is “logged in or not.”

**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 selected 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 selected features such as “number of file creations” and “number of shell prompts invoked,” while we ignored features such as “protocol” and “source bytes.”

```
Connection
   ↓
  LAYER1
  ↓
  LAYER2
  ↓
  LAYER3
  ↓
  LAYER4
```

**Algorithm & Training:**

Step 1: Select the number of layers, n, for the complete system.

Step 2: Separately perform features selection for each layer.

Step 3: Train a separate model with CRFs for each layer using the features selected from Step 2.

Step 4: Plug in the trained models sequentially such that only the connections labeled as normal are passed to the next layer. Testing

Step 5: For each (next) test instance perform Steps 6 through 9.
Step 6: Test the instance and label it either as attack or normal.
Step 7: If the instance is labeled as attack, block it and identify it as an attack represented by the layer name at which it is detected and go to Step 5. Else pass the sequence to the next layer.
Step 8: If the current layer is not the last layer in the system, test the instance and go to Step 7. Else go to Step 9.
Step 9: Test the instance and label it either as normal or as an attack. If the instance is labeled as an attack, block it and identify it as an attack corresponding to the layer name.

CONCLUSIONS

In this paper, we have addressed the dual problem of Accuracy and Efficiency for building robust and efficient intrusion detection systems. Our experimental results show that CRFs are very effective in improving the attack detection rate and decreasing the FAR. Having a low FAR is very important for any intrusion detection system. Further, feature selection and implementing the Layered Approach significantly reduce the time required to train and test the model. Even though we used a relational data set for our experiments, we showed that the sequence labeling methods such as the CRFs can be very effective in detecting attacks and they outperform other methods that are known to work well with the relational data. This can further be extended to implement pipelining of layers in multicore processors, which is likely to result in very high performance.

REFERENCES


