Multi Model Transmission Analysis Based Efficient Intrusion Detection System for Improved Performance

A. Anthony Paul Raj, J. K. Kani Mozhi

***Abstract:** The problem of intrusion detection in network systems has been well studied. There exist numerous techniques in the mitigation of intrusion attacks, but they struggle to produce expected performance. To solve this issue, an efficient multi model analysis based approach is described in this article. The network systems faces various challenges like modification, distributed denial of service, spoofing, eavesdrop and so on. The proposed multi model approach monitors the network packets in different level by analyzing the payload, path, host and frequency of incoming packets. The method considers the frequency of packets, path being used, and frequency of transmission, host details and payload features. For each features, the method computes the trust measure which has been used to classify the packets. The method estimates cumulative multi mode trust weight towards any packet being received. According to the weight measures of different analysis, the attack has been identified. The proposed method improves the performance of intrusion detection and increases the accuracy.*

***Keywords:** Intrusion Detection Systems, Multi Model Analysis, Payload Analysis, Path Analysis, Frequency Analysis, MMTW.*

I. INTRODUCTION

The modern information technology support the human society in accessing different network resources and services through different devices namely mobile phones, PDA and many more. However, the sophistication of service access encourages the malicious users to intrude the network to perform different malicious activities. When the malicious is capable of intrude into the network where the service is available, he can perform different threats like Distributed Denial of Service Attack, where the malicious user sends large number of packets towards the access point which suffocate service and leads to higher packet drop. This affects the genuine user in accessing the service. By performing the DDoS attack, the malicious user can degrade the service performance which affects the network performance also.

Similarly, the malicious user can perform eavesdrop attack, by dropping the incoming packet anonymously. By performing eavesdrop attack; the throughput performance of the network can be reduced highly. Similarly, there are number of threats can be performed by the malicious user towards the degradation of network services. To mitigate such attacks, there are number of methods available and discussed earlier. The host based algorithms, identifies the intrusion based on the details of host by maintaining a set of host which are identified as malicious. Only the host from where the packet is received is classified as malicious and the host id should be present in the malicious list. Similarly, there are rule based algorithms and systems like SNORT are available, which identifies the network intrusion attack according to the rule set. The packet feature has been extracted and matched with the rule available, if there is any match found then the packet has been identified as malicious. The data mining techniques has been used in intrusion detection in network systems. The pattern based algorithms are available for the intrusion detection which maintains the set of patterns of intrusion attack. Suppose the pattern match with the incoming packet feature, and then it has been identified as malicious threat. Similarly, there are number of approaches available for the detection of intrusion attacks. However, they suffer to achieve higher performance in producing accuracy in intrusion detection. To overcome this, this paper presents a multi model network analysis algorithm for efficient intrusion detection. The method analyzes various features of network communication like payload, frequency, packet, path and hosts. Based on the result of analysis of various features, the method performs intrusion detection.

The payload is the network feature which represents the frequency of packets towards any service point. Any service point is capable of handling number of requests at a specific point of time. The malicious user would generate huge payload packets to degrade the service performance and to perform intrusion attack. By monitoring the payload features of the network packets, the intrusion attack can be detected efficiently. Similarly, the path analysis is the most important one in the problem of intrusion detection. The routes available and the path followed have been used to perform this. Based on the route available, and the path used, the analysis is performed to identify the trustworthy of transmission. Frequency analysis is performed to measure the trustworthy of the incoming frequency of packets being received at any point of time. By analyzing the features of transmission in multiple ways, the accuracy of intrusion detection can be improved. Such approach is presented in this paper and how it has been implemented is presented in the next sections.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author

A.Anthony Paul Raj *, Research Scholar, Periyar University, Salem, India.

Dr. J. K. Kani Mozhi *, Professor, Department of Computer Applications, Sengunthar Arts & Science College, Salem Road, Tiruchengode, Namakkal, Tamil Nadu,

II. RELATED WORKS

There are number of approaches available for the problem of intrusion detection in networks. This part of article details few methods around the problem.

(Jabez Z, 2015) present an outlier based intrusion prevention technique which monitors th incidents and store information to generate reports. The method also generate alert to the administrator. Each neighbor has been measured for their outlier factor which has been used to classify them towards attack.

(Jayakumar Kaliappan, 2015) present a genetic algorithm based multi unit detection system where each unit act independently. Each unit detects the threat based on the voting rule and combines the result of each unit to produce result. The feature selection has been performed using genetic algorithm and the majority vote has been selected for classification.

(Uma R. Salunkhe, 2017) present a ensemble based classification algorithm for improved detection of intrusion attack. The method works in both data and feature level; uses the opinion obtained from different experts to improve the performance of system.

(T.H.Divyasree, 2018) present a ensemble approach with vector machine for efficient detection of intrusion attack. The method works based on the minimum enclosing ball approach. For different threat types distinct classifier has been designed. The feature selection is performed using chi-square test.

(Lidong Wang, 2017) present the application of big data in the problem of IDS. Also introduces various data mining algorithm and describe their application in detail. The method considers multiple features for classification and real world traffic has been considered.

(Bekti CahyoHidayanto, 2017) present a pattern mining algorithm for NIDS which works based on apriori and frequent pattern max algorithms. The method classifies the incoming traffic according to the frequency of pattern arrived earlier. Based on the frequency of pattern, the classification of real-time payload has been performed.

(Pooja Preet, 2017) Intrusion detection system for manet [7], defines the IDS for the mobile adhoc network. The method enforces distributed IDS in multiple nodes of Manet which has been shared between them.

(Yuancheng Li, 2018) present a sequence learning machine based IDS which uses online sequences towards the support of advanced metering infrastructure. The model is designed to support the electric data transmission through networks. The OSLEM algorithm produces noticeable result in intrusion detection.

(Bing Zhang, 2018) present a combined approach for NIDS which uses principle component analysis for the feature selection and classifies using naïve bayes classification algorithm. The method reduces the dimensionality in feature selection with PCA.

(D. Gupta, S. Singhal, et.al, 2016) present a rule based classifier for NIDS. The k means algorithm has been used for the clustering of network data and the classification is performed with linear regression analysis. The method has been evaluated with KDD data set.

(Ali Ahmadian Ramaki, 2018) present a taxonomy based classifier for IDS. The fields of alert have been generated by systematic mapping to produce taxonomy. According to the fields of taxonomy, the classification and alert generation is performed.

(Ruirui Zhang, 2019) present a spatial partition based negative selection approach for IDS in WSN. The self set distribution in real world space has been analyzed and further different subspace has been generated. Based on the space generated, the classification is performed.

(Jiadong Ren, 2019) present a data optimization based IDS which is a hybrid algorithm which combines both isolation forest and GA. The isolation forest algorithm removes the outliers where GA is used to optimize the preprocessing result. The classification is performed with random forest algorithm. The DO-IDS algorithm produces noticeable results in IDS.

(Simone A. Ludwig, 2019) present a ensemble based IDS with the support of Neural network. The method monitors the activity of users in the network and generates ensembles for different class. Such ensembles generated are feed to the neural network to perform classification.

(M. Almi'ani, et.al, 2018) present a self organized map based IDS where the network data has been used to generate SOM and clustered using K means. The agglomerative clustering has been applied to SOM neurons to perform classification. The methods discussed have the deficiency of producing higher accuracy in detecting intrusion attacks.

III. MULTI MODEL TRANSMISSION ANALYSIS BASED INTRUSION DETECTION

The proposed multi model transmission analysis algorithm monitors the incoming traffic. Upon receiving a packet, the method extracts the payload features, frequency feature, path features and payload features. Using the features extracted, the method performs various analyses like payload analysis, path analysis, and frequency analysis. Based on the value of all the above, the method estimates the cumulative trust weight for the incoming packets. Based on the value, the method performs intrusion detection. The proposed method has been detailed in this section.

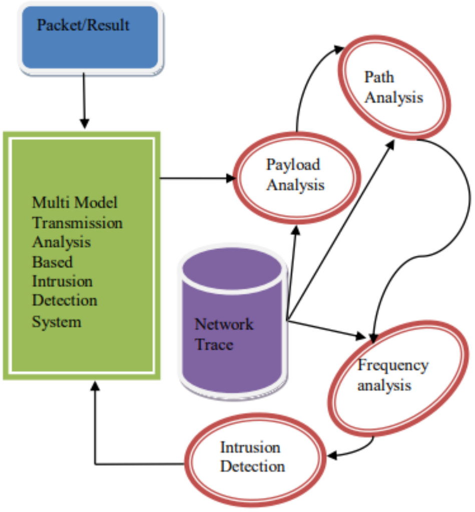

Figure 1: Architecture of Proposed Multi Model

Transmission Analysis Intrusion Detection System

The Figure demonstrates the architecture of future intrusion detection system and it shows the various stages of intrusion detection system. Each stage has been explained in detail in this section.

A. *Payload Analysis*

The network service has been accessed by different users and in general, the service data has fixed length. The malicious user in turn would generate packets with higher volume data to the service. By analyzing the payload features of the data packet received, the trustworthy of the packet can be identified. The incoming packets are received and payload features are extracted. Similarly, the previous traces of the network service accessed by the different user have been retrieved from the network trace. Using the trace, the method extract the payload features and estimates the average payload value. Based on the average payload value and the payload value of the packet received, the method estimates the payload weight to conclude the trustworthy of the packet received.

Payload Analysis Algorithm:

```
Given: Network Trace NetTrace, Packet P
Obtain: Payload Weight Sw.
Start
    Read network trace NetTrace, and packet P.
    Extract Payload Feature Sf = $\int \sum \mathrm{PayloadFeature} \in \mathrm{P}$
    Collect all the traces of service S.
    Service Trace St =
    $\int_{\mathrm{i=1}}^{\mathrm{size(NetTrace)}} \sum \mathrm{NetTrace(i).Service} == \mathrm{P.Service}$
    Compute Average Payload value APv = $\frac{\sum_{i=1}^{size(St)} \sum Pf \in St(i)}{size(st)}$
    If size(pf)<= Apv then
        Compute Payload weight Pw =1 × 0.8
        Return Pw
    Else
        Return 1 × 0.3
    End
Stop
```

The working principle of payload analysis algorithm is presented above which shows how the payload weight has been estimated for the incoming packet. The payload weight has been measured based on the payload feature of incoming and previous traces. Estimated payload weight value has been used to perform intrusion detection in the final stage.

B. *Path Analysis*

The path analysis is the process of analyzing the path being used for data transmission. The network would contain number of paths to reach the service point. The genuine node would follow the routing protocol to deliver the packet but the presence of malicious node would change the path and does not follow them. By identifying and monitoring the path of data transmission, the presence of the malicious node can be identified. For example, if the routing algorithm enforced would use shortest path for data transmission and some other algorithms uses traffic free routes in data transmission. So, the path analysis algorithms extract the path feature and extract the list of paths followed by previous data transmission. Using both of them, the method estimates the average hop count and estimates the path weight for the current packet. Based on the path weight estimated, the intrusion detection can be performed.

Path Analysis Algorithm:

```
Given: Network Trace NetTrace, Packet P
Obtain: Path Weight Pw

Start
    Read network trace NetTrace, Packet P
    Extract packet path Pr = $\int \mathrm{Path} \in \mathrm{P}$
    Collect the traces of service access from network trace.
    Service trace St =
$\int_{\mathrm{i=1}}^{\mathrm{size(NetTrace)}} \sum \mathrm{NetTrace(i).Service} == \mathrm{P.Service}$
Identify distinct path Dr = $\int_{\mathrm{i=1}}^{\mathrm{size(St)}} \sum (\mathrm{St(i).path} \nexists \mathrm{Dr}) \cup \mathrm{Dr}$
Compute average hop count Ah= $\frac{\sum_{i=1}^{size(Dr)} Dr(i).Hops}{size(Dr)}$

    If hopCount(Pr)<=Ah then
        Compute path weight Pw = 1 × 0.9
        Return Pw
    Else
        Compute path weight Pw = 1 × 0.4
    End

Stop
```

The working principle of path analysis algorithm is presented above which explains how the path weight for the incoming packet has been estimated. Based on the value of path weight being estimate, the method concludes the presence of network threat in the path or transmission.

C. *Frequency Analysis*

The Packet's flow playing an important role to identifying presence of intrusion attacks. By monitoring the frequency of packets towards any service point, the intrusion attack can be detected. According to this, the frequency analysis algorithm monitors the incoming packet towards the service point. From the packet received, the method identifies the host and uses the network trace to identify the number of times the user has accessed the service and number of times the user has accessed correctly. Using this information, the method estimates the frequency weight towards the request to conclude the trustworthy of the user and the request.

Frequency Analysis Algorithm:

```
Given: Network Trace NetTrace, Packet P
Obtain: Frequency Weight Fw.
Start
    Read network trace NetTrace and packet P.
    Identify the host information.
    Host H = $\int \mathrm{Host} \in \mathrm{P}$
    Extract the host logs from network trace NetTrace.
    Host Trace Ht = $\int_{\mathrm{i=1}}^{\mathrm{size(NetTrace)}} \sum \mathrm{NetTrace(i).Host} == \mathrm{H}$
    Compute total access Toa = size(Ht)
    Compute Number of correct access Noca =
    $\int_{\mathrm{i=1}}^{\mathrm{size(Ht)}} \sum \mathrm{Ht(i).status} == \mathrm{Correct}$
    Compute average correct access Aca = $\frac{Noca}{Toa}$
    If Aca>ATh then
        Compute frequency weight Fw = 1×0.8
        Return
    Else

        Compute frequency weight Fw = 1×0.2

        return

    end

Stop
```

The above algorithm demonstrates how the frequency analysis is performed for a packet being received. The method estimates the number of correct access and average correct access to measure the frequency weight. Estimated frequency weight has been used to perform intrusion detection finally.

D. *Intrusion Detection*

The proposed intrusion detection algorithm reads the incoming packet and extracts different features like payload, path and frequency. Based on the features being extracted, the method performs path analysis, payload analysis and frequency analysis. Each analysis returns a weight measure for the specific feature. Based on the analysis weights obtained, the method computes the multi model trust weight for the incoming packet. According to the value of multi model trust weight, the method classifies the packet as genuine or malicious to perform intrusion detection.

Intrusion Detection Algorithm:

```
Given: Network Trace NetTrace, Packet P
Obtain: Boolean
Start
    Read network trace NetTrace, Packet P
    Compute payload weight Sw = Payload-Analysis (NetTrace, P)
    Compute path weight Pw = path-Analysis (NetTrace,P)
    Compute Frequency weight Fw = frequency -Analysis (NetTrace,P)
    Compute multi model trust weight MmTw = $\frac{Sw}{Fw} \times Pw$
    If MmTw>Th then
        Conclude genuine
        Return true
    Else
        Conclude malicious
        Return false
    End
Stop
```

The working principle of intrusion detection is presented above. The method extracts the features of incoming packet and performs analysis on various features.

Based on the value returned at each analysis, the method estimates the multi model trust weight to classify the packet as genuine or malicious. It has been used to perform intrusion detection.

IV. RESULTS AND DISCUSSION

The proposed multi model transmission analysis based intrusion detection system is hard coded and its performance has been measured. The method is implemented in advanced java and KDD and real time data set is used for performance evaluation. The method has been validated for its efficiency under different parameters. The results obtained have been compared with the results of other methods. The results obtained have been presented below:

Table 1: Details of Experiment

Parameter	Value
Tool Used	Advanced Java
Data Set	KDD, Real Time
Number of Users	200
Number of Services	20

The experimental details of evaluation are presented in Table 1. The method has been validated for its performance using the KDD data set which is provided by the UCI repository and has learned its own data set. The method has been measured for its performance under the following parameters.

Intrusion Detection Accuracy:

The intrusion detection accuracy represents the efficiency of the algorithm in detecting the intrusion based on the incoming packets. It has been measured based on the number of correct classification performed on a given number of threats.

$$\text{Intrusion detection accuracy} = \frac{\text{Number of Correct Detection Performed}}{\text{Total Number of Intrusion Attack Generated}}$$

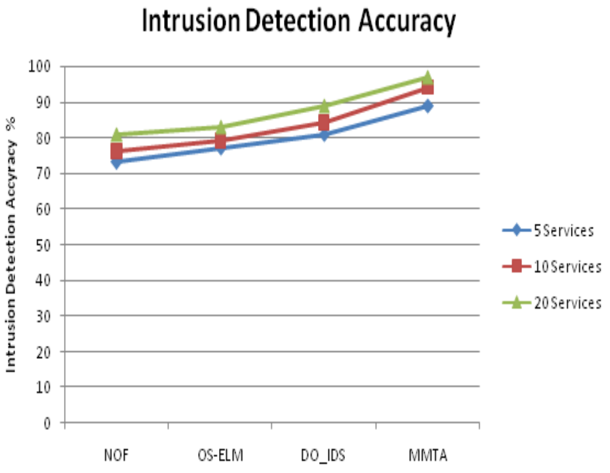

Figure 1: Performance on intrusion detection accuracy

The performance on intrusion detection accuracy has been measured for each method at varying number of services. At each condition, the proposed multi model transmission analysis algorithm has produced advanced intrusion detection accuracy than other methods.

False Classification Ratio:

The false ratio represents the inefficiency of the algorithm in detecting the intrusion attack. It has been measured according to the number of intrusion attacks classified as normal and number of correct request classified as genuine. It has been measured as follows:

False Ratio = (TF+FT) / (Total Number of Requests) Here TF = Number of true requests classified as intrusion FT = number of intrusion packets classified as genuine request.

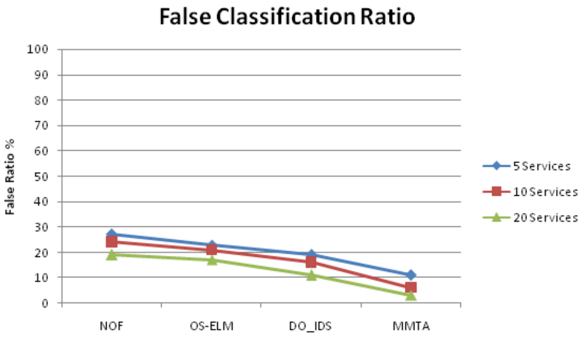

Figure 2: Performance on False Classification Ratio

The performance on false ratio in classification has been measured for different algorithms and presented in Figure 3. The proposed multi model transmission analysis algorithm has formed a lesser amount of false ratio than any other algorithm compared.

Time Complexity:

The time complexity represents the time taken for classification of packet. It has been measured based on the time it takes for classification.

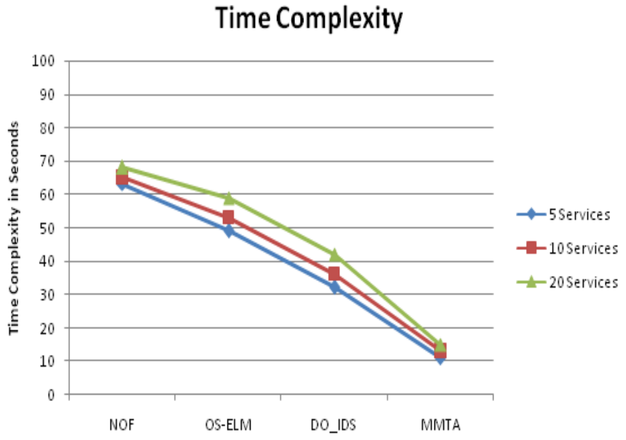

Figure 3: Performance on time complexity

The time complexity in classifying the requests on varying number of services has been measured for different methods and presented in Figure 3. The proposed multi model transmission analysis algorithm has produced less time complexity than other methods at each condition.

V. CONCLUSION

The problem of intrusion detection in network systems has been approached with the multi model transmission analysis algorithm in this paper. The method monitors the incoming traffic and extracts the payload, path and frequency features. Each feature has been analyzed for their trustworthy by measuring the weight for the feature considered. Based on the values returned at each analysis, the method estimates the multi model trust weight based on which the method performs intrusion detection. The proposed MMTA algorithm has improved the performance of intrusion detection accuracy at different conditions considered. The false sratio has been minimized and time complexity has been reduced well.

ACKNOWLEDGMENT

Foremost, my gratitude goes to Dr. J. K. Kani Mozhi, Professor, Department of Computer Application, Sengunthar Arts & Science College, Tiruchengode, who guided me into the fractal realm. Her vision, her enthusiasm and her spirit inspired and enlightened me to carry out this research paper with curiosity and involvement. And I thank my wife Mrs. A. Arockia Vinnarasi and my son Master A.Joel Roy, My daughter A. Jessica Mariam who always supported to me. Finally, I thank God who gives me good health, continuous encouragement and support throughout the research work and my life

REFERENCES

1. Jabez Z, Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach, ELSEVIER, Procedia Computer Science, Volume 48, 2015, pp 338 – 346.
2. Jayakumar Kaliappan, Fusion of Heterogeneous Intrusion Detection Systems for Network Attack Detection, HINDAWI, The Scientific World Journal, 2015.
3. Uma R. Salunkhe, Security Enrichment in Intrusion Detection System Using Classifier Ensemble, HINDAWI, Journal of Electrical and Computer Engineering, 2017.
4. T.H.Divyasree, A Network Intrusion Detection System Based On Ensemble CVM Using Efficient Feature Selection Approach, ELSEVIER, Procedia Computer Science, Volume 143, 2018, PP 442-449.
5. Lidong Wang, Big Data in Intrusion Detection Systems and Intrusion Prevention Systems, Journal of Computer Networks. 2017, Voluem 4, Number 1, pp 48-55.
6. Bekti CahyoHidayanto, Network Intrusion Detection Systems Analysis using Frequent Item Set Mining Algorithm FP-Max and Apriori, ELSEVIER, Procedia Computer Science, Volume 124, 2017, PP 751-758.
7. Pooja Preet, intrusion detection system for manet, (IJESRT), Volume 6, Issue 5, 2017, pp 402-406.
8. Yuancheng Li, Intrusion detection system using Online Sequence Extreme Learning Machine (OSELM) in advanced metering infrastructure of smart grid, PLoS ONE, Volume 13, Issue 2, 2018, pp 1-15.s
9. Bing Zhang, Network Intrusion Detection Method Based on PCA and Bayes Algorithm, HINDAWI, Security and Communication Networks, 2018.
10. D. Gupta, S. Singhal, S. Malik and A. Singh, "Network intrusion detection system using various data mining techniques," IEEE (RAINS), 2016, pp. 1-6.
11. Ali Ahmadian Ramaki, A Systematic Mapping Study on Intrusion Alert Analysis in Intrusion Detection Systems, ACM (CSUR), Volume 51 Issue 3, 2018.
12. Ruirui Zhang, Intrusion Detection in Wireless Sensor Networks with an Improved NSA Based on Space Division, HINDAWI, Journal of Sensors, 2019.
13. Jiadong Ren, Building an Effective Intrusion Detection System by Using Hybrid Data Optimization Based on Machine Learning Algorithms, HINDAWI, Security and Communication Networks, 2019.
14. Simone A. Ludwig, Applying a Neural Network Ensemble to Intrusion Detection, SCIENDO, Volume 9, Issue 3, 2019, pp 177-188.
15. M. Almi'ani, A. A. Ghazleh, A. Al-Rahayfeh and A. Razaque, "Intelligent intrusion detection system using clustered self organized map," IEEE (SDS), 2018, pp. 138-144.

AUTHORS PROFILE

A. Anthony Paul Raj received his B.Sc., B.Ed degree in Computer Science from Pope John Paul II College of Education under Pondicherry University. He completed his M.Sc in Computer Science from St. Joseph College, Trichy under Bharathidasan University. He is completed M.Phil in Computer Science under Bharathidasan University. He is pursuing her Ph.D in Periyar University, Salem. He has 11 years of Teaching Experience. His area of interest is Network Security.

Dr. J. K. Kani Mozhi working as a Professor, in Department of Computer Applications, Sengunthar Arts & Science College, She has 17 years of teaching experience. Her area of interest is Image processing