International Journal of Applied Research

ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2015; 1(7): 300-303
www.allresearchjournal.com
Received: 02-04-2015
Accepted: 05-05-2015

A Human Cell Theory Adaptive Intrusion Detection Model for Real time Network

Monika Jain, Vijay Bhardwaj

Monika Jain
Student, M. Tech Dept. of Computer Science & Engg., Manav Institute of Technology & Management, Jevra, Hisar (Haryana)

Dr. Vijay Bhardwaj
Asstt. Professor & HOD, Dept. of Computer Science & Engg., Manav Institute of Technology & Management, Jevra, Hisar (Haryana)

Correspondence:
Monika Jain
Student, M. Tech Dept. of Computer Science & Engg., Manav Institute of Technology & Management, Jevra, Hisar (Haryana)

Abstract
Security is always the critical challenge for any distributed information sharing system. These kinds of networks suffer from a different kind of man-in-middle attacks. To improve the network reliability, it is required to identify these attacks over the network. In this work, an intelligent human cell theory adaptive model is presented. The presented model has performed the communication parameter analysis to identify different kinds of DOS attacks. The result shows that the work has successfully as well provided the effective recognition rate.

Keywords: Security, Cell, DDOS, Human, Detection Model

1. Introduction

An Open network is the today requirement to provide the transmission of different kind of information. But even in private network, the information communication is not safer. Instead, the network suffers from various kinds of internal and external attacks. These attacks are performed either to reveal the information or to degrade the network QoS. To provide the safe communication in private or public network various approaches are applied by different security models. Some of these approaches are shown in figure 1. The figure showed the different approaches adapted by different communication network to deal with intrusion problem. The foremost problem identified here is the authentication model. The authentication model saves the network from external attacks. This kind of model defines a signature check using a cryptographic approach to verify the node validity. The digital signature adaptive communication provides the initial level intrusion protection. In public network the cryptographic schemes are integrated.

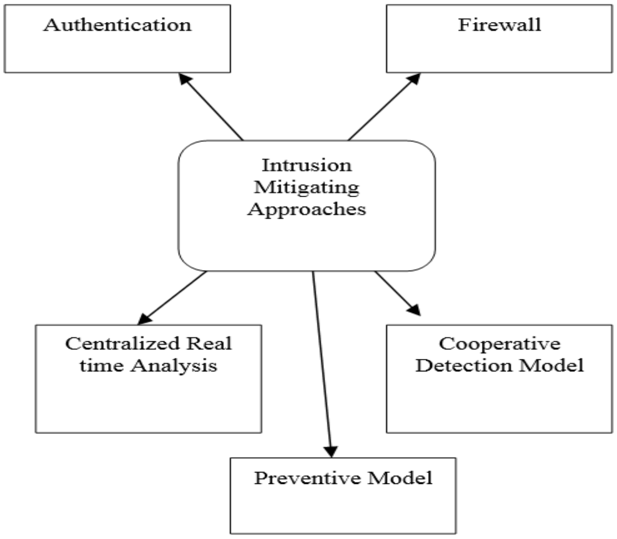
Authentication
Firewall
Intrusion Mitigating Approaches
Centralized Real time Analysis
Cooperative Detection Model
Preventive Model

Fig 1: Intrusion Mitigation Approaches

Another model to provide the secure communication transition is done using a firewall. The firewall is basically attached with specific application or system to verify the node validity. The node firewall filters all the communication to the application based on the incoming and outgoing message filtration under some defined standards. The messages fulfill the constraints will be considered as the secure communication. Another intrusion detection model applied in the network is centralized system based real time communication analysis model. This kind of model is applied on some server that communicate information obtained from various nodes. The node statistics are analyzed to identify the intrusion nodes or communication in the network. The cooperative communication model is applied in adhoc network or the peer to peer network in which each node tracks the communication information of neighbor nodes. The neighbor node communication analysis is performed to identify the effective node. The attack specific analysis is applied to perform the attacked node detection. The final model for intrusion reduction is the preventive model. In this model, the attack sensitive route is generated over the network so that the safe communication will be performed. The formation is based on the identification of safe nodes so that the reliable communication will be obtained from the work.

In this paper, an improved network analysis model is provided to identify the man in the middle attack over the network. The presented work model is inspired from human cell formation. In this section, various intrusion mitigation approaches are discussed. The section also discussed the requirement of security models in the network. In section II, the work defined by earlier researchers is presented. In section III, the research methodology is presented and discussed. In section IV, the results obtained from the work are presented. In section V, the conclusion obtained from the work is presented.

2. Existing Work

A lot of researchers provided a different work model provides the solution for attack preventive communication models and to provide the safe and secure information transition over the network. Some of the contributions of earlier researchers have been discussed in this section. T. Subbulakshmi [1] has presented the SVM based model to identify the man in the middle attack over the network. Author applied the work on different dataset and analyzes the attack features to identify the attack category. The model also provided the separation of various attack classes based on which the reliable communication was performed. Vera Marinova [2] has provided an attack adaptive security violation analysis model to identify the unauthorized users over the network. Author provided the analysis on different service disruption features so that the secure and reliable communication will be obtained. Author applied the classification rules for attack identification. Neelam Sharma [3] has provided the probabilistic analysis model under layered approach. Author provided the prediction under various attack specification. Author defined the attack driven class to generate the attack category, so that the reliable communication modeling will be done. C.I. Ezeife [4] has provided a neural adaptive model for safe and secure communication with rule formation. Author provided the real time communication modeling to provide the attack solution with pattern analysis. Author used the back propagation model to provide the real time communication in attacking networks. Author defined hardware based network analysis approach for safe communication.

Wenke Lee [5] has provided a network experience based data flow analysis approach for providing the safe and secure communication in the network. Author provided the unstructured communication analysis model for real time dependent communication in the network. Author provided the safe communication under structured phenomenon and semantic communication check so that the analytical communication behaviour. Author defined the level adaptive analysis of the structured communication behavior. Author provided the attack frequency based analysis and generated the communication pattern for attack prediction. LTC Bruce [6] has provided the dynamic communication analysis approach for attack identification. Author provided a tree based analytical model to identify the data transition so that the evaluation of various network attacks will be done. K C Nalavade [7] has provided a work on mining approaches to identify the network attack and provide the preventive communication under security constraints. Author defined the attack aware communication in the network with network host analysis so that the preventive route will be obtained over the network. C.I. Ezeife [8] has provided the sensor adaptive communication analysis model for intrusion detection. Author presented the communication model under training information processing so that the network effectiveness will be improved and the secure communication will be performed. Klaus Julisch [9] has presented the knowledge based intrusion detection model to generate the history rules so that the secure communication will be performed in the network. Author provided the extensive information processing model for intrusion detection so that the secure communication will be performed. Author defined the difficulty analysis model for effective information processing so that the conceptual rules will be obtained. Guanhua Yan [10] has presented the defensive model for attack detection so that the secure information transition will be performed over the network. Author provided the attack modeling for attack defending communication. Neelam Sharma presented the probabilistic communication model to reduce the communication attack and to provide the safe communication in the network.

3. Research Methodology

In this present work, a human cell formation model is presented to identify the man in the middle attack over the real time network. The centralized system is designed to perform the communication. The communication information is processed to identify the attack over the network. The presented model is divided into three main stages.

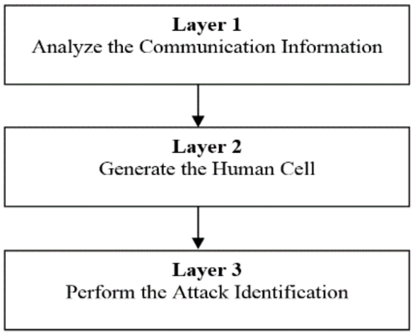
Layer 1
Analyze the Communication Information
Layer 2
Generate the Human Cell
Layer 3
Perform the Attack Identification

Fig 2: Proposed Model

Here figure 2 is showing the proposed model for attack detection for a centralized network model. On the first layer of this model, the network communication analysis will be performed. This analysis is required to analyze the attack type, protocol involved, time stamp of communication etc. Various communication features will be analyzed in this stage to identify different kinds of attacks. After this analysis, the human cell formation will be done and finally this cell will be identified under different attacks and the attack class will be identified over the network.

A) Layer I

The first stage of this proposed model is to analyze the network communication. The communication feature specification is here done under the real time network specification. In this work, the centralized system is considered under the dense network specification. The network is defined by the specification of a hybrid communication mechanism with inclusion of different information type and the protocols. The cooperative communication in the network is performed using the centralized device. The network model is here formed to identify these communication features. These communication features considered in this work includes the protocol specific features, communication time stamp, data transition features, network formation features, attack specific features etc. The communication analysis is the key strength of this proposed work model and based on the communication characteristics based on which the attack detection is performed. The characteristic formation is the analysis stage of this model.

B) Layer II

The second stage of this model is the adaption to the human cell formation. This adaptation is here defined as the feature adaptively to the cell formation with attack specific mapping. The mapping is here applied to provide the identification of the communication deficiency in the network. The node acceptance is here defined to provide the different kind of communication attack identification. In this work, the cell formation is done under the acceptance of the communication under different parameters. These parameters will collectively analyze the communication features with the human cell specifications. Once the cell is formed, the final stage is to perform the attack detection.

C) Layer III

The final stage of this work models it to provide the attack detection in the network. The model begins as the cell formation under the communication analysis is done. The communication is analyzed under different attack forms and the mapping of the communication features with the attacks is done with kernel specification. The kernel adaptive mapping will be here done to identify the attack type so that the safe communication will be performed in the network. The model is here applied in real time network so that the safe communication phenomenon will be obtained and the network reliability will be improved. This stage given the decision regarding the attack identification that is later on being used to identify the detection ratio. The predictive model is defined under the attack modeling so that the recognition rate will be improved.

The experimentation is here done in real time simulation environment. The result shows that the work has provided the secure and reliable communication. The experimental results are discussed in the next section.

4. Results

The presented work is implemented on communication information provided for the real time centralized system. The communication parameters are collected, including the protocol specification, traffic parameters, packet type communication, communication time stamp etc. The communication information is here processed to identify the attacked and the normal communication over the network. The analysis results obtained from the work have been discussed in this section. The analysis of the work is here done in terms of attack ratio identification.

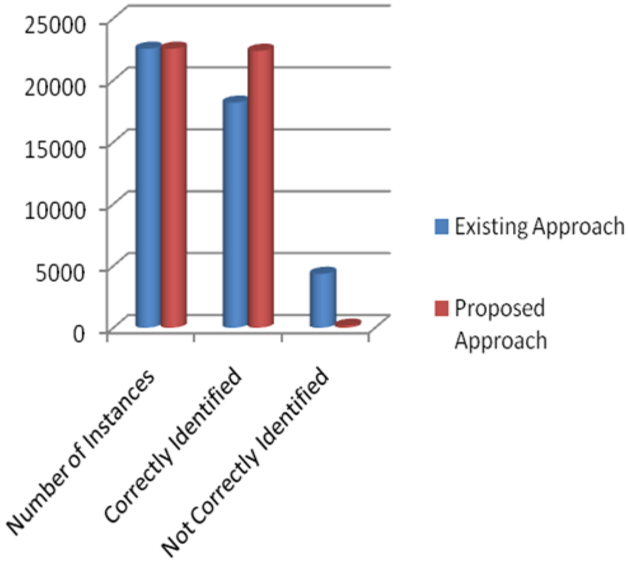

Fig 3: Attack Detection Analysis

Here figure 3 is showing the attack detection analysis applied with the network. The figure shows that the proposed work has improved the detection rate so that the overall accuracy of the work is improved. The figure shows the analysis in terms of attack detection and the normal communication detection. The figure shows that the presented work is effective in all respects.

5. Conclusion

In this work, an improved human cell based analytical model is presented under attacked identification in real time centralized network. The proposed model is the improvement against the network architecture so that the man in the middle attack over the network will be reduced. The proposed model has improved the network communication and improved the network strength by detecting the attack over the network correctly.

6. References

1. Subbulakshmi T. Detection of DDoS Attacks using Enhanced Support Vector Machines with Real Time Generated Dataset, IEEE-ICoAC 2011; 978-1-4673-0671-3/11©2011 IEEE
2. Vera Marinova-Boncheva, Applying a Data Mining Method for Intrusion Detection, International Conference on Computer Systems and Technologies - CompSysTech'07

3. Neelam Sharma. Layered Approach for Intrusion Detection Using Naive Bayes Classifier, ICACCI'12, August 3-5, 2012, Chennai, T Nadu, India. ACM 978-1-4503-1196-0/12/08
4. Ezeife CI. NeuDetect: A Neural Network Data Mining Wireless Network Intrusion Detection System, IDEAS10 2010, August 16-18, Montreal, QC [Canada]; Editor: Bipin C. DESAI; ACM 978-1-60558-900-8/10/08
5. Wenke Lee. Mining in a Data-flow Environment: Experience in Network Intrusion Detection, KDD-99 San Diego CA USA 1999 l-581 13-143-7/99/08
6. LTC Bruce D. Caulkins. A Dynamic Data Mining Technique for Intrusion Detection Systems.
7. KC Nalavade. Intrusion Prevention Systems: Data Mining Approach, International Conference and Workshop on Emerging Trends in Technology (ICWET 2010) – TCET, Mumbai, India ICWET'10, February 26–27, 2010, Mumbai, Maharashtra, India. ACM 978-1-60558-812-4
8. CI Ezeife. WIDS: A Sensor-Based Online Mining Wireless Intrusion Detection System, ACM 978-1-60558-188-0/08/09
9. Klaus Julisch. Mining Intrusion Detection Alarms for Actionable Knowledge, SIGKDD '02 Edmonton, Alberta, Canada ACM 1-58113-567-X/02/0007
10. Guanhua Yan. Towards a Bayesian Network Game Framework for Evaluating DDoS Attacks and Defense, CCS'12, October 16–18, 2012, Raleigh, North Carolina, USA. ACM 978-1-4503-1651-4/12/10
11. Neelam Sharma. Layered Approach for Intrusion Detection Using Naive Bayes Classifier, ICACCI'12, August 3-5, 2012, Chennai, T Nadu, India. ACM 978-1-4503-1196-0/12/08