ENHANCED MOVING TARGET DEFENSE MECHANISMS TO HANDLE CYBER ATTACKS

CHAPTER 9

Conclusion and Future Directions

9.1. Summary and Conclusions

9.2. Future Research Directions

9.1. Summary and Conclusion

In this communication world, it is very important to ensure that the communication received is from an authorized user. In recent years, economic loss is more due cyber attacks. Cyber attacks are more dangerous to the entire Internet world. The goal of this research work is to defend against known and unknown cyber attacks and to ensure quality of service. In order to achieve the same, the existing network traffic monitoring and dimensionality reduction techniques are well examined. The improvements are carried out in this research work.

Based on the literature study, it is very obvious that the existing methods need some more improvements to increase the efficiency in monitoring the traffic and to increase the Quality of service (QoS). The new feature is added to the existing network traffic monitoring methods and the outcomes of the improved method are increased efficiency in traffic monitoring, adaptability for various network surface areas, various secure routing protocols, different traffic models, varying number of nodes, reduced retransmission and time saving.

Dimensionality reduction technique is also analyzed to make use of it defending against the known cyber attacks. After analysis, it is enhanced with computational intelligence techniques to overcome the limitations. The results of the enhanced PCA with SVM gives the improved accuracy in detection of known cyber attacks.

Recently, Game Changing Approaches like Tailored Trustworthy Spaces, Moving Target Defense and Cyber Economics are receiving more attention in research directions. Four moving target defense mechanisms are well analyzed and improvement is done with the existing methods. They are:

i. Smart Motion Adaptation/Management using Game Theory
ii. Robust Cryptographic Authentication using Click Dynamics
iii. Improved Data chunking through non-sequential storage

iv. Enhanced Decoys with Integrated Time and Event Triggered approach

The proposed secure hash based game theory approach is introduced. This method ensures confidentiality, neighbor authentication, secured packet communications. The data communicated in this method is fully encrypted. In this phase the cryptographic client puzzle is used to ensure neighbor authentication. Every node in the network will be ensured for authentication with a secret key and puzzle. The proposed method is evaluated with Quality of Service (QoS) parameters, namely an average end to end delay, Average throughput, Average routing overheads, Average packet delivery ratio, Average packet drop ratio, Average No of claims Based on time.

Enhanced click dynamics for user authentication is introduced. The integration of graphical password, one class classifier, Manhattan distance and anytime algorithm for more accuracy in user authentication is proposed. The proposed method is developed to ensure user authentication and it requires the user to operate graphical passwords for login. The accomplishment of the proposed method is evaluated in terms of performance metrics like false acceptance rate, false rejection rate and attack detection rate to predict its efficiency in defending against cyber attacks.

The proposed non-sequential data chunking is introduced to defend against cyber attacks, to ensure integrity, user authentication and authorized access of data or information to authorized users. In the existing method, the files uploaded will be chunked into two or more files and will be stored in sequential order in various servers. In this research work, the traditional way of storing the chunked files is rearranged in various unique combinations and non-sequential order of storing the chunked files is introduced. This proposed non-sequential data chunking method is implemented using JAVA1.7 and mysql. The result of the experimentation envisions the performance of the proposed method based on performance metrics such as false acceptance rate, false rejection rate and cyber attack detection rate.

The proposed integrated time and event triggered approach is to ensure Quality of Service (QoS) in communication of network setup established and it also provides privacy and secrecy in of packets in routing. The entire communication between the nodes is done through data encryption. The proposed integrated time and event triggered approach is tested and the experimentation is done using network simulator NS2. The results of simulation using NS2 shows that the proposed method outperforms the existing method based on the QoS parameters like end to end delay, latency and routing overheads are minimized. Packet delivery ratio and throughput are increased.

The simulation result shows that the proposed methods predicts and defends the cyber attacks in a better manner than the existing methods. The four moving target defense mechanisms are enhanced and the results are compared. Among the four methods integrated Time and Event Triggered approach detects more cyber attacks.

9.2. Future Research Directions

The proposed methods make it very robust against unknown cyber attacks that can be well suited for Wireless Local Area Network. This research work is conducted via simulation. Only four methods out of eleven methods are taken for this research work. As a future work, some more moving target defense mechanisms can be analyzed and can be enhanced in handling the unknown cyber attacks. The proposed methods can be evaluated in real time by integrating them in hardware components.