WSN : An Advanced MC Analysis Technique For Detecting The Denial-Of-Service Attack

Chintalakumar Shiva
Asst. Professor
Department of ECE
Siddhartha Institute of Technology and Sciences
Narapally, Hyderabad, Telangana, India

Varikuppala Ganesh
Asst. Prof.
Department of CSE
Siddhartha Institute of Technology and Sciences
Narapally, Hyderabad, Telangana, India

Abstract **- Network Threats are possible against inter-networking systems such as Web servers, database servers, and cloud computing servers by network attackers. One of the most common attacks that has a significant impact on computing systems is denial of service (DoS). The shared nature of wireless networks makes it very easy for an attacker to launch a Wireless Denial of Service (WDoS) assault. Consider a malicious node that can broadcast a radio signal indefinitely, blocking any allowed access to the network medium and interfering with reception. Jamming is the term for this operation, and the malicious nodes are referred to as jammers. Jamming techniques range from simple assaults based on the continuous transmission of interference signals to more sophisticated attacks aimed at exploiting flaws in the protocol in question. DoS attack detection systems utilize Multivariate Correlation Analysis (MCA) to determine the accurate network traffic characterization by distinguishing geometrical correlations across network traffic parameters. At the time of attack identification, the proposed MCA-based DoS attack detection system uses an anomaly-based detection technique. To discriminate between authorized and attack traffics, a threshold limit is defined. As a result, the suggested approach may efficiently detect known and unknown DoS assaults by analyzing the patterns of allowed network traffic alone.**

Key words: DoS, learning patterns, MCA, malicious node, jamming, jammer and WDoS

1. INTRODUCTION

Wireless communication has grown in popularity in both academic and commercial domains in recent years, and security has become a key topic. Some wireless networks, such as Ad hoc, Wi-Fi, or wireless sensor networks (WSNs), must guarantee security for its users during data transfer. This is due to the availability of hackers and other nasty or malicious behaviors that occur in the same manner as other daily activities. Wireless networks are becoming a reality as a result of technological advancements, as they have become more affordable and accessible through ready-to-wear components. As a result, they have some equipment to halt these developments.

Wireless networks are more accessible for internet usage in the past and future than wired networks, and these wireless networks are more vulnerable to numerous attacks than wired networks. The widely accepted reality about wireless networks is that they are easily accessible and have a sharable type of surroundings. This reality has both benefits and drawbacks when it comes to a wireless network, as it is relatively easy for an adversary to launch an assault. These attacks have the potential to disrupt network operations by saturating user and kernel buffers. It is classified as jamming or a denial of service (DoS) attack, depending on whether the effect or the effort of the attack is visible. When browsing the internet, one of the most obvious examples of a DoS attack is when the web page to be visited does not load properly and we need to press the refresh button more than necessary, either accidentally or deliberately. Consider how a mobile phone can be used to transmit SMS in the hinterland. This is sufficient to prevent wireless node communication.

Actually, it's more likely that it's become a race between the competitor to attack a wireless network and the security authorities to develop effective countermeasures. Regardless of the adversary's attack, the corresponding network must be able to send data between legitimate nodes. There is no interruption between authorized users for effective communication. The presence of an attacker in the network should be reported to the network's administrator. If the authorized node/user communicates with the attacker, it is not presumed that they are acting honestly and morally. At these times, the required node in such a scam must be located, and any other evasive acts in the wireless network must be reminded, so that both the data and the network may be accommodated. The following is how this paper is structured: In section 2, we discuss related work on DoS, jamming, and other strategies for identifying attackers.

2. RELATED WORK

In most cases, a DoS attack is used to prevent a device or node from receiving permitted or correct data, or to completely isolate the device/node from another authorized node. This type of signal jamming can be done with data packets that are continuously broadcast, radio signals, or other means of propagation signal jamming. Several authors have discussed numerous jamming approaches, as well as detection and preventive techniques. Pelechrinis et al [1] examined the various types of DoS attacks and the performance repercussions in all networks as a result of the denial of service attack. In their review, they provided several intrusion detection systems and concluded that a system implementation is required to avoid real-world competitors. The obtained throughput is 0 in jamming procedures and detecting techniques, which substantially reduces network performance. Proano, A., and Lazos, L. [2] provide a detailed analysis of the selective jamming attack, in which the adversary chooses which data packets to jam, particularly high-priority data packets, when it comes to network privacy and security. They accomplish this by performing data packet classification at the physical layer.

For delay sensitive applications in WSN, Ghosal et al [3] suggested a jamming defending data-forwarding technique. The suggested method uses network nodes as clustering forms at a predetermined frequency. The transmitted packets are jammed at a specific frequency, rendering the clusters in that frequency inactive and requiring backup from neighboring clusters. Sagduyu et al[4] proposed the game theory technique, which provides some effective tools for designing and analyzing diverse attacks. This article discusses a type of jamming game in which a set of transmitters and network jammers are simulated at the MAC layer. The symmetry tactics resulting from jamming games differentiate the required performance under DoS assaults and inspire a robust network protocol model for secure communications. The fact that network users do not have comprehensive information about the other user's singularities, jamming dynamics, channel peculiarities, or the costs and honors of other users is a basic feature of distributed wireless networks. User kinds, physical presence, packet traffic, system parameters, and physical channel are some of the different sorts of uncertainty that might be proposed: User Types: A user may not be aware of the type of other users, and type refers to whether a node acts as a transmitter or receiver. Physical appearance: Users may not be aware of whether or not the attacker has been physically shown to send. Packet traffic: Users may not be aware of the attackers' traffic dynamics, such as whether or not the attacker's queue has accumulated. System parameters: Others may not be aware of each user's utility, such as reward and cost functions. Physical channel: Users may be unaware of physical channel characteristics such as channel gains, channel noise, or packet capture probability.

3. PROPOSED WORK

Step 1 involves inducing essential features from network traffic entering the internal network, where secured servers reside and are used to create traffic logs for a predetermined time span. By focusing primarily on appropriate inbound network traffic, analyzing and observing at the target network reduces the detection overhead of malicious behavior. Because permitted traffic records are needed by the detectors for a smaller number of network services, this procedure allows the proposed detector to provide the best security for the destination internal network. Step 2, the Triangle Area Map Generation phase is used to isolate the correlations between two discrete characteristics among each traffic profile generated in the first step, and the traffic profile is normalized by the "Feature Normalization" phase. Because the presence of network attacks causes changes in certain correlations, the changes can be used as indicators of attacker activity. To display traffic profiles, all of the isolated correlations such as triangle areas accumulated in Triangle Area Maps (TAMs) are then used to replace the original fundamental characteristics or the normalized characteristics. This makes it possible to discriminate between permitted and non-authorized traffic profiles with more judicial information.

The anomaly-based detection technique is taken over in step 3 of the Decision-Making procedure. It makes it easier to identify denial of service attacks without requiring any prior information of the attack. The labor-intensive attack analysis and frequent updating of the attack signature database are avoided in the misuse-based detection phase. At the same time, the method improves the detectors' robustness and makes them more difficult to avoid, because attackers want to create attacks that match the typical traffic records created by a specific detection technique. This is a time-consuming task that requires understanding of the intended detection technique. In the Decision-Making process, two modules in particular, the Training Phase and the Test Phase, are required. The Normal Profile Generation module is used in the Training phase to develop profiles for various sorts of allowed traffic profiles, which are then stored in a database. The Tested Profile Generation module is used to create profiles for individual identified traffic records during the Test phase. The attack detection module then

collects the tested profiles and compares them to the equivalent normal profiles that have been kept. At the Attack Detection phase, a threshold-based classifier is required to distinguish between denial of service attacks and approved traffic.

4. MULTIVARIATE CORRELATION ANALYSIS

In a Denial of Service attack, network traffic behaves differently from allowed network traffic, and network traffic performance is indicated by statistical properties. As a result, we suggested a new Multivariate Correlation Analysis (MCA) technique to display these statistical qualities among the features. The proposed MCA technique separates the correlated information among the characteristics inside a recognized data object using triangular area.

5. EXPERIMENTAL RESULTS

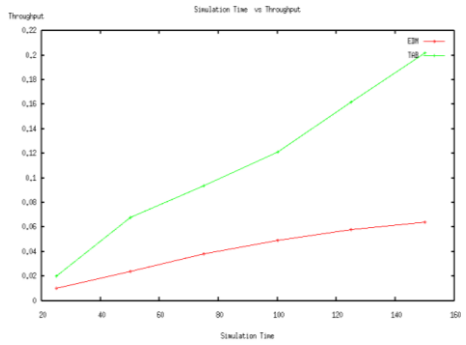

Figure 1: Simulation Time Vs Throughput

Figure 1 compares the simulation time and throughput of the Triangular Area Map and the Euclidean Distance Map, showing that the proposed TAM outperforms the latter by boosting throughput.

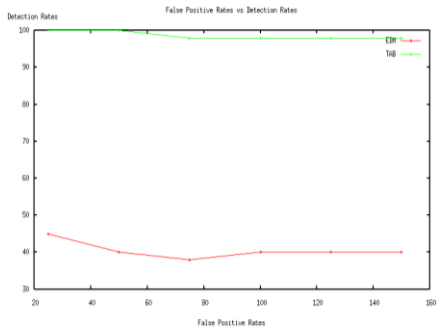

Figure 2: False Positive Rate Vs Detection Rate

Figure 2 compares the false positive rate and detection rate of the Triangular Area Map with the Euclidean Distance Map, showing that the proposed TAM outperforms the other by improving detection rates while lowering false positive rates.

6. CONCLUSION

As a result, the MCA-based DoS attack detection approach is proposed, which uses the triangular area-based MCA technique as well as the anomaly-based detection technique. The prior method separates geometrical correlations concealed in single pairs of two discrete features in each traffic record, allowing for more detailed traffic behavior characterization. The proposed strategy is alleviated by the contemporary technique, which can distinguish both known and unknown DoS attacks from allowed network data.

7. REFERENCES

[1] Konstantinos Pelechrinis, MariosIliofotou and Srikanth V. Krishnamurthy(2011), “Denial of Service Attacks in Wireless Networks:The Case of Jammers” Communications Surveys & Tutorials, IEEE, vol 13: issue:2, nos 245- 257.

[2] Proano, A.; Lazos, L.;(2011) “Packet-Hiding Methods for Preventing Selective Jamming Attacks” Dependable and Secure Computing, IEEE, vol. 9 issue 1. Nos 101- 114.

[3] Ghosal, A.; Halder, S.; Mobashir, M.; Saraogi, R.K.; DasBit, S.;(feb- 28th to march 3rd 2011)” A jamming defending data-forwarding scheme for delay sensitive applications in WSN” Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference, nos 1- 5.

[4] Sagduyu, Y.E.; Berry, R.A.; Ephremides, A.;(aug 2011)” Jamming games in wireless networks with incomplete information”, Communications Magazine, IEEE, vol 49, issue 8, nos 112- 118.

[5] Zhiyuan Tan, ArunaJamdagni, Xiangjian He, Priyadarsi Nanda, Member, IEEE, and Ren Ping Liu, Member, IEEE,” A System for Denial-of- Service Attack Detection Based on Multivariate Correlation Analysis” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. , NO. , 2013 1