A Survey Paper on
Detection of Denial of Service Attack on Wireless Network

Pooja Gudadhe
Department of Computer Science & Engineering
Student at G. H. Raisoni College of Engineering,
Nagpur, India

Sonali Nimbhorkar
Department of Computer Science & Engineering
Assistant Professor at G. H. Raisoni College of
Engineering, Nagpur, India

Abstract- In today's networks and computers attackers consume the resources of the victim, a server or a network. It also consumes the victim's computational power by flooding the channel with huge amount of useless packets and jamming the network. This results in performance degradation and consumes a large amount of traffic, CPU or the bandwidth of the victim. The most aggressive and severe attack is Denial of Service (DoS) attack launched by malicious users on a victim, which can be a host, a router, or an entire network. This paper considers various approaches to detect the Dos attack. This would also maximize the expected average estimation error while it would also save time and energy.

Index terms- Dos Attack, Security attacks, Dos attack detection, Intrusion detection system (IDS)

1. INTRODUCTION

THE most aggressive and severe attack is Denial of Service (DoS) attack launched by malicious users on a victim, a host, a router, or an entire network. It is also possible that the victim be forced out of service for some time or many days, thus causing severe damage on the system of the victim. Therefore, online services should have an effective detection of DoS attacks

The major issue to secure the network is to handle the Denial of Service (DoS) attacks. This includes detection and suppression of the DoS attacker as it increases the system overhead. But the present techniques mainly focus on the detection and recovery of the system. Recovery of the system is done after the system is damaged. Thus, though the attack is detected system is not much benefited as complete state recovery is not guaranteed.

There are two challenges in blocking the attacks is to identify the attackers and block the response only to the attackers.

DoS Detection System should be fault tolerant and perform in a distributed manner in which many components cooperate with each other. It should perform in an online manner, where the detection is done in real time for known and unknown attacks.

2. SECURITY ATTACKS

Security attacks in Wireless network can be categorized into two branches:

- Active
- Passive

2.1 Passive Attacks

In passive attacks, attackers are hidden or collect the data by tapping the communication link. They also destroy the functioning elements of the network. Passive attacks can be eavesdropping, node malfunctioning, node tampering/destruction and traffic analysis types.

2.2 Active Attacks

In active attacks, the operations are actually affected. The networking services may be degraded or terminated by these attacks. Active attacks can be into Denial-of-Service (DoS), jamming, hole attacks (blackhole, wormhole etc), flooding.

Solutions to security attacks against networks can be categorized into three main components:-

1) Prevention (defense against attack): The main aim of this step is to 'prevent' any attack before it happens. Any techniques are proposed to defend against the targeted attack.
2) Detection (being aware of the attack that is present): Detection phase of an attack is when an attacker manages to pass through the 'prevention' step. The technique is to identify the compromising nodes.
3) Mitigation (reacting to the attack): This step aims to react on any attack after it happens by removing the affected nodes. Thus making the network is secure.

3. DoS ATTACK DETECTION TYPES

Intrusion is an activity in a network that is either achieved passively (e.g., information gathering, eavesdropping) or actively (e.g., harmful packet forwarding, packet dropping, hole attacks) by an unauthorized user. In any security system, if Intrusion Prevention does not prevent intrusions, then Intrusion Detection comes into play. The detection of any suspicious behavior in a network is performed by the network members.

DoS attack detection focuses on the development of network-based detection mechanisms. In these mechanisms detection systems monitor traffic transmitting over the protected networks. In these mechanisms protected online servers are released from monitoring attacks and ensured that the servers can dedicate themselves to provide quality services with minimum delay in response. Network-based detection systems are loosely coupled with operating systems running on the host machines which they are protecting. Hence network-based detection systems configurations are less complicated. Network-based detection systems can be classified into two main categories, namely

[1] Misuse-based detection systems
[2] Anomaly based detection systems

3.1 Misuse-based detection systems→ Detect attacks by monitoring activities in network and looking for matches with the existing attack signatures. These systems are like anti-virus systems, which can detect all the known attack patterns, but are less used of an unknown attack. It is also called as signature based or rule based detection systems.

The advantage of this detection system is high detection rates to known attacks and low false-positive rates. But the disadvantage is that system is easily evaded by any new attacks and even variants of the existing attacks. Moreover it is labor intensive task to keep signature database updated as signature generation is a manual process and heavily involves network security expertise.

3.2 Anomaly based detection systems→ It monitors and flags any network activities presenting

Significant deviation from the authorized traffic profiles as suspicious objects. Anomaly based detection techniques detects zero-day intrusions in an accurate and consistent way, thus following static behavioral patterns. The disadvantage of this detection system is that it suffers high false-positive rates and updating normal profile consumes energy and time

The anomaly based detection systems are categorized in three types according to the nature of processing.

3.2.1 Statistical Based→ In this technique the network traffic is captured and then a profile representing its stochastic behavior is generated. The network operation in the normal condition is considered as a reference profile. The network is periodically monitored and score is generated by comparing with the reference profile. The occurrence of the anomaly is detected if the score passes the threshold. E.g. Univariate, Multivariate and Time series models.

A System for Denial of-Service Attack Detection Based on Multivariate Correlation Analysis uses MCA based DoS attack detection system and Triangle- area- based MCA technique. This Offers more accurate characterization for network traffic behaviors and detects known and unknown attacks. This technique does not detect DOS attacks on real-world data and doesn't have any repair strategies on the attacked data [4] .

3.2.2 Knowledge Based→ This technique relies on the availability of the prior knowledge (data) of the network parameters in normal condition. E.g. Expert Systems, Description languages, Finite State Machine, Data clustering and outlier detection models.

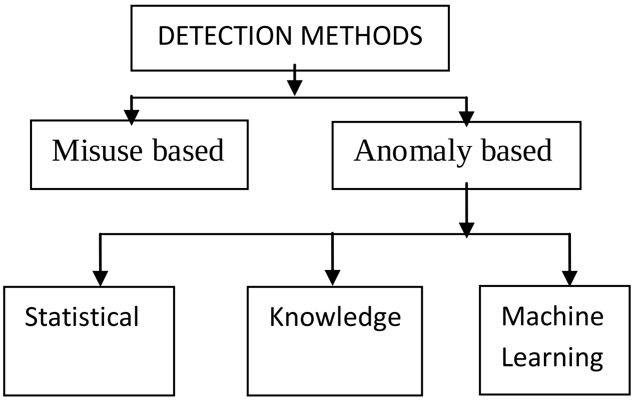
A Tunable Finite Automaton (TFA) for Pattern Matching is also used in Network Intrusion Detection Systems. It deals with the DFAs' state explosion problem and NFAs' unpredictable performance problem. It also allows multiple concurrent active states. Thus matching status is much smaller. This technique is costly and does not consider more compact finite automatons [5] .

3.2.3 Machine learning Based→ In this technique explicit or implicit model of the analyzed patterns is generated. It is based on approximation and uncertainty and models updated periodically based on the previous results. E.g. Bayesian networks, Markov models, Fuzzy logic, Genetic algorithm, Neural networks, Principal Component Analysis (PCA) models are used.

Incorporating Soft Computing Techniques into the Probabilistic Intrusion Detection System uses Self-Organizing Map (SOM) which reduces raw audit data and Hidden Markov Model (HMM) which Models user's normal behavior and detect anomalies. The Fuzzy logic ability in this detects unknown and novel attacks against computer systems. Hence the anomalies are detected efficiently. But it does not consider hard computing [8].

PCA model analyze the attacks and helps in clustering. Thus, two or more algorithms can be used to detect DoS attacks in Wireless Network.

The challenge of this detection type is to update the normal profiles periodically, since the network behavior may change rapidly which increases the load on the resources.



Requirements of the perfect Intrusion Detection System are:

• Do not introduce new weaknesses to the system.

• Use less system resources which should not degrade overall system performance by introducing overheads.

• Should run continuously and remain transparent to the system as well as to the users.

• Should use standards so that it would be cooperative and open.

• Should be reliable and minimize false positives and false negatives in the initial detection phase.

4. CONCLUSION

In this paper we studied the security attacks and its types. The attack detection methods are also studied. We also studied the requirements of the Intrusion Detection System which can be used to detect the attacks. Machine Learning based intrusion detection system is an evolving detection method. The major challenge in this system is to recover the system after the detection of the attack.

REFERENCES

[1] Heng Zhang, Peng Cheng, Ling Shi and Jiming Chen, **Optimal Denial-of-Service Attack Scheduling with Energy Constraint** , IEEE transactions on automatic control, 2015.

[2] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar, **A Survey of Intrusion Detection Systems in Wireless Sensor Networks**, IEEE communications surveys & tutorials, vol. 16, no. 1, first quarter 2014

[3] Yang Xu, Junchen Jiang, Rihua Wei, Yang Song, and H. Jonathan Chao, **TFA: A Tunable Finite Automaton for Pattern Matching in Network Intrusion Detection Systems**, IEEE journal on selected areas in communications, vol. 32, no. 10, october 2014

[4] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda and Ren Ping Liu, **A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis**, IEEE transactions on parallel and distributed systems, vol. 25, no. 2, february 2014

[5] Yongdong Wu, Zhigang Zhao, Feng Bao and Robert H. Deng, **Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service Attacks**, IEEE transactions on information forensics and security, vol. 10, no. 1, january 2015.

[6] Udi Ben-Porat, Anat Bremler-Barr and Hanoch Levy, **Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks**, IEEE transactions on computers, vol. 62, no. 5, may 2013

[7] Song Han, Miao Xie, Hsiao-Hwa Chen and Yun Ling, **Intrusion Detection in Cyber-Physical Systems: Techniques and Challenges**, IEEE systems journal, vol. 8, no. 4, december 2014

[8] Sung-Bae Cho, **Incorporating Soft Computing Techniques Into a Probabilistic Intrusion Detection System,** IEEE transactions on systems, man, and cybernetics—part c: applications and reviews, vol. 32, no. 2, may 2002

[9] Robert Mitchell, Ing-Ray Chen, **Behavior-Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications**, IEEE transactions on smart grid, vol. 4, no. 3, september 2013

[10] Khalil El-Khatib, **Impact of Feature Reduction on the Efficiency Of Wireless Intrusion Detection Systems**, IEEE transactions on parallel and distributed systems, vol. 21, no. 8, august 2010

[11] Heng Zhang, Peng Cheng, Ling Shi and Jiming Chen, **Optimal Denial-of-Service Attack Scheduling Against Linear Quadratic Gaussian Control**, 2014 American Control Conference (ACC), June 4-6, 2014