IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

“Implementation and Comparative Analysis of PTP in Network Security for Malicious Misbehavior Activity Detection”

Tejaswini S. Akulwar[1], P. S. Kulkarni[2]

Student of M.Tech (CSE), R.C.E.R.T, Chandrapur, India[1]

Department (I.T), R.C.E.R.T, Chandrapur, India[2]

Abstract: A PTP approach in network security for misbehavior detection system present a method for detecting malicious misbehavior activity within networks. Along with the detection, it also blocks the malicious system within the network and adds it to Blacklist. Malicious node defined as a compromised machine within the network that performs the task provided by i.e. it does not forward the legitimate message to another node in the network or sends some other message to a neighbor node. This system is based on Probabilistic threat propagation. This scheme is used in graph analysis for community detection. The proposed system enhances the prior community detection work by propagating threat probabilities across graph nodes. To demonstrate Probabilistic Threat Propagation (PTP) considers the task of detecting malicious node in the network. Proposed System also shows the relationship between PTP and loopy belief propagation.

Keywords: PTP, Malicious, Blacklist, Probabilistic, legitimate.

1. INTRODUCTION

1.1 Motivation

A PTP approach in network security for misbehavior detection system present a method for detecting malicious misbehavior activity within networks. Along with the detection, it also blocks the malicious system within the network and adds it to Blacklist. Malicious node defined as a compromised machine within the network that performs the task provided by server i.e. it does not forward the legitimate message to another node in the network or send some other message to a neighbor node. This system is based on Probabilistic threat propagation. This scheme is used in graph analysis for community detection. The proposed system enhances the prior community detection work by propagating threat probabilities across nodes. To demonstrate Probabilistic Threat Propagation (PTP) considers the task of detecting malicious node in the network. Proposed System also shows the relationship between PTP and loopy belief propagation.

1.2 Scope of Work

Intrusion Detection Systems (IDS) Nevertheless, none of the above solutions offer protection from both inside and outside intruders. Intrusion detection systems, on the other hand, can do this. Those intrusion detection systems are necessary because simple security mechanisms, such as cryptography, cannot offer the needed security. For example cryptographic mechanisms provide protection against some types of attacks from external nodes, but it will not protect against malicious inside nodes, which already have the required cryptographic keys. Therefore, intrusion detection mechanisms are necessary to detect these nodes. In this section we describe IDS architectures for widely known networks.

2. EXISTING PROBLEM STATEMENT

The main aim of our proposed work is to develop defense mechanisms against Distributed Denial of Service (DDos) zombie in which our objective is to design a simulation environment with the used of dot net framework 3.0 where following objective is achieved.

- Design of Dynamic network
- Secured Date Packet
- Intruder detection and their Countermeasure

Time complexity

Detection rate (D_R): is defined as the ratio between the numbers of correctly detected anomalous measurements to the total number of anomalous measurements.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

$$D_R = \frac{\text{Number of correct classified anomalous mesurements}}{\text{Total number of anomalous measurements}} \times 100\%$$

DR=Number of correct classified anomalous measurements Total number of anomalous measurements×100%

False alarm rate (F_A): is the ratio between the numbers of normal measurements that are incorrectly misclassified as anomalous to the total number of abnormal measurements.

$$F_A = \frac{\text{Number of misclassified normal measurements}}{\text{Total number of anomalous measurements}} \times 100\%$$

FA=Number of misclassified normal measurements Total number of anomalous measurements×100%

False positive rate (F_P): is the ratio between the numbers of abnormal measurements that are incorrectly misclassified as normal to the total number of normal measurements.

$$F_P = \frac{\text{Number of misclassified abnormal measurements}}{\text{Total Number of normal measurements}} \times 100\%$$

This pointer indicates how much of the data in the segment, counting from the first byte, is urgent. So if urgent pointer contains null value even after. Most of them fairly distribute workload among nodes, prolonging life time of the network. E

Working of proposed system

Trust mechanism

In general, trust mechanism works in the following stages.

1) Node behavior monitoring: Each sensor node monitors and records its neighbors' behaviors such as packet forwarding. This collected data will be used for trustworthiness evaluation in the next stage. Watchdog is a monitoring mechanism popularly used in this stage. The confidence of the trustworthiness evaluation depends on how much data a sensor collects and how reliable such data is.

2) Trust measurement: Trust model defines how to measure the trustworthiness of a sensor node. Introduced several representative approaches to build the trust model, which include Bayesian approach, Entropy approach, Game-theoretic approach, and Fuzzy approach. The trust value of a node may be different when we use different trust models. For example, when a node is observed to forward the packet sometimes and drops the packet

Insider trust Management Intelligent inside attacks against trust mechanism Vulnerabilities in the inside attacker detection stage Average End-to-End delay Packet Delivery Ratio Energy Consumption Multi-hop Chain Topology

Inside attack detection: Based on the trust value, a sensor node determines whether its neighbor is trustworthy for collaboration (such as packet forwarding). If a neighbors trust value is less than a certain threshold, it will be considered as an entrusted or malicious node. Depending on the WSN's trust mechanism, the detection of such insider attacker may or may not be broadcast to the rest of the nodes in the WSN.

Data Flow of Project Work

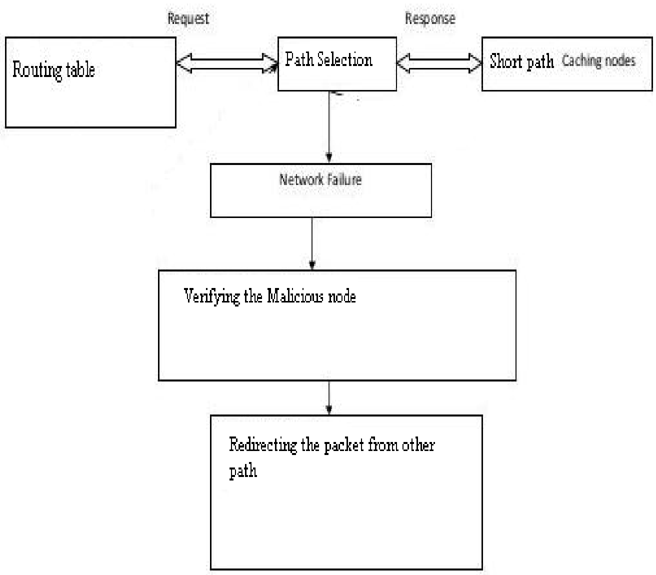


Fig 1 Flow Chart

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

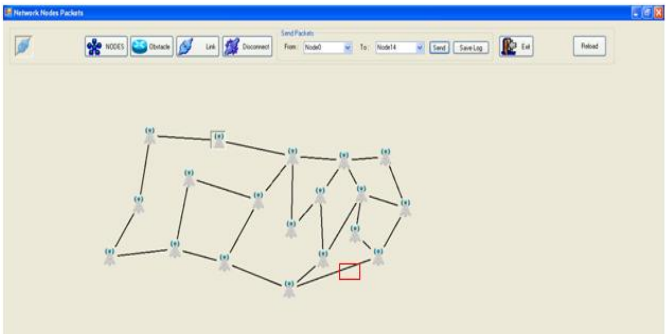
International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 7, July 2017

3. DESIGN MODULE

During a malicious detection using PTP system the following steps follows,
1. Initially sender sends a packet to the receiver.
2. Shortest path select between sources to a receiver.
3. IF (receiver! receive packet)
4. PTP detects the malicious node present in the path between sources to the receiver.
5. IF (malicious node = present) then
6. This system Block that node and add to it in Blacklist.
7. Select another short path and forward from this new path to the receiver.
8. Receiver receives the packet.



Design Environment or Virtual Environment for Network Scenario

Here With the help of Tools box user can design a network as experimental output. Data packet can be sent from source to destination by selecting appropriate node Network can be constructed in Virtual environment by deploying node from tool box. Here 'n' number of nodes can be deployed in design environment. Any type of network can be design in the modify system will automatically adopt the defense mechanism according to newer zombies will study in future work. Misuse detection refers to techniques that use patterns of known Clones e.g., more than three consecutive failed logins or weak spots of a system (e.g., system utilities that have the "buffer overflow" vulnerabilities) to match and identify Clones. The sequence of attack actions, the conditions that compromise a systems security, as well as the evidence (e.g., damage) left behind by Clones can be represented by a number of general pattern matching models. For example, NIDES uses rules to describe attack actions, STAT uses state transition diagrams to model general states of the system and access control violations, and IDIOT uses Colored Petri nets to represent Clone signatures as sequences of events on the target system. The key advantage of misuse detection systems is that once the patterns of known Clones are stored, future instances of these Clones can be detected effectively and efficiently. However, newly invented attacks will likely go undetected, leading to unacceptable false negative error rates.

We are assuming data packet for this we are using method available in dot net environment. Packet depends on its types and on the protocol. Normally, a packet has a header and a payload. The header keeps overhead information about the packet, the service and other transmission related things. Such as data packet structure, structure include source IP address, destination IP address, sequence number of packet, type of service, flags etc.

The main aim of our proposed work is to develop defense mechanisms against DDos zombie in which our objective is to design a simulation environment with the used of dot net framework 3.0 where following objective is achieved.
- Design of Dynamic network
- Secured Date Packet
- Intruder detection and their Countermeasure

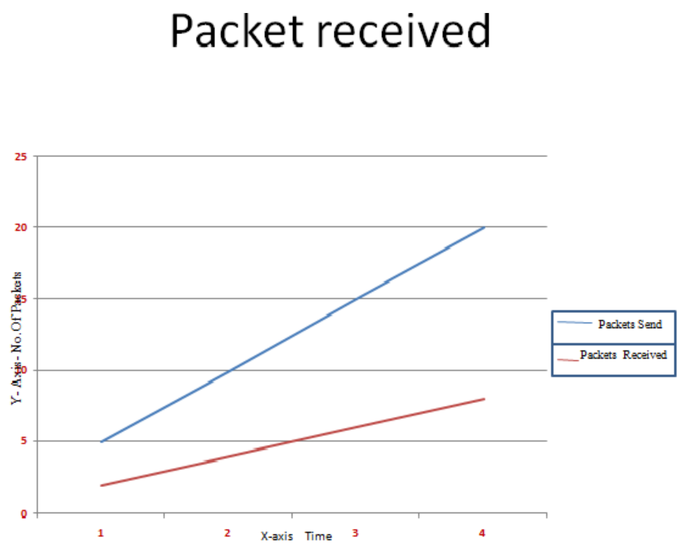
4. COMPARISON OF EXISTING SYSTEM WITH DEVELOPED SYSTEM

Sr. No	Characteristics	Existing System	Developed System
1	Platform	C	.Net Frame Work
2	Attack Type Addressed	Malicious and Infected Node	Malicious and Infected Node
3	Algorithm Used	Statistical Probabilistic	Dijkstra's - Shortest Path

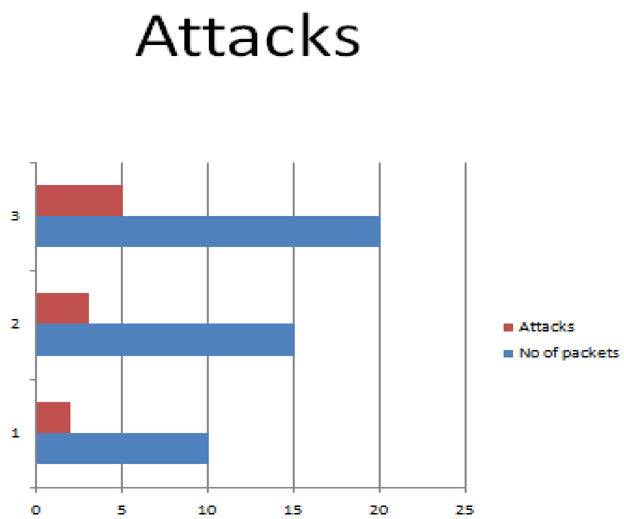
IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

4	Detection Technique	Probabilistic Threat Propagation	Hop by Hop
5	False Positive Rate	Low	0.1%(Medium)
6	Approaches consider association of node with other node	Yes	Yes
7	Advantages	Useful To solve Graphical Model	1.highly prevalent in the graph analytics world 2.Effective in Detecting Botnet and malicious web destination
8	Disadvantage	Does not consider Weight matrix	Takes time for network verification for across network.

5. EXPERIMENTAL RESULT



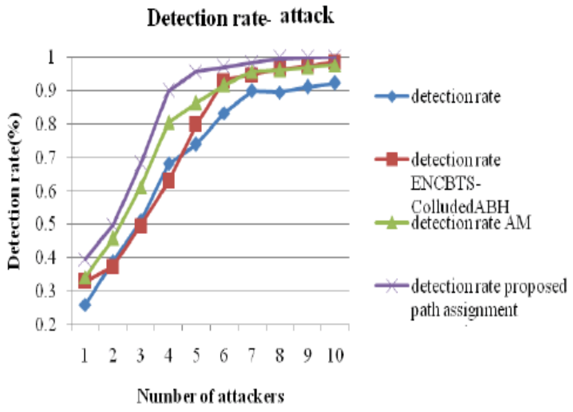
The x-axis show the no. of packets received and the y-axis show the no. of packets send hop by hop.



Here the blue colour shows no. of packets send and the red colour shows the number of attacks.

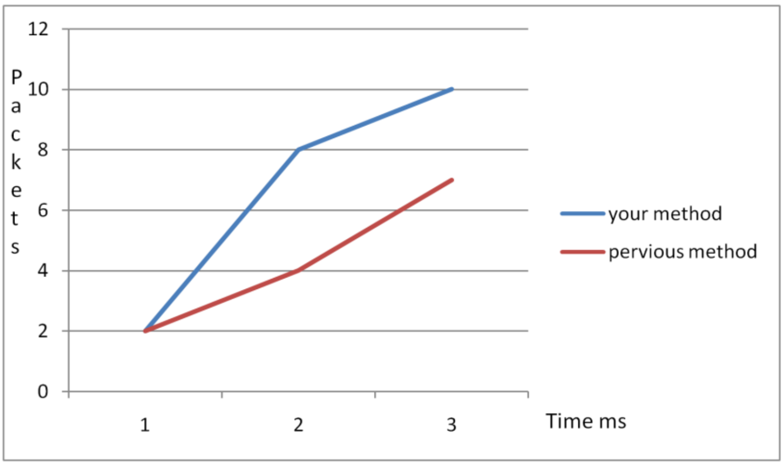
IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

Comparison of Detection rate with attack



Comparison of detection rate with attack.

Here the x-axis show the no. of attack performed and the y-axis shows the detection rate in percentage.



Here the above graph shows that the proposed system is more efficient than the previous method.

6. ANALYSIS

The proposed system is useful for any kind of network because verification methodology is implemented at each hop through which attack accuracy is improved. Attack is countermeasure before attack happened in network. The proposed solution is implemented in Network intrusion Detection System and Host-based Intrusion Detection which also improved the attack detection accuracy. Network traffic is not disturbed because attack completely countermeasure. Data is secured after attack happened because it prevented before its reaction. Countermeasure selection is useful after attack happened because with used of it network traffic is not disturb.

7. ADVANTAGES

This methodology is highly prevalent in the graph analytics world, the effectiveness of probabilistic threat propagation on the tasks of detecting botnets and malicious web destinations. The task is detecting malicious node in the network. Proposed System also shows the relationship between PTP and loopy belief propagation. The propagating threat probabilities across network nodes, give an initial set of known malicious nodes.

8. DISADVANTAGES

Takes time for network verification for across network.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

9. CONCLUSION

The system has program which verifies the packet and its behavior. Which will be verifies at each pass of packet in the network if any anomalies are found the packet will be block from entering into the network. For this purpose the packets are protected by encryption and provided with the security key pass by cipher. Md5 is provided for to enhance the protection layer for the packet which will be protected.

FUTURE SCOPE

In the future, we plan to investigate this issue. Our future plan also includes fathering in coverage and ongoing application tasks in the recovery process and developing a tested for evaluating the various failure recovery schemes.

REFERENCES

[1] Dr.Balachandra, D.N.Karthek," An Overview on Security Issues in Cloud Computing"IOSR Journal of Computer Engineering,Volume 3, Issue 1, 2012
[2] Hamoud Alshammari and Christian Bach,"Administration Security Issues In Cloud Computing" International Journal of Information Technology Convergence and Services, Volume.3, No.3, August 2013
[3] Manavi, Sadra Mohammadalian, Nur Izura Udzir, Azizol Abdullah," Secure Model for Virtualization Layer in Cloud Infrastructure" International Journal of Cyber-Security and Digital Forensics.The Society of Digital Information and Wireless Communications, 2012
[4] Mr. V.V.Prathap, Mrs.D.Saveetha," Detecting Malware Intrusion in Network Environment" Mr. V.V.Prathap, International. Journal of Engineering Research and Applications, Volume. 3, Issue 3 ,Version 5, pp.75-80, March 2013
[5] Chung,Tianyi Xing,Dijiang Huang," NICE: Network Intrusion Detectin and Countermeasure Selectionin Virtual Network Systems" IEEE Transaction on Dependable and Secure Computing, Volume. 10, No. 3, JULY/AUGUST 2013
[6] Shina Sheen,R Rajesh," Network Intrusion Detection using Feature Selection and Decision tree classifier" IEEE Region 10 Conference,200
[7] Polat, K., & Gunes, S. (2007). An expert system approach based on principal component analysis and adaptive neuro-fuzzy inference system to diagnosis of diabetes disease. Digital Signal Processing, 17(4), 702–710.
[8] Delen, D., Walker, G., & Kadam, A. (2005). Predicting breast cancer survivability: A comparison of three data mining methods. Artificial Intelligence in Medicine Artificial Intelligence in Medicine, 34(2), 113–127.
[9] Kayaer, K., & Yildirim, T. (2003). Medical diagnosis on Pima Indian diabetes using general regression neural networks. In Proceedings of the international l conference on artificial neural networks and neural information processing (ICANN/ICONIP) (pp. 181–184).
[10] Temurtas, F. (2009). A comparative study on thyroid disease diagnosis using neural networks. Expert Systems with Applications, 36, 944–949
[11] Rumelhart, D. E., Hinton, G. E., & Williams, R. J. (1986). Learning internal representations by error propagation. In D. E. Rumelhart & J. L. McClelland (Eds.). Parallel distributed processing: Explorations in the microstructure of cognition (Vol. 1, pp. 318–362). Cambridge, MA: MIT Press.
[12] Brent, R. P. (1991). Fast training algorithms for multi-layer neural nets. IEEE Transactions on Neural Networks, 2, 346–354
[13] Gori, M., & Tesi, A. (1992). On the problem of local minima in backpropagation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 14, 76–85
[14] Gulbag, A. (2006). Dagaalty work **. Ph.D. Thesis, Sakarya University, Institute of Science & Technology.
[15] Gulbag, A., & Temurtas, F. (2006). A study on quantitative classification of binary gas mixture using neural networks and adaptive neuro fuzzy inference systems. Sensors and Actuators B, 115, 252–262
[16] Hagan, M. T., & Menhaj, M. (1994). Training feed forward networks with the Marquardt algorithm. IEEE Transactions on Neural Networks, 5, 989–993.