# "PTP in Network Security for Malicious Misbehavior Activity Detection"

Tejaswini S. Akulwar
Student of M.tech.(CSE)
R.C.E.R.T
Chandrapur, India

Associate Prof. P. S. Kulkarni
Department (I.T)
R.C.E.R.T
Chandrapur, India

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. Literature Survey`

[1] Dr.Balachandra et al an Overview on Security Issues in computing Level Agreement or any Trust third party that can control the processing over Computing. They are offering an adequate level of security and privacy for the information.

Dr.Balachandra also works on how security and compliance integrity can be maintained in new environment. The prosperity in computing literature is to be coming after security and privacy issues are resolved. Environment to achieve the 5 goals i.e. availability, confidentiality, data integrity, control and audit.

[2] Christian Bach et al have work on most administration security issues and concept of the service level agreement. The solution to get more secure computing environment is to have a strong service in the NICE: Network Intrusion Detection and Countermeasure Selection Virtual Network Systems

The system and security evaluations demonstrate the efficiency and effectiveness of the proposed solution. NICE, which is proposed to detect and mitigate collaborative zombies in the virtual networking environment.

[3] Azizol Abdullah et al have worked on entropy method which is used to identify the zombie's efficiently and supports a large scalability. An effective and efficient IP Trackback scheme against Distributed Denial of Service (DDOS) zombies based on entropy variations. The entropy algorithms are independent from the current routing software; they can work as independent modules at routers.

[4] Mrs. D. Saveetha et al have worked on entropy based detection of DDos zombies. Interesting feature of this method is that source of zombie can easily trace back by calculating the packet size, which shows the variation between normal and DDOS zombie traffic, which is fundamentally different from commonly used packet marking techniques

[5] Mr. V.V.Prathap et al have implemented three different approaches for feature selection such as chi square, information gain and relief which is based on filter approach Intrusion Detection with feature selection was able to outperform the decision tree algorithm without feature selection Intrusion Detection approach is very useful for counter measure.

[6] A System Introspection Based Architecture for Intrusion Detection an architecture that retains the visibility of host-based IDS, but drag the IDS outside of the host for greater zombie resistance. The pattern recognition technique to intrusion detection and proposes a network intrusion detection approach based on multiple classifier selection, called CDS. This method is very useful intrusion detection. Approach for intrusion detection which co-locates IDS on the same machine as the host it is monitoring and leverages a system monitor to isolate the IDS from the monitored host.

[7] Shina Sheen et al have proposed a model to secure and proper mechanism to react reasonable against the detected zombie by intrusion detection system. With the secured model (SNODE) against the zombie SVL model, (Secure Model for Virtualization layer) which combines virtualization and intrusion detection system, can increase the detection rate and provide protection against zombies targeting virtualization, and consequently will result in reliable cloud security the proposed model and framework will be implemented in order to compare and evaluate it.

[8] Detecting Malware Intrusion in Network Environment three model intrusion detection Threat model, zombie graph model, existing model NICE utilizes the zombie graph model to conduct zombie detection and prediction. NICE only investigates the network IDS approach to counter zombie explorative zombies.

[10]Network Intrusion Detection using Feature Selection and Decision tree classifier three different approaches for feature selection such as chi square, information gain and relief which is based on filter approach Intrusion Detection with feature selection was able to outperform the decision tree algorithm without feature selection Intrusion Detection approach is very useful for counter measure.

Paper [2] Hamoud Alshammari et al shows that by using a single peer to peer method if a bot is detected then it is possible to detect another member of the same network. In a paper, a simple method is presented to identify member host from known peer nodes, of an unstructured P2P botnet in a network. Method provides a list of hosts ordered by a degree of certainty that belong to the same P2P botnet as discovered node belong. Method represents that peers of a P2P botnet communicate with other peers to receive command and update. In spite of some different bots can communicate with another peer bot. Paper shows that for P2P botnets is an unstructured topology where bots randomly select peers for communication it is rarely high probability that bots communicate with external bot though a given time window. There is a probability pair of malicious within a network has a mutual contact.

[3] Manavi et al a Botnet Sniffer method is given to detect botnet C&C problem. A proposed approach uses network based anomaly detection to identify botnet C&C channels in a local area network (LAN) without the knowledge of signature or C&C server addresses. This method can identify both the C&C servers and infected hosts or bots present in the network. This

approach based the observation of the pre-programmed activities related to C&C. A bot node within the same botnet will likely show the spatial-temporal correlation and similarity. Paper [4] presents conditional random fields method to build probabilistic models to segment and label sequence data. Methods provide several advantages over Markov models and stochastic grammars for such tasks. Conditional random fields also avoid a limitation of the label biased problem present in maximum entropy Markov models (MEMMs) and other Markov models using directed graphical models. Paper used iterative estimation algorithms for conditional random fields.

## 3. Existing Problem Statement:-

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

IP Trace back (IPT)is a method that enables the proper identification of the source of a packet on a network and may at the same time provide the full or partial path reconstruction of that packet as it traverses the network.
Proposed mechanism is consists for following steps.

**Module 1)** Source Port and Destination Port: If source port or destination port is blank or 0 then it will treated it as zombie packets.
**Module 2)** Checksum: Network data transmissions often produce errors, such as toggled, missing or duplicated bits. As a result, the data received might not be identical to the data transmitted, which is obviously a bad thing. Because of these transmission errors, network protocols very often use checksums to detect such errors. If the checksum field of incoming packets is empty or contains invalid value then that packet will be treated as zombie.

**Module 3)** Time To Live: Time-to-live (TTL) is a value in an Internet Protocol (IP) packet that tells a network router whether or not the packet has been in the network too long and should be discarded. TTL is an 8-bit field so its value ranges from 0 to 255. If TTL field of incoming packets contains value outside the range then that packet will be treated as zombie packet.
**Module 4)** Total Length: Total length defines the entire packet (fragment) size, including header and data, in bytes. So header length must be less than that of total length.
**Module 5)** A SYN flood is a form of denial-of-service zombie in which and zombie's sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

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.

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

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 neighbor's 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**

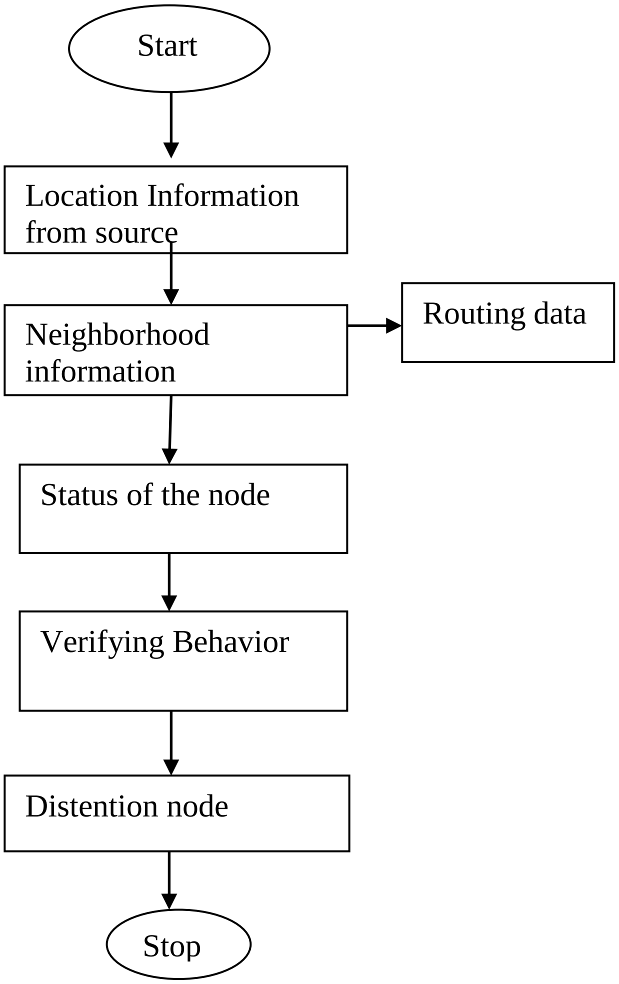

**Fig 1. Flow Chart**

## 4. DESIGN MODULE

**User Module:**

In this module, Users are having authentication and security to access the detail which is presented in the ontology system. Before accessing or searching the details user should have the account in that otherwise they should register first.

**Countermeasure Selection:**

Countermeasure Selection to illustrate how works, let us consider for example, an alert is generated for node 16 (*vAlert* = 16) when the system detects Buffer overflow. After the alert is generated, the cumulative probability of node 16 becomes 1 because that attacker has already compromised that node. This triggers a change in cumulative probabilities of child nodes of node 16. Now the next step is to select the countermeasures from the pool of countermeasures *CM*.

**Attack Analyzer:**
The major functions of system are performed by attack analyzer which includes procedures such as attack graph construction and update, alert correlation and countermeasure selection. The process of constructing and utilizing the Scenario Attack Graph consists of three phases: information gathering, attack graph construction, and potential exploit path analysis. With this information, attack paths can be modeled using. Each node in the attack graph represents an exploit by the attacker. Each path from an initial node to a goal node represents a successful attack.

**False Alarms**:
A virtual network system with hundreds of nodes will have huge amount of alerts raised by Snort. Not all of these alerts can be relied upon, and an effective mechanism is needed to verify if such alerts need to be addressed. Since Snort can be programmed to generate alerts with CVE id, one approach that our work provides is to match if the alert is actually related to some vulnerability being exploited. If so, the existence of that vulnerability in means that the alert is more likely to be a real attack. Thus, the false positive rate will be the joint probability of the correlated alerts, which will not increase the false positive rate compared to each individual false positive rate. Moreover, we cannot keep aside the case of zero day attack where the vulnerability is discovered by the attacker but is not detected by vulnerability scanner. In such case, the alert being real will be regarded as false, given that there does not exist corresponding node. Thus, current research does Not address how to reduce the false negative rate. It is important to note that vulnerability scanner should be able to detect most recent vulnerabilities and sync with the latest vulnerability database to reduce the chance of Zero-day attacks.

## ANYLYSIS

The system has level of security for protection of data which verifies the packet for detection of intruder so that the countermeasure can be applied zombies usually involve early stage actions such as multistep exploitation, vulnerability scanning, and compromising identified vulnerable virtual machines as zombies, and finally DDoS zombies through the compromised zombies. Within the system, especially the detection of zombie exploration is extremely difficult. Another important function of the network controller is to assist the zombie analyzer module. According to the controller receives the first packet of a flow, it holds the packet and checks the flow for complying traffic policies. The methods for selecting the countermeasures for a given scenario. When vulnerabilities are discovered or some are identified as suspicious, several countermeasures can be taken to restrict zombie's capabilities and it is important to differentiate between compromised and suspicious packets.

The countermeasure serves the purpose of: 1) protecting the target VMs from being compromised, and 2) making zombie behavior stand prominent so that the actions can be identified. The proposed system is useful for any kind of network because verification methodology is implemented at each hop through which zombie accuracy is improved. is countermeasure before zombie happened in network. The proposed solution is implemented in Network intrusion Detection System and Host-based Intrusion Detection which also improved the zombie detection accuracy. Network traffic is not disturbed because zombie completely countermeasure. Data is secured after zombie happened because it prevented before its reaction. Countermeasure selection is useful after zombie happened because with used of it network traffic is not disturb. 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 protecting from the zombies.

- The proposed system is useful in Network intrusion Detection System and Host-based Intrusion Detection, which exactly finds the source of zombie by studying the variation of packed size in travelled path. Our solution will also be applicable on decentralized network because we have included verification methodology at each hop. Verification methodology provides detection accuracy in host based solution to cover whole network segment. Is countermeasure before zombie happened?

- 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 system’s 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.

## 5. 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.

## 6. 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.