Intrusion Detection Systems: Enhancing Network Security in the Digital Age A Botnet: Swarm of Infected Devices

Mohammed Ehsan Ullah Shareef [1], Ms. Momin Misbah[2]

[1]Research Author, Hyderabad, India.
[2]Incharge Department of Information Technology, G. M. Momin Women's college, Bhiwandi, Mahrastra, India.

Abstract:
In the era of cyber security threats, the botnet represents the extremely thoughtful threats being met by various organizations in recent times. It is reported that botnets are used to handle many cybercrimes recently. Though much research has been skilled in analyzing and detecting botnets, numerous challenges such as the ability to design detectors that deal with new forms of botnets stay unaddressed. In this thesis, I represent the work on the identification of Command & Control (2C) traffic of IRC-based botnets, HITP-based botnets, and P2P-based botnets using machine-learning-based classification techniques.

Once identification of the bot is completed, the system will raise an alarm sound and also send a text note to the system administrator. The system administrator immediately performs the utmost needed security actions like blockage of the corresponding IP address, placing them under profound observation or interim over the same apprehensive network segments. The primary emphasis of this thesis is on, development of a system for the detection of P2P botnet from network traffic using 2 steps or phases namely P2P host detection and P2P botnet detection. The host-based approach is used for P2P host detection while P2P botnet detection uses a flow-based approach and accrued a combined accuracy of 99.98% for both phases. We also assessed the presence of the model developed on the offline network traffic and established a modest GUI-based engine that accepts the input as the host IP address and spots the hosts if any based on the botnet behavior.

Based upon the key factors Bot Ransack is the system developed to detect IRC, HTTP, and P2P botnets. The results after several experiments illustrated the proposed system detects all the botnet IRC traffic and spots the affected hosts as well as the 2C server. During the implementation of Bot Ransack, the considered and finalized threshold values as 0.63, 0.61, and 0.62 for IRC botnet, HTTP botnet, and Peer to Peer botnet respectively for which the results showed earlier have illustrated the optimum performance which even compared with the earlier research work based on traditionally based botnet detection approaches.

Even though there are other cyber-attacks taking place, one of the significant bot-based attacks is currently making headlines. The importance of botnets prompted researchers to study them and develop solutions to eliminate them. Peer-to-peer (P2P) architecture for botnets provides improved detection resistance over client-server architecture.

Keywords: Control and command, 2C, Botnet, IRC-based botnet, HITP-based botnet, P2P-based botnet[1]

I. Introduction:

People have access to the Internet. According to global Internet user statistics, nearly half of the world's population uses the Internet for communication, banking transactions, and information. Organizations use it for business purposes, such as connecting with customers, partners, and suppliers. Such widespread Internet use inaugurates a brand-new era of cybercrime. Among all cyber-attacks, bot attacks appear to be one of the most significant players on the cybercrime scene.

Botnet: The botnet is resultant of the words "Robot" and "Network'. A Botnet is a combination of at least one Bot Controller or Bot Server and one or multiple Bot Clients. The fundamental concept of a Botnet is to behave in a coordinated fashion with all or a few parts of the botnet. A botnet is not a virus but an assortment of malicious software for malicious purposes. In simple, a Botnet is a cluster of infected devices with a bot program. In other words, BOT is a blend of software instructions connected to Command and Control (hereafter called C&C or 2C) Network.

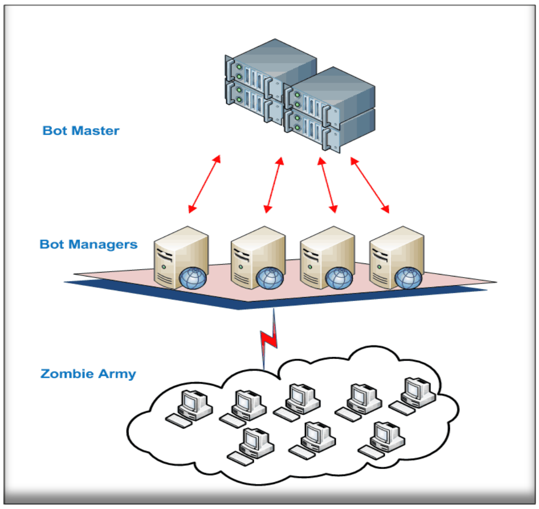

Figure 1.1 Bot Controller

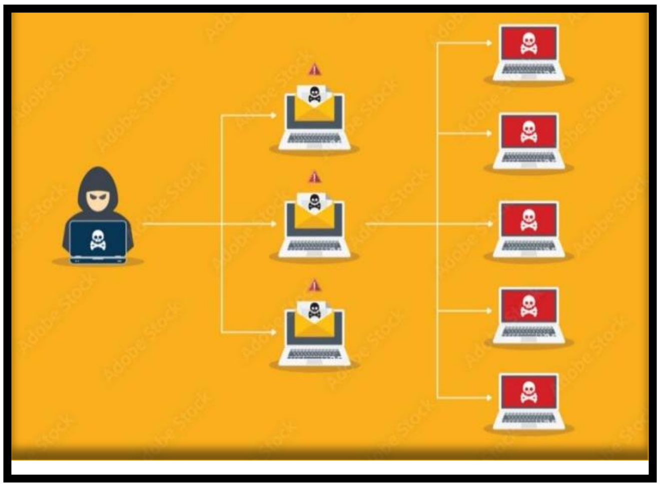

Figure 1.2 Botnet Attack

[1] An enhanced model for network flow-based botnet detection

Botnets are controlled by a botherder or a bot herder which acts as a service tool. Botnets are evolving threats to information security and are thus attractive to hackers because botnet clients carry out the hackers' commands on devices that are not directly connected to them, making prosecution and investigation much more difficult. The command interpreter of a botnet can autonomously retrieve commands and carry them. Botnets are now a part of Cyberwarfare, Cybercrime, and Cyber terrorism (96).

Every individual device in a botnet network is called a Bot. The Bot controls 2C servers using botnets as a botnet attack is a cyber-attack on a large-scale controlled remotely supported by malware-infected systems 971. These malware-infected devices are used as missiles to accomplish malevolent happenings such as monetary fraud and cyber espionage. The Botherder or Bot Herder is an individual who works on the botnet infrastructure and practices the affected computers to launch attacks intended to crash a target's network, insert mal-ware, yield credentials or implement CPU-intensive tasks.

In today's Internet era, botnets are the intensive threats that lead to several forms of Internet crimes, immensely profitable which still depend on centralized IRC 2C structure. Most of the Click frauds, DDoS attacks, spyware, Spam, and many more originated from botnets and mysterious establishments behind them. A new example of a P2P botnet on a large scale is Strom Worm which is widely covered in the media 102. Several botnet countermeasures are happening,

The botmaster traceback comes across encryption, steppingstones, and low traffic volume as the three most significant challenges. Even though the obstacles are overcome with a technical solution, the touch of the challenge is outside the reach of the Internet as mobile device networks, public computers; open wireless access points offer a supplementary layer of concealment for the botmasters.

In this instance, the remaining botmasters analyze the greater risk over benefits by monitoring more and more colleague botmasters getting caught. Even if the traceback technique is imperfect, the equation drastically changes by convincing. More botmasters that are not[2]worth the risk of passing the next 10-20 years in prison.

Famous Botnet Attacks:

- **Agobot (2002)**: One of the earliest botnets, Agobot was designed to distribute spam and steal personal information.
- **Storm Botnet (2007)**: Named after the email subject “230 dead as storm batters Europe”, it was one of the first botnets to use peer-to-peer communication.
- **Conficker (2008)**: Also known as Down up or Downdip, Conifer infected millions of computers worldwide, leading to a massive botnet that could launch destructive attacks.
- **Zeus (2009)**: This botnet was used to steal banking details and other personal information from infected computers, leading to significant financial losses.
- **Cutwail (2009)**: One of the largest spam botnets, responsible for a large portion of the world’s spam emails at its peak.
- **Miraibotnet (2016)**: Notorious for a massive DDoS attack that took down major websites, including Twitter, Netflix, and Reddit.
- **Emotet (2014-2020)**: Originally a banking Trojan, it evolved into a botnet delivering a variety of malware.

[2]Labridis, D.P. Short-term risk assessment of botnet attacks on advanced metering infrastructure

Life Cycle of a Botnet

Financial profits are the main motivation for botmasters to design and develop botnets. For instance, a 21years old hacker member named Jean-son Ancheta has profited more than 100,000 Dollars from multiple Internet ad vendors for designing malicious code into 400,000 and more vulnerable devices Wilson 2007. Analyzing the scope, Vinton Cerf has estimated that there are nearly 100-150 million out of 600 million hosts that are a part of the botnet Weber 2007.

Botnet when viewed from a product life-cycle perspective, we can understand the work of creation of a botnet, implementation of a botnet, integration of a botnet, usage of the botnet, and additionally organizing a huge number of projects to defeat botnets. Excluding the above-cited main components (Bots and Botmaster) of the botnet, other characters which appear during the botnet's life cycle are Developer, Client, Victim, and Passive participant.

- **A "Developer"** is a person or group of persons whose job is to plan and develop the botnet. These are usually named "Do-It-Yourself" (DIY) malware generation kits or malware creation kits.
- **"Client"** of a botnet are of 2 key types. A few clients lease services of the botnet from a botmaster and the other few clients pursue becoming botmasters.
- **"Victim"** is the network, a system, or a person depending upon the purpose of the botnet which establishes the object of the attack accomplished. A user receiving spam, stealing confidential information from a user, losing millions of dollars by a company because of a DDoS attack, and many more.

II. Literature Review:

Botnet Detection:

A botnet comprises many malware-infected client computers that are controlled by a remote server to perform malicious acts. A remote command and control server cancontrol botnet computers to perform these types of attacks:

- Denial-of-service attacks
- Sending spam and viruses
- Stealing private data from clients

Botnets have traditionally used HTTP and IRC protocols to communicate with infected botnet clients. To block this communication, network security services can control access to these services and ports. For example, the Firebox can use the Web Blocker *Command and Control* and *Botnet Activity* categories to block communication from infected botnet clients on your network to botnet sites over HTTP. For more information about Web Blocker.

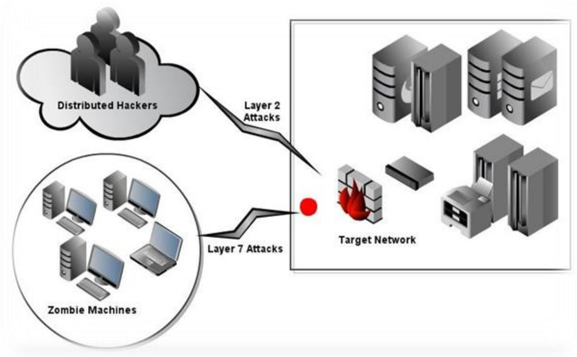

Figure 2.1: How machines get attacked.

HTTP-based botnet Detection: the web-based botnet is also named an HIPP-based botnet whose interaction channel among the 2C server, and its bot clients is through HITP. A 2C server of an HTTP-based botnet works like a regular HTTP server, and bot clients of an HTTP-based botnet work as regular HTTP clients. The 2 botnets Spy eye and Zeus are well-known HTTP-based botnets. As per the work mentioned in Chapter 3 regarding IRC protocols and P2P protocols Chapter 4 introduces HTTP protocols and HTTP is quite striking to the botnet possessors.

Firstly, nowadays HTTP traffic is the prevalent Internet traffic so web-based botnet traffic can easily be masked as regular HTTP traffic by making the botnets undiscovered. Secondly, hosts are allowed by the network firewalls or network proxies to access the Internet through the HTTP thus resulting in web-based botnets providing constant and competent client-server connectivity.

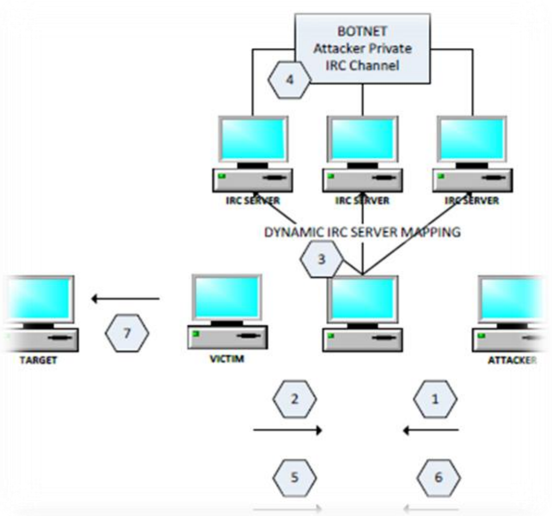

Figure 2.2: Infected network of bot system

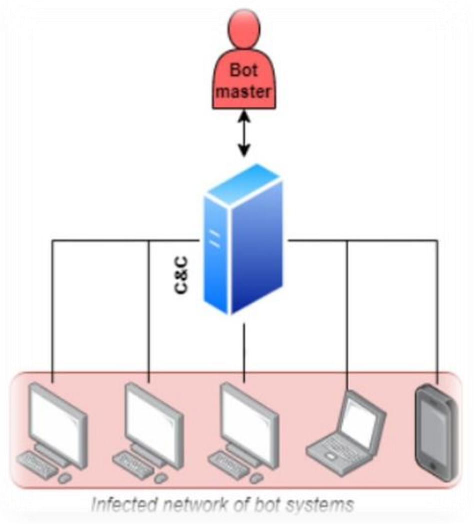

Figure 2.3: IRC based botnet detection.

IRC based Botnet Detection: is in the application layer of the network model.

The process of communicating or chatting follows the Client/Server model. IRC clients are none other than the system programs that any user can install on their devices irrespective of the location, time, and operating system. These IRC clients use chat servers to communicate among themselves or other clients as the primary purpose of Internet Relay Chat is designed for cluster messaging in channels (101 and also allows client-to-client communication by a private message either to transfer the data or to share the files or both. Virtual rooms are arranged to communicate globally by enabling Internet Relay Chat. These IRC clients join central IRC over the internet to distribute the messages throughout the network.[3]

III. Research Methodology

The faked packets are utilized in this simulation to validate the proposed system by acting like a botnet. To create these forged packets and send them to the destination port as if they were normal devices, Python programming is employed. depicts the implementation code for the falsified packets: When the code is run, the following interface is generated, as and we can see that every field is empty in this first interface, which is titled "Before Operation Starts."

The intercepted packet field displays packets with the ICMP and ICP proto-cols. a few parameters such as Source and Destination ports, Source and Destination address, and Protocol are the minimum adequate parameters provided to characterize the packet. The application provides an auxiliary function along with the sniffing packet, namely, the percentage of the packet that is HTTP, the maximum group size, total HTTP traffic, and total sniffed packet, in order to evaluate the further study from the "during the packet sniffing starts" observation.

Before the timer occurs, the packets sniffed from the ports are merely placed on a provisional list. After the timer starts, or "during the timer event," this tetrapolar list will be created. the paths and methods through which the current packet list is modified in real-time. a sample implementation code for the timer event function. This serves as a helping hand to the administrator by allowing them to examine how packets are handled at each level.

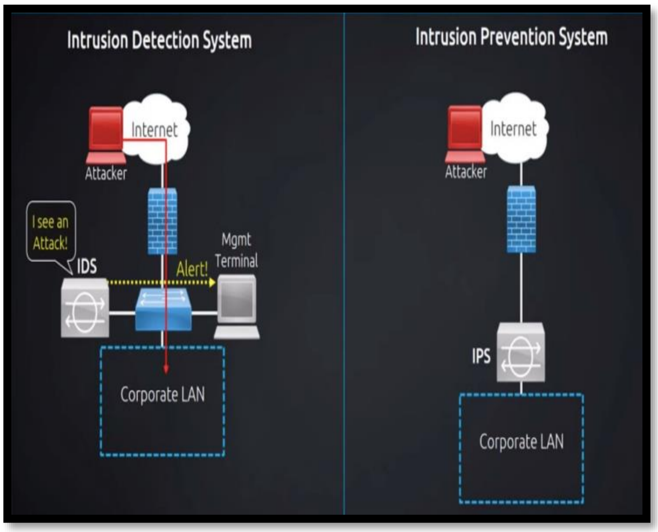

Figure 3.1: Intrusion mechanism system

The following is the description of the code steps:

- Filter local address, which performs packet filtering along with source IP address within the LAN. Likelihood botnet group, in which packets are grouped according to their destination IP address. Each group is saved in a separate list before moving on to the next phase.

[3] Wang, Z. Gong, and J. Hou, "Overview of botnet detection," Computer Research and Development

- Group homogeneous response, where the packets grouped in step 2 are grouped again depending on payload size and destination port number. Filter destination port, where full temporary packets are grouped according to the destination port number.
- Packet synchronization to a certain C2 server is indicated by traffic correlation. The higher the correlation, the more synchronized the system is. Meanwhile, the time gap between the longest and shortest time stamps is known as traffic correlation.
- Keep track of group flows, noting key events such as forming a homogeneous group from the blacklist, calculating group confidence, and sending an alert message if group confidence reaches a certain threshold number.
- Flow record where the group activity blacklist is stored for further group confidence calculations.

"During the botnet detection process," when a specified packet group is analyzed and the group confidence value exceeds a threshold value, an indication of botnet detection appears. The system subsequently sends an email to the administrator, as to inform them that a bot has been discovered in the LAN.

The administration is also notified of bot detection, via a message delivered to a mobile phone, commonly known as SMS,

The logs are likewise kept throughout the network Using the model trained in two stages, we created a system for botnet detection that works on live traffic and has a simple GUI (Graphical User Interface).

The IP addresses that need to be inspected are entered by the user. the user can enter the I address in two ways: as a comma-separated list or as a CIDR (Classless Inter-Domain Routing) format, such as 172.27.20.0/28. All IP addresses in the subnet are being monitored. The system automatically detects all available network interfaces and displays a list of them to the user. After choosing a network interface and entering an IP address, as soon as the user presses the start detection button, the system begins to detect.[4]

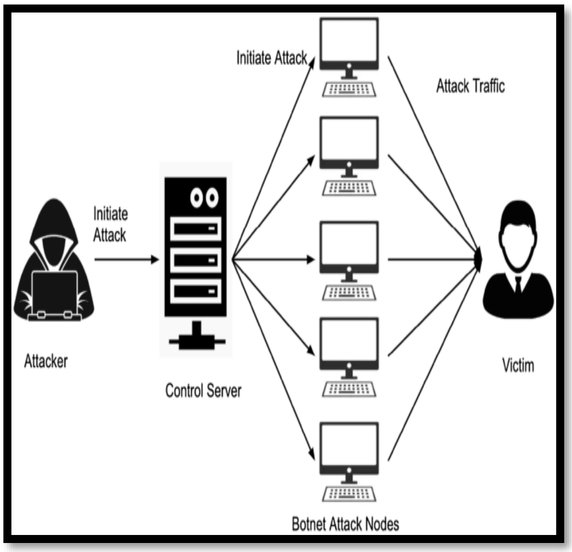

Figure 3.2: Bonet attacking

[4] Bot Tracer: execution-based bot-like malware detection

Figure 4.1 Network security

IV. Research Objectives for Proposed Work:

The objective of the title is to deliver the finest methodology to sense botnets using the evidence of by Net Flow dataset. This approach uses a machine to perform classification network flows as cither normal data flow or a botnet. 'The objective also specifies whether a botnet is classified under IRC botnet or ITTP botnet or Peer to Peer botnet. The objective apart from the classification of the botnet type also concentrates on the behavior of hosts as well as the network with and without the presence of the bots. Overall, the objective of the proposal is to detect and classify the type of botnets as INC, HTTP, and Peer to Peer along with the hosts behavior and network behavior using Machine Learning.

In particular. the specific objectives are determined to

- Settle optimum classification of the data flows among the botnet and the normal traffic.
- Select the appropriate machine learning algorithm for the prompt classification of network flows.

Neural network-based Botnet Detection

Proposed method used Backpropagation techniques for botnet detection using network traffic detected botnets with no false positives with 98.89% detection rate, 95.69% accuracy, FP rates of 0.00956 set back of the method is only a few types of botnet characteristics. The proposed method used PSI- Graph for botnet detection with faster FCGs, better FNR, FPR, and accuracy.

The proposed Convolution Neural Network is used for botnet detection automatic feature detection is used to achieve an accuracy of 99.98% for Dense Net and 83.15% for SVM setback of the method is training process.[5]

V. Conclusion

The era of the Internet is so connected to the people that most humans use the Internet for communication, retrieving information, banking transactions, leisure and entertainment purposes, etc. Governments and various administration departments utilize the internet for connecting with people, partners, suppliers, and their business purposes. Such huge usage of the Internet is leading to the period of Cybercrimes.

A framework is designed to detect botnets, and the method for detecting P2P hotnets in the network is a two-step process. In step 1, all hosts involved in P2P activity are identified using a host-

[5]5David Zhao, Issa Iraore, Ali Ghorbani, Bassam Sayed, Sherif Saad and Wei Lu, "Peer to Peer Botnet Detection

based approach that looks for features that distinguish P2P hosts, such as failed connections, destination diversity, non-DNS connections, and so on. In step 2, P2P bots are detected using a flow-based approach from recognized P2P hosts by extracting flow-based features such as the number of bytes received and sent, packet inter-arrival time, packet frequency, and so on. These characteristics are used to construct a classifier model for detecting P2P bots.

Thus, by combining both approaches, a system with the simplest GUI to detect hotnets directly from real-time data is created in which the user enters the IP address or entire network to be observed and the system displays the status Of each host. To be more specific, the first phase is P2P host detection, and the second phase is P2P botnet detection.

Most predominantly IRC traffic is used by botnet detection systems as a means of interaction among the bots. In recent times botnets are using HTTP and P2P protocols which contribute the better secrecy than the earlier protocols. Analyzing IRC traffic alone is inadequate to identify bots. Thus, the research has a further scope on Peer-to-Peer botnet detection and HTTP botnet detection which has been implemented here.

There can be several developments that can be exhibited to spread this thesis by applying a few among the following:

- To train the model on live traffic as the current work mentioned in the thesis work on the offline traffic data and thus can be prolonged to train the model on live network traffic which help us to understand more about the traffic behaviour.
- Selection of another feature selection algorithm which helps in the reduction of the dimensionality of feature vector without compromising the performance. In vice versa, another feature selection may obtain a better feature selection.

References:

1. C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the loT: Mirai and Other Botnets," in Computer, vol. 50, no. 7, pp. 80-84, 2017, DOI: 10.1109/MC.2017.201.
2. Dev, J.A. Usage of botnets for high speed MD5 hash cracking. In Proceedings of the 2013 3rd International Conference on Innovative Computing Technology, Intech 2013, London, UK, 29-31 August 2013; p. 6653658.
3. Guntuku, Sharath Chandra & Narang, Pratik & Hota, Chittaranjan. (2013). Real-time Peer-to-Peer Botnet Detection Framework based on Bayesian Regularized Neural Network. Networking and Internet Architecture.
4. H. Wang, Z. Gong, and J. Hou, "Overview of botnet detection," Computer Research and Development, vol. 47, no. 12, pp. 2037-2048, 2010.
5. J.Liang, N. Naoumor and K. W. Ross, "The Index Poisoning Attack in P2P File Sharing Systems," Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications, 2006, pp.
6. K. Li, B. Fang, X. Cui, and Q. Liu, Research on the development of botnets," Computer Research and Development, vol. 53, no. 10, pp. 2189-2206, 2016.
7. K. Rajam, M. Chandramouleeswaran, "Fuzzy Implicative Ideals of - Algebras", International Journal of Pure and Applied Mathematics, Vol112 No. 5, pp.

8. L. Liu, S. Chen, G. Yan et al., "Bot Tracer: execution-based bot-like malware detection," in Proceedings of the 11th international conference on Information Security, pp. 97-113, Taipei, Taiwan, September 2008.
9. Nazario, J. politically motivated denial of service attacks. Crypto. Inf. Secure. Ser. 2009, 3, 163-181.
10. Sgouras, K.I.; Kyriakidis, A.N.; Labridis, D.P. Short-term risk assessment of botnet attacks on advanced metering infrastructure. IE'T Cyber-PhysSyst. Theory Appl. 2017, 2, 143-151.
11. Wu, Wei & Alvarez, Jaime & Liu, Chengcheng& Sun, Hung-Min. (2016). Bot detection using unsupervised machine learning. Microsystem Technologies. DOI: 10.1007/00542-016-3237-0.
12. Xians, C.; Lihua, Y.; Shuyuan, J.; Zhiyu, H.; Shuhao, L. Botnet spoofing: Fighting botnet with itself. Secure. Commun. Newt. 2015, 8, 80-89.
13. Y. Xie, Y. Fang, and K. Achan, "Spamming botnets signatures and characteristics," Computer Communication Review, vol. 38, no. 4, Pp. 171-182, 2008.