ENHANCEMENT OF IP TRACE BACK PACKET MARKING ALGORITHM TO DETECT DENIAL OF SERVICE ATTACK

BY

HABIBULLAH SALEEM

A dissertation submitted in fulfilment of the requirement for the degree of Communication engineering

Kulliyyah of Education
International Islamic University Malaysia

SEPTEMBER 2015

ABSTRACT

The Internet attack has been made possible by lack of source authentication in the IP protocol. The nature of identifying the internet attacker has been made difficult because of the open, trusting nature of the protocol which makes it possible for an attacker to spoof the source address. By using IP spoofing the attackers are able to hide their identity, thus making it extremely difficult to identify the source of the attack. Therefore, the main aim of using IP trace back scheme is to detect the source of the attack. This work focuses on enhancing IP trace back algorithm and applies egress filtering to detect denial of service attack. Qualnet 5.2 simulation software is used to simulate denial of service attack and IP trace back is used for trace back. The enhancement algorithm compromises of egress filtering and packet marking, the use of egress filtering is to discard the packets with illegitimate IP address. The performance metrics are throughput, jitter and delay, the simulation results shown that IP trace back enhancement improves detection of denial of service attack by observing performance metrics. The performance metrics is verified and the effectiveness is observed through simulation. The average percentage reduction of throughput was 44%, average delay was 63% and average jitter was 61% when comes to detection of DoS attack by using egress filtering. It is expected that further research would help improve the performance of this algorithm to expected level.

ملخص البحث

اصبحت هجمات الإنترنت ممكنة بسبب الافتقار إلى مصادقة المصدر في بروتوكول IP. كما اصبح تحديد طبيعة المهاجم الالكتروني أمر صعب بسبب طبيعة البروتوكول المفتوحة والثقة والذي يتيح للمهاجمين انتحال عنوان المصدر. باستخدام الحيل يستطيع المهاجمين إخفاء هويتهم، مما يجعل تحديد مصدر الهجوم صعباً للغاية. ولذلك، الهدف الرئيسي من استخدام نظامالتتبع الخلفي لل IP هو الكشف عن مصدر للهجوم. هذا العمل يتركز على تعزيز خوارزمية تتبع لل IP وتطبيق التصفية المكثفة (egress filtering) للكشف عن منع مهاجمة الخدمة. تم استخدام برنامج Qualnet 5.2 لتحفيز منع هجوم الخدمة واستخدم تتبع IP للتتبع. تتضمن حلول الخوارزمية تعزيز التصفية المكثفة وتحديد الحزم، استخدام التصفية المكثفة لتجاهل الحزم القادمة من عنوان IP غير مصرح له. مقاييس الأداء هي الأداء والتقطع والتأخير. اظهرت نتيجة المحاكاة أن تتبع ال IP يساعد على كشف هجوم رفض الخدمة عن طريق مراقبة مقاييس الأداء. مقاييس الأداء هي التحقق ولوحظت الفاعلية عن طريق المحاكاة. بلغمتوسطنسبةالانخفاضإلى 44%،متوسطمدةالتأخير63% ومتوسطتوترالإرسال 61% عندمايتعلقالأمربالكشفعنهجماتالدوسباستعمالتصفيةالمخارج (egress filtering).ان إجراء المزيد من البحوث من شأنه أن يساعد على تحسين أداء هذه الخوارزمية إلى المستوى المتوقع.

APPROVAL PAGE

I certify that I have supervised and read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Science in Communication Engineering.

.....
Suhaimi Abd Latif
Supervisor

.....
Md Rafiqul Islam
Co-Supervisor

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Science in Communication Engineering

.....
Teddy Surya Gunawan
Internal Examiner

.....
Othman O-Khalifa
Internal Examiner

This dissertation was submitted to the Department of Communication Engineering and is accepted as a fulfilment of the requirement for the degree of Master of Science in Communication Engineering

.....
Teddy Surya Gunawan
Head, Department of
Communication Engineering

This dissertation was submitted to the Kulliyyah of Engineering and is accepted as a fulfilment of the requirement for the degree of Master of Science in Communication Engineering.

.....
Md. Noor B. Salleh
Dean, Kuliyyah of
Engineering

DECLARATION

I hereby declare that this dissertation is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Habibullah Saleem

Signature..... Date....5/10/2015

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

ENHANCEMENT OF IP TRACE BACK PACKET MARKING ALGORITHM TO DETECT DENIAL OF SERVICE

Affirmed by Habibullah Saleem

..... 5/10/2015

Signature Date

ACKNOWLEDGEMENTS

Firstly, it is my utmost pleasure to dedicate this work to my dear parents and my family, who granted me the gift of their unwavering belief in my ability to accomplish this goal: thank you for your support and patience.

I wish to express my appreciation and thanks to those who provided their time, effort and support for this project. To the members of my dissertation committee, thank you for sticking with me.

Finally, a special thanks to Associative Professor Dr. Suhaimi Abd Latif for his continuous support, encouragement and leadership, and for that, I will be forever grateful.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

DDoS	Distributed Denial of Service
DNS	Domain Name Service
DoS	Denial of Service
HCR	Hop Count Radius
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
ISP	Internet Service Provider
PPM	Probabilistic Packet Marking
RAM	Radom Access Memory
SA	Security Association
SCAR	SPIE Collection and Reduction Agent
SMTP	Simple Mail Transfer Protocol
SPIE	Source Path Isolation Engine
SSH	Secure Shell
SYN	Synchronous

LIST OF SYMBOLS

$\sum$	Total number of packets
$E(X)$	Expected number of packets
$p(1-p)^{d-1}$	Unmarked packets
K	Number of fragments the address of the router
$ln(d)$	Log natural of number of hops
$\leq$	Number of packets
N	Number of packets
$ln(kd)$	Fragments number of hop
d	d is the number of hops

CHAPTER ONE

INTRODUCTION

1.1 INTRODUCTION AND OVERVIEW

The purpose of internet protocol (IP) trace back is to recognize the source of sequences of IP packets (e.g., identify the origin of Distributed Denial of Service (DDoS) packets) in the case of the origin of the IP addresses of these packets being spoofed. Routers and gateways assist with IP trace back, a method mostly conducted at the network layer. An attack on a victim host using a chain of connections (a 'stepping stone' chain) to hide the attacker's origin can be sourced using trace back. The stepping stones could be connections formed with telnet rlogin or Secure Shell (SSH).

Further, at each intermediate host the data is conveyed to the application layer in one connection and then resent to the network in the subsequent connection – meaning trace back across stepping stones is beyond the bounds of the network layer.

Research on IP trace back bloomed upon the increase in Denial of Service (DoS) attacks in the recent years. A number of DoS detection and response methods have been suggested since then, but they suffer from unpredictability and imperfections that render them incapable to recognize DoS attacks. The main problems with these methods are their incapacity to differentiate between DoS attack traffic and normal traffic, and their inability to source the DoS attacks in a distributed network.

During attack detection, the initial response is usually to source the attacker, which can be unachievable due to the plethora of vulnerable hosts involved in the

attack – the fact that the majority of attackers use fake source IP addresses makes sourcing more challenging. Fake source IP addresses refers to attackers using fake source addresses in the packet they release for attack. When this occurs, resolution involves all intermediate routers being scrutinized individually in order to discover the attack path. One can conclude that the internet has not been designed to deal with these kinds of attacks, and hence a real solution means re-engineering the whole network architecture.

In order to bring any attackers to justice, there must be identification of the attackers, though the use of vulnerable hosts by attackers as platforms to initiate DoS attacks makes this difficult. From a theoretical perspective, the originator of each IP packet is evident because it has the address of its source host, however pragmatically; no method exists to ascertain whether that an attacker has not placed a false, or "spoofed", address into the Source Address field. Moreover, it is not possible for every internet router to be able to discern the source of a packet they have received on their ports, much less its actual provenance.

The undertaking of finding an IP packet's originator is termed the 'IP trace back problem', and so far no clear answer to this problem has been offered. Various approximate solutions have been offered for IP version 4 (IPV4) (Lee, Thing & Xu, 2003). Nonetheless, IP version 6 (IPv6) has been made to deal with the exponential rise of the Internet and aims to take the place of IPv4. Although IPv6 is a young infrastructure, the majority of the operating systems and network devices (routers) are IPv6-capable as of yet, while lots of applications have been ported to IPv6.

There are various methods available to handle anonymous attacks, including source address filtering, SYN (Synchronous) Flood Protection, and applying a Black Hole Router server. The technique called 'source address filtering', initiated by

(Ferguson, 2000), filters out packets not possessing values in their SA (Security Association) field as being from those from an appropriate pre-set range. These packets cannot access the internet (Chen et al., 2011). Use of this technique on each interface, would result in a significantly smaller number of anonymous packets on the internet. Regrettably, source address filtering has a high overhead and results in administrative burden, and hence in reality it is not used extensively (Ohsita, Ata, & Murata, 2004). SYN Flood protection tracks half-open TCP connections and has a threshold for the number of these connections permitted to exist at the same time.

SYN Flood protection stops only SYN Flood types (D)DoS attacks, and is therefore attempts to use SYN Flood protection against other types of anonymous attacks is unavailing (Gavaskar, Surendiran & Ramaraj, 2010). Internet Service Provider (ISP) can also regulate the interface through their customers, who can report attacks after packets of DoS infiltrate the network, after which the ISPs can BlackHole a router on its network.

It is successful only with backscatter attacks, as explained by Moore, (Afanasyev et al., 2011), and ought to be carried out in the duration of the attack. A glaring drawback is that this method is confined to the boundaries of the given ISP. An intention-driven iTrace is also proposed to decrease excess Trace messages and hence advance iTrace systems' performance (Malliga & Tamilarasi, 2008). Another method proposed by (Chin & Chih, 2011) involves disallowing packets to get to victim(s).

This is useful as it takes a realistic approach. It is unfeasible to stop attackers from launching attacks, and so this method minimizes the potential effects of the attacks, in some cases removing the effects altogether.

An algebraic approach can be used to transform the IP trace back problem into a polynomial reconstruction problem, using methods from algebraic coding theory to regain the true origin of spoofed IP Packets (Zhang & Guan, 2006). Finally, a classical log-based IP trace back system termed 'Source Path Isolation Engine' (SPIE) has been created; its ability include the storage of message digests of recently obtained IP packets and rebuilding of the attack paths of given spoofed IP packets (Gong & Sarac, 2008). Apart from the previously mentioned methods, a number of methods and concerns about IP trace back exists including approximate trace back (Hussain, Heidemann &Papadopoulos, 2003), legal and societal issues (Duwari, & Govindarasu, 2006), vendors' solutions (Hussain, Heidemann & Papadopoulos, 2003).

Presently, the techniques accessible to handle anonymous attacks are hard to understand. Their drawbacks are due to them being confined to dealing with a small number of problems, and also due to their high cost of implementation. All methods described thus far are effective to some extent, however in real-life; complete eradication of internet attacks is unfeasible.

There are certain drawbacks of these schemes. Specifically, IP trace back cannot go beyond the hosts that send the spoofed IP packets. A typical attacker will naturally employ a number of stepping stones before they resort to, for example, a DOS attack. In order words, merely only identifying the origin of IP packets is not enough to bring the attack to justice.

DoS attacks are spread out by default; therefore they are able to give out a maximum number of packets from various attackers to a victim. The net sum of packets generates multiple attacks on the victim. A trace back scheme which necessitates fewer packets is needed for a complete trace back of the attackers. A lot

of IP trace back schemes were initiated and many of them need hundreds of packets to trace back the attackers.

Thus, the best measure is to recognize the source or sources of the attack in order to pave the way for assigning attackers with liability for their attacks. IP Trace back schemes use this philosophy to help solve the problem of internet attacks. This is the motivation for enhancing an IP trace back algorithm that will enable the detection of DoS attacks and minimize the DoS attacks

1.2 BACKGROUND AND RESEARCH MOTIVATION

Traceability systems impose a considerable burden upon routers, resulting in ISP providers being hesitant to set up these systems on the internet. In particular, one of the aims is to decrease the storage and trace back overhead, while also giving ISP incentives to deploy the traceability system.

1.3 PROBLEM STATEMENT AND ITS SIGNIFICANCE

The detection of denial of service attack by using IP trace back schemes has been extensively discussed in literature and is very important for an organization to assist in identifying the user who launched the attack. Although there have been many improvement in this area, the use of IP trace back scheme with intrusion detection system (IDS) and combine with filtering schemes can work together against security threats in the internet is a relatively new field compared to without using multiple detection schemes (Santhanam, Kumar, Agrawal, 2006).

The algorithm developed by Vamshi (2012), has a number of challenges such as, no filtering to separate invalid IP addresses from valid IP addresses, bandwidth consumption such as not separating legitimate traffic and filtering attack traffic.

With the advancement in IP trace back schemes, it is possible to enhance the IP trace back packet marking algorithm by combining it with egress filtering. This will enable it to separate the attack traffic from legitimate traffic and then filters out the attack traffic.

Hence, this research will investigate by using the egress filtering and improve detection of denial of service attack.

1.4 RESEARCH OBJECTIVES

i. To enhance IP packet marking algorithm using egress filtering.

ii. To simulate the enhanced IP trace back marking algorithm using Qualnet simulator.

iii. To evaluate performance of the enhanced IP trace back marking algorithm.

1.5 RESEARCH METHODOLOGY

The research methodology is explained in this section:

I. Literature review: Existing research on IP trace back schemes will be reviewed.

II. Enhancement: The IP trace back algorithm is enhanced by adding egress filtering to it and the filter discards invalid IP address.

III. Implementation of enhance IP trace back algorithm: The algorithm is implemented in QualNet simulator version 5.2.

IV. Evaluation and benchmarking: An analysis of the results is benchmarked and the option to improve detection of denial of service attack is discussed.

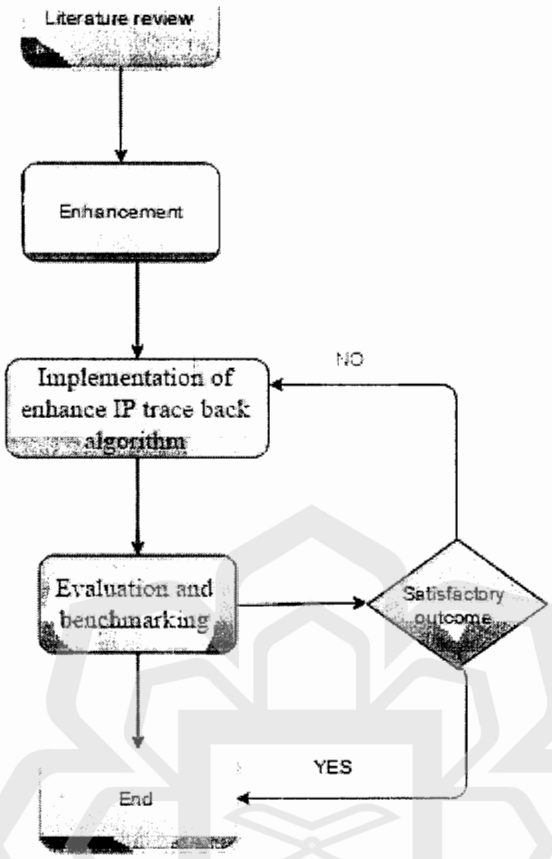

Figure 1.1 Research Methodology Flowchart

The summary of the Research Methodology is depicted in the flow chart shown in Figure 1.1. The current scheme was enhanced from previous master "Vamshi Krishna Eranti, (2012) "Implementation of Hop-Based Packet Marking for IP Trace back", university of Texas A&M University.

1.6 CURRENT SCHEME

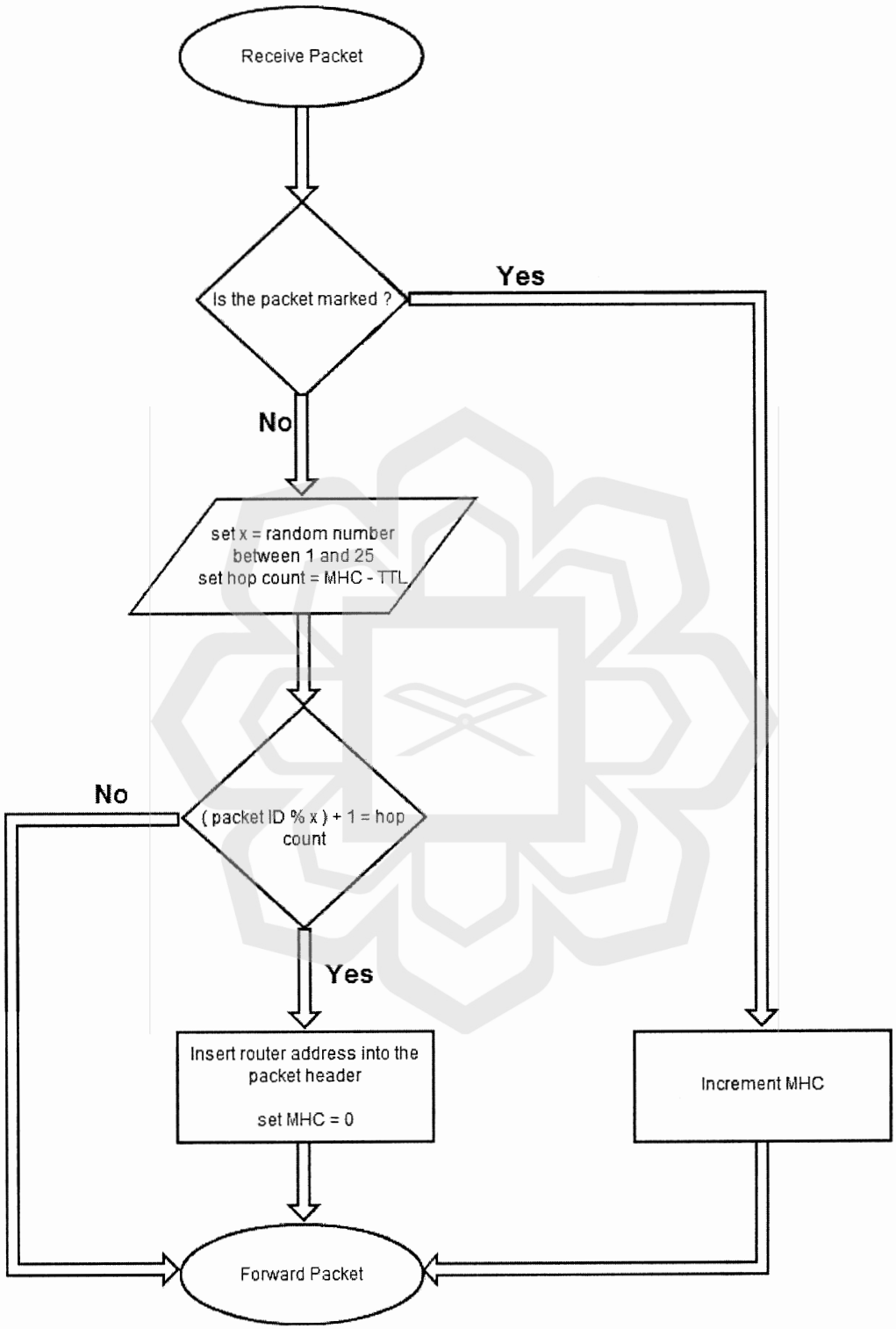

Figure 1.2 Flow chart Algorithms (Krishna, 2012)

1.7 PROPOSED SCHEME

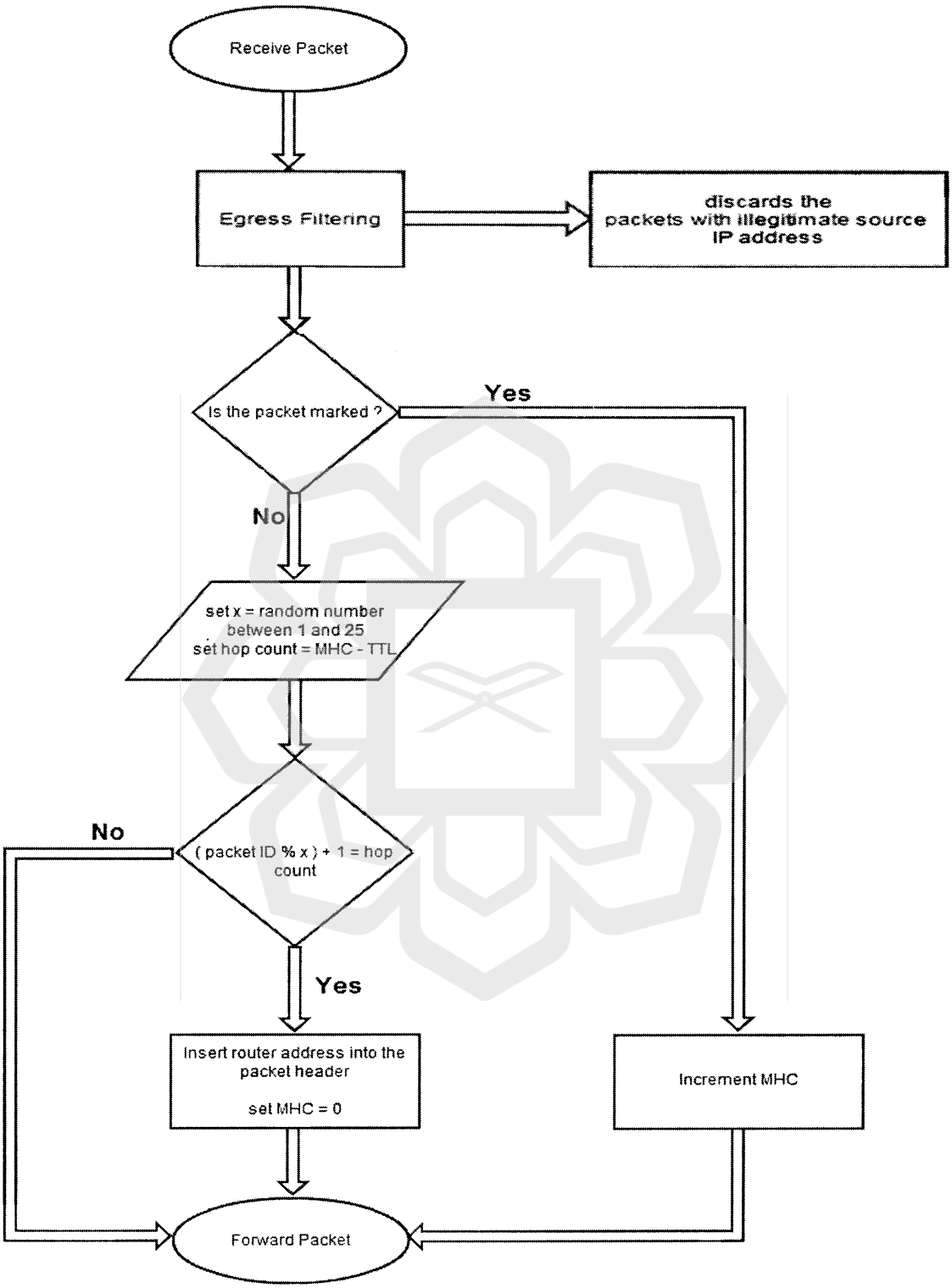

Figure 1.3 Enhanced Flow Chart Algorithm