République Algérienne Démocratique et Populaire
Ministère de l'enseignement et de la recherche scientifique
Université Dr Moulay Tahar de Saida
Faculté de technologie
Département d'Electronique
Spécialité : Télécommunications

Mémoire de fin d'études pour l'obtention du diplôme de master en Télécommunications

Option : Systèmes des télécommunications

Thème

Détection des Cyber-attaques par les mesures de divergence

Présenté par :

- Heni Mebarka
- Abdelli Nour El Houda

Soutenue le 06/07/2019, devant le jury composé de:

Mr. A.Garadi	*Président*
Mr. A.BENSAAD	*Examinateur*
Mr. B.BOUYEDDOU	*Encadreur*

Année Universitaire
2018-2019

Remerciements

Mon premier remerciement va a Allah soubhanou Wa ta hala

Nous tenions remercient vivement notre encadreur, ***Mr B.BOUYEDDOU****, pour sa gentillesse, sa disponibilité et sa contribution générale à l'élaboration de ce travail.*

Nos remerciements également les membres du jury qui ont pris la peine de juger ce modeste travail, qu'ils trouvent ici l'expression de notre profond respect et nos vifs remerciements.

Tout nos remerciements à tout les membres de nos familles d'avoir été toujours la pour nous, de leurs soutient de tout ordre.

Nous souhaiterions également remercient nos enseignants de la faculté de science et technologie et surtout les enseignants de département d'électronique qui ont participé à notre formation pendant toutes ces formidables années universitaires.

Nous remercient vivement tout notre promotion et leur souhaite bon courage pour leur travaux.

Pour tout, merci infiniment.

DEDICACE

Je dédie ce travail qui n'aura jamais pu voir le jour sans les soutiens indéfectibles et sans limite de mes chers parents qui ne cessent de me donner avec amour le nécessaire pour que je puisse arriver à ce que je suis aujourd'hui. Que dieux vous protège et que la réussite soit toujours à ma portée pour que je puisse vous combler de bonheur.

Je dédie aussi ce travail à :

Mes frères, mes sœurs et leur famille, pour leurs encouragements permanents, et leur soutien moral,

Ma grande mère, mes oncles, mes tantes et leur famille.

Tous mes amis, mes collègues et tous ceux qui m'estiment.

Je vous remercie tous

Heni Mebarka

DEDICACE

C'est avec une très grande émotion et un immense plaisir que je dédie ce modeste travail :

A mes très chers parents qui m'ont soutenu durant toute la durée de mes études.

Mes frères.

A tous les membres de ma famille, petits et grands.

A mes chères amies qui m'ont beaucoup aidé durant ces années d'études.

A tous ceux qui m'aiment et que j'aime.

Je vous remercie tous

Abdelli Nour El Houda

Résumé

Aujourd'hui la sécurité des réseaux informatiques est vitale et indispensable de repousser les attaques visant divers systèmes d'information dans tous les domaines. Par conséquent, les systèmes de sécurité doivent abolir ces attaques et ne pas permettre aux infiltrés d'exploiter une éventuelle violation du système, et corriger les vulnérabilités exploitées.

Le travail présenté dans ce mémoire se rapporte à la détection des différents types des cyber-attaques dans un réseau IP. Précisément, on utilise les mesures de divergence telles que Kullback-Leibler divergence (KLD), Hellinger Distance (HD) et CHI square (CHI) pour la détection des attaques de dénies de service DOS et DDOS de types SYN flood, UDP flood, Ping flood et Smurf.

A travers de nombreuses simulations, effectuées, sous Matlab, les résultats obtenus montrent que les mesures de divergences peuvent avoir un intérêt certain dans la détection des Cyber-attaques DOS et DDOS.

Mots clés : Cyber-attaques, mesures de divergences, KLD, HD, CHI square, attaques DOS DDOS, IDS datasets, DARPA 99, MAWI.

Abstract

Today the security of the computer network is vital and indispensable to repel attacks against various information systems in all applications. Therefore, the security systems must abolish the attacks and not allow the intruders to exploit a possible violation of the system, and correct the exploited vulnerabilities.

The work presented in this thesis targets the detection of different cyber attack's type's against IP network. Precisely, we use divergence measures such as Kullback-Leibler divergence (KLD), Hellinger Distance (HD) and CHI square (CHI) to reveal Denial Of Service DOS and DDOS attacks including SYN flood, UDP flood, Ping flood and Smurf.

Through numerous simulations carried out, under Matlab, the obtained results show that the divergence measurements can be very helpful in detecting DOS and DDOS cyber-attacks.

Keywords: Cyber-attacks, divergence measures, KLD, HD, CHI square,DOS/DDOS attacks, IDS datasets, DARPA 99, MAWI

Table des matières

Chapitre II: Les mesures de divergence

Liste des figures

Liste des tableaux

Liste des abréviations

ACK : Acknowledgement

CL : Control Limit

CLT : Control

CUSUM : Cumulative Sum

DARPA99: Defense Advanced Research Projects Agency

DDOS : Distributed Denial Of Service

DOS: Denial Of Service

EWMA: Exponentielly Weighted Moving Average

FIN : Final

FTP : File Transfer Protocol

JSD : Jensen-Shannon Divergence

HD : Hellinger Distance

HTTP : Hypertext Transfer Protocol

ICMP : Internet Control Message Protocol

IP : Internet Protocol

KLD : Kullback-Leibler Divergence

LCL : Low Control Limit

LGR en-tête : Longueur de l'en-tête ou offse

NSA : National Security Agency

OSI : Open System Interconnection

PING : Packet INternet Groper

POP3 : Post Office Protocol

PSH : Push

RST : Rest

SMTP : Simple Mail Transfer Protocol

SNMP : Simple Network Management Protocol

SYN : Synchronize TCP : Transmission Control Protocol

UCL : Upper Control Limit

UDP : User Datagram Protocol

URG : Urgent

Introduction Générale

Introduction générale

Les systèmes et réseaux informatiques contiennent diverses formes de vulnérabilités, faisant de la sécurité un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet.

Pour faire face aux différents problèmes de sécurité informatique, différents mécanismes ont été mis en place pour prévenir tout sort d'attaque comme les pare-feux, antivirus, qui s'avèrent limités face au développement rapide des techniques de piratage, d'où la nécessité de mettre en place une politique de sécurité appropriées de détection et de prévention.

Pour chaque système informatique, telle politique de sécurité doit donc être définie pour garantir les propriétés de sécurité qui doivent être rendues par ce dernier. Cette politique s'exprime par des règles fixant trois objectifs distincts :

- Confidentialité des données : seuls les utilisateurs autorisés peuvent consulter une information donnée.
- Intégrité physique et logique : seuls les utilisateurs autorisés peuvent modifier une information ou une configuration matérielle donnée.
- Disponibilité du système : le système doit être capable de rendre le service prévu en un temps borné (c'est-à-dire le fait d'être prêt à l'utilisation).

A cet égard, une cyber-attaque est une atteinte à des systèmes informatiques qui viole ces objectives et poussée par différentes motivations. Elle cible différents serveurs informatiques, les ordinateurs, les équipements d'interconnexion, les équipements finaux, les téléphones mobiles et smartphones. Les cyber-attaques peuvent être divisées en deux types principaux : les attaques de dénies de service DOS (Denial Of Service) où le but est de désactiver le système cible et les attaques qui tentent d'obtenir l'accès aux données des victimes voire souvent l'obtention des privilèges d'administrateur et leur contrôle total.

D'autre part, les performances des mesures de divergence statistiques ont été approuvées lorsqu'il s'agit de la quantification de la différence entre les distributions et constituant donc, un outil très performant pour la maitrise d'un processus donnée. Parmi ces mesures on peut citer : Kullback-Leibler divergence (KLD), Hellinger Distance (HD) et CHI square (CHI). Ces mesures peuvent être combinées avec les cartes de contrôle monovariable comme la carte EWMA pour applications dans le domaine de détection.

En exploitant leur capacité de révéler la différence entre des ensembles de données, mis sous surveillance, pour déterminer les éventuelles anomalies intervenant dans un processus, en plein de fonctionnement. Précisément, nous proposons dans ce travail, une combinaison de ces mesures de divergences avec les cartes de contrôle pour la détection les différents type des attaques DOS.

Le manuscrit est organisé comme suit :

Dans **le premier chapitre**, nous introduisons le concept des attaques DOS. Nous décrivons leur principe de fonctionnement et les protocoles de la pile TCP/IP sur lesquels sont basées.

Dans **le deuxième chapitre,** nous présentons une description générale des mesures de divergence.

Dans **le troisième chapitre,** nous présentons une évaluation de performances des mesures KLD, HD et CHI dans la détection des attaques DOS. Une étude comparative entre ces trois mesures est effectuée en utilisant deux de base de données de trafic IP qui sont DARPA99 et MAWI.

CHAPITRE I

Les cyber-attaques de dénie de service dans les réseaux Ip

Chapitre I :

Les cyber-attaques de dénie de service dans les réseaux IP

I.1. Introduction :

L'architecture TCP/IP (Transmission Control Protocol/ Internet Protocol) fut crée au début des années 1970 [1]. Elle est constituées d'un ensemble de protocoles de communication qui sont utilisés dans le réseau Internet et qui permettent de gérer la circulation des données dans à travers des réseaux, éventuellement hétérogènes, tout en assurant la fiabilité des échanges de ces données. Cependant, les différents protocoles présentent de nombreuses vulnérabilités qui peuvent être exploitées par les hackers pour déclencher différents types d'attaques et touchent pratiquement tous les composants des réseaux déployés.

Après une brève description de l'architecture TCP/IP, nous présentons dans ce chapitre les différents attaques de dénie de service (DOS) ainsi que les protocoles auxquels sont liées.

I.2. La pile de protocole TCP/IP :

I.2.1. L'architecture TCP/IP :

L'architecture TCP/IP a été développée par la DARPA (Defense Advanced Research Project Agency – USA) [2]. TCP/IP est en fait une architecture réseau à quatre couches : couche accès réseau, Internet, couche transport et application. La figure I.1 illustre cette architecture comparée à l'architecture OSI (Open System Interconnection).

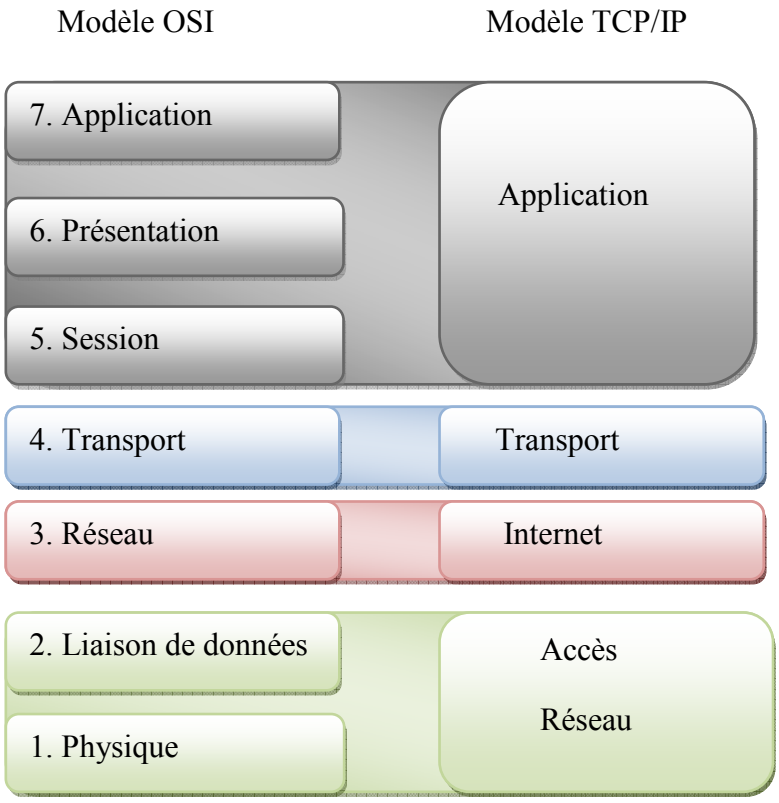

Figure I.1 :**L'architecture TCP/IP**

I.2.2. Description des couches protocolaires [1]:

- **Couche Accès réseau :** cette couche spécifie la forme des données selon l'acheminement dans un réseau quel qu'il soit, La fonction de la couche d'accès au réseau consiste à déplacer des bits (0 et 1) sur le support réseau.

- **Couche internet :** elle traite, achemine les paquets et connecte des réseaux indépendants pour transporter les paquets au-delà des limites du réseau, donc elle réalise l'interconnexion. Les protocoles de couche réseau sont l'IP et le protocole ICMP (Internet control Message Protocol).

- **Couche transport :** elle est responsable de la maintenance de bout en bout des communications sur le réseau. Les protocoles de transport incluent le TCP et le protocole UDP (User Datagram Protocol).

- **Couche application** : elle fournit aux applications un échange de données normalisé à travers un réseau pour communiquer. Ces protocoles incluent le HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), POP3 (Post Office Protocol 3),

SMTP (Simple Mail Transfer Protocol) et le protocole SNMP (Simple Network Management Protocol).

I.3. Cyber-attaques :

I.3.1. Définition :

Une cyber-attaque prend plusieurs définitions selon les pays, les organisations internationales, etc. Elle se définit comme une tentative illégale de nuire un système informatique ou l'information hébergée. Via l'Internet, elle peut être lancée depuis un ou plusieurs ordinateurs, et par une seule personne ou un groupe d'attaquants. Selon leur objectifs, les cyber-attaques peuvent être divisées en deux types principaux : les attaques DOS où le but est de désactiver le système cible et les attaques qui tentent d'obtenir l'accès aux données des victimes voire souvent l'obtention des privilèges d'administrateur et leur contrôle total [3].

I.3.2. Exemples de cyber-attaques :

Les cyber-attaques peuvent se manifester en plusieurs formes, on peut citer [3] [4] :

- Les attaques par déni de service (DoS) : pour empêcher certains services en ligne de fonctionner correctement et les rend temporairement indisponibles à partir d'une seule source. Lorsqu'une attaque DOS est déclenchée depuis plusieurs sources, on parle alors des attaques DOS distribuées (DDoS : Distributed Denial of Service).
- Les attaques de balayage : ces attaques visent à identifier tous les systèmes présents dans le but de dresser les futurs moyens de pénétration du réseau ou des systèmes qui le composent. Il existe pour cela différentes techniques de balayage des systèmes : Attaque par balayage ICMP, Attaque par balayage TCP…
- Les attaques par ingénierie sociale : consiste à envoyer des messages personnels pour voler des données sensibles aux professionnels.
- L'usurpation d'adresse IP ou Spoofing IP : c'est le remplacement d'une adresse IP par une autre a fin de masquer son accès ou d'usurper l'identité.
- L'attaque avec malwares : c'est un type de cyber-attaque dans le cadre duquel un logiciel malveillant exécute des activités sur le système informatique de la victime, généralement à son insu.

- L'attaque man in the middle : les attaquants parviennent à s'interposer secrètement entre l'utilisateur et un service Web auquel ils tentent d'accéder.

- Attaque d'écoute du trafic réseau : cette technique est généralement utilisée par les pirates pour capturer les mots de passe. Parmi ces attaques on trouve : attaque par sniffing et attaque de commutateurs.

I.3.3. Les attaques DOS/DDOS :

Les attaques DOS et leur forme distribuée DDOS visent à rendre indisponible un service, un système ou un réseau. Ces attaques s'appuient généralement sur une faiblesse d'implémentation, ou bogue, ou sur une faiblesse d'un protocole.

On distingue généralement deux types de dénis de service [4] :

I.3.3.1. DOS/DDOS par flooding :

Ce type d'attaques consiste à submerger la victime par volume important de trafic, afin qu'elle ne soit plus en mesure de répondre aux requêtes réelles.

De très nombreuses méthodes permettent de réaliser cette attaque :

- ✓ ***Le SYN Flood :*** en envoyant un nombre important de segments TCP avec le flag SYN armé, le serveur victime devient saturé.
- ✓ ***L'UDP Flood :*** le trafic réseau d'une machine est saturé lorsqu'il reçoit un très grand nombre de datagramme UDP.
- ✓ ***Le Smurfing et Ping flood:*** attaques basées sur le protocole ICMP.
- ✓ ***Les bombes e-mail :*** consistent à envoyer sur le réseau des mails trop volumineux.

I.3.3.2. DOS/DDOS par exploitation des protocoles :

Une attaque DOS/DDOS peut être réalisée par exploitation des failles d'un système. Dans ce cas, généralement, un seul message est suffisant pour crasher la victime. La littérature compte déjà un nombre important d'attaques, on peut citer par exemples :

- ✓ ***Le ping of death :*** utilise aussi une faiblesse de certaines piles TCP/IP lors de la gestion de messages ICMP trop volumineux.
- ✓ ***Teardop*** : est une attaque qui consiste à envoyer des paquets mal fragmentés à une machine cible. Causant un chevauchement lors du réassemblage.

- ✓ ***Land*** : cette attaque consiste à envoyer un paquet à chaque port ouvert contient les adresses source et destination du cible lui-même.

I.4. L'attaque SYN Flood :

I.4.1. Définition :

Une attaque SYN Flood est un type d'attaque de déni de service qui exploite une partie de la prise de contact à trois voies normale d'une connexion TCP, pour rendre le serveur ciblé insensible. Essentiellement, le délinquant envoie les demandes de connexion TCP plus rapidement que le serveur cible ne peut les traiter, ce qui entraîne sa saturation.

I.4.2. Le protocole TCP :

I.4.2.1. Présentation générale [1]:

TCP est un protocole de transport de bout en bout, orienté connexion, ce qui signifie qu'une connexion est établie et maintenue jusqu'à ce que les programmes d'application à chaque extrémité ont fini d'échanger des messages.

Pour les échanges de données exigeant une grande fiabilité, le protocole TCP est utilisé. Il met en œuvre la détection et la correction d'erreurs, gère le contrôle de flux et négocie les conditions du transfert des données entre les deux extrémités de la connexion.

I.4.2.2. Structure de segment [1] :

Un segment TCP a la structure générale suivante :

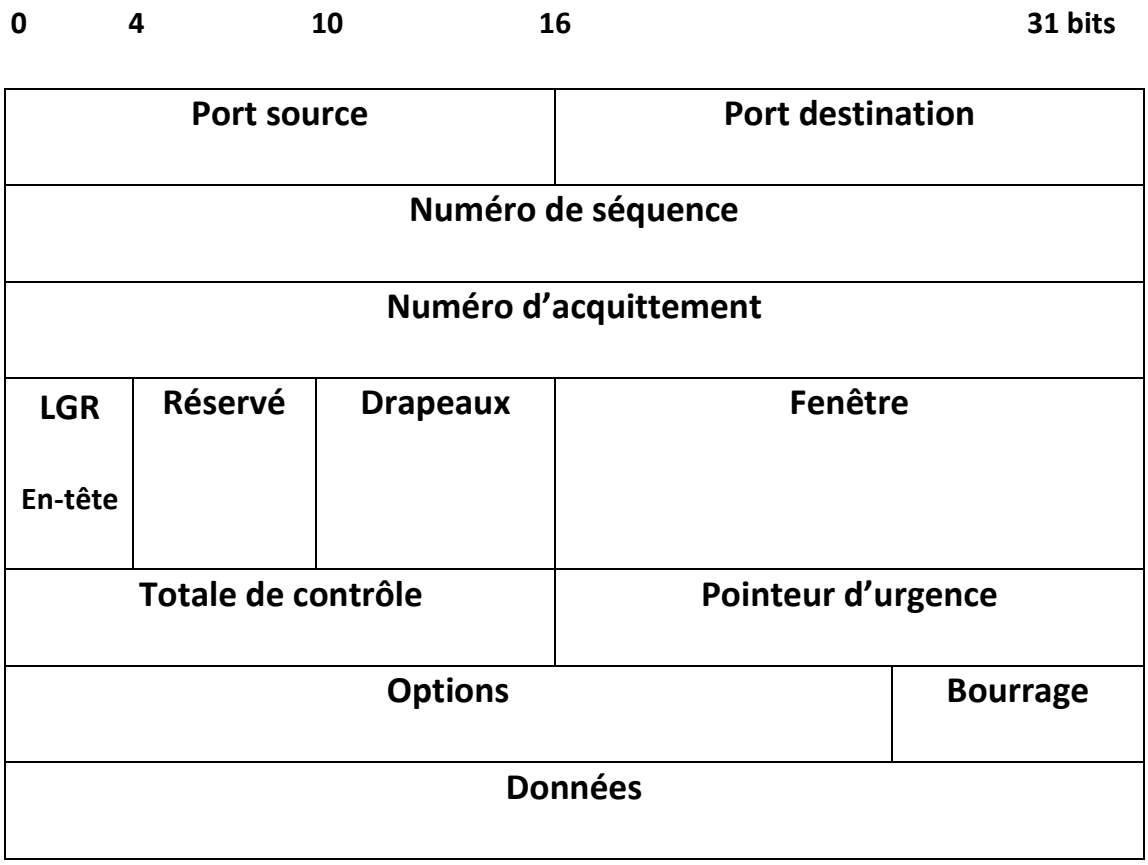

Figure I.2 : Format d'un segment TCP

1-Port source (16 bits) :

Il s'agit du numéro de port correspondant à l'application émettrice du paquet.

2-Port destination (16 bits) :

Numéro du port relatif à l'application en cours sur la machine de destination.

3-Numéro de séquence (32 bits) :

C'est le numéro de séquence du premier octet de données de ce segment.

4-Numéro d'acquittement (32 bits):

Lorsque le bit ACK est activé, ce segment sert comme accusé de réception. Il indique le numéro du prochain octet attendu incrémenté de la taille des données reçues, ensuite la destination à envoyer.

5-LGR en-tête (Longueur de l'en-tête ou offset (4 bits)):

Contient la longueur de l'en-tête du segment TCP qui doit toujours être un multiple de quatre octets.

6-Réservé (6 bits) :

Réservés pour une utilisation future, envoyé comme zéro.

7-Drapeaux (6 bits) :

Permettent de préciser les fonctions du segment, contient six indicateurs sont les suivantes :

- URG (Urgent):

  Lorsque ce bit est réglé à 1, le segment transporte des données à traiter en urgence et le pointeur de données urgentes est valide.

- ACK(Acknowledgement):

  Quand il est positionné à 1, cela indique que ce segment porte un accusé de réception.

- SYN (Synchronize):

  A 1, ce bit correspond à une demande d'établissement de connexion et synchronisation du numéro de séquence.

- RST(Reset) :

  Dans le cas d'une désynchronisation, il indique que le destinataire doit réinitialiser la connexion.

- PSH (Push):

  L'émetteur de ce segment utilise la fonctionnalité « TCP PUSH » demandant que les données de ce segment soient immédiatement données à l'application.

- FIN (Final):

  L'émetteur a atteint la fin de son flot de données, donc il demande que la connexion soit fermée.

8-fenêtre (16 bits):

Indique le nombre d'octets de données que l'émetteur de ce segment est prêt à accepter du récepteur à la fois la taille de la fenêtre de réception actuelle pour le périphérique envoyant ce segment.

9-Totale de contrôle (16 bits):

Il est calculé sur l'ensemble du datagramme TCP plus un "pseudo-en-tête", Il est utilisé pour protéger l'ensemble du segment TCP contre non seulement les erreurs de transmission, mais aussi les erreurs de livraison.

10-Pointeur d'urgence (16 bits):

Lorsque le bit URG est positionné, il pointe sur le dernier octet urgent du champ de données.

11-Options (taille variable):

Permet la négociation de la taille maximale des segments échangés.

12-Bourrage (taille variable):

Si le champ options n'est pas un multiple de 32 bits de longueur, des bits des zéros sont assez ajoutés pour occuper l'en-tête.

13-Données :

Ce sont les octets de données envoyés dans le segment.

I.4.2.3. Etablissement d'une connexion TCP [5]:

Avant qu'une session TCP soit ouverte et pour échanger les données, une connexion TCP est établie en trois étapes essentielles (three-way handshake) :

Etape N°1 : Envoi de SYN :

Le client effectue une ouverture active, demande l'établissement d'une session de communication en envoyant un message SYN au serveur qui attend le contact de client.

Etape N°2 : Envoi de SYN, ACK :

Le serveur reçoit le SYN et accuse la réception, il lui envoie un seul message SYN, ACK au client qui contient un accusé de réception (ACK) de SYN du client avec sa propre requête de synchronisation (SYN), et le client attend la réception de l'acquittement de message envoyé.

Etape N°3 : Etabli :

Le client reçoit le message émis par le serveur et lui répond par un accusé de réception, maintenant l'établissement de connexion est fait.

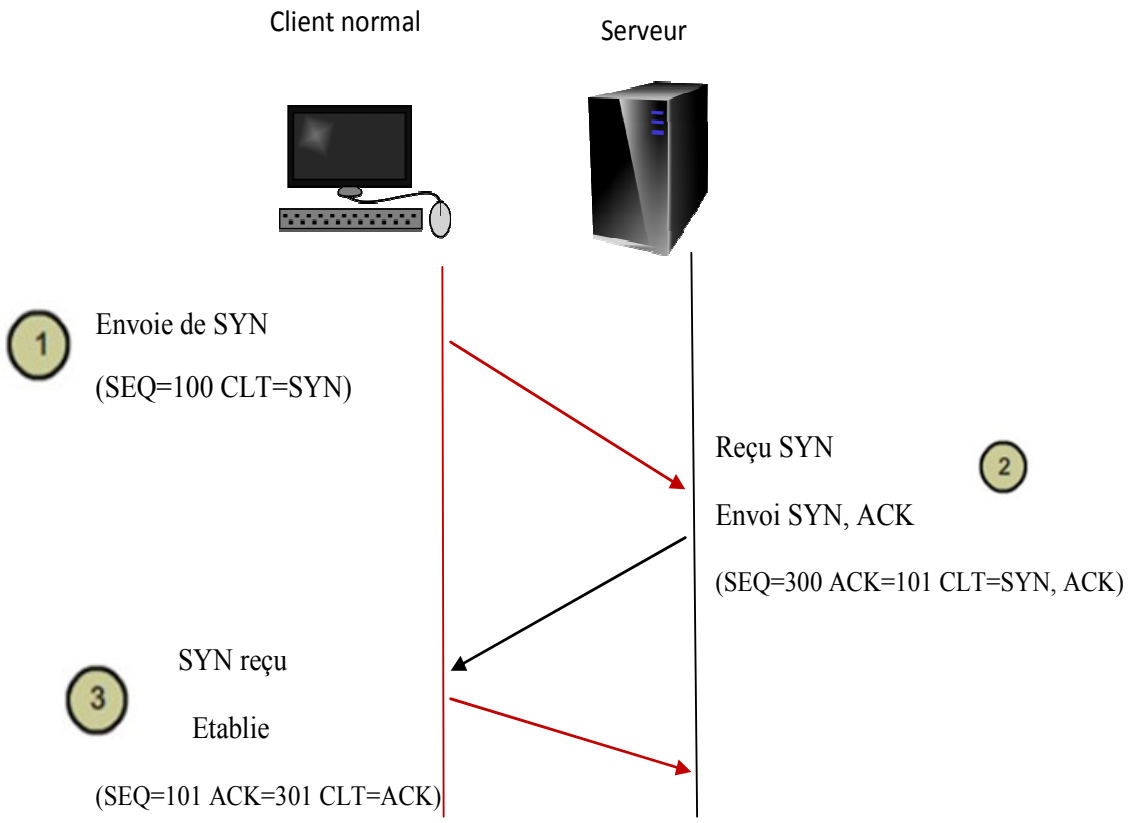

Figure I.3 : Etablissement de connexion TCP

I.4.3. Principe de fonctionnement de l'attaque SYN flood [6]:

Dans une attaque SYN flood, l'attaquant envoie des segments SYN répétés à chaque port sur le serveur ciblé, souvent en utilisant une fausse adresse IP. Le serveur, inconscient de l'attaque, reçoit plusieurs demandes apparemment légitimes pour établir une communication. Il répond à chaque tentative avec un segment SYN-ACK de chaque port ouvert.

L'utilisateur malveillant n'envoie pas le ACK attendu ou, si l'adresse IP est usurpée, ne reçoit jamais le SYN-ACK en premier lieu. Dans les deux cas, le serveur attaqué attendra l'accusé de réception de son paquet SYN-ACK pendant un certain temps. Pendant ce temps, le serveur ne peut pas fermer la connexion en envoyant un segment RST et la connexion reste ouverte.

Avant que la connexion puisse expirer, un autre segment SYN arrivera. Cela laisse un nombre de plus en plus grand de connexions semi-ouvertes, les attaques SYN flood sont également appelées attaques «semi-ouvertes».

Au fur et à mesure que les tables de débordement de connexion du serveur se remplissent, le service offert aux clients légitimes sera refusé et le serveur risque même de ne pas fonctionner correctement ou de tomber en panne.

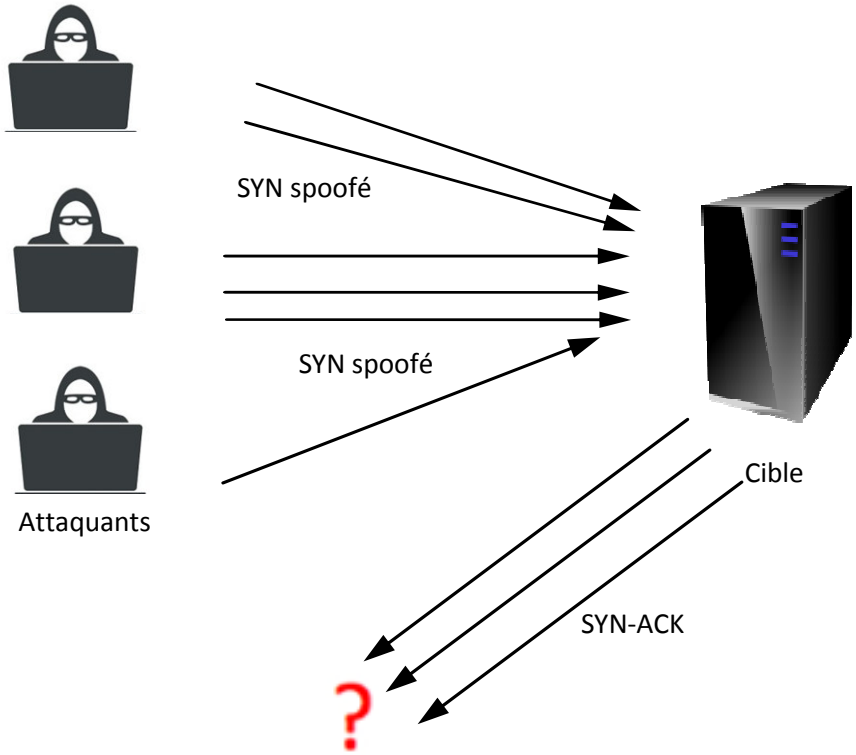

Figure I.4 : Principe de l'attaque SYN Flood DDOS

I.5. L'attaque UDP flood *[4][7][8]*:

I.5.1. Le protocole UDP :

I.5.1.1. Présentation générale :

Le protocole UDP (User Datagram Protocol), ou le protocole de datagramme utilisateur. Ce protocole est non orienté connexion de la couche transport du modèle TCP/IP. Ce protocole est très simple, étant donné qu'il ne fournit pas de contrôle d'erreurs. Ce protocole permet la transmission de données entre deux entités avec une grande facilité, chacune d'entre elles possédant une adresse IP propre et un numéro de port.

Cependant, ces mêmes propriétés rendent également UDP plus vulnérable aux abus. En l'absence d'une négociation initiale, pour établir une connexion valide, un volume élevé de

trafic peut être envoyé sur les canaux UDP vers n'importe quel hôte, sans protection intégrée pour limiter le débit de l'inondation DOS UDP.

I.5.1.2.Structure d'un datagramme :

Le datagramme UDP est encapsulé dans un paquet IP. Il comporte un en-tête suivi des données proprement dites à transporter.

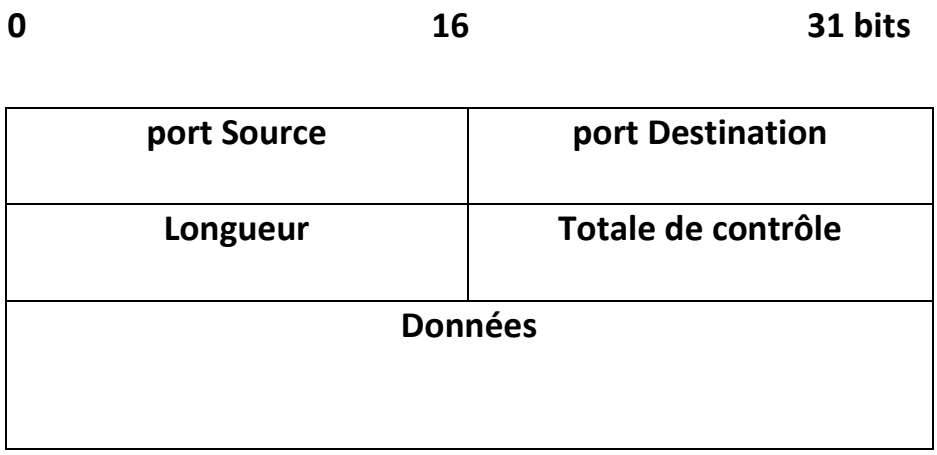

Figure I.5 : Structure d'un datagramme UDP

- ***Port Source*** (16 bits): il indique depuis quel port le paquet a été envoyé. Il s'agit du numéro de port correspondant à l'application émettrice du paquet. Ce champ représente une adresse de réponse pour le destinataire.

- ***Port Destination*** (16 bits): il indique à quel port le paquet doit être envoyé. Il contient le port correspondant à l'application de la machine à laquelle on s'adresse. Les ports source et destination ont évidemment la même signification que pour TCP.

- ***Longueur*** (16 bits) : il indique la longueur totale (exprimée en octets) du datagramme UDP (en-tête et données). La longueur minimale est donc de 8 octets (taille de l'en-tête).

- ***Total de contrôle*** (16 bits)***:*** celle-ci permet de s'assurer de l'intégrité du datagramme reçu quand elle est différente de zéro. Elle est calculée sur l'ensemble de l'en-tête UDP et des données, mais aussi sur un pseudo en-tête (extrait de l'en-tête IP).

I.5.2. Principe de fonctionnement de l'attaque UDP flood :

UDP flood est un type d'attaque DOS dans lequel l'attaquant inonde des ports aléatoires sur l'hôte ciblé avec des paquets IP contenant des datagrammes UDP. L'hôte destinataire vérifie les applications associées à ces datagrammes et, sans en trouver aucune, renvoie un message «Destination inaccessible». A mesure que de plus en plus de paquets UDP sont reçus et traités, le système devient submergé et ne répond plus aux autres clients.

Dans le cadre d'une attaque par inondation UDP, l'attaquant peut également usurper l'adresse IP des paquets, à la fois pour s'assurer que les paquets ICMP renvoyés n'atteignent pas leur hôte et pour rendre l'attaque anonyme.

L'utilisation de plusieurs machines permettra de classer cette attaque dans la catégorie de menace DDoS. Avec cette attaque, le but du délinquant est de maîtriser les pare-feu et d'autres composants des infrastructures de réseau.

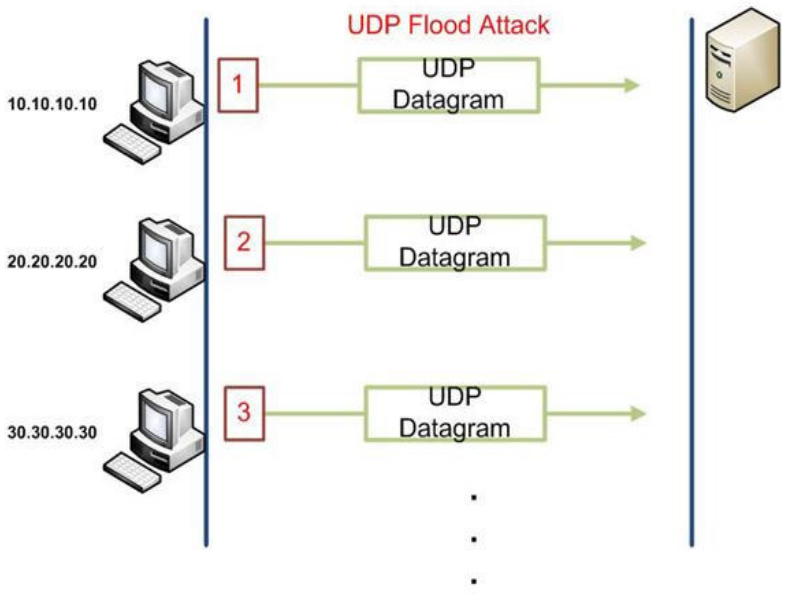

Figure I.6: Principe de fonctionnement de l'attaque UDP flood

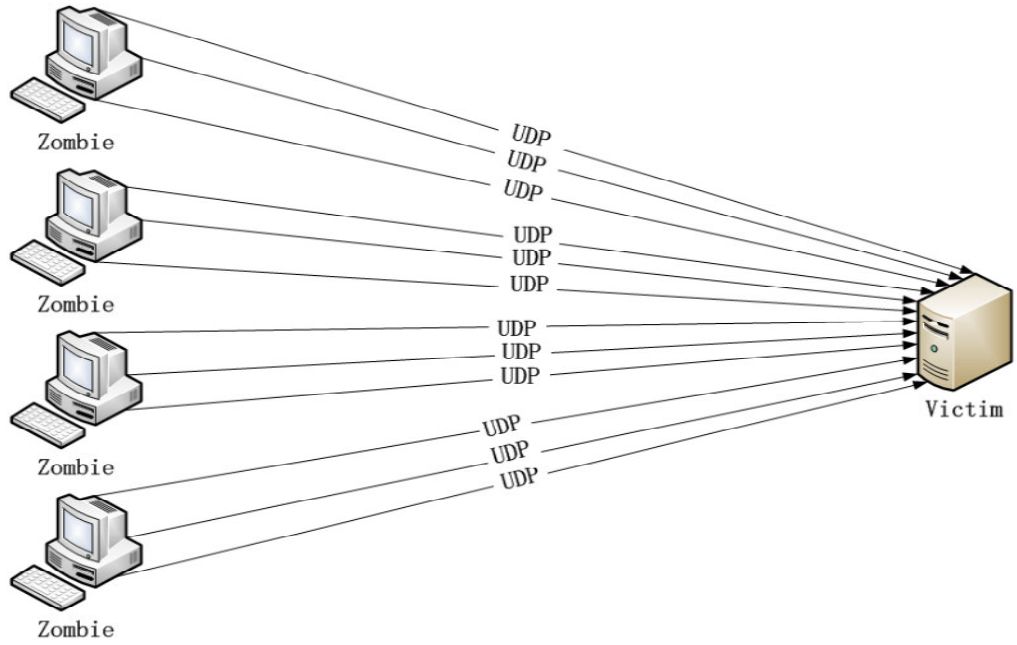

Figure I.7:Principe de fonctionnement de l'attaque UDP DDOS

I.6. L'attaque Ping flood [2][8]:

Cette attaque consiste à envoyer un flux maximal de ping vers une cible.

I.6.1. Le protocole ICMP :

I.6.1.1. Présentation du protocole ICMP :

Le protocole ICMP est utilisé par les routeurs et les hôtes pour s'échanger des informations de contrôle du réseau. Du point de vue des couches, ICMP est un protocole distinct situé au-dessus de IP et utilisant IP pour le transport des messages. En pratique, ICMP est une partie intégrante d'IP et tous les modules IP doivent prendre en charge le protocole ICMP.

I.6.1.2.Structure de message :

Les messages ICMP sont véhiculés à l'intérieur des paquets IP et donc routés comme n'importe quel datagramme.

Un message ICMP a un en-tête de 8 octets et une section de données de taille variable. Bien que le format général de l'en-tête soit différent pour chaque message type, les 4 premiers octets sont communs à tous.

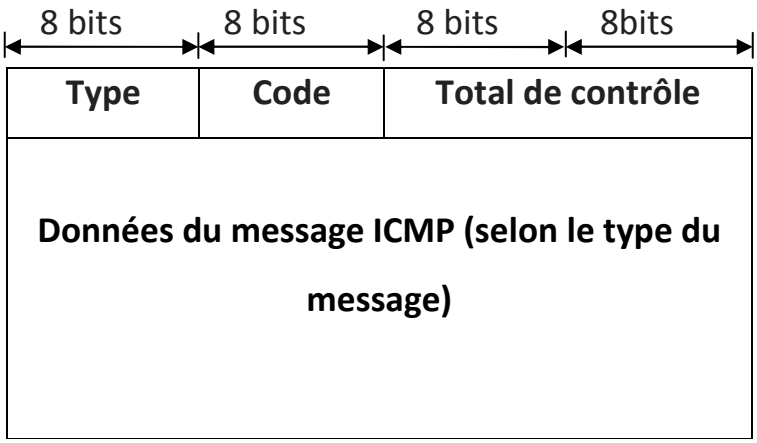

Figure I.8 : Structure d'un message ICMP

Les informations contenues dans un message ICMP sont :

- **Type (**8 bits) : type de message ICMP envoyé. Plus 20 types de messages ICMP différents. Il y a deux grandes catégories de message dans ce champ :

  - message généré à la suite d'une erreur.

  - message d'administration.

- **Code** (8 bits) : inclut des informations supplémentaires spécifiques au type de message.

- **Total de contrôle (**16 bits) : champ de contrôle qui permet de détecter et corriger les erreurs de transmission.

- **Données du message ICMP:** correspond aux données du paquet ICMP, parfois précédées de bits de bourrage (pour que l'en-tête ICMP ait une taille fixe).

I.6.1.3. Description du message ICMP :

Le message ICMP utilise ses champs Type et Code pour dire quelle est l'origine de l'erreur, à savoir est-ce que la machine destination est inaccessible, est-ce que le protocole utilisé est mauvais, etc. On peut classer les messages selon la valeur du champ Type.

Les messages sont divisés en deux grandes catégories: les messages de rapport d'erreur et les messages de requête. Les messages de rapport d'erreur signalent les problèmes qu'un routeur ou un hôte (destination) peut rencontrer lors du traitement d'un paquet IP. Les messages de requête, qui se produisent par paires, aident un hôte ou un gestionnaire de réseau

à obtenir des informations spécifiques auprès d'un routeur ou d'un autre hôte. De plus, les hôtes peuvent découvrir et connaître les routeurs de leur réseau et peuvent aider un nœud à rediriger ses messages.

Type	Nom	Code
0	**Réponse par écho**	**0 – Aucun code**
3	**Destination inaccessible**	**0 – Réseau inaccessible** **1 – Hôte inaccessible** **2 – Protocole inaccessible** **3 – Port inaccessible** **4 – Fragmentation requise et bit *Don't fragment* activé** **5 – Echec du routage source** **6 – Réseau destinataire inconnu** **7 – Hôte destinataire inconnu** **8 – Hôte de la source isolé** **9 – La communication avec le réseau destinataire est interdite par l'administrateur** **10 – La communication avec l'hôte destinataire est interdite par l'administrateur** **11 – Réseau destinataire inaccessible pour ce type de service** **12 – Hôte destinataire inaccessible pour ce type de service** **13 – Communication interdite par l'administrateur** **14 – Violation de priorité de l'hôte**
8	**Requête par écho**	**0 – Aucun code**
11	**Temps dépassé**	**0 – Time to Live dépassé en transit** **1 – Temps de rassemblement des fragments dépassé**
30	**Utilitaire de routage Traceroute**	**0 – Aucun code**

Tableau I.1 : Exemples de messages ICMP

I.6.1.4.L'utilitaire PING : requête et réponse par écho ICMP

L'utilitaire PING (Packet INternet Groper) permet de tester l'accessibilité d'un système et d'évaluer le temps allé et retour entre le système source et le système cible.

Une machine envoie un message ICMP "echo request" pour tester si son destinataire est accessible. N'importe quelle machine qui reçoit une telle requête doit formuler un message ICMP "echo reply" en retour.

Le principe du Ping étant, à la base, de valider la présence d'un Hôte IP. Pour cela, l'application Ping utilisera la séquence 8-0 afin d'émettre une demande d'écho. Les données reçues dans un message d'écho doivent être remises dans la réponse. Ainsi, si le message de retour correspond à l'émission, on en déduit que l'Hôte est présent. De plus, on peut en déduire d'autres services, tel que le temps de réponse, la taille paquet maximum la durée de vie, fragmentation et etc…

L'identificateur et le numéro de séquence peuvent être utilisés par l'émetteur du message d'écho afin d'associer facilement l'écho et sa réponse. Par exemple, l'identificateur peut être utilisé comme l'est un port pour TCP ou UDP, identifiant ainsi une session. Et le numéro de séquence peut être incrémenté pour chaque message d'écho envoyé. L'hôte de destination respectera ces deux valeurs pour le retour.

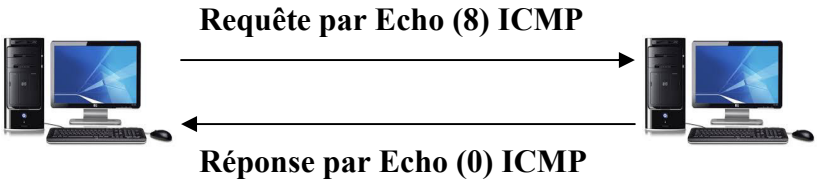

Figure I.9 : Principe de la commande PING

I.6.1.5.: Principe de l'attaque PING flood :

Une demande ICMP nécessite certaines ressources du serveur pour traiter chaque demande et envoyer une réponse. La demande nécessite également une bande passante sur le message entrant (demande d'écho) et la réponse sortante (réponse d'écho). L'attaque Ping flood vise à surcharger la capacité du périphérique ciblé à répondre au nombre élevé de demandes et / ou à surcharger la connexion réseau. Si de nombreux périphériques d'un réseau de zombies ciblent la même propriété Internet ou le même composant d'infrastructure que les demandes ICMP, le trafic d'attaque augmente considérablement, ce qui peut entraîner une interruption de l'activité réseau normale.

La forme DDoS d'un déluge Ping (ICMP) peut être décomposée en 2 étapes répétitives:

L'attaquant envoie de nombreux paquets de requêtes d'écho ICMP au serveur ciblé utilisant plusieurs périphériques.

Le serveur ciblé envoie ensuite un paquet de réponse d'écho ICMP à l'adresse IP de chaque dispositif demandeur en réponse

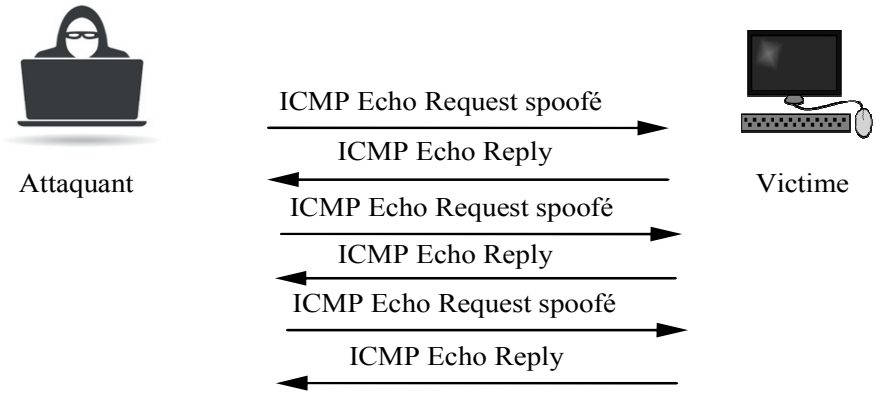

Figure I.10 : Principe de l'attaque PING flood

I.7. L'attaque Smurf [9]:

I.7.1. Définition :

Smurf est une attaque par déni de service distribuée (DDoS) sur la couche réseau, nommée d'après le programme malveillant DDoS smurf qui permet son exécution.

Ces attaques ressemblent un peu aux inondations de ping, car les deux sont effectués en envoyant une série de paquets de requêtes ICMP Echo.

Contrairement au flot de ping classique, il s'agit d'un vecteur d'attaque par amplification qui augmente son potentiel de dommages en exploitant les caractéristiques des réseaux de diffusion.

I.7.2. Principe de fonctionnement de l'attaque Smurf :

La vérification de l'accessibilité d'un ordinateur spécifié se fait en envoyant une demande ICMP Echo (ping) et cela déclenche une réponse ICMP automatique, en passant par un réseau de diffusion IP, la requête ping est envoyée à chaque hôte, invitant chacun des destinataires à répondre.

Dans le cas d'une attaque Smurf, les logiciels malveillants Smurf permettent de générer une fausse requête Echo contenant une adresse IP source usurpée correspond à l'adresse du serveur cible.

- La demande est envoyée à un réseau de diffusion IP intermédiaire.
- La demande est transmise à tous les hôtes du réseau.
- Chaque hôte envoie une réponse ICMP à l'adresse source usurpée.
- Avec suffisamment de réponses ICMP transférées, le serveur cible est arrêté.

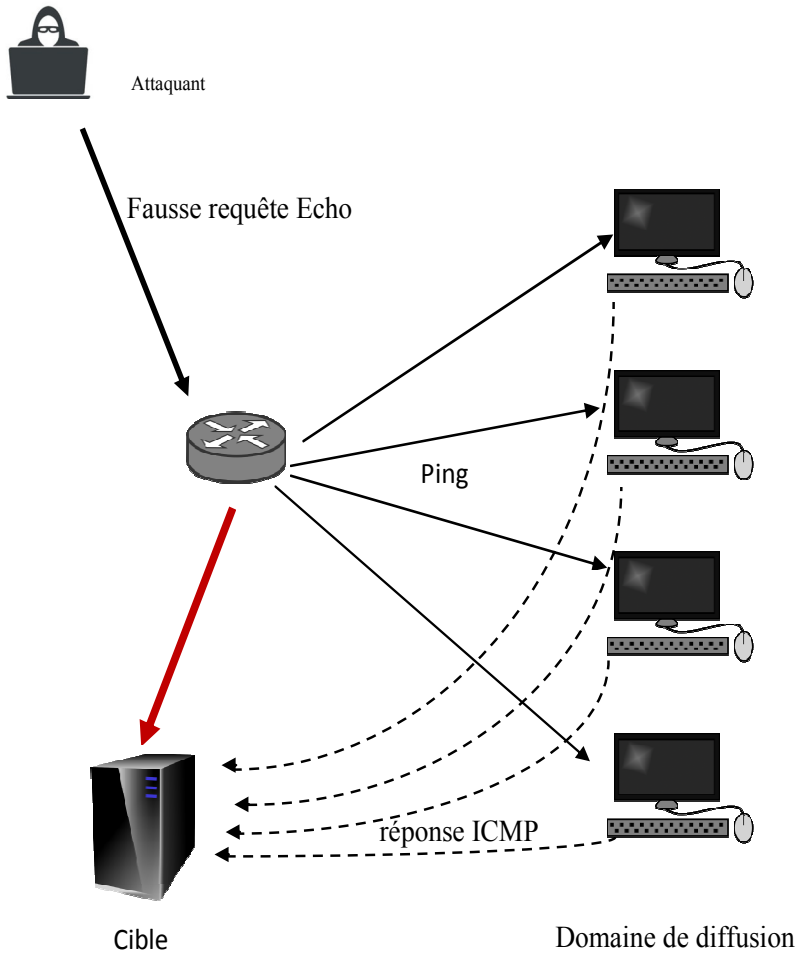

Figure I.11: Principe de l'attaque Smurf

I.8. Conclusion :

Nous avons présenté dans ce chapitre les attaques de dénies de service DOS et DDOS, les protocoles sur lesquels sont basées et leur principe de fonctionnement. Mieux s'en protéger et atteindre niveau approprié de sécurité devient alors une tache primordiale. Dans ce contexte

les approches statistiques devient de plus en plus attractives et prend l'intention des chercheurs et des experts du domaine. En effet, dans le chapitre II, nous introduisons les mesures de divergence statistiques qui peuvent être utilisées pour la détection de différentes attaques DOS et DDOS.

CHAPITRE II

Les mesures de divergence

Chapitre II :

Les mesures de divergence

II.1. Introduction :

Les mesures de divergence sont des méthodes statistiques utilisées pour mesurer la dissimilarité entre les distributions de probabilités. Ces mesures peuvent être combinées avec les cartes de contrôle pour applications dans le domaine de détection. Dans ce chapitre nous introduisons les mesures de divergence et des cartes de contrôle les plus connues.

II.2. Définition des mesures de divergence :

Les mesures de divergence sont des fonctions qui visent de mesurer la différence d'une distribution par rapport à une autre [10]. La figure II.1 montre deux lois probabilités p(x) et q(x). Une mesure de divergence D de P par rapport à Q quantifie la différence entre eux. Elle est définit pour toute fonction convexe f telle que $f(1) = 0$, par :

$$Df(P \parallel Q) = \int_{\Omega} f\left(\frac{dP}{dQ}\right) dQ \quad \text{(II.1)}$$

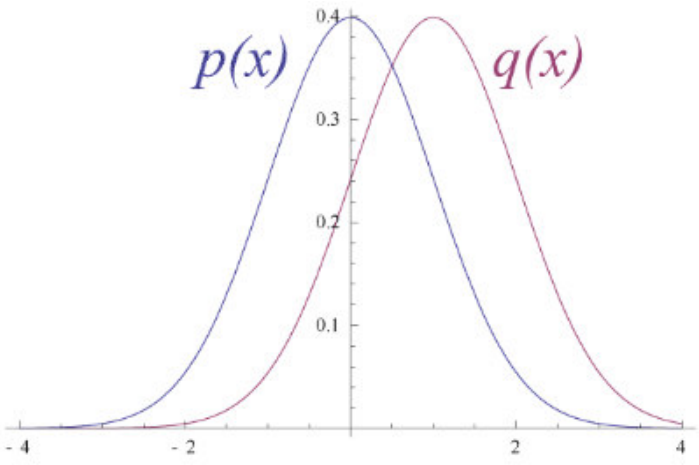

Figure II.1 : Divergence entre deux lois de probabilité

II.2.1. Différents types de mesures de divergence :

Les choix possibles de la fonction *f* permettent d'obtenir plusieurs types de mesures de divergence. Dans les paragraphes suivants nous décrivons celles les plus connues, à savoir les divergences de Kullback Leibler, de Hellinger, CHI square et de Jensen Shanon.

II.2.1.1. Divergence de Kullback-Leibler:

En théorie de l'information et de probabilité, la divergence de Kullback Liebler ou l'entropie relative doit son nom à Solomon Kullback et Richard Leibler [11]. Selon la NSA, c'est durant les années 50, alors qu'ils travaillaient pour cette agence, que Kullback et Leibler ont inventé cette mesure.

La Divergence Kullback-Leibler (KLD) est une équation fondamentale de la théorie de l'information et est utilisée pour calculer la divergence entre deux ensembles de valeurs de probabilité [12]:

$P = (p_0, p_1, \ldots, p_{k-1})$ et $Q = (q_0, q_1, \ldots, q_{k-1})$ avec $p_i \geq 0, q_i \geq 0$ et :

$$\sum_{i=0}^{K-1} p_i = \sum_{i=0}^{K-1} q_i = 1 \qquad \text{(II.2)}$$

KLD entre P et Q est défini par [12]:

$$KLD(P \parallel Q) = \sum_x P(x) \log \frac{P(x)}{Q(x)} \qquad \text{(II.3)}$$

C'est une mesure non symétrique. Plus précisément, la KLD de P par rapport à Q est, généralement, différente de la KLD de Q par rapport à P , c à d :

$$KLD(P \parallel Q) \neq KLD(Q \parallel P) \qquad \text{(II.4)}$$

KLD est égale à zéro si les deux distributions correspondent exactement et devient importante si les deux distributions sont très différentes. La figure II.2 illustre graphiquement ce comportement [13].

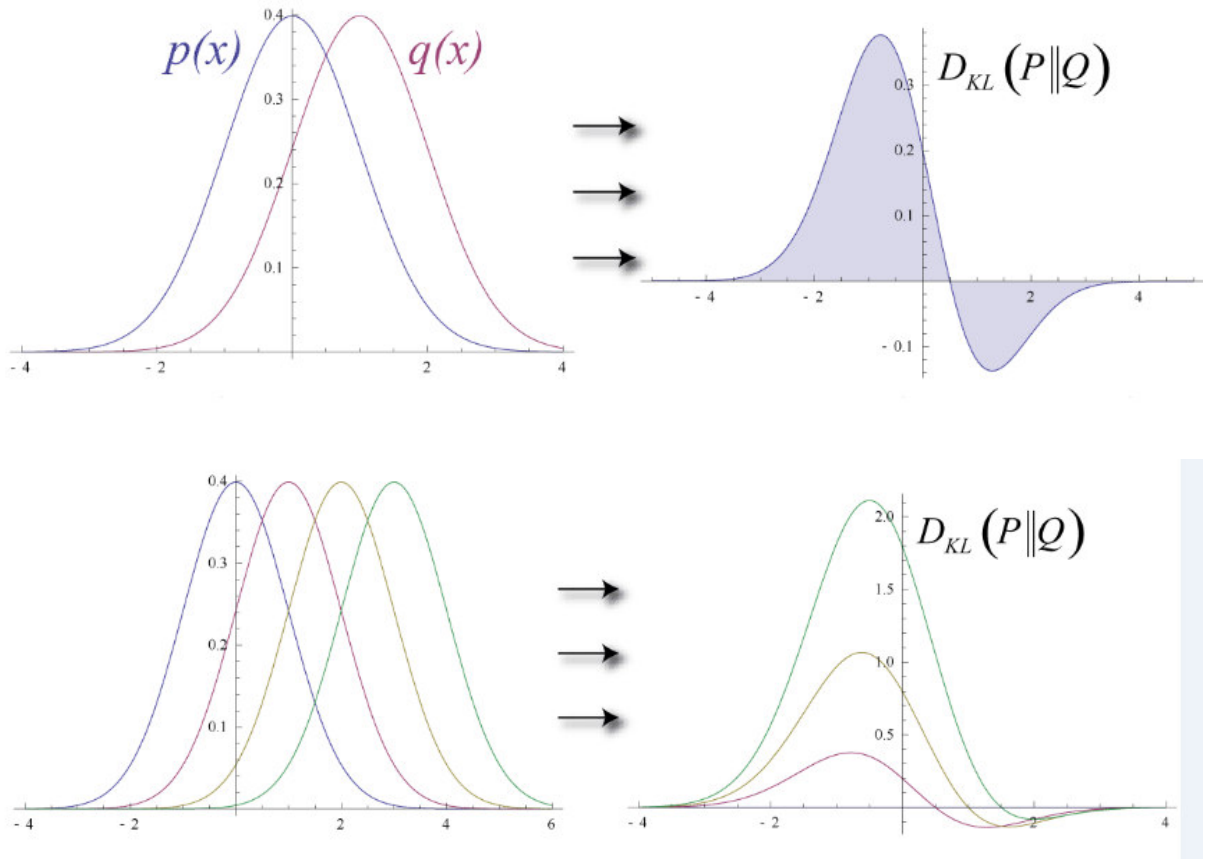

Figure II.2 : La divergence Kullback-Leibler (KLD)

II.2.1.2. La distance de Hellinger :

Hellinger Distance est utilisé pour calculer la divergence entre deux ensembles de valeurs de probabilité. Pour deux distributions de probabilité discrètes :

$P = (p_0, p_1, \ldots, p_{k-1})$ et $Q = (q_0, q_1, \ldots, q_{k-1})$ avec $p_i \geq 0, q_i \geq 0$

HD entre la distribution actuelle P et la distribution de référence Q est définie comme suit [14] :

$$\sum_{i=0}^{K-1} p_i = \sum_{i=0}^{K-1} q_i = 1 \qquad \text{(II.5)}$$

$$\mathrm{HD}(P, Q) = \frac{1}{2} \sum_{i=0}^{K-1} \left(\sqrt{p_i} - \sqrt{q_i}\right)^2 \qquad \text{(II.6)}$$

Où HD vérifier l'inégalité : 0 ≤ HD (P,Q) ≤ 1, et HD (P,Q) = 0 si et seulement si P=Q.

HD est une distance symétrique (HD (P, Q) = HD (Q, P)).

II.2.1.3. CHI square :

CHI-square divergence entre deux distributions de probabilité P=$(p_0, p_1,..., p_{k-1})$ et $Q = (q_0, q_1,..., q_{k-1})$ avec $p_i \geq 0$, $q_i \geq 0$ est définit par [15] :

$$X^2(P\|Q) = \sum_{i=0}^{K-1} \frac{(p_i - q_i)^2}{q_i} \qquad \text{(II.7)}$$

Avec $p_i \geq 0, q_i \geq 0$ et :

$$\sum_{i=0}^{K-1} p_i = \sum_{i=0}^{K-1} q_i = 1 \qquad \text{(II.8)}$$

Où Q est la distribution de probabilité d'avant et P la distribution actuelle. La divergence de X^2 peut prendre des valeurs de zéro jusqu'à l'infini.

X^2 (P‖Q) = 0 si et seulement si P=Q et sa valeur augmente si les deux distributions deviennent dissemblables, jusqu'à l'infini lorsque les deux distributions sont indépendante. Il est important de noter que la divergence de X^2 est asymétrique.

La divergence de X^2entre deux distributions similaires de probabilité P et Q doit être proche de zéro, et elle doit avoir un pic lorsqu'un changement de distribution de probabilité se produit.

II.2.1.4. Divergence de Jensen-shannon :

Jensen-Shannon Divergencev (JSD) est utilisée pour calculer la divergence entre deux ensembles de valeurs de probabilité P=$(p_0, p_1,..., p_{k-1})$ et $Q = (q_0, q_1,..., q_{k-1})$ avec $p_i \geq 0$, $q_i \geq 0$ et :

$$\sum_{i=0}^{K-1} p_i = \sum_{i=0}^{K-1} q_i = 1 \qquad \text{(II.9)}$$

JSD est une version lissée de *Kullback-Leibler Divergence* [16] et est définie comme suit :

$$JSD(P,Q) = \frac{1}{2} KL(P,M) + \frac{1}{2} KL(Q,M) \qquad \text{(II.10)}$$

Avec M est la distribution moyenne de P et Q.

$$M = \frac{P+Q}{2} \qquad \text{(II.11)}$$

D'où JSD peut être exprimée sous la forme suivante [16] :

$$JSD(P\|Q) = \frac{1}{2}\left[\sum_{i=0}^{K-1} p_{\mathrm{i}} \ln\left(\frac{2p_{\mathrm{i}}}{p_{\mathrm{i}} + q_{\mathrm{i}}}\right) + \sum_{i=0}^{K-1} q_{\mathrm{i}} \ln\left(\frac{2q_{\mathrm{i}}}{p_{\mathrm{i}} + q_{\mathrm{i}}}\right)\right] \quad \text{(II.12)}$$

JSD=0 si et seulement si P et Q sont identiques ($p_i = q_i$), et JSD > 0 lorsque P≠Q.

Comme nous cherchons à détecter les anomalies grâce à la détection des déviations du trafic normal, JSD détermine la divergence entre deux distributions de probabilité P et Q, qui désignent les distributions avant et âpres l'attaque. JSD entre P et Q doit être proche de zéro dans le cas de trafic normal, avec une grande déviation (une pointe) lorsque les distributions subissent un changement.

II.3. Les cartes de contrôle mono variable [17]:

II.3.1. Définition :

Une carte de contrôle est un graphique, document, ou bien un tableau de contrôle qui permet de visualiser graphiquement les variations sur lequel sont reportées les valeurs (une série d'échantillons, de mesures ou de données) d'une ou suite de variables aléatoires.

Elle se compose généralement d'une ligne centrée CL (Central Line) qui représente la moyenne globale et des deux limites de contrôle au-dessous et en dessus la ligne centrale qui représentent respectivement les limites inférieures LCL (Low Control Limit) et les limites supérieures UCL (Upper Control Limit), elles encadrent la dispersion des données.

Les graphiques de contrôle comparent ces données aux limites supérieures et inférieures pour voir si elle correspond aux niveaux de variation attendus, spécifiques, prévisibles et normaux. Toutefois, la variation tombe en dehors des limites, ou s'il a une série de points non naturels, le processus est considéré comme hors de contrôle. Les cartes de contrôles sont utilisées dans des plusieurs domaines comme : l'informatique, l'industrie, la géophysique, la biologie, l'économie…

Les cartes de contrôles mono variables les plus connues sont : Shewhart, CUSUM (Cumulative Sum) et EWMA (Exponentially Weighted Moving Average).

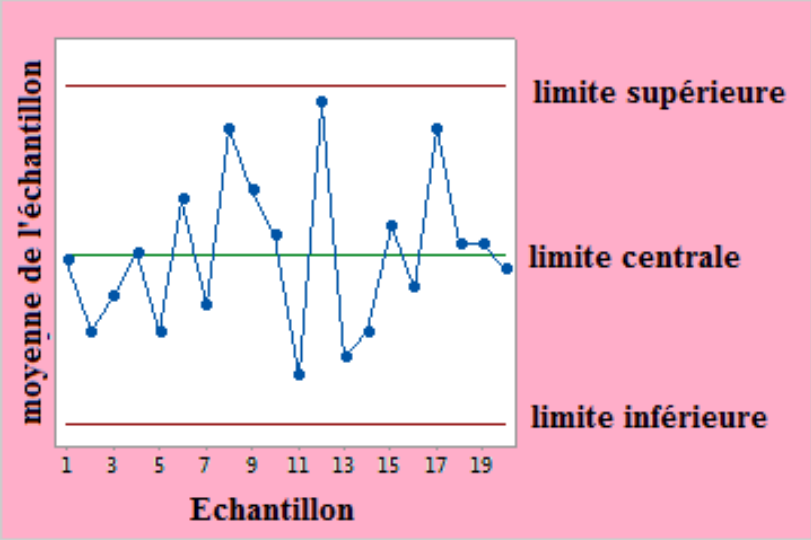

Figure II.3 : Principe des cartes de contrôle

II.3.2. La carte Shewhart :

La cartes de contrôle de Shewhart du nom de W. A. Shewhart a été proposée en 1931, elle est la carte de contrôle la plus populaire à cause de sa simplicité.

Il s'agit d'un outil graphique standard largement utilisé dans le contrôle de qualité statistique. Tendance mondiale est assez simple : on extrait des échantillons d'une certaine taille dans un processus de production en cours. On produit alors des cartes linéaires de la dispersion de ces échantillons, et on constate leur proximité par rapport aux spécifications cibles (les limites UCL, LCL). Si une tendance émerge ou si des échantillons sortent des limites prédéfinies, le processus est déclaré hors-contrôle et l'opérateur doit faire une action pour trouver la cause du problème.

On a les échantillons X_i (i =1 ….n) d'un processus normal N (μ,σ^2), les expressions II.13, II.14 et II.15 montrent les limites de contrôles utilisées par la carte Shewhart.

$$CL = \mu_0 \qquad \text{(II.13)}$$

$$UCL = \mu_0 + 3\sigma \qquad \text{(II.14)}$$

$$LCL = \mu_0 - 3\sigma \qquad \text{(II.15)}$$

Où :

μ_0 : la moyenne.

σ : l'écart type.

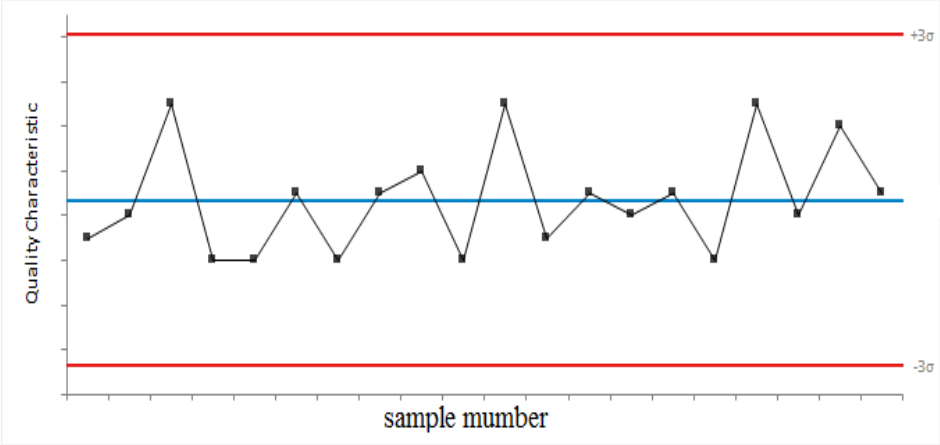

Figure II.4 : Exemple de la carte Shewhart

II.3.3. La carte EWMA :

La carte EWMA (Exponentially Weighted Moving Average) accumule, avec une pondération exponentielle, les échantillons prélevés, en donnant les poids élevés aux échantillons plus récents. Les échantillons x_i suivent une distribution normale de moyenne μ0 et d'écart type σ.

EWMA est définie par la formule suivante :

$$Z_i = \lambda x_i + (1-\lambda) Z_{i-1} \qquad (\text{II.16})$$

Pour montrer que Z_i est une moyenne pondérée, (II.16) peut être reformulée comme suit :

$$Z_i = \lambda \sum_{j=0}^{i-1} (1-\lambda)^j x_{i-j} + (1-\lambda)^i Z_0 \qquad (\text{II.17})$$

Les limites de contrôles pour EWMA sont calculées par les équations (II.18), (II.19) et (II.20) :

$$UCL = \mu_0 + L\sigma \sqrt{\left(\frac{\lambda}{2-\lambda}\right)[1-(1-\lambda)^{2i}]} \qquad (II.18)$$

$$CL = \mu_0 \qquad (II.19)$$

$$LCL = \mu_0 - L\sigma\sqrt{\left(\frac{\lambda}{2-\lambda}\right)[1-(1-\lambda)^{2i}]} \qquad (II.20)$$

Avec:

x_i: Valeur d'i^{ieme} échantillon

Z_{i-1} : EWMA de l'échantillon précédent

Z_0: Valeur initial de l'EWMA, généralement, choisie égale à μ_0 .

$\lambda\ (0 < \lambda \leq 1)$: Constante d'ajustement comprise entre 0 et 1. Elle représente le poids apporté aux résultats antérieurs.

- **Plus λ est proche de 0 :** le poids $\lambda(1-\lambda)^j$ diminue lentement, et plus on tient compte du passé. Cela implique que l'on identifiera plus facilement les faibles dérives. Par contre, les dérives brutales et les déréglages importants, seront moins bien détectés.
- **Plus λ est proche de 1 :** $\lambda(1-\lambda)^j$ diminue rapidement, et moins on tient compte du passé. Cela implique que l'on aura une meilleure réactivité pour identifier les déréglages brusques mais à contraire, on détectera moins bien les faibles variations.
- **Si λ = 1 :** EWMA sera équivalente à la carte de contrôle classique Shewhart.

L : La largeur des limites de contrôle.

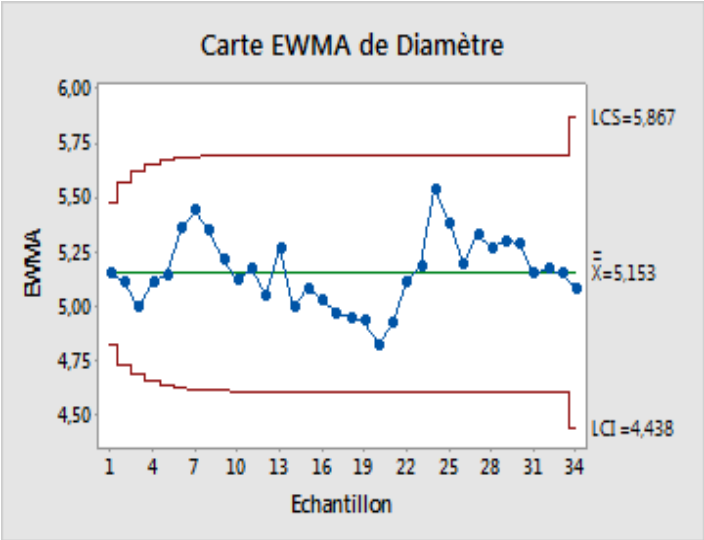

Figure II.5: Exemple de la carte EWMA

II.3.4. Combinaison entre les mesures de divergence et la carte EWMA :

Nous avons vu que les mesures de divergence sont utilisées pour calculer la différence entre deux distributions de probabilités. Ces mesures tendent vers zéro si les distributions sont similaires. Dans le cas contraire, c à d si les distributions comparées sont différentes, ces mesures prennent des valeurs importantes. Ce comportement est très intéressant dans le domaine de détection d'anomalie.

Etant donnée qu'une anomalie peut être caractérisée par une déviation importante de l'état du système par rapport à l'état de référence ou normal. Par analogie, la quantification de cette déviation via les mesures de divergences permet de révéler les éventuelles anomalies présentent dans un système donné. Pour distinguer les valeurs normales de ces mesures des valeurs anormales, on fixe les limites de détection par les cartes de contrôle. Nous présentons ici une combinaison des mesures KLD, HD et CHI avec la carte EWMA.

II.3.4.1. KLD-EWMA:

L'équation II.16 devient :

$$Z_{ikld} = \lambda d_{kld} + (1-\lambda) Z_{i-1kld} \qquad (\text{II.21})$$

Et les limites de contrôles pour KLD-EWMA sont calculées parles équations (II.22), (II.23) et (II.24) :

$$UCL = \mu_{0kld} + L\sigma_{kld}\sqrt{\left(\frac{\lambda}{2-\lambda}\right)[1-(1-\lambda)^{2i}]} \qquad (II.22)$$

$$CL = \mu_{0kld} \qquad (II.23)$$

$$LCL = \mu_{0kld} - L\sigma_{kld}\sqrt{\left(\frac{\lambda}{2-\lambda}\right)[1-(1-\lambda)^{2i}]} \qquad (II.24)$$

II.3.4.2. HD-EWMA:

L'équation II.16 devient :

$$Z_{iHD} = \lambda d_{HD} + (1-\lambda) Z_{i-1HD} \qquad (\text{II.25})$$

Et les limites de contrôles pour KLD-EWMA sont calculées par les équations (II.26), (II.27) et (II.28) :

$$UCL = \mu_{0HD} + L\sigma_{HD}\sqrt{\left(\frac{\lambda}{2-\lambda}\right)[1-(1-\lambda)^{2i}]} \qquad (II.26)$$

$$CL = \mu_{0HD} \qquad (II.27)$$

$$LCL = \mu_{0HD} - L\sigma_{HD}\sqrt{\left(\frac{\lambda}{2-\lambda}\right)[1-(1-\lambda)^{2i}]} \qquad (II.28)$$

II.3.4.3. CHI-EWMA:

L'équation II.16 devient :

$$Z_{iCHI} = \lambda d_{CHI} + (1-\lambda)Z_{i-1CHI} \qquad (II.29)$$

Et les limites de contrôles pour KLD-EWMA sont calculées par les équations (II.30), (II.31) et (II.32) :

$$UCL = \mu_{0CHI} + L\sigma_{CHI}\sqrt{\left(\frac{\lambda}{2-\lambda}\right)[1-(1-\lambda)^{2i}]} \qquad (II.30)$$

$$CL = \mu_{0CHI} \qquad (II.31)$$

$$LCL = \mu_{0CHI} - L\sigma_{CHI}\sqrt{\left(\frac{\lambda}{2-\lambda}\right)[1-(1-\lambda)^{2i}]} \qquad (II.32)$$

II.4. Conclusion :

Dans ce chapitre nous avons vu que les mesures de divergence peuvent être utilisées pour révéler les éventuelles anomalies dans le fonctionnement d'un système. Ainsi pour automatiser la détection de ces anomalies, les cartes de contrôles peuvent être utilisées comme règles de décision. Etant données que les cyber-attaques, en particuliers, les attaques de dénies de service DOS et DDOS peuvent être considères comme des anomalies dans le trafic réseau, dans le chapitre III, nous essayons de détecter les différents types de ces attaque en utilisation

une procédure de détection basées sur les mesures de divergence KLH, HD et CHI et la carte de contrôle EWMA.

CHAPITRE III

Simulations et interprétations

Chapitre III

Simulations et interprétations

III.1. Introduction :

A travers la simulation sous Matlab, nous investiguons, dans ce chapitre, l'utilité des mesures de divergence pour la détection des cyber-attaques dans un réseau IP.

Pour cela, nous avons utilisé les mesures de divergence détaillées dans chapitre deux, en particulier KLD, HD et CHI. Pour automatiser la tache de détection, ces mesures seront combinées avec le contrôle monovariable EWMA pour la détection des attaques DOS de types : TCP SYN flood, UDP flood, Smurf et Ping flood en utilisant le trafic réseau fournit par les bases de données DARPA99 et MAWI.

III.2. Détection des attaques DOS et DDOS par les mesures de divergence :

Pour détecter les attaques DOS comme TCP SYN flood, UDP flood, Smurf et Ping flood par les mesures de divergence KLD, HD et CHI square, nous avons mis en place la procédure suivante :

- Les données d'apprentissage des bases de données du trafic fournit par DARPA99 et MAWI c à d le trafic normal en termes de messages SYN, datagram UDP, messages ICMP ECHO REQUEST et ECHO REPLY sont utilisés pour calculer les limites de contrôle CL/UCL/LCL en utilisant la carte EWMA.
- On calcul les statistiques de la mesure de divergence combinées avec la carte EWMA pour les données de test qui contiennent les différents types des attaques.
- Ces statistiques sont en suite comparées avec les limites de contrôle.
- Si ces statistiques, du trafic testé, sont comprises entre limites de contrôles UCL/LCL alors le trafic est considéré comme normal.

- Sinon, si ces statistiques dépassent l'une des limites de contrôle, le trafic, dans ce cas, a un comportement anormal, une alarme de détection d'attaques DOS est déclenchée et fournit ses caractéristiques (type, victime et la date d'apparition).

  La figure III.1 récapitule la procédure de détection décrit ci-dessus.

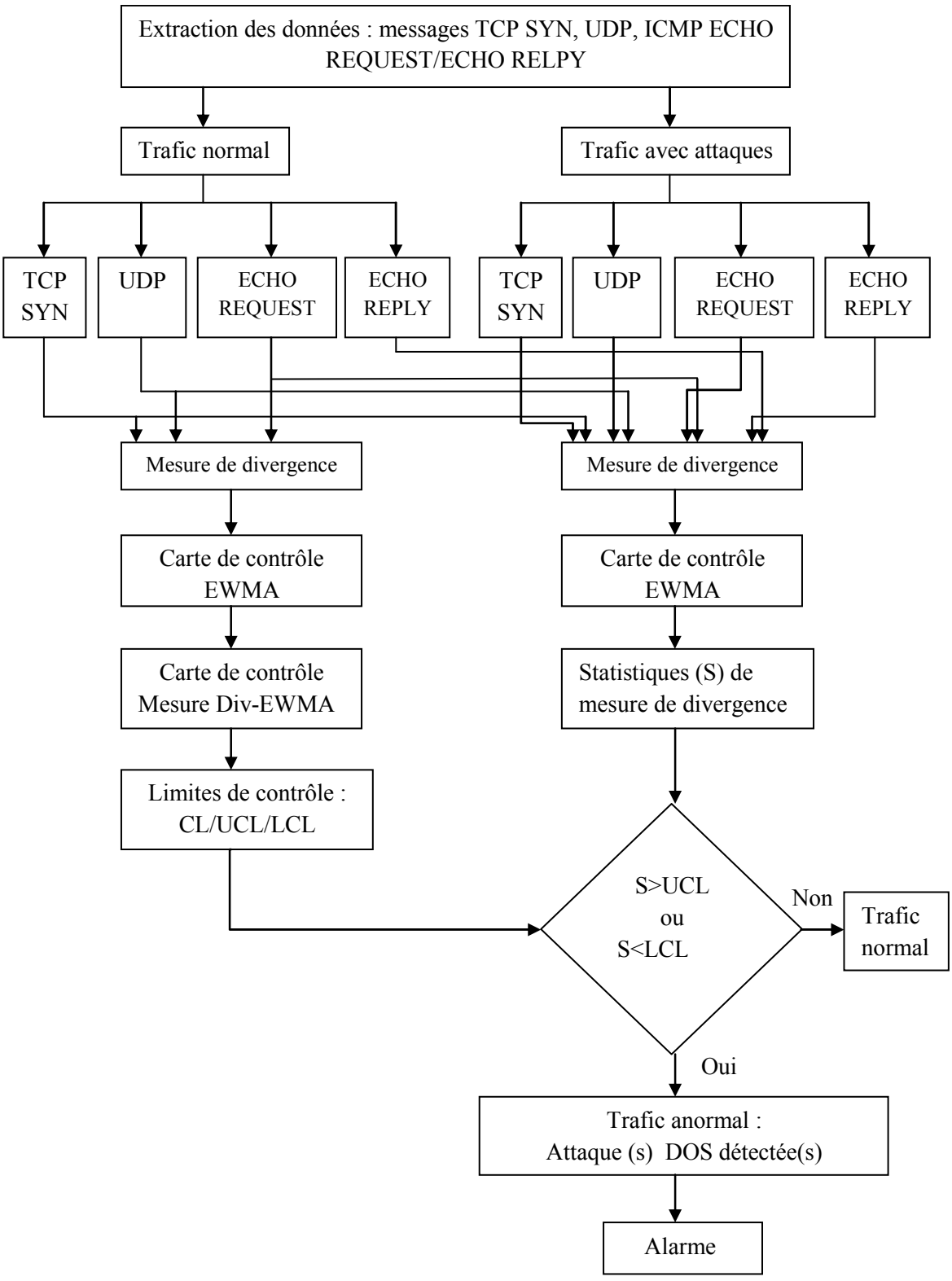

Figure III.1 : Procédure générale de détection des attaques DOS/DDOS par les mesures de divergence (KLD, HD et CHI square)

III.3. Présentation des bases de données de trafics réseau IP :

Pour appliquer les mesures de divergence citée ci-dessus et faire une comparaison au niveau des performances de détection des différents types d'attaques DOS/DDOS, nous allons utiliser des traces de trafic IP de deux bases de données publiquement disponibles qui sont DARPA99 et MAWI.

III.3.1.La base DARPA99 [18]:

III.3.1.1. Le réseau DARPA99 :

La figure ci-dessous présente la topologie du réseau utilisé dans nos simulations. Il s'agit du réseau mis en place par Lincoln Laboratory à Massachusetts Institute of Technology (MIT) sous le sponsor de Defense Advanced Research Projects Agency (DARPA) et Air Force Research Laboratory (AFRL), et similaire au réseau d'une base militaire aérienne.

Ce réseau était utilisé pour générer les traces de trafic (et par suite toute une base de données) facilitant aux développeurs et des chercheurs, dans le domaine de la sécurité informatique, la tâche d'évaluation de leurs solutions et systèmes proposés pour la détection des attaques dans les réseaux informatiques.

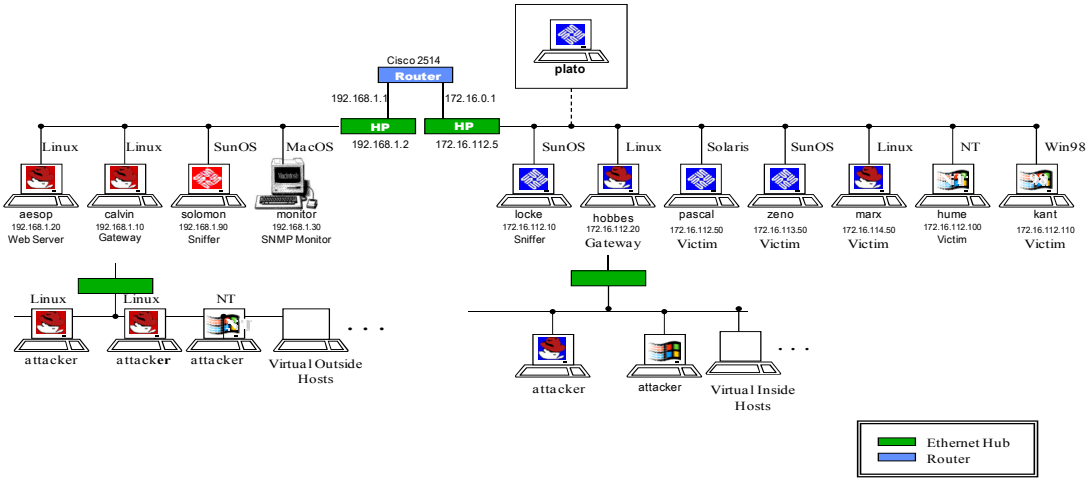

Figure III.2 : La topologie de réseau utilisé par DARPA 99

III.3.1.2. La base de trafic DARPA99 :

En utilisant le trafic capturé à partir du réseau la figure III. 2, les auteurs du projet ont construit la base donnée DARPA99.

La base DARPA99 s'inscrit parmi les bases de données les plus importantes et les plus utilisées pour l'évaluation des IDS (Intrusion Détection System). Elle mit à la disposition, des chercheurs, plus de 8Goctets de trafic réseau (entrant et sortant) sous forme de fichiers

compressés tcpdump, pour une période de 5 semaines (5 jours par semaine, et autour de 22h par jour).

Le trafic collecté est divisé en deux catégories : les données d'apprentissage (training data) et les données de test (test data). Les données d'apprentissage contiennent 3 semaines (semaines 1, 2 et 3) de trafic normal sans attaques. Tandis que, les données de test consistent du trafic des semaines 4 et 5, et introduisent de nombreuses attaques.

III.3.2.La base MAWI [19]:

La base de données MAWI (Measure and Analyse over Internet WIDE) est un trafic Internet réel fourni par le référentiel de trafic du MAWI Working Group. Dans cette base de données, le trafic est capturé à partir de nombreuses liaisons transpacifiques (c'est-à-dire, sampleponit-A, sampleponit-C, sampleponit-D et sampleponit-F) entre le réseau Japonais WIDE et les Etats-Unis. L'échantillon point-F, qui est le plus utilisé, fournit une trace quotidienne de 15mn. Nous avons utilisé la trace TCPDUMP du 1er janvier 2010; de 14h00 à 14h15mn.

III.3.3.Extraction des données : les messages TCP SYN, Datagram UDP et les messages ICMP ECHO REQUEST et ECHO REPLY :

Nous avons vu que les attaques DOS/DDOS de type SYN flood, UDP flood, Smurf et Ping flood sont basées sur l'envoi massif des segments SYN, des datagram UDP, des messages ICMP ECHO REQUEST et ECHO REPLY, respectivement. En effet, la première étape dans le processus de la détection de telles attaques, est l'extraction et l'isolation de ces messages.

Les bases DARPA99 et MAWI fournit des traces de trafic brut, avec la totalité des échanges (différents protocoles, différents messages,…) pendant la période d'étude. Pour faire l'extraction des différents messages, un prétraitement de ces traces est nécessaire.

A partir des fichiers TCPdump des bases données, nous avons utilisé le logiciel Wireshark [20] pour filtrer les messages différents messages. Les fichiers résultants contiennent seulement ces messages. Ensuite, nous avons utilisé MySql et Java pour traiter ces fichiers. A l'issue de ce traitement, nous avons obtenu des données sous formats supportés par les utilitaires de calcul mathématique comme Excel et Matlab.

III.4. Résultats et interprétation :

En se basant sur la procédure de détection détaillée précédemment, nous avons réalisé de nombreuses simulations, sous Matlab. Les figures ci-dessous illustrent quelques résultats.

III.4.1. DARPA99 :

III.4.1.1. Détection des attaques SYN flood:

Pour évaluer les performances des mesures de divergence, combinées avec la carte EWMA, nous les utilisons dans cette étape pour la détection des attaques SYN flood du trafic du deuxième jour de la semaine 5 du trafic DARPA99.

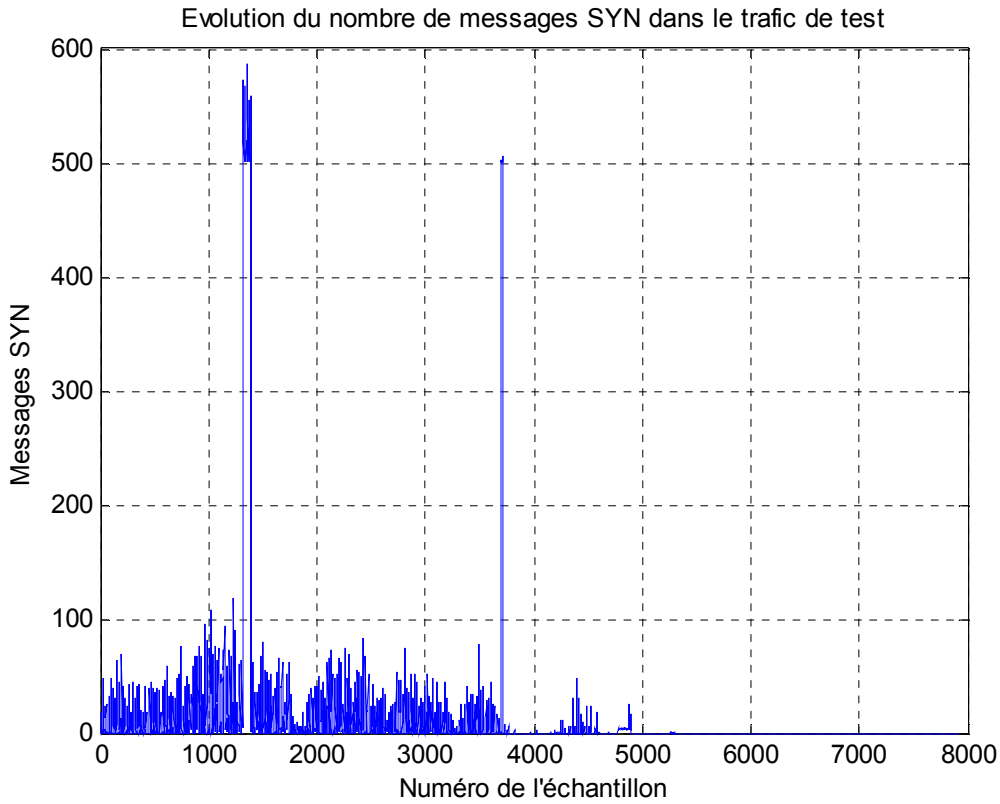

Figure III.3 : Evolution du nombre des messages SYN en fonction du numéro de l'échantillon (semaine 5 jour 2)

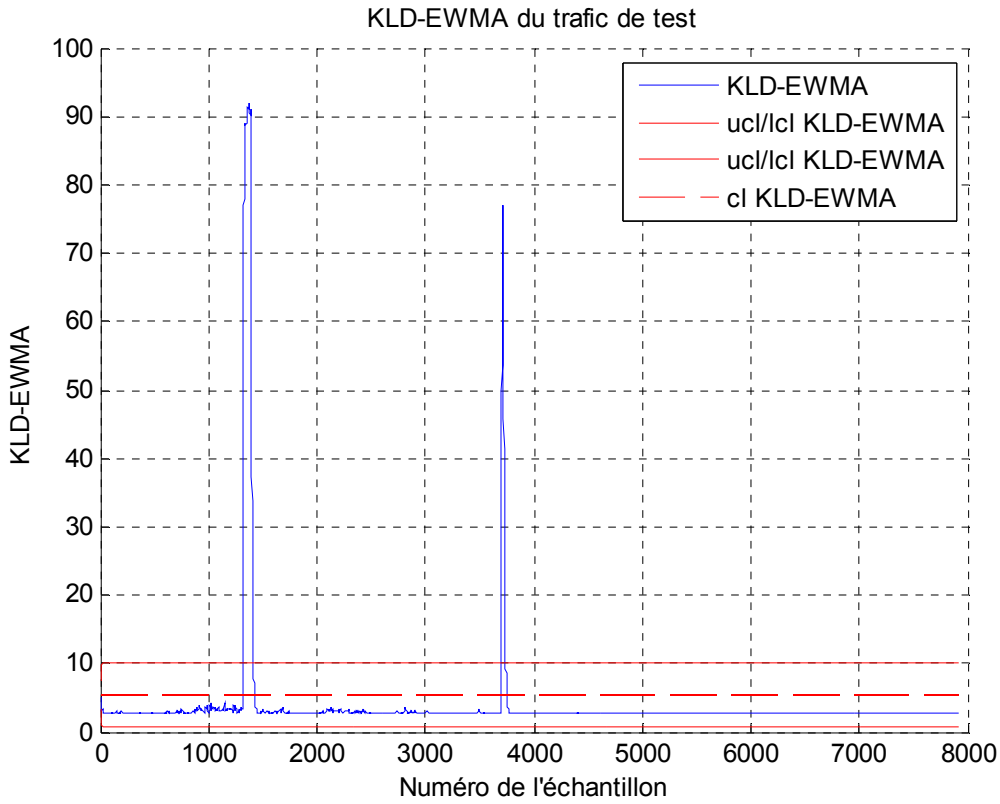

Figure III.4: Résultat de détection des attaques SYN flood par KLD-EWMA

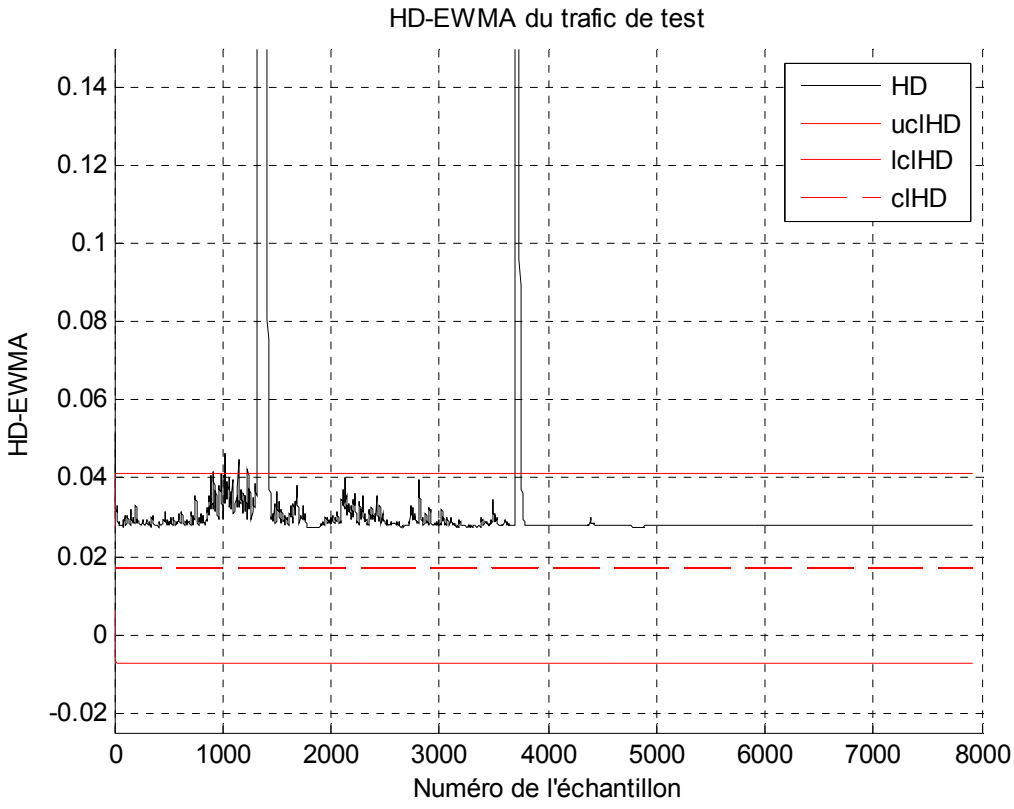

Figure III.5: Résultat de détection des attaques SYN flood par HD-EWMA

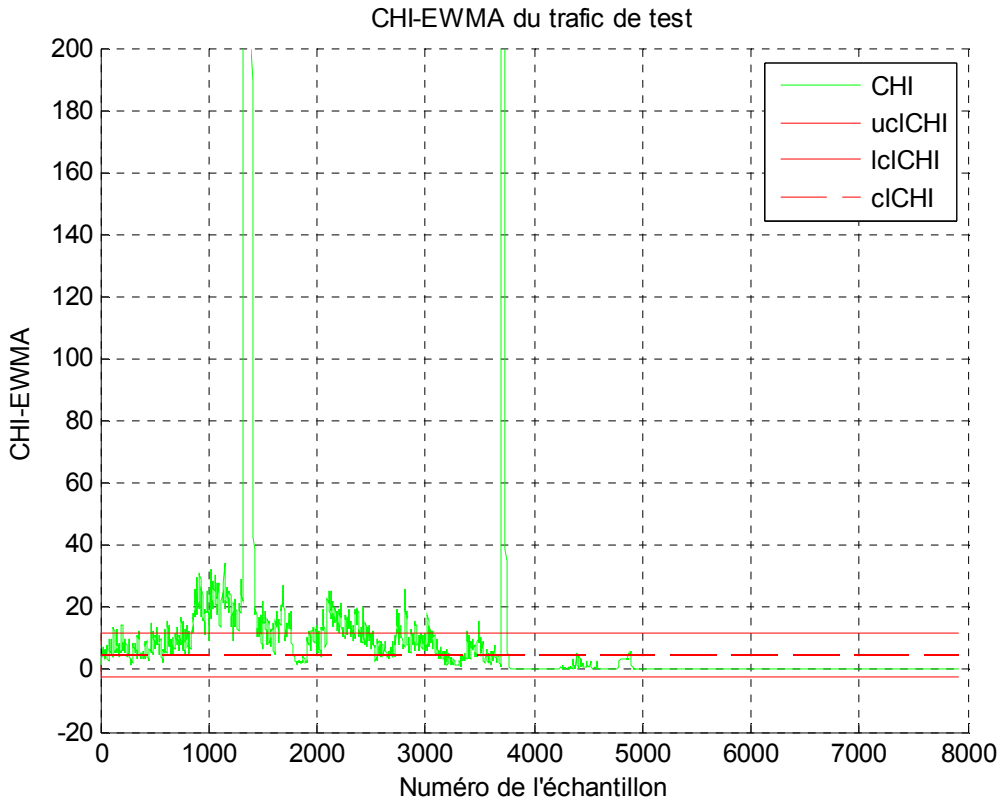

Figure III.6: Résultat de détection des attaques SYN flood par CHI-EWMA

III.4.1.2. Détection des attaques UDP flood :

Dans cette étape, nous évaluons la capacité des mesures de divergence à détecter les attaques DOS /DDOS de type UDP flood. Le trafic de test est celui fournit par le jour 1 de la semaine 5 du la base DARPA99.

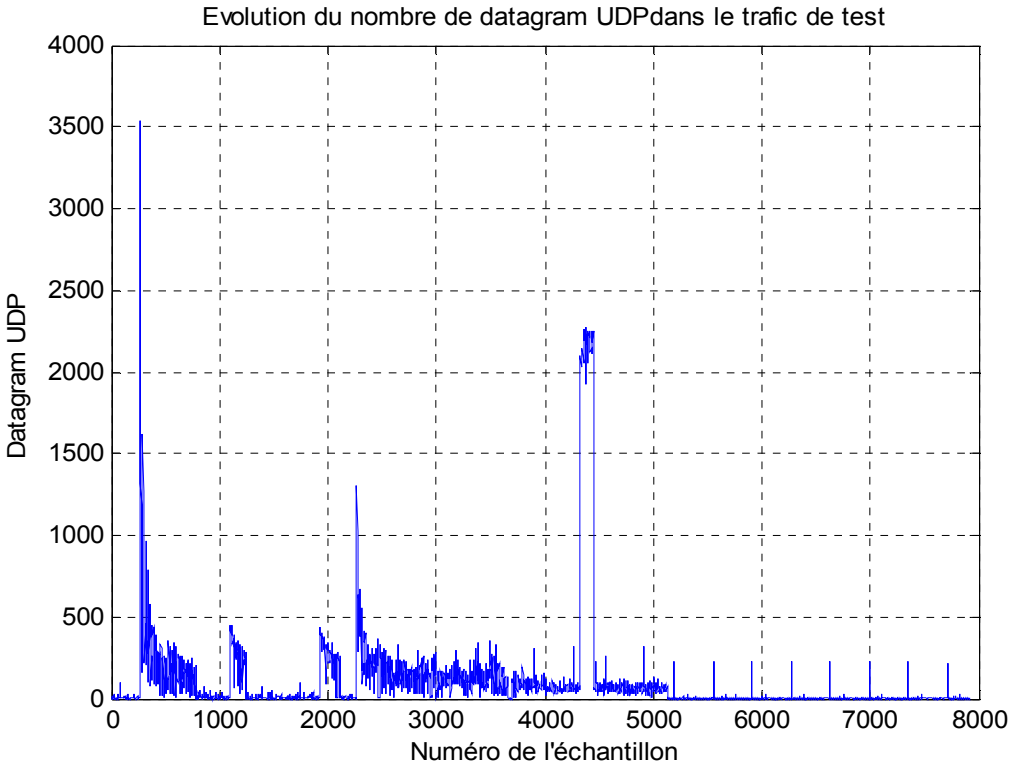

Figure III.7 : Evolution du nombre de datagramme UDP en fonction du numéro de l'échantillon (semaine 5 jour 1)

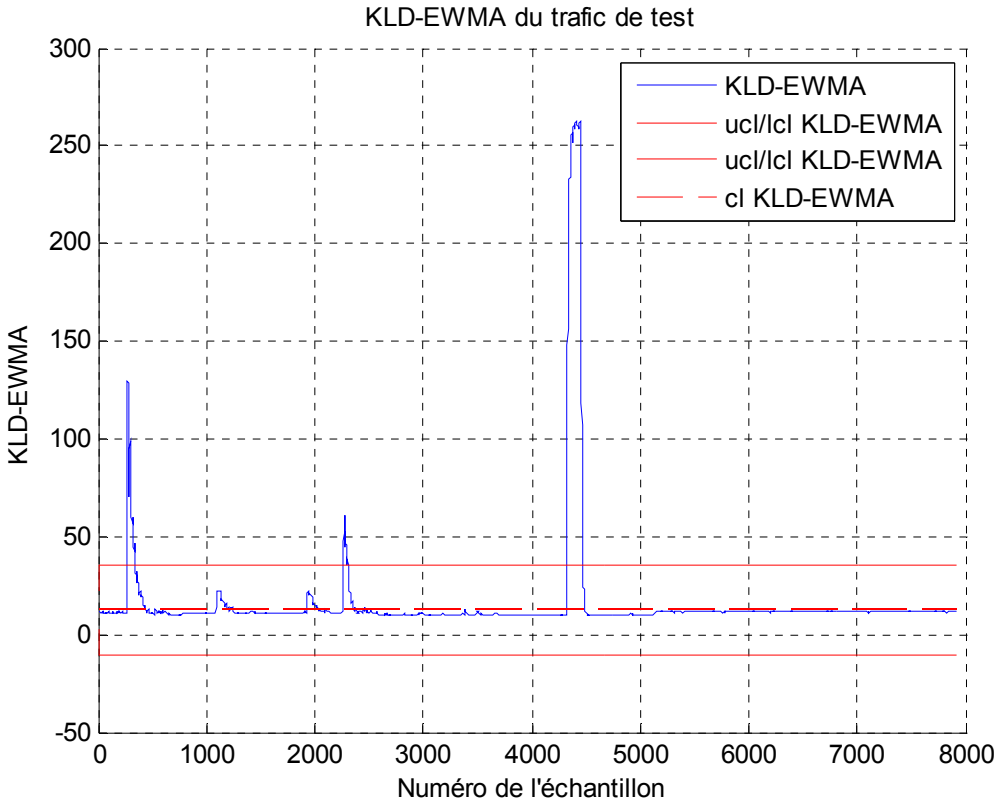

Figure III.8: Résultat de détection des attaques UDP flood par KLD-EWMA

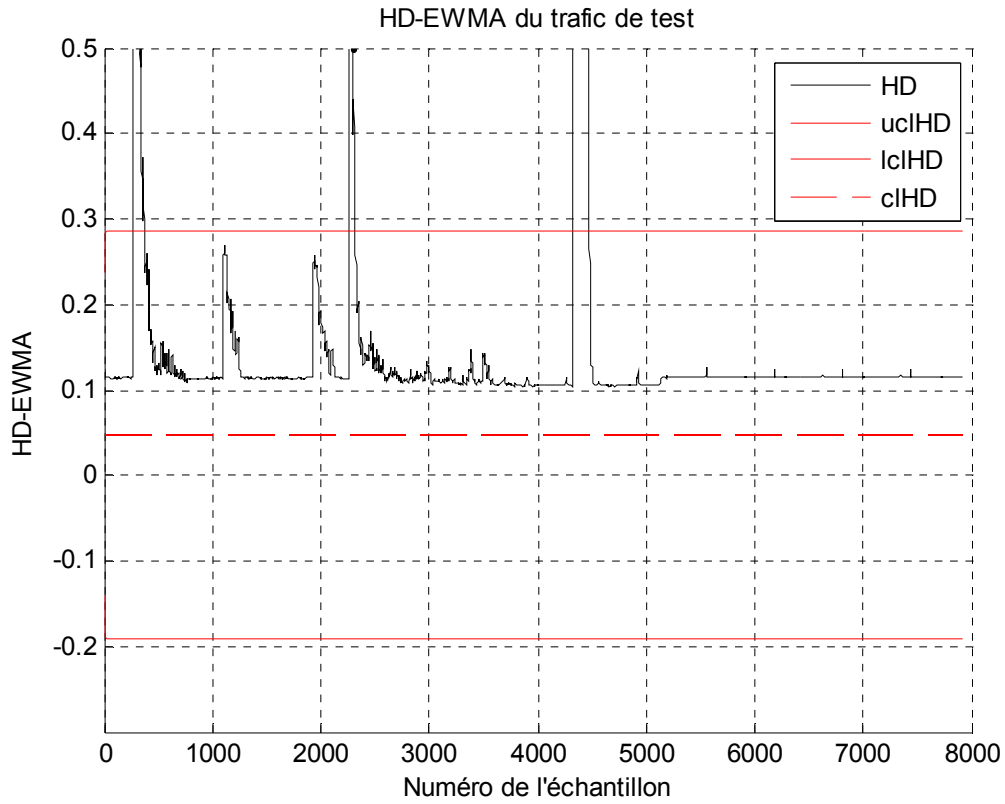

Figure III.9: Résultat de détection des attaques UDP flood par HD-EWMA

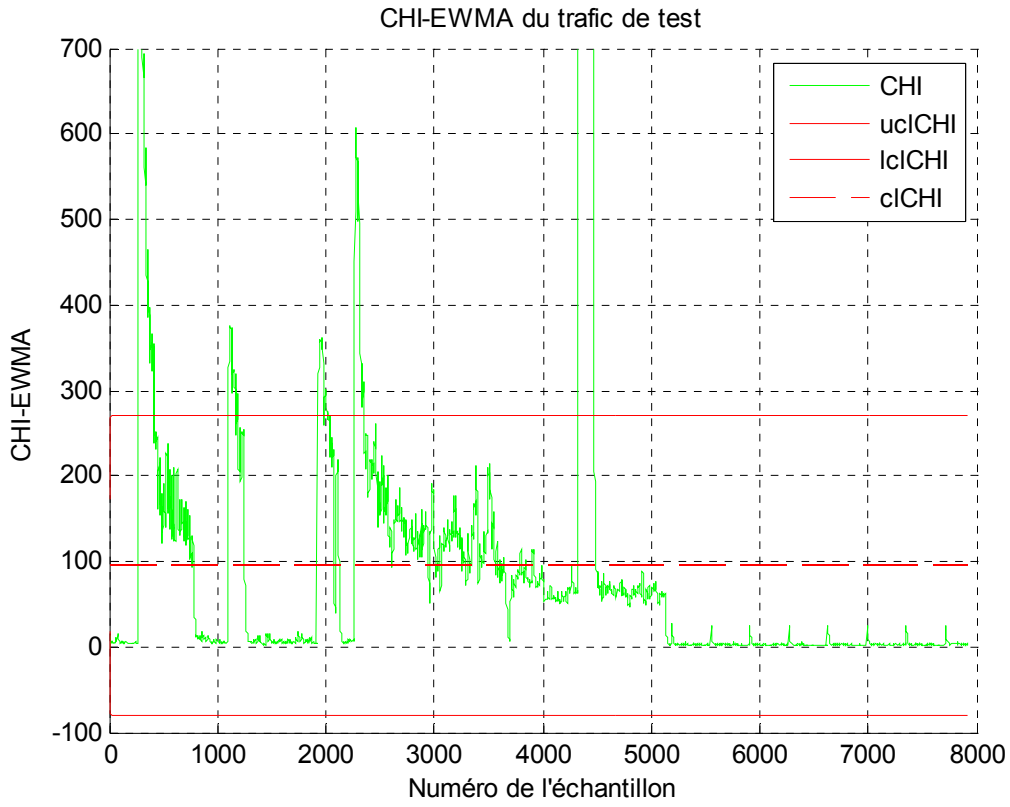

Figure III.10: Résultat de détection des attaques UDP flood par CHI-EWMA

III.4.1.3. Détection des attaques Smurf:

Ici, nous utilisons KLD, HD et CHI pour détecter les attaques DOS/ DDOS Smurf. Le trafic de test dans ce cas représente le flux de messages ICMP ECHO REPLY dans le trafic DARPA99 du jour 1 de la semaine 5.

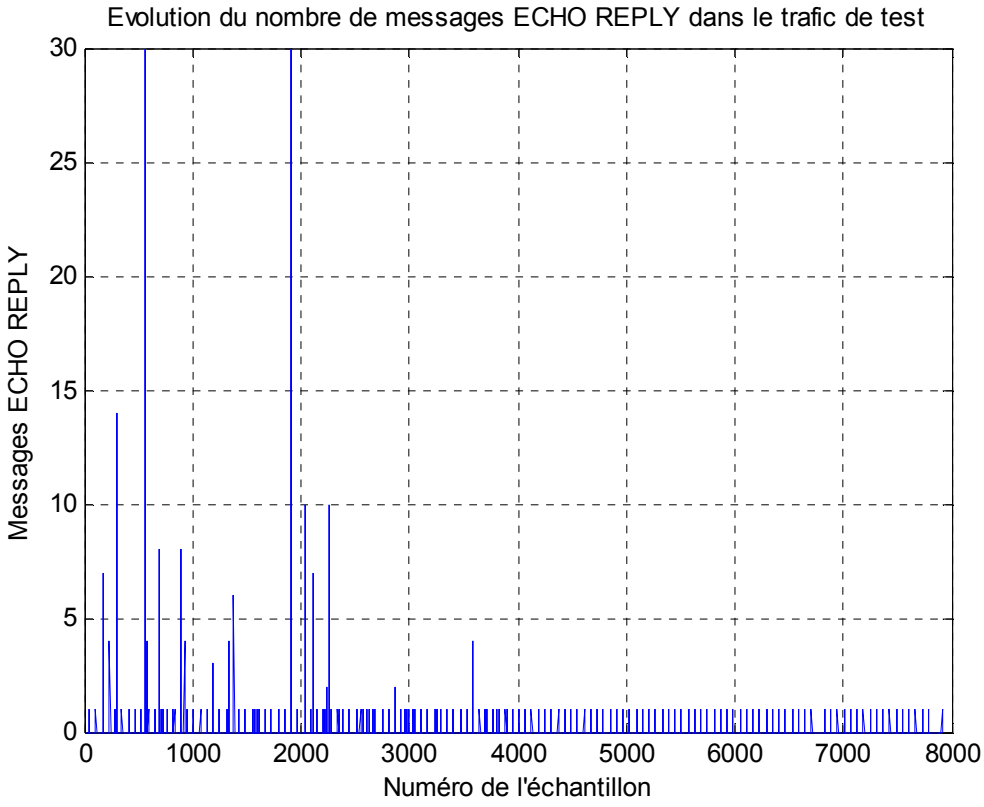

Figure III.11 : Evolution du nombre des messages ECHO REPLY en fonction du numéro de l'échantillon (semaine 5 jour 1)

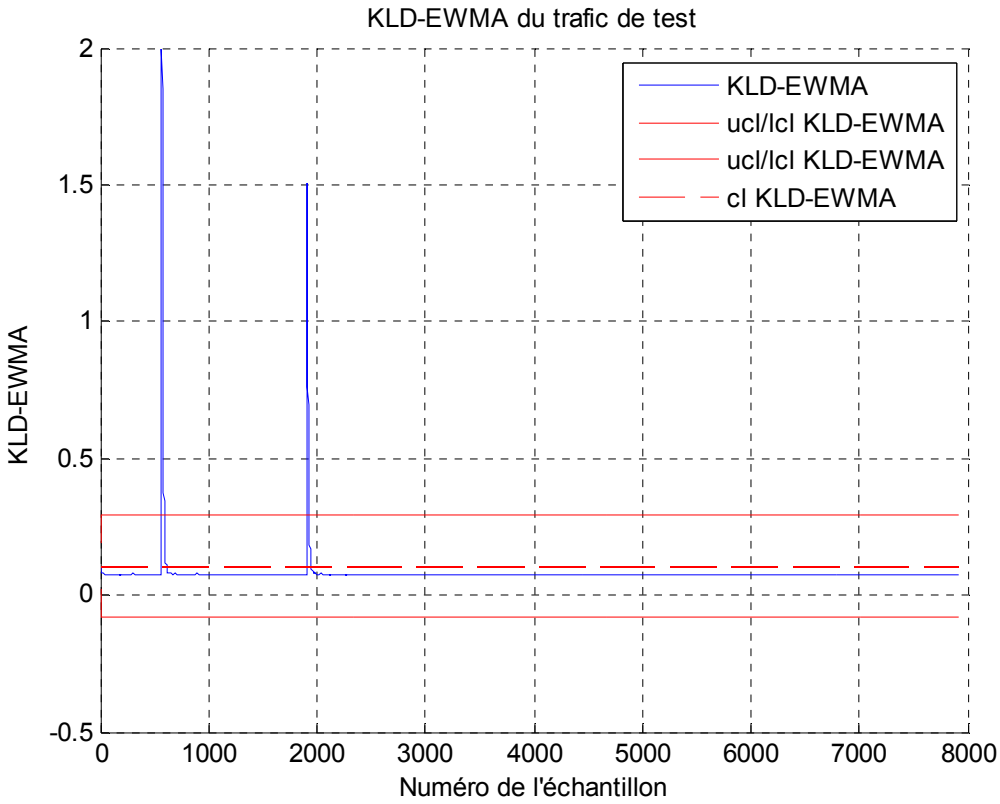

Figure III.12: Résultat de détection des attaques Smurf par KLD-EWMA

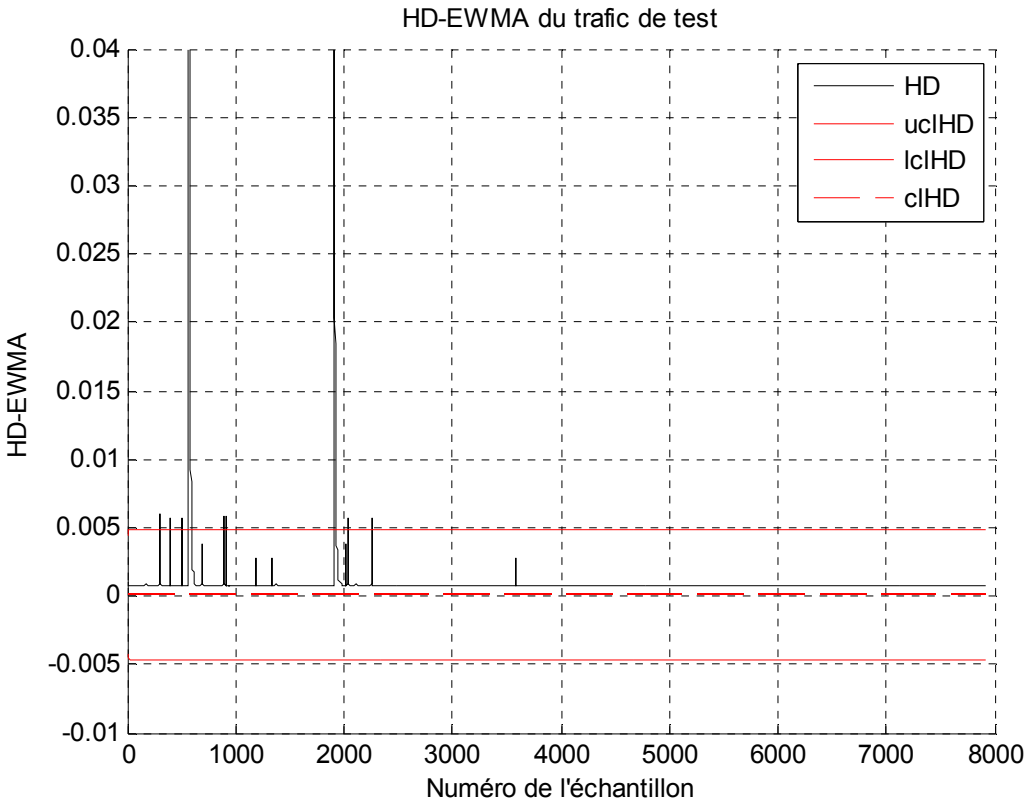

Figure III.13: Résultat de détection des attaques Smurf par HD-EWMA

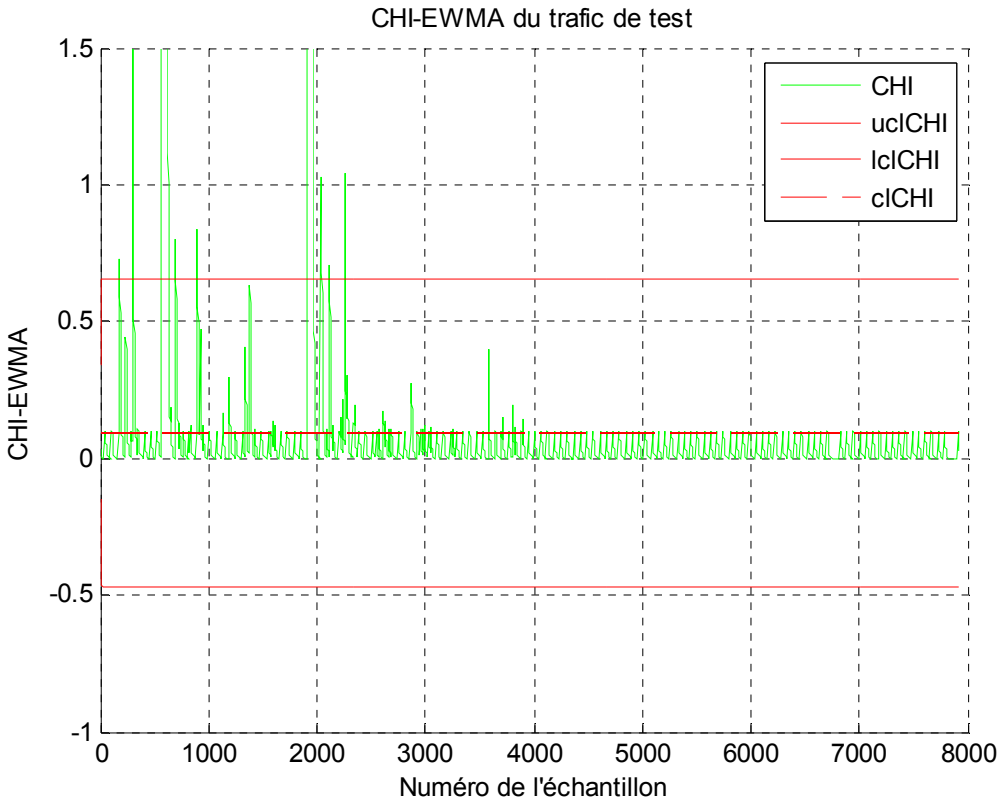

Figure III.14: Résultat de détection des attaques Smurf par CHI-EWMA

III.4.2. MAWI :

III.4.2.1. Détection des attaques SYN flood :

Pour mettre en évidence l'utilité des mesures de divergence dans la détection des différents types des attaques DOS/DDOS, nous les utilisons cette fois pour révéler les éventuelles attaques DOS/DDOS dans le trafic réel de la base MAWI. Dans cette étape, nous essayons de détecter les attaques SYN flood. La figure III.15 illustre notre résultat d'extraction des messages SYN du trafic brute MAWI.

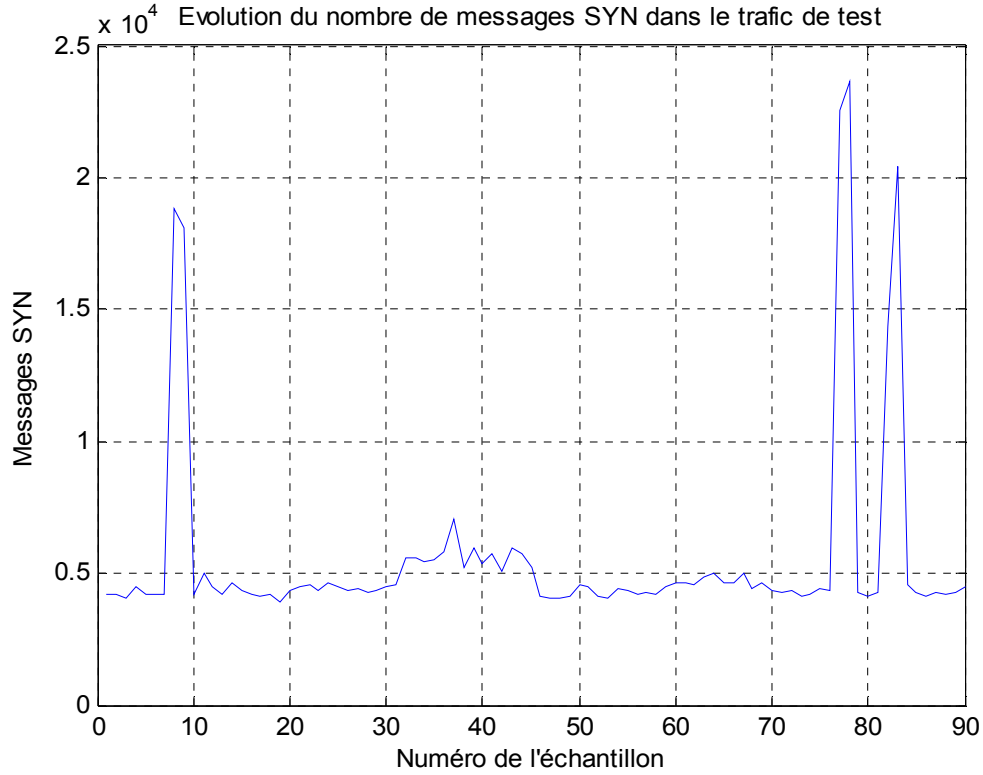

Figure III.15 : Evolution du nombre des messages SYN en fonction du numéro de l'échantillon

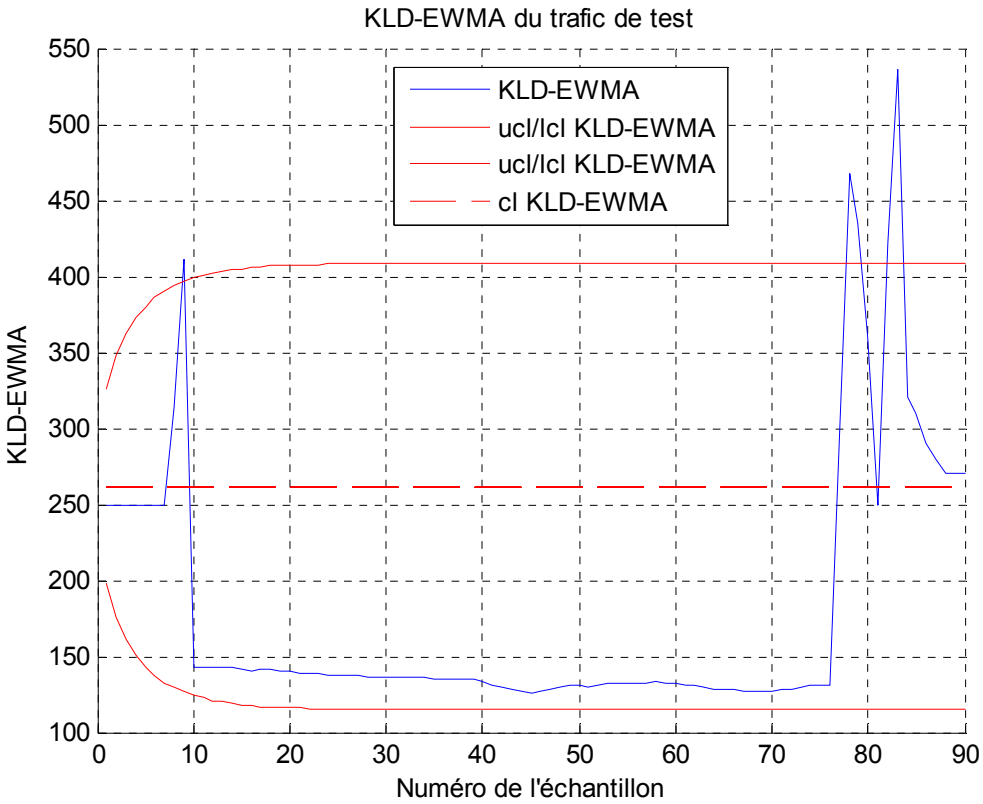

Figure III.16: Résultat de détection des attaques SYN flood par KLD-EWMA

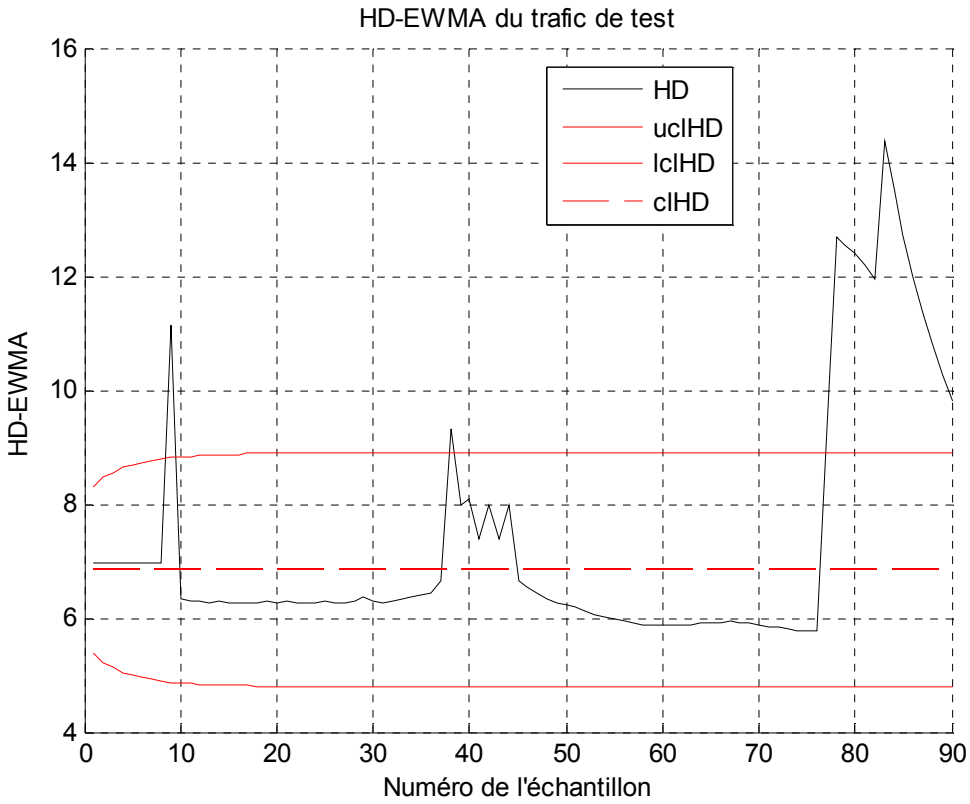

Figure III.17: Résultat de détection des attaques SYN flood par HD-EWMA

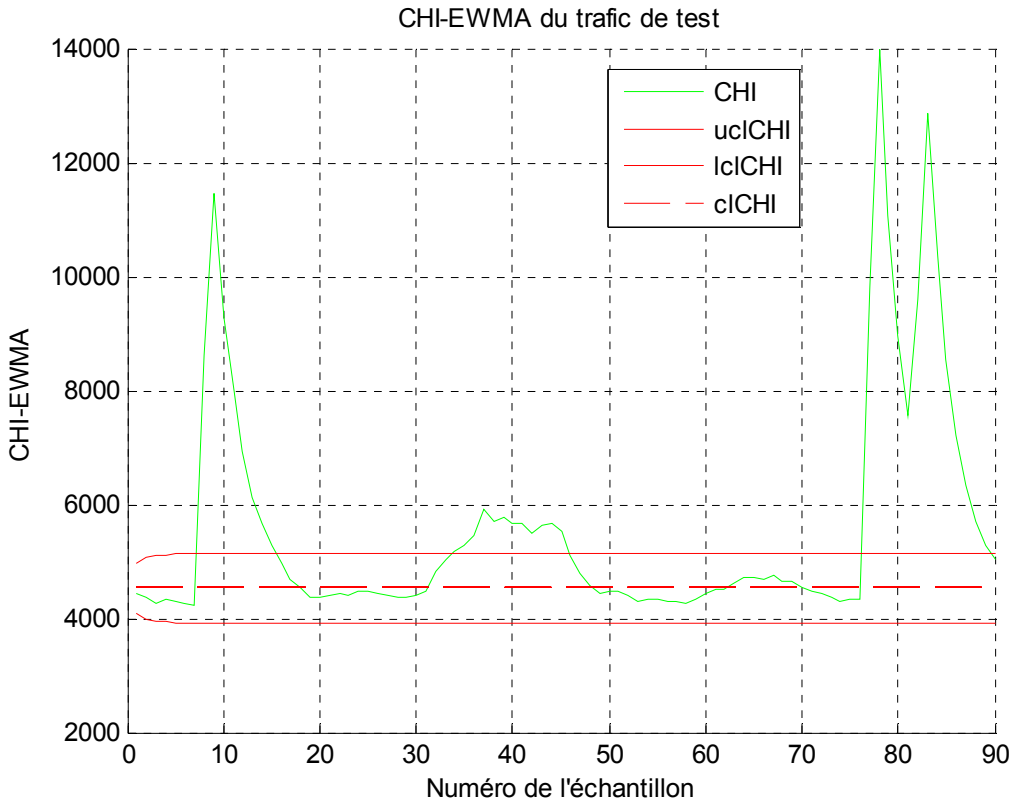

Figure III.18: Résultat de détection des attaques SYN flood par CHI-EWMA

III.4.2.2. Détection des attaques UDP flood:

Dans cette étape, nous cherchons à détecter les attaques UDP flood. La figure III.19 illustre le flux UDP issue du trafic brut MAWI.

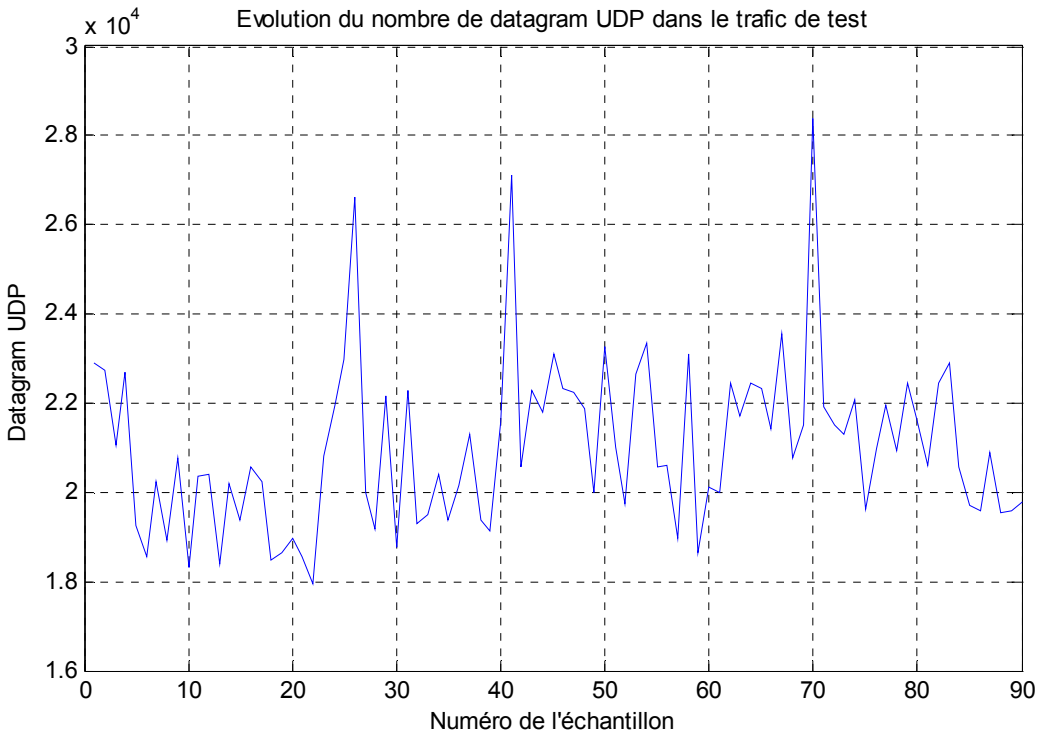

Figure III.19 : Evolution du nombre de datagramme UDP en fonction du numéro de l'échantillon

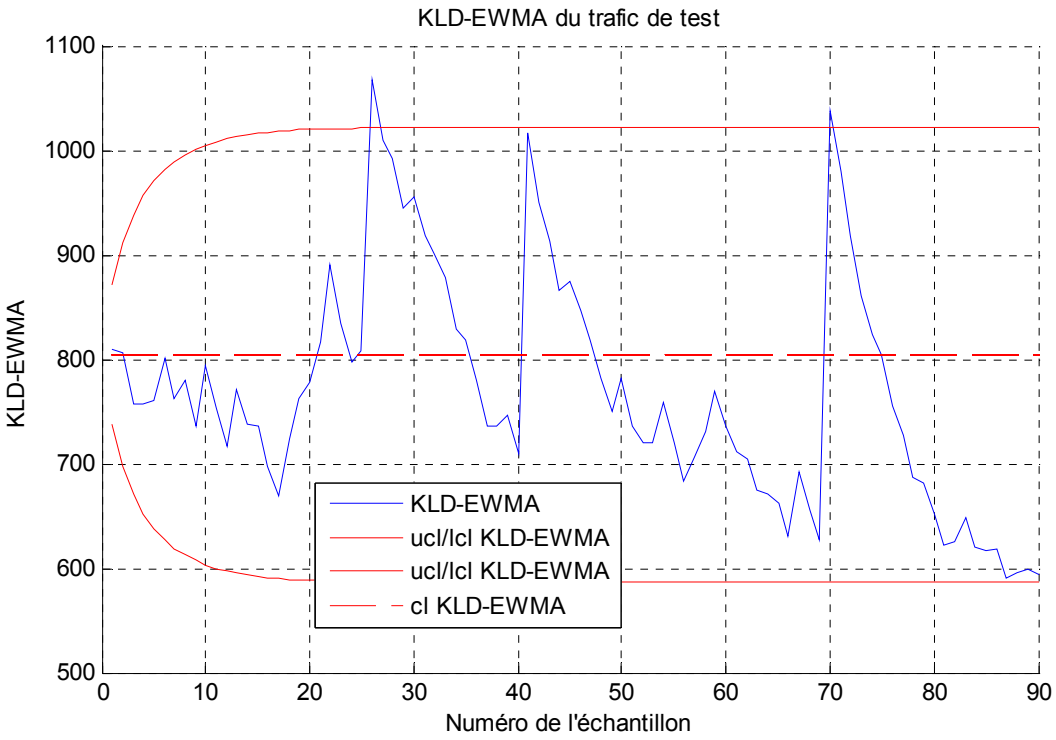

Figure III.20: Résultat de détection des attaques UDP flood par KLD-EWMA

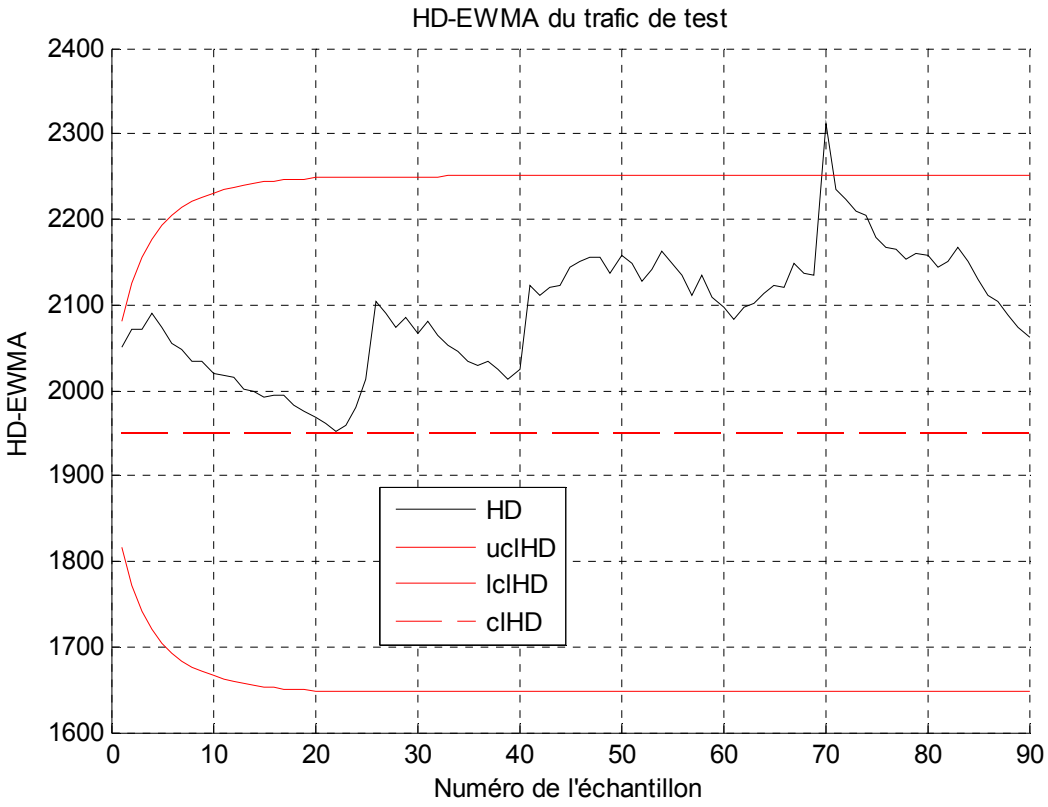

Figure III.21: Résultat de détection des attaques UDP flood par HD-EWMA

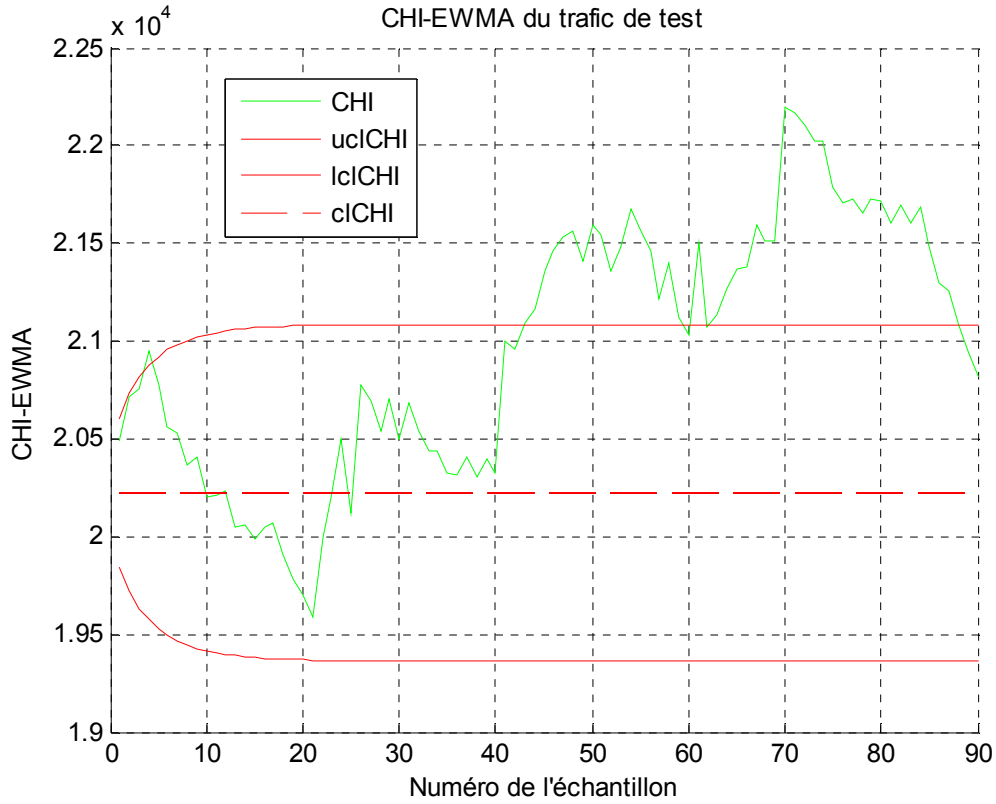

Figure III.22: Résultat de détection des attaques UDP flood par CHI-EWMA

III.4.2.3. Détection des attaques Ping flood:

Toujours avec le trafic MAWI, ici nous nous somme intéressés par la détection des attaques Ping flood. Après extraction des messages ICMP ECHO REQUEST, nous avons obtenu le flux de la figure III.23. Par ailleurs, les résultats de détection par les mesures KLD, HD et CHI sont illustrés dans les figures III.24, III.25 et III.26, respectivement.

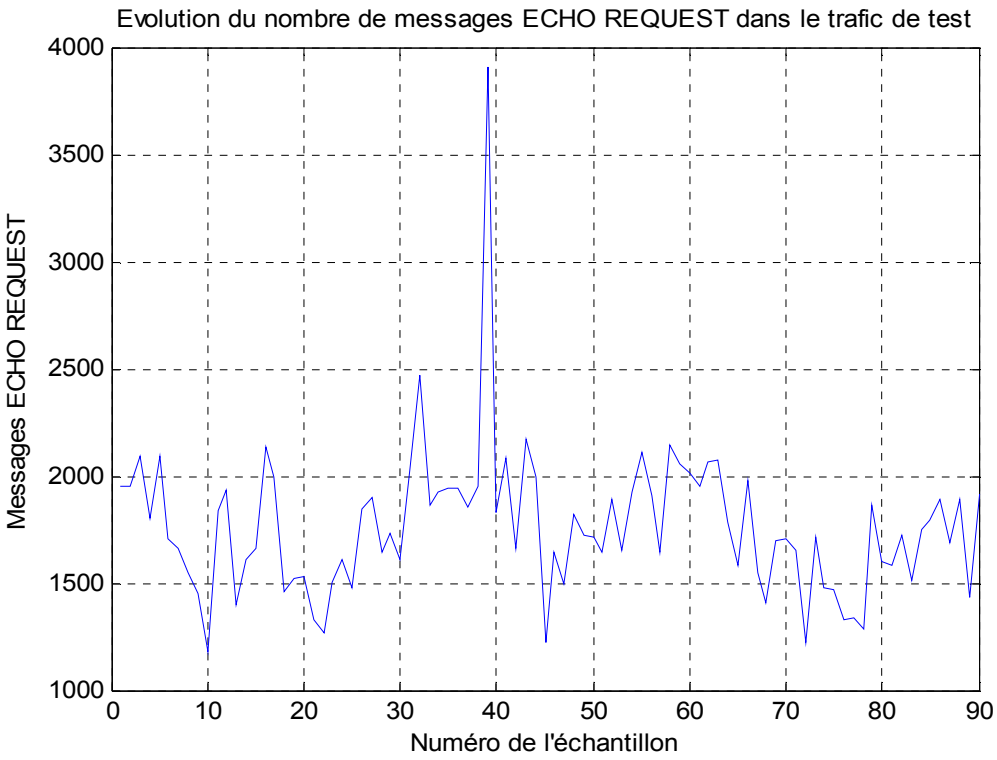

Figure III.23 : Evolution du nombre des messages ECHO REQUEST en fonction du numéro de l'échantillon

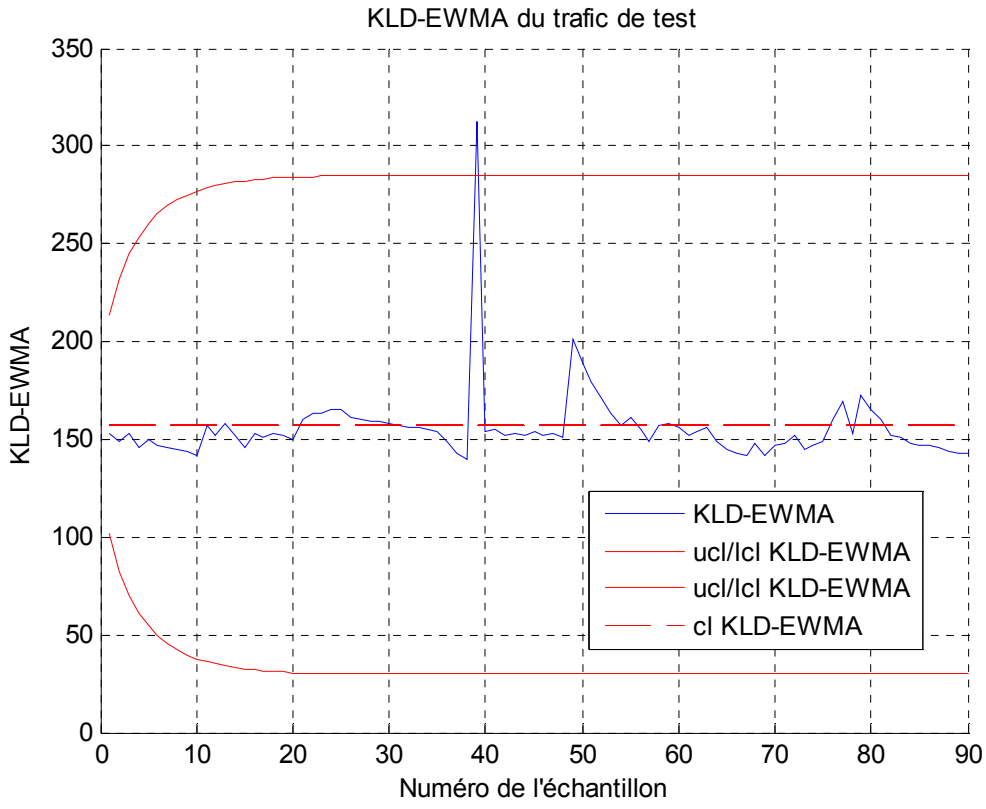

Figure III.24: Résultat de détection des attaques Ping flood par KLD-EWMA

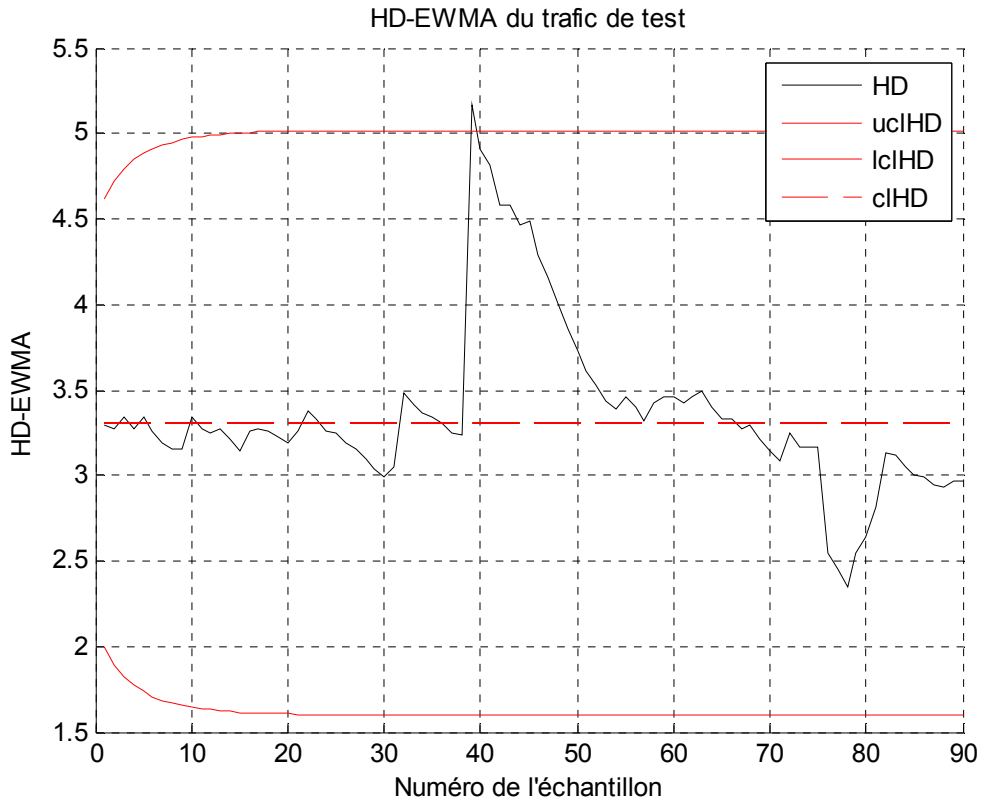

Figure III.25: Résultat de détection des attaques Ping flood par HD-EWMA

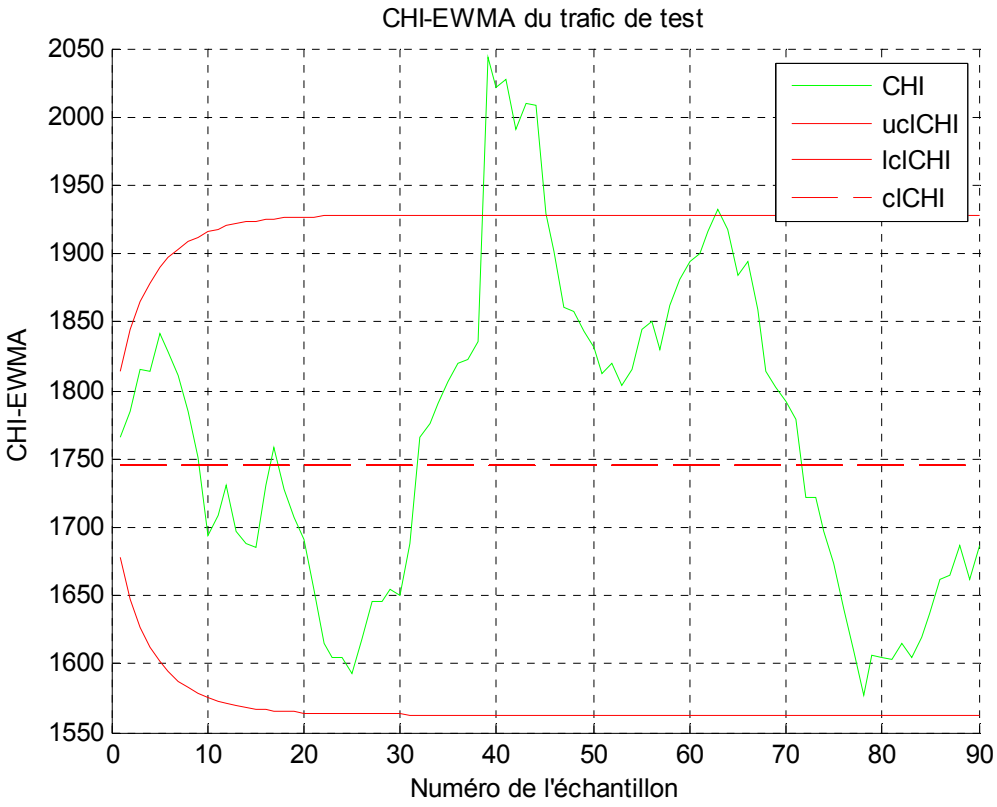

Figure III.26: Résultat de détection des attaques Ping flood par CHI-EWMA

III.5. Interprétations :

Les résultats obtenus montrent, en général, l'utilité des mesures de divergence dans la détection des attaques DOS/DDOS contre les réseaux IP :

- On remarque que les différents types attaques se manifestent, en général, par un changement brusque et important des caractéristiques des combinaisons Kld-EWMA, HD-EWMA et CHI-EWMA. Lorsque le trafis est normal, les mesures ont de petites valeurs, et elle deviennent importante durant les attaques à cause de la grande déviation du trafic avec attaques DOS/DDOS par rapport à l'état normal.
- Pour les differentes attaques et les deux base de données de trafic IP, Kld-EWMA a présenté les meilleurs performances. Elle a permis la détections de la majorité des attaques avec avec un taux minimal de fausse alarmes.
- D'autre part, la divergence CHI était moins performants par rapport aux KLD et HD, elles n'a pas détecté qulques attaques tout en provoquant plus de fausses alarmes.

III.6. Conclusion :

Dans ce chapitre nous avons essayé de mettre en évidence l'utilité des mesures de divergence dans la détection des attaques DOS/DDOS dans les réseaux IP. Nous avons adopté une procédure de détection basée sur les mesure de divergence KLD, HD et CHI comme indicateurs et la carte de contrôle EWMA comme règle de décision.

Avec les deux bases de données DARPA99 et MAWI, les résultats obtenus montre l'utilité des mesures de divergences dans la détection des attaques DOS et DDOS. Les meilleures performances étaient avec KLD.

Conclusion Générale

Conclusion générale

Dans le monde entier, l'émergence de menaces de plus en plus virulentes sur Internet fait que la sécurité informatique n'a jamais autant été si importante. Parmi les menaces dont les conséquences sont les plus catastrophiques, on trouve les cyber-attaques par dénies de service DOS et DDOS. Les sites de e-commerce, les institutions financières, les gouvernements ou les structures d'hébergement sont des cibles fréquentes de ces attaques.

A travers ce mémoire, nous nous sommes intéressés par l'utilisation des mesures de divergence pour détecter les cyber-attaque de types DOS et DDOS. En particulier, nous avons utilisé les mesures de divergence KLD, HD et CHI pour détecter les attaques SYN flood, UDP flood, Ping flood et les attaques Smurf.

Notre procédure de détection consiste à utiliser les mesures de divergence comme indicateur de changement de l'état de trafic dans un réseau IP. Pour différencier les mesures normales des mesures anormale qui reflètent la présence des attaques DOS et DDOS, nous avons fixé les limites de détection par la carte de contrôle EWMA. Précisément, une attaque DOS/DDOS est annoncée lorsque les valeurs des mesures de divergence entre le trafic de test et le trafic normal de référence dépassent les limites UCL/UCL calculées via la carte EWMA.

Les performances de ces mesures sont vérifiées à travers la simulation sous Matlab. Nous avons utilisé le trafic IP fourni par deux bases de données disponibles au grand public : DARPA99 et MAWI.

Les résultats obtenus montrent, d'une part, que les mesures de divergence combinés avec les cartes de contrôle peuvent être utiles dans la détection des différents types de attaques DOS et DDOS. D'autre part, les meilleures performances de détection (taux de détection et de fausses alarmes) sont celles de la divergence KLD.

Vue ces prometteuses résultats, et comme continuité logique de ce travail, nous prévoyons dans premier temps de prendre, en considération plusieurs paramètres du trafic

réseau en même temps pour renforcer le taux de détection et de réduire le taux de fausse alarmes. Ensuite, le développement d'une application pour utilisation réelle sur réseau online.

Références bibliographiques

Références bibliographique

[1] M. Servin « Réseaux et Télécom cours avec 129 exercices corrigés », 2eme édition, Dunod, 2006.

[2] G. Pujolle « Initiation aux réseaux : Cours et exercices » Eyrolles, 2001.

[3] J-F. PILLOU et J-P BAY «Tout sur la sécurité informatique, » 2016.

[4] C. LIORENS, L. LEVIER et D. VALOIS «Tableaux de bord de la sécurité réseau», 2006

[5] D.Dromard et D.Seret « Architecture des réseaux » Pearson Education, 2009

[6] A.Almehmadi « Intrusion Detection System for SYN Flood Attack: Methods and Implementation » International Journal of Computer Science and Information Security (IJCSIS), Vol. 15, No. 1, January 2017.

[7] T.Gunasekhar, K.Thirupathi Rao, P.Saikiran, P.V.S Lakshmi « A Survey on Denial of Service Attacks » International Journal of Computer Science and Information Technologies, Vol. 5, 2014

[8] A-A. Acharya, K-M.Arpitha, S.Kumar B.J « An Intrusion Detection System Against UDP Flood Attack and Ping of Death Attack (DDOS) in MANET», International Journal of Engineering and Technology (IJET), Vol 8 No 2 Apr-May 2016

[9] M.Azahari, M.Yusof, F. Hani and M. Ali, and M.Yusof Darus « Detection and Defense Algorithms of Different Types of DDoS Attacks » International Journal of Engineering and Technology, Vol. 9, No. 5, 2017

[10] M.Basseville « Divergence measures for statistical data processing — An annotated bibliography », Signal Processing, Elsevier, vol. 93, no 4, p. 621-633, 2013.

[11] S. Kullback, R. Leibler, « On information and sufficiency », Annals of Mathematical Statistics, vol. 22, p. 79-86, , 1951.

[12] Sung-Hyuk Cha, "Comprehensive Survey on Distance/Similarity Measures between Probability Density Functions», International Journal of Mathematical Models and Methods in Applied Sciences, Volume 1 (Issue 4), pages: 300-307, 2007.

[13] F. Harrou, Y. Sun, and M. Madakyaru, «Kullback-leibler distance-based enhanced detection of incipient anomalies» Journal of Loss Prevention in the Process Industries, vol. 44, pp. 73–87, 2016.

[14] O. Salem, S. Vaton, and A. Gravey, «A Novel Approach for Anomaly Detection over High-Speed Networks, » in Proceedings of the 3rd European Conference on Computer Network Defense (ECND'07), vol. 30, pages: 49-68, 2009.

[15] G. Cormode and S. Muthukrishnan, «An Improved Data Stream Summary: The Count-Min Sketch and its Applications, » Journal of Algorithms, volume 55, Issue 1, pages: 58-75, April 2005.

[16] M. Deza and E. Deza, «Encyclopedia of Distances», Springer, 2009.

[17] D.C. Montgomery « Introduction to Statistical Quality Control » 6eme edition, Wiley, 2009.

[18] https://www.ll.mit.edu/ideval/data/1999data.html

[19] http://www.fukuda-lab.org/mawilab/data.html

[20] https://www.wireshark.org/download.html