

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
25 janvier 2007 (25.01.2007)

PCT

(10) Numéro de publication internationale
WO 2007/010101 A2

(51) Classification internationale des brevets :
H04L 12/22 (2006.01)

[FR/FR]; 2, rue d'Alembert, F-92130 Issy les Moulineaux (FR).

(21) Numéro de la demande internationale :
PCT/FR2006/001508

(74) Mandataires : **FRECHÉDE, Michel** etc.; Cabinet Plasseraud, 52 Rue de la Victoire, F-75440 Paris Cedex 09 (FR).

(22) Date de dépôt international : 28 juin 2006 (28.06.2006)

(25) Langue de dépôt : français

(81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(26) Langue de publication : français

(30) Données relatives à la priorité :
0507532 13 juillet 2005 (13.07.2005) FR

(71) Déposant (pour tous les États désignés sauf US) :
FRANCE TELECOM [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

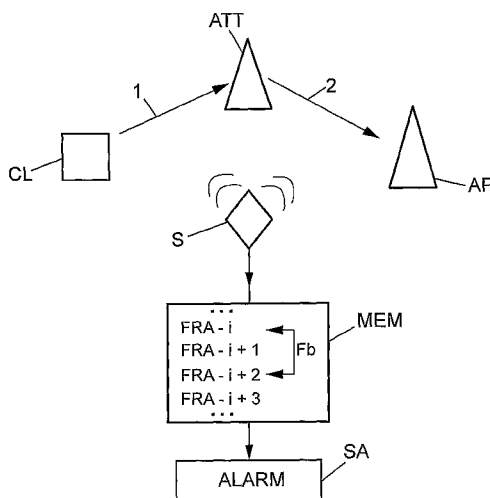
(75) Inventeurs/Déposants (pour US seulement) : **BUTTL, Laurent** [FR/FR]; 184, avenue de Verdun, F-92130 Issy les Moulineaux (FR). **DUFFAU, Roland** [FR/FR]; 66, rue de la Fédération, F-75015 Paris (FR). **VEYSSET, Franck**

(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Suite sur la page suivante]

(54) Title: DETECTING AN INTRUSION BY ALTERNATIVE ROUTING OF DATA PACKETS IN A TELECOMMUNICATION NETWORK

(54) Titre : DETECTION D'UNE INTRUSION PAR DETOURNEMENT DE PAQUETS DE DONNEES DANS UN RESEAU DE TELECOMMUNICATION



(57) Abstract: The invention concerns a "Man-In-The-Middle" intrusion detection between an entity (CL) and an access point of a network in particular an IEEE-802.11 network. Therefor, the invention concerns a method including the following steps: a) reading the bodies of the frames (FRA-i,...,FRA-i+3) transmitted between the entity and the access point; b) detecting frames (FRA-i,FRA-i+2) transmitted at different respective times, but yet comprising identical bodies of frames (fb); and c) triggering an alarm in case of a positive detection at step b).

[Suite sur la page suivante]

WO 2007/010101 A2



ZW), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

Publiée :

- *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

(57) Abrégé : L'invention propose une détection d'intrusion de type "Man-In-The-Middle" entre une entité (CL) et un point d'accès (AP) d'un réseau notamment selon la norme IEEE-802.11. Elle propose à cet effet les étapes suivantes : a) lire les corps de trames (FRA-i,...,FRA-i+3) transmises entre l'entité et le point d'accès, b) détecter des trames (FRA-i,FRA-i+2) transmises à des instants respectifs distincts, mais comportant pourtant des corps de trames (fb) identiques, c) et déclencher une alarme en cas de détection positive à l'étape b).

Détection d'une intrusion par détournement de paquets de données
dans un réseau de télécommunication

La présente invention concerne, de manière générale, la détection d'une
5 intrusion entre une entité communicante via un réseau et un point d'accès de
ce réseau.

En particulier dans les réseaux sans fil, spécifiés notamment dans les normes
[IEEE802.11-1997] et [IEEE802.11-1999] et largement utilisés dans les
10 réseaux dits "*Hot-Spots*", Entreprises et Résidentiels, des techniques de
piratage sont apparues et l'un des risques les plus importants pour de tels
réseaux est de créer un faux point d'accès afin d'intercepter les
communications d'entités légitimes dites "*clients*" et récupérer ainsi des
données privées (ou "*Payload*" en anglais). Cette catégorie d'attaque est alors
15 dite "*attaque par point d'accès illégitime*".

Le point d'accès est en effet un élément primordial de la communication entre
un client et un réseau. Une attaque connue mettant en œuvre un faux point
d'accès consiste, pour l'attaquant, à se retrouver entre un client légitime et un
20 point d'accès légitime du réseau. Dans cette position, l'attaquant est alors
capable d'intercepter toutes les communications. On parle d'attaque de type
"*Man-In-The-Middle*".

Dans le contexte de la présente invention, la communication a lieu par paquets
25 de données comportant, de manière générale, un champ dans lequel peuvent
être identifiées au moins les adresses de départ et de destination des paquets
(dites aussi "*adresse source*" et "*adresse destination*"). Il peut typiquement
s'agir d'adresses MAC (pour "*Medium Access Control*") ou IP (pour "*Internet*
"*Protocol*").

D'une manière générale, les attaques de type "*Man-In-The-Middle*" sont difficilement détectables car elles peuvent mettre en œuvre une technique d'usurpation d'adresse MAC notamment. Il devient difficile alors de distinguer deux équipements différents émettant à partir d'une même adresse MAC.

5

Ce type d'attaque est particulièrement efficace et intéressant pour l'attaquant lorsque la connexion légitime, par exemple dans un réseau sans fil, n'est pas chiffrée et a lieu en mode dit "*infrastructure*", c'est-à-dire entre un client et un point d'accès. C'est typiquement le cas de la technologie "*hot-spot*" déployée par les opérateurs de téléphonie mobile, et celui de la majorité des réseaux d'accès sans fil aux entreprises (même si ces derniers utilisent des mécanismes de sécurité des couches supérieures (au dessus de niveau 2) tels que IPsec, SSH (Secure Shell) ou TLS (Transport Layer Security) pour l'accès des collaborateurs).

10

15

La présente invention vise en particulier une détection efficace d'une attaque de type "*Man-In-The-Middle*" pour les réseaux de type "*hot-spot*" ou entreprise. L'efficacité de l'attaque, dans ce dernier cas, dépend beaucoup des mécanismes de sécurité utilisés par l'entreprise, en particulier leur vulnérabilité à des attaques actives.

20

On décrit ci-après de façon détaillée une attaque de type "*Man-In-The-Middle*" (notée ci-après MITM).

En référence aux figures générales 1 et 2, lors d'une communication classique en mode infrastructure, le client CL est directement connecté au point d'accès AP via un réseau de télécommunication RES. Dans une connexion standard telle que représentée sur la figure 1, il accède alors aux services offerts par un second réseau qui est situé derrière le(s) point(s) d'accès, par exemple à un accès Internet dans le cas de l'utilisation d'un hot-spot WiFi.

25

Malheureusement, le client légitime CL n'a que peu d'informations sur le point d'accès légitime auquel il se connecte. En pratique, ces informations sont

30

souvent le nom de réseau (ESSID, pour "*Extended Service Set Identifier*" en anglais), voire l'adresse MAC (BSSID, pour "*Basic Service Set Identifier*" en anglais). Toutefois, ces éléments peuvent habituellement être usurpés facilement.

5 Dans de nombreux environnements, un pirate est généralement en mesure de mener une attaque de type MITM en usurpant la fonction de point d'accès pour le client, et la fonction de client pour le point d'accès. En référence à la figure 2 illustrant une attaque de type MITM, le pirate PI se positionne ainsi en relais "*transparent*" et intercepte donc l'ensemble des paquets émis par le
10 client et par le point d'accès légitime.

Pour émuler un faux point d'accès, l'attaquant choisit un nom de réseau (identifiant "*ESSID*"), une adresse MAC pour son interface sans fil (identifiant "*BSSID*"), et un canal radio sur lequel émettre. Ces trois éléments peuvent
15 éventuellement être choisis de manière à être les mêmes que ceux du point d'accès légitime, de manière à réduire au maximum les chances pour l'attaquant d'être détecté facilement car, en effet, des outils de détection d'intrusion appropriés pourraient facilement repérer un écart, tel que l'apparition d'un nouveau point d'accès avec d'autres caractéristiques que
20 celles des points d'accès légitimes. Toutefois, pour des raisons d'interférence et donc d'efficacité de l'attaque, l'attaquant devra généralement choisir un canal différent de celui du point d'accès légitime.

La présente invention ne se limite pas à l'un des cas particuliers relatifs à ces variantes de l'attaque. On comprendra par conséquent que ces différentes
25 variantes ne sont pas décrites en détail.

Par ailleurs, pour que l'attaque se déroule sans être détectée facilement par le client, le pirate retransmet l'ensemble des informations reçues entre le client légitime et le point d'accès légitime. En référence à la figure 2, le pirate PI
30 relaye par la flèche 2 les données qu'il reçoit de la flèche 1 et inversement.

Actuellement, aucune technique, unique et sûre, pour la détection d'attaque de type MITM n'a apparemment été proposée. En général, on utilise la conjonction de plusieurs techniques permettant de détecter les différentes phases de cette attaque. Puis, via une corrélation des différents résultats
5 obtenus (typiquement mettant en œuvre un mécanisme de détection de séquence d'événements), on procède à l'identification de l'attaque proprement dite.

Les techniques suivantes peuvent être utilisées simultanément :

- 10 - détection d'une dé-association (ou dé-authentification) d'un client qui a pour but de déconnecter un client légitime du point d'accès légitime auquel il est associé ;
- détection d'une (ou de plusieurs) usurpation(s) d'adresse(s) MAC(s), selon que l'attaquant usurpe l'adresse MAC du point d'accès seulement ou également celle du client, via l'analyse des identifiants "*Sequence Number*"
15 par exemple ;
- détection de la création d'un point d'accès illégitime (par exemple un même BSSID et un même ESSID qu'un point d'accès légitime, mais le canal radio est différent) ;
- et éventuellement détection d'un nombre de messages EAP ("*Extensible Authentication Protocol*") supérieur au nombre normalement utilisé par un
20 client pour se connecter à un point d'accès. Dans ce type d'attaque, le client légitime s'associe au point d'accès illégitime et l'attaquant usurpe l'identité du client légitime pour s'associer au point d'accès légitime. On comprendra ainsi que deux fois plus de trames EAP sont diffusées avec les
25 mêmes adresses MAC source et destination. Le critère des adresses MAC peut varier selon que l'attaquant usurpe également l'adresse MAC du client légitime ou bien uniquement celle du point d'accès légitime.

Ainsi, on détecte habituellement une attaque à l'aide d'une succession logique d'événements. Toutefois, ces événements peuvent être chacun sujet à des faux positifs (alarmes levées à tort), mais aussi et surtout à des faux négatifs (attaques non détectées) dans le cas où l'on décide de ne détecter l'attaque que si toutes les conditions précitées sont remplies.

La technique basée sur l'analyse du Sequence Number nécessite la gestion de seuils très précis et délicats à positionner. Par conséquent, cette technique seule est difficile à mettre en œuvre afin de s'assurer de l'absence de faux positifs et faux négatifs. La difficulté principale réside dans la gestion des pertes de paquets lors, par exemple, d'une transmission à longue distance. En effet, certains paquets seront perdus, ce qui entraînera des problèmes de faux positifs car les Sequence Number varieront fortement d'un paquet à l'autre. Il est donc nécessaire de gérer des seuils de manière très fine.

Les techniques d'identification de dé-association d'un client et d'analyse du nombre de trames EAP utilisées lors de la reconnexion d'un client sont également soumises au risque de perte de paquets. En effet, la dé-authentification d'un client ne repose que sur un seul paquet (trame de dé-association ou dé-authentification), qui, par exemple en cas d'une surcharge des capacités de calcul d'une sonde, peut ne pas être vu par cette sonde. De même, la méthode d'énumération des paquets EAP ne tolère pas la perte de paquets.

En outre, l'attaque de type MITM peut aussi se dérouler lors de l'arrivée initiale du client sur le réseau. Ce nouveau client se connecte alors sur un faux point d'accès qui attendait son arrivée et ce faux point d'accès peut ensuite effectuer la deuxième partie de l'attaque, en usurpant les informations du client pour se connecter au point d'accès légitime. Dans ce cas, aucune trame de dé-association ou dé-authentification n'est échangée, rendant la détection de l'attaque encore plus improbable.

La présente invention vient améliorer la situation.

Elle propose à cet effet un procédé de détection d'une intrusion dans une communication de données privées entre une première entité et une seconde entité, communicantes via un réseau de télécommunication,

- 5 * la communication étant effectuée par transmission de paquets successifs, chaque paquet comportant au moins :

- un champ d'en-tête incluant au moins une adresse de source du paquet et/ou une adresse de destination du paquet pour un routage approprié des paquets,

- 10 - et un corps de paquet incluant des données privées,

- * ladite intrusion consistant au moins à :

- s'interconnecter entre la première et la seconde entité,

- usurper l'adresse de la première entité et/ou l'adresse de la seconde entité en tant qu'adresse de source et/ou de destination, et

- 15 - détourner ainsi les paquets pour récupérer notamment les données privées,

le procédé comportant les étapes :

- a) détecter au moins un premier paquet et un second paquet, transmis à des instants respectifs distincts entre la première et la deuxième entité, et
20 comportant des corps de paquet identiques,

- b) et déclencher une alarme si un nombre de paquets dont le corps est identique et détectés à l'étape a) est supérieur à un seuil prédéterminé.

La présente invention trouve une application avantageuse dans sa mise en
25 œuvre dans un réseau de télécommunication sans fil, avantageusement configuré selon la norme IEEE-802.11, ce réseau sans fil pouvant être relié à un réseau étendu, notamment dans un contexte de type "*hot-spot*", pour une

détection d'intrusion du type "*Man-In-The-Middle*". La seconde entité précitée peut alors être un point d'accès du réseau sans fil.

5 D'ailleurs, d'autres caractéristiques et avantages de l'invention apparaîtront à l'examen de la description détaillée ci-après, et des dessins annexés sur lesquels :

- la figure 1, présentée ci-avant, illustre schématiquement un exemple d'une situation de communication normale entre une entité client et un point d'accès d'un réseau de télécommunication,
- 10 - la figure 2 illustre schématiquement la situation d'une attaque de type "*Man-In-The-Middle*" dans le contexte de la figure 1,
- la figure 3 représente à titre d'exemple la structure d'un paquet ou "*trame*" de données transmis selon le standard IEEE 802.11,
- la figure 4A illustre les principales étapes du procédé au sens de l'invention, dans un premier exemple de réalisation, correspondant à un
15 organigramme d'un programme d'ordinateur dans ledit premier exemple de réalisation,
- la figure 4B illustre partiellement les étapes d'une variante du procédé de la figure 4A, dans un second exemple de réalisation, correspondant à un
20 organigramme d'un programme d'ordinateur dans ledit second exemple de réalisation, et
- la figure 5 illustre l'opération d'une sonde, par exemple d'un système de contrôle d'un réseau, pour la mise en œuvre de la présente invention.

25 Dans les exemples de réalisation donnés dans la description détaillée ci-après, on considère un réseau sans fil selon la norme IEEE 802.11 en mode infrastructure (entre un client et un point d'accès) et sans chiffrement des données au niveau radio. On décrit, dans ce contexte, une détection, au sens

de l'invention, d'attaques de type "*Man-In-The-Middle*" entre un point d'accès considéré comme légitime et le client. L'invention s'adapte tout particulièrement au contexte des hot-spots.

5 Pour réaliser cette détection, il est avantageux de prévoir une infrastructure d'écoute de la voie radio. Les clients et les points d'accès légitimes ne sont pas capables de voir les attaques et en particulier ne peuvent repérer des attaques du type MITM. L'infrastructure d'écoute peut être déployée en sus d'une architecture de type IEEE 802.11 existante.

10 L'invention utilise, dans ce contexte, le principe suivant.

Dans un réseau local sans fil de type IEEE 802.11, composé d'au moins un point d'accès légitime et d'un client légitime, on suppose qu'un attaquant a réalisé une attaque de type "*Man-In-The-Middle*" entre le client légitime et le point d'accès légitime, et qu'il retransmet donc les paquets reçus du client vers
15 le point d'accès légitime.

Lorsque le client légitime émet un paquet de données IEEE 802.11, ce paquet est composé d'un en-tête IEEE 802.11 et d'une partie "*données*". L'en-tête contient des informations relatives au réseau IEEE 802.11 et permettant le bon acheminement du paquet de la source jusqu'à la destination. Lorsque
20 l'attaquant ré-émet ce paquet à destination du point d'accès légitime, un certain nombre de champs de cet en-tête sont modifiés (on peut même dire que l'en-tête est totalement recréé par l'attaquant). En revanche, la partie "*données*" ne change pas. Cette partie "*données*" du paquet contient les en-têtes des couches réseaux supérieures (par exemple IP, TCP, UDP, ICMP)
25 ainsi que les données des couches applicatives.

L'invention se base alors sur le principe suivant. Il est possible, à partir d'une sonde, d'effectuer une capture puis une analyse des variations de ces champs de "*données*" des paquets. Lorsque deux champs de "*données*" ont été identifiés comme identiques dans des paquets distincts à l'intérieur d'un

intervalle de temps relativement court, on peut supposer qu'il s'agit d'une attaque de type "*Man-In-The-Middle*".

La sonde écoute avantageusement la voie radio sur différents canaux. Ainsi, en termes plus génériques, le réseau comporte une pluralité de canaux de communication, et les étapes du procédé de détection sont menées sur au
5 moins deux de ces canaux et, de préférence, sur chacun des canaux.

On décrit ci-après le contenu d'un paquet ou "*trame*" de données selon le standard IEEE 802.11, en référence à la figure 3.

10 La trame comporte d'abord un champ d'en-tête MAC (ou "*MAC Header*") qui est défini par la norme précitée IEEE 802.11. Elle comporte également un champ CRC associé à un code détecteur d'erreurs.

Ensuite, le contenu des données privées transportées est inclus dans un corps de paquet fb ou "*corps de trame*" (selon la dénomination anglo-saxonne
15 "*frame body*"). Ce champ "*frame body*" comporte aussi les données utiles des communications (en particulier TCP/IP). Le contenu applicatif du "*frame body*" peut généralement être de la forme :

- Couche Liaison, par exemple "LLC" (pour "Logical Link Control") ;
- Couche Réseau, généralement IP (pour "Internet Protocol") ;
- 20 - Couche Transport, généralement TCP (pour "Transport Control Protocol") ou UDP (pour "User Datagram Protocol") ;
- puis un protocole applicatif particulier, encapsulé dans le protocole de transport.

Dans le cas des trames IEEE 802.11 transitant sur la voie radio, on cherche à
25 mener une écoute sur cette voie radio. En particulier, le contenu des trames de données (en fait tout ou partie du "*frame body*") est comparé à chaque fois avec le contenu des trames de données précédemment reçues de manière à détecter les trames reçues en double quant à leur '*frame body*'. Si de telles

trames sont repérées sur la voie radio, et ce, de manière régulière, alors une attaque de type "Man-In-The-Middle" est en cours.

5 Un principe de la présente invention consiste en ce que les paquets appartenant aux protocoles des couches supérieures à la couche MAC (notamment dans le modèle OSI) sont généralement sujet à d'importantes variations. En effet, ces différents protocoles utilisent pour la plupart des mécanismes d'identification des paquets émis, par exemple un identifiant codé sur 2 octets pour le protocole IP, un numéro de séquence codé sur 2 octets
10 pour le protocole ICMP ("*Internet Control Message Protocol*" en anglais), un numéro de séquence et un numéro d'acquittement codés sur 4 octets pour le protocole TCP. Ainsi, en pratique, les paquets, en particulier les corps de trame ne sont généralement jamais égaux, même s'ils correspondent à une ré-émission de trame (changement d'un champ spécifiant qu'il s'agit d'une ré-
15 émission, ou changement d'un numéro de séquence). Par conséquent, l'invention est particulièrement adaptée pour réaliser une analyse efficace avec un taux de faux positifs et faux négatifs très faible.

20 En termes plus génériques, on retiendra que les paquets peuvent être transmis selon un protocole de communication qui utilise des données identifiant les paquets émis, ces données étant incluses dans les corps de paquet, ce qui permet de détecter assurément alors une intrusion de type MITM si les corps des paquets sont identiques.

25 On indique en outre qu'il existe toutefois un mode de la norme 802.11 particulier dénommé "*mode répéteur*" et visant à utiliser un point d'accès 802.11 pour retransmettre à l'identique les trames reçues. Ce mode est très peu utilisé en pratique. Son utilisation serait détectée comme une attaque par la précédente invention. Toutefois, une simple utilisation de "*liste blanche*"
30 réglerait facilement le problème.

La présente invention vise aussi une sonde pour la mise en œuvre du procédé ci-avant et qui sera définie plus loin en termes génériques. Il peut s'agir avantageusement d'une sonde de détection d'intrusion adaptée aux réseaux sans fils et localisée sur un site géographique à surveiller. Cette sonde est capable de lever des alarmes en fonction de certains événements repérés. Une analyse particulière du contenu des trames émises ou même des séquences de trames constitue une signature qu'un outil de détection d'intrusion est capable de repérer. Cette signature caractérise un événement, tel qu'une attaque ou simplement un comportement normal.

La sonde a préférentiellement des capacités spécifiques qui lui permettent "d'écouter" sur plusieurs canaux en même temps en assurant, de préférence, qu'il n'y pas ou peu de pertes de trames de données durant l'écoute.

On décrit ci-après deux réalisations possibles dans la mise en œuvre de l'invention.

Un premier mode de réalisation comporte les étapes illustrées sur la figure 4A et susceptibles de représenter un exemple d'organigramme d'un programme d'ordinateur pour la mise en œuvre de l'invention.

En écoutant un réseau typiquement selon la norme IEEE 802.11 à l'aide d'une sonde du type précité, on récupère des paquets de données successifs FRA-i (étape 40). On analyse alors un paquet reçu FRA-i en récupérant en particulier son corps de trame fb-i ou "*frame body*" (étape 41) qui inclut des données privées qu'une entité cliente souhaitait par exemple transmettre vers un point d'accès. L'étape 42 consiste à calculer une signature sgn-i par une fonction de hachage H de tout ou partie du corps de trame fb-i. Le résultat peut par exemple se présenter par un nombre sur 128 bits (en utilisant la fonction MD5 pour "*Message Digest 5*") ou 160 bits (en utilisant la fonction SHA1 pour "*Secure Hash Algorithm 1*") ou sur n bits (avec une autre fonction de hachage). Cette valeur, notée sgn-i sur la figure 4A est appelée

HASH_FRAMEBODY ci-après. La partie du corps de trame hachée pour le calcul de la signature peut être un élément important pour des raisons de performances. En effet, l'invention peut être optimisée de manière à ne faire un calcul du haché que sur les 100 premiers octets par exemple. Il peut alors
5 s'agir d'un paramétrage de la sonde implémentant l'invention. Ce point peut aussi avoir son importance sur certaines catégories d'attaques qui peuvent entraîner des modifications de certains octets fixes du corps de trame fb-i. Il est alors possible de définir les octets à ne pas vérifier de manière à pouvoir détecter certaines classes d'attaques. Ce point peut aussi être un paramétrage
10 de l'outil implémentant l'invention.

Ainsi, en termes plus génériques, pour chaque paquet reçu :

- on calcule une signature du corps du paquet en appliquant une fonction de hachage à tout ou partie des données du corps de paquet,
- on stocke en mémoire ladite signature, et
- 15 - on compare ladite signature à des signatures de corps de paquet précédemment stockées dans ladite mémoire.

Préférentiellement, la fonction de hachage est appliquée à une partie des données du corps de paquet, cette partie des données étant choisie en fonction de la configuration du réseau et/ou en fonction de la pertinence de
20 ces données pour la détection d'intrusion.

A l'étape 43, les informations d'adresses (dans l'en-tête du paquet principalement), par exemple au moins du type @MAC_source (adresse MAC de départ), @MAC_destination (adresse MAC de destination), et avantageusement du type @MAC_BSSID, ainsi, éventuellement, qu'un
25 drapeau TO_DS/FROM_DS (nommé STATE_DS) sont archivées en même temps que la signature du frame body. On indique que le drapeau précité TO_DS est un champ indiquant que le paquet en provenance du client est à destination du réseau derrière le point d'accès (typiquement un réseau filaire). Le drapeau FROM_DS est un champ indiquant que la trame en provenance

du point d'accès provient d'un équipement situé derrière le point d'accès (dans le réseau filaire). Ces identifiants sont couramment utilisés en contexte Wi-Fi, comme on le verra en référence à un troisième mode de réalisation décrit plus loin.

- 5 On stocke ces cinq données (@MAC_source, @MAC_destination, @MAC_BSSID, STATE_DS, HASH_ FRAMEBODY) avantageusement dans une mémoire de type FIFO (pour "*First In First Out*"), en tant que quintuplé préférentiellement pendant une durée prédéfinie, les plus anciens quintuplés étant automatiquement effacés et remplacés lors de l'arrivée à leur fin de
- 10 durée de vie. Cette durée peut être fixée en pratique à une valeur de l'ordre de la dizaine de secondes. En effet, il n'est pas nécessaire de garder un historique important du frame body des trames hachées dans la mémoire précitée car l'attaque doit être réalisée en direct par l'attaquant et ce dernier ne peut se permettre de ralentir fortement le relais des trames.
- 15 Au test 44, on compare le nouveau HASH_ FRAMEBODY sgn-i avec ceux présents dans la mémoire en faisant préférentiellement cette comparaison de manière séquentielle. Si il existe dans la mémoire un HASH_ FRAMEBODY sgn-j égal au HASH_ FRAMEBODY courant sgn-i (les indices i et j étant différents), ce qui correspond à la flèche o en sortie du test 44, alors il est levé
- 20 une alarme de type "*Man-In-The-Middle*" à l'étape 45. Sinon (flèche n en sortie du test 44), le procédé se poursuit en analysant une trame FRA-i suivante (étape 46) et le procédé est réitéré pour cette nouvelle trame à l'étape 40.

L'organigramme ci-avant présente le procédé le plus optimisé en terme de rapidité de traitement des informations IEEE 802.11 reçues par la sonde.

25

Il est possible de limiter les faux positifs avec la réalisation plus sophistiquée qui est présentée en figure 4B. Dans cette réalisation, à l'issue du test 44 de la figure 4A, on compte le nombre K de fois où le nouveau HASH_ FRAMEBODY est égal à ceux présents dans la mémoire en faisant la comparaison 44 de

manière séquentielle (étape 47). Dès que ce compteur dépasse un seuil prédéfini K_{TH} (flèche o en sortie du test 48), alors il peut être levé une alarme de type "*Man-In-The-Middle*" (étape 45 de la figure 4A). La valeur du seuil K_{TH} peut être un paramètre de la sonde au sens de l'invention. En termes plus
5 génériques, on retiendra que le déclenchement de l'étape b) du procédé général défini ci-avant est conditionné par la détection d'un nombre de paquets dont le corps est identique à l'étape a), ce nombre (correspondant en pratique au seuil $K_{TH}+1$) étant préférentiellement choisi selon une configuration donnée du réseau. Dans le cas particulier de la figure 4A, ce seuil K_{TH} a simplement
10 une valeur de 1.

L'organigramme de la figure 4B présente le procédé le plus optimisé en terme de réduction de faux positifs dans le traitement des informations IEEE 802.11 reçues par la sonde. L'outil peut implémenter les deux méthodes et
15 sélectionner de manière dynamique la plus adaptée en fonction du contexte. Il est bien entendu possible de paramétrer la fenêtre de temps d'écoute pour optimiser le processus de détection. Ainsi, en termes plus génériques, le déclenchement de l'alarme à l'étape b) est effectif si des premier et second paquets de même corps sont détectés à l'étape a) dans un intervalle de temps
20 inférieur à une durée prédéterminée, cette durée étant préférentiellement choisie en fonction d'une configuration du réseau.

En effet, selon les environnements, il peut être possible que des re-émissions normales entraînent des faux positifs (par exemple en mode répétitif de la norme 802.11). Cependant, ce comportement est rare en principe, et ne peut
25 en soi impliquer des problématiques importantes car une attaque de type "*Man-In-The-Middle*" entraînerait un nombre important d'alertes contrairement à des re-émissions sporadiques dans la fenêtre de temps qui peut être définie comme étant courte car il est rappelé que l'attaquant a la contrainte de devoir re-émettre le paquet rapidement.

L'alarme levée par la sonde peut indiquer les cinq données précitées @MAC_source, @MAC_destination, @MAC_BSSID, TO_DS/FROM_DS et HASH_FRAMEBODY associées à la trame actuelle, et à celle d'une trame précédemment stockée en mémoire. Il est alors possible de donner des informations supplémentaires telles que les adresses MAC source, destination et BSSID. Même si, en principe, elles ne sont pas nécessaires pour réaliser la détection d'attaque, elles peuvent en revanche aider l'opérateur à tracer l'événement de manière plus précise.

On décrit ci-après un troisième mode de réalisation dans un contexte spécifique correspondant à des communications entre clients Wi-Fi.

Dans plusieurs hot-spots et réseaux d'accès sans fil d'entreprise, une fonctionnalité est activée sur les points d'accès légitimes pour interdire les connexions inter-clients d'un même point d'accès. Il s'agit d'un fonctionnement dit en mode relais (ou *"bridge"*) du point d'accès. Un exemple concret est la fonction PSPF (pour *"Publicly Secure Packet Forwarding"*) proposée par les points d'accès CISCO (marque déposée). Lorsque cette fonctionnalité est activée, l'invention s'avère particulièrement efficace.

En revanche, en l'absence d'une telle fonctionnalité, un paquet émis par un client à destination d'un autre client du même point d'accès est retransmis par le point d'accès légitime sans modification du *"frame body"*. Ce phénomène serait détecté comme une possible attaque de MITM au sens de l'invention. Il est donc possible d'ajouter une étape de vérification supplémentaire à effectuer sur les paquets identifiés dans ces conditions. Cette étape de vérification supplémentaire peut être par exemple activable par l'administrateur du réseau sans fil selon la configuration choisie pour son réseau.

Elle se décrit comme suit. Lorsqu'une trame est émise par un client A à destination d'un autre client B du même point d'accès, le drapeau *"To DS"* décrit ci-avant de cette trame est mis à 1, tandis que le drapeau *"From DS"* est mis à zéro. Les champs @MAC_destination et @MAC_source sont remplis

respectivement avec l'adresse MAC de B et l'adresse MAC de A, et le champ BSSID présente l'adresse MAC du point d'accès.

5 Puis, lorsque ce paquet est retransmis par le point d'accès à destination du client B, le champ "To DS" est mis à zéro tandis que le champ "From DS" est mis à 1. Les champs @MAC_destination et @MAC_source sont remplis respectivement avec l'adresse MAC de B et l'adresse MAC de A, et le champ BSSID présente l'adresse MAC du point d'accès.

10 Ainsi, il suffit de vérifier que les deux paquets identifiés comme possédant un même 'frame body' ont les mêmes @MAC_destination, @MAC_source, et BSSID, mais en particulier des drapeaux "To DS" et "From DS" de valeurs opposées, ce qui permet de lever une alarme sans pratiquement aucun risque de faux positifs.

15 En termes plus génériques, on retiendra que lorsque l'intrusion comporte en outre une étape de modification de données (telles que les valeurs de drapeaux TO DS/FROM DS) dans le champ d'en-tête :

- à l'étape a), on compare en outre les champs d'en-tête des premier et second paquets,
- et à l'étape b), on déclenche l'alarme si les corps de paquet sont identiques et si les champs d'en-tête sont différents.

20 Ainsi, l'invention s'adapte avantageusement à un contexte non dépendant d'une contrainte de type "*pas de communications entre clients via un point d'accès*". Il suffit à cet effet de rajouter un test sur les valeurs de drapeaux To DS/ From DS en sortie du test 44 sur le HASH_ FRAMEBODY représenté sur la figure 4A.

25

Une fois déployée, une sonde mettant en œuvre le procédé, se retrouve dans la situation représentée sur la figure 5. La sonde S écoute les deux voies 1 et

2 reliant l'attaquant ATT au client CL, d'une part, et l'attaquant ATT au point d'accès AP d'autre part. Elle stocke dans la mémoire MEM et lit les paquets transitant sur ces deux chemins et détecte en particulier ceux qui ont le même corps de trame en déclenchant, le cas échéant, une alarme.

5

La présente invention vise aussi une telle sonde S, agencée pour détecter une intrusion dans une communication de données privées entre une première entité et une seconde entité (telle qu'un point d'accès), ces entités étant communicantes via un réseau de télécommunication, la sonde comportant :

- 10 - de préférence, des moyens de lecture au moins des corps des paquets transmis entre la première entité et la seconde entité, par exemple dans la mémoire MEM,
- des moyens de comparaison des corps de paquet pour détecter au moins un premier paquet et un second paquet, transmis à des instants respectifs
15 distincts entre la première entité et la seconde entité, et comportant des corps de paquet identiques,
- et des moyens SA pour déclencher une alarme si le nombre de paquets détectés dont le corps est identique est supérieur à un seuil K_{TH} .

- 20 La présente invention vise aussi un programme d'ordinateur pouvant être téléchargé via un réseau de télécommunication et/ou destiné à être stocké dans une mémoire d'une sonde du type décrit ci-avant et/ou stocké sur un support mémoire destiné à coopérer avec un lecteur de cette sonde. En particulier, le programme comporte des instructions pour la mise en œuvre du
25 procédé du type décrit ci-avant. La présente invention vise aussi un support de stockage de données comportant des instructions de code de programme informatique pour l'exécution des étapes du procédé au sens de l'invention.

La présente invention vise aussi un système pour la mise en œuvre d'un procédé de détection d'une intrusion dans une communication de données privées, typiquement entre une pluralité d'entités communicantes via un réseau de télécommunication et une pluralité de points d'accès du réseau. A
5 cet effet, il comporte une pluralité de sondes formant une architecture déployée sur le réseau et de contrôle du réseau, chaque sonde comportant les moyens énoncés ci-avant.

Selon l'un des avantages que procure l'invention, la détection au sens de
10 l'invention est entièrement passive. Elle ne nécessite aucune interaction avec les équipements constituant le réseau sans fil (point d'accès, clients).

Selon un autre avantage que procure l'invention, la détection en cours n'est pas décelable par un attaquant.

Selon un autre avantage encore que procure l'invention, la détection est
15 indépendante du fait que les adresses MAC soient usurpées ou non puisque l'on s'attache au contenu du corps de trame. Elle est aussi indépendante du fait que les noms de réseaux ESSID soient usurpés ou non.

Un autre avantage majeur est qu'elle est indépendante du fait que les canaux radio soient les mêmes ou non.

20 La détection est facile à implémenter en pratique. Elle tolère en particulier que l'équipement en écoute de la voie radio perde des paquets. En effet, cet effet n'a aucun impact en terme de faux positifs. Comme une attaque de type MitM nécessite de nombreux paquets successifs, elle sera nécessairement détectée.

25 Le procédé au sens de l'invention peut être implémenté très simplement dans un outil de détection d'intrusion dans les réseaux sans fil IEEE 802.11, des équipements capables d'écouter la voie radio IEEE 802.11 étant courants.

Revendications

1. Procédé de détection d'une intrusion dans une communication de données
privées entre une première entité et une seconde entité, communicantes via
5 un réseau de télécommunication,

* la communication étant effectuée par transmission de paquets successifs,
chaque paquet comportant au moins :

- un champ d'en-tête incluant au moins une adresse de source du
paquet et/ou une adresse de destination du paquet pour un routage
10 approprié des paquets,

- et un corps de paquet incluant des données privées,

* ladite intrusion consistant au moins à :

- s'interconnecter entre la première et la deuxième entité,
- usurper l'adresse de la première entité et/ou l'adresse de la
15 deuxième entité en tant qu'adresse de source et/ou de destination, et
- détourner ainsi les paquets pour récupérer notamment les données
privées,

caractérisé en ce qu'il comporte les étapes :

a) détecter au moins un premier paquet et un second paquet, transmis à des
20 instants respectifs distincts entre la première et la deuxième entité, et
comportant des corps de paquet identiques,

b) et déclencher une alarme si un nombre de paquets dont le corps est
identique et détectés à l'étape a) est supérieur à un seuil prédéterminé
(K_{TH}).

25

2. Procédé selon la revendication 1, caractérisé en ce que le réseau de
télécommunication est un réseau sans fil.

3. Procédé selon la revendication 2, caractérisé en ce que le réseau sans fil est configuré selon la norme IEEE-802.11.

5 4. Procédé selon l'une des revendications précédentes, caractérisé en ce que ledit réseau est un réseau sans fil relié à un réseau étendu.

5. Procédé selon l'une des revendications précédentes, caractérisé en ce que la seconde entité est un point d'accès du réseau.

10

6. Procédé selon l'une des revendications précédentes, caractérisé en ce que ledit réseau comporte une pluralité de canaux de communication, et en ce que les étapes a) et b) sont menées sur au moins deux de ces canaux.

15 7. Procédé selon l'une des revendications précédentes, caractérisé en ce que le déclenchement de l'étape b) est effectif si lesdits premier et second paquets sont détectés à l'étape a) dans un intervalle de temps inférieur à une durée prédéterminée, ladite durée étant préférentiellement choisie en fonction d'une configuration du réseau.

20

8. Procédé selon l'une des revendications précédentes, caractérisé en ce que, au cours de ladite étape a) :

- on calcule une signature du corps d'au moins un second paquet en appliquant une fonction de hachage à tout ou partie des données du corps de paquet,
- 25 - on stocke en mémoire ladite signature, et

- on compare ladite signature à la signature de corps d'au moins un premier paquet précédemment stockée dans ladite mémoire.

5 9. Procédé selon la revendication 8, caractérisé en ce que ladite fonction de hachage est appliquée à une partie des données du corps de paquet, ladite partie des données étant choisie en fonction de la configuration du réseau et/ou en fonction de la pertinence de ces données pour la détection d'intrusion.

10 10. Procédé selon l'une des revendications précédentes, dans lequel ladite intrusion comporte en outre une étape de modification de données (TO DS/FROM DS) dans le champ d'en-tête, caractérisé en ce que :

- à l'étape a), on compare en outre les champs d'en-tête des premier et second paquets,
 - et à l'étape b), on déclenche l'alarme si les corps de paquet sont identiques et si les champs d'en-tête sont différents.
- 15

20 11. Procédé selon l'une des revendications précédentes, caractérisé en ce que les paquets sont transmis selon un protocole de communication qui utilise des données identifiant les paquets émis, lesdites données étant incluses dans les corps de paquet.

25 12. Procédé selon l'une des revendications précédentes, caractérisé en ce que le seuil prédéterminé (K_{TH}) est choisi selon une configuration donnée du réseau.

13. Sonde, pour la mise en œuvre du procédé selon l'une des revendications 1 à 12, de détection d'une intrusion dans une communication de données

privées entre une première entité et une seconde entité, communicantes via un réseau de télécommunication,

* la communication étant effectuée par transmission de paquets successifs, chaque paquet comportant au moins :

- 5 - un champ d'en-tête incluant au moins une adresse de source du paquet et/ou une adresse de destination du paquet pour un routage approprié des paquets,
- et un corps de paquet incluant des données privées,

* ladite intrusion consistant au moins à :

- 10 - s'interconnecter entre la première entité et la seconde entité,
- usurper l'adresse de la première entité et/ou l'adresse de la seconde entité en tant qu'adresse de source et/ou de destination, et
- détourner ainsi les paquets pour récupérer notamment les données privées,

15 caractérisée en ce que la sonde comporte :

- des moyens de comparaison des corps de paquet pour détecter au moins un premier paquet et un second paquet, transmis à des instants respectifs distincts entre la première et la seconde entité, et comportant des corps de paquet identiques,
- 20 - et des moyens pour déclencher une alarme si un nombre de paquets dont le corps est identique et détectés par les moyens de comparaison est supérieur à un seuil prédéterminé (K_{TH}).

25 14. Système, pour la mise en œuvre du procédé selon l'une des revendications 1 à 12, pour détecter une intrusion dans une communication de données privées entre une pluralité d'entités communicantes via un réseau de télécommunication,

* la communication étant effectuée par transmission de paquets successifs, chaque paquet comportant au moins :

- un champ d'en-tête incluant au moins une adresse de source du paquet et/ou une adresse de destination du paquet pour un routage approprié des paquets,
- et un corps de paquet incluant des données privées,

* ladite intrusion consistant au moins à :

- s'interconnecter entre une première et une seconde entité,
- usurper l'adresse de la première entité et/ou l'adresse de la seconde entité en tant qu'adresse de source et/ou de destination, et
- détourner ainsi les paquets pour récupérer notamment les données privées,

caractérisé en ce qu'elle comporte une pluralité de sondes formant une architecture de contrôle du réseau, chaque sonde comportant :

- des moyens de comparaison des corps de paquet, propres à détecter au moins un premier paquet et un second paquet, transmis à des instants respectifs distincts entre les première et seconde entités, et comportant des corps de paquet identiques,
- et des moyens de déclenchement d'une alarme si un nombre de paquets dont le corps est identique et détectés par les moyens de comparaison est supérieur à un seuil prédéterminé (K_{TH}).

15. Programme d'ordinateur, pour la mise en œuvre du procédé selon l'une des revendications 1 à 12, téléchargeable via un réseau de télécommunication et/ou destiné à être stocké dans une mémoire d'une sonde et/ou stocké sur un support mémoire destiné à coopérer avec un lecteur de ladite sonde,

ladite sonde étant agencée pour détecter une intrusion dans une communication de données privées entre une première et une seconde entité, communicantes via un réseau de télécommunication,

5 * la communication étant effectuée par transmission de paquets successifs, chaque paquet comportant au moins :

- un champ d'en-tête incluant au moins une adresse de source du paquet et/ou une adresse de destination du paquet pour un routage approprié des paquets,
- et un corps de paquet incluant des données privées,

10 * ladite intrusion consistant au moins à :

- s'interconnecter entre la première et la seconde entité,
 - usurper l'adresse de la première entité et/ou l'adresse de la seconde entité en tant qu'adresse de source et/ou de destination, et
 - détourner ainsi les paquets pour récupérer notamment les données
- 15 privées,

caractérisé en ce que le programme comporte des instructions pour, lorsqu'il est exécuté à partir d'une mémoire de la sonde :

- a) détecter au moins un premier paquet et un second paquet, transmis à des instants respectifs distincts entre la première et la seconde entité, et
- 20 comportant des corps de paquet identiques,
- b) et déclencher une alarme si un nombre de paquets détectés dont le corps est identique est supérieur à un seuil prédéterminé (K_{TH}).

25 16. Support de stockage de données comportant des instructions de code de programme informatique pour l'exécution des étapes d'un procédé selon l'une quelconque des revendications 1 à 12.

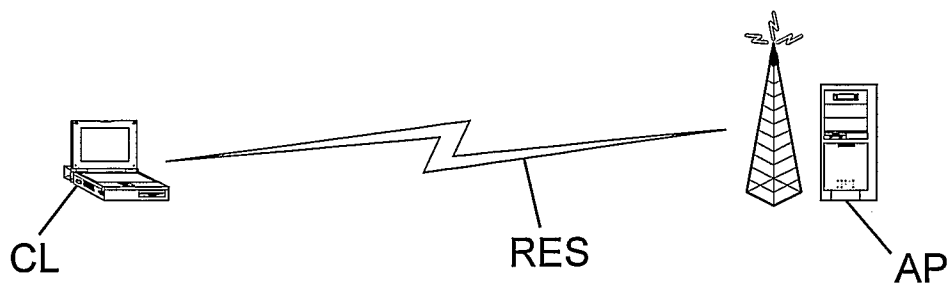


FIG. 1

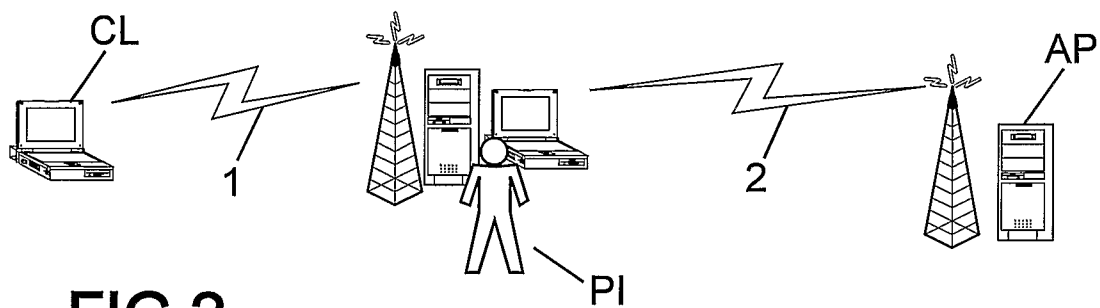


FIG. 2

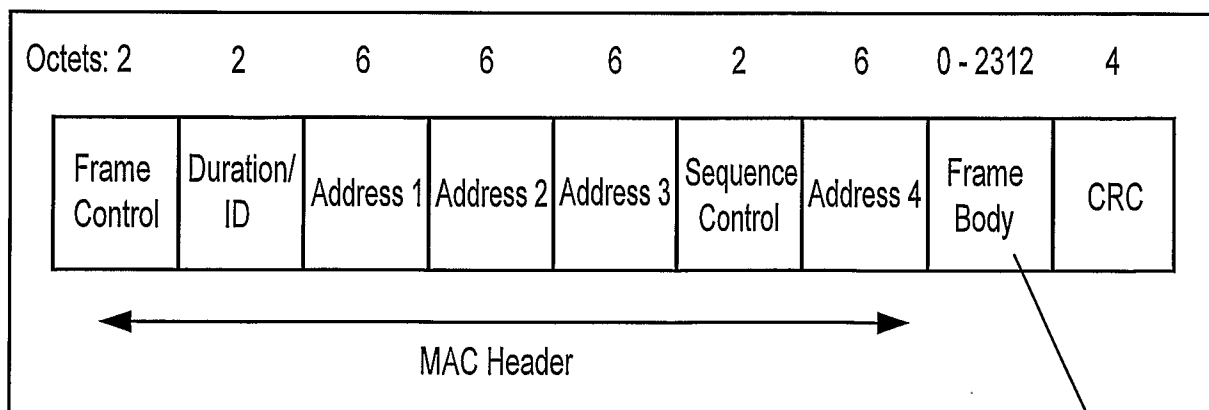


FIG. 3

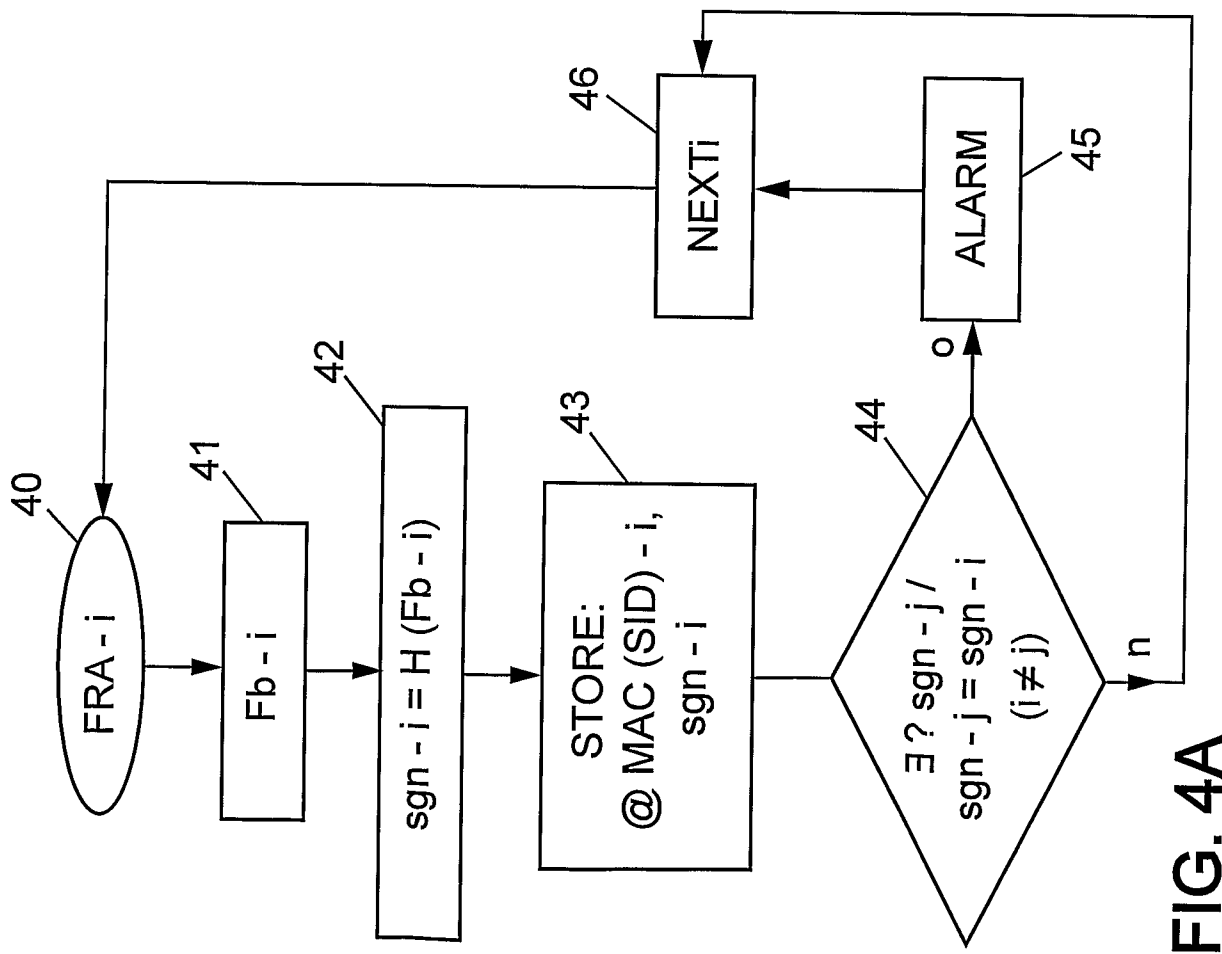


FIG. 4A

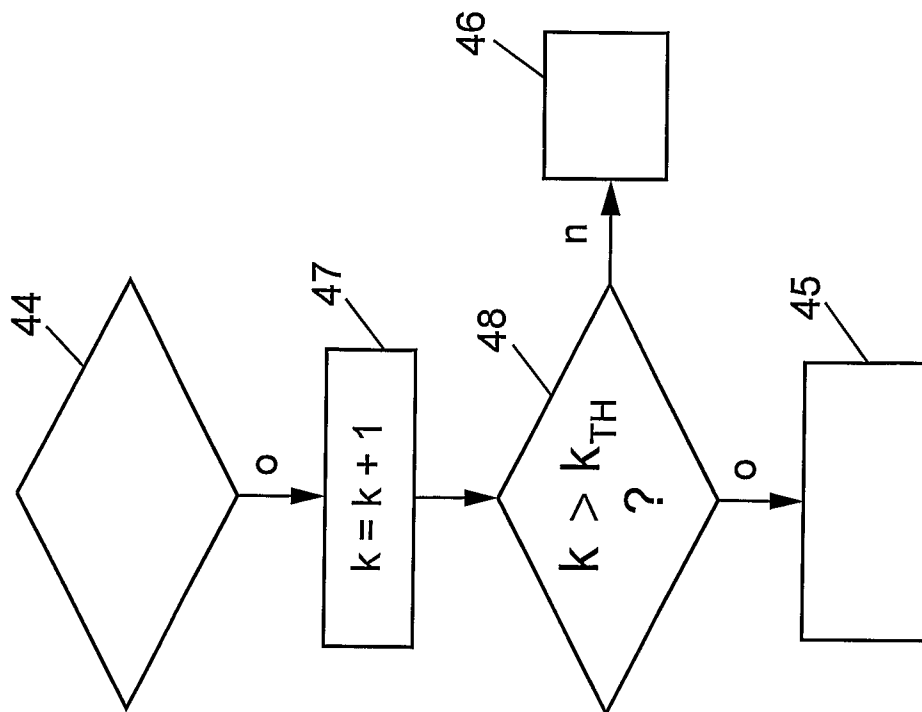


FIG. 4B

FIG.5

