ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) BREVET D'INVENTION

(11) N° de publication :
MA 42357 B1

(51) Cl. internationale :
H04W 4/00

(43) Date de publication :
28.02.2020

(21) N° Dépôt :
42357

(22) Date de Dépôt :
07.05.2018

(71) Demandeur(s) :
Université Mohammed V - RABAT, Avenue des Nations Unies, Agdal, bp 8007 NU, Rabat, 10000 (MA)

(72) Inventeur(s) :
Habbani Ahmed ; El mahdi fatna ; BENJBARA CHAIMAE

(74) Mandataire :
Kartit Zaid

(54) Titre : **Procédé de localisation et isolation des trous noirs dans un réseau mobile Ad Hoc**

(57) Abrégé : L'attaque du trou noir est considérée comme menace à la disponibilité du service dans les réseaux Ad Hoc. Pour lutter contre ce type d'attaque, la présente invention fournit une solution qui, en se basant sur la méthode de Shamir, permet à la destination de vérifier l'intégrité du message reconstruit à partir des différentes combinaisons des fragments reçus. Ainsi la destination et la source échangent les informations concernant le comportement des nœuds et identifient celles qui ne collaborent pas correctement à la transmission. Ceci permettra aux nœuds de détecter les chemins qui contiennent des trous noirs et ceux qui contiennent des nœuds malicieux qui modifient les messages. En appliquant ce procédé, chaque nœud broadcaste, dans le réseau, l'information qui a pu construire sur les chemins. Les autres nœuds, profitent de ces informations diffusées pour appuyer leurs propres jugements et pouvoir localiser et isoler, d'une manière progressive, les trous noirs et les nœuds malicieux capables de modifier les données.

ABRÉGÉ

L'attaque du trou noir est considérée comme menace à la disponibilité du service dans les réseaux Ad Hoc. Pour lutter contre ce type d'attaque, la présente invention fournit une solution qui, en se basant sur la méthode de Shamir, permet à la destination de vérifier l'intégrité du message reconstruit à partir des différentes combinaisons des fragments reçus. Ainsi la destination et la source échangent les informations concernant le comportement des nœuds et identifient celles qui ne collaborent pas correctement à la transmission. Ceci permettra aux nœuds de détecter les chemins qui contiennent des trous noirs et ceux qui contiennent des nœuds malicieux qui modifient les messages.

En appliquant ce procédé, chaque nœud broadcaste, dans le réseau, l'information qui a pu construire sur les chemins. Les autres nœuds, profitent de ces informations diffusées pour appuyer leurs propres jugements et pouvoir localiser et isoler, d'une manière progressive, les trous noirs et les nœuds malicieux capables de modifier les données.

Titre : Procédé de localisation et isolation des trous noirs dans un réseau mobile Ad Hoc

Description :

Domaine technique :

La transmission est la base du routage dans tous les types des réseaux, il permet à une source d'envoyer un message à une destination qui appartient au même réseau. La présente invention concerne le domaine de la sécurité de la transmission des réseaux de communication sans infrastructure MANET.

Plus précisément, elle concerne un procédé d'identification, de détection, et de localisation & isolation des trous noirs afin d'assurer la confidentialité, l'intégrité et la disponibilité des messages échangés dans un réseau ad hoc.

ETAT antérieur :

Un réseau ad-hoc comprend des plates-formes mobiles appelées nœuds qui sont libres de se déplacer sans contrainte. Un réseau ad-hoc est donc un système autonome. Ce système peut fonctionner d'une manière isolée ou s'interfacer à des réseaux fixes à travers des passerelles.

La différence entre le mode ad-hoc et le mode infrastructure est que dans le second, toutes les communications passent par un point d'accès qui sécurise et organise l'échange des paquets, alors que dans le premier mode la communication entre deux machines se fait soit directement si elles se trouvent à la portée l'une de l'autre, soit de faire passer ses données par une ou plusieurs machines intermédiaires jusqu'à l'arrivé à la destination, parce que chaque station peut se retrouver à jouer le rôle d'un routeur.

Il est clair donc qu'il est primordial d'utiliser un protocole de routage afin de déterminer le chemin optimal entre la source et la destination en prenant en considération la mobilité des nœuds.

Il y a trois types de protocole de routage dans les réseaux MANET, le premier nommé « proactif » comme son nom indique, les nœuds établissent les routes à l'avance, contrairement au deuxième type « réactif » où les nœuds déterminent la route uniquement sur demande, et le troisième type « hybride » combine des aspects des routages proactifs et réactifs.

Dans les trois types de protocoles de routage dans les réseaux MANET la transmission de donnée se passe à travers les nœuds intermédiaires, à cette étape de transfert de donnée, le paquet qui encapsule cette donnée est susceptible aux plusieurs attaques qui menacent :

- **La confidentialité** si les nœuds intermédiaires lisent le contenue des messages qu'ils les acheminent
- **L'intégrité** si les nœuds intermédiaires changent le contenu des messages avant de les transmettre
- **La disponibilité** si les nœuds intermédiaires suppriment les messages et ne collaborent pas à l'acheminement des paquets.

Ce type de réseau permet de déployer, rapidement et n'importe où, un réseau sans fil. Le fait de ne pas avoir besoin d'infrastructure, autre que les stations et leurs interfaces, permet d'avoir des nœuds mobiles. D'un point de vue militaire, c'est très intéressant. Sur le champ de batailles, même si une partie des équipements est détruite, il est toujours possible de communiquer. On imagine aussi, l'intérêt lors des catastrophes naturelles, tel que les tremblements de terre. Les réseaux ad-hoc permettent d'établir très rapidement un système de communication.

Vue qu'on souhaite échanger des données sensibles, et on veut qu'elles arrivent à la personne exacte sans qu'elle soit ni divulgué, ni modifié, ni supprimé, donc on doit s'assurer de la fiabilité de transmission entre les nœuds.

Plusieurs recherches ont été effectuées pour sécuriser la communication dans les réseaux. Mais celles qui utilisent la méthode de Shamir pour partager le massage sur n parties avec un seuil k avant de

l'envoyer, elles se focalisent sur la confidentialité de la transmission, et la reconstitution du message chez la destination à partir de k parties reçus, et ne montrent pas comment vérifier l'intégrité du message reconstruit, elles ne permettent pas de détecter les chemins qui suppriment ou qui modifient quelques parties du message, donc elles ne aident pas à localiser les nœuds malveillants qui suppriment ou qui modifient les messages au cours de la transmission.

Brève description des figures :

La figure 1 représente la vue générale sous forme d'organigramme des trois étapes Identification, Détection, Localisation et Isolation

La figure 2 représente l'organigramme de la première étape qui est l'Identification

La figure 3 représente l'organigramme de la deuxième étape qui est la Détection

La figure 4 représente l'organigramme de la troisième étape qui est la Localisation et l'Isolation

La figure 5 représente un exemple scénario

Description détaillée :

Notre invention se base sur trois étapes essentielles pour assurer la disponibilité, la confidentialité et l'intégrité, ces trois étapes **Identification**, **Détection**, **Localisation** & **isolation** viennent après l'étape d'initialisation qui existe dans l'état de la technique :

Etapes d'initialisation : où chaque nœud source marquer n chemins vers la destination, Soit **P**n l'ensemble des chemins entre S et D, n variable d'un nœud à un autre selon le voisinage de chaque nœud, puis choisit le seuil de la méthode Shamir k (k =< n), k aussi variable selon le nombre n et le nombre des chemins nœud-disjoints, la source fragmente le message à communiquer sur n fragments selon la méthode de Shamir, et encapsule chaque fragment dans un paquet, puis envoyer chaque paquet dans un chemins, la destination reçoit r paquets (r =< n)

Etape d'identification (1):

La destination va recevoir r fragments du message

- Si r=0 : (11)

La destination n'a rien reçu, donc elle ne peut pas reconstruire le message M envoyé par S, donc l'ensemble des versions du message **V**m est vide **V**m = Ø. Donc la source S déclare que tous les chemins Pi ($1 \leq i \leq n$) Pi$\in$**P**n peuvent contenir des trous noirs, regroupe ces chemins dans un ensemble **ζ**tn= **P**n et affecte la valeur 1 au coefficient de trous noir à tous les nœuds qui constituent ces chemins,

- Si $0 < r < k$: (12)

La destination ne peut pas reconstruire le message M envoyé par S, **V**m = Ø et déclare l'ensemble **P**r des chemins à travers lesquels elle a reçu des paquets comme des chemins qui collaborent à la transmission, et envoie cette ensemble à la source pour quelle renvoie les fragments manquants dans ces chemins,

La source revient à l'étape d'initialisation et recalcule n et k de telle sorte que n devient égale à r et $k \leq n=r$, la source détecte donc les chemins qui peuvent contenir des trous noirs, et les regroupe dans un ensemble **ζ**tn où **ζ**tn = **P**n – **P**r et affecte la valeur 1 au coefficient de trous noir à tous les nœuds qui constituent ces chemins, puis partage cet ensemble avec la destination D

- Si r=k : (13)

La destination D peut reconstruire une version du message M en utilisant le polynôme de Lagrange, le cardinale de l'ensemble Vm égale à 1 card(**V**m) = 1, et déclare l'ensemble **P**r des chemins dont elle a reçu des paquets comme des chemins qui collaborent à la transmission, et envoie cette information à la source

La source détecte donc les chemins qui peuvent contenir des trous noirs, et les regroupe un ensemble **ζ**tn où **ζ**tn = **P**n – **P**r et affecte la

valeur 1 au coefficient de trous noir à tous les nœuds qui constituent ces chemins, puis partage cet ensemble avec la destination D

∀ Pi∈ **ζ**tn ∀ N ∈ Pi TN (N) = 1

➢ Si k +1 ≤ r ≤ n : (14)

La destination déclare l'ensemble **P**r des chemins dont elle a reçu des paquets comme des chemins qui collaborent à la transmission, et envoie cette information à la source.

La source détecte donc les chemins qui peuvent contenir des trous noirs, et les regroupe dans un ensemble **ζ**tn où **ζ**tn = **P**n – **P**r et affecte la valeur 1 au coefficient de trous noir TN à tous les nœuds qui constituent ces chemins, et affecte la valeur 1 au coefficient de non fiable NF à tous les nœuds qui constituent les chemins non fiables **ζ**nf envoyés par la destination, puis la source envoie l'ensemble **ζ**tn à la destination D,

∀ Pi∈ **ζ**tn ∀ N ∈ Pi TN (N) = 1

La destination utilise le polynôme de Lagrange pour calculer le message de départ envoyé par la source. Le polynôme de Lagrange associé s'écrit :

$$L(0) = \sum_{j=0}^{k-1} f(x_j) \prod_{\substack{m=0 \\ m \neq j}}^{k-1} \frac{x_m}{x_m - x_j}$$

Elle va reconstruire plusieurs versions du message en combinant k fragments reçu, et les comparer entre eux en utilisant l'algorithme de combinaison pour s'assurer de l'intégrité.

Algorithme de combinaison

Soit i = partie_entière_sup (r / k) la partie entière supérieure (Round up)

Donc la destination calcule les combinaisons possibles qui couvrent tous les éléments de notre ensemble {F1, F2, … Fr}

En totalité en a le nombre suivant des combinaisons possibles $C_r^k = \frac{A_r^k}{k!} = \begin{cases} 0, si\ k > r \\ \frac{r!}{k!(r-k)!}, si\ 0 \leq k \leq r \end{cases}$

Mais pour optimiser le calcul des combinaisons nécessaires pour vérifier l'intégrité on va calculer juste i combinaisons de telle sorte de parcourir la liste des fragments du message avec un pas de k

$C1 = L\ (F1, \ldots Fk)$

$C2 = L\ (F(k+1), \ldots F2k\ )$

…

$Ci = \begin{cases} L\ (F(i-1)k+1, \ldots\ Fik\ ) & si\ r\ multiple\ de\ k \\ L\ (les\ k\ derniers\ fragments) & sinon \end{cases}$

Ensuite la destination va comparer les Ck :

1≤ k ≤ i = partie_entière_sup(r/k)

- Si tous les Ck ne sont pas égaux, (141) donc tous les chemins Pj responsables à l'acheminement des fragments Fj 1 ≤ j ≤ r sont des chemins non fiables. Donc la destination ne peut pas reconstruire le message M envoyé par la source et déclare la liste des chemins non fiables

ζf = Ø

•j 1≤ j ≤ r ζnf = {Pj}

- Si tous les Ck sont égaux, (142) donc tous les chemins Pj responsables à l'acheminement des fragments Fj 1 ≤ j ≤ r sont des chemins fiables, et le message initiale envoyé par la source égale à Cl

•k 1≤ l ≤ i Cl=M

Donc la destination reconstruit correctement le message envoyé par la source et déclare la liste des chemins fiables

•j 1≤ j ≤ r ζf = {Pj}

ζnf = Ø

- S'il y a des combinaisons différentes aux autres, et au moins deux combinaisons égaux, (143), donc les combinaisons

égaux Cfl (1≤ l ≤ i) sont des combinaisons correctes égales au message M, donc les fragments qui constituent ces combinaisons fiables sont forcément tous des fragments fiables Fflj (1≤ j ≤ k). Et les combinaisons différentes Csspt (1≤ t ≤ i) sont des combinaisons suspects constituent par des fragments suspects Fssptj (1≤ j ≤ i), c'est pour cela on passe à la deuxième étape pour localiser le / les fragments non fiables qui ont été modifié au cours de la transmission et qui donnent des combinaisons différentes.

Cfl = L (Ff(l-1)k+1, … Fflk) (1≤ l ≤ i) i = partie_entière_sup(r/k)

Csspt = L (Fsspt(t-1)k+1, … Fssptk) (1≤ t ≤ i)

Parce que une combinaison différente au autre ne confirme pas que tous les k fragments qui constituent cette combinaison sont tous non fiables, il se peut qu'un fragment (ou plusieurs) qui a été modifié, et qui donne cette combinaison différente

Etape de detaction: (2)

(21) La destination regroupe dans un ensemble **F**f (Fragments fiables) les fragments Fflj (1≤ l ≤ i et 1≤ j ≤ k) qui constituent des combinaisons égaux et fiable Cfl (1≤ l ≤ i), ensuite regroupe dans un autre ensemble **F**ssp (Fragments suspects) les fragments Fssptj (1≤ t ≤ i et 1≤ j ≤ k) qui donnent des combinaisons différentes aux autres Csspt (1≤ t ≤ i) combinaison suspcet, puis élimine de **F**ssp tous les fragments fiables qui appartiennent à **F**f de telle sorte qu'on aura toujours **F**f ∩ **F**ssp = Ø.

Par la suite la destination effectue des permutations d'un et un seul fragment suspect Fssptj∈**F**ssp qui donne une combinaison différente aux autres Csspt, avec un fragment fiable Fflj∈**F**f qui constitue une combinaison fiable Cfl, la permutation donne deux combinaisons

Cp1 = L (Ff(l-1)k+1, … Fssptj, …. Fflk)

Cp2 = L (Fsspt(t-1)k+1, … Fflj, …. Fssptk)

1≤ l ≤ i 1≤ t ≤ i i = partie_entière_sup(r/k)

Et à chaque fois la destination compare les combinaisons trouvés Cp1 et Cp2 avec l'une des combinaisons fiables Cfl par exemple,

- Si Cp1 ≠ Cfl et Cp2 ≠ Cfl : (211)

Donc on est sûr maintenant que Fssptj est un fragment non fiable, et qui a été modifié au cours de la transmission, parce qu'il donne une combinaison non correcte avec des fragments fiables.

La destination donc mis à jour les deux ensembles **F**nf et **F**ssp, elle élimine le fragment non fiable Fssptj de l'ensemble **F**ssp et on les met dans l'ensemble **F**nf, elle revient à l'étape (21) pour appliquer la permutation aux fragments suspects restants dans Cp2

- Si Cp1 ≠ Cfl et Cp2 = Cfl : (212)

Donc on est sûr maintenant que Fssptj est un fragment non fiable qui a été modifié au cours de la transmission, et que tous les fragments de Cp2 sont des fragments fiables

La destination donc mis à jour les ensembles **F**f, **F**nf et **F**ssp, elle élimine le fragment non fiable Fssptj de l'ensemble **F**ssp et on les met dans l'ensemble des fragments non fiables **F**nf, et elle élimine tous fragments suspect de Cp2 de l'ensemble **F**ssp et on les met dans l'ensemble des fragments fiables **F**f et on revient à (22) pour vérifier si on a balayé tous les fragments suspects de **F**ssp

- Si Cp1 = Cfl et Cp2 ≠ Cfl : (213)

Donc on est sûr maintenant que Fssptj est un fragment fiable qui n'a pas été modifié au cours de la transmission, et qu'il y a encore des fragments suspects de Cp2

La destination donc mis à jour les deux ensembles **F**f, **F**ssp, elle élimine le fragment fiable Fssptj de l'ensemble **F**ssp et elle le met dans l'ensemble des fragments fiables **F**f, elle revient à (22) pour vérifier si on a balayer tous les fragments suspects de **F**ssp

- Si **F**ssp = Ø (22)

Donc la destination a classé tous les fragments suspects dans deux ensembles, ensemble des fragments fiables **F**f, et ensemble des fragments non fiables **F**nf

Ff = {fragment de combinaison Cl tq ∀o 1≤ l ≠ o ≤ i Cl=Co=M}

Fnf = {fragment de combinaison Cl' tq ∀o' 1≤ l' ≠ o' ≤ i Cl'≠Co'≠M}

Puis la destination localise l'ensemble **ζ**nf des chemins responsables de l'acheminement des fragments non fiables qui appartiennent à Fnf, ensuite elle incrémente à tous les nœuds de ces chemins l'indice de non fiabilité avec 1

∀ Pi∈ **ζ**nf ∀ N ∈ Pi NF (N) = 1

La destination envoie à la source les ensembles **ζ**f et **ζ**nf des chemins fiables et non fiables.

Finalement, chaque nœud broadcaste l'information des coefficients TN trous noir et NF non fiable des nœuds dans tout le réseau,

Etape de localisation et isolation: (3)

Le broadcaste des informations sur les nœuds qui existent dans le réseau, leurs coefficients de trou noir et de non fiabilité, les chemins non fiables **ζ**nf et les chemins trous noirs **ζ**tn, permet de localiser exactement les nœuds trous noirs et non fiables.

Tant qu'il y a des intersections entre les chemins trous noirs, donc il y a plusieurs nœuds qui votent que le nœud d'intersection est un trou noir et qui a un coefficient de trou noir ≠ 0, donc tous les nœuds du réseau isole ce nœud et le considère un trou noir, la même chose pour les nœuds suspect d'être des nœuds non fiables qui modifient l'information avant de la transmettre

On initialise à tous les nœuds du réseau les coefficients trou noir TN et non fiable NF à 0

∀N Nœud du réseau TN(N)=0 NF(N)=0

Soit N un nœud du réseau qui a reçu un nombre Ktn (seuil trou noir) de messages de différentes sources qui disent qu'un nœud X il a le coefficient de trou noir TN(X) égale à 1, donc le nœud N considère que X est un trou noir, et il va l'isoler, et broadcaste cette information dans tout le réseau.

La même chose lorsqu'un nœud N a reçu un nombre Knf (seuil non fiabilité) de messages de différentes sources qui disent qu'un nœud X il a le coefficient de non fiable NF(X) égale à 1, donc le nœud N considère que X est un nœud non fiable qui modifie l'information avant de la transmettre, et il va l'isoler, et broadcaste cette information dans tout le réseau.

Exemple:

Soit n=12 et k=4 et r=11

La source découpe de message M par la méthode de Shamir sur n=12 fragments F1', … F12' avec un seuil k=4 et envoie chaque fragment Fi dans un chemin Pi,

Pn={P1, P2, P3, P4, P5, P6, P7, P8, P9, P10, P11, P12}

La destination reçoit r=11 fragments F1, … F11

Pr={P1, P2, P3, P4, P5, P6, P7, P8, P9, P10, P11 }

i= partie_entière_sup (11/4) = partie_entière_sup(2,75) = 3

C1={F1,F2,F3,F4}

C2={F5,F6,F7,F8}

C3={F8,F9,F10,F11}

C1=C2≠C3 de C1 et C2 sont deux combinaisons correctes égale au message M envoyé par la source, et C3 combinaison non correcte

Ff= {F1,F2,F3,F4,F5,F6,F7,F8}

Fssp= {F8,F9,F10,F11} puisque F8∈**Ff** donc **Fssp**={F9,F10,F11} et **F**nf= Ø

Permuter F9 de la combinaison non correcte C3 avec F2 de la combinaison correcte C1

Cp1= {F1,F9,F3,F4} Cp1'={F8,F2,F10,F11}

Cp1 ≠C1 Donc on est sûr que le fragment F9 a été modifié au cour de la transmission, alors **F**f= {F1,F2,F3,F4,F5,F6,F7,F8} **F**nf={F9} et **Fssp**={F10,F11}

Cp1' ≠C1 Donc on n'est pas sûr que les deux fragments F10 et F11 sont tous les deux non fiables ou un parmi eux, pour cela ou va répéter une autre permutation de F10 de la nouvelle combinaison Cp1' qui contient deux fragments correcte F8 et F2 et deux autres fragments suspects F10 et F11, avec F3 de C1

Cp2= {F1,F2,F10,F4} Cp2'={F8,F2,F3,F11}

Cp2= C1 Donc on est sûr que le fragment F10 n'a pas été modifié au cour de la transmission, donc F10 est correct,

Alors **Ff**= {F1,F2,F3,F4,F5,F6,F7,F8,F10}, **F**nf={F9} et **Fssp**={F11}

Cp2' ≠C1 Donc on est sûr que le fragment F11 a été modifié au cour de la transmission, alors **Ff**= {F1,F2,F3,F4,F5,F6,F7,F8,F10} **F**nf={F9,F11} et **Fssp**= Ø donc on s'arrête ici

REVENDICATIONS :

1. Procédé de routage à base de la méthode de Shamir dans les réseaux mobiles Ad Hoc pour détecter les nœuds malicieux comprenant les étapes suivantes :

- Etape d'identification
  a) Un protocole de routage multi-chemins fourni au nœud source n chemins disponibles, ledit nœud applique la méthode de Shamir pour fragmenter le message en ledit n parties avec un seuil k (k = < n) ; chacun desdits fragments est envoyé sur un seul desdits chemins.
  b) Le nœud destination procède à la reconstitution d'au moins deux versions du message à partir de k combinaisons de fragments pour vérifier l'intégrité du message émis ; marque les chemins à partir du quels la destination a reçu les fragments (Fi) avec intégrité validée, comme des chemins fiables (Cf)
  c) Le nœud destination communique à la source la liste des chemins (Pr) à travers lesquels il a reçu les fragments reçus et la liste des chemins fiables (Cf),
  d) La source et la destination marquent les chemins liés aux fragments manquants qui n'appartiennent pas à l'ensemble des chemins qui collaborent à la transmission Pr; lesdits chemins constituent une liste noire **C**tn = Pn – Pr
  e) La destination calcule des combinaisons des fragments reçus afin de vérifier l'intégrité desdits fragments, et regroupe ces fragments en deux ensembles, ensemble des fragments fiables Ff et ensemble des fragments suspects Fssp qui donnent des combinaisons différentes, si un fragment appartient en même temps à Ff et Fssp, donc la destination élimine ce fragment de Fssp et le considère appartenir à Ff

- Etape de détection

a) La destination effectue des permutations d'un et un seul fragment suspect dudit ensemble **F**ssp avec un fragment fiable dudit ensemble **F**f

b) Si la combinaison qui contient que des fragments fiables et un seul fragment suspect est égale aux combinaisons du message correcte, la destination élimine ce fragment suspect de l'ensemble Fssp et l'insert dans l'ensemble des fragments fiables Ff, sinon la destination élimine ce fragment de l'ensemble Fssp et l'insert dans un ensemble des fragments non fiable Fnf

c) La destination détecte l'ensemble des chemins fiable Cf à partir des quels elle a reçu des fragments fiables, et l'ensemble des chemins non fiable Cnf dont elle a reçu des fragments non fiables modifié au cours de transmission, et transmit ces deux ensembles à la source

d) Pour chaque nœud, s'il trouve un autre nœud dans un chemin qui appartient à Ctn donc il affecte la valeur 1 au coefficient TN de ce nœud, sinon ce coefficient prend la valeur 0, la même chose s'il trouve qu'un nœud fait partie d'un chemin qui appartient à Cnf donc il lui affecte la valeur 1 pour le coefficient NF, sinon cette valeur reste 0, puis il diffuse cette information dans le réseau,

- Etape de localisation & d'isolation

a) Chaque nœud calcule la valeur moyenne des coefficients TN et NF à partir de nombre d'occurrence du nœud dans les ensembles Ctn et Cnf constatés, et à partir des listes Ctn et Cnf reçus, et mettre à jour ces coefficients,

b) Après un certain nombre de communication, chaque nœud vérifie la valeur des coefficients TN et NF qui varie entre 0 et 1 ; les nœuds fiable ont lesdits coefficients TN et NF qui tendent vers 0 ; les nœuds malicieux ont lesdits coefficients TN et NF qui tendent vers 1.

c) Chaque nœud dans le réseau compare les coefficients TN et NF avec le seuil trou noir Ktn et avec le seuil non fiabilité Knf pour créer une liste noir des nœuds trou noir et des nœuds non fiable.

2. Le procédé selon la revendication 1 caractérisé en ce que les paramètres de ladite méthode Shamir sont dynamiques ; ledit paramètres n est recalculé en fonction de nombre de chemins initiales disponibles et le nombre de chemins fiables sans trou noir suivant les informations communiquées par la destination après chaque envoie.
3. Le procédé selon les revendications 1 et 2 caractérisé en ce qu'il utilise une méthode optimale de combinaison de k fragments pour vérifier l'intégrité du message ; le nombre i desdites combinaisons est calculé comme suit i = partie_entière_sup(r/k).
4. Le procédé selon l'une quelconques des revendications précédentes caractérisé en ce que dans la vérification d'intégrité une permutation des fragments est faite entre deux combinaisons fiable et suspecte ; ladite permutation consiste à :
    a. Dans la combinaison suspecte Cs on marque les fragments suspects Fm qui n'apparait pas audit Ff.
    b. On permute un desdits fragments Fm de ladite combinaison suspecte avec un fragment de ladite combinaison fiable Cf
    c. On compare le message reconstruit à partir de ladite nouvelle combinaison Cf avec le message d'une desdites combinaison fiable et si c'est égale le fragment est déclaré fiable sinon il déclarer malicieux.
    d. On compare le message reconstruit à partir de ladite nouvelle combinaison Cs avec le message d'une desdites combinaison fiable et si c'est égal le reste desdits fragments Fm est déclaré fiable et on arrête l'opération de détection.

Dessins et Figures

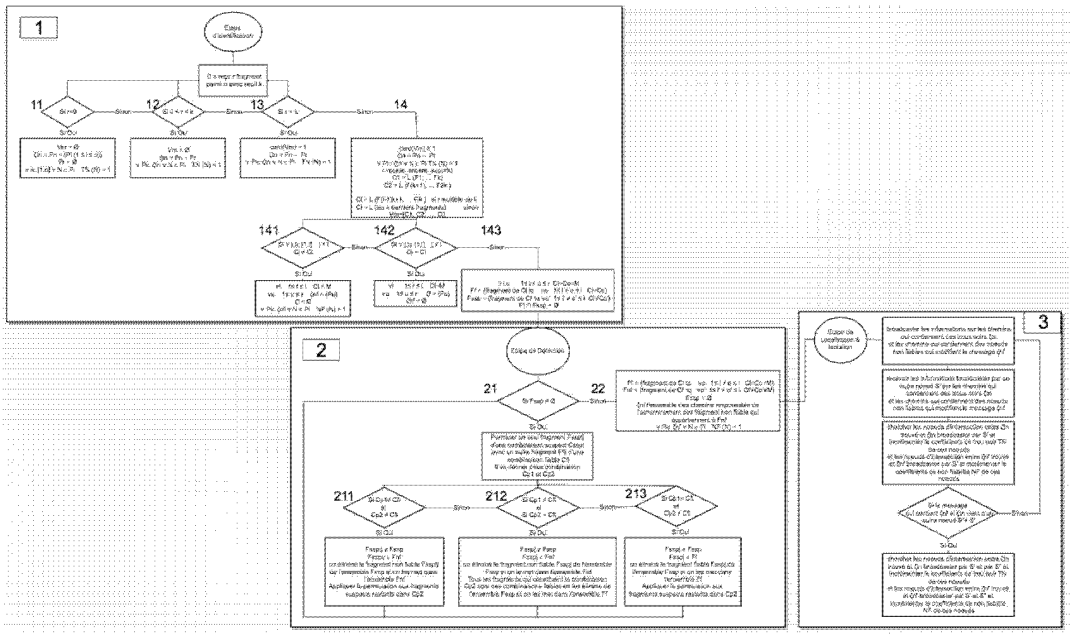

Figure 1

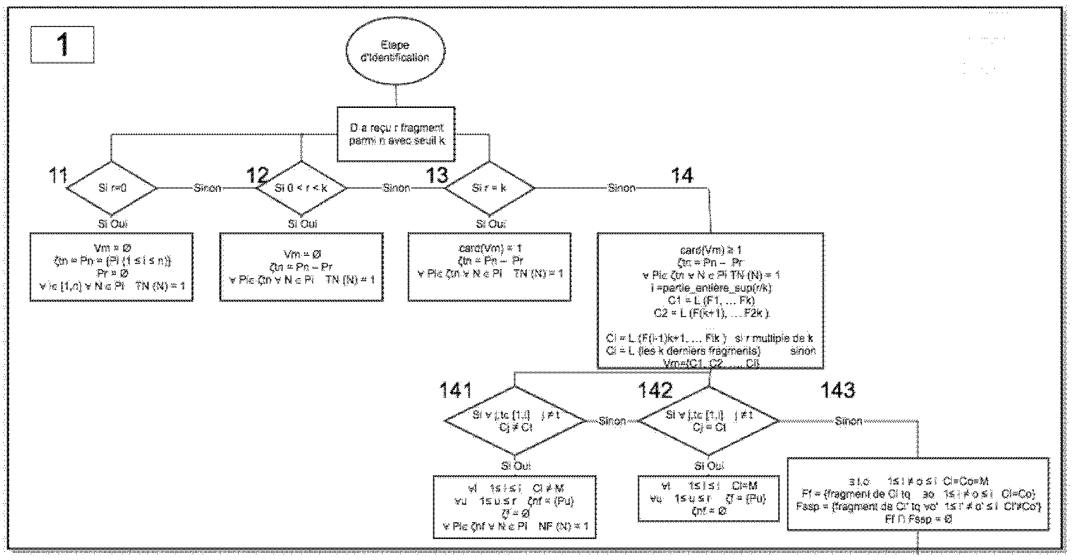

Figure 2

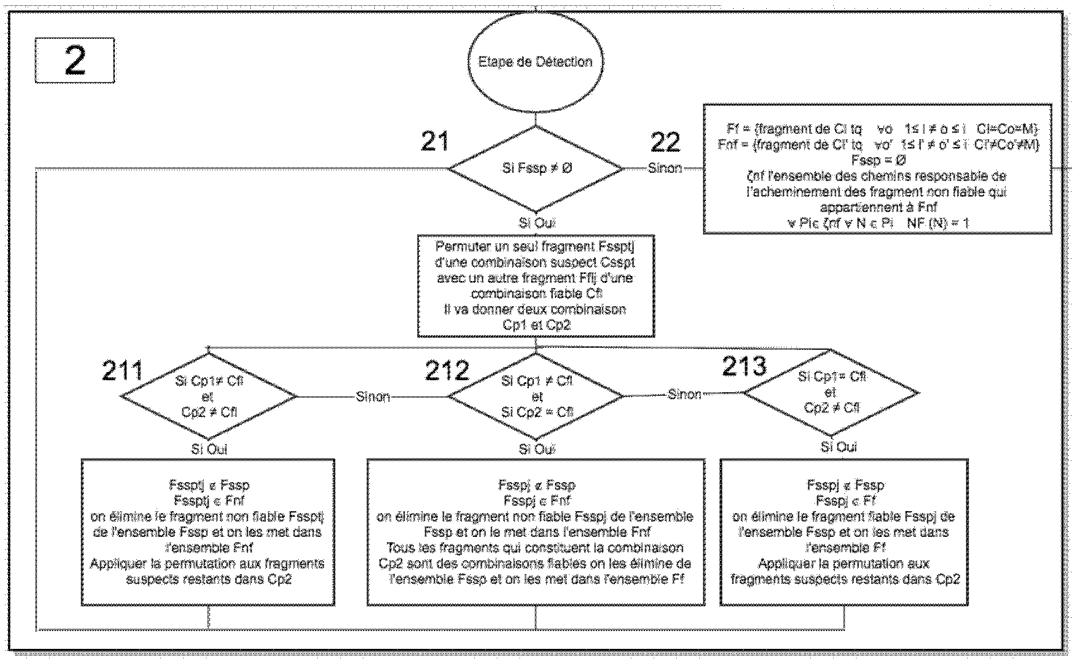

Figure 3

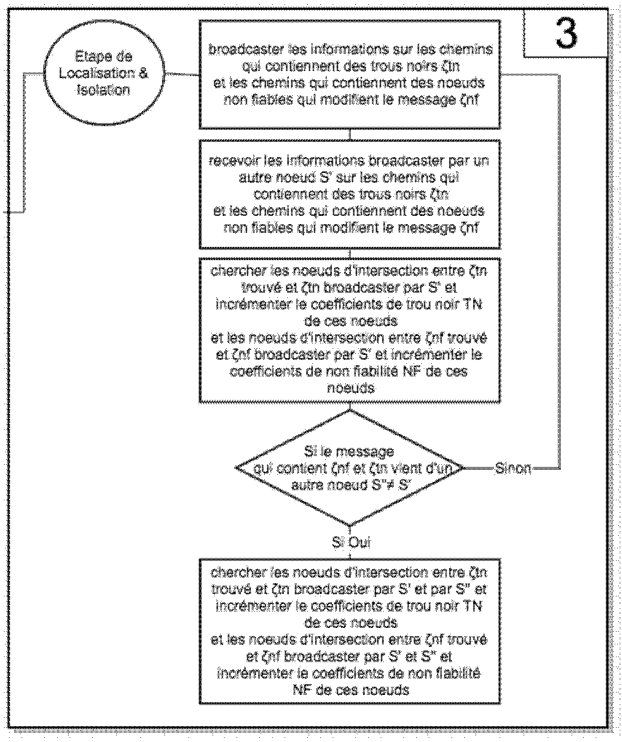

Figure 4

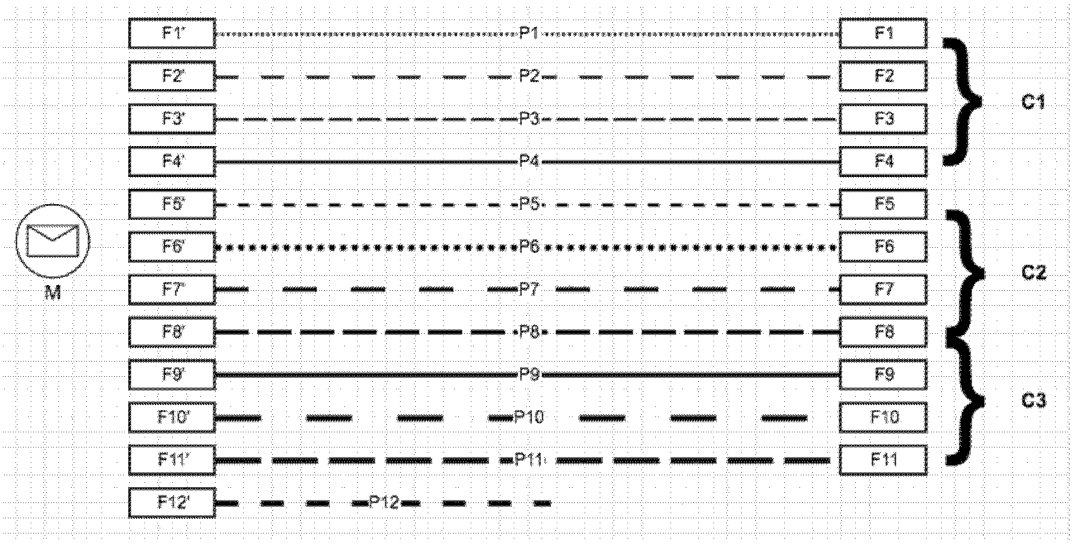
F1'
F2'
F3'
F4'
F5'
F6'
F7'
F8'
F9'
F10'
F11'
F12'
P1
P2
P3
P4
P5
P6
P7
P8
P9
P10
P11
P12
F1
F2
F3
F4
F5
F6
F7
F8
F9
F10
F11
C1
C2
C3
M

Figure 5

ROYAUME DU MAROC
****
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
****

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

RAPPORT DE RECHERCHE AVEC OPINION SUR LA BREVETABILITE

(Conformément aux articles 43 et 43.2 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13)

Renseignements relatifs à la demande	
N° de la demande : 42357	Date de dépôt : 07/05/2018
Déposant : Université Mohammed V - RABAT	
Intitulé de l'invention : Procédé de localisation et isolation des trous noirs dans un réseau mobile Ad Hoc	

Le présent document est le rapport de recherche avec opinion sur la brevetabilité établi par l'OMPIC conformément aux articles 43 et 43.2, et notifié au déposant conformément à l'article 43.1 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13.

Les documents brevets cités dans le rapport de recherche sont téléchargeables à partir du site http://worldwide.espacenet.com, et les documents non brevets sont joints au présent document, s'il y en a lieu.

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales
- ☒ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité
- ☐ Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés

Partie 2 : Rapport de recherche

Partie 3 : Opinion sur la brevetabilité
- ☐ Cadre 4 : Remarques de clarté
- ☒ Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle
- ☐ Cadre 6 : Observations à propos de certaines revendications dont aucune recherche significative n'a pu être effectuée
- ☐ Cadre 7 : Défaut d'unité d'invention

Examinateur: BAMI MOHAMMED	**Date d'établissement du rapport** : 30/10/2018
Téléphone: **212 5 22 58 64 14/00**	ROYAUME DU MAROC OMPIC CASABLANCA

Partie 1 : Considérations générales

Cadre 1 : base du présent rapport

Les pièces suivantes de la demande servent de base à l'établissement du présent rapport :

- Description
  11 Pages
- Revendications
  1-4
- Planches de dessin
  3 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : H04L63/1416

Bases de données électroniques consultées au cours de la recherche :

EPOQUE, Orbit

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
A	WO2009065937A1 ; Siemens Aktiengesellschaft ; 2009-05-28	1-4
A	US8065725B2 ; CALYPTIX SECURITYNORTH CAROLINA AT CHARLOTTE THE, University of ; 2011-11-22	1-4
A	US20080140795A1 ; Motorola Solutions Inc ; 2008-06-12	1-4

***Catégories spéciales de documents cités :**

-« **X** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
-« **Y** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
-« **A** » document définissant l'état général de la technique, non considéré comme particulièrement pertinent
-« **P** » documents intercalaires ; Les documents dont la date de publication est située entre la date de dépôt de la demande examinée et la date de priorité revendiquée ou la priorité la plus ancienne s'il y en a plusieurs
-« **E** » Éventuelles demandes de brevet interférentes. Tout document de brevet ayant une date de dépôt ou de priorité antérieure à la date de dépôt de la demande faisant l'objet de la recherche (et non à la date de priorité), mais publié postérieurement à cette date et dont le contenu constituerait un état de la technique pertinent pour la nouveauté

Partie 3 : Opinion sur la brevetabilité

Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté (N)	Revendications 1-4 Revendications aucune	Oui Non
Activité inventive (AI)	Revendications 1-4 Revendications aucune	Oui Non
Possibilité d'application Industrielle (PAI)	Revendications 1-4 Revendications aucune	Oui Non

Il est fait référence aux documents suivants. Les numéros d'ordre qui leur sont attribués ci-après seront utilisés dans toute la suite de la procédure

D1 : WO2009065937A1

1. **Nouveauté (N) :**

Aucun document ne divulgue l'objet des revendications 1-4 qui est donc nouveau au sens de l'article 26 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

2. **Activité inventive (AI) :**

Le document D1 est considéré comme l'état de la technique le plus proche de l'objet de la revendication 1 et divulgue :
Un procédé de routage à base de la méthode de Shamir dans les réseaux mobiles Ad Hoc pour détecter les nœuds malicieux (voir description) par la comparaison des données issues d'un nœud source et un nœud de destination.

L'objet de la revendication 1 diffère de D1 par les étapes de l'algorithme de détection du nœud malicieux.

Le problème objectif que la présente demande se propose de résoudre peut donc être considéré comme : Fournir une alternative au procédé de D1.

Aucun document de l'état de la technique ne contient un enseignement ou une suggestion qui aurait incité l'homme du métier à adopter la solution proposée sans faire preuve d'esprit inventif.

L'objet des revendications 1-4 implique donc une activité inventive au sens de l'article 28 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

3. **Possibilité d'application industrielle (PAI) :**

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible