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 39226 A1

(51) Cl. internationale :
H04W 40/00

(43) Date de publication :
31.01.2018

(21) N° Dépôt :
39226

(22) Date de Dépôt :
26.07.2016

(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

(74) Mandataire :
FATIMA ZAOUI

(54) Titre : **Nouveau procédé multi-chemin de sécurité dans les réseaux MANET**

(57) Abrégé : Notre invention apporte une solution face aux limites de sécurité qui menace la confidentialité, l'intégrité et la disponibilité. Cette invention propose une nouvelle méthode pour trouver un nombre n variable des chemins multiples, avec un seuil égale à k, en évaluant le réseau et les points d'intersection entre les chemins. Elle permet au noeud de prendre la décision sur le nombre des chemins selon la situation, en fiabilisant les routes pour les prochaines communications.

Abrégé

Notre invention apporte une solution face aux limites de sécurité qui menace la confidentialité, l'intégrité et la disponibilité. Cette invention propose une nouvelle méthode pour trouver un nombre n variable des chemins multiples, avec un seuil égale à k, en évaluant le réseau et les points d'intersection entre les chemins. Elle permet au nœud de prendre la décision sur le nombre des chemins selon la situation, en fiabilisant les routes pour les prochaines communications.

Titre : Méthode dynamique et intelligente de routage muti-chemins

Description

Cette invention a trait au domaine des réseaux sans fil, elle concerne un procédé de routage multi chemins dans un environnement ad hoc qui fournit une nouvelle méthode qu'on applique aux dispositifs mobiles (nœuds), caractérisée en ce qu'elle permet de trouver un nombre optimal de routes d'une manière dynamique assurant l'acheminement du trafic vers la destination d'une manière sécurisée. Avec cette méthode les nœuds deviennent intelligents et capables de réagir et de prendre les bonnes décisions selon l'évolution de la topologie.

Les réseaux ad hoc sont des réseaux sans fil capables de s'organiser sans infrastructure définie préalablement. Chaque entité (nœud) communique directement avec sa voisine. Pour communiquer avec d'autres entités, il lui est nécessaire de faire passer ses données par d'autres qui se chargeront de les acheminer. Pour cela, il est d'abord primordial que les entités se situent les unes par rapport aux autres, et soient capables de construire des routes entre elles: c'est le rôle du protocole de routage. Mais ces réseaux souffrent des problèmes de sécurité, qui menacent :

- La confidentialité si les nœuds intermédiaires tentent de lire 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.

Dans l'état antérieur, les protocoles de routage multi-chemins existants ont plusieurs limites:

- Génération d'un nombre fixe de chemins multiples
- Ils ne prennent pas en considération la situation actuelle, ni les changements de topologie, ni le nombre d'intersections entre les routes trouvées.
- La génération d'un nombre fixe de chemins apporte des limitations au niveau de déploiement d'une méthode de partage
- Ils considèrent les multi-chemins comme des chemins redondants (backup)
- L'acheminement de la totalité de message sur la même route risque de menacer la confidentialité.
- une fois l'intégrité est menacé la destination rejette le message et demande sa retransmission.
- En présence d'un nœud malicieux de type trou noir (black hole) la disponibilité sera menacée.

Notre invention apporte les solutions suivantes :
L'agent (nœud F1) source applique l'algorithme I (figure 1 F1-1) afin d'évaluer le réseau et détecter la variable n qui est le nombre optimal des chemins dont il a besoin

- L'agent source fragmente le message sur n parties avec un seuil égale à k (tel que $k \leq n$) par la méthode de partage, puis encapsuler chaque partie du message dans un paquet à part, et envoyer chaque paquet dans un chemin différent.
- Notre méthode utilise la technique de partage de secret de Shamir (F1-2), qui se base sur le polynôme de Lagrange, pour découper le message chez le dispositif source sur n parties, et pour reconstruire le message initiale à partir de k parties reçus chez la destination
- A la réception d'au moins k+1 parties, la destination pourra détecter l'existence d'une menace d'intégrité en comparant l'égalité des résultats des combinaisons de k parties
- La solution en elle-même, assure à la fois la disponibilité, la confidentialité et l'intégrité des messages échangés. Plusieurs approches ont été utilisées dans ce contexte mais elles souffrent de limites dans la gestion automatique et en temps réel des paramètres dynamiques liés aux nombre des chemins à déduire qui égale au nombre total des parties « n » selon lequel on va distribuer les messages, et le seuil « k » nécessaire pour la reconstruction des messages échangés.

    - La confidentialité est assurée par le découpage du message avant d'envoyer chaque partie dans un chemin, donc même si on suppose l'existence d'une attaque de type «écoute passive » qui menace la confidentialité, l'attaquant ne sera pas capable de comprendre le message de départ parce qu'il va recevoir juste une partie
    - Le dispositif qui représente la destination sera capable de surmonter les attaques qui menacent l'intégrité dans le cas de réception d'au moins (k+1). Si le réseau dispose d'un mécanisme de détection de ce type d'attaque, la destination détecte les parties du message qui sont modifiées, et elle va reconstruire le message original à partir de k parties reçus sans modification, si on suppose que le nombre des messages modifiés ne dépasse pas (n-k)
    - La disponibilité sera assurée par la réception d'au moins k parties parmi n, dans ce cas la destination reconstruit le message de départ en se basant sur les k parties reçus. Dans ce cas on va surmonter les attaque de type trou noir si le nombre les attaquant ne dépasse pas (n-k)
- Nous proposons dans cette invention une architecture dynamique du choix des chemins, installée au niveau d'agent mobile, chose qui rend ce dernier intelligent, et capable de prendre des décisions concernant la gestion des deux paramètres déjà cités (n, k) qui ont été fixés auparavant dans toutes les simulations.
- Cette invention permet la connaissance, la prédiction et l'apprentissage des chemins :
    - Elle permet aussi au nœud destination de connaitre les chemins par lesquels il a reçue des parties du message, en les signalant comme des routes fiables, et il va envoyer cette information à la source (F1-3)
    - Les dispositifs deviennent intelligents tant qu'ils peuvent apprendre les chemins fiables qui participent à la transmission après la réception de certaines parties, et ils vont baser le choix des chemins sur cette information afin de prédire les routes dans les prochaines communications,
- Les anciennes solutions se comportent de la même façon dans les réseaux à forte mobilité que dans les réseaux quasi-statiques. Elles génèrent un nombre fixe des chemins sans prendre en considération la distribution des nœuds dans le réseau ainsi que la vitesse de mobilité. Aussi, elles ont des limitations en termes de délai et d'énergie. Notre invention a traité les faiblesses des travaux précédents, afin de proposer une approche générique capable de détecter automatiquement l'évolution des

paramètres ainsi que de s'adapter aux changements de la topologie, afin de prendre la bonne décision.

- Pour surmonter les problèmes de diminution des performances, notre procédé propose l'utilisation des « threads » afin d'attribuer chaque activité d'envoi à un processus, chose qui garantit l'envoi parallèle en temps réel, ainsi que le gain en terme de délai et en énergie.

Description des figures

Figure1 : Représente le datagramme de notre algorithme (I) qui permet la détermination du nombre variable de chemins
Figure 2 : Explique le processus d'échange de messages entre la source et la destination
Figure 3 : Donne un exemple de scénario de communication entre deux nœuds en présence des différents types d'attaques

Pseudo code :

S : la source, D : la destination.

Soient V un ensemble (fini ou infini) et E une partie de V × V (i.e., une relation sur V). Le graphe G = (V,E) est la donnée du couple (V,E). Les éléments de V sont appelés les sommets1 ou nœuds de G. Les éléments de E sont appelés les arcs2 ou arêtes de G. Si V est fini, on parlera de graphe fini.
NT : l'ensemble des nœuds qui existent dans la topologie
Ci le i i ième chemin trouvé

1) La source va effectuer l'algorithme de dijikstra afin de trouver le plus court chemin vers la destination
   Il va attribuer la valeur 1 à l'attribut visité de tous les nœuds qui constituent ce plus cours chemins
2) Si la source ou la destination sont isolées ou appartient à une région isolée
   a. Dans ce cas on affecte la valeur 1 à n et k, et programme se termine
3) Sinon
   a. on applique dijikstra multipath afin de trouver d'autres chemins possibles, en incrémentant à chaque fois la valeur visité des nœuds intermédiaires visités
4) Si les chemins trouvés sont nœuds disjoints
   a. S'il existe d'autre nœuds du premier voisinage de la source qui ne sont pas encore visité (dont la valeur visité=0)
      i. Dans ce cas on affecte la valeur 2 à n et k, et programme se termine
   b. Sinon
      i. on affecte la valeur 3 à n et k, et programme se termine (a discuter le fait d'affecter 3 à k et revenir à l'étape 3 pour calculer n)
5) Sinon on calcule x tq x= max(visité(N)) pour tout N appartient aux chemins trouvés
   a. Si x<nombre des chemins trouvé
      i. k va prendre la valeur de nombre des chemins trouvés
         n va prendre la valeur k+cte tq cte<k-x, et programme se termine
   b. sinon
      i. S'il y a encore des nœuds non visité (dont la valeur visité égale à 0)
         1. il va revenir à l'étape 3)
         Sinon n va prendre la valeur x et k prend la valeur x-1, et programme se termine

Revendications

1) Nouveau procédé de détection de nombre optimale variable des chemins comprenant :
   - Dispositif électronique qui communique avec ses voisins, et pour atteindre les autres dispositifs du réseau, il doit forcément passer par les nœuds jouant le rôle des routeurs pour acheminer les paquets.
   - Il y a deux types de paquets : des paquets de contrôle, permettant la découverte du réseau, et des paquets de données qui contient l'information utile envoyée d'un nœud source à la destination,
   - Un réseau constitué par un ensemble de nœuds qui communiquent sans infrastructure préexistante, donc il y a trois situations pour chaque nœud, il est soit une source, soit une destination, soit un routeur qui achemine le paquet vers la destination

Caractérisé en ce que le nouveau procédé fournit au dispositif électronique une pluralité de chemins optimaux qui permettent à un nœud source d'acheminer d'une manière fiable et sécurisé les messages vers la destination. Le dit procédé permet aux nœuds de réseau de déterminer le nombre des chemins n variable, avec un seuil égale à k, et permet aussi d'appliquer la méthode de partage de secret Shamir afin de diviser le message et envoyer chaque partie dans un chemin.

2) Un procédé selon la revendication 1 caractérisé en ce qu'il permet la reconnaissance, la prédiction, et l'apprentissage de situations dans un environnement mobile sans fil, et sans infrastructure, en signalant les chemins fiables.
3) Un procédé, selon les revendications 1 et 2, subdivise le message sur plusieurs parties, puis les encapsuler dans des paquets, et les envoyant vers la destination, à travers des chemins multiples. Le dit procédé utilise Shamir's secret-sharing scheme pour : (1) partager le message sur n nœuds, avec un seuil égale à k ($k \leq n$). (2) une fois reçue les parties de message, il reconstitue le message en se basant sur le polynôme de Lagrange
4) Un procédé, selon les revendications précédentes, caractérisé en ce que le dit procédé assure la disponibilité du service de communication, et réduit le risque en présence des attaques de type trou noir,
5) Dans le cas où la destination reçoit moins de k partie - le nombre des attaquants trou noir dépasse n-k, - elle demande la retransmission en précisant les chemins fiables qui ont acheminé les autres parties du message.
6) Un procédé, selon les revendications précédentes, caractérisé en ce que le procédé vérifie l'intégrité des messages en cas de réception de plus que (k+1) parties, par la reconstruction des versions du message initial, par des combinaisons de k parties, puis s'assurer de l'égalité de toutes les versions du message, et de lutter contre les attaques qui menacent la confidentialité et l'intégrité des messages

Annexe

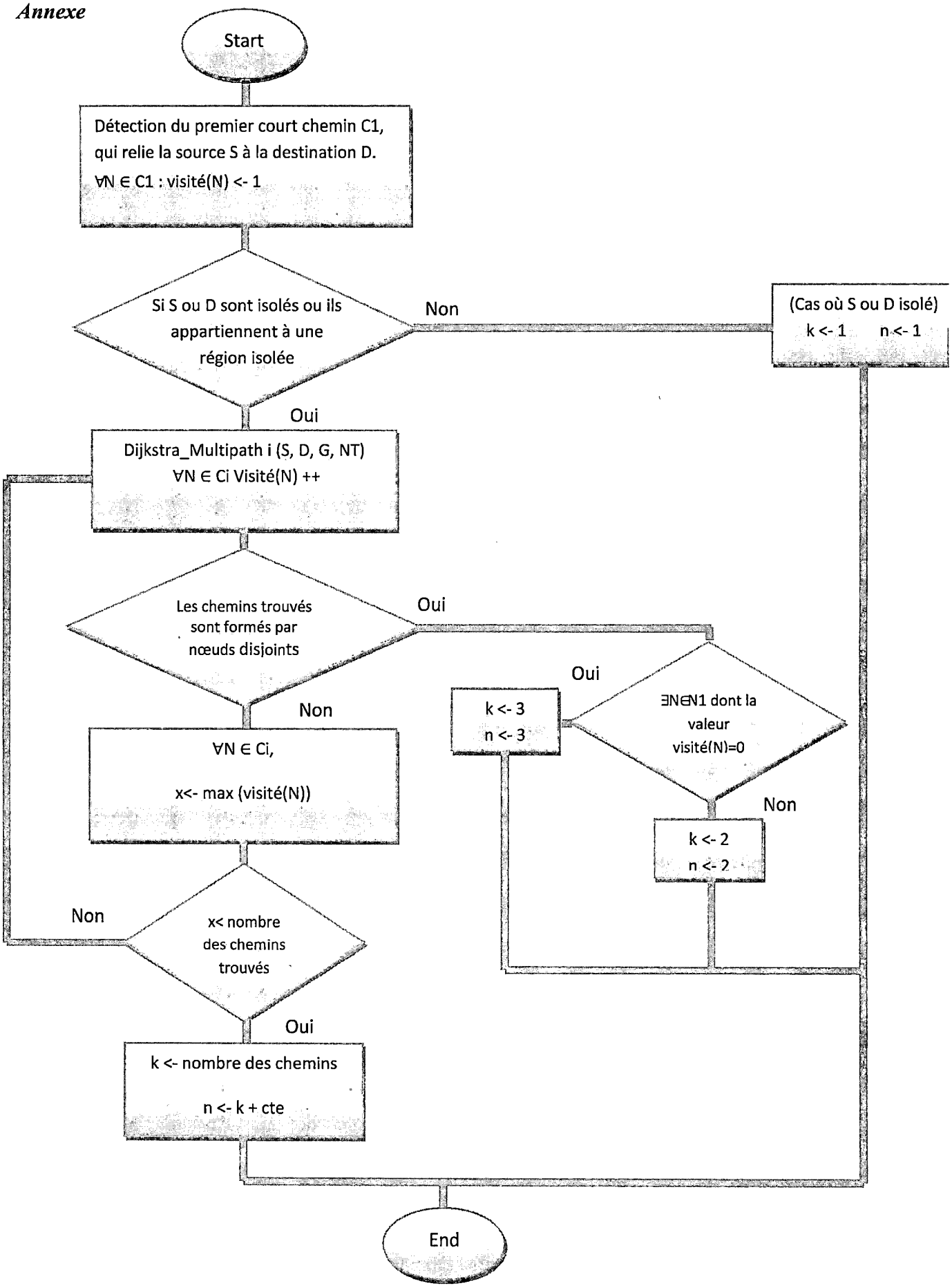

Figure 1: Algorithme I de détermination du nombre de chemins nécessaires

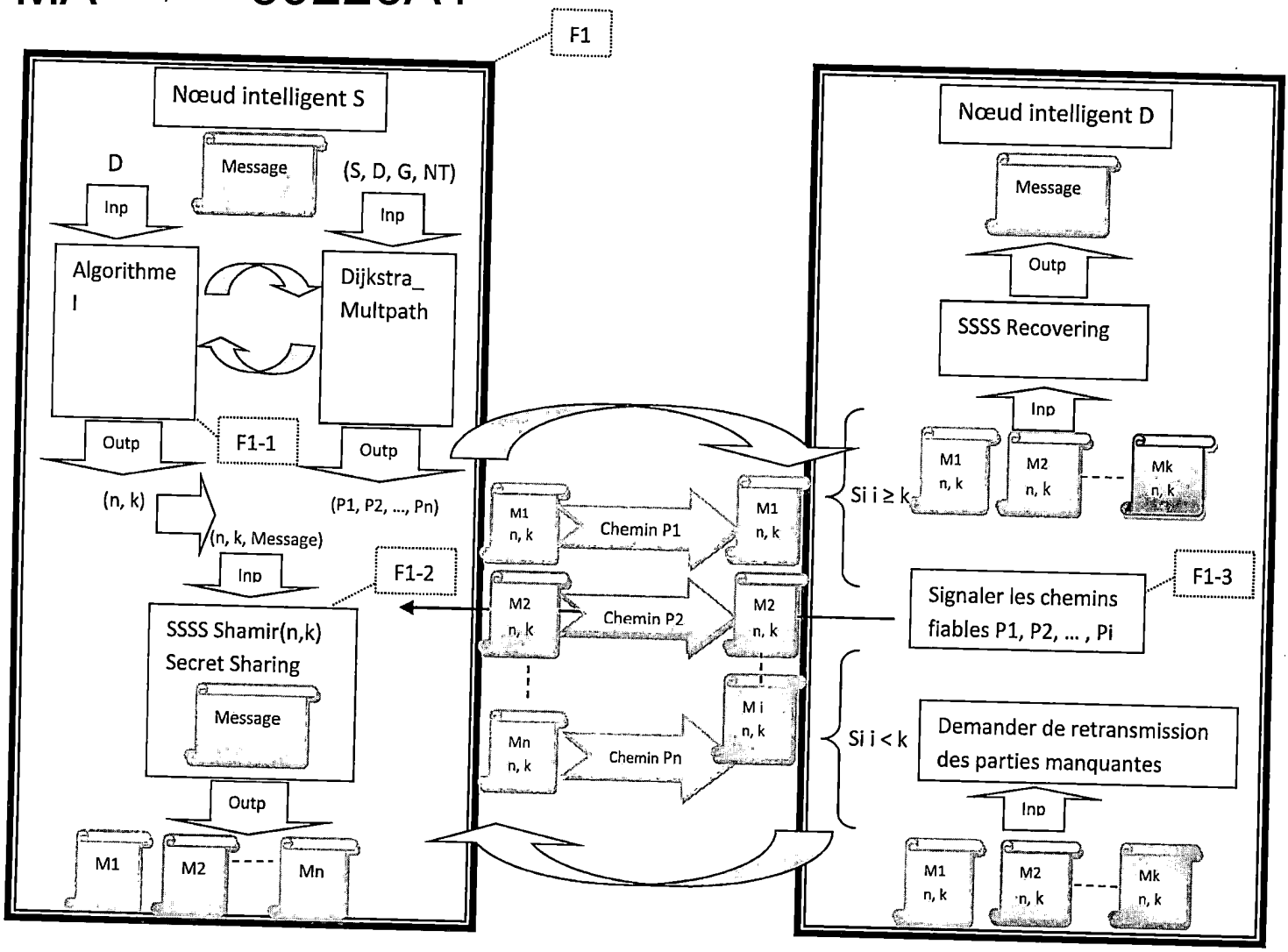

Figure 2: Processus d'échange de messages

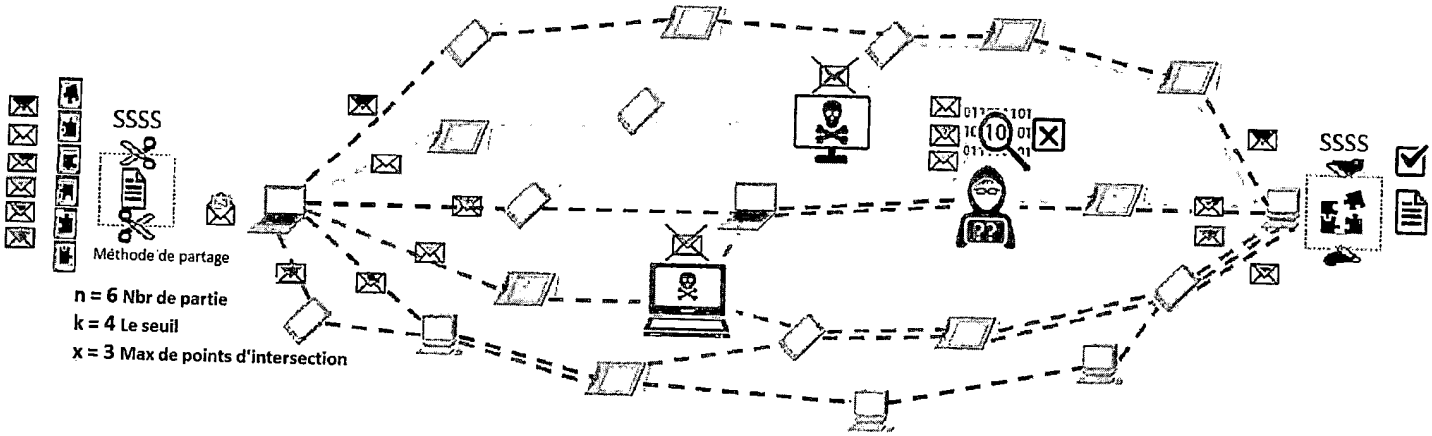

Figure 3: Scénario de communication entre deux nœuds

MA 39226A1

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 : 39226	Date de dépôt : 26/07/2016
Déposant : UNIVERSITE MOHAMMED V RABAT	
Intitulé de l'invention : Nouveau procédé multi-chemin de sécurité dans les réseaux MANET	

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 cités par l'examinateur dans la partie rapport de recherche sont joints au présent document

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** : 12/10/2016
Téléphone: **212 5 22 58 64 14/00**	

ROYAUME DU MAROC
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
Brevets, Dessins et Modèles

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
  4 Pages
- Revendications
  6
- Planches de dessin
  2 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : H04W40/00

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
X	SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks ; Wenjing Lou Wei Liu ; 2004 URL: http://infocom2004.ieee-infocom.org/Papers/50_2.PDF; Tout le document	1-6
X	SPREAD : IMPROVING NETWORK SECURITY BY MULTIPATH ROUTING ; Wenjing Lou,Wei Liu ; 2003	1-6
A	US2011211701 A1 ; GRALL ERIC [FR]; SINTES NICOLAS [FR]; 01/09/2011	1-6
A	Djamel Djenouri, Othmane Mahmoudi, Mohamed Bouamama, David Llewellyn-Jones, Madjid Merabti, on Securing MANET Routing Protocol Against Control Packet Dropping, pp. 100-108, IEEE International Conference on Pervasive Services, Jul. 15-20, 2007, Istanbul, Turkey.	1-6

***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 4 : Remarques de clarté

La revendication 2 tente de définir l'objet par le résultat recherché. Les caractéristiques de procédé qui assurent la reconnaissance, la prédiction et l'apprentissage doivent figurer dans la revendication.
Le même raisonnement s'applique à la revendication 4.
La revendication 5 n'est pas rédigée en deux parties. La revendication doit commencer par un préambule qui indique la catégorie de la revendication et, le cas échéant, les revendications dont elle dépend.
L'objet des revendications 2,4 et 5 manque de clarté au sens de l'article 35 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

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

Nouveauté (N)	Revendications 5-6 Revendications 1-4	Oui Non
Activité inventive (AI)	Revendications aucune Revendications 1-6	Oui Non
Possibilité d'application Industrielle (PAI)	Revendications 1-6 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 : SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks

1. Nouveauté (N) :

Le document D1 divulgue (voir abrégé, partie 2 et partie 3) un procédé de détection de nombre optimale variable des chemins comprenant :

- Un dispositif électronique (nœud source) qui communique avec ses voisins, et pour atteindre les autres dispositifs (nœud de destination) du réseau il doit forcément passer par les nœuds jouant le rôle des routeurs pour acheminer les paquets.
- Il y a deux types de paquets : des paquets de contrôle et des paquets de données (c'est le cas pour tous les protocoles de routage) ;
- Un réseau constitué par un ensemble de nœuds qui communiquent sans infrastructure préexistante (réseau MANET) ;

Le procédé comprend les étapes suivantes :

- Fournir au dispositif une pluralité de chemins optimaux qui permettent à un nœud source d'acheminer d'une manière fiable et sécurisée les messages vers la destination ;
- Permettre aux nœuds de réseau de déterminer le nombre de chemins n variables, avec un seuil égal à k, et permet aussi d'appliquer la méthode de partage de secret de shamir afin de diviser le message afin de diviser le message et envoyer chaque partie dans un chemin.

L'objet de la revendication 1 manque donc de nouveauté au sens de l'article 26 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

D1 précise en outre que le procédé permet la reconnaissance, la prédiction et l'apprentissage de situations dans un environnement mobile sans fil et sans infrastructure (voir abrégé) en signalant les chemins fiables.
L'objet de la revendication 2 manque donc de nouveauté au sens de l'article 26 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.
D1 divulgue que le procédé subdivise le message en plusieurs parties, puis les encapsules dans des paquets, et les envoie vers la destination à travers des chemins multiples (voir partie C). Ledit procédé utilise Shamir secret sharing scheme pour partage le message sur n nœuds, avec un seuil égal à k (k est inférieur ou égale à n). Une fois reçue les parties du message, il reconstitue le message en se basant sur le polynôme de Lagrange (voir partie 2.A). Ledit procédé assure la disponibilité du service de communication et réduit le risque en présence des attaques de type trou noir.
L'objet des revendications 3 et 4 manque de nouveauté au sens de l'article 26 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.
L'objet des revendications 5 et 6 est 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) :

Bien que D1 ne divulgue pas explicitement que le nœud source demande la retransmission suite à des attaques et vérifie l'intégrité des messages en cas de réception de plus de (k+1) parties, il est évident que tout protocole de routage utilisant le partage de clé de Shamir inclut des mécanismes de retransmission suite à des attaques et de aussi une vérification de l'intégrité des messages reçus.
Les revendications 5 et 6 ne contiennent aucune caractéristique technique qui implique une activité inventive au sens de l'article 28 de la loi 17-97 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.