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 53526 A1

(51) Cl. internationale :
H04W 12/00; H04W 12/00

(43) Date de publication :
30.12.2022

(21) N° Dépôt :
53526

(22) Date de Dépôt :
14.06.2021

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

(72) Inventeur(s) :
Habbani Ahmed ; BENJBARA CHAIMAE ; Mouchfiq Nada

(74) Mandataire :
Kartit Zaid

(54) Titre : **Procédé sécurisé basé sur un compromis conventionnel**

(57) Abrégé : L'échange des informations personnelles et professionnelles au niveau des systèmes communicants a accru dans les dernières années, à cause des conditions sanitaires et de limitation de déplacement. Donc, la sécurité des communications est devenue une préoccupation majeure pour les utilisateurs afin de respecter et protéger leurs données. Les réseaux avec infrastructures possèdent un niveau de sécurité moyen et qui est encours d'amélioration, mais ceux sans infrastructures (ad hoc) restent toujours moins sécurisés et représentent un défi pour les gens de ce métier. C'est dans ce sens que notre invention propose un nouveau procédé sécurisé basé sur une approche intelligente multitâches de collaboration conventionnelle entre les différents composants du réseau ad hoc en assurant un stockage et un échange d'informations d'une façon confidentielle et en préservant au maximum l'efficacité et le rendement de chaque noeud et du réseau tout entier sans qu'il impacte la QoS et les performances de ce dernier.

Abrégé :

L'échange des informations personnelles et professionnelles au niveau des systèmes communicants a accru dans les dernières années, à cause des conditions sanitaires et de limitation de déplacement. Donc, la sécurité des communications est devenue une préoccupation majeure pour les utilisateurs afin de respecter et protéger leurs données. Les réseaux avec infrastructures possèdent un niveau de sécurité moyen et qui est encours d'amélioration, mais ceux sans infrastructures (ad hoc) restent toujours moins sécurisés et représentent un défi pour les gens de ce métier. C'est dans ce sens que notre invention propose un nouveau procédé sécurisé basé sur une approche intelligente multitâches de collaboration conventionnelle entre les différents composants du réseau ad hoc en assurant un stockage et un échange d'informations d'une façon confidentielle et en préservant au maximum l'efficacité et le rendement de chaque nœud et du réseau tout entier sans qu'il impacte la QoS et les performances de ce dernier.

Titre : Procédé sécurisé basé sur un compromis conventionnel

Domaine technique :

La présente invention concerne le domaine de sécurité des réseaux de communication.

Plus précisément, elle propose un procédé de sécurité de données basé sur une nouvelle approche regroupant des mécanismes bien précis et assurant une coopération entre les nœuds au sein des réseaux sans fils et sans infrastructures (ad hoc sans fils).

Etat antérieur :

Le réseau ad hoc se caractérise par son architecture sans fil décentralisée qui ne dépend pas d'une infrastructure préalablement établie, comme des routeurs dans les réseaux filaires ou des points d'accès dans les réseaux sans fil administrés.

Pour assurer la communication au sein de ce réseau, il est nécessaire de passer par des agents intermédiaires qui s'occuperont de l'acheminement des données entre une entité (nœud) source vers une entité destination.

L'échange des données entre ces équipements est assuré par des protocoles de routage qui n'intègrent pas obligatoirement un niveau de sécurité. Par conséquent, les informations échangées peuvent être divulguées à des entités inconnues, modifiées de manière non autorisée ou encore une entité engagée dans la communication peut carrément nier avoir reçu ou envoyé un message.

Ainsi la notion de réseaux détient de plus en plus d'importance, et ce type de réseau exige un routage spécifique avec un niveau de sécurité élevé.Les auteurs de **[A HybridWormholeAttackDetection in Mobile Ad-Hoc Network (MANET).]**ont amélioré un algorithme pour améliorer la détection des attaques par trou de ver pour les deux types, dans la bande grâce à l'exécution du temps de parcours (RTT) basé sur le nombre de sauts et le taux de livraison des paquets (PDR) et hors de la bandegrâce à l'exécution de la portée de transmission entre les nœuds successifs. Dans **[MultiSec: A Bionics Security Architecture of Ad-hoc Network.],** les auteurs ont mis en place une nouvelle architecture combinant logiciel et matériel, appelée MultiSec, inspirée de la méthode d'immunisation des animaux contre les agents pathogènes et dont l'idée principale est de se défendre contre l'attaque en utilisant toute la puissance d'un réseau.

Notre invention apporte des solutions différentes et originales par rapport à celles de l'état de l'art :

- Propose un procédé basé sur une approche intelligente qui est liée à l'apprentissage du réseau.
- Assure une certaine balance entre les nœuds à travers le choix démocratique et coopératif pour qu'ils aient tous la chance d'orchestrer le réseau suivant des règles bien précises dans le cadre d'un compromis/contrat.
- Protège le nœud qui sera chargé de l'orchestration du réseau contre les attaques.

- Améliore aussi la sécurité collective des nœuds : si un attaquant cherche à compromettre tous les nœuds, pour pouvoir poursuivre son attaque discrètement, la mise à jour dynamique résiste efficacement à l'attaque en compliquant fortement le nombre de cibles à détruire.
- Garantit l'apprentissage au sein du réseau en prenant en compte les nœuds qui ont participé aux échanges les plus fiables dans les communications précédentes.
- Assure la mise en place d'un procédé de sécurité dédié pour les réseaux ad hoc afin de sécuriser l'envoi des messages via l'élection de nœuds qui seront chargés d'orchestrer l'échange des messages dans le réseau.
- Garantit la coopération et l'effort collectif des composants qui est géré par une convention qui consiste à activer et désactiver les taches affectées aux différents nœuds chacun selon son rôle au sein du réseau.
- Permet de cerner la zone où une attaque a eu lieu, assurant ainsi d'isoler seuls les éléments nuisibles non pas un chemin tout entier.
- Calcule une version concise du message initialappelée condensat/condensé, qui est une représentation unique d'un message de taille quelconque sous forme de suite de caractères alphanumériques ayant une longueur fixe suivant un algorithme, ceci permet d'établir des opérations sans pour autant dévoiler le contenu du message lui-même.
- Garde une trace de l'authenticité en produisant rapidement la même valeur du condensé pour des entrées différentes afin d'assurer la qualité de communication via sécurisation des données.
- Maximise le nombre de paquets approuvés fiables reçus par la destination.
- Ajoute les nœuds suspects malicieux à la liste de nœuds isolésµdont la mise à jour sera envoyée en broadcast dans le réseau.

Brève description des figures :

Le principe de l'invention sera mieux expliqué et l'objectif de l'idée plus éclaircit dans la description détaillée suivante, fourni à titre d'exemple non limitatif, en référence aux dessins annexés, dans lesquels :

- Figure 1 représente le réseau avec les nœuds du réseau ordinaire dotés du nouvel algorithme proposé
- Figure2 représente l'élection des ND
- Figure 3 représente l'élection des NO
- Figure 4 représente la phase de l'isolation des nœuds malicieux
- Figure 5représente un scénario de chemin sans NO
- Figure 6représente un cas spécial du scénario de chemin sans NO
- Figure 7représente un scénario de chemin avec un NO
- Figure 8représente un scénario de chemin avec deux NO

Description détaillée :

La figure1 représente la phase de départ selon notre invention qui constitue à doter tous les nœuds du réseau par un nouvel algorithme de sécurité regroupant des tâches précises qui ne s'activent qu'à la demande. Ce dernier fait apparaître de nouveaux concepts tel que nœuds délégués « ND » et nœuds orchestres « NO » qui collaborent entre eux pour assurer leur sécurité ainsi que celle de leurs voisins.

La figure2 représente la première partie de la phase d'initialisation de notre réseau, chaque groupe de nœuds va élire un nœud de leur premier voisinage qui se caractérise par sa stabilité relative et son énergie résiduelle qui dépasse les 50% de la batterie. Une fois élu, ce nœud joue le rôle de délégué en partageant son statut « Tag = ND » avec ses sélecteurs.

- ***{S, N1, N2, N3}*** → ***N2 (Tag : ND1)***
- ***{N4, N5, N6}*** → ***N5(Tag : ND2)***
- ***{N8, N9, N10}*** → ***N8(Tag : ND3)***
- ***{N7, N11, N12, N13, N14}*** → ***N11 (Tag : ND4)***
- ***{N14, N15, N19}*** → ***N14(Tag : ND5)***
- ***{N16, N17, N18, D}*** → ***N17 (Tag : ND6)***

N.B : Chaque nœud doit choisir un et un seul ND.

La figure3 illustre la deuxième partie de la phase de l'initialisation de notre réseau, qui consiste en ce que les nœuds ND doivent voter pour le meilleur parmi eux en lui attribuant le statut d'orchestre. Une fois élu, ce nœud partage son « Tag = NO » avec ses votants.

- ***{ND1, ND2, ND3}*** → ***ND2 (Tag : NO1)***
- ***{ND4, ND5, ND6}*** → ***ND5 (Tag : NO2)***

Les nœuds normaux qui ont choisi ce NO tant que leur ND vont être affectés aux nœuds délégués les plus proches. Cela permet de sécuriser ce NO et de l'isoler des menaces possibles pour qu'il puisse accomplir sa mission dans des conditions convenables.

- ***{N4, N6}*** —*Redirigévers*→ ***ND3***
- ***{N15, N19}*** —*Redirigévers*→ ***ND6***

Un nœud ne peut être élu comme NO que deux fois successives afin de le garder protégé, de préserver son énergie, et de laisser la chance aux autres nœuds d'accomplir la mission, sans oublier que la mise à jour dynamique résiste efficacement à l'attaque en compliquant fortement le nombre de cibles à détruire.

Afin de prédisposer notre réseau à l'envoi des messages, la figure4 illustre la première tâche assurée après l'élection. Dans un premier temps, les No distribuent des clés de restauration « Cres_NO » auprès de leurs ND et ces derniers font la même chose avec leurs électeurs en envoyant cette fois ci des clés de restauration « Cres_ND ».

En se basant sur ces Cres_ND, chaque nœud délégué peut nettoyer son lot avant d'entamer le processus de l'envoi des messages. Pour cela, il va vérifier la compatibilité entre les clés partagées, afin d'isoler des nœuds malicieux appartenant à son groupe des électeurs.

- ***ND3{N4, N6, N9, N10}*** —*isole*→ ***{N6, N9}***
- ***ND6 {N16, N17, N18, N15, N19, D}*** → ***{N16, N19}***

La figure5 vient alors illustrer une autre tâche accomplie par un ND dans notre réseau, qui estla vérification des nœuds participants à l'envoi, et qui consiste à demander la clé au nœud concerné et la comparer contre celle envoyée. Les nœuds qui n'ont pas retourné la même clé partagée vont être isoler du chemin d'envoi.

Cette opération est expliquée davantage à travers le scénario d'un chemin constitué juste de nœuds normaux et des ND :

« **S-ND1-N3-N4-ND3-N10-N15-ND6-D** »

- ***ND1*** active la tâche de vérification avec ***N3*** :

- Si le résultat de la vérification montre que ***N3*** est malicieux, *ND1* ne transmet pas le message, isole ***N3*** et avertit la source pour que cette dernier calcul un autre chemin d'envoi.
- Sinon dans le cas où la vérification est favorable, *ND1* continue l'envoi, ***N3*** reçoit le message et le transmet à ***N4*** qui à son tour le transmettra à *ND3*.

➢ *ND3* active la vérification avec ***N4*** et ***N10***, si la vérification est affirmative, la donnée sera envoyée à ***N10***et une fois qu'elle atteint *ND6*, il va faire la même procédure avec ***N15*** avant detransmettre le paquet à la destination.

La figure6 représente un cas spécial du scénario entamé par la figure précédente, notamment le chemin :

« **S-N3-N4-ND3-N10-N15-ND6-D** »

Dans ce cas, chaque ND vérifie les clés de restauration avec son arborescence avant de continuer l'envoie en tirant profit du fait que chaque nœud connait son suivant, et une fois qu'il reçoit un message de la part d'un nœud normal, le ND ne continue l'envoie qu'après avoir activé la tâche de vérification avec ce nœud et que le résultat est favorable. En fait a tâche de vérification est activée pour les ND concernés lançant ainsi le processus de localisation, et si jamais à la réception du message, la destination détecte une attaque, alors le seul nœud restant suspect c'est celui qui n'a pas été objet de vérification notamment ***N3*** car son nœud délégué *ND1* ne fait partie du chemin d'envoi, ***N3*** est donc isolé.

La figure7 illustre un scénario du chemin contenant un seul NO, ce qui va expliquer le rôle de ce type de nœud au sein du réseau:

« **S-ND1-N1-N7 -ND4-NO2-ND6-D** »

➢ *ND1* et *ND4* vont activer la phase de vérification avec ***N1*** et ***N7***avant qu'ils procèdent à l'envoi du message reçu de la part de la source.

➢ *NO1* active la tâche de vérification de clés de restauration avec *ND4*
- Si elles sont identiques, ND4 transmet le message au *NO2*
- Sinon, NO2 va isoler ND4 du chemin et il va demander à la source de chercher un nouveau chemin pour envoyer son paquet.

➢ Une fois *NO2* reçoit les données, elle active la tâche de vérification du message qui consiste à déchiffrer le message et son condensé à l'aide de sa propre clé privée et les compare pour s'assurer de sa validité c'est-à-dire le message reçu est conforme au message envoyé.
- Si la vérification n'est pas favorable, il va exécuter des tâches en parallèles « Multi-tâches »:
  - Copie du message reçu où NOreproduit ce dernier en se basant sur son condensat afin d'assurer son acheminement jusqu'à la destination (NO porte la casquette de la source).
  - Vérification de clés qui consiste à demander la clé « Cres_NO » au nœud *ND6* et la comparer contre celle envoyée :
    - Si elles sont identiques, *NO2* transmet le message à la destination en toute sécurité via *ND6.*
    - Sinon*NO2* va isoler*ND6* du chemin et il va demander à la source de chercher un nouveau chemin pour envoyer son paquet.
  - Vérification de la clé de restauration avec *ND4* qui lui a transmis le message erroné pour savoir s'il est malicieux.

- Sinon, il ajoute un Flag mis à 1 indiquant que le message est correct, ensuite il chiffre le message condensé avec la clé publique de la destination D et l'envoie à ***ND6***.

- ***ND6*** consulte la valeur du Flag ajouté au paquet reçu afin de s'assurer de sa validité et l'envoi à D. Cette phase permet au ND de savoir la nature du nœud qui le précède pour éviter l'activation de la tâche de vérification.

La figure8 présente un autre cas de scénario où le chemin reliant la S à la D comprend deux NO ou plus :

« **S-ND1-NO1-ND3-N10-N12-ND4-NO2-ND6-D** »

- ***NO1*** active la tâche de vérification de clés de restauration avec ***ND1***
  - Si elles sont identiques, ***ND1*** transmet le message au ***NO1***
  - Sinon, NO1 va isoler ***ND1*** du chemin et il va demander à la source de chercher un nouveau chemin pour envoyer son paquet.
- Une fois ***NO1*** reçoit les données, il active la tâche de vérification du message :
  - Si elle n'est pas valide, il va faire :
    - Vérification de clés qui consiste à demander la clé « Cres_NO » au nœud ***ND3***et la comparer contre celle envoyée :
      - Si elles sont identiques, ***NO1***va faire une copie du message reçu (récupère le message en se basant sur son condensat afin d'assurer son acheminement jusqu'à la destination), le chiffre avec la clé publique de ***NO2***, garde la valeur initiale de Flag qui est à 0 et le transmet à ***ND3.***
      - Sinon***NO1***va isoler***ND3*** du chemin et il va demander à la source de chercher un nouveau chemin pour envoyer son paquet.
    - Vérification de la clé de restauration avec ***ND1***qui lui a transmis le message erroné pour savoir s'il est malicieux.
  - Sinon, il ajoute un Flag mis à 1 indiquant que le message est correct, ensuite il envoie à ***ND3*** le message chiffré avec la clé publique de ***NO2***.
- ***ND1*** et ***ND4*** vont activer la phase de vérification avec ***N1*** et ***N7***avant qu'ils procèdent à l'envoi du message reçu de la part de la source
- Une fois ***NO2***reçoit le paquet, ilvérifie le Tag du nœud qui lui a transmis le message :
  - Si Tag = ND, ***NO2*** va vérifier la validité du message :
    - Si elle n'est pas favorable, il va faire :
      - Vérification de clés qui consiste à demander la clé « Cres_NO » au nœud ***ND6***et la comparer contre celle envoyée :
        - Si elles sont identiques, ***NO2*** va faire une copie du message reçu, le chiffre avec la clé publique de la destination D, garde la valeur initiale de Flag qui est à 0 et le transmet à ***ND6.***
        - Sinon***NO2***va isoler***ND6*** du chemin et il va demander à la source de chercher un nouveau chemin pour envoyer son paquet.
      - Vérification de clés qui consiste à demander la clé « Cres_NO » au nœud ***ND4*** et la comparer contre celle envoyée :
        - Si elles sont identiques, ***NO2***envoieun message de réclamation aux ***ND3*** et ***ND4*** afin de lancer le processus de

localisation et de détection du nœud qui en était le responsable.

- Sinon *NO2* va ajouter*ND4*à la liste de nœuds isolés **µ.**

- Sinon, il ajoute un Flag mis à 1 indiquant que le message est correct, ensuite il envoie à ***ND6*** le message chiffré avec la clé publique de la destination.

- Sinon si Tag = NO, *NO2* va vérifier le Flag :
  - Si le Flag = 1, il chiffre le message avec la clé publique de la destination D et le transmet à ***ND6***.
  - Sinon si le Flag = 0, il procède à la vérification du message :
    - Si le message est vérifié, *NO2* le chiffre avec la clé publique de la destination et le transmet à ***ND6***.
    - Sinon, *NO2* va demander à la sourcede chercher un nouveau chemin pour envoyer son paquet.

- *NO2*va activer la phase de vérification avec *ND6*avant qu'il procède à l'envoi du message.
- ***ND6*** consulte la valeur du Flag ajouté au paquet reçu afin de s'assurer de sa validité et l'envoi à D. Cette phase permet au ND de savoir la nature du nœud qui le précède pour éviter l'activation de la tâche de vérification.

Revendications :

1) Une méthode intelligente multitâche pour sécuriser l'échange de données dans les réseaux Ad hoc à base d'un consensus en trois étapes comme suit :
   a) Une étape d'initialisation pour désigner les nœuds délégués ND et les nœuds orchestre NO par acquisition de connaissance sur leur environnement en introduisant un mécanisme coopératif de gestion de conflit
   b) Une étape de préparation
   c) Une étape d'envoi des données.

2) La méthode selon la revendication 1 caractérisé en ce que la dite étape d'initialisation se déroule comme suit :

   1. les dits nœuds délégués sont élus par les nœuds de leur premier voisinage comme suit :
      a) Le plus stable avec une distance minimale
      b) Ayant une énergie résiduelle qui dépasse les 50% de la batterie.
   2. les dits nœuds orchestres sont élus parmi les ND voisins comme suit :
      c) Le plus stable avec une distance minimale
      d) Ayant une énergie résiduelle maximale.

3) La méthode selon les revendications 1 et 2 caractérisé en ce que chaque nœud de réseau désigne un et un seul nœud délégué ND, chaque dit nœud ND choisisse un et un seul NO ; le dit nœud ND partage son statut Tag=ND avec ses sélecteurs, le dit nœud orchestre élu partage son statut « Tag = NO » avec ses sélecteurs.

4) La méthode selon les revendications 1,2 et 3 caractérisé en ce que l'élection des ND et NO après la dite étape d'initialisation du réseau se fait en se basant sur un consensus entre les différents nœuds du réseau.

5) La méthode selon les revendications caractérisé en ce qu'après chaque transmission de donnée réussite, les dits nœuds ND et NO incrémentent la valeur de crédibilité de ses sélecteurs qui y participent.

6) La méthode selon les revendications précédentes caractérisé en ce que chaque dit nœud du réseau i génère un pourcentage de crédibilité entre 0 et 1 et le compare à un nombre prédéfini seuil du dit pourcentage de crédibilité P(i) ; la valeur du dit pourcentage de crédibilité soit exploitée dans le vote des ND et NO comme suit :
   a) Un nœud délégué doit avoir un $P_i \in [0.8,1]$.
   b) Un nœud orchestre correspond au nœud ND ayant le plus grand P_i.

7) La méthode selon les revendications précédentes caractérisées en ce que la dite étape de préparation se déroule comme suit :

a) Chacun des nœuds NO qui ont été en activité est initialisé par une valeur d'orchestration qui est égale à 0 et qui peut atteindre une valeur maximale de 2 durant tout le processus d'envoi.
b) Les nœuds normaux qui ont choisi ce NO tant que leurs nœuds ND vont être affectés aux nœuds délégués les plus proches.
c) Chacun des nœuds élus comme NO construit sa propre clé de restauration « Cres_NO » et la décortique en plusieurs clés partielles de restauration pour que chaque partie soit envoyée à un ND constituant sa hiérarchie.
d) Chacun des nœuds élus comme ND la décortique en plusieurs clés partielles de restauration « Cres_ND », et active la tâche de distribution pour que chaque partie soit envoyée à un nœud constituant son hiérarchie.
e) Les NO et ND activent la tâche de vérification de clés avec les nœuds de son arborescence pour isoler les nœuds malicieux et nettoyer ainsi le réseau.
f) Le processus de vérification de messages n'est activé que pour les NO qui feront partie de l'acheminement du message.
g) Une fois le chemin d'envoi déterminé, le premier NO partage sa clé publique avec la source, chaque NO partage sa clé publique avec le NO qui le précède ainsi que ses informations, et la destination partage sa clé publique avec le dernier NO.

8) La méthode selon les revendications précédentes caractérisées en ce que la dite étape d'envoi se déroule comme suit :

- En absence de NO dans le chemin, c'est à dire que des ND et des nœuds normaux N qui participent à l'envoi :

  - ✓ Chaque ND active la tâche de vérification avec le nœud N auquel il correspond avant qu'il procède à l'envoi du message reçu de la part de la source :
    a) Si le résultat de la vérification montre que N est malicieux, le ND ne transmet pas le message, isole le nœud N et avertit la source pour que cette dernière calcule un autre chemin d'envoi.
    b) Sinon dans le cas où la vérification est favorable, ND continue l'envoi.
  - ✓ Dans le cas où une attaque a été détectée par la destination à la réception du message, et qu'un nœud normal N du chemin n'a pas subi le processus de vérification de clés (vu que le ND qui lui correspond ne fait pas partie du chemin d'envoi), il va être considéré comme malicieux et va désormais être isolé.

- En présence d'un seul NO dans le chemin, en plus des ND et des nœuds normaux N :

- ✓ Les ND qui précédent le NO vont tous activer la phase de vérification avec les nœuds de leur arborescence avant qu'ils procèdent à l'envoi du message reçu de la part de la source.

- ✓ NO(k) active la tâche de vérification de clés de restauration avec son ND précédent :
  a) Si elles sont identiques, ce ND transmet le message au NO(k)
  b) Sinon, NO(k) va isoler ce ND du chemin et il va demander à la source de chercher un nouveau chemin pour envoyer son paquet.

- ✓ Une fois NO(k) reçoit les données, elle active la tâche de vérification du message qui consiste à déchiffrer le message et son condensé à l'aide de sa propre clé privée et les compare pour s'assurer de sa validité c'est-à-dire le message reçu est conforme au message envoyé.
  a) Si la vérification n'est pas favorable, il va exécuter des tâches en parallèles « Multi-tâches » :
     I. Copie du message reçu où NO reproduit ce dernier en se basant sur son condensat afin d'assurer son acheminement jusqu'à la destination (NO porte la casquette de la source).
     II. Vérification de clés qui consiste à demander la clé « Cres_NO » au nœud ND suivant et la comparer contre celle envoyée :
        i. Si elles sont identiques, NO(k) transmet le message à la destination en toute sécurité.
        ii. Sinon NO(k) va isoler le ND suivant du chemin et il va demander à la source de chercher un nouveau chemin pour envoyer son paquet.
     III. Vérification de la clé de restauration avec le ND précédent qui lui a transmis le message erroné pour savoir s'il est malicieux.
  b) Sinon, il ajoute un Flag mis à 1 indiquant que le message est correct, ensuite il chiffre le message condensé avec la clé publique de la destination D et l'envoie au ND suivant.

- ✓ Les ND qui se trouvent après le NO consultent tous la valeur du Flag ajouté au paquet reçu afin de s'assurer de sa validité et l'envoi à D. Cette phase permet au ND de savoir la nature du nœud qui le précède pour éviter l'activation de la tâche de vérification.

- En présence de plus qu'un NO dans le chemin, en plus des ND et des nœuds normaux N :

  - ✓ Les ND qui précédent le NO(k) vont tous activer la phase de vérification avec les nœuds de leur arborescence avant qu'ils procèdent à l'envoi du message reçu de la part de la source.

- ✓ NO(K) active la tâche de vérification de clés de restauration avec son ND précédent :
  c) Si elles sont identiques, ce ND transmet le message au NO(k)
  d) Sinon, NO(k) va isoler ce ND du chemin et il va demander à la source de chercher un nouveau chemin pour envoyer son paquet.

- ✓ Une fois NO(K) reçoit les données, il active la tâche de vérification du message :
  - Si elle n'est pas valide, il va faire :
    I. Vérification de clés qui consiste à demander la clé « Cres_NO » au ND qui le précède et la comparer contre celle envoyée :
       i. Si elles sont identiques, NO(K) va faire une copie du message reçu (récupère le message en se basant sur son condensat afin d'assurer son acheminement jusqu'à la destination), le chiffre avec la clé publique de NO(K+1), garde la valeur initiale de Flag qui est à 0 et le transmet à son ND suivant.
       ii. Sinon NO(K) va isoler son ND suivant du chemin et il va demander à la source de chercher un nouveau chemin pour envoyer son paquet.
    II. Vérification de la clé de restauration avec son ND précédent qui lui a transmis le message erroné pour savoir s'il est malicieux.
  - Sinon, il ajoute un Flag mis à 1 indiquant que le message est correct, ensuite il envoie à son ND suivant le message chiffré avec la clé publique de NO(K+1).

- ✓ Une fois NO(K+1) reçoit le paquet, il vérifie le Tag du nœud qui lui a transmis le message :
  - Si Tag = ND, NO(K+1) va vérifier la validité du message :
    I. Si elle n'est pas favorable, il va faire :
       i. Vérification de clés qui consiste à demander la clé « Cres_NO » au nœud ND qui le suit et la comparer contre celle envoyée :
          - Si elles sont identiques, NO(K+1) va faire une copie du message reçu, le chiffre avec la clé publique de la destination D, garde la valeur initiale de Flag qui est à 0 et le transmet au ND suivant.
          - Sinon NO(K+1) va isoler son ND suivant du chemin et il va demander à la source de chercher un nouveau chemin pour envoyer son paquet.

ii. Vérification de clés qui consiste à demander la clé « Cres_NO » au nœud ND précédent et la comparer contre celle envoyée :
- Si elles sont identiques, NO(K+1) envoie un message de réclamation aux ND qui se situent entre NO(K) et NO(K+1) afin de lancer le processus de localisation et de détection du nœud qui en était le responsable.
- Sinon NO(K+1) va ajouter son ND précédent à la liste de nœuds isolés μ.

II. Sinon, il ajoute un Flag mis à 1 indiquant que le message est correct, ensuite il envoie au ND suivant le message chiffré avec la clé publique de la destination.

- Sinon si Tag = NO, NO(K+1) va vérifier le Flag :
  I. Si le Flag = 1, il chiffre le message avec la clé publique de la destination D et le transmet au ND suivant.
  II. Sinon si le Flag = 0, il procède à la vérification du message :
    i. Si le message est vérifié, NO(K+1) le chiffre avec la clé publique de la destination et le transmet au ND suivant.
    ii. Sinon, NO(K+1) va demander à la source de chercher un nouveau chemin pour envoyer son paquet.

✓ NO(K+1) va activer la phase de vérification avec son ND suivant avant qu'il procède à l'envoi du message.
✓ Les ND qui suivent NO(K+1) consultent la valeur du Flag ajouté au paquet reçu afin de s'assurer de sa validité et l'envoi à la destination.

9) La méthode selon l'une quelconque des revendications précédente caractérisé en ce que les nœuds détectés comme malicieux sont isolés et ajoutés à une liste de nœuds morts **μ** qui sera envoyée en broadcast dans le réseau.

Figures :

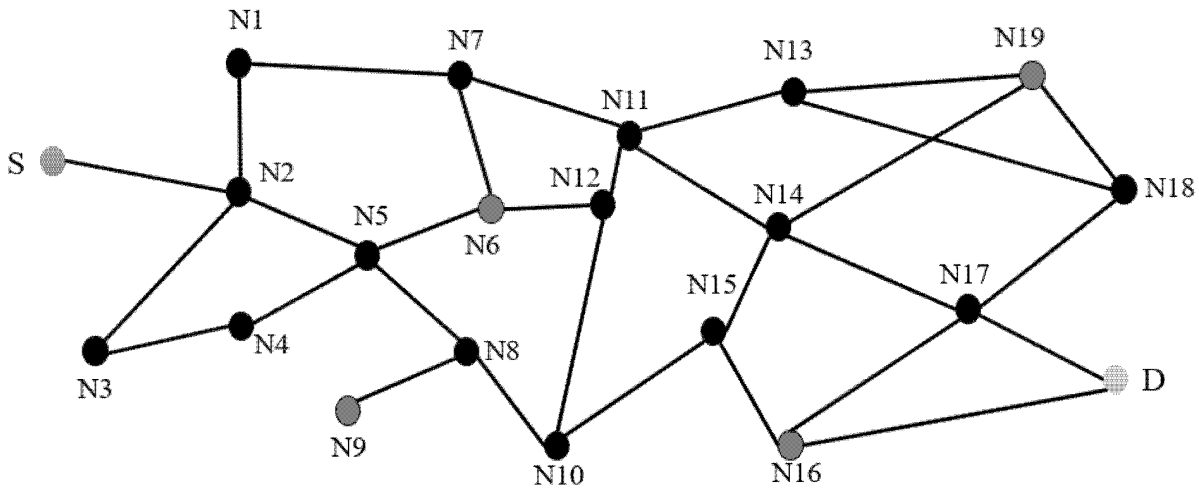

FIG .1

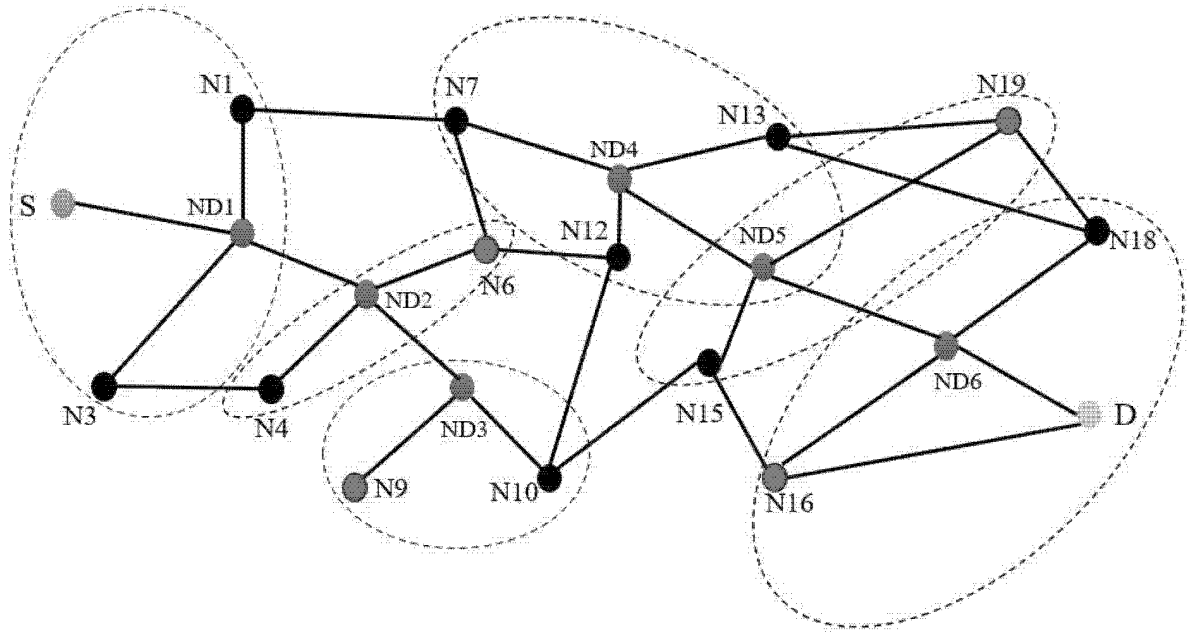

FIG .2

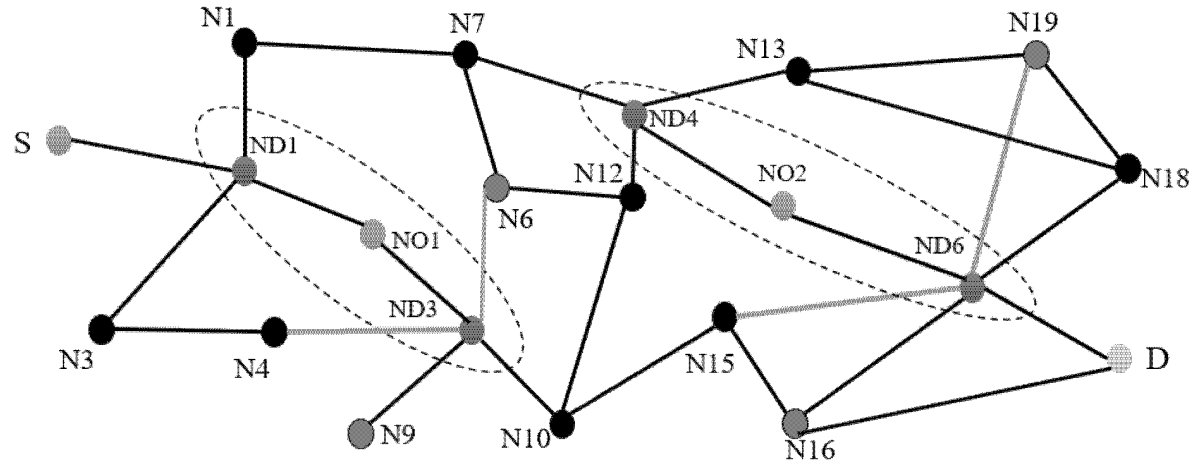

FIG .3

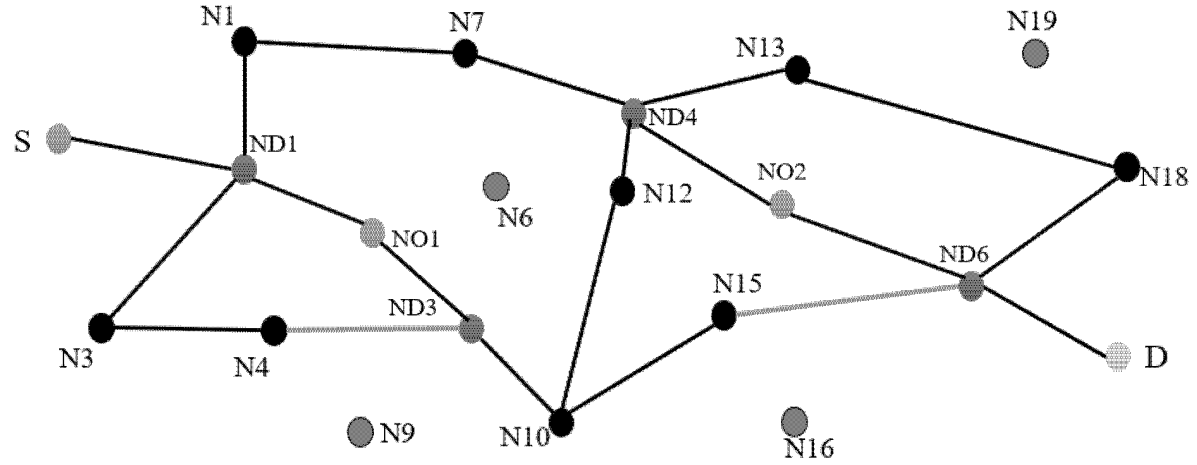

FIG .4

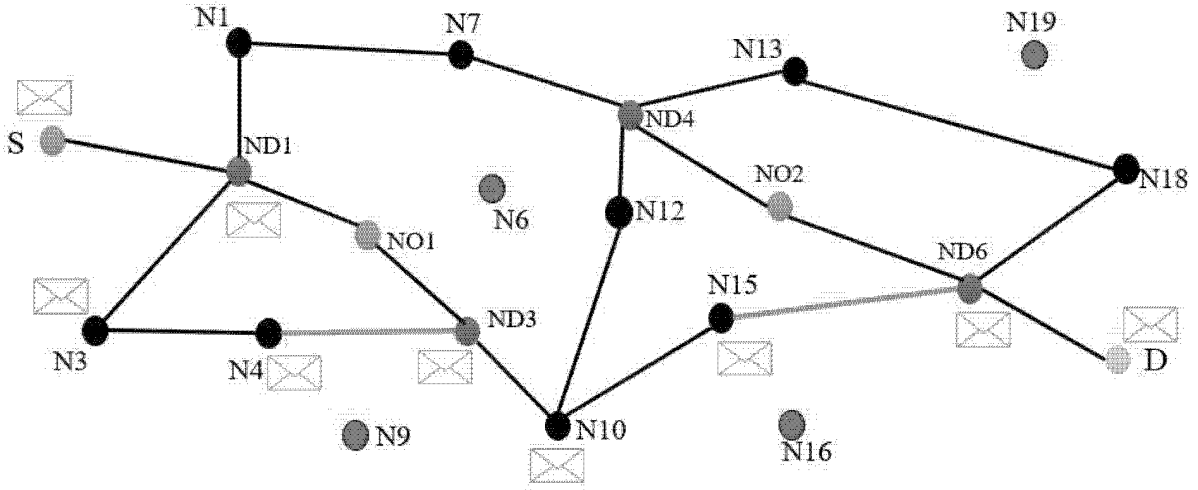

FIG .5

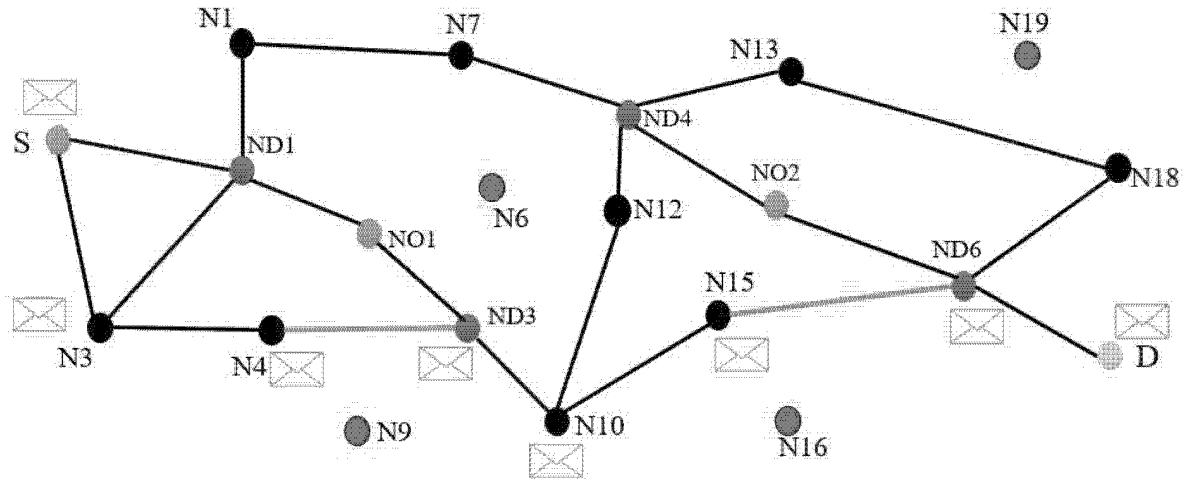

FIG .6

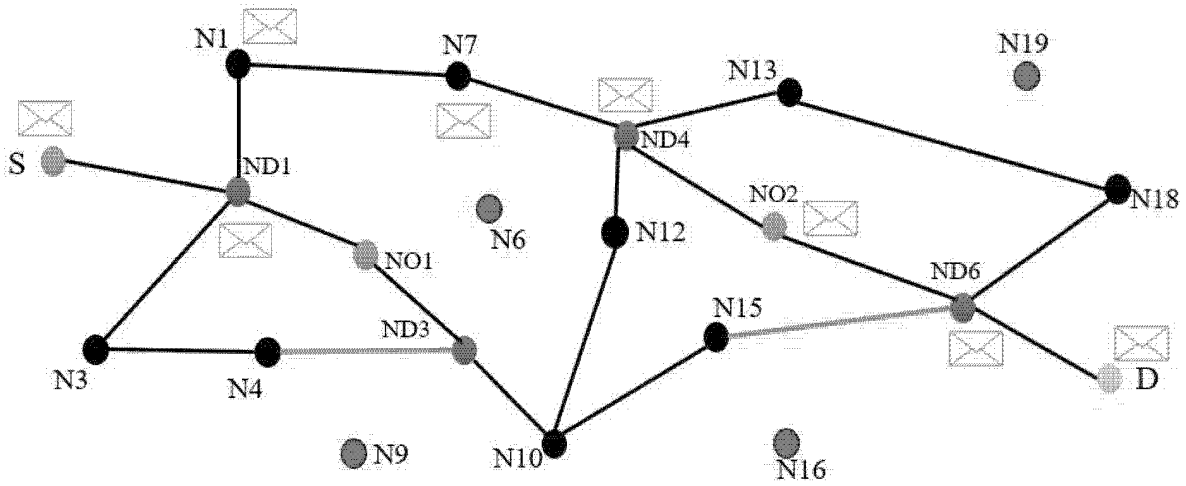

FIG .7

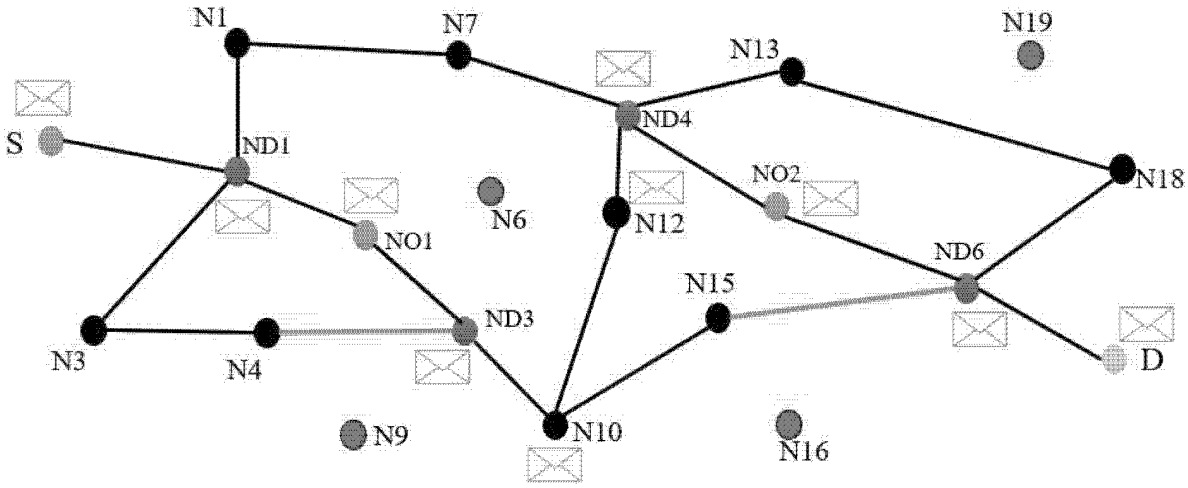

FIG .8

MA 53526A1

ROYAUME DU MAROC
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE

OMPIC

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 : 53526	Date de dépôt : 14/06/2021
Déposant : Université Mohammed V - Rabat	
Intitulé de l'invention : Procédé sécurisé basé sur un compromis conventionnel	

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 forme et de clarté
- ☐ Cadre 5 : Défaut d'unité d'invention
- ☐ Cadre 6 : Observations à propos de certaines revendications exclues de la brevetabilité
- ☒ Cadre 7 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Examinateur: BAMI MOHAMMED	**Date d'établissement du rapport** : 30/09/2021
Téléphone: **212 5 22 58 64 14/00**	

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
  6 Pages
- Revendications
  1-9
- Planches de dessin
  3 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : H 04W12/00
CPC :H04W12/00

Plateformes et bases de données électroniques de recherche :

EPOQUENET, WPI, ScienceDirect, IEEE, ORBIT

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
A	CN103347260A ; Anhui Licha Information Technology Co., Ltd ; 13/02/2018	1-9
A	US7506042B2 ; SHARP LAB OF AMERICA INC ; 17/03/2009	1-9

***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 7 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté	Revendications 1-9 Revendications aucune	Oui Non
Activité inventive	Revendications 1-9 Revendications aucune	Oui Non
Application Industrielle	Revendications 1-9 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 : CN103347260A

1. Nouveauté

Aucun document ne divulgue l'objet des revendications 1-9 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

Le document D1 est considéré comme l'état de la technique le plus proche de l'objet de la revendication 1 et divulgue :
Une méthode intelligente multitâche pour sécuriser l'échange des données dans les réseaux ad hoc comprenant :
Une étape d'initialisation pour désigner les nœuds délégués et les nœuds orchestre par acquisition de connaissance sur leur environnement.
Une étape de préparation
Une étape d'envoi de données.

L'objet de la revendication 1 diffère de D1 en ce que la méthode comprend un mécanisme coopératif de gestion de conflit.

Le problème objectif que la présente demande se propose de résoudre peut donc être considéré comme : Améliorer l'efficacité et la sécurité de l'échange de données.

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

Par conséquent, l'objet de la revendication 1 implique une activité inventive au sens de l'article 28 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

L'objet des revendications 2-9 implique 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. Application industrielle

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.