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 50778 B1

(51) Cl. internationale :
H04L 12/00

(43) Date de publication :
30.06.2022

(21) N° Dépôt :
50778

(22) Date de Dépôt :
27.10.2020

(71) Demandeur(s) :
Université Mohammed V de Rabat, Angle avenue Allal El Fassi et Mfadel Cherkaoui Al Irfane , Rabat, 8007 (MA)

(72) Inventeur(s) :
KARTIT ZAID ; DIOURI OUAFAA

(74) Mandataire :
Kartit Zaid

(54) Titre : **Méthode pour anticiper une attaque trou noir (Blackhole) dans les réseaux Ad hoc.**

(57) Abrégé : Une méthode pour anticiper l'attaque trou noir dans les réseaux Ad hoc. Dans un mode de réalisation, chaque nœud doit s'enregistrer dans une Chaine de blocs afin de faciliter l'authentification et l'intégrité des messages. Le principe de PoId (une variante de PoA) est choisi comme consensus pour notre Chaine de blocs. Dans cette méthode nous avons exploité la diffusion sélective par les points relais multipoints MPR pour conserver les ressources des nœuds. Afin de détecter une attaque trou noir causée par les fausses informations qui viennent d'une réponse RREP, nous avons utilisé les accumulateurs cryptographiques dynamiques combinés avec une chaine de hachage comme mécanisme de détection de la véracité de ces informations.

ABRÉGÉ

Une méthode pour anticiper l'attaque trou noir dans les réseaux Ad hoc. Dans un mode de réalisation, chaque nœud doit s'enregistrer dans une Chaine de blocs afin de faciliter l'authentification et l'intégrité des messages. Le principe de PoId (une variante de PoA) est choisi comme consensus pour notre Chaine de blocs. Dans cette méthode nous avons exploité la diffusion sélective par les points relais multipoints MPR pour conserver les ressources des nœuds. Afin de détecter une attaque trou noir causée par les fausses informations qui viennent d'une réponse RREP, nous avons utilisé les accumulateurs cryptographiques dynamiques combinés avec une chaine de hachage comme mécanisme de détection de la véracité de ces informations.

Titre : Méthode pour anticiper une attaque trou noir (Blackhole) dans les réseaux Ad hoc.

Domaine technique

La présente invention se rapporte au domaine des réseaux de communication et en particulier les réseaux Ad hoc. Il s'agit plus précisément d'une technique à base d'accumulateur cryptographique à utiliser dans un protocole de routage réactif. En effet cette technique permet de vérifier la véracité des informations communiquées par un nœud intermédiaire dans une réponse (RREP) à une requête de découverte de route (RREQ) entre deux nœuds du réseau.

Etat antérieur :

Un réseau Ad hoc est composé des nœuds, équipés d'une carte sans fil, capables de s'organiser sans infrastructure fixe définie préalablement. En particulier, il n'y a pas de « points d'accès » et chaque nœud du réseau communique directement avec ses voisins. Pour communiquer avec des nœuds éloignés, il est nécessaire de faire passer ses données par des nœuds intermédiaires qui se chargent de les acheminer jusqu'au nœud destination.

Dans un réseau Ad hoc les nœuds doivent se situer les uns à côté des autres pour qu'ils puissent construire des chemins entre eux en toute confiance. En effet, les nœuds ne connaissent ni la topologie du réseau, ni la fiabilité des liens et ni celles des nœuds dont ils sont composés. Ainsi un protocole de routage sécurisé est indispensable pour établir un chemin de communication entre deux nœuds qui ne sont pas directement en contact. Ce chemin doit être composé des nœuds honnêtes possédant un certain niveau de confiance.

Deux paradigmes de découverte de réseau sont proposés, le premier étant celui des protocoles « proactifs », qui construisent les tables de routage avant que la demande en soit effectuée. Ils identifient en fait à chaque instant la topologie du réseau. Le second paradigme de découverte de réseau est celui des protocoles « réactifs », qui construisent les tables de routage lorsqu'un nœud en effectue la demande. Ils ne connaissent pas la topologie du réseau, il détermine le chemin à prendre pour accéder à un nœud du réseau lorsqu'on lui demande via l'envoi (possiblement diffusion) de messages RREQ « route request » et attend de recevoir un message RREP « route reply » du destinataire souhaité.

Dans le cas des protocoles réactif pendant la phase de découverte de route (RREQ), il se trouve qu'un nœud intermédiaire possède un chemin vers la destination, c'est pour cela

ce type de protocole (AODV par exemple) autorise un nœud intermédiaire de fournir une réponse RREP dans l'objectif de réduire temps d'établissement de chemin entre deux nœuds. Cependant cette réponse peut venir d'un nœud malveillant qui répond par un message contenant de fausses informations, par exemple un numéro de séquence très grand (figure 2). Par conséquent ce nœud malveillant a plus de chances d'être sur le chemin à choisir par le nœud source et mener une attaque trou noir. La question qui se pose alors comment faire confiance à une telle réponse ?

Une solution évidente à ce problème consiste à désactiver la capacité de répondre par un nœud intermédiaire pendant la phase de découverte de route, de sorte que tous les messages de réponse doivent être envoyés uniquement par le nœud de destination. Par conséquent, un nœud malveillant ne peut plus exploiter cette faille pour causer une attaque trou noir. Cependant, cette solution présente les inconvénients suivants :

- L'établissement des chemins est grandement augmenté surtout pour un réseau de taille importante.
- Un nœud intermédiaire malveillant peut fabriquer un message de réponse au nom du nœud de destination sans que le nœud source ne puisse le détecter.

Une autre solution consiste à exploiter, dans le cas du protocole AODV, le drapeau qui autorise une réponse RREP gratuite (bit G) à envoyer en unicast vers le nœud spécifié dans le champ adresse IP destination lui indiquant que tel nœud source tente de le joindre. De cette manière, le nœud destination est mis au courant et ajoute dans sa table du routage le chemin vers le nœud source. Une confirmation envoyée au nœud source via ce chemin peut être exploitée pour détecter le nœud malveillant.

Une autre solution a été proposée en utilisant une route supplémentaire en rejouant un message RREQ vers un second nœud intermédiaire mentionné dans le message RREP comme témoin pour vérifier si l'itinéraire du nœud intermédiaire au nœud de destination existe ou non. S'il existe, nous pouvons faire confiance au nœud intermédiaire en choisissant le chemin qui passe par ce nœud. Dans le cas contraire, nous rejetons simplement le message de réponse du nœud intermédiaire. Un message d'alarme est diffusé sur le réseau pour isoler le nœud en question. Cependant cette mesure produit une surcharge de réseau et diminue les performances de protocole de routage. Un autre inconvénient de cette solution est que rien ne peut garantir que le nœud malveillant n'a pas fourni un second nœud malveillant comme témoin (une attaque collaborative).

Dans une autre solution, le nœud source vérifie l'honnêteté du nœud qui initie le paquet RREP en utilisant la redondance réseau. Puisque n'importe quel message peut être arrivé à la destination par de nombreux chemins redondants, l'idée de cette solution est d'attendre que le message de réponse RREP arrive de plus de deux nœuds. Le principal inconvénient de cette solution est le délai à cause de la nécessité de recevoir et traiter plusieurs messages de réponses par la source. Par conséquent cette solution risque de consommer les ressources des nœuds surtout l'énergie.

Les méthodes de prévention et de détection de trou noir souffrent en résumé de plusieurs limitations telles que problème de latence, consommation de ressources et production de plus de charge.

Il serait donc souhaitable de disposer d'une méthode de vérification de la validité de réponse de la route communiquée par un nœud intermédiaire de sorte à limiter la consommation de l'énergie et augmenter les performances du réseau.

Brève description des figures :

Figure 1 : Un scénario d'attaque trou noir dans un réseau Ad hoc.

Figure 2 : Structure des blocs dans la Chaine de blocs

Figure 3 : Principe de génération et stockage des clés dans un nœud équipé PUF

Figure 4 : Diffusion sélective via les MPRs et le réseau Chaine de blocs BCN

Figure 5 : Utilisation d'une chaine de hachage dans une découverte de route RREQ pour contrôler le nombre de saut (hop count).

La figure 1 illustre un scénario d'attaque trou noir dans un réseau Ad hoc. Dans ce scénario le nœud S souhaite atteindre le nœud D. Il diffuse un message RREQ. Le nœud B lui envoie un message RREP avec un numéro de séquence plus grand que celui des autres nœuds. Par conséquent le nœud source choisit le chemin qui passe par B pour atteindre le nœud D ce qui permet au nœud B de détruire toutes les données et produire ainsi l'attaque trou noir.

La figure 3 illustre le principe de fonctionnement des opérations de chiffrement par le système PUF. Seul la clé publique et le challenge utilisé lors de sa génération sont stockés dans une mémoire non volatile NVL. Afin de protéger la clé privée, elle n'est jamais enregistrée. Le nœud peut la générer en utilisant le challenge Ci stocké dans sa mémoire NVL et la fonction PUF pour effectuer une opération cryptographique nécessitant ladite clé.

Dans un mode de réalisation de cette méthode, le nœud source (figure 5) initialise le calcul des éléments de la chaine de hachage à m fois appliquée à x ($h^m(x)$).Les valeurs de x et de m sont inconnu dans la phase de diffusion de la demande RREQ pour les nœuds qui vont participer à l'établissement du chemin vers la destination. En effet seul le nœud destination est capable de divulguer les valeurs de x et de m dans la phase d'une réponse RREP puisque le nœud source à apposer le chiffrement de x et m dans RREQ en utilisant sa clé publique. Lors de l'envoi de ladite réponse, les nœuds intermédiaires reçoivent des informations caractérisant le chemin établi dont la valeur de m et celle de x.

Description détaillée

La présente méthode résout le problème de l'art antérieur par utilisation des fonctions de hachage combinées avec les accumulateurs cryptographiques dynamiques comme mécanisme de vérification de la véracité des informations de routage. Lesdits accumulateurs sont des structures de données efficaces dans l'espace et dans le temps qui sont utilisés pour vérifier si un élément est membre dans à un ensemble X. Ils sont formés par plusieurs algorithmes suivants :

- AccVal pour calculer la valeur de l'accumulateur d'un ensemble.
- Add pour ajouter un élément
- Delete pour supprimer un élément
- WitGen pour générer la preuve d'appartenance à l'ensemble
- UpdWit pour générer une mise à jour de la preuve d'appartenance après l'ajout d'un élément.
- Verify pour vérifier la preuve d'appartenance d'un élément.

La présente invention développe un mécanisme pour sécuriser le protocole de routage réactif AODV et ses variantes en utilisant des accumulateurs cryptographiques dynamiques combinés avec une chaine de hachage.

Dans un mode de réalisation de la présente invention un réseau Ad hoc peut être un réseau Manet, un réseau Vanet ou un réseau Fanet. Le réseau Ad hoc est composé de nœuds équipés de fonctions physiquement non clonables (PUF).Chaque nœud de réseau Ad hoc :

- Est configuré avec une adresse IP unique.
- Est configuré pour utiliser le principe des relais multipoints MPR à base de confiance dans la diffusion (sélective) des informations de routage.

- Calcule son vecteur de coopération comme suit : VCap= {NP [ID, Stabilité, Accessibilité] ; NC [Energie, CPU, Stockage]} avec NP : propriétés d'un nœud, NC : Capacités d'un nœud.

Dans un autre mode de réalisation de la présente invention un nœud du réseau Ad hoc peut être un simple nœud ordinaire ou un nœud chaine de blocs :

✓ Nœud Ordinaire NO :

Un nœud ordinaire est un nœud qui assure les fonctions de base d'un réseau Ad hoc. IL soumet son identité et sa propre clé publique aux nœuds validateurs dans la phase d'enregistrement. Il interroge la Chaine de blocs pour obtenir son propre témoin pour une future authentification d'identité une fois il se reconnecte au réseau.

✓ Nœud NBH :

Un nœud tête du réseau chaine de blocs est un nœud qui initialise sa formation une fois élu par les autres nœuds de réseau Ad hoc. Il permet d'assurer le rôle de premier validateur pour son ensemble de nœuds MPR. Ces derniers sont les premiers à enregistrer leurs identifications dans le réseau chaine de blocs BCN pour devenir des validateurs à leur tour chacun pour son ensemble MPR.

✓ Nœud Chaine de Blocs NB :

Un nœud Chaine de blocs est un nœud du réseau Ad hoc qui assure des fonctions de chaine de blocs en tant que validateur des informations des nœuds ordinaires. Il applique la procédure de consensus PoA pour vérifier le lien entre l'identité et les clés d'un nœud. En effet un nœud NB génère des certificats numériques pour les autres nœuds de réseau Ad hoc. Il fabrique les blocs des transactions Tx, contenant les clés publiques, identificateurs et autres (figure 3) des nœuds du réseau pour les diffuser dans le réseau BCN. Il reçoit la demande d'autorisation envoyée par un nœud, vérifie et authentifie et renvoie une mise à jour des paramètres de sécurité.

Dans un réseau Ad Hoc, le vecteur de capacité de chaque nœud change dans le temps. C'est pour cela un nœud peut passer d'un nœud ordinaire NO à un nœud chaine de blocs NB et inversement. Par conséquent dans la présente invention le réseau chaine de blocs BCN lui-même est dynamique. Cependant la chaine de blocs reste stable parce que pour qu'un nœud passe d'un nœud ordinaire à un nœud chaine de blocs doit faire preuve d'avoir une copie de la chaine de blocs.

Dans un mode de réalisation de la présente invention notre méthode intègre un mécanisme que nous appelons PoR proof-of-Route composé des phases suivantes :

A. Phase de création de Réseau Chaine de blocs BCN :

Dans la présente invention, la zone de niveau 2 N2 (n_i) d'un nœud n_i est l'ensemble de ses voisins à 2 sauts, les accumulateurs utilisés sont enregistrés dans la table de routages de chaque nœud. Un message de mise à jour $UpAcc_s$ est diffusé par le réseau BCN.

a. **Initialisation et annonce** :

Chaque nœud sélection son ensemble de nœuds MPRs. Un premier nœud N_0 s'annonce, accepte de mettre sa réputation en jeu, pour être tête de réseau chaine de blocs appelé NBH, pour cela un consensus de vote est lancé pour élire Ce nœud selon le critère de la meilleure valeur du vecteur VCap.

En effet quand un nœud reçoit cette annonce, si son VCap est plus important et qu'il accepte de mettre sa réputation en jeu, s'annonce pour être un nœud NBH, ce processus se répète jusqu'à l'entente global sur un nœud NBH.

b. Création du réseau haine de blocs :

Le nœud élu tête de réseau chaine de blocs change son état de nœud ordinaire au nœud tête de réseau chaine de blocs NBH et envoie une requête à son ensemble MPRs pour changer également leurs états en nœud chaine de blocs NB. Ces derniers réagissent de la même manière pour changer l'état des nœuds de leurs ensembles MPRs en nœud NB pour former enfin le réseau chaine de blocs BCN. Les dits nœuds jouent le rôle de validateurs des informations annoncées par les nœuds qui rejoignent le réseau pour la première fois. Ils assurent leur authentification s'ils sont déjà enregistrés précédemment dans la Chaine de blocs.

B- Phase d'enregistrement d'un nouveau nœud :

Pour rejoindre le réseau, un nœud n_i vérifie en premier lieu s'il possède un identificateur et une paire de clés, si c'est le cas il s'authentifie auprès de réseau chaine de blocs. Cette authentification est assurée par un accumulateur d'authentification AutAcc qui accumule les clés publiques, identités des nœuds qui ont réussi à s'enregistrer dans le réseau Ad hoc. Dans le cas ou si la première fois il envoie une requête d'inscription dans le réseau BCN, un Nœud BN (NB_{ci}), se trouvant dans la zone N2 (n_i), répond par un challenge C_i. Le nœud n_i, une fois reçu le challenge C_i, génère via son PUF une réponse R_i à utiliser

pour générer sa clé privée. Le nœud n_i calcule sa propre clé publique correspondante à partir de la clé privée obtenu et ajoute le challenge correspondant dans sa mémoire non volatile NVM. Il diffuse un message d'enregistrement suivant :

$$M = (ID, IPA, PK, T, OP, Sig_{KS}(C_i))$$

Les nœuds validateurs NB de zone N2 (n_i) vérifient la signature pour prouver le lien entre la clé PK et SK. Si c'est le cas, chaque validateur génère un jeton d'acceptation JA signé, le nœud Nc_i reçoit les jetons des validateurs JA et produit une preuve d'identité PoId à partir de ces jetons $PoId = Sig_{KSNBci}(h(JA_{v1}||JA_{v2}\ldots))$, récompense les validateurs par un jeton signé par sa clé privée JR, génère un certificat pour le nœud n_i. Pour vérifier ce certificat chaque nœud du réseau Ad hoc peut solliciter le nœud NBc_i pour lui fournir la preuve d'identité PoId. L'adresse IP, identité de nouveau nœud, C_i et sa clé publique sont enregistrées dans BCN en diffusant la transaction Tx via le réseau BCN.

C. Phase de communication :

Pour établir une communication entre deux nœuds n_1 et n_2, nous utilisons le principe de diffusion sélective via les nœuds MPRs. Une technique que nous appelons PoV (Proof-of-Veracity) est appliquée pendant la phase de découverte de route RREQ comme suit :

1. Le nœud source n_1 génère un nombre g, choisit p et q deux nombres premiers assez grands, calcul N=pq, choisit un nonce x à utiliser dans la chaine de hachage et un secret s0.
2. Le nœud source n_1 procède comme suit :
   - Calcule le hash $h^m(x)$ de nonce x qui va servir à la vérification de nombre de saut hc.
   - Produit un accumulateur AccVal initial $V_0 = g^{e_0} \bmod N$ avec $e_0 = h_0 \cdot s_0$, $h_0 = h^m(x)$
   - Diffuse via ces nœuds MPRs une requête RREQ avec les paramètres suivants : V_0, N, h_0, $E_{KPD}(x,m)$, T, $Sig_{KS}(RREQ)$
3. Nœud intermédiaire n_i :
   - message reçu est une demande RREQ :
     - S'il possède une route vers la destination n_2, il génère une réponse RREP toute en ajoutant les informations $(S, D2, V, H_{cf}, Wit, s_i, h_i, E_{KSD}(x,m), T, sig_D(S, D, V, H_{cf}))$ signées avec sa clé privée KS_i. Ces informations constituent la preuve qui va servir à la source n_1 de s'assurer de la véracité des informations fournies dans la réponse RREP tout en vérifiant que le nœud intermédiaire n_i possède un chemin vers la destination n_2 comme il

le prédit en exécutant Verify. Dans ce cas n_2 peut être un nœud source ou nœud destination dans une route déjà enregistrée dans sa table de routage.

- S'il n'a pas d'information et dans le cas où il est désigné comme MPR de nœud précédent, il exécute UpdEle pour accumuler son secret, il diffuse la demande RREQ :

  Vi, N, h_i, EKPD(x,m), T, sig(RREQ) avec $V_i=V_{i-1}{}^{e_i}$ Mod N , $e_i=h_i*s_i$

- Sinon il arrête la propagation de la requête de la demande RREQ.

▪ message reçu est une réponse RREP d'origine la destination n_2 :

- Il exécute WitGen pour générer son témoin d'appartenance à la route reliant la source n_1 et la destination n_2.
- Il extrait les informations complémentaires nécessaires pour la preuve de future réponse à une demande de route vers la source n1 ou la destination n2 par d'autres nœuds.

4. Le nœud destination n_2 :

   Pour plus de sécurité, le nœud n_2 participe au calcul de la valeur final de l'accumulateur V. Il génère un message RREP avec d'autres informations contenant Les valeurs V,m,H_{cf},x qui deviennent publics pour les membres de la route, ces informations portent sa signature pour assurer l'authenticité et l'intégrité de ces paramètres. Ces informations vont être utilisées dans une réponse RREP à une nouvelle RREQ qui pourrait venir d'un autre nœud qui sollicite soit n_1 ou n_2.

5. Le nœud n_1 traite les réponses de la même manière s'elles viennent de la destination, par contre si c'est d'un nœud intermédiaire, il exécute Verify en utilisant le témoin (witeness) et le secret de nœud ayant répondu par une RREP pour s'assurer que ce nœud possède une route vers la destination. Quant à la distance il utilise la chaine de hachage pour vérifier le nombre de saut qui sépare ce nœud de la destination.

Cas d'utilisation :

- ✓ L'agriculture intelligente : Nous pouvons mettre en place un système hybride Manet-IoT sécurisé afin de réaliser une interaction entre un réseau de capteurs sans fil et l'internet en passant par un réseau Ad hoc dont les utilisateurs sont le personnel de la ferme.

- ✓ Parcs d'attraction connecté : les citoyens arrivent dans ces parcs équipés de leurs smartphone ou autres, ils souhaitent être servi par les restaurants de voisinage .Un réseau ad hoc se met en place pour acheminer leur commandes vers un des restaurants d'une manière sécurisé.

Revendications :

1. Une méthode pour anticiper une attaque trou noir dans un réseau Ad hoc, les nœuds de dit réseau Ad hoc comprennent chacun un bloc de fonctions nonclonables physiquement PUF leur permettant une autogénération d'identité et une clé publique unique sans confusion avec celles des autres nœuds à partir d'un challenge C_i comprenant les phases suivantes :

a) Une première phase d'initialisation ou chaque nœud exécute le consensus preuve de capacité PoC pour élire le nœud tête de réseau chaine de blocs et former ledit réseau Chaine de blocs BCN.

b) Une seconde phase d'enregistrement ou chaque nœud génère et enregistre son identité et sa clé publique dans ledit réseau BCN en exécutant le consensus preuve d'identité PoId.

c) Une troisième phase de découverte de route entre deux nœuds de réseau ad hoc.

2. La méthode selon la revendication 1 caractérisée en ce que dans ladite phase d'initialisation un consensus PoC est lancé par tous les nœuds de réseau pour former un réseau chaine de blocs BCN ; ledit consensus est composé des étapes suivantes :
   - Calculer le vecteur de capacité VCap des nœuds de réseau Ad hoc
   - Elire un nœud tête de réseau de réseau chaine de blocs NBH
   - Informer l'ensemble MPR de nœud NBH pour passer en mode nœud chaine de blocs BN
   - Informer l'ensemble MPR de chaque nœud BN pour passer en mode BN

3. La méthode selon les revendications 1 et 2 caractérisée en ce que dans ladite phase d'enregistrement ledit consensus PoId est appliqué comme suit :
   - Pour rejoindre le réseau Ad hoc un nouveau nœud ordinaire NO diffuse une requête, un des nœuds validateurs NB se trouvant dans sa zone N2 répond par un challenge C_i ; ledit nœud NO applique ce dit challenge C_i à son système PUF pour générer son identité et ces clés de sécurité, ledit nœud NO soumet aux dits nœuds validateurs NB pour générer et enregistrer son certificat dans le réseau chaine de blocs.
   - Quant aux nœuds NB, ils s'enregistrent auprès de ces sélecteurs MPR.

4. La méthode selon les revendications 1,2 et 3 caractérisée en ce qu'elle intègre dans ladite phase de découverte de route entre un nœud source n1 et un nœud destination n2 une technique dite PoV pour vérifier et valider la véracité des informations contenues dans une réponse d'un nœud intermédiaire RREP moyennant un accumulateur cryptographique dynamique combiné à une chaine de hachage comme suit :
   - le nœud source n1 initialise un accumulateur V et calcule un $h_0^m(x)$ tout en gardant x et m secret.
   - chaque nœud participant à l'établissement de dite route applique une fonction de hachage sur le hache hn_{i-1} du nœud précédent et ajoute son secret combiné au hache calculé dans ledit accumulateur cryptographique V.
   - le nœud destination n2 envoie une réponse en divulguant des informations permettant aux nœuds intermédiaires de générer une preuve de possession PoV des informations sur la route reliant n1 et n2.
   - un nœud n3 sollicitant n1 ou n2 peut vérifier la véracité d'une réponse d'un nœud moyennant ladite preuve PoV.
5. La méthode selon les revendications 1,4 caractérisée en ce que ledit accumulateur est utilisé pour qu'un nœud présente la preuve de possession d'une route vers le nœud n1 ou n2.
6. Un Système selon les revendications 1,4, et 5 caractérisée en ce que l'utilisation de la chaine de hachage permet à un nœud de présenter la preuve de sa distance en nombre de sauts au dit nœud destination.
7. La méthode selon les revendications 1,2 et 3 caractérisée en ce que les nœuds dedit réseau Ad hoc passent d'un nœud ordinaire NO à un nœud chaine de blocs BN selon l'évolution de leur vecteur de capacité dans le temps.
8. La méthode selon les revendications 1, 2,3 et 7 caractérisée en ce que le réseau chaine de bloc BCN est dynamique.
9. La méthode selon les revendications précédentes caractérisées en ce que l'authentification des nœuds est assurée par un accumulateur cryptographique dynamique de clés publiques enregistrées dans le réseau chaines de blocs BCN.
10. La méthode selon l'une quelconque des revendications précédentes caractérisé en ce que le mode de diffusion sélective à base des nœuds relais multipoints MPR est utilisé.

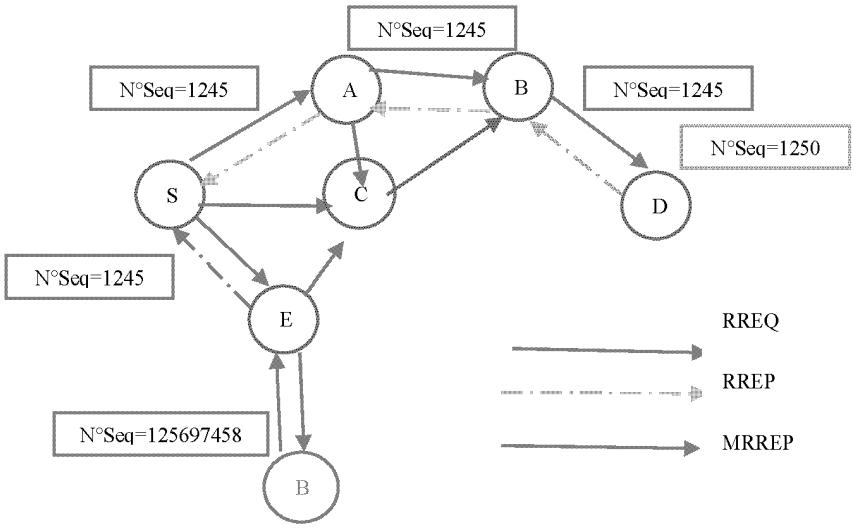

Figure 1

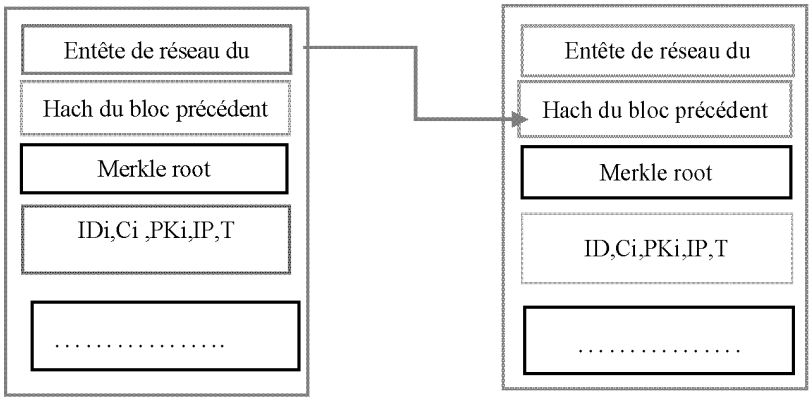

Figure 2

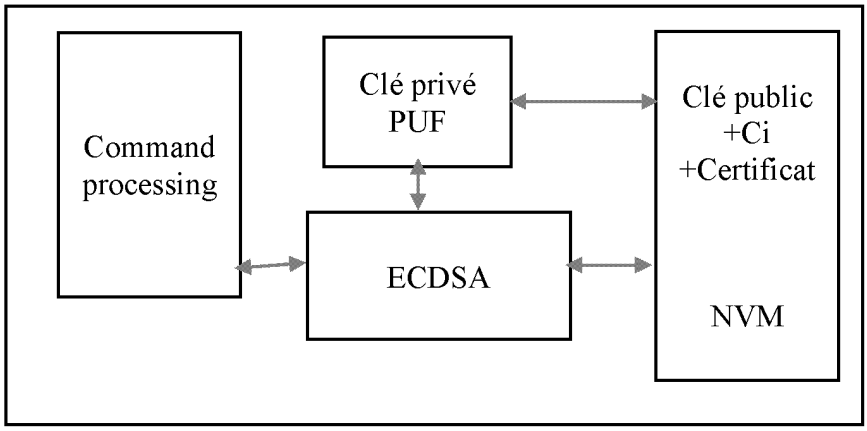

Figure 3

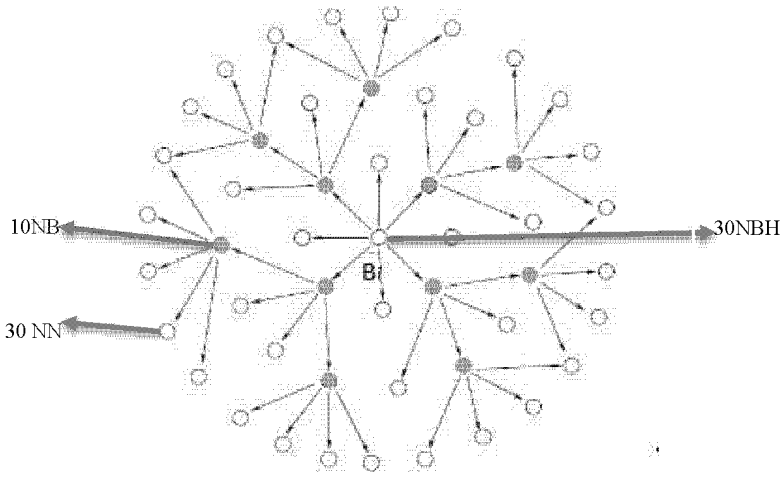

Figure 4

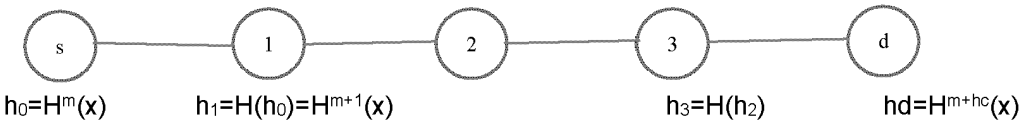

Figure 5

MA 50778B1

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 : 50778	Date de dépôt : 27/10/2020
Déposant : Université Mohammed V de Rabat	
Intitulé de l'invention : Méthode pour anticiper une attaque trou noir (Blackhole) dans les réseaux 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 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

Téléphone: **212 5 22 58 64 14/00**

Date d'établissement du rapport : 17/11/2020

ROYAUME DU MAROC OFFICE MAROCAIN de la PROPRIETE INDUSTRIELLE et COMMERCIALE 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
  9 Pages
- Revendications
  1-10
- Planches de dessin
  2 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : H04L45/00
CPC : H04L45/00

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	US9344418B2 ; Columbia University of New York ; 17/05/2016	1-10
A	CN103957097A ; UNIV HOHAI ; 30/07/2014	1-10

***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 1-10 Revendications aucune	Oui Non
Activité inventive	Revendications 1-10 Revendications aucune	Oui Non
Application Industrielle	Revendications 1-10 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 : US9344418B2

1. Nouveauté

Aucun document ne divulgue l'objet des revendications 1-10 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 pour anticiper une attaque trou noir dans un réseau Ad Hoc, à travers la génération d'une clé par chaque nœud du réseau.
L'objet de la revendication diffère de D1 en ce que : les nœuds du réseau Ad Hoc comprennent chacun un bloc de fonctions nonclonables physiquement PUF leur permettant une auto génération d'identité et une clé publique unique sans confusion avec celles des autres nœuds à partir d'un challenge Ci.

Le problème objectif que la présente demande se propose de résoudre peut donc être considéré comme : Fournir une alternative à la prévention des attaques Black Hole dans un réseau Ad Hoc.

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 dépendantes 2-10 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.