

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

(19) Organisation Mondiale de la
Propriété Intellectuelle
Bureau international



(43) Date de la publication internationale
26 juin 2014 (26.06.2014)

WIPO | PCT

(10) Numéro de publication internationale
WO 2014/094948 A1

(51) Classification internationale des brevets :
H04L 29/06 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2013/003461

(22) Date de dépôt international :
18 novembre 2013 (18.11.2013)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
12/03585 21 décembre 2012 (21.12.2012) FR

(71) Déposant : CASSIDIAN SAS [FR/FR]; 1 Boulevard Jean
Moulin, ZAC de la Clef Saint Pierre, F-78990 Elancourt
(FR).

(72) Inventeurs : DENIAUD, Thierry; 37 rue de la Gre-
nouillette, F-78180 Montigny le Bretonneux (FR). CAR-
NUS, Romain; 23 bis rue du Surmelin, F-75020 Paris
(FR).

(81) États désignés (sauf indication contraire, pour tout titre
de protection nationale disponible) : AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,

BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM,
ZW.

(84) États désignés (sauf indication contraire, pour tout titre
de protection régionale disponible) : ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,
UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ,
TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— relative à la qualité d'inventeur (règle 4.17.iv))

Publiée :

— avec rapport de recherche internationale (Art. 21(3))

(54) Title : METHODS FOR PROTECTING DATA TRANSMISSIONS AND FOR CARRYING OUT AN AUTHENTICATION CHECK OF AD HOC NETWORK NODES

(54) Titre : PROCEDES DE SECURISATION DE TRANSMISSIONS DE DONNEES ET DE CONTROLE D'AUTHENTIFICATION DE NOEUDS D'UN RESEAU AD HOC

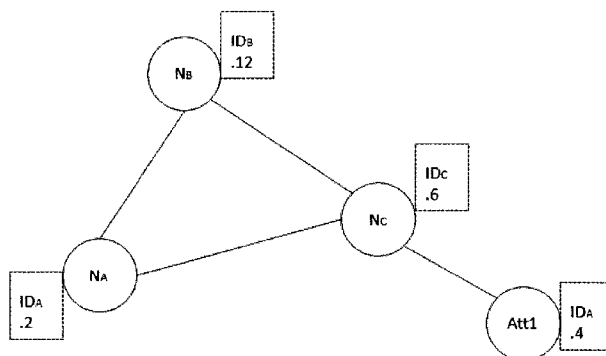


FIG. 3

(57) Abstract : Method for protecting data transmission in an ad hoc network comprising nodes, each node (Ni) comprising a private key (ki), a public key (Ki) and a certificate (Ci) of the public key (Ki) signed by a certification authority (CA). The first node (Na) transmits to the second node (Nb) : • a first message (M1) signed (M1/ka) with the private key of the first node (Na); • a third message (M3) containing a first set (ENS1) of initialisation data comprising: - a first certificate including the public key (KA) of the first node (Na), signed by the certification authority (CA), designated KA/kCA; - a second data set (ENS2) comprising: · the IP address (IPa) of the first node (Na); · and the first certificate associated with the IP address (IPa) of the first node (Na), wherein the second data set (ENS2/ka) is signed with the private key (ka) of the first node (Na).

(57) Abrégé :

[Suite sur la page suivante]



Le procédé de sécurisation de transmission de données dans un réseau ad hoc comportant des nœuds, chaque nœud (N_i) comportant une clef privée (k_i), une clef publique (K_i), un certificat (C_i) de la clef publique (K_i) signée par une autorité de certification (CA). Le premier nœud (N_A) transmet au second nœud (N_B) : • un premier message (M_1) signée (M_1/k_A) par la clef privée du premier nœud (N_A); • un troisième message (M_3) comportant un premier ensemble (ENS_1) de données d'initialisation comportant : - un premier certificat comprenant la clef publique (K_A) du premier nœud (N_A) signée par l'autorité de certification (CA), notée K_A/k_{CA} ; - un second ensemble de donnée (ENS_2) comportant : • l'adresse IP (IP_A) du premier nœud (N_A); • le premier certificat associé à l'adresse IP (IP_A) du premier nœud (N_A), le second ensemble de données (ENS_2/k_A) étant signé par la clef privée (k_A) du premier nœud (N_A).

PROCEDES DE SECURISATION DE TRANSMISSIONS DE DONNEES ET DE CONTROLE D'AUTHENTIFICATION DE NŒUDS D'UN RESEAU AD HOC

5 **Domaine Technique**

Le domaine de l'invention concerne la sécurisation des transmissions dans un réseau ad hoc et l'authentification des nœuds tels que des équipements réseaux ou terminaux. Une problématique réside dans l'architecture de tels réseaux dans lesquels la topologie est dynamique et
10 dans lesquels une grande flexibilité de configuration et une sécurité maximale doivent être fournies. Les approches centralisées des schémas de confiance et de distribution des clés ne peuvent convenir pour de tels réseaux. La décentralisation des contrôles d'accès et d'authentification implique que chaque nœud est capable de mettre en œuvre à minima
15 certaines exigences de sécurité pour préserver l'intégrité du réseau, pour préserver le réseau d'attaques, d'intrusions ou d'usurpation d'identités ou encore de substitution d'adresses réseaux.

Etat de la technique et problèmes techniques rencontrés

Les protocoles de routage permettent aux nœuds de connaître la
20 topologie du réseau, de calculer les routes pour joindre d'autres nœuds et de distribuer aux différents nœuds du réseau les routes ainsi calculées. En outre, un protocole de routage peut intégrer des éléments de sécurité pour sécuriser le réseau d'attaques internes ou externes (intrusion non-autorisée dans le réseau, usurpation d'identité, corruption des données d'un message,
25 etc.). La sécurisation du protocole de routage est nécessaire pour préserver l'intégrité du réseau.

Le protocole OLSR, dont l'acronyme signifie dans la terminologie anglo-saxonne : « Optimized Link State Routing Protocol », est particulièrement adapté aux réseaux ad hoc de type mobile et sans fil.

30 Ce protocole s'appuie sur l'utilisation de relais multipoints (MPR) et permet l'échange des informations de topologie (voisinage, état des liens, liste des voisins à un nœud l'ayant choisi comme MPR) entre les différents nœuds via les messages HELLO et TC. Ces informations de topologie permettent de construire les tables de routage utilisées dans le routage des
35 paquets de données.

En revanche, le protocole OLSR ne comprend pas toutes les couches de sécurité nécessaires à la protection complète d'un réseau ad hoc. A titre d'exemple, le protocole OLSR ne prend pas en compte les problématiques relatives à l'authentification, notamment vis-à-vis de l'arrivée d'un nouveau
5 nœud dans le réseau. Un nœud malicieux peut aussi usurper l'identité d'un nœud sain. Un nœud malicieux peut aussi corrompre les messages du protocole de routage pour transformer la topologie du réseau vue par tous les nœuds (y compris les nœuds sains) à sa guise.

Pour résoudre en partie la problématique de la sécurité et de la
10 prémunition contre des attaques extérieures et intérieures au réseau, les authentifications de nœuds, la distribution de clefs et la signature des messages peuvent permettre de sécuriser un réseau.

Pour cela, des solutions ont été proposées pour être compatible du protocole OLSR. Il existe le protocole SOLSR, désignant « Secure OLSR »
15 (basée sur des signatures pour l'authentification des paquets OLSR et sur l'utilisation de clés symétriques) ; la solution nommée « Web-of-trust OLSR extension » (basée sur des signatures pour l'authentification des paquets OLSR ; la distribution des clés s'effectuant par un principe basé sur le « PGP web-of-trust »). Ces solutions ont été implémentées sous formes de plug-ins
20 pour le démon OLSRd. Ces dernières améliorations permettent de prendre en compte certaines problématiques d'authentification de manière à répondre aux exigences d'un réseau sécurisé.

Une autre solution est une solution basée sur le protocole OLSR mettant en œuvre de nouveaux types de messages (message de signature)
25 pour authentifier les messages HELLO et TC. Ces messages permettent de distribuer des signatures, de mettre en œuvre des minuteurs ou encore de gérer le nombre et les séquences de messages pour effectuer des contrôles.

Un mécanisme de clef publique et de clefs privées peut être mis en œuvre pour permettre de crypter des données transmises dans le réseau. Un
30 mécanisme de distribution de certificats d'authentification peut être associé avec le précédent mécanisme pour garantir la confiance qu'un nœud peut porter à un autre nœud. Cette solution permet d'augmenter le niveau de sécurité d'un réseau mobile ad hoc.

En revanche, de tels mécanismes ne permettent pas d'éviter les attaques internes provenant du réseau telles que celles connues sous le nom « link-spoofing » (mascarade).

Concernant la distribution des éléments de sécurité nécessaires pour l'authentification des nœuds, deux approches existent :

- une approche centralisée (exemples : Kerberos plutôt pour des réseaux fixes ; « Public Key Infrastructure » s'appuyant sur une autorité de certification mais nécessitant la présence constante d'une entité centrale) ;
- une approche décentralisée (exemples : « web-of-trust » type PGP mais avec des problèmes de distribution des certificats ; « Public Key Infrastructure » distribué).

Exposé de l'invention

L'invention permet de résoudre les inconvénients précités.

L'invention propose un procédé de sécurisation de données transmises à l'émission et de contrôle de ces données à la réception, en utilisant une clef public pour protéger notamment les messages de contrôle CT du protocole OLSR.

Un premier objet de l'invention concerne un procédé de sécurisation de transmission de données dans un réseau ad hoc, ledit réseau comportant une pluralité de nœuds, les données étant transmises selon un protocole de routage d'un premier nœud vers un second nœud, chaque nœud comportant une clef privée k_i , une clef publique K_i , un certificat C_i de la clef publique K_i signée par une autorité de certification CA.

En outre, le premier nœud transmet au second nœud :

- au moins un premier message signée M_1/k_A par la clef privée du premier nœud ;
- au moins un troisième message vers le second nœud lorsqu'un second message provenant du second nœud est reçu par le premier nœud suite à l'émission du premier message, le troisième message comportant un premier ensemble de données d'initialisation comportant :
 - un premier certificat comprenant la clef publique du premier nœud signée par l'autorité de certification, notée K_A/k_{CA} ;
 - un second ensemble de données ENS_2 comportant :
 - l'adresse IP du premier nœud ;
 - le premier certificat associé à l'adresse IP du premier nœud,

le second ensemble de données ENS_2/k_A étant signé par la clef privée du premier nœud.

Avantageusement, chaque nœud comporte, en outre, une clef privée temporaire k_{ti} et une clef public temporaire K_{ti} , les clefs temporaires
5 comportant une durée de vie prédéfinie, le premier ensemble de données comportant également :

- un second certificat comprenant la clef publique temporaire K_{tA} du premier nœud signée par la clef privée du premier nœud, notée K_{tA}/k_A ;

- un troisième ensemble de donnée ENS_3 comportant en outre :

10 i. l'adresse IP du premier nœud;

ii. le second certificat associé à l'adresse IP du premier nœud,

le troisième ensemble de données ENS_3/k_{tA} étant signé par la clef privée temporaire du premier nœud.

Un second objet de l'invention concerne un procédé de sécurisation
15 de transmission de données dans un réseau ad hoc, ledit réseau comportant une pluralité de nœuds, les données étant transmises selon un protocole de routage d'un premier nœud vers un second nœud, chaque nœud comportant une clef privée k_i , une clef publique K_i , un certificat C_i de la clef publique signée par une autorité de certification CA, une clef privée temporaire k_{ti} et
20 une clef public temporaire K_{ti} , les clefs temporaires comportant une durée de vie prédéfinie.

En outre, le premier nœud transmet au second nœud :

- au moins un premier message signée M_1/k_{tA} par la clef privée temporaire du premier nœud ;

25 • au moins un troisième message vers le second nœud lorsqu'un second message provenant du second nœud est reçu par le premier nœud suite à l'émission du premier message, le troisième message comportant un troisième ensemble de données d'initialisation comportant :

- un second certificat comprenant la clef publique temporaire du
30 premier nœud signée par la clef privée du premier nœud, notée K_{tA}/k_A ;

- un quatrième ensemble de donnée ENS_4 comportant :

- l'adresse IP du premier nœud;

- le second certificat associé à l'adresse IP du premier nœud,

le quatrième ensemble de données ENS_4/k_{tA} étant signé par la clef
35 privée temporaire du premier nœud.

Avantageusement, le procédé de sécurisation de transmission désignant le second objet de l'invention peut être réalisé consécutivement au premier objet de l'invention.

Avantageusement, le $p^{\text{ième}}$ nœud transmet à un $q^{\text{ième}}$ nœud des données de routage provenant du premier nœud, dit « nœud générateur » du message, les $p^{\text{ième}}$ et $q^{\text{ième}}$ nœuds étant des nœuds calculés sur la route permettant d'acheminer un message du nœud générateur vers un nœud destinataire. Les dites données transmises du $p^{\text{ième}}$ nœud au $q^{\text{ième}}$ nœud comportant :

- 10 • au moins un premier message signée M_1/k_{tA} par la clef privée temporaire du premier nœud ;
- au moins un troisième message M_3 lorsqu'un second message M_2 provenant du second nœud est reçu par le premier nœud suite à l'émission du premier message, le troisième message comportant :
 - 15 • soit un premier ensemble de données d'initialisation comportant :
 - le premier certificat K_A/k_{CA} comprenant la clef publique (K_A) du premier nœud signée par l'autorité de certification CA, notée K_A/k_{CA} ;
 - un second ensemble de donnée ENS_2 comportant :
 - 20 ▪ l'adresse IP du premier nœud ;
 - le premier certificat associé à l'adresse IP du premier nœud,
 - le second ensemble de données ENS_2/k_A étant signé par la clef privée k_A du premier nœud.
 - soit un troisième ensemble ENS_3 de données d'initialisation comportant :
 - 25 ○ un second certificat K_{tA}/k_A comprenant la clef publique temporaire du premier nœud signée par la clef privée du premier nœud ;
 - un quatrième ensemble de donnée ENS_4 comportant :
 - 30 ▪ l'adresse IP du premier nœud ;
 - le second certificat associé à l'adresse IP du premier nœud,
 - le quatrième ensemble de données ENS_4/k_{tA} étant signé par la clef privée temporaire k_{tA} du premier nœud.

Un troisième objet de l'invention concerne un procédé de contrôle de données d'authentification par un second nœud, les données d'authentification permettant d'assurer la sécurisation d'échanges de données utiles transitant d'un premier nœud vers un second nœud, les

données d'authentification étant transmises par le premier nœud défini précédemment dans l'un des deux premiers objets de l'invention vers un second nœud.

Le procédé comprend :

- 5 • une extraction de données reçues par le second nœud dont :
 - le premier certificat K_A/k_{CA} extrait du premier message envoyé par le premier nœud et ;
 - le second ensemble de données ENS_2/k_A signé par la clef privée du premier nœud du troisième message;
- 10 • une génération d'un acquittement à la réception du premier message vers le premier nœud;
- un enregistrement des données extraites dans une mémoire du second nœud;
- une comparaison des certificats des deux messages contenus
- 15 dans respectivement les premier et troisième messages permettant une vérification de l'authentification du premier nœud.

Avantageusement, l'enregistrement des données est réalisé de sorte à faire correspondre bijectivement les trois données suivantes :

- 20 • une unique identification du premier nœud;
- une adresse IP du premier nœud;
- un premier certificat de la clef publique du premier nœud signé par l'autorité de certification.

Avantageusement, l'extraction de données reçues par le second nœud comprend l'extraction :

- 25 ○ d'un second certificat K_{tA}/k_A du premier message ;
- du quatrième ensemble de données ENS_4/k_{tA} signé par la clef temporaire privée k_{tA} du premier nœud du troisième message.

Avantageusement, l'enregistrement des données est réalisé de sorte à faire correspondre les trois données suivantes :

- 30 • une unique identification du premier nœud;
- une adresse IP du premier nœud ;
- un premier certificat de la clef publique du premier nœud signé par l'autorité de certification ;
- un second certificat K_{tA}/k_A de la clef publique temporaire K_{tA} du
- 35 premier nœud signé la clef privée du premier nœud.

Avantageusement, le protocole de routage est le protocole OLSR et que le premier message est un message de type HELLO ou TC.

Avantageusement, au moins un nœud comprend un terminal mobile.

Un autre objet de l'invention concerne un nœud d'un réseau ad hoc
5 sécurisant des transmissions de données par la mise en œuvre du procédé de sécurisation de l'invention.

Un autre objet de l'invention concerne un nœud d'un réseau ad hoc, contrôlant les données d'authentification d'un nœud émetteur par la mise en œuvre du procédé de sécurisation de l'invention.

10 **Brève description des figures**

D'autres caractéristiques et avantages de l'invention ressortiront à la lecture de la description détaillée qui suit, en référence aux figures annexées, qui illustrent :

- figure 1 : un modèle d'authentification de message de l'invention,
15 partagé par les différents services réseaux générant du trafic de contrôle ;
- figure 2 : un schéma d'architecture centré autour d'une base de données nommée ID TABLE, comprenant tous les éléments pour permettre l'authentification des messages et la sécurisation des protocoles ;
- figure 3 : une parade à l'intrusion dans le réseau par usurpation
20 d'identité, selon un procédé de l'invention ;
- figure 4 : une parade à l'intrusion dans le réseau par usurpation de l'adresse IP, selon un procédé de l'invention ;
- figure 5 : un exemple de stockage de données d'authentification par un nœud du réseau, selon un procédé de contrôle de l'invention ;
- 25 • figure 6 : un premier exemple d'échanges de données, selon le procédé de sécurisation de l'invention ;
- figure 7 : un second exemple d'échanges de données, selon le procédé de sécurisation de l'invention.

Description de l'invention

30 Dans la suite de la description, on nomme un « nœud générateur » : le premier nœud envoyant un message d'un protocole de routage vers un nœud destinataire, le message parcourant une route calculée par une table de routage et comprenant en général une pluralité de nœuds intermédiaires.

Un « nœud émetteur » est un nœud qui génère un message ou qui le transfère à un nœud voisin qui est sur une route à destination d'un nœud destinataire.

Un « nœud récepteur » est un nœud recevant un message qui lui est
5 soit destiné, soit non destiné. Dans ce dernier cas, le nœud récepteur après un traitement de données, tel qu'un contrôle d'authentification, autorise ou non le transfert du message vers le nœud destinataire ou le prochain nœud voisin sur la route.

Dans la suite de la description, les fonctions d'authentification
10 comprennent les fonctions habituellement utilisées pour les services d'authentification et comprennent également les procédés de l'invention qui constituent des services améliorant la sécurité des transferts de données dans un réseau ad hoc.

La figure 1 représente une architecture représentant les composants
15 essentiels pour la mise en œuvre des procédés de l'invention. Selon un mode de réalisation, le composant OLSR permet de traiter les messages entrants et sortants relatifs au protocole de routage OLSR. Les fonctions permettant la gestion de l'interface du nœud pour la réception et l'émission des messages de contrôle sont représentées par un composant « CONT.
20 MESS » sur la figure 1. Les interactions entre les composants OLSR et CONT. MESS sont représentées par le lien 12. Un nœud générateur vu par un nœud récepteur peut prendre part à la topologie du réseau et les informations et les données relatives au nœud générateur peuvent être ensuite sauvegardées dans la table « ID TABLE » qui est décrite ci-après
25 lorsque les messages OLSR ont été acceptés après contrôle d'authentification.

Un composant DDHCP permet de traiter les messages entrants et sortants relatifs au protocole DDHCP. Les interactions entre les composants DDHCP et CONT. MESS sont représentées par le lien 10. L'adresse IP
30 obtenue par le protocole peut être ensuite sauvegardée dans la table « ID TABLE » qui est décrite ci-après lorsque les messages ont été acceptés après contrôle d'authentification.

Un composant supplémentaire « DIST SE » permet de traiter les messages entrants et sortants relatifs à un service distribué autre que

DDHCP et OLSR. Les interactions entre les composants DIST SE et CONT. MESS sont représentées par le lien 11.

Un composant AUTH MOD prend en charge les opérations pour vérifier la validité de l'authentification (vérification de signature) pour les messages entrants associés aux protocoles DDHCP (lien 14), OLSR (lien 13) ou à tout autre service distribué (lien 15). Ce composant AUTH MOD prend aussi en charge le calcul des signatures des messages sortants associés aux protocoles DDHCP (lien 14), OLSR (lien 13) ou à tout autre service distribué (lien 15) lorsque le nœud est le nœud générateur du message. La méthode d'authentification pour protéger le trafic de contrôle est basée sur la cryptographie à clé publique. Les services distribués doivent être adaptés pour que les messages protocolaires transportent signature et identifiant..

Le composant CERT DB permet la gestion des certificats d'authentification du nœud et des certificats d'authentification connus du nœud qui les stocke. Les certificats d'authentification peuvent être sauvegardés dans une base qui est régulièrement mise jour. Une interface permet aux fonctions de contrôle et de gestions des données d'authentification d'accéder aux certificats d'authentification CERT DB.

Le composant O SSL permet de stocker les outils cryptographiques servant aux fonctions d'authentifications du composant AUTH MOD. Il peut s'agir d'une bibliothèque de fonctions telle que par exemple une fonction de hachage ou encore une fonction chiffrement de données. Le composant AUTH MOD accède au services du composant O SSL au moyen d'une interface 17.

Enfin, le composant AUTH MOD avec le composant CERT DB permettent la sauvegarde de données d'authentification et leur organisation de manière à garantir l'authentification des nœuds entrant en communication avec le nœud considéré dans la figure 1. En outre, le composant AUTH MOD permet d'assurer un degré élevé de sécurité notamment en ce qui concerne les intrusions extérieurs et les substitutions au sein même du réseau. Les composants AUTH MOD et CERT DB permettent l'exécution des procédés de l'invention et sont détaillés ci-après.

La figure 2 permet de décrire plus en détail les différentes fonctions nécessaires à la réalisation des procédés de l'invention. Le composant

CERT DB comprend une table de données regroupant différentes données d'authentifications stockées dans un nœud. Les données d'authentifications concernent les données de nœuds connus d'un nœud donné du réseau notamment ceux stockés dans la table de routage, notée ROU PROT, dans la figure 2. Notamment, les données d'authentification sont sauvegardées dans une table 26, notée ID TABLE, sur la figure 2. La table ID TABLE permet d'associer à un identifiant d'un nœud connu, un certificat d'authentification correspondant. Cette association permet de contrôler l'authentification d'un message reçu provenant d'un nœud connu de la table de routage. La table ID TABLE peut être stockée dans le composant CERT DB.

Le procédé de contrôle de l'invention permet la mise à jour de l'ID TABLE au moyen d'un protocole d'échange de certificats représenté par le bloc CERT EXCH PROT et le lien 20. Les fonctions d'authentification réalisées par le composant AUTH MOD permettent de réaliser des opérations utilisant les données stockées dans l'ID TABLE et les données extraites des messages entrants (vérification de signature).

Notamment, l'authentification des messages entrants relatifs au protocole DDHCP peuvent être réalisées au niveau du composant assurant la mise en œuvre du protocole d'adressage DDHCP via le composant AUTH MOD par la vérification de la signature de messages entrants. En utilisant l'identifiant contenu dans la signature, le service peut récupérer les certificats correspondants dans l'ID TABLE du composant CERT DB pour la vérification de signature et peut vérifier que l'adresse IP correspond à celle du nœud générateur. Les liens 21 et 22 entre l'ID TABLE et la fonction authentification AUTH1 du composant AUTH MOD utilisant son interface avec le composant DDHCP est illustré sur la figure 2.

Notamment, l'authentification des messages entrants relatifs au protocole OLSR peuvent être réalisées au niveau du protocole de routage OLSR via le composant AUTH MOD par la vérification de la signature de messages entrants. En utilisant l'identifiant contenu dans la signature, le service peut récupérer les certificats correspondants dans l'ID TABLE du composant CERT DB pour la vérification de signature et peut vérifier que l'adresse IP correspond à celle du nœud générateur. Le lien 24 entre l'ID

TABLE et la fonction authentification AUTH2 du composant AUTH MOD utilisant le composant OLSR est illustré sur la figure 2.

Un avantage de l'architecture permettant la réalisation des procédés de l'invention est que les fonctions d'authentification sont réalisées
5 indépendamment du protocole d'échange de certificats.

La table de routage d'un nœud, notée ROUT PROT, est représentée sur la figure 2. Elle s'interface nécessairement avec la couche OLSR permettant d'implémenter les fonctions relatives au protocole de routage du réseau ad hoc. Cette interface est représentée par le lien 25 de la figure 2.

10 Une interface 23 entre la table de routage ROUT PROT et l'ID TABLE permet d'effectuer des contrôles et des synchronisations entre la table de routage et la table ID TABLE.

Un autre protocole de routage qu'OLSR, de la même famille qu'OLSR (protocole de routage proactif) pourrait néanmoins être utilisé dès lors que
15 les étapes des procédés de l'invention puissent s'appuyer sur les fonctions nécessaires d'un tel protocole de routage.

Les figures 3 et 4 représentent respectivement un cas d'une usurpation d'identité d'un nœud (figure 3) et un cas d'une usurpation d'adresse IP (figure 4). Les procédés de l'invention permettent d'éviter de
20 telles attaques au sein du réseau.

Notamment, l'ID TABLE permet de faire correspondre de manière bijective : un identifiant d'un nœud, une adresse IP et un certificat d'authentification.

Un objectif de la table ID TABLE est de permettre la construction
25 d'une table sécurisée comprenant la liste des nœuds ayant des certifications d'authentification validés et comportant des données de confiance vis-à-vis des nœuds connus de la table de routage. Ainsi un premier nœud qui est authentifié par un second nœud après un contrôle d'authentification par échanges de certificats selon le procédé de l'invention pourra transmettre
30 des messages provenant de ce nœud à un autre nœud. De cette manière, la confiance d'un nœud se propage de proche en proche par un contrôle de nœud à nœud.

Un autre objectif de la table ID TABLE est de stocker les informations relatives aux données d'authentification des autres nœuds de sorte à pouvoir
35 mettre à jour ces données constamment.

Lorsqu'un nœud rejoint le réseau pour la première fois, son adresse IP ne lui est peut-être pas encore attribuée lorsqu'il tente de joindre un nœud du réseau. Dans ce dernier cas, l'ID TABLE ne prend pas en compte le champ d'adresse IP du nœud dans la table ID TABLE et ne compare donc pas cette
5 entrée avec le champ vide d'adresse IP des messages reçus. L'adresse IP sera, par la suite, ajoutée aux données d'authentification dans la table lorsque l'identification du nœud en question sera reconnue.

La figure 3 représente un réseau dans lequel les nœuds suivants sont illustrés avec leurs données d'adressage et d'identifiants :

- 10 • un premier nœud N_A a une adresse IP .2 et un identifiant ID_A ;
- un second nœud N_B a une adresse IP .12 et un identifiant ID_B ;
- un troisième nœud N_C a une adresse IP .6 et un identifiant ID_C .

Un nœud tiers noté Att1 tente une attaque en usurpant l'identifiant du nœud N_A : ID_A et une adresse IP .4.

- 15 Le procédé de contrôle de l'invention permet notamment d'organiser les données d'authentification de nœuds voisins, de manière à ce qu'un unique identifiant d'un nœud soit associé à une unique adresse IP et à un unique certificat d'authentification du même nœud.

- 20 Ainsi la configuration représentée à la figure 3 peut être détectée grâce aux fonctions d'authentification exploitant les données stockées et mises à jour dans l'ID TABLE par la comparaison des données des messages entrants et des données stockées dans l'ID TABLE.

La figure 4 représente un réseau dans lequel les nœuds suivants sont illustrés avec leurs données d'adressage et d'identifiants :

- 25 • un premier nœud N_A a une adresse IP .2 et un identifiant ID_A ;
- un second nœud N_B a une adresse IP .12 et un identifiant ID_B ;
- un troisième nœud N_C a une adresse IP .6 et un identifiant ID_C ;
- un quatrième nœud N_D a une adresse IP .4 et un identifiant ID_D ;
- un cinquième nœud N_E a une adresse IP .2 et un identifiant ID_E .

- 30 Le cinquième nœud N_E tente une attaque de l'intérieur du réseau par usurpation de l'adresse IP .2 du premier nœud N_A .

- 35 Le procédé de contrôle de l'invention permet notamment d'organiser les données d'authentification de nœuds voisins, de manière à ce qu'une unique adresse IP d'un nœud soit associée à un unique certificat d'authentification du même nœud et à son identifiant.

Ainsi la configuration représentée à la figure 4 peut être détectée grâce aux fonctions d'authentification exploitant les données stockées et mises à jour dans l'ID TABLE par la comparaison des données des messages entrants et des données stockées dans l'ID TABLE.

5 Lorsqu'un message est reçu et authentifié par un nœud, le composant d'authentification AUTH MOD traite les données d'authentification de sorte à les enregistrer dans l'ID TABLE, soit en créant une nouvelle entrée pour un nouveau nœud, soit en mettant à jour des données déjà enregistrées.

10 Lorsque les données contrôlées sont identiques à des données déjà présentes dans l'ID TABLE, l'ID TABLE n'est pas mise à jour. En revanche, une comparaison de données permet de vérifier l'authentification de messages provenant d'un nœud connu de la table de routage et donc de l'ID TABLE.

15 Les messages reçus lorsqu'ils sont signés peuvent être vérifiés grâce aux certificats enregistrés dans la table ID TABLE. Dans ce cas l'interrogation de la base peut s'effectuer en comparant l'adresse IP du message reçu et l'adresse IP correspondante stockée dans l'ID TABLE.

Une autre entrée possible est celle des identifiants des nœuds.

La figure 5 représente une table 26 ID TABLE comportant :

- 20 • les identifiants ID des nœuds connus de la table de routage ROUT PROT d'un nœud : ID_A , ID_B , ID_C ;
- les adresses IP des nœuds connus des données référencés dans le composant DDHCP : IP_A , IP_B , IP_C ;
- les certificats C_i , notés CERT (K) sur la figure 5, des clefs publiques K_i des nœuds i connus de la table de routage d'un nœud, lesdites clefs étant signées par une autorité de certification CA, les certificats sont également notés K_i/K_{CA} ,
- 25 • les certificats C_{ti} , notés CERT TEMP (K_t) sur la figure 5, des clefs publiques temporaires K_{ti} de nœuds i connus de la table de routage d'un nœud, lesdites clefs publiques temporaires étant signées par la clef privée k_i du nœud i , ces certificats sont également notés K_{ti}/k_i .
- 30

35 Parmi les fonctions d'authentification de l'invention, l'une d'elle comprend un procédé de sécurisation de transmission des données dans le réseau. Le procédé est mis en œuvre pour la sécurisation des transmissions des données de deux nœuds adjacents communiquant au travers du réseau.

De cette manière, la sécurisation des transmissions est assurée par la mise en œuvre du procédé de proche en proche d'un premier nœud générateur de messages vers un nœud destinataire. Entre le nœud générateur et le nœud destinataire, les nœuds coopèrent de proche en proche en transférant les données après un contrôle des données à transmettre.

La figure 6 représente une transmission de messages d'un protocole de routage d'un nœud N_A vers un nœud N_B . Le nœud N_A est un nœud générateur de messages. Le nœud N_E est le nœud destinataire des messages provenant du nœud N_A .

Les nœuds N_B , N_C , N_D représentent des nœuds transférant, selon une route calculée, les messages du nœud N_A vers le nœud N_E .

Le procédé de sécurisation des données transmises permet de sécuriser le transfert d'un premier nœud sur la route calculée vers son nœud aval et ainsi de suite jusqu'au nœud destinataire.

Le procédé de sécurisation de l'invention s'appuie sur l'exploitation de données d'authentification qui ont été distribuées dans les nœuds du réseau. Parmi ces données distribuées, une clef privée k_i , une clef publique K_i ont été distribuées à chaque nœud N_i . Les données d'authentification peuvent être distribuées par une autorité de certification.

En outre, un certificat est généré avec notamment la clef publique K_i et est signée par l'autorité de certification CA. Un certificat auto-signé par l'autorité de certification CA peut être également transmis de manière à distribuer la signature de l'autorité de certification. Ce certificat permet notamment d'effectuer les contrôles des signatures lors de la réception de messages signés.

La figure 6 représente donc une première transmission du nœud N_A vers le nœud N_B . Le nœud N_A transmet un message au nœud N_B d'un protocole de routage par exemple OLSR qui peut être par exemple un message HELLO ou TC.

Selon un premier mode de réalisation du procédé de l'invention, au moins un message M_1 transmis est signé par la clef privée du nœud N_A , le message signé est noté M_1/k_A .

Une étape préliminaire consiste à comparer l'identifiant ID du nœud générateur N_A avec la liste des identifiants ID des nœuds connus et compris dans la table ID TABLE. L'identifiant ID peut être transmis par l'intermédiaire

des messages du protocole OLSR, tel que le message M_1 qui peut être soit un message HELLO, soit un message TC.

Si l'identifiant est connu et authentifier grâce à la signature, alors le message M_1 est transféré au prochain nœud se situant sur la route calculée par le protocole de routage. Si l'identifiant est inconnu ou comporte des données d'authentifications incomplètes ou non à jour, alors le procédé de sécurisation des données transmises peut être activé.

Dans ce dernier cas, lorsque le nœud N_B reçoit le premier message M_1 , une fonction d'authentification peut stocker la signature du message M_1 .
Un second message M_2 est émis du nœud N_B vers le nœud N_A de manière à demander un troisième message M_3 .

Un troisième message, sur requête du nœud N_B , est donc généré par le nœud N_A vers le nœud N_B . Le troisième message M_3 permet de transmettre des données d'authentifications du nœud N_A pour sécuriser le transfert des messages au travers du réseau. Le message M_3 comprend des données ENS_1 comportant :

- un premier certificat comprenant la clef publique K_A du premier nœud N_A signé par l'autorité de certification CA, notée K_A/k_{CA} ;
- un ensemble de donnée ENS_2 comportant :
 - l'adresse IP_A du premier nœud N_A ;
 - le premier certificat associé à l'adresse IP_A du premier nœud N_A .

En outre, l'ensemble de données ENS_2/k_A , aussi noté $\{IP_A ; K_A/K_{CA}\}/k_A$, est signé par la clef privée k_A du premier nœud N_A .

Lorsque le nœud N_A n'a pas encore d'adresse IP, l'adresse IP_A n'est pas envoyée parmi les données ENS_2 . Les données sont stockées dans le nœud N_B .

La comparaison des données du message M_1 et M_3 permet d'authentifier le générateur de messages M_1 et d'établir un lien de confiance entre les deux nœuds. La signature des certificats par l'autorité de certification permet de renforcer ce lien de confiance entre les deux nœuds.

Les données d'authentification du nœud N_A sont sauvegardées dans la table ID TABLE du nœud N_B : l'identifiant du nœud N_A , l'adresse IP du nœud N_A et le certificat du nœud N_A lorsque ces derniers ne sont pas

présents dans la table ID TABLE ou que les valeurs ne sont pas identiques à celles décodées des messages.

Le message M_3 , qui comprend l'ensemble de donnée ENS_2 qui comporte l'adresse IP du nœud A et la clef publique signée, permet :

- 5 • d'une part, de garantir que le premier message M_1 est bien un message en provenance du nœud N_A et ;
- d'autre part, d'associer une adresse IP du nœud N_A à un unique certificat d'authentification et ;
- enfin, de garantir que le nœud N_A est bien en possession de la clé
- 10 privée k_A .

Ainsi le nœud N_B a établi un lien sécurisé avec le nœud N_A de manière à traiter tous les messages signés du nœud N_A suite à cette phase d'authentification.

Un autre mode de réalisation de l'invention peut être également traité

15 soit en concurrence de ce premier mode, soit de manière complémentaire.

Dans ce second mode, au moins un message M_1 transmis par le nœud N_A est signé par une clef privée temporaire du nœud N_A , le message signé est noté M_1/k_{tA} .

Une clef privée temporaire d'un nœud donné est générée par le nœud

20 lui-même à partir des données d'authentification qui ont été transmises et certifiées par une autorité de certification. Ainsi, une partie de la gestion de la sécurité est déléguée à chaque nœud à partir de ces données d'authentification.

La requête contenue dans le message M_2 est similaire dans le second

25 mode de réalisation au premier mode de réalisation. Lorsque le nœud N_B reçoit le premier message M_1 , une fonction d'authentification peut stocker la signature du message M_1 . Un second message M_2 est émis du nœud N_B vers le nœud N_A de manière à demander un troisième message M_3 .

Un troisième message, sur requête du nœud N_B , est donc généré par

30 le nœud N_A vers le nœud N_B . Le troisième message M_3 comprend des données ENS_1 comportant :

- un premier certificat comprenant la clef publique K_A du premier nœud N_A signé par l'autorité de certification CA, noté K_A/k_{CA} ;
- un second certificat, notée K_{tA}/k_A , comprenant la clef publique
- 35 temporaire K_{tA} du premier nœud N_A signée par la clef privée k_A du nœud N_A ;

- un ensemble de donnée ENS_2 comportant :
 - l'adresse IP_A du premier nœud N_A ;
 - le premier certificat associé à l'adresse IP_A du premier nœud N_A .

5 En outre, l'ensemble de données ENS_2/k_A , aussi noté $\{IP_A ; K_A/K_{CA}\}/k_A$, est signé par la clef privée k_A du premier nœud N_A .

- un ensemble de donnée ENS_3 comportant :
 - l'adresse IP_A du premier nœud N_A ;
 - le second certificat associé à l'adresse IP_A du premier nœud N_A .

10

En outre, l'ensemble de données ENS_3/k_{tA} , aussi noté $\{IP_A ; K_{tA}/K_A\}/k_{tA}$, est signé par la clef privée temporaire k_{tA} du premier nœud N_A .

Le nœud N_B peut ne demander via le message M_2 que le second certificat et l'ensemble ENS_3 s'il connaît déjà le nœud N_A (le nœud N_A apparaît déjà dans l'ID TABLE).

15

Ce mode de réalisation permet de ne pas utiliser à de trop nombreuses reprises les clés maîtres distribuées par l'autorité de certification CA. Seules les clés temporaires sont utilisées pour signer les messages de manière à éviter les attaques dans le réseau.

20

Les deux modes de réalisation sont complémentaires dans la mesure où une première authentification peut être effectuée avec la signature de l'autorité de certification entre deux nœuds. Puis par la suite, des clés temporaires peuvent être utilisées de manière à limiter l'utilisation des clés maîtres distribués par l'autorité de certification CA. Un avantage de cette utilisation complémentaire de ces deux modes de réalisation est de pouvoir

25 changer de clés temporaires fréquemment, de sorte à garantir un haut niveau de sécurité dans le réseau ad hoc tout en limitant le trafic généré par ces messages.

25

Un autre avantage est de gérer une sécurisation des transmissions de proche en proche, c'est-à-dire d'un nœud à un autre.

30

A chaque réception d'un message OLSR signé, le nœud récepteur du message M_1 engage le procédé de contrôle de sorte à valider la signature et l'authenticité du message du nœud émetteur et/ou du nœud générateur avant de traiter le message ou de le transférer.

Chaque nœud émet des messages OLSR, tel que des messages TC, dans le réseau. La propagation des messages OLSR dans le réseau permet aux nœuds découvrant un nouveau nœud ou un nœud ayant changé de données d'authentification, tel qu'un nouveau certificat, d'engager un procédé de sécurisation des transmissions avec ce nouveau nœud.

La figure 7 illustre ce fonctionnement de déploiement de la sécurisation des transmissions de proche en proche au travers le réseau.

Le nœud N_C transmet le message M_1 au nœud N_D . Le message M_1 est en provenance du nœud N_A et à destination du nœud N_E . Les nœuds entre le nœud N_A et le nœud N_E sont des nœuds de transitions qui visent à contrôler l'authentification du nœud N_A puis à transférer les messages provenant de ce nœud s'il est de confiance vers un nœud destinataire. La sécurisation du transfert s'effectue de proche en proche.

Si par exemple le nœud N_D ne comporte pas d'entrée dans la table ID TABLE du nœud N_A , un fonctionnement analogue que celui décrit précédemment se produira entre deux nœuds consécutifs.

Le message M_1 est signé par la clef privée du nœud N_A , soit la clef privée maître soit la clef privée temporaire selon le mode de réalisation. Un message M_2 est généré du nœud N_D vers le nœud N_C à réception du message M_1 par le nœud N_D .

Le nœud N_C qui a préalablement authentifié le nœud N_A comme un nœud « sûr », peut transmettre le message M_1 et transférer les données contenues dans le message M_3 car le nœud N_C a lui-même sauvegardé ces informations dans sa table ID TABLE.

Le message M_3 est donc envoyé du nœud N_C vers le nœud N_D , sur requête du nœud N_D . Le troisième message M_3 comprend des données ENS_1 comportant, selon le mode de réalisation retenu :

- le premier certificat ou le premier et le second certificats, comme défini précédemment ;

- un ensemble de données ENS_2 ou les ensembles de données ENS_2 et ENS_3 comportant :

- l'adresse IP_A du premier nœud N_A ;
- le premier ou le second certificat associé à l'adresse IP_A du premier nœud N_A selon qu'il s'agit de l'ensemble de données ENS_2 ou ENS_3 .

En outre, l'ensemble de données ENS_2/k_A ou ENS_3/kt_A , est signé respectivement soit par la clef privée du nœud N_A soit par la clef privée temporaire du nœud N_A .

La table ID TABLE peut stocker pour chaque entrée, c'est-à-dire pour
5 chaque nœud nouvellement authentifié : son adresse IP, son identifiant, un premier certificat comprenant la clef publique du nœud signé par l'autorité de certification CA, un second certificat comprenant la clef publique temporaire du nœud signé par la clef privée du nœud. La table ID TABLE peut comprendre en outre :

- 10 • un premier ensemble de données signé par la clef privée du nœud générateur du message, également considérée comme une première association comportant :
 - l'adresse IP du nœud générateur du message, soit N_A dans l'exemple.
 - 15 ○ le premier certificat.
- un second ensemble de données signé par la clef privée temporaire du nœud générateur du message, N_A , également considérée comme une seconde association comportant :
 - l'adresse IP du nœud générateur du message, soit N_A dans l'exemple.
 - 20 ○ le second certificat.

En outre, chaque nœud peut comporter une liste de révocation des certificats :

- Les seconds certificats ont une durée de vie limitée et sont
25 renouvelés périodiquement. Les seconds certificats obsolètes sont révoqués. Les nouveaux seconds certificats sont transmis de proche en proche par les mécanismes illustrés au travers des figures 6 et 7. Chaque nœud met à jour sa liste de révocation des certificats lorsqu'il remplace dans ID TABLE l'ancien certificat par le nouveau.
- 30 • Le premier certificat peut être révoqué par le nœud le possédant.
 - S'il possède un nouveau premier certificat signé par l'autorité de certification, il remplace le premier certificat obsolète par le nouvel premier certificat, modifie le second certificat (maintenant signé par la nouvelle clé privée),
35 modifie les ensembles ENS_2 et ENS_3 en conséquence. Les

5 nouveaux premiers et seconds certificats sont transmis de proche en proche par les mécanismes illustrés au travers des figures 6 et 7. Chaque nœud met à jour sa liste de révocation des certificats lorsqu'il remplace dans ID TABLE l'ancien certificat par le nouveau.

- 10 ○ S'il ne possède pas de nouveau premier certificat signé par l'autorité de certification, il doit transmettre un message M_4 signé par la clé privée en vigueur vers les nœuds de confiance les plus proches qu'il connaît (via ID TABLE et table de routage) indiquant qu'il souhaite révoquer tous ses certificats. A la réception d'un message M_4 et après contrôle de son authenticité, le nœud récepteur met à jour sa table ID TABLE en supprimant l'entrée relative au nœud générateur du message M_4 et sa liste de révocation des
15 certificats et envoie un acquittement M_5 signé par sa clé privée temporaire vers le nœud générateur du message M_4 . Le nœud générateur supprime définitivement ses éléments de sécurité dès lors qu'il a reçu suffisamment de message M_5 dont il a contrôlé l'authenticité. Il est noté que hors
20 réseau, l'autorité de certification doit être informée de la révocation d'un certificat qu'elle avait signé pour qu'il puisse mettre à jour sa propre liste de révocation.

Un état intermédiaire « en suspens » entre non révoqué et révoqué peut être introduit pour qu'un nœud fasse part d'un comportement erratique
25 d'un autre nœud. Cette information est introduite dans la liste de révocation des certificats du nœud ayant fait cette observation. La révocation des certificats du nœud en question ne peut être faite que par le nœud en question ou l'autorité de certification.

La liste de révocation des certificats gérée par un nœud peut être
30 transmise aux autres nœuds sur modification et périodiquement par l'intermédiaire d'un message M_6 signé par sa clé privée temporaire. La révocation d'un certificat par l'intermédiaire des messages M_6 n'est prise en compte par un nœud (modification de sa liste de révocation des certificats) que s'il reçoit et authentifie la révocation du certificat de suffisamment de
35 nœuds de confiance.

- La liste de révocation des certificats gérée par l'autorité de certification peut être transmise aux nœuds via des nœuds du réseau par l'intermédiaire d'un message M_7 signé par l'autorité de certification. La révocation d'un certificat par l'intermédiaire des messages M_7 est immédiatement prise en
- 5 compte par un nœud après authentification du message (modification de sa liste de révocation des certificats).

REVENDICATIONS

1. Procédé de sécurisation de transmission de données dans un
réseau ad hoc, ledit réseau comportant une pluralité de nœuds (N_i), les
données étant transmises selon un protocole de routage d'un premier nœud
(N_A) vers un second nœud (N_B), chaque nœud (N_i) comportant une clef
privée (k_i), une clef publique (K_i), un certificat (C_i) de la clef publique (K_i)
signé par une autorité de certification (CA), caractérisé en ce que le premier
nœud (N_A) transmette au second nœud (N_B) :

- au moins un premier message (M_1) signé (M_1/k_A) par la clef privée
du premier nœud (N_A) ;
 - au moins un troisième message (M_3) vers le second nœud (N_B)
lorsqu'un second message (M_2) provenant du second nœud (N_B) est reçu par
le premier nœud (N_A) suite à l'émission du premier message (M_1), le
troisième message (M_3) comportant un premier ensemble (ENS_1) de
données d'initialisation comportant :
 - un premier certificat comprenant la clef publique (K_A) du
premier nœud (N_A) signé par l'autorité de certification (CA),
noté K_A/k_{CA} ;
 - un second ensemble de donnée (ENS_2) comportant :
 - l'adresse IP (IP_A) du premier nœud (N_A) ;
 - le premier certificat associé à l'adresse IP (IP_A) du premier
nœud (N_A);
- le second ensemble de données (ENS_2/k_A) étant signé par la clef
privée (k_A) du premier nœud (N_A).

2. Procédé de sécurisation selon la revendication 1, caractérisé en
ce que chaque nœud comporte en outre une clef privée temporaire (k_{ti}) et
une clef publique temporaire (K_{ti}), les clefs temporaires comportant une
durée de vie prédéfinie, le premier ensemble de données (ENS_1) comportant
en outre :

- Un second certificat comprenant la clef publique temporaire (K_{tA})
du premier nœud (N_A) signé par la clef privée (k_A) du premier nœud (N_A),
noté K_{tA}/k_A ;
- un troisième ensemble de donnée (ENS_3) comportant en outre :

- l'adresse IP (IP_A) du premier nœud (N_A) ;
- le second certificat associé à l'adresse IP (IP_A) du premier nœud (N_A);

le troisième ensemble de données (ENS_3/k_{tA}) étant signé par la clef
5 privée temporaire (k_{tA}) du premier nœud (N_A).

3. Procédé de sécurisation de transmission de données dans un réseau ad hoc, ledit réseau comportant une pluralité de nœuds (N_i), les données étant transmises selon un protocole de routage d'un premier nœud (N_A) vers un second nœud (N_B), chaque nœud (N_i) comportant une clef
10 privée (k_i), une clef publique (K_i), un certificat (C_i) de la clef publique (K_i) signé par une autorité de certification (CA), une clef privée temporaire (k_{ti}) et une clef publique temporaire (K_{ti}), les clefs temporaires comportant une durée de vie prédéfinie, une nouvelle paire étant générée à la fin de vie de la paire précédente, caractérisé en ce que le premier nœud (N_A) transmette au
15 second nœud (N_B) :

- au moins un premier message (M_1) signé (M_1/k_{tA}) par la clef privée temporaire du premier nœud (N_A) ;
- au moins un troisième message (M_3) vers le second nœud (N_B) lorsqu'un second message (M_2) provenant du second nœud (N_B) est reçu par
20 le premier nœud (N_A) suite à l'émission du premier message (M_1), le troisième message (M_3) comportant un quatrième ensemble (ENS_4) de données d'initialisation comportant :

- un second certificat comprenant la clef publique temporaire (K_{tA}) du premier nœud (N_A) signé par la clef privée (k_A) du
25 premier nœud (N_A), notée K_{tA}/k_A ;
- un cinquième ensemble de donnée (ENS_5) comportant :
 - l'adresse IP (IP_A) du premier nœud (N_A) ;
 - le second certificat associé à l'adresse IP (IP_A) du premier nœud (N_A),

le cinquième ensemble de données (ENS_5/k_{tA}) étant signé par la clef
30 privée temporaire (k_{tA}) du premier nœud (N_A).

4. Procédé de sécurisation de transmission de données dans un réseau ad hoc, ledit réseau comportant une pluralité de nœuds (N_i), les données étant transmises selon un protocole de routage d'un premier nœud
35 (N_A) vers un second nœud (N_B), caractérisé en ce que le procédé selon l'une

des revendications 1 à 2 est effectué préalablement au procédé selon la revendication 3.

- 5 5. Procédé de sécurisation de transmission de données dans un réseau ad hoc, ledit réseau comportant une pluralité de nœuds (N_i), les données étant transmises selon un protocole de routage d'un $p^{\text{ième}}$ nœud (N_P) vers un $q^{\text{ième}}$ nœud (N_Q), chaque nœud (N_i) comportant une clef privée (k_i), une clef publique (K_i), un certificat (C_i) de la clef publique (K_i) signée par une autorité de certification (CA), une clef privée temporaire (k_{ti}) et une clef publique temporaire (K_{ti}), les clefs temporaires comportant une durée de vie
- 10 prédéfinie, une nouvelle paire étant générée à la fin de vie de la paire précédente, caractérisé en ce que le $p^{\text{ième}}$ nœud transmette à un $q^{\text{ième}}$ nœud des données de routage provenant du premier nœud (N_A), les dites données transmises comportant :
- au moins un premier message (M_1) signé (M_1/k_{tA}) par la clef privée
 - 15 temporaire du premier nœud (N_A) ;
 - au moins un troisième message (M_3) lorsqu'un second message (M_2) provenant du second nœud (N_Q) est reçu par le premier nœud (N_P) suite à l'émission du premier message (M_1), le troisième message (M_3) comportant :
 - 20 • soit un premier ensemble (ENS_1) de données d'initialisation comportant :
 - le premier certificat (K_A/k_{CA}) comprenant la clef publique (K_A) du premier nœud (N_A) signée par l'autorité de certification (CA), noté K_A/k_{CA} ;
 - un second ensemble de donnée (ENS_2) comportant :
 - 25 ■ l'adresse IP (IP_A) du premier nœud (N_A) ;
 - le premier certificat associé à l'adresse IP (IP_A) du premier nœud (N_A);
- le second ensemble de données (ENS_2/k_A) étant signé par la clef privée (k_A) du premier nœud (N_A).
- 30 • soit un premier ensemble (ENS_1) de données d'initialisation comportant en outre:
 - Un second certificat comprenant la clef publique temporaire (K_{tA}) du premier nœud (N_A) signé par la clef privée (k_A) du premier nœud (N_A), noté K_{tA}/k_A ;

- un troisième ensemble de donnée (ENS_3) comportant en outre :
 - l'adresse IP (IP_A) du premier nœud (N_A) ;
 - le second certificat associé à l'adresse IP (IP_A) du premier nœud (N_A);
 - le troisième ensemble de données (ENS_3/k_{tA}) étant signé par la clef privée temporaire (k_{tA}) du premier nœud (N_A).
 - soit un quatrième ensemble (ENS_4) de données d'initialisation comportant (si le procédé de sécurisation utilisant l'ensemble ENS_1 selon une des deux précédentes formes est effectué au préalable) :
 - un second certificat (K_{tA}/k_A) comprenant la clef publique temporaire (K_{tA}) du premier nœud (N_A) signée par la clef privée (k_A) du premier nœud (N_A) ;
 - un cinquième ensemble de donnée (ENS_5) comportant :
 - l'adresse IP (IP_A) du premier nœud (N_A) ;
 - le second certificat associé à l'adresse IP (IP_A) du premier nœud (N_A);
 - le cinquième ensemble de données (ENS_5/k_{tA}) étant signé par la clef privée temporaire (k_{tA}) du premier nœud (N_A).
6. Procédé de contrôle de données d'authentification par un second nœud (N_B), les données d'authentification permettant d'assurer la sécurisation d'échanges de données utiles transitant d'un premier nœud (N_A) vers un second nœud (N_B), les données d'authentification étant transmises par le premier nœud (N_A) selon un procédé de l'une des revendications précédentes, caractérisé en ce que le procédé comprend :
- une extraction de données reçues par le second nœud (N_B) dont :
 - l'identifiant du nœud générateur extrait de l'entête de la signature du premier message envoyé par le premier nœud (N_A) et ;
 - la signature du premier message envoyé par le premier nœud (N_A) et ;
 - le premier certificat (K_A/k_{CA}) extrait du troisième message (M_3) envoyé par le premier nœud (N_A) et ;

- le second ensemble de données (ENS_2/k_A) signé par la clef privée (k_A) du premier nœud (N_A) du troisième message (M_3) ;
 - une génération d'une requête d'éléments de sécurité (M_2) à la réception du premier message (M_1) vers le premier nœud (N_A) si le nœud N_A est inconnu de N_B ou si le message M_1 n'est pas authentifié par le nœud N_B ;
 - un enregistrement des données extraites dans une mémoire du second nœud (N_B) ;
 - une vérification de la signature associée au premier certificat signée par l'autorité de certification aussi connue du nœud B ;
 - une vérification de la possession du trousseau de clé k_A/K_A par le nœud N_A d'adresse IP IP_A en vérifiant la signature de l'ensemble ENS_2 signé par la clé privée k_A du nœud N_A ;
 - une comparaison des adresses IP et des identifiants du nœud N_A contenus dans respectivement les premier et troisième messages permettant une vérification de l'authentification du premier nœud (N_A) ;
 - une vérification de la signature du message M_1 à partir de la clé publique K_A signée par l'autorité de certification.
7. Procédé de contrôle selon la revendication précédente, caractérisé en ce que l'enregistrement des données est réalisé de sorte à faire correspondre les trois données suivantes :
- une unique identification du premier nœud (N_A) ;
 - une adresse IP (IP_A) du premier nœud (N_A) ;
 - un premier certificat de la clef publique du premier nœud signé par l'autorité de certification.
8. Procédé de contrôle selon l'une quelconque des revendications 6 à 7, caractérisé en ce que :
- l'extraction de données reçues par le second nœud (N_B) comprend en outre :
 - le second certificat (K_A/k_{CA}) du troisième message (M_3)
 - le cinquième ensemble de données (ENS_5/k_{tA}) signé par la clef temporaire privée (k_{tA}) du premier nœud (N_A) du troisième message (M_3).

- Le procédé comprend en outre une vérification de la signature du second certificat à partir de la clé publique K_A signée par l'autorité de certification
- 5 • Le procédé comprend en outre une vérification de la possession du trousseau de clé k_{tA}/K_{tA} par le nœud N_A d'adresse IP IP_A en vérifiant la signature de l'ensemble ENS_5 signé par la clé privée k_{tA} du nœud N_A ;
- 10 • Le procédé comprend une vérification de la signature du message M_1 à partir de la clé publique K_{tA} signée par la clé privée k_A du nœud N_A au lieu d'une vérification de la signature du message M_1 à partir de la clé publique K_A signée par l'autorité de certification

9. Procédé de contrôle selon la revendication précédente, caractérisé en ce que l'enregistrement des données est réalisé de sorte à
15 faire correspondre les quatre données suivantes :

- une unique identification du premier nœud (N_A) ;
- une adresse IP (IP_A) du premier nœud (N_A) ;
- un premier certificat (K_A/k_{CA}) de la clef publique du premier nœud signé par l'autorité de certification ;
- 20 • un second certificat (K_{tA}/k_A) de la clef publique temporaire (K_{tA}) du premier nœud (N_A) signé la clef privée (k_A) du premier nœud (N_A).

10. Procédé de sécurisation selon l'une quelconque des revendications 1 à 5 et procédé de contrôle selon l'une quelconque des revendications 6 à 9, caractérisé en ce que le protocole de routage est le
25 protocole OLSR et que le premier message M_1 est un message de type HELLO ou TC.

11. Procédé de sécurisation selon l'une quelconque des revendications 1 à 5 et procédé de contrôle selon l'une quelconque des revendications 6 à 9, caractérisé en ce qu'au moins un nœud comprend un
30 terminal mobile.

12. Procédé de transmission des certificats révoqués, caractérisé en ce que :

- Si ledit procédé est initié par le nœud propriétaire du premier certificat :

- Le nœud propriétaire du premier certificat transmet un message M_4 signé par sa clé privée en vigueur vers les nœuds de confiance les plus proches stipulant la révocation de ses certificats ;
- 5 ○ Le nœud propriétaire du premier certificat supprime définitivement ses éléments de sécurité dès lors qu'il a reçu suffisamment de messages M_5 d'acquittement dont il a contrôlé l'authenticité ;
- Si ledit procédé est initié par l'autorité de certification :
 - 10 ○ L'autorité de certification charge un ou plusieurs nœuds de transmettre sa liste de certificats révoqués par l'intermédiaire d'un message M_7 signé par l'autorité de certification ;
 - Si ledit procédé est entretenu par les nœuds du réseau :
 - 15 ○ Un nœud transmet périodiquement sa liste de certificats révoqués par l'intermédiaire d'un message M_6 signé par sa clé privée temporaire.

13. Procédé de gestion d'une liste de révocation des certificats gérées par un nœud, caractérisé en ce que :

- 20 • Le nœud intègre dans sa liste les premiers et seconds certificats obsolètes lorsqu'ils sont renouvelés par les nœuds générateurs (en possession de ces certificats) et transmis selon l'une quelconque des revendications 1 à 5 ;
- Le nœud intègre dans sa liste les premier et second certificats révoqués extrait d'un message M_4 authentifié, issu du nœud en ayant la propriété et signé par la clé privée temporaire de ce nœud, et transmet un acquittement M_5 signé par sa clé temporaire vers le nœud générateur propriétaire des certificats révoqués ;
- 25 • Le nœud intègre dans sa liste les certificats révoqués extraits de suffisamment de messages M_6 authentifiés, issus de plusieurs nœuds et signés par la clé privée temporaire de ces nœuds ;
- 30 • Le nœud intègre dans sa liste les certificats révoqués extraits de suffisamment de messages M_6 authentifiés, issus de plusieurs nœuds et signés par la clé privée temporaire de ces nœuds ;

- Le nœud intègre dans sa liste les certificats révoqués extraits d'un message M_7 authentifié, signé par l'autorité de certification et transmis par des nœuds tiers.

14. Nœud d'un réseau ad hoc, caractérisé en ce qu'il permet de
5 sécuriser une transmission de données par la mise en œuvre du procédé de sécurisation de l'une quelconque des revendications 1 à 5.

15. Nœud récepteur d'un réseau ad hoc, caractérisé en ce qu'il
permet de contrôler les données d'authentification d'un nœud émetteur par la
mise en œuvre du procédé de sécurisation de l'une quelconque des
10 revendications 6 à 11.

1/7

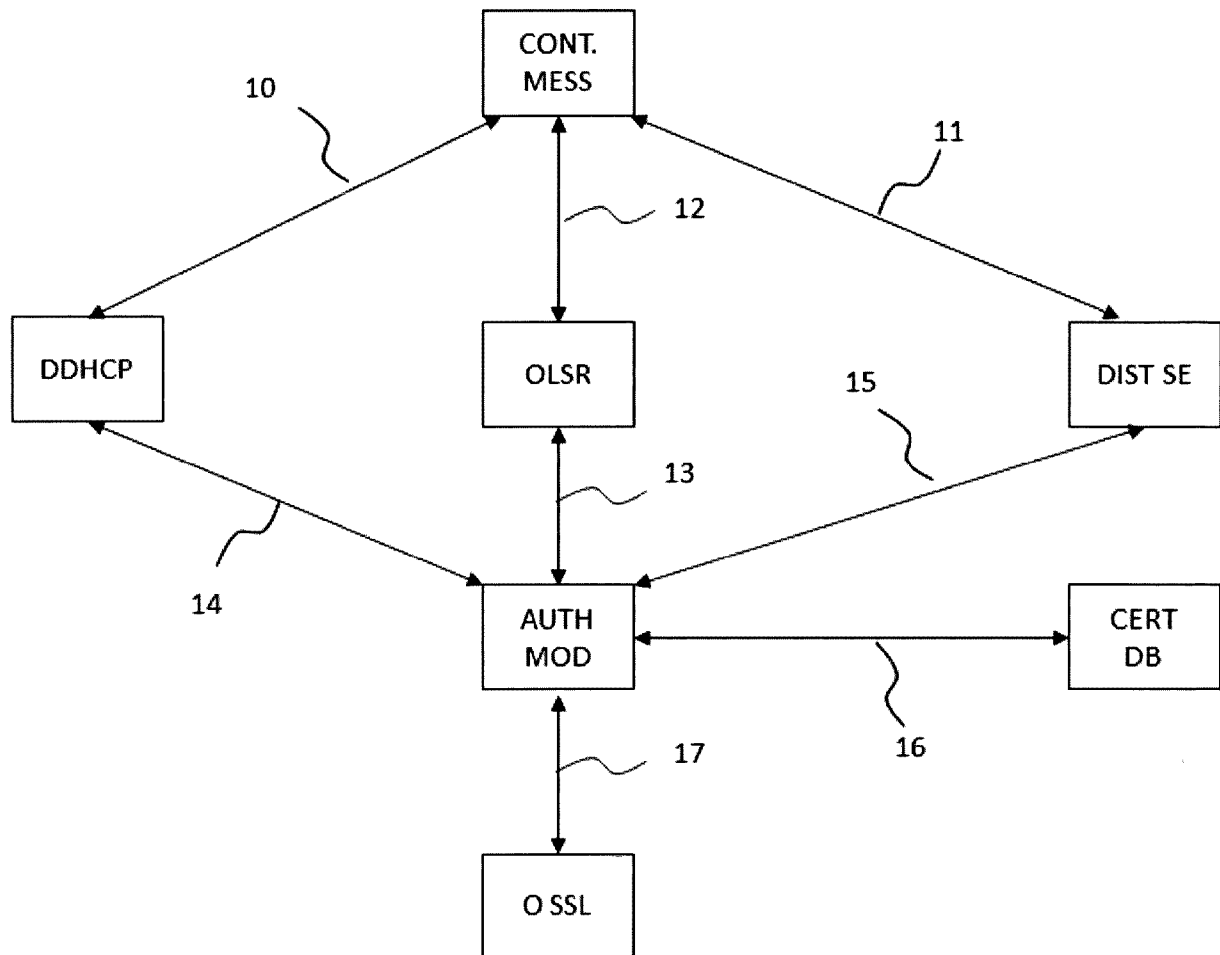


FIG. 1

2/7

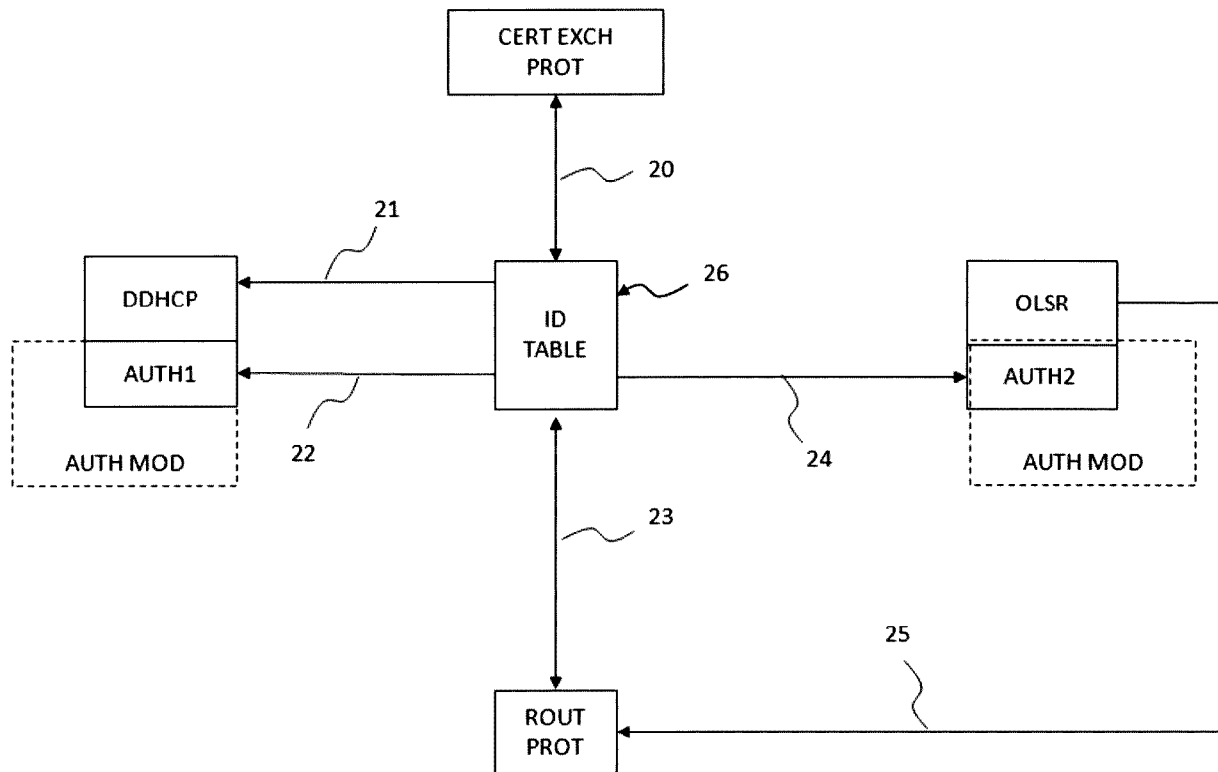


FIG. 2

3/7

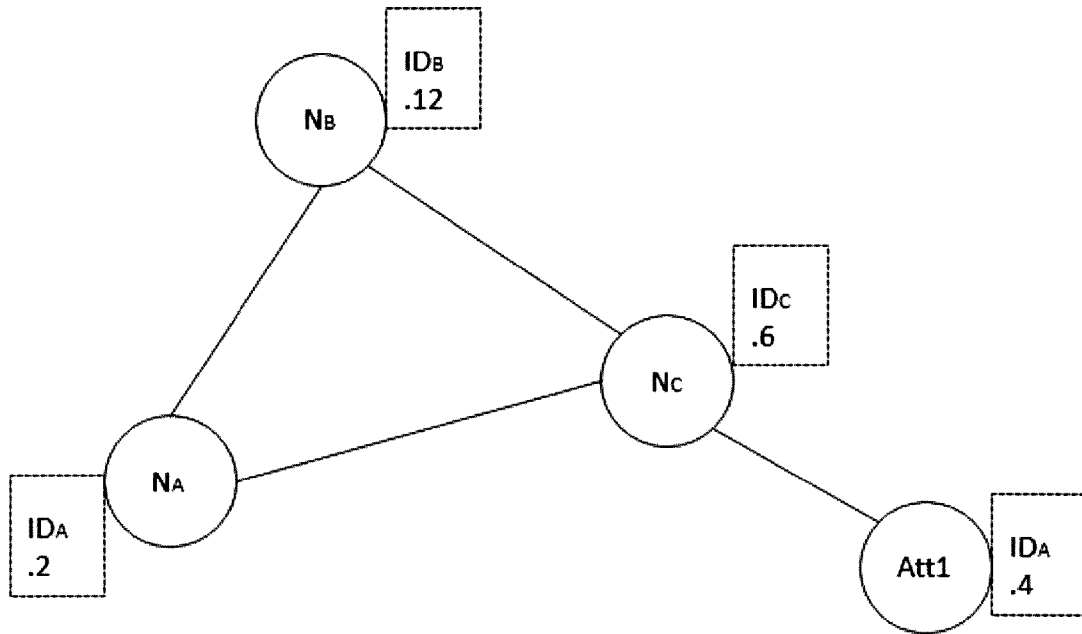


FIG. 3

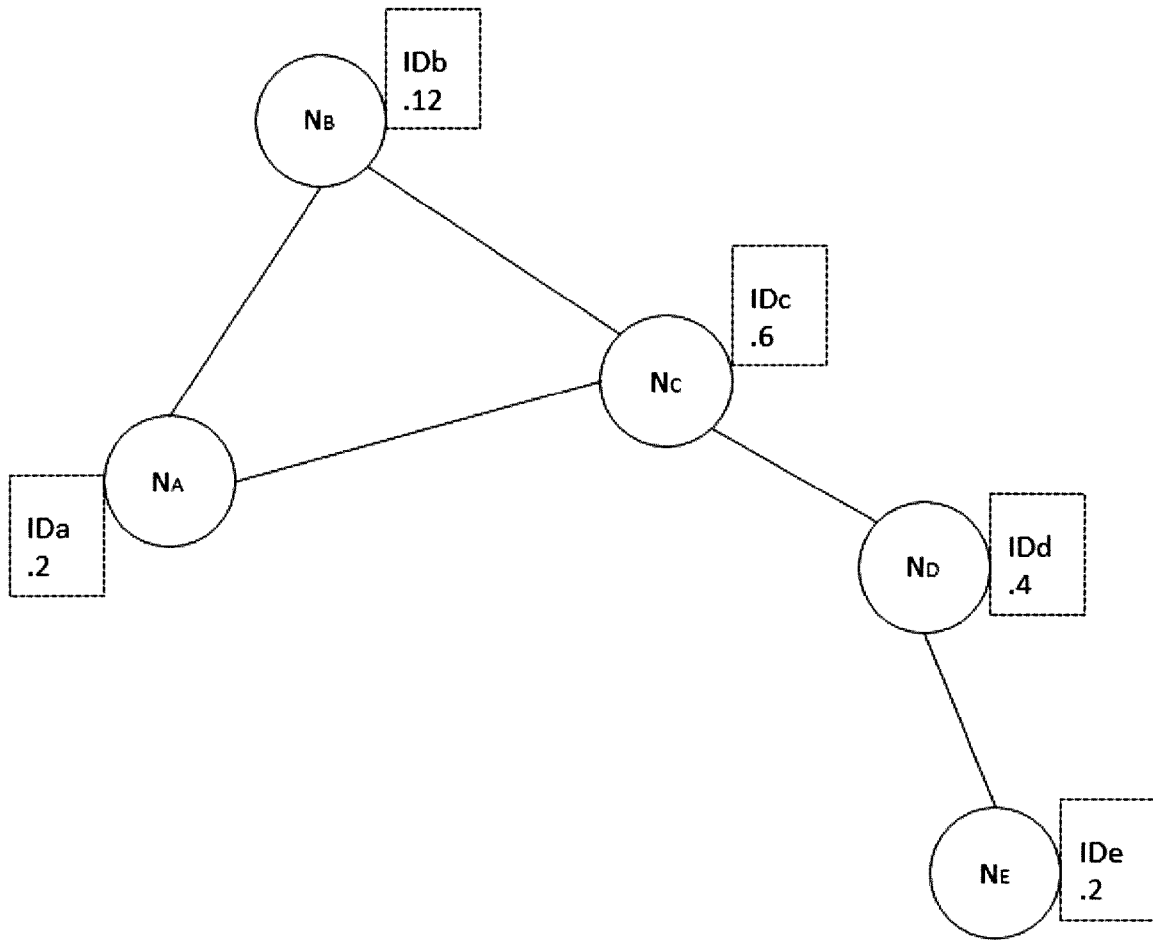


FIG. 4

26



ID	@IP	CERT (K)	CERT TEMP (K _t)
IDA	IPA	C _A (K _A /k _{CA})	C _{tA} (K _{tA} /k _A)
IDB	IPB	C _B (K _B /k _{CA})	C _{tB} (K _{tB} /k _B)
IDC	IPC	C _C (K _C /k _{CA})	C _{tC} (K _{tC} /k _C)
...	...	...	...

FIG. 5

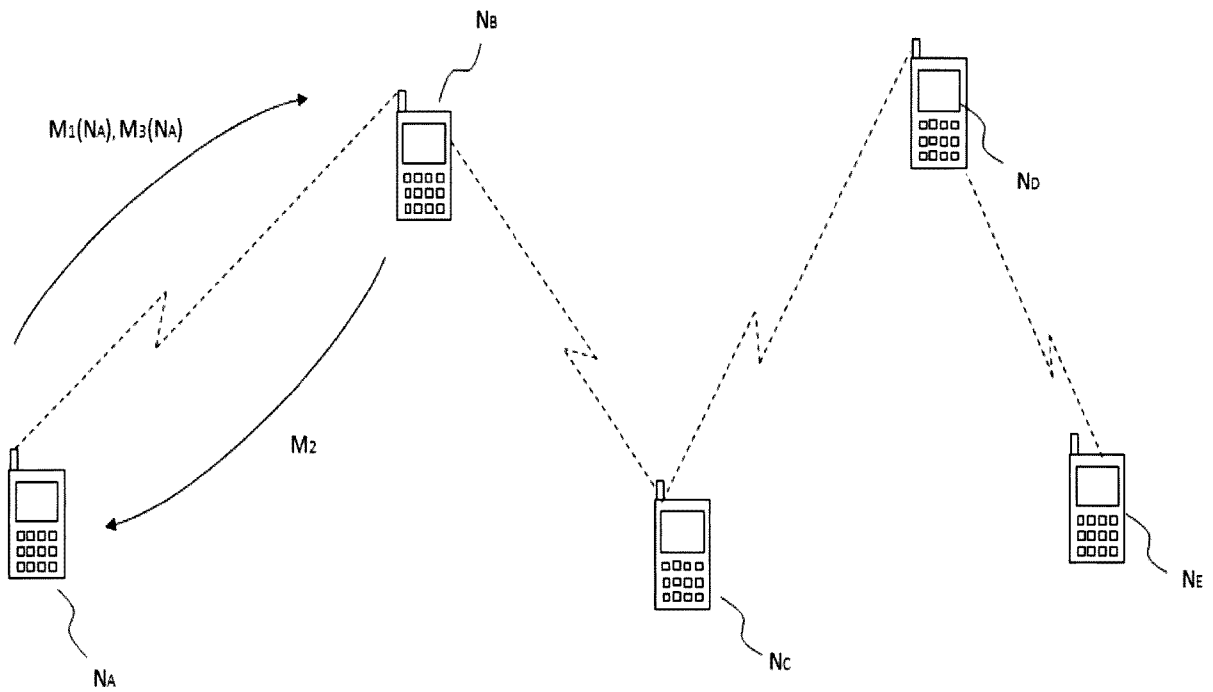


FIG. 6

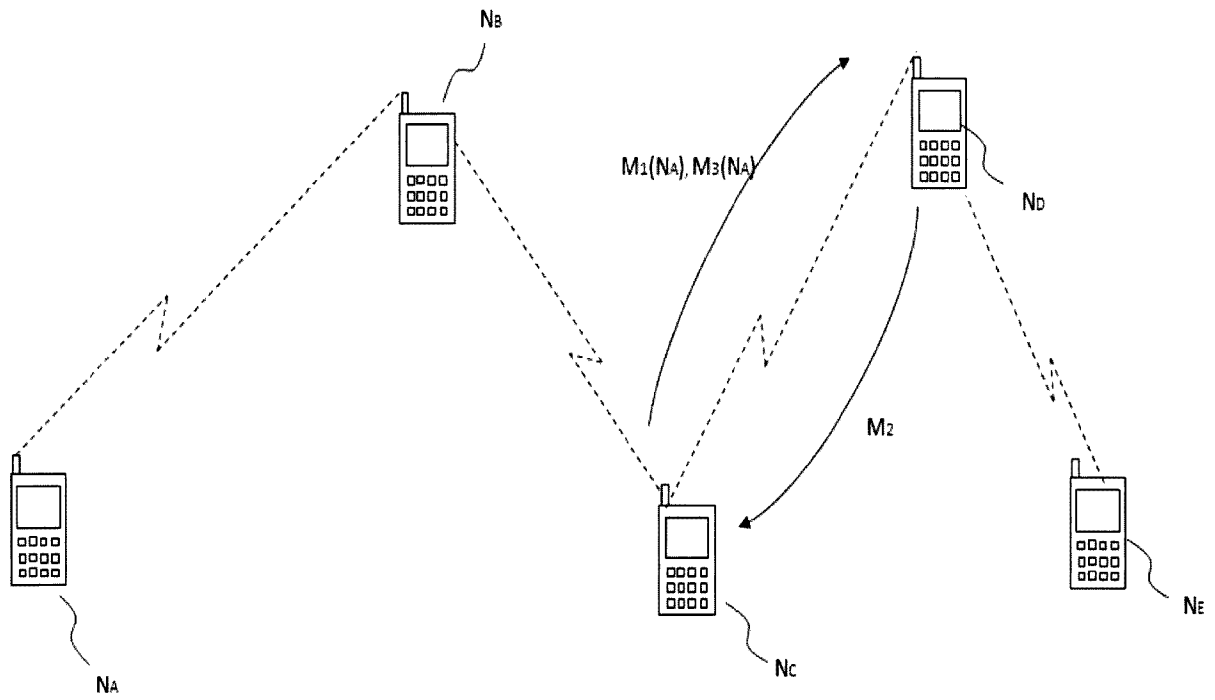


FIG. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/003461A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ADNANE A ET AL: "Trust-Based Countermeasures for Securing OLSR Protocol", COMPUTATIONAL SCIENCE AND ENGINEERING, 2009. CSE '09. INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 29 August 2009 (2009-08-29), pages 745-752, XP031543704, ISBN: 978-1-4244-5334-4 page 747, right-hand column, line 1 - page 749, left-hand column, line 8 ----- -/--	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

27 March 2014

Date of mailing of the international search report

07/04/2014

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Raposo Pires, João

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2013/003461

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KHADIDJA AYAD ET AL: "New efficient mechanisms to secure OLSR protocol", FUTURE GENERATION COMMUNICATION TECHNOLOGY (FGCT), 2012 INTERNATIONAL CONFERENCE ON, IEEE, 12 December 2012 (2012-12-12), pages 46-51, XP032340865, DOI: 10.1109/FGCT.2012.6476572 ISBN: 978-1-4673-5859-0 abstract page 48 -----	1-15

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/06
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	ADNANE A ET AL: "Trust-Based Countermeasures for Securing OLSR Protocol", COMPUTATIONAL SCIENCE AND ENGINEERING, 2009. CSE '09. INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 29 août 2009 (2009-08-29), pages 745-752, XP031543704, ISBN: 978-1-4244-5334-4 page 747, colonne de droite, ligne 1 - page 749, colonne de gauche, ligne 8 ----- -/--	1-15



Voir la suite du cadre C pour la fin de la liste des documents



Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"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

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

27 mars 2014

Date d'expédition du présent rapport de recherche internationale

07/04/2014

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Raposo Pires, João

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	KHADIDJA AYAD ET AL: "New efficient mechanisms to secure OLSR protocol", FUTURE GENERATION COMMUNICATION TECHNOLOGY (FGCT), 2012 INTERNATIONAL CONFERENCE ON, IEEE, 12 décembre 2012 (2012-12-12), pages 46-51, XP032340865, DOI: 10.1109/FGCT.2012.6476572 ISBN: 978-1-4673-5859-0 abrégé page 48 -----	1-15