Gestion de confiance et résistance aux attaques dans les réseaux Ad hoc mobiles

Abderrezak Rachedi, Abderrahim Benslimane

Gestion de confiance et résistance aux attaques dans les réseaux Ad hoc mobiles

Abderrezak RACHEDI et Abderrahim BENSLIMANE

Laboratoire d'Informatique d'Avignon
LIA/CERI, Univesité d'Avignon – Agroparc, BP 1228
84911, Avignon, France

{abderrezak.rachedi, abderrahim.benslimane}@univ-avignon.fr

RÉSUMÉ. *La mise en place d'une solution permettant d'assurer que les réseaux Ad hoc mobiles (MANETs) soient sécurisés n'est pas une tâche simple. En effet, les réseaux MANETs comportent de nombreuses caractéristiques, comme l'absence d'une infrastructure préexistante, la topologie dynamique du réseau,etc. Dans cet article, nous étudions le concept de "la zone dynamique démilitarisée" (DDMZ), étudiée dans notre architecture hiérarchique, pour éviter toute vulnérabilité dans les réseaux MANETs. La DDMZ est constituée des nœuds dispensables ou sacrifiables, qui appartiennent au groupe des nœuds de confiance. Nous proposons un modèle probabiliste pour définir la connectivité directe qui existe entre les nœuds de confiance dans le but d'étudier le degré de résistance de la DDMZ contre différents types d'attaques. De plus, nous évaluons la robustesse et la disponibilité de la DDMZ et analysons les effets de la connectivité directe et de la portée de transmission sur la stabilité et la sécurité au sein du réseau.*

ABSTRACT. *Providing a security solution for Mobile Ad-hoc Networks (MANETs) is not an easy task. This is due to the unique characteristics of MANETs, such as the lack of a pre-existent infrastructure, the dynamic topology of the network, etc. In this paper, we study the concept of Dynamic Demilitarized Zone (DDMZ) defined in our hierarchical architecture to avoid a single point of failure in MANETs. The DDMZ is formed by the dispensable nodes which belong to the confident group. We propose a probabilistic model to define the direct connectivity between confident nodes in order to study the resistance degree of DDMZ against different attacks. Furthermore, we estimate the robustness and the availability of DDMZ and we also analyze the effects of direct connectivity and transmission range on the stability and security of the network.*

MOTS-CLÉS : *Les réseaux Ad hoc mobiles, Sécurité des réseaux, modèle de confiance, une infrastructure à clé publique, la zone dynamique démilitarisée.*

KEYWORDS: *MANET, Networks Security, PKI, DDMZ (Dynamic Demilitarized Zone), Algorithms.*

1. Introduction

Un réseau Mobile Ad Hoc (MANET) est constitué d'un groupe de nœuds autonomes ne possédant aucune infrastructure de réseau au préalable. Ces nœuds communiquent entre eux au moyen de liens sans fil, si les nœuds ne sont pas proches, ils peuvent aussi communiquer grâce à des liens de plusieurs sauts pour assurer le trafic du point source à la destination. La topologie du réseau dépend de la mobilité des nœuds. Toutes ces caractéristiques font des réseaux MANETs des réseaux originaux et populaires dans de nombreux domaines d'application. Cependant, les caractéristiques propres aux réseaux MANETs les rendent vulnérables à de nombreux types d'attaques. C'est pourquoi la mise en place de solutions pour sécuriser ces réseaux n'est pas une tâche facile. Le but de ces solutions est d'assurer des services de sécurité, comme l'authentification, la confidentialité, l'intégrité, la non répudiation, et la disponibilité des services du réseau. Pour atteindre ces objectifs, certaines questions doivent être résolues : Qui assure les services de sécurité dans les réseaux MANETs ? Quelles sont les caractéristiques des nœuds capables d'assurer les services de sécurité ? . . .etc.

De nombreux travaux de recherche ont été menés dans ce domaine. Pour sécuriser le protocole de routage, Perrig et Johnson [HU 02] ont proposé le protocole *Ariadne*, une version sécurisée du DSR via l'utilisation du protocole d'authentification diffusée *TESLA* (Timed Efficient Stream Loss-tolerant Authentication). Sinzgiri et Cie [SAN 05] ont présenté le protocole ARAN (protocole de routage authentifié pour les réseaux Ad Hoc), une version sécurisée du protocole AODV, mise en place à partir d'une unique autorité de certification (CA) pour le réseau tout entier. Zhou et Cie [ZHO 99][ZHO 02] ont proposé le modèle de distribution de l'autorité de certification en utilisant la cryptographie à seuil. Dans cet article, nous nous concentrons sur notre architecture hiérarchique distribuée [RAC 06] pour développer les systèmes dynamiques de gestion de clés adaptés aux caractéristiques du réseau MANET.

Dans cet article, nous proposons un modèle probabiliste pour définir et étudier la connectivité entre les nœuds de confiance (nœuds possédant un certain degré de confiance et assurant les services de sécurité), afin d'évaluer la robustesse de notre nouvelle architecture hiérarchique dans le but de sécuriser les réseaux MANETs. Cette architecture est conçue en divisant le réseau en différents groupes et en établissant l'infrastructure dynamique de clé publique avec la CA (autorité de certification) en tant que chef de groupe. Ce dernier changera en fonction des changements de topologie. Chaque groupe est contrôlé par le nœud CA, qui joue le rôle de certification des clés publiques des nœuds membres du groupe et d'un groupe de nœuds RA (autorité d'enregistrement) ; leur fonction consiste à filtrer et analyser les demandes de certification avant de les transmettre au nœud CA et sont également responsables de surveiller le comportement des nœuds membres du groupe. Les rôles des autorités de certification et d'enregistrement ne sont assurés que par des nœuds qui appartiennent à la communauté de confiance (un groupe de nœuds de confiance). L'ensemble des nœuds RA situés à un seul saut du nœud CA forme la zone DDMZ. Dans notre article, nous nous concentrons sur la connectivité entre les différents nœuds qui forment la DDMZ et qui

peuvent également assurer une connexion sécurisée entre les groupes (rôle de départ). Le reste de cet article est organisé ainsi : Dans la section 2, nous présentons une architecture hiérarchique pour distribuer et gérer les clés cryptographiques dans le réseau MANET. Dans la section 3, nous proposons le module de surveillance et le module de gestion de groupe. Dans la section 4, nous présentons notre modèle de connectivité sécurisée. Nous présentons dans la section 5 les résultats théoriques de notre modèle de connectivité sécurisée ainsi que les résultats des simulations afin d'évaluer la robustesse et la stabilité des groupes de nœuds, en particulier la DDMZ. Enfin, la section 6 conclut cet article.

2. ARCHITECTURE HIERARCHIQUE DISTRIBUEE

Dans notre travail [RAC 06], nous avions proposé une architecture hiérarchique distribuée qui divisait le réseau en groupes pour sécuriser le réseau. Ainsi, nous avons défini un modèle de confiance pour assigner différents rôles comme les rôles d'autorité de certification (CA) et d'autorité d'enregistrement (RA) au sein de chaque groupe. Nous avons également proposé l'algorithme sécurisé de groupage distribué (SDCA) pour diviser le réseau en un certain nombre de groupes. De plus, nous avons introduit le nouveau concept de DDMZ pour sécuriser le nœud CA dans chaque groupe. Une zone DDMZ est une zone intermédiaire déployée entre des nœuds inconnus et le nœud CA dans chaque groupe. Elle est constituée d'un ensemble de nœuds de confiance. L'un d'entre eux assure le rôle de nœud CA, et au moins un autre a le rôle de nœud RA. Le nœud CA peut communiquer directement (1 saut) avec les nœuds RA. La communication est chiffrée puisque les nœuds de confiance connaissent leurs clés publiques au préalable. Les caractéristiques de cette architecture sont énumérées comme suit :

1) Le système n'a besoin d'aucun tiers de confiance central. Ce système est dynamiquement adapté à tout changement de topologie.

2) La fonction d'authentification est distribuée à chaque groupe. Les nœuds ayant un degré de confiance élevé contrôleront le comportement de chaque nœud ayant un degré de confiance faible au sein du groupe.

3) La stabilité de la gestion des clés publiques dépend de la stabilité du groupe.

3. CONTRÔLE DES NOEUDS ET GESTION DES GROUPES

3.1. *Contrôle des nœuds (monitoring)*

Dans le module de contrôle, chaque nœud ayant un degré de confiance élevé contrôle ses nœuds voisins, c.à.d ceux qui ont un degré de confiance faible. Dans le cas que nous étudions, le processus de contrôle agit sur deux couches différentes du réseau. Le schéma 3 montre les différents composants du module de contrôle et

l'interaction avec le chef du groupe. Le module de contrôle intervient sur différentes couches protocolaires :

– La couche MAC : les nœuds responsables du contrôle surveillent l'occupation du canal de communication par leurs voisins. Cette opération consiste à mesurer la durée de l'occupation du canal par des nœuds. Le but de cette fonction est de détecter les nœuds qui exercent un certain type de comportement égoïste [KYA 05] : les nœuds égoïstes trichent en choisissant leur backoff, dans le but d'obtenir une bande plus importante et de pénaliser les nœuds qui se comportent bien. Plusieurs solutions ont été proposées dans la littérature, pour contrôler les nœuds égoïstes dans la couche MAC. Nous supposons que les nœuds chargés du contrôle à ce niveau génèrent un rapport noté (R_1) sur ses voisins qui ont un degré de confiance faible. Dans cet article, nous ne nous focalisons pas sur le contrôle de la couche MAC.

– La couche réseau : les nœuds chargés du contrôle surveillent les activités de transmission de paquets de leurs nœuds voisins, qui ont un degré de confiance faible. Cette idée est basée sur le paramètre de coopération des nœuds dans le réseau. La définition de ce paramètre consiste à calculer pour chaque nœud la proportion de paquets bien retransmis par rapport au nombre total de paquets devant être transmis sur une certaine période. Cette période est la période d'observation qui consiste à collecter les informations données par les nœuds pour calculer le niveau de réputation. Soient deux nœuds x et y avec $Tm(x) > Tm(y)$, dans ce cas, le nœud x peut contrôler le nœud y. Le nœud x envoie un certain nombre de paquets de données au nœud y avec un autre nœud comme destination, et après une période de temps limitée, le nœud x peut calculer le niveau de réputation :

$$R_2(X,Y) = \frac{\text{Nombre des paquets acheminé}}{\text{Nombre total des paquets}} \qquad [1]$$

Dans [REB 05] Yacine et Cie ont proposé une idée similaire pour calculer le niveau de réputation. La différence entre notre module de contrôle et celui de Yacine est l'attribution d'un degré de confiance. Dans notre modèle, chaque nœud inconnu commence avec un degré de confiance le plus faible ($Tm = 0.1$) et ce degré augmente au fur et à mesure que le nœud prouve sa coopération et son bon comportement. Ainsi dans notre approche, nous prenons en compte le degré de confiance des nœuds chargés du contrôle. Les niveaux de réputation générés par les nœuds sont liés aux degrés de confiance correspondant à chaque nœud. Telle est la tâche du chef de groupe. Le rapport final concernant le nœud y généré par chaque nœud chargé du contrôle x, est :

$$R(x,y) = \frac{w_1.R_1(x,y) + w_2.R_2(x,y)}{w_1 + w_2} \qquad [2]$$

tel que, w_1 et w_2 représentent les coefficients des rapports au niveau des couches MAC et réseau respectivement. Ces coefficient peuvent être déterminer en fonction de l'importance des paramètres de chaque couche. Par example, le cas de même coefficient pour les deux couches MAC et réseau $w_1 = w_2 = 1$.

3.2. *Le gestionnaire du groupe*

Le gestionnaire du groupe est constitué de l'autorité de certification du groupe (le nœud CA) et d'un ensemble de nœuds ayant des degrés de confiance élevés. Si les nœuds de confiance sont situés à un saut du nœud CA, ils deviennent l'autorité d'enregistrement (RA). Le rôle de gestionnaire du groupe est d'assurer la sécurité du groupe là où le nœud CA génèrera un certificat pour les membres du groupe. Un ensemble de nœuds RA forme la DDMZ dans le but de protéger le nœud CA contre les attaques via le filtrage des communications entre un nœud inconnu et le nœud CA. La DDMZ utilise le niveau de réputation délivré par le processus de contrôle pour évaluer les membres du groupe.

Le module gestionnaire du groupe collecte le rapport de réputation des membres du groupe. Les nœuds chargés du contrôle génèrent des rapports évaluant la réputation de leurs voisins sur demande. Le nœud CA exige que les nœuds chargés du contrôle génèrent le rapport de reputation des nœuds. Lorsque le CA reçoit le rapport d'évaluation de réputation envoyé par les nœuds chargés du contrôle, le calcule du rapport de réputation finale de chaque nœud est effectué comme indiquer dans l'équation 3. Si le CA reçoit k rapports de la part des nœuds chargés du contrôle, pour évaluer le nœud y, alors :

$$\text{Rapport de Réputation :} RR(y) = \frac{1}{k} \sum_{i=1}^{k} Tm(x_i) \times R(x_i, y) \qquad [3]$$

Lorsque le nœud CA possède les rapports de réputation, la classification des comportements est effectuée pour classer les nœuds. Si le rapport de réputation dépasse un certain seuil, le degré de confiance augmente, sinon, le degré de confiance ne change pas. Cependant, si le rapport est en-dessous d'un certain seuil, le degré de confiance diminue et les nœuds se comportant mal seront punis. Dans le cas où les nœuds ont un rapport négatif plusieurs fois (récidivistes), les nœuds se comportant mal seront rejetés du groupe et le CA informe les autres CA de groupe adjacentes de la récidive des nœuds se comportant mal.

Dans cette architecture, les nœuds doivent appartenir à au moins un groupe pour pouvoir sécuriser leur communication avec des nœuds membres du groupe, parce que les nœuds du groupe communiquent seulement avec les nœuds qui possèdent le certificat du nœud CA de ce groupe. La communication entre les groupes est assurée par les nœuds passerelles qui appartiennent à au moins deux groupes et possèdent un certain degré de confiance. La sécurité de cette architecture dépend directement du modèle de confiance adopté et du degré de connexion entre les nœuds de confiance. La connectivité entre les nœuds de confiance indique la disponibilité des services de sécurité dans le réseau, le degré de résistance face à des attaques telles que le déni de service (DoS), et la robustesse de la DDMZ dans cette architecture. Pour toute ces raisons, nous allons nous intéresser à l'étude de la connectivité entre les nœuds de confiance.

4. LE MODELE DE CONNECTIVITE DE CONFIANCE

L'idée de base consiste à distribuer k nœuds de confiance parmi un nombre total de n nœuds dans le réseau. Ces nœuds de confiance doivent collaborer entre eux pour diviser le réseau en différents groupes et pour assigner les rôles de CA (autorité de certification) et de RA (autorité d'enregistrement) au sein de chaque groupe créé. Ainsi, les règles pour qu'un groupe soit établi sont les suivantes :

– un groupe ne peut accepté d'autres nœuds s'il est saturé.

– l'existence d'au moins deux nœuds de confiance qui doivent être directement connectés (reliés) l'un à l'autre.

Dans chaque groupe, le nœud CA et les nœuds de confiance directement reliés les uns aux autres forment la DDMZ.

Nous supposons qu'il n'existe aucun obstacle dans la surface de déploiement des nœuds, et que tous les nœuds possèdent le même rayon de transmission R, nous pouvons écrire la connectivité directe suivante : $\mid Xi - Xj \mid < R$, où X_i désigne l'endroit où se trouve le nœud (i). Nous supposons que chaque nœud de confiance connaît les clés publiques du chiffrement de tous les nœuds de confiance. Les nœuds inconnus peuvent devenir des nœuds de confiance, mais cela dépend du modèle de confiance ; dans notre architecture sécurisée, le module chargé du contrôle et de la surveillance est responsable de cette tâche. Nous supposons que n nœuds sont distribués avec un taux d'arrivée qui suit une loi de Poisson afin d'estimer le nombre de no euds dans rayon donné. La probabilité qu'un nœud (i) puisse communiquer directement avec un nœud (j) est : $P(R) = Pr\{\mid X_i - X_j \mid \leq R\} = 1 - e^{-\lambda.R}$ Dans notre cas, la probabilité d'avoir (d+1) nœuds de confiance directement connectés entre eux est :

$$P_d(R) = \prod_{i=1}^{d}(1 - e^{-\lambda.R}) = (1 - e^{-\lambda.R})^d \qquad [4]$$

Le paramètre d ne peut prendre que des valeurs entière et représente le degré de connectivité directe entre les nœuds de confiance. La probabilité d'avoir un réseau muni d'une forte connectivité dépend de rayon de transmission des nœuds. Plus la portée de transmission est élevée, plus la probabilité d'une forte connectivité sur le réseau est grande.

La probabilité d'avoir deux nœuds (i) et (j) directement connectés entre eux, sachant qu'ils appartiennent à l'ensemble des nœuds de confiance K qui contient $\|K\| = k$ nœuds dans le réseau sur un nombre total de nœuds (de confiance ou non) n, est : $P = P(R).Pr\{node(i) \in K\}.Pr\{node(j) \in K \setminus node(i) \in K\}$

D'après l'équation 4, la probabilité d'avoir (d+1) nœuds directement connectés entre eux, sachant qu'ils appartiennent à l'ensemble des nœuds de confiance $|K| = k$, est :

$$P_{n,k}(R) = (1 - e^{-\lambda.R})^d.\Big\{\frac{k}{n}.\frac{k-1}{n-1}\cdots\frac{k-d}{n-d}\Big\} \qquad [5]$$

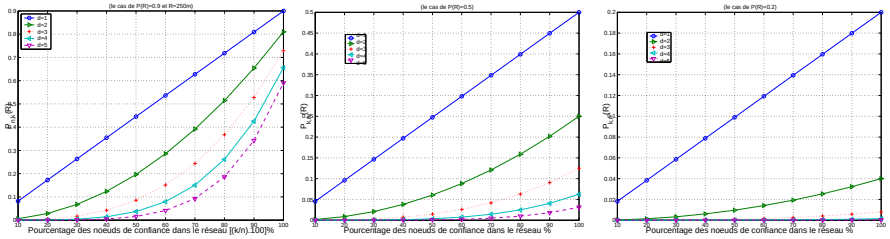
tel que, $d < k$ et $k \leq n$

Dans la DDMZ, d est un paramètre qui indique la robustesse et le degré de résistance de la DDMZ contre des attaques telles que le DoS, mais également la disponibilité des services de sécurité, comme par exemple, le filtrage des demandes de certification avant leur transmission au nœud CA.

5. SIMULATIONS ET EVALUATION DU MODELE

5.1. *Résultats théoriques*

Dans cette partie, nous présentons les principaux résultats de simulation du modèle de connectivité sécurisée. Les résultats présentés ci-dessous montrent la probabilité d'avoir des nœuds de confiance directement connectés entre eux comme l'indique l'équation 5. La figure 1 montre la probabilité d'avoir des nœuds de confiance directement connectés les uns aux autres avec un degré d en fonction du pourcentage de nœuds de confiance dans le réseau. Les différents cas de probabilité d'avoir deux nœuds directement connectés entre eux $P(R)$ sont présentés. Le cas d'une forte probabilité $P(R) = 0.9$, c.à.d dans le cas d'une grande portée de transmission, les résultats obtenus sont montrés dans la figure 1(a). Nous remarquons que plus le pourcentage de nœuds de confiance augmente, plus la probabilité de constituer une DDMZ robuste augmente avec le paramètre d. Les figures 1(b) et 1(c) montrent les effets de



(a) Le cas de P(R)=0.9 (b) Le cas de P(R)=0.5 (c) Le cas de P(R)=0.2

Figure 1. *Probabilité de former une DDMZ avec un degré d, en fonction du taux de nœuds de confiance*

la portée de transmission (une faible connectivité $P(R) \leq 0.5$). Au niveau de la figure 1(b), nous étudions les résultats dans le cas où la probabilité d'avoir deux nœuds directement connectés entre eux est égale à 0.5 ($P(R) = 0.5$). Nous remarquons que la probabilité d'avoir des nœuds directement connectés entre eux avec un degré d en fonction du pourcentage de nœuds de confiance dans le réseau diminue par rapport au cas où la probabilité d'une connectivité directe était forte. Alors, la probabilité de constituer une DDMZ diminue. Enfin, la figure 1(c) illustre le cas d'une faible probabilité de connectivité directe ($P(R) = 0.2$). Nous remarquons que la probabilité

d'avoir deux nœuds de confiance directement connectés entre eux dépend directement de la probabilité d'avoir deux nœuds directement connectés entre eux (P(R)). La probabilité P(R) dépend de la portée de transmission.

5.2. *Résultats des simulations*

Pour évaluer la robustesse de la DDMZ au sein de chaque groupe, nous avons mis en place l'algorithme décrit ci-dessus. Nous utilisons le simulateur de réseau (NS-2). Chaque nœud mobile a une antenne omnidirectionnelle qui utilise le gain d'unités avec un rayon de transmission radio qui varie entre (50-250)m. Le waypoint est sélectionné comme modèle de mobilité dans le champ ($670x670m^2$) avec la vitesse de nœud distribuée uniformément entre 0 et 20m/sec. Le nombre total de nœuds dans le réseau est $N = 50$.

La figure 2 montre le nombre moyen de nœuds CA dans le réseau. Nous remarquons que le nombre de nœuds CA diminue lorsque la marge de transmission augmente. Ce fait prouve que notre architecture est stable. La figure 3 illustre le nombre

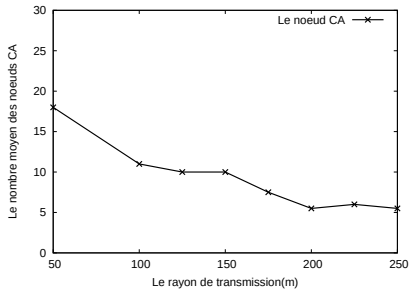


Figure 2. *Le nombre moyen des CAs en fonction du rayon de transmission (R)*

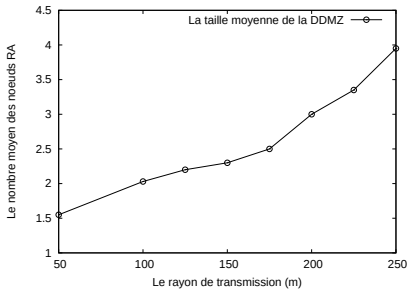


Figure 3. *La taille moyenne de la DDMZ en fonction du rayon (R)*

moyen de nœuds RA au sein de chaque groupe avec des rayons de transmission différents. Le nombre de nœuds RA augmente au sein de chaque groupe lorsque le rayon de transmission augmente. Cela signifie que les groupes et les nœuds CAs deviennent plus résistants contre les attaques de type DoS (déni de services) lorsque le rayon de transmission devient plus grand. Le résultat montre que : a) lorsque le rayon de transmission augmente, la probabilité d'avoir deux nœuds directement connectés entre eux est plus importante ; b) de plus, la probabilité d'avoir des nœuds de confiance directement connectés entre eux est aussi plus grande. Cela indique que la probabilité de former une DDMZ robuste dépend du rayon de transmission. La meilleure configuration de groupe consiste à trouver un compromis entre le nombre de nœuds RAs et le nombre de nœuds ayant un faible degré de confiance.

6. CONCLUSION

Dans cet article, nous avons proposé un modèle de connectivité de confiance pour étudier la robustesse de la sécurité au sein des groupes. Nous avons présenté les différents modules de l'architecture : le modèle de confiance, le processus d'élection, le gestionnaire de groupe et le module chargé du contrôle. Dans cette étude, nous nous sommes concentrés sur le gestionnaire de groupe, en particulier sur la DDMZ. Les résultats des simulations confirment ce qu'a montré notre modèle de connectivité sécurisé, à savoir que lorsque la probabilité d'avoir deux nœuds directement connectés entre eux augmente, la probabilité d'avoir une DDMZ robuste augmente aussi parallèlement. Dans un prochain travail, nous étudierons les différents modèles de mobilité pour évaluer l'efficacité de cette architecture.

7. Bibliographie

[HU 02] HU Y., PERRIG A., JOHNSON D. B., « Adriane : A Secure On-Demand Routing Protocol for Ad Hoc Network », *In Proc. of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom'02)*, Atlanta, Georgia, US., September 2002, p. 12-23.

[KYA 05] KYASANUR P., VAIDYA N., « Selfish MAC layer misbehavior in wireless networks », *IEEE Transactions on Mobile Computing*, vol. 4, n° 5, 2005, p. 502-516.

[RAC 06] RACHEDI A. ET BENSLIMANE A., « A secure Architecture for Mobile Ad Hoc Networks », *Proc. of International Conference on Mobile Ad-Hoc and Sensor Networks (MSN'06)*, Hong Kong, China, December 2006, Lecture Notes in Computer Science (4325), p. 424-435.

[REB 05] REBAHI Y., MUJICA-V V. E., SISALEM D., « A Reputation-Based Trust Mechanism for Ad hoc Networks », *In Proc. of the Symposium on Communications (ISCC'05)*, 2005, p. 37-42.

[SAN 05] SANZGIRI K., DAHILL B., LAFLAMME D., LEVINE B. N., SHIELDS C., BELDING-ROYER E. M., « An Authenticated Routing Protocol for Secure Ad Hoc Networks », *IEEE Journal on Selected Areas in Communication (JSAC)*, vol. 23, n° 3, 2005, p. 598- 610.

[ZHO 99] ZHOU L., HAAS Z. J., « Securing Ad Hoc Networks », *IEEE Network*, vol. 13, n° 6, 1999, p. 24-30.

[ZHO 02] ZHOU L., SCHNEIDER F. B., RENESSE R. V., « COCA : A secure distributed online certification authority », *ACM trans. Computer Systems*, vol. 20, n° 4, 2002, p. 29-368.