Securité de transfert de données dans les réseaux tolérant aux délais

Djoudi Touazi, Mawloud Omar
Université Abderrahmane Mira, Département d'Informatique, ReSyD.
Bejaïa, Algérie

Abdelmadjid Bouabdallah
Université de Technologie de Compiègne, Heudiasyc-UMR CNRS 6599.
Compiègne, France.

Résumé — **Le développement effréné des technologies de réseaux informatiques (câblé, cellulaire, ad hoc, etc) mène vers la cohabitation d'innombrables architectures réseaux différentes dont l'objectif est de servir les consommateurs finaux ou utilisateurs. Le modèle de confiance définit une relation de confiance entre les acteurs d'une architecture réseau, fournit des moyens élémentaires pour sécuriser des services importants et garantir la disponibilité des services de sécurité. Dans ce papier, nous proposons un modèle de confiance pour sécuriser le transfert de données dans les réseaux tolérants aux délais (DTN). Notre proposition est destinée à un type spécifique d'architecture DTN. Le réseau regroupe plusieurs sous-réseaux géographiquement dispersés dans des régions isolées et ayant un accès intermittent (irrégulier) à un réseau avec infrastructure comme l'internet. Dans un tel réseau, nous considérons qu'il y a deux catégories de nœuds : des nœuds clients (ou utilisateurs) et les nœuds transporteurs qui sont mobiles et ont le rôle de transmettre les données d'utilisateurs de/vers le réseau à infrastructure. Notre modèle de confiance est basé sur les relations sociales entre les différents nœuds parmi les clients et les transporteurs**

Mots clés — DTN; Security; Trust

I. INTRODUCTION

L'utilisation massive des applications distribuées a orienté de nombreux travaux de recherche sur la nécessité d'offrir des services de sécurité (telles que l'authentification, l'intégrité et la confidentialité) afin d'augmenter l'espace d'activité des utilisateurs ayant besoin de la confiance dans leurs transferts de données. D'autre part, le besoin à plus de mobilité a rendu très répandue la notion de réseaux sans infrastructure tels que les réseaux tolérants aux délais (DTN : *Delay Tolerant Network*). Un réseau DTN est un réseau qui interconnecte plusieurs sous-réseaux, éventuellement raccordé à l'Internet. Le réseau DTN supporte l'interopérabilité de l'ensemble des sous-réseaux à travers une couche de recouvrement appelée couche « bundle » située au-dessus de la couche transport, ce qui engendre une latence imprévisible du délai de communication entre les sous-réseaux.

L'élaboration de tout service de sécurité nécessite la connaissance préalable du modèle de confiance sous-jacent. Dans la littérature, il existe plusieurs modèles de confiance. Les plus répandus se basent sur une ou plusieurs tierces parties de confiance, comme les infrastructures à clés publiques [1] et Kerberos [2]. Il existe d'autres modèles plus appropriés aux réseaux sans infrastructures de communication fixe, comme les modèles distribués [3], les modèles basés sur les graphes de confiance [4,5], ou les modèles tolérants aux défaillances comme ceux basés sur la cryptographie à seuil [6,7,8,9].

Dans cet article, nous proposons un modèle de confiance pour les réseaux tolérants aux délais. Notre modèle de confiance est destiné à un type particulier d'architecture du réseau DTN. Ceci est composé de plusieurs sous-réseaux se trouvant dans des régions géographiquement isolées et qui ont un accès intermittent à un réseau avec infrastructure de communication. Dans ce modèle de communication, nous considérons deux catégories de nœuds : les nœuds clients qui sont les utilisateurs de chaque région et les nœuds transporteurs qui sont chargés de transmettre les données des utilisateurs de/vers le réseau avec infrastructure. Notre modèle de confiance est établi à travers les relations sociales qui relient l'ensemble des nœuds dans le réseau. La relation sociale est définit sur la base de la confiance mutuelle existante entre deux nœuds. Si un nœud client et un nœud transporteur se font mutuellement confiance, chacun d'eux délivre à l'autre un certificat à clé publique afin qu'ils puissent s'authentifier et sécuriser leurs échanges de données. Nous montrons à travers les résultats de simulations l'adéquation de ce modèle de confiance pour le cadre des réseaux DTN.

Le reste de cet article est organisé comme suit. Nous donnons dans la Section II un état de l'art sur la sécurité dans les réseaux DTN. Dans la Section III, nous présentons notre modèle de confiance pour le cadre des réseaux DTN, et nous présentons ensuite les résultats de simulations dans la Section IV. Enfin, la Section V conclut l'article.

II. ETAT DE L'ART

Les réseaux tolérants aux délais sont particulièrement caractérisés par des délais élevés, des débits faibles, des taux d'erreurs élevés, l'irrégularité des liens. Ceci rend l'intégration des services de sécurité un véritable challenge. La première solution qui a été développée pour sécuriser de tels réseaux est basée sur la technologie de la clé publique [10,11]. Chaque utilisateur génère ses propres paires de clés (publique, privée)

et enregistre sa clé publique auprès d'une autorité de certification. Lorsqu'un utilisateur souhaite envoyer ou transmettre ses données, il doit en premier lieu présenter au routeur une preuve d'authentification à travers la signature numérique. Le routeur vérifie la validité de cette dernière en contactant l'autorité de certification pour pouvoir vérifier la validité de la clé publique de l'utilisateur. Le problème majeur de cette solution est que le routeur ne routera ni mettra en file d'attente les données de l'utilisateur jusqu'à ce que l'autorité ait envoyé le certificat. Ceci rend cette solution inadaptée à cause du délai imprévisible de communication entre le routeur et l'autorité de certification.

Un tel état est établi à travers l'interaction avec une autorité de certification de confiance et d'enregistrement avec les voisins de routage du saut suivant (routeurs et passerelles DTNs). Chaque nœud, une fois qu'il contrôle, il authentifie et vérifie les capacités demandées de son client (nœud prédécesseur et courant) et devient, à son tour, le nœud courant dont les capacités sont l'intersection de ses capacités avec celles de son prédécesseur. Il se présentera à son tour comme client devant le nœud successeur. Ce qui est bien différent dans le modèle usuel où la vérification de l'identité du client et des services demandés se fait au niveau de la destination.

A l'heure actuelle, le groupe DTNRG de l'IRTF, groupe de recherche sur la gestion des réseaux tolérants aux délais, relate deux approches de sécurité au profit des réseaux tolérants aux délais [12]. La première concerne le protocole de sécurité du Bundle dont la spécification décrit trois entêtes de sécurité pouvant être additionnées "aux bundles" :

- L'entête d'authentification du bundle ou BAH (*Bundle Authentication Header*) pour le service contrôle d'accès qui est utilisé pour fournir l'authentification de nœud à nœud en ajoutant un message de code d'authentification ou une signature au bundle.
- L'entête de sécurité du poids de charge utile ou PSH (*Payload Security Header*) utilisée pour fournir l'authentification de bout en bout d'une façon continue et similaire de la source à la destination.
- L'entête de confidentialité ou CH (*Confidentiality Header*) qui est utilisée pour encapsuler la charge utile de chiffrage du bundle.

Chaque entête de sécurité contient l'information sur la sécurité source et l'information sur la sécurité de destination et un texte chiffré. Le texte chiffré définit les algorithmes qui vont être employés pour traiter la sécurité des entêtes reçues. La partie sécurité de l'expéditeur et l'information du texte chiffré déterminent ensemble les clés qui vont être employées. Différentes combinaisons de ces entêtes de sécurité peuvent être utilisées simultanément. La politique de sécurité des routeurs utilise le PSH pour renforcer le contrôle d'accès.

La seconde approche, additionnelle, explique le raisonnement des choix de la conception cryptographique basée sur l'identité hiérarchisée (HIBC), qui est utilisé pour viser des questions telles que l'établissement d'un canal sécurisé, l'authentification mutuelle et la révocation de clés. Pour la protection de l'infrastructure DTN, des services de sécurité d'agents des Bundles sont proposés tel que le contrôle d'accès, la vérification d'intégrité des données saut-par-saut, l'authentification des terminaux saut-par-saut et le manque de détection de réplication dans les routeurs. Le contrôle d'accès est effectué afin de s'assurer que seules les demandes légitimes de l'autorité et les permissions appropriées sont autorisés à envoyer des bundles dans le réseau. Le protocole Bundle supporte l'intégrité des données et des services d'authentification des nœuds le long de chaque saut [13]. Ces services peuvent être fournis sur un lien DTN soit par l'utilisation de BAH (entête d'authentification du bundle) sur ce lien ou bien par la couche de recouvrement bundle de l'hôte récepteur assurant l'authenticité le long de ce lien. Quand le bundle est envoyé d'une seule source à une seule destination, à chaque saut qui intervient, l'agent qui envoie le bundle calcule le haché du bundle, signe le hach avec sa clé privée, et retransmet le bundle vers le prochain agent du Bundle. L'agent récepteur reçoit le bundle, vérifie la validité de la valeur du hach signé en le comparant avec la valeur du hach calculée. Ensuite, il calcule un nouveau hach signé du bundle avant sa retransmission via une seule interface au prochain saut le long de son chemin. Le fait que l'agent récepteur du bundle puisse décrypter le hach signé en une valeur correcte permet aussi bien l'authentification de l'émetteur et du destinataire du bundle ainsi que la vérification de l'intégrité du bundle.

Globalement, le système des mécanismes de sécurité est basé sur l'infrastructure technologique à clé publique ou PKI [11]. Chaque nœud utilise une paire de clés délivrées par une Autorité de Certification. Cette approche ne convient pas dans un environnement de réseau DTN vu qu'il est difficile d'accéder en ligne (instantanément) pour obtenir et vérifier la validité des clés et la liste de révocation.

Une approche dite *Cryptographie à base d'Identité* ou IBC (*Identity-Based Cryptography*) fût proposée [14]. C'est une méthode cryptographique qui permet le chiffrement de message et la vérification de signature utilisant l'identité publique de la cible comme clé. Dans IBC, un nœud source obtient la clé publique de destination à partir de l'identité de destination, par exemple une adresse électronique. Cependant, dans le domaine public spécifique d'IBC, les paramètres d'IBC doivent être distribués de manière à permettre aux utilisateurs d'obtenir les clés publiques d'une identité donnée. La distribution de tels paramètres peut poser des problèmes car tous les utilisateurs n'appartiennent pas forcément au même groupe et des groupes différents pourraient avoir des paramètres différents.

L'approche hiérarchisée d'IBC ou HIBC (*Hierarchical IBC*) [15] quant à elle considère des régions différentes ayant des sous-régions et chacune maintient ses propres PKGs. Le problème majeur avec HIBC est qu'une compromission d'un générateur à clés publiques (PKG) implique la compromission de toutes les clés générées par les PKGs de niveaux inférieurs. Les méthodes actuelles n'améliorent pas, globalement, d'une façon significative la sécurité des DTNs (authentification, confidentialité, l'intégrité et autres) car les ressources des DTNs et le champ d'expression de ces réseaux sont limités. Il a fallu traiter cas par cas pour espérer améliorer la sécurité d'une architecture réseau DTN donnée. La nécessité de sécuriser ces

réseaux est grande car leur présence sur le terrain apparait de plus en plus (voir KIOSKNET) importante.

III. NOTRE MODELE DE CONFIANCE

A. *L'architecture ciblée du réseau DTN*

Dans cet article, nous nous intéressons à l'architecture d'un réseau doté d'une infrastructure de communication connectée à un ensemble de sous-réseaux sans infrastructure à travers des passerelles de communication. Chaque sous-réseau couvre une région géographiquement isolée. Dans la figure 1, nous illustrons un exemple de cas d'application. Dans ce modèle de communication, chaque région isolée comprend des utilisateurs qui ont besoin de recevoir/transférer des données de/vers le réseau avec infrastructure. Cette communication est assurée à travers les bus urbains de chaque région qui se déplacent régulièrement à partir de la région vers la partie avec infrastructure. Chaque bus est doté d'un équipement sans fil qui lui permet d'ouvrir une session de transfert avec les utilisateurs qui se trouvent dans sa portée de communication lors de son passage. Les données des utilisateurs récoltées seront transmises, à son arrivée, à la partie du réseau avec infrastructure. Inversement, lors de son retour, il rapporte les données destinées aux utilisateurs de la région. Nous considérons aussi qu'il est possible qu'un bus réplique les données détenues vers les bus qui le croisent sur sa trajectoire. Cette opération est importante dans le sens où le premier arrivé s'en charge de les délivrer au destinataire, ce qui améliore relativement la fiabilité des communications. Egalement, la réplication des données minimise le risque de perte. Ce modèle de communication peut être utilisé dans d'autres cas d'applications. Par exemple, dans le domaine militaire, les données peuvent être échangées entre la zone de bataille et le centre de commandement à travers des avions militaires. Il est possible également de faire échanger des données entre les ports et les bateaux qui se trouvent dans le grand océan à travers les avions de voyage.

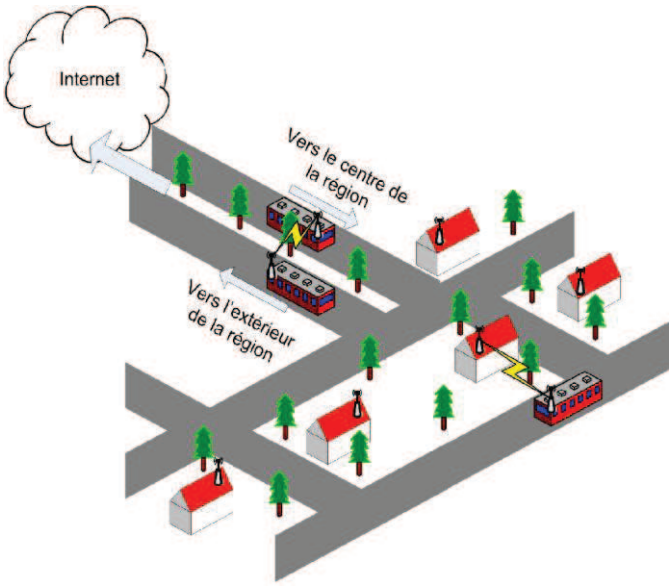

Figure 1. L'architecture ciblée du réseau DTN

B. *Modèle de Confiance*

Nous classifions les nœuds en deux catégories : *les nœuds clients*, qui représentent les utilisateurs de la région, et *les nœuds transporteurs* qui assurent l'opération de transfert des données des utilisateurs de/vers la partie du réseau avec infrastructure. Chaque nœud transporteur ne peut ouvrir une session de transfert qu'avec un nœud client ou un nœud transporteur, à travers un seul saut. Nous supposons que la relation de confiance entre l'ensemble des nœuds est préétablie à travers les relations sociales entre les utilisateurs. Ceci permet à chaque nœud de choisir uniquement ceux envers lesquels il fait confiance pour envoyer ou recevoir ses données. D'un autre côté, chaque nœud transporteur va choisir uniquement ceux envers lesquels il fait confiance pour transférer leurs données. Ceci permet d'élaborer un graphe de confiance particulier qui relie d'une manière réciproque chaque nœud client et chaque nœud transporteur dans le réseau (cf. figure 2). Pour ouvrir une session de transfert entre un nœud client et un nœud transporteur, il est nécessaire qu'il y ait une confiance réciproque entre les deux nœuds. Pour mettre en œuvre cette confiance mutuelle, chaque nœud délivre à l'autre un certificat à clé publique afin de pouvoir s'authentifier et sécuriser les sessions de transferts qui seront établies ultérieurement. Dans le cas d'un transfert de données entre deux nœuds transporteurs, chacun d'eux doit prouver à l'autre qu'il est certifié par le nœud dont ses données font l'objet du transfert.

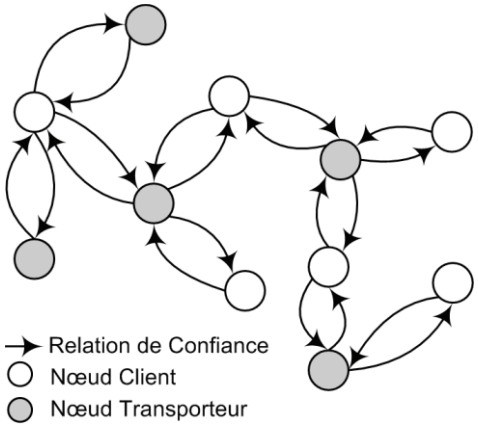

Figure 2. Le graphe de confiance établi

C. *Délivrance des certificats*

La décision de délivrance des certificats est basée sur le rapport social entre les nœuds du réseau. Si un nœud client (respectivement transporteur) croit qu'un nœud transporteur (respectivement client) qu'il est digne de confiance dans le sens où il va assurer correctement le transfert de ses données, alors le nœud client peut lui délivrer un certificat à clé publique signé avec sa propre clé privée. Les certificats sont délivrés selon une période de validité décidée par le nœud émetteur. Quand un certificat expire et son émetteur croit que le nœud est toujours digne de confiance, l'émetteur peut lui délivrer un nouveau certificat avec une nouvelle période de validité.

D. Authentification lors d'une session de transfert

Les sessions de transferts de données sont ouvertes seulement à travers un seul saut de communication, c'est-à-dire que la communication sera directe entre le nœud client et le nœud transporteur sans l'aide de nœuds intermédiaires. Ceci est nécessaire dans le sens ou le processus d'authentification doit s'achever instantanément pour pouvoir commencer le transfert. Si on adopte une communication à multi-sauts, le processus d'authentification va être perturbé par le délai de réponse qui est une caractéristique particulière du réseau DTN. Egalement, avec cette façon, l'authentification sera binaire seulement entre le nœud client et le nœud transporteur. Par ailleurs, adoptant une session de transfert à multi-sauts complique davantage le processus d'authentification qui va devoir être établi dans ce cas de bout en bout avec toujours un délai de réponse imprévisible.

Avant d'initier le processus de transfert, chaque nœud envoie à l'autre son certificat qui doit être signé antérieurement par son interlocuteur même. Si les certificats sont corrects par rapport à la validité des signatures et à la période de validité, le nœud client chiffre ses données avec la clé publique du nœud transporteur avant de les envoyer pour les protéger contre l'écoute clandestine. Dans le cas d'un transfert entre deux nœuds transporteurs, chacun d'eux va devoir tout d'abord délivrer à l'autre un *certificat de croisement*. Avec ce dernier, un nœud transporteur donné peut prouver à son nœud client d'être entré en contact avec un autre nœud transporteur en qui il fait confiance. Ensuite, chaque nœud transporteur identifie les identités des utilisateurs qui détiennent leurs données. Les deux nœuds transporteurs doivent s'échanger seules les données des utilisateurs en qui les deux font confiance. Ceci sera vérifié seulement à travers les certificats qu'aura délivrés le nœud client pour les deux nœuds transporteurs. Une fois l'échange est fait, le nœud transporteur qui a répliqué les données délivre à l'autre un *certificat de réplication*. En réponse, le deuxième nœud transporteur lui délivre *un certificat de réception*.

A chaque opération de transfert accomplie vers le réseau avec infrastructure, le nœud transporteur doit répondre (justifier), lors de son prochain contact avec le nœud client, avec un accusé de réception du destinataire et l'ensemble des certificats de réplication, de réception et de croisement qu'ont lui ont délivré les nœuds transporteurs avec lesquels ses données ont été échangées. Ceci est nécessaire pour le nœud client afin qu'il puisse mettre à jour le degré de confiance de ses nœuds transporteurs.

E. Mise à jour de la confiance des nœuds transporteurs

Chaque nœud client évalue régulièrement le degré de la confiance C_i (initialisé à 1) de chaque nœud transporteur i par rapport à l'ensemble des différents certificats qu'il détient. Les règles d'évaluation sont faites selon trois cas possibles :

1. Le nœud transporteur i est rentré en contact avec le nœud client pour un nouveau transfert de données, alors qu'il n'a pas remis l'accusé de réception du transfert précédent.
2. Le nœud client détient un certificat de croisement de deux nœuds transporteurs i et j, alors que chacun d'eux n'a délivré à l'autre ni certificat de réplication, ni certificat de réception.
3. Le nœud client détient un certificat de croisement de deux nœuds transporteurs i et j, dans lequel j a reçu un certificat de réplication et i a reçu un certificat de réception.

Pour le premier cas, le nœud client constate que le nœud transporteur i a quitté puis rejoint la région sans faire suivre ses données vers le destinataire dans le réseau avec infrastructure, ce qui lui permet de dégrader son degré de confiance ($C_i \leftarrow C_i$-1). Autrement, à chaque réception d'un accusé de réception, le nœud client augmente le degré de confiance du nœud transporteur i ($C_i \leftarrow C_i$+1). Pour le deuxième cas, le nœud client constate qu'il y a eu un contact entre deux de ses nœuds transporteurs alors qu'il n'a eu aucune réplication de ses données, ce qui lui permet de dégrader le degré de confiance du nœud transporteur qui détient les données. Pour le troisième cas, le nœud constate que les deux nœuds transporteurs ont effectué la réplication de ses données, ce qui lui permet d'augmenter le degré de la confiance des deux nœuds.

F. Révocation des certificats

Chaque nœud client peut annuler ses certificats pour deux raisons : (1) si le degré de la confiance du nœud transporteur est inférieur à 1, ou (2) si la période de validité du certificat est expirée. La révocation d'un certificat se fait à travers la création d'un certificat particulier que nous nommons *certificat de révocation*. Il certifie à travers ce dernier d'avoir annulé le certificat du nœud transporteur en question, et ceci pour informer le reste de l'ensemble de ses nœuds transporteurs de ne plus répliquer ses données vers le transporteur suspect.

IV. RESULTATS DE SIMULATIONS

A. Environnement et paramètres des simulations

Les simulations sont faites sous l'environnement *matlab*. Nous avons opté pour un modèle de simulation qui comporte un réseau avec une taille de 100 nœuds dans une surface rectangulaire de 1000 m^2. Les nœuds sont répartis comme suit : 30% de nœuds transporteurs qui sont mobiles, et 70% de nœuds clients qui sont fixes. Les nœuds transporteurs se déplacent sur la surface suivant le modèle de mobilité *random waypoint* [16] avec une vitesse variable entre 0 et 20 m/s et une durée de pause variable entre 0 et 20 s. Nous considérons que le point d'accès vers la partie du réseau avec infrastructure se trouve à la plage rectangulaire délimitée par les points cartésiens {(0,0), (10,10)} sur la surface, vers lequel les nœuds transporteurs achèvent le transfert de données des nœuds clients. Le graphe de confiance est fixé par le simulateur d'une manière aléatoire. Les requêtes de transfert de données des clients s'exécutent à chaque croisement d'un nœud client avec un nœud transporteur. Le critère évalué est le taux moyen du nombre d'opérations de transfert accomplies vers le réseau avec infrastructure.

B. *Impact du nombre de nœuds transporteurs malicieux*

Dans cette sous-section, nous nous sommes intéressés à étudier les performances de notre système avec la présence des nœuds transporteurs malicieux dans le réseau. En effet, un nœud transporteur malicieux tente de perturber le fonctionnement du transfert des données des utilisateurs en les récoltants (1) sans les faire suivre aux destinataires, et (2) sans les répliquer vers les autres nœuds transporteurs. Nous avons varié le pourcentage des nœuds transporteurs malicieux de 0 à 100% en observant le taux moyen du nombre d'opérations de transfert accomplies. Nous illustrons dans la figure 3 les résultats de cette expérience.

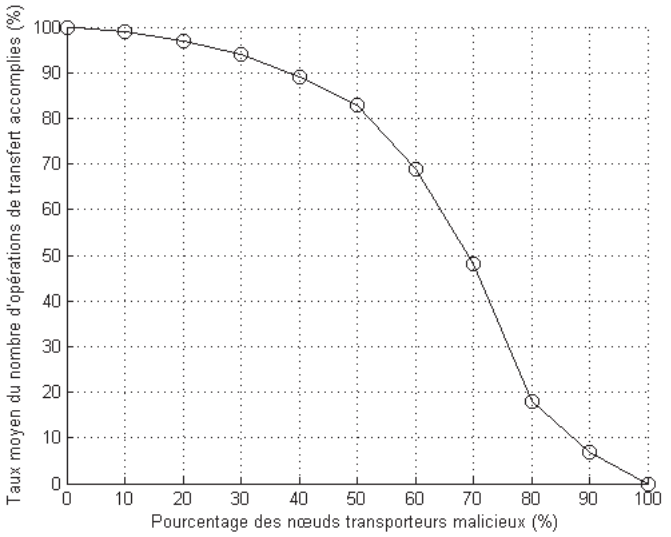

Figure 3. Impact du nombre de nœuds transporteurs malicieux

Nous constatons que notre système résiste d'une façon acceptable jusqu'à 50% de nœuds transporteurs malicieux. Au-delà de ce pourcentage, les performances subissent une chute considérable ; conséquence logique à cause du nombre important de nœuds malicieux qui paralysent le transfert de données. Par ailleurs, les performances du système sont favorables pour un pourcentage de nœuds transporteurs malicieux jusqu'à 50%. Ceci est dû au fait que les nœuds clients révoquent les nœuds transporteurs qui n'accomplissent pas correctement l'opération de transfert. Ceci permet d'isoler les nœuds transporteurs suspect malicieux. D'un autre côté, les nœuds clients répliquent leurs données à travers plusieurs nœuds transporteurs, ce qui augmente les chances d'accomplir l'opération d'acheminement de leurs données.

C. *Impact de la défaillance des nœuds transporteurs*

Dans cette sous section, nous nous sommes intéressés à étudier l'impact de la défaillance des nœuds transporteurs sur les performances du système en terme du taux moyen du nombre d'opérations de transferts accomplies. Pour cela, nous définissons deux paramètres : α et β. Le paramètre α représente la durée moyenne d'inter-défaillances. C'est la durée moyenne entre deux pannes successives d'un nœud transporteur donné. Le paramètre β représente la durée moyenne de la panne. C'est le temps écoulé entre le moment de la panne et le moment de la reprise du nœud transporteur. Nous avons varié la durée moyenne d'inter-défaillances α de 0 à 1800s pour β=900s, β=1800s, et β=2700s. Nous illustrons dans la figure 4 les résultats de cette expérience. Durant la variation de α, nous remarquons que les performances de notre système restent approximativement stables. Néanmoins, vu la fréquence aigüe des pannes impliquée pour le cas de α=0s, α=200s, et α=400s, nous estimons que cette marge ne met pas en cause la qualité des performances restantes. D'un autre côté, nous remarquons qu'il y a un écart de performances étroit pour les différentes valeurs de β. Ceci, est interprété par la forte disponibilité des données des utilisateurs qui sont répliquées par les nœuds transporteurs. De ce fait, nous estimons que notre modèle résiste contre *l'intensité* et la *durabilité* des pannes.

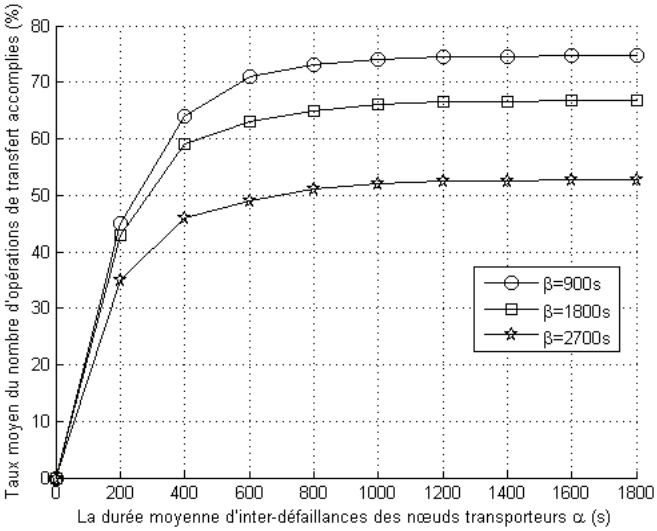

Figure 4. Impact de la durée moyenne d'inter-défaillances α pour β=900s, β=1800s, et β=2700s

V. CONCLUSION

Dans cet article, nous avons proposé un modèle de confiance pour une architecture spécifique du réseau DTN. Le réseau est composé de plusieurs sous-réseaux se trouvant dans des régions géographiquement isolées et qui ont un accès intermittent au réseau avec infrastructure de communication. Chaque sous-réseau comporte des nœuds clients et des nœuds transporteurs qui assurent l'acheminement des données vers le réseau avec infrastructure. Avec notre modèle, la confiance est gérée d'une manière autonome par les utilisateurs eux-mêmes. Le degré de la confiance initiale est établi par rapport aux relations sociales qui relient l'ensemble des nœuds dans le réseau. La mise en œuvre de cette relation de confiance est maintenue à travers la délivrance de certains types de certificats avec lesquels les nœuds clients évaluent périodiquement le degré de la confiance de leurs nœuds transporteurs. Pour mettre en valeur les qualités de performance de notre solution, nous avons effectué des simulations, où ces dernières ont montré que notre modèle résiste aux comportements malicieux et la défaillance.

REFERENCES

[1] R. Perlman. *An Overview of PKI Trusts Models*. IEEE Network, 1999.

[2] J. Kohl, B. Neuman. *The Kerberos Network Authentication Service Version 5*. RFC-1510, 1991.

[3] A. Abdulrahman, S. Hailes. *A Distributed Trust Model*. In Proceedings 97 New Security Paradigms, 1997.

[4] S. Capkun, L. Buttyan, J. Hubaux. *Self-ogranized public key management for mobile Ad hoc networks*. IEEE Transactions on Mobile Computing, 2003.

[5] A. Abdulrahman. *The PGP Trust Model*. The Journal of Electronic Commerce, 1997.

[6] J. Luo, J. Hubaux, P. Eugster. *DICTATE: Distributed Certification Authority with Probabilistic Freshness for Ad hoc Networks*. IEEE Transactions on Dependable and Secure Computing, 2005.

[7] L. Zhou, F. Schneider, R. Renesse. *COCA: A Secure Distributed Online Certification Authority*. ACM Transactions Computing Systems, 2002.

[8] H. Luo, S. Lu. *Ubiquitous and Robust Authentication Services for Ad hoc Wireless Networks*. Technical Report, UCLA Computer Science, 2000.

[9] L. Zhou, Z. Haas. *Securing Ad hoc Networks*. IEEE Network, 1999.

[10] R.C. Durst. *An infrastructure security model for delay tolerant networks*. Révision 5, 2002.

[11] R. Housley, W. Polk, W. Ford, D. Solo. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 2459, 2002.

[12] S.F. Symington, S. Farrell, H. Weiss, P. Lovell. *Bundle Security Protocol Specification*. Technical Report in Computer Science and Engineering Lehigh University, 2005.

[13] S. Farrell, S.F. Symington, H. Weiss, P. Lovell. *Delay-Tolerant Networking Security Overview*. draft-irtf-dtnrg-sec-overview, 2009.

[14] A. Shamir. *Identity-Based Cryptosystems and Signature Schemes*. Lecture notes in computer science, springer, 1985.

[15] A. Seth, S. Keshav. *Practical Security for Disconnected Nodes*. ICNP Workshop on Secure Network Protocols (NPSec), 2005.

[16] C. Bettstetter. *Topology Properties of Ad Hoc Networks with Random Waypoint Mobility*. In Proceedings of ACM Int. Symposium in Mobile Ad Hoc on Networking and Computing (MobiHoc), 2003.