Séminaire Mathématique de Béjaia (LaMOS),
Volume 14, 2015, pp. 15 - 18

3

La Théorie des Jeux pour la Clusterisation, l'Énergie et la Sécurité des Réseaux Ad hoc

M. BOUHADDI et S. M. RADJEF

Laboratoire de Modélisation et d'Optimisation des Systèmes (LAMOS)
Université de Béjaïa, Béjaïa 06000, Algérie
Tél. (213) 34 81 37 08

Résumé L'absence d'une gestion centralisée des fonctionnalités des réseaux MANETs les rend beaucoup plus vulnérables que leurs homologues sans fil et filaires. Malheureusement, les protocoles de sécurité classiques ne sont pas conçus pour un environnement tel que celui des MANETs. Non seulement l'environnement est dynamique, mais en plus les ressources y sont limitées (mémoire, capacité de calcul et plus particulièrement l'énergie). La problématique en devient plus complexe, car comme nous le savons, les solutions de sécurité sont gourmandes en ressources. Le défi à relever est alors de concevoir un mécanisme de sécurité infaillible pour les MANETs. Dans ce travail, nous étudions les solutions susceptibles d'assurer la sécurité des réseaux mobiles Ad-hoc, en proposant une architecture hiérarchique permettant d'établir une infrastructure dynamique basée sur les outils de la théorie des jeux.
Mots clés : MANETs, Sécurité, Système de détection d'intrusion (IDS), Clustering, Théorie des jeux.

Les réseaux Ad hoc connaissent un engouement de plus en plus important dans le domaine de la recherche, du fait notamment de leur extensibilité par rapport aux réseaux avec infrastructures [2]. Les réseaux mobiles Ad hoc, ou bien appelés MANET (Mobile Ad hoc NETwork), sont définis comme un ensemble de nœuds mobiles et autonomes qui sont interconnectés par des liens de communication sans fils [1].

Ces réseaux constituent une technologie émergeant offrant à leurs utilisateurs de nombreux avantages en termes de coût et de facilité d'utilisation, ce qui a popularisé leurs domaines d'application [2]. Nous les retrouvons aussi bien dans des applications militaires, commerciales, le travail collaboratif, mais aussi dans les services d'urgence et les réseaux de capteurs.

Position du problème

Reste que si les perspectives sont prometteuses, les contraintes en sont à la hauteur. En effet, ces réseaux sont caractérisés par des ressources limitées en énergie. La conservation de cette dernière s'avère donc être un facteur primordial pour la durée de vie du réseau.
Ajouté à cela, la présence de nœuds refusant la participation aux fonctionnalités du réseau, comme la retransmission, la sécurité ou même être délégués avec comme objectif de maximiser leur propre bénéfice tout en minimisant leur propre contribution au profit des autres nœuds du réseau et sont appelés nœuds égoïstes.

Ces réseaux sont également, par nature, plus vulnérables et plus difficiles à protéger que les réseaux filaires en raison de leur caractère spontané, ces derniers ne peuvent bénéficier des mécanismes de sécurité s'appuyant sur l'infrastructure, comme un pare-feu ou un serveur d'authentification. En conséquence, chaque nœud constitue un point de vulnérabilité qui ne peut compter que sur ses propres ressources et ses services pour se protéger.

Etat de l'art

Il existe différents travaux dans la littérature qui ont traité de ces problématiques définies, la gestion de l'énergie [5], le problème d'égoïsme [3] et de sécurité [7].
Une méthode efficace pour réduire les dépenses des nœuds en énergie, qui constitue une denrée rare, est une technique de regroupement connu sous le nom de clusterisation. Elle consiste à structurer le réseau en groupes d'entités appelés clusters donnant ainsi au réseau une structure hiérarchique.
Chaque cluster est représenté par un nœud particulier appelé cluster-head. Un nœud est élu cluster-head selon une métrique telle que le degré, la mobilité, l'identité des nœuds, ou bien sur la base d'une combinaison de ces paramètres.

Parmi les algorithmes de clusterisation les plus connus, on retrouve l'algorithme **LEECH**, qui se base sur une sélection aléatoire des cluster-heads et se fait en rotation afin d'équilibrer la consommation d'énergie. L'algorithme **HEED** qui sélectionne le cluster-head sur la base de l'énergie consommée et ne fait aucun hypothèse sur l'emplacement des nœuds. L'algorithme **ILBH** qui est utilisé pour équilibrer la consommation des nœuds, deux paramètres α et β sont utilisés tels que $\alpha < \beta$. Lorsque l'énergie d'un nœud diminue jusqu'à atteindre un seuil α, il réduit sa puissance de transmission et passe à l'état sommeil et ne change d'état qu'une fois que son niveau de batterie ré-atteint le seuil β, et il ne sera pas élu cluter-head pendant cette période de temps. Les paramètres α et β sont choisis avec soin de manière à ce que tous les nœuds ne se mettent pas en veille en même temps. Les résultats de la simulation ont montré que pour atteindre un résultat optimal, l'écart entre α et β ne doit pas dépasser 0.1.

Nous remarquons que dans ces algorithmes que nous venons de citer, aucun ne traite de la question des nœuds égoïstes.
Le problème de l'égoïsme des nœuds, est défini dans le cadre de cette recherche comme la non-collaboration du nœud dans le processus de sécurité et cela dans le but de conserver l'énergie. Les mécanismes d'incitation se distinguent par la manière dont les nœuds sont incités à coopérer. Nous retrouvons les mécanismes basés sur les crédits et ceux basés sur la réputation.

- Mécanismes basés sur les crédits : l'idée de base de ce système est d'utiliser les crédits pour récompenser les nœuds qui participent aux services du réseau. Ces crédits agissent comme

une compensation pour les coûts liés aux dépenses énergétiques, ils peuvent être par la suite utilisé par les nœuds pour bénéficier eux aussi des services du réseau.

- Mécanismes basés sur la réputation : la réputation d'un nœud est une quantité dynamique qui est formée et mise à jour en utilisant des observations directes ou des informations fournies par les autres membres du réseau. Si la réputation est inférieure à un seuil pré-défini, il sera considéré comme égoïste et donc sera écarté du réseau pour une certaine période appelée "phase de punition".

Modèle proposé

L'idée proposée pour une gestion efficace du réseau en terme d'énergie et de sécurité, est de clusteriser le réseau en utilisant le jeu de clustering. Cette technique de clusterisation, à la différence des autres techniques :

- Induit moins de messages à envoyer et donc moins de dépenses en énergie,
- Equilibre la consommation en énergie, car la sélection du cluster-heads se fait en rotation,
- La procédure de clusterisation sera basée sur l'incitation naturelle des nœuds à participer au processus d'élection et donc à la coopération.

Le modèle présenté, viendra améliorer les travaux [4]. En effet, en plus de considérer le voisinage des nœuds et le rayon de transmission lors du déroulement du jeu, on considérera également l'impact de la présence d'un mécanisme de sécurité dans le déroulement du jeu mais également, l'énergie résiduelle dans la sélection du cluster-head. Pour la sécurisation des données du réseau, on installera un système de détection d'intrusions (IDS) sur chaque nœud du réseau qui analysera le trafic circulant sur le support sans fil pour détecter les activités malveillantes. A des fins de conservation d'énergie, on n'activera ces IDSs uniquement sur les cluster-heads. Par la suite, on s'intéressera au problème d'égoïsme des cluster-heads dans leur participation à la sécurisation de leurs membres afin de conserver leur énergie. Dans le but d'inciter les cluster-heads à garder leur IDS actif pour sécuriser le trafic entrant et sortant de son cluster, on introduira un système de réputation qui mesurera la participation des cluster-heads dans la sécurité suivant le taux de détection, ainsi cette valeur se mettra à jour à chaque tour. Dans la dernière étape du modèle, on considérera l'interaction existant entre un nœud intrus dans le type n'est pas connu et le cluster-head qui veillera à la sécurité de ses membres en attribuant plus d'attention aux nœuds dans la valeur de réputation est plus élevée. Cette partie du travail, viendra améliorer les travaux [6].

Références

[1] D.P. Agrawal, Q.A. Zeng (2003). Introduction to wireless and mobile systems, Ad Hoc and Sensor Networks. Brooks/Cole-Thomson Learning pp. 297-348.

[2] A. Deodhar, R. Gujarathi (2003), "A Cluster Based Intrusion Detection System for Mobile Ad Hoc Networks".

[3] D. J. Goodman and N. B. Mandayam (2000), "Power control for wireless data", IEEE Person. Comm., Vol. 7, No. 2, pp. 48–54.

[4] G. Koltsidas, F-N. Pavlidou (2011), "A game theoretical approach to clustering of ad-hoc and sensor networks", Telecommunication Systems, Volume 47, Issue 1-2, pp 81-93.

[5] S. Lasaulce, Y. Hayel, R. El Azouzi and M. Debbah (2009), "Introducing hierarchy in energy games", IEEE Trans. on Wireless Comm., Vol. 8, No. 7, pp. 3833–3843.

[6] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, P. Bhattacharya (2007), "A game-theoretic intrusion detection model for mobile ad hoc networks", Computer Communications 31, 708–721.

[7] Yi Ping, Jiang Xinghao, Wu Yue, Liu Ning (2000), Distributed intrusion detection for mobile ad hoc networks, Journal of Systems Engineering and Electronics Vol. 19, No. 4, pp.851–859.