Communication fiable dans un réseau dynamique en présence de fautes Byzantines

Alexandre Maurer, Xavier Defago, Sébastien Tixeuil

Communication fiable dans un réseau dynamique en présence de fautes Byzantines

Alexandre Maurer[1], Xavier Defago[2] et Sébastien Tixeuil[3,4]

[1] *École Polytechnique Fédérale de Lausanne (EPFL)*
[2] *Japan Advanced Institute of Science and Technology (JAIST)*
[3] *Sorbonne Universités, UPMC Univ. Paris 06, LIP6 CNRS UMR 7606*
[4] *Institut Universitaire de France*

On considère un réseau multi-sauts sujet à k fautes Byzantines : jusqu'à k nœuds peuvent avoir un comportement malveillant arbitraire et totalement imprévisible. Dans cet article, nous prouvons une condition nécessaire et suffisante pour communiquer fiablement en présence de k fautes Byzantines dans un réseau dynamique, où la topologie peut évoluer au fil du temps. La preuve est constructive : un algorithme est proposé pour la condition suffisante. Nous considérons les cas cryptographique et non-cryptographique. Nous appliquons ensuite cette condition à deux cas d'étude : des participants interagissant dans une conférence, et des agents se déplaçant dans le métro parisien.

Keywords: Tolérance aux fautes Byzantines, réseaux dynamiques, protocole de communication.

1 Introduction

Dans un contexte où les réseaux deviennent de plus en plus grands, ils deviennent de plus plus susceptibles de défaillir. En effet, les nœuds du réseau peuvent être sujets à des pannes, attaques, corruptions de mémoire... Nous considérons ici le modèle de faute le plus général possible : le modèle Byzantin [LSP82], où les nœuds fautifs ont un comportement totalement arbitraire. Par conséquent, tolérer des nœuds Byzantins implique de garantir qu'il n'existe aucune stratégie (aussi improbable soit-elle) leur permettant de déstabiliser le réseau.

Il a été montré que, pour tolérer k nœuds Byzantins arbitrairement placés dans un réseau statique, il est nécessaire et suffisant d'avoir $2k+1$ chemins nœud-disjoints entre l'émetteur et le récepteur[Dol82, NT09]. La preuve de ce résultat utilise le théorème de Menger [BGH01], qui garantit l'équivalence entre coupe minimale et connectivité. Ce théorème ne s'applique pas aux réseaux dynamiques [KKK02] dont la topologie évolue pendant l'exécution de l'algorithme. Par exemple, dans la Figure 1, il faut supprimer aux minimum 2 nœuds pour déconnecter l'émetteur du récepteur. Or, il est impossible de trouver 2 chemins nœud-disjoints les reliant. La conséquence de ce résultat, c'est que les algorithmes conçus pour les réseaux statiques peuvent ne délivrer aucun message (un tel algorithme attend typiquement pour délivrer une information de la recevoir via $2k+1$ chemins nœud-disjoints) dans un graphe dynamique.

Dans cet article, nous prouvons une condition nécessaire et suffisante pour garantir la communication fiable dans un réseau dynamique. Notre condition suffisante est constructive (nous donnons un algorithme). Nous appliquons ensuite cette condition à divers cas d'étude.

2 Condition de communication fiable

Modèle. On considère le modèle de réseau dynamique défini par Casteigts *et al.* [CFQS12] : un réseau dynamique est un quadruplet (V, E, ρ, ζ) où :

- V est l'ensemble des nœuds.
- $E \subseteq V \times V$ est l'ensemble des canaux de communication.
- $\rho : E \times \mathbb{R}^+ \to \{0,1\}$ est la fonction de présence : $\rho(e,t) = 1$ indique que le canal e est présent à la date t.

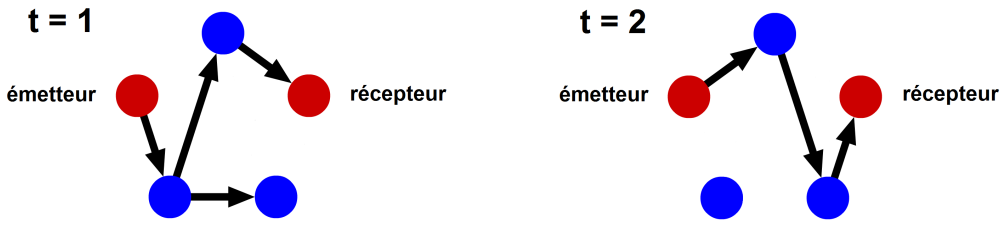

FIGURE 1: Contre-exemple au théorème de Menger dans les graphes dynamiques. Les flèches noires représentent les canaux de communication présents à la date donnée. La coupe minimale est 2 alors que la connectivité est 1.

– $\zeta : E \times \mathbb{R}^+ \to \mathbb{R}^+$ est la fonction de latence : $\zeta(e,t) = T$ indique qu'un message envoyé à la date t prend le temps T pour franchir le canal e.

Définitions. Dans un réseau dynamique, un *chemin dynamique* entre deux nœuds p et q est une séquence de nœuds tel qu'il existe une séquence de dates croissantes qui permet à un message envoyé par p de passer par les nœuds du chemin pour parvenir à q. On note $Dyn(p,q)$ l'ensemble des chemins dynamiques de p vers q. Pour tout ensemble de chemins dynamiques Ω, on note $MinCut(\Omega)$ le nombre minimal de nœuds qu'il faut supprimer pour couper tous les chemins dynamiques de Ω.

Hypothèses. Nous faisons les même hypothèses que les travaux précédents [Dol82, NT09] : chaque nœud a un identifiant unique, et lorsqu'un message est reçu par un canal (p,q), q connaît l'identité de p. Un adversaire omniscient peut choisir jusqu'à k nœuds et les rendre Byzantins (ce choix se fait avant le début de l'exécution du système). Les nœuds corrects n'ont aucun moyen de savoir *a priori* quels nœuds sont Byzantins.

Communication fiable. On dit qu'on peut garantir une *communication fiable* d'un nœud correct p à un nœud correct q lorsque les deux conditions suivantes sont satisfaites :
– Si p diffuse un message, alors q finit par le recevoir et l'accepter.
– Si q accepte un message comme provenant de p, alors p est nécessairement l'auteur de ce message.

Algorithme. Chaque nœud correct u possède les variables suivantes :
– $u.m_0$, le message que u souhaite diffuser.
– $u.\Omega$, un ensemble dynamique enregistrant tous les triplets (s,m,S) reçus par u, où s est la source du message m, et S est l'ensemble des nœuds visités par m depuis son envoi par s.
– $u.Acc$, un ensemble dynamique de couples (s,m) confirmés. Lorsque $(s,m) \in u.Acc$, u considère que s est l'auteur du message m.

Initialement, $u.\Omega = \{(u,u.m_0,\emptyset)\}$ et $u.Acc = \{(u,u.m_0)\}$. Chaque nœud correct u obéit aux trois règles suivantes :

1. Initialement, et à chaque fois que $u.\Omega$ ou que le voisinage local de u change : envoyer $u.\Omega$ à tous les voisins de u.
2. Lorsque Ω' est reçu par le canal (v,u) : $\forall (s,m,S) \in \Omega'$, si $v \notin S$, ajouter $(s,m,S \cup \{v\})$ à $u.\Omega$.
3. Dès qu'il existe s, m et $\{S_1,\ldots,S_n\}$ tels que $\forall i \in \{1,\ldots,n\}$, $(s,m,S_i \cup \{s\}) \in u.\Omega$ et $MinCut(\{S_1,\ldots,S_n\}) > k$, ajouter (s,m) à $u.Acc$.

Condition de communication fiable sans crypotographie (modèle oral [LSP82]). Dans le papier complet [MDT15], nous montrons que deux nœuds corrects p et q communiquent fiablement si et seulement si $MinCut(Dyn(p,q)) > 2k$.

La condition nécessaire utilise des arguments classiques d'indiscernabilité entre les nœuds corrects et les nœuds Byzantins, en raisonnant sur les coupes minimales dynamiques plutôt que sur les chemins nœud-disjoints.

La condition suffisante utilise l'algorithme ci-dessus. Cet algorithme fonctionne par inondation du réseau de messages qui contiennent l'ensemble des nœuds déjà visités (si tous les nœuds visités sont corrects, cet ensemble est constitué de nœuds appartenant au parcours effectivement suivi par le message ; si un Byzantin ou plus fait partie des nœuds visités, cet ensemble peut être arbitraire). Un nœud correct q ne délivre un message m de p que si l'ensemble des parcours reçus concernant m originaire de p satisfait $MinCut(Dyn(p,q)) > k$: on a alors la certitude que le message a transité par au moins un parcours composé uniquement de nœuds corrects, et qu'il est donc authentique.

Condition de communication fiable avec cryptographie (modèle écrit [LSP82]). Si les nœuds peuvent utiliser de la cryptographie à clé publique, alors il devient possible d'identifier l'émetteur après de multiples retransmissions (l'émetteur chiffre le message avec sa clef privée, et chaque nœud intermédiaire utilise la clef publique de l'émetteur pour authentifier le message). Nous montrons alors que la condition de communication fiable devient $MinCut(Dyn(p,q)) > k$. Si cette condition est vraie, alors il existe un parcours composé uniquement de nœuds corrects entre la source et la destination, et il suffit à la destination de délivrer le premier message correctement authentifié. Si cette condition n'est pas vérifiée, les nœuds Byzantins sont en mesure de déconnecter la source de la destination, et le message n'est jamais délivré.

3 Cas d'étude

Participants interagissant dans une conférence Lors de la conférence Infocom 2005, les interactions entre participants ont été enregistrées à l'aide de capteurs [CHC+07], ce qui correspond à un réseau dynamique où chaque participant est un nœud. Nous considérons une période de 8 heures du second jour de conférence. Sur cette période, nous considérons les 10 nœuds les plus "sociables" (la sociabilité étant définie ici par le nombre de contacts initiés). Nous supposons qu'un de ces nœuds peut être Byzantin ($k = 1$).

Soient deux nœuds corrects p et q. Supposons que p veuille transmettre un message à q dans un intervalle de dix minutes. Si on veut garantir la communication fiable de p à q, la stratégie simple consiste à attendre que p rencontre q directement. Montrons que notre approche multi-sauts pour la communication fiable permet un gain de performance significatif, c'est à dire qu'un pourcentage plus élevé de nœuds est en mesure de communiquer fiablement.

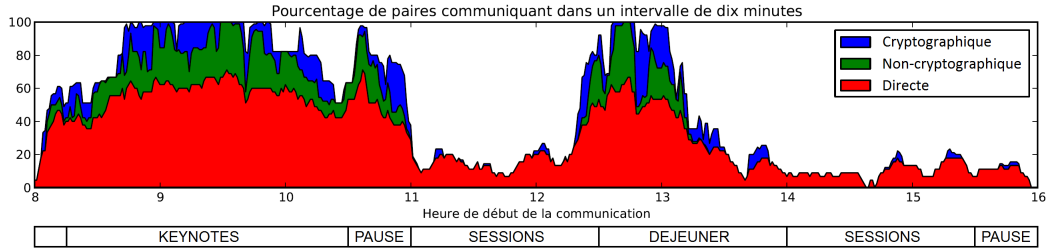

FIGURE 2: Communication fiable entre 10 nœuds lors de la conférence Infocom 2005.

Sur la Figure 2, nous avons représenté le pourcentage de paires (p,q) qui communiquent dans un intervalle de dix minutes, en fonction de l'heure de début de la communication. On peut corréler les pics de la figure avec le programme de la conférence : la première période correspond aux arrivées du matin pendant les keynotes, le pic entre 10h30 et 11h correspond à la première pause, et le pic débutant à 12h30 correspond à la fin des sessions parallèles et aux départs pour le déjeuner.

On observe en particulier que de nombreuses paires de nœuds qui ne se rencontrent pas directement parviennent néanmoins à communiquer fiablement, avec ou sans usage d'une infrastructure cryptographique. A 9h15, par exemple, 60% des paires de nœuds se rencontrent directement, 80% communiquent fiablement sans cryptographie (la coupe minimale dynamique est strictement supérieure à 2 dans l'intervalle considéré), et 100% communiquent fiablement avec cryptographie (la coupe minimale dynamique est strictement supérieure à 1 dans l'intervalle considéré).

Agents mobiles dans le métro parisien On considère un réseau de 10 agents mobiles se déplaçant dans le métro parisien. Les agents utilisent les lignes 1 à 14 pour se déplacer. Chaque agent est initialement situé à une station de jonction choisie aléatoirement (c'est à dire, une station connectant au moins deux lignes). Puis, il choisit aléatoirement une station de jonction voisine, attend le prochain train, se rend à cette station et répète le procédé. On utilise les horaires de trains fournis à `http://data.ratp.fr`. On considère que deux agents peuvent communiquer dans les cas suivants :

- Il se trouvent simultanément à la même station.
- Ils se croisent : Par exemple, si a un instant donné, un agent se déplace de la station A à la station B, alors que l'autre se déplace de la station B à la station A, on considère qu'ils peuvent communiquer.

En prenant pour point de départ l'horaire du premier métro, le temps moyen avant qu'une communication directe survienne entre deux agents (et leur permette ainsi de communiquer fiablement) est de 131 minutes. En utilisant notre approche multisaut, il est possible par exemple, pour tolérer un agent Byzantin, de réduire le temps de communication de 36% sans cryptographie, et de 49% avec cryptographie. Des résultats complémentaires sont présentés dans le papier complet [MDT15].

4 Conclusion

Dans ce papier, nous avons donné une condition nécessaire et suffisante pour communiquer fiablement dans un réseau dynamique sujet à des fautes Byzantines, et montré l'intérêt de notre approche multi-sauts sur plusieurs exemples.

Nous avons ici considéré le placement au pire cas de k nœuds Byzantins (ce qui est l'approche usuelle pour étudier les fautes Byzantines). Pour aller plus loin, un problème intéressant serait de trouver la condition de communication fiable pour un *placement* donné de nœuds Byzantins. Cela permettrait, par exemple, de déterminer précisément la probabilité de communication entre deux nœuds, dans le cas d'une distribution aléatoire et uniforme de fautes Byzantines.

Références

[BGH01] T. Böhme, F. Göring, and J. Harant. Menger's theorem. *Journal of Graph Theory*, 37(1) :35–36, 2001.

[CFQS12] Arnaud Casteigts, Paola Flocchini, Walter Quattrociocchi, and Nicola Santoro. Time-varying graphs and dynamic networks. *International Journal of Parallel, Emergent and Distributed Systems*, 27(5) :387–408, 2012.

[CHC+07] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott. Impact of human mobility on opportunistic forwarding algorithms. *TMC*, 6(6) :606–620, 2007.

[Dol82] D. Dolev. The Byzantine generals strike again. *Journal of Algorithms*, 3(1) :14–30, 1982.

[KKK02] David Kempe, Jon Kleinberg, and Amit Kumar. Connectivity and inference problems for temporal networks. *Journal of Computer and System Sciences*, 64(4) :820–842, 2002.

[LSP82] Leslie Lamport, Robert E. Shostak, and Marshall C. Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4(3) :382–401, 1982.

[MDT15] Alexandre Maurer, Xavier Defago, and Sébastien Tixeuil. Reliable communication in a dynamic network in the presence of byzantine faults. Technical report, http ://hal.upmc.fr/hal-00940569, 2015.

[NT09] Mikhail Nesterenko and Sébastien Tixeuil. Discovering network topology in the presence of byzantine nodes. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 20(12) :1777–1789, December 2009.