Cahier des charges PRO – 2018 Groupe 2 B

Odeep

Tables des matières

1. Description générale du projet

Odeep - *Original Decentralized Encrypted Exchange Protocol* - est une application de partage de fichiers chiffrés dans un réseau *Friend-to-Friend (F2F)*. Le réseau *F2F* est un modèle particulier de réseau *Peer-to-Peer (P2P)*. Le *P2P* est un réseau qui n'utilise pas forcément le schéma client-serveur. En effet, chacun des utilisateurs joue, ici, le rôle de client et de serveur. Les machines connectées composent le réseau *P2P* et sont nommées *"pair" ou "nœud"*. Un nœud est directement connecté à des dizaines, voire des centaines d'autres nœuds.

La force du réseau *P2P* est qu'il peut fonctionner sans serveur centralisé et que les ressources partagées entre les *"pairs"* peuvent être de natures très différentes : fichiers stockés, puissance de calcul processeur, messages et communication…

Odeep fonctionne dans un réseau *F2F.* À la différence du *P2P*, le réseau d'Odeep ne permet pas une communication entre utilisateurs inconnus, mais utilise une notion de groupe, où tous les utilisateurs se connaissent et se font confiance. Les communications ne peuvent avoir lieu qu'entre les membres d'un même groupe. Un utilisateur ne faisant pas partie d'un groupe ne peut obtenir aucune information sur celui-ci, ce qui assure l'anonymat des membres au sein du réseau. Un groupe est basé sur la confiance entre ses membres et est vivant tant qu'il en possède au moins un.

2. Les utilisateurs et leurs droits

Odeep peut être utile à toute personne soucieuse de partager des informations de manière sécurisée avec un groupe de personnes de confiance.

Néanmoins, tous ses membres possèdent les mêmes droits : il n'existe pas de notion d'administrateur au sein des groupes.

3. Description des fonctionnalités offertes

L'utilisateur a la possibilité de créer un groupe dans lequel il peut ensuite inviter d'autres personnes.

Un membre d'un groupe peut inviter un ami à le rejoindre. Ce dernier doit accepter l'invitation avant de devenir membre du groupe à son tour.

Un utilisateur peut quitter un groupe. Celui-ci n'aura plus accès aux fichiers partagés ni à la liste des membres du groupe. Il ne pourra plus rejoindre le groupe sans invitation.

Un membre d'un groupe peut choisir quel(s) fichier(s) il veut partager et rendre disponible à l'ensemble du groupe.

Un utilisateur pourra supprimer un fichier partagé au sein du groupe.

Un utilisateur pourra télécharger un fichier disponible au sein du groupe qui sera obtenu à partir des membres possédant le fichier.

4. Fonctionnalités facultatives

- Amélioration de la distribution des ressources lors d'un partage de fichier. Tous les utilisateurs possédant une copie locale du fichier contribuent à l'envoi du fichier.
- Chiffrement des fichiers de configurations des groupes pour une meilleure sécurité
- Gérer les connexions UDP
- Suppression d'un membre du groupe
- Amélioration des créations de groupes et ajout de personnes
- *Drag and Drop* pour l'ajout de fichiers aux groupes
- Affichage d'une barre de progression du téléchargement
- Différentes informations sur le téléchargement courant

5. Description de l'environnement de développement envisagé

Le langage de programmation utilisé est *Java*. Dans le cadre de ce projet, c'est la version 8 de *Java* qui a été retenue. Ce choix est motivé par la disparition de la librairie *sun.misc.Unsafe* dans *Java* 9. Cette dernière étant présente dans de nombreux projets *open source* potentiellement utilisables.

L'application n'utilisera pas de base de données. Des fichiers de configuration seront partagés entre les utilisateurs au lieu d'avoir un serveur centralisé les stockant.

L'interface graphique sera réalisée à l'aide de *JavaFX.* Cette librairie est le successeur de swing et offre donc plus de fonctionnalités que son prédécesseur. De plus, *JavaFX* est contenu dans le *JDK* ce qui règle des problèmes de portabilité qui pourrait se poser.

La librairie *Bouncy Castle* sera utilisée afin de réaliser les opérations cryptographiques.

Les fichiers de configurations des groupes seront au format XML.

Les schémas UML seront réalisés avec StarUML.

6. Principe de fonctionnement et mise en œuvre de l'application

Mise en place du protocole P2P

La première étape consiste à implémenter un protocole P2P basique sur lequel le partage de fichiers se basera.

Toute machine connectée au réseau est un *"pair"*. Un *pair* attend constamment une connexion entrante. Différentes actions de l'utilisateur pourront engager une connexion : *Illustration figure 1.*

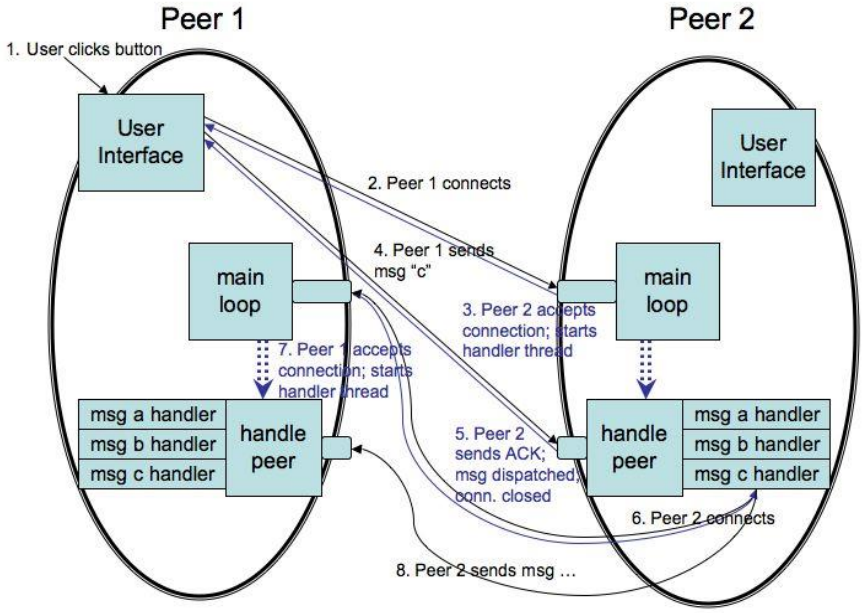


Figure 1 - source : http://cs.berry.edu/~nhamid/P2P

Chacun des *pairs* possède une interface graphique. (1) Lorsqu'un *pair* 1 clique sur un bouton (action quelconque), (2) une demande de connexion est envoyée au *pair* 2. La boucle principale de l'application est infinie et attend une connexion depuis l'extérieur. Lors de la réception d'une demande de connexion, (3) cette boucle principale choisit de l'accepter (envoi d'un paquet ACK) ou non et crée un *thread* qui pour gérer le futur message reçu du *pair* 1. (4) Le *pair* 1 envoie son message au *pair* 2. Le *thread* ("*handle peer*") du *pair* 2 se charge de gérer le message reçu. (5) Ce *thread* envoie un paquet ACK pour confirmer la réception du message. Il transmet ensuite ce message à la bonne fonction de gestion en fonction du type du message. (6) La fonction établit une connexion avec le *pair* 1 (via sa boucle principale), si elle le juge nécessaire. (7) Le *pair* 1 accepte la connexion et crée un *thread* afin qu'il puisse (8) recevoir le message du *pair* 2.

Partage de fichier

Une fois le framework P2P disponible, le système de partage de fichier sera implémenté. Celui-ci permettra d'envoyer des fichiers entre les *pairs* utilisant le réseau. Le gestionnaire de nœud pourra traiter les différents messages gérés par l'application et lancer des actions concrètes.

Chiffrement/authentification

Le chiffrement sera effectué à l'aide de la librairie Bouncy Castle.

La suite cryptographique sera *ECDH_RSA_HMAC* with SHA3.

Chaque groupe possédera sa propre clé symétrique, établi entre les deux premiers nœuds du groupe, à l'aide du protocole *ECDH*.

La clé symétrique sera ensuite répliquée vers les autres nœuds et permettra le chiffrement des fichiers en utilisant *AES-256*.

Une signature *HMAC* sera également envoyée avec chaque paquet pour vérifier son intégrité.

La fonction HMAC utilisée correspond à la fonction standard, à savoir :

$$HMAC_k(m) = h((K \oplus opad) \,||\, h((K \oplus ipad) \,||\, m))$$

avec :

K : la clé symétrique du groupe

ipad = 0x363636……3636, le nombre de 36 correspondant à la taille d'un bloc

opad = 0x5C5C5…….5C5C, le nombre de 5C correspondant à la taille d'un bloc

|| : correspond à la concaténation

⊕ : correspond au OU exclusif

h() : correspond à la fonction de hachage, dans notre cas *SHA3*.

Passer au F2F

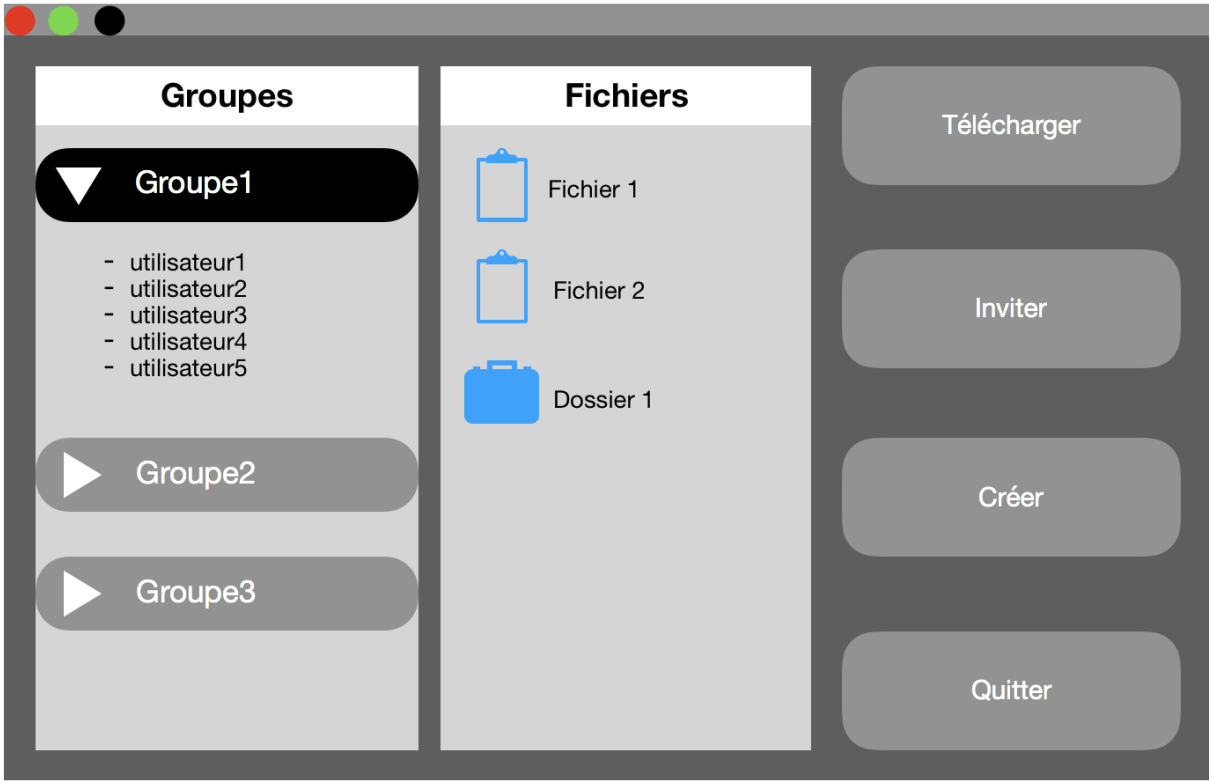
Afin de réaliser cette partie, l'application intégrera la notion de groupe. Tous les utilisateurs auront un fichier de configuration par groupe, regroupant les informations nécessaires (les pairs en faisant partie, les fichiers disponibles dans chaque nœud). Ce fichier sera sauvegardé chez chaque utilisateur dans le dossier de partage du groupe.

Afin de gérer les groupes, les actions suivantes seront implémentées :

- Créer un groupe
- Inviter à rejoindre un groupe

- Quitter un groupe (broadcast à tous les membres du groupe)
- Ajouter/supprimer un fichier pour le groupe

7. Mockup



La fenêtre se divise en plusieurs parties :

Nous avons une partie Groupes qui contient les groupes dont l'utilisateur fait partie. En sélectionnant un groupe, il est possible de voir les utilisateurs autorisés à partager des dossiers/fichiers entre eux.

Dans la partie Fichiers, nous avons les dossiers/fichiers disponibles qu'il est possible de télécharger dans le groupe choisi.

Il y a 4 boutons différents, le premier "Télécharger" permet de lancer le téléchargement du fichier/dossier choisi. Le bouton "Inviter" permet à une personne d'un groupe d'inviter une personne non membre. "Créer" permet de créer un nouveau groupe. Finalement, le bouton "Quitter" permet de mettre à jour les fichiers/dossiers disponibles pour les autres membres du groupe et quitter proprement l'application. En effet, il se peut qu'un fichier ne soit présent que sur une machine, il sera donc indisponible si la personne n'est pas connectée.

Pour la gestion des invitations, nous avons choisi d'utiliser un pop-up quand une invitation est reçue. La personne devra alors choisir si, oui ou non, elle rejoindra le groupe.