Nouvelle approche pour sécuriser un agent mobile

Amrani ayoub, Rafalia Najat, Abouchabaka Jaafar

Résumé— Le système multi-agent (MAS) apparaît comme une solution pour satisfaire l'exigence d'intelligence dans un système distribué. Ce paradigme accepte également la distribution et la mise en réseau comme concept de base. MAS est un système qui dispose d'un agent capable d'agir de manière autonome avec un comportement intelligent et de résoudre des problèmes complexes. La mobilité est une propriété de l'agent qui lui permet de passer d'un nœud à un autre pour atteindre son objectif. Des chercheurs de différents domaines ont été attirés par les systèmes basés sur l'agent mobile, en raison des aspects proactifs et des tâches autonomes de l'agent. Malheureusement, la sécurité des agents mobiles est très difficile, en particulier lorsqu'il s'agit de sécuriser une entité migrant d'une plateforme à une autre sur le réseau et qui doit être exécutée correctement et en toute sécurité sur la plateforme d'hébergement. Dans cet article, nous allons nous concentrer sur l'aspect sécurité d'un agent mobile d'une plate-forme à l'autre, en introduisant une nouvelle approche basée sur des mécanismes cryptographiques. Cette approche implique l'Amrani et al. Protocole pour obtenir une clé de session, afin de garantir une authentification mutuelle et la confidentialité des données échangées, après nous appliquons une sérialisation binaire pour assurer la mobilité de l'agent sur le réseau.

Mots-clés— Sécurité, Courbe elliptique, Système multi agent, agent mobile; authentification mutuelle.

———————— ◆ ————————

1 INTRODUCTION

Les systèmes multi-agents sont un ensemble d'agents, qui interagissent les uns avec les autres, situés dans un environnement commun, avec un comportement intelligent, et capables d'atteindre un certain objectif. Les agents peuvent aider les dispositifs à prendre des décisions autonomes et réduire la quantité de communication entre les plates-formes. La mobilité est l'une des capacités les plus importantes de cette technologie, qui permet à un agent transportant des informations (données ou code, etc.) de migrer d'une plate-forme à une autre [1].

Cependant, l'aspect de la mobilité peut poser des problèmes de sécurité majeurs, vu que l'agent transporte des informations très sensibles d'un nœud à un autre. L'agent peut être attaqué par des agents ou par une plateforme malveillante. Dans cet article, nous modéliserons un nouveau protocole de sécurité automatisé, basé sur un nouveau schéma d'authentification mutuelle ECC [2] et utilisant un système multi-agents, entre la plate-forme d'hébergement et la plate-forme de destination, afin de garantir la migration d'un agent mobile. Cette nouvelle approche permet de garantir l'authentification, la confidentialité et l'intégrité d'un agent lors de sa migration.

2 APPROCHE PROPOSE

2.1 Notion utilisé dans ce papier

Table 2. Illustre les notation utilise dans notre approche

NOTION	DESCRIPTION
ID_N	Identité de la platforme-native
ID_H	Identité de la platform d'hebergement
K_m	Clé principale aléatoire
K_i	Cle pour le dispositive i
R	Nombre aléatoire
Z_n	Groupe fini
P	Grand nombre premier $> 2^{160}$
N_1, N_2	Nombres aléatoires générés pour les paramètres ECC
G	Point générateur
H(.)	Fonction de hachage
K	Cle Mutual auth

Dans cette section, nous avons conçu un schéma d'authentification mutuelle qui a acquis l'expérience de [2] sur la base de courbes elliptiques et d'un système multi-agents. Dans cette section, nous allons détailler notre modèle MAS et expliquer le rôle de chaque agent utilisé. Notre modèle comprend trois phases: la phase d'initialisation, la phase d'enregistrement et enfin la phase de connexion et d'authentification.

2.2 Phase d'initialisation

Dans notre conception, c'est la plate-forme Destination qui est chargée d'initier les paramètres des paramètres nécessaires à la génération et à la distribution des clés, comme illustré à la figure 1.

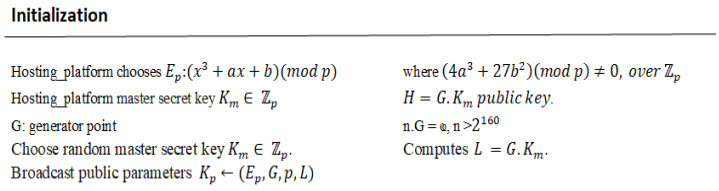

Figure 1 : la phase d'initialisation

2.3 Registration phase

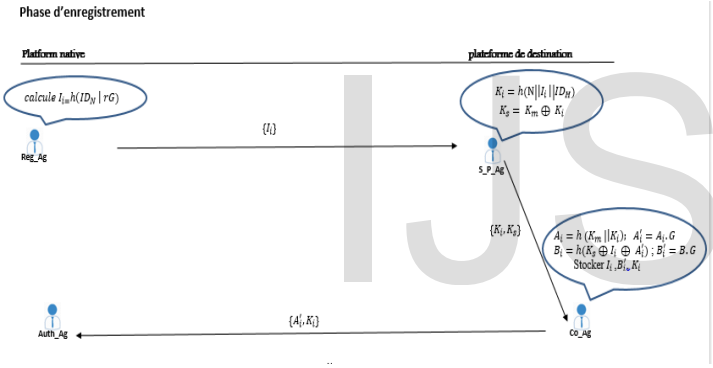

Figure 2 : la phase d'enregistrement

2.4 Phase de Login & Authentification

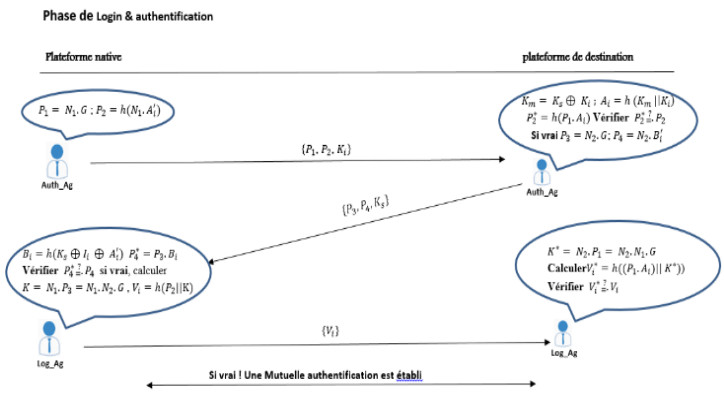

Figure 3 : la phase de Login & authentification

3. Conclusion

Dans cet article, nous avons détaillé les défaillances et les besoins de sécurité requis par un environnement de migration d'agent mobile. Nous avons également mentionné quelques travaux dans la littérature qui ont essayé avec différents protocoles de sécuriser un agent mobile sur plusieurs plates-formes. Nous avons ensuite résumé les conditions préalables de la courbe elliptique nécessaire pour développer un protocole d'authentification mutuelle. Tout en soulignant l'utilité et les avantages que les systèmes multi-agents peuvent apporter dans un environnement aussi intelligent, nous avons proposé une approche assurant, dans un premier temps, l'authentification mutuelle basée sur la courbe elliptique, à l'aide d'un système multi-agents, et migration sécurisée pour un agent sur plusieurs plates-formes. En tant que travail futur, nous allons essayer de mettre en œuvre notre approche en utilisant la plate-forme JADE [3] avec les spécifications FIPA [8] pour obtenir un résultat exact, puis comparer nos résultats avec ceux d'autres.

References

[1]
[2] Jacques Ferber. Multi-agent systems: an introduction to distributed artificial intelligence. Addison-Wesley.
[3] Amrani Ayoub, Rafalia Najat, and Abouchabaka Jaafar. LIGHTWEIGHT SECURE SCHEME FOR IOT-CLOUD CONVERGENCE BASED ON ELLIPTIC CURVE. (1):12, 2018.
[4] A. Rimassa G Bellifemine, F. Poggi. a _pa 2000 compliant agent evelopment environment. pages 216 | -217, 2001.
[5] Deok-gyu lee, seo-il kang, dae-hee seo, im-yeong lee: Authentication for sin gle/multi domain in ubiquitous computing using attribute certi_cation. Iccsa (4) 2006.
[6] Nicolae Constantinescu and Claudiu Ionut Popirlan. Authentication model based on multi-agent system. pages 11,2011.
[7] Sanae Hanaoui. On the security communication and migration in mobile agent systems. pages 12,2019.
[8] B. hancock, security views, computer & security. 18(7) (1999) 553-564.