Solution multi-agents basé sur Diffie-Hellman à courbe elliptique pour la communication sécurisée d'agent mobile

Yousra Berguig, Jalal Laassiri, Sanae Hanaoui

Résumé— Le système d'agent mobile est un nouveau paradigme, très utilisé dans les systèmes distribués, il aide à résoudre des problèmes complexes. Les agents mobiles sont autonomes, intelligents, robustes et tolérants aux pannes. Ils ont la capacité de migrer d'un nœud à un autre via le réseau, ce qui permet de réduire les coûts de communication. Malgré cela, leur utilisation dans des systèmes distribués augmente le risque pour la sécurité des agents mobiles. Dans un premier temps, ce document discute la sécurité du système d'agent mobile distribué. Nous proposons ensuite notre solution basée sur l'échange de clés Diffie-Hellman à courbe elliptique et la sérialisation binaire afin de sécuriser la communication d'agent mobile dans les environnements distribués.

Mots-clés— Agent mobile, Sécurité, Diffie-Hellman, Cryptographie à courbe elliptique (ECC), Sérialisation binaire.

1 INTRODUCTION

Récemment, avec l'évolution des systèmes intelligents et autonomes, les agents mobiles sont largement utilisés dans de nombreuses applications. Il s'agit d'un nouveau moyen de communication par rapport à l'environnement réseau hétérogène offrant de nombreux avantages. Cette technologie devient un domaine de recherche très attractif. Cependant, les problèmes de sécurité, d'infrastructure et de normalisation constituent toujours des contraintes importantes. Dans cet article, nous proposons une nouvelle solution pour sécuriser la communication d'agent mobile en utilisant un protocole d'échange de clé Elliptic Curve Diffie-Hellman [2] et une sérialisation binaire. Le reste du document est organisé comme suit. Dans la section 2, nous étudions la problématique de la sécurité dans les agents mobiles. Dans la section 3, nous présentons un aperçu de la cryptographie à courbe elliptique et Diffie-Hellman. Dans la section 4, nous proposons et discutons notre solution basée sur le protocole d'échange de clés Diffie-Hellman Elliptic Curve et la sérialisation binaire, afin d'assurer une communication sécurisée entre agents mobiles. Enfin, la section 6 conclut le document.

2 SECURITE DES AGENTS MOBILES

Pendant la mobilité, les menaces pesant sur la sécurité des agents mobiles sont classées dans quatre cas [3, 4]. Le premier concerne les menaces d'agent à agent, lorsqu'un agent mobile malveillant a tendance à attaquer un autre agent; tels que mascarade, déni de service, répudiation et accès non autorisé [5]. Le second est constitué par les menaces d'agent à plateforme, lorsqu'un agent mobile devient une menace pour la plateforme de destination. Ici, l'agent mobile est malveillant et peut lancer une attaque sur la plateforme d'exécution. Les attaques telles que le masquage, le déni de service et les accès non autorisés relèvent de cette caractéristique [5]. Menaces entre plates-formes lorsque la plate-forme d'exécution compromet la sécurité de l'agent mobile. Cela inclut des attaques telles que le masquage, le déni de service, les écoutes et les altérations [5].

3 DIFFIE-HELLMAN ET COURBES ELLIPTIQUES

3.2. Cryptographie a courbe elliptique

As ECC est un algorithme asymétrique, une alternative à RSA qui est le plus utilisé pour les certificats SSL [1]. Ces deux crypto-systèmes partagent la même propriété importante d'avoir une clé à chiffrer et une autre clé à déchiffrer. Cependant, ECC peut offrir le même niveau de puissance de cryptage pour des clés beaucoup plus courtes, offrant une meilleure sécurité tout en réduisant les besoins en informatique. Les clés courtes font de l'ECC une option très intéressante et attrayante pour les appareils avec une capacité de stockage et de traitement limitée.

3.2. Protocole d'échange de clé Diffie-Hellman à courbe elliptique utilisé

Dans le protocole utilisé, deux parties en communication, Alice et Bob, conviennent d'utiliser une courbe elliptique Ep (a, b) où p est un nombre premier et un générateur G de Ep (a, b). Alice et Bob choisissent respectivement un nombre aléatoire α <ord (G) et β <ord (G), ainsi qu'un point A et B sur la courbe elliptique comme clés secrètes. H et I sont les clés publiques. U est la clé publique spécifique d'Alice pour Bob. V est la clé publique spécifique de Bob pour Alice [2]. Comme le montre la figure 1.

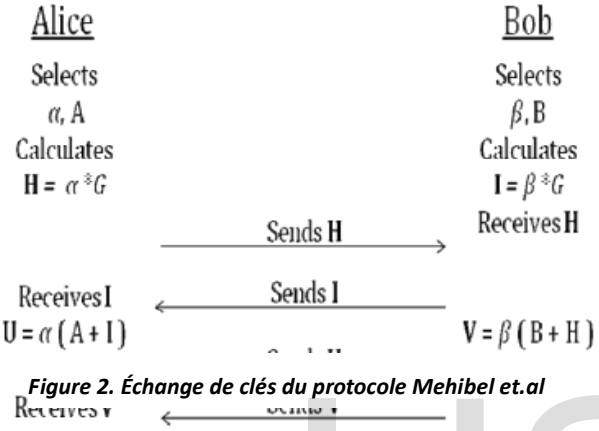

Figure 2. Échange de clés du protocole Mehibel et.al

4.SOLUTION PROPOSEE

Notre objectif principal dans ce travail est de sécuriser la communication d'agent mobile entre deux entités. Pour cela, nous adoptons une architecture multi-agents afin d'automatiser notre solution et de la rendre intelligente, robuste et autonome.

La figure 2 présente tous les agents qui interagissent les uns avec les autres pour former un système de sécurité coopératif.

1.Private-Key-Agent-A sélectionne (α, A) où α est respectivement un nombre aléatoire α <ord (G) et un point de la courbe elliptique. Puis envoie (α, A) à Public-Key-Agent-A.

2. Private-Key-Agent-B sélectionne (β, B) où α est respectivement un nombre aléatoire β <ord (G) et un point B sur la courbe elliptique. Puis envoie (β, B) à Public-Key-Agent-B.

3. Public-Key-Agent-A calcule (H = α * G) et envoie (H) à Public-Key-Agent-B.

4. Public-Key-Agent-B calcule (I = β * G) et envoie (I) à Public-Key-Agent-A.

5. Specific-Public-Key-Agent-A calcule U = α (A + I) et envoie (U) à Specific-Public-Key-Agent-B.

6. Specific-Public-Key-Agent-B Calcule U = β (B + H) et envoie (V) à Specific-Public-Key-Agent-A.

7. Key-Agent-A choisit S (x, y) comme point aléatoire sur la courbe elliptique, chiffre (s) en calculant = S + U + bb et envoie à Key-Agent-B, qui le stocke la base de données de la plateforme B.

8. Sérialisation-Agent-A sérialisez (Agent) et envoyez le résultat à Encryption-Agent-A.

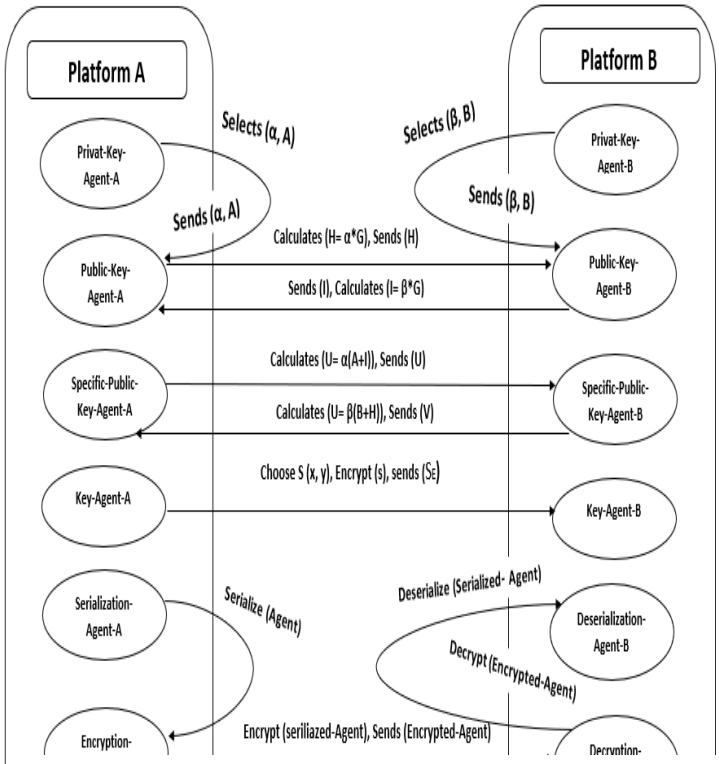

Figure 1 système multi-agent baser sur Diffie-Hellman à courbe elliptique pour la sécurité des agents mobiles

9. Encryption-Agent-A chiffre (seriliazed-Agent) en calculant C = S + et envoie (C) Decryption-Agent-B.

10. Decryption-Agent-B Décryptez C en calculant SAG = C - S = S + SAG - S. et envoyez à Deserialization-Agent-B.

11. Deserialization-Agent-B deserilize SAG pour obtenir l'agent.

5.CONCLUSION

Cet article discute la sécurité des agents mobiles tout en évaluant l'impact de cette technologie sur les systèmes distribués. Il présente également la cryptographie à courbe elliptique et du protocole Diffie-hellman. Nous avons étudié de nombreuses approches et méthodes pour proposer notre solution qui garantis une communication d'agent mobile sécurisé, nous avons appliqué l'échange sécurisé de clés publiques et de clés publiques spécifique sen se basant sur le protocole de Diffie-Hellman à courbe elliptique et les systèmes multi-agents. Dans les prochains travaux , nous allons implémenter la solution proposée dans ce travail et la comparer d'autres solution cryptographique pour la sécurité des communications de l'agent mobile.

REFERENCES

[1] ALFRED, J. MENEZES, PAUL C. VAN OORSCHOT, SCOTT A. VANSTONE. HANDBOOK OF APPLIED CRYPTOGRAPHY. CRC PRESS, 1996.

[2] N. MEHIBEL, M. HAMADOUCHE. A NEW APPROACH OF ELLIPTIC CURVE DIFFIEHELLMAN KEY EXCHANGE, THE 5TH INTERNATIONAL CONFERENCE ON ELECTRICAL ENGINEERING, 2017

[3] J.J. ADRI JOVIN, M. MARIKKANNAN. A REVIEW ON ATTACKS AND SECURITY APPROACHES IN MOBILE AGENT TECHNOLOGY. AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES, 2016.

[4] M.H. SHAO, J. ZHOU. PROTECTING MOBILE-AGENT DATA COLLECTION AGAINST BLOCKING ATTACKS. COMPUTER STANDARDS & INTERFACES, 2006.

[5] G. CARL, G. KESIDIS, RR. BROOKS, S. RAI. DENIAL-OF-SERVICE ATTACK DETECTION TECHNIQUES TRANS INTERN COMPUT 10(1):82–89, 2006.