MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE DJILLALI LIABES SIDI BEL ABBES

FACULTE DE TECHNOLOGIE

RESUME DE THESE DE DOCTORAT

Nom & Prénom(s)	GHARIB Hadj
E-mail (obligatoire)	gharib@univ-sba.dz
Spécialité	Electronique
Titre	Architecture d'authentification pour assurer la mobilité et la qualité de service dans les réseaux sans fil
Date de soutenance	24/11/2014
Nom, prénom(s) et grade de l'encadreur	BELLOULATA Kamel (Professeur)

Résumé :
L'objectif de cette thèse est de fournir une nouvelle architecture d'authentification adaptée aux réseaux sans fil et plus particulièrement les réseaux Ad hoc. Nous utilisons pour cela un schéma basé sur le protocole d'authentification KERBEROS amélioré par la division de la partie TGS à l'aide d'une cryptographie à seuil sur des courbes elliptiques. Notre proposition a permet d'éviter le point de défaillance unique habituellement trouvé dans les schémas de base de KERBEROS. Les contributions présentées se concentrent sur les axes suivants : Tout d'abord, c'est la première fois qu'un schéma d'authentification combine à la fois le protocole d'authentification KERBEROS avec un TGS distribué à l'aide du schéma de seuil d'ELGAMAL sur des courbes elliptiques.

Le second axe a été consacré à la modélisation de la sécurité en tant que paramètre dans la qualité de service pour cela, nous avons proposé une méthode basée sur l'optimisation multi-objectifs qui a permet de quantifier la qualité de service (QoS) par rapport aux déférents niveaux de sécurité.

Mots clés :

Authentification, Ad hoc, Kerberos, cryptographie à seuil, courbes elliptiques

---

Abstract
The objective of this thesis is to provide new authentication architecture adapted to wireless networks especially Ad hoc networks. For this we use a model based on the KERBEROS authentication protocol improved the divisions of the TGS party to the KDC scheme using threshold cryptography on elliptic curves. Our proposal avoids single point of failure usually Locate in the KDC database schemas. The papers presented will focus on the following areas:
First, this is the first time an authentication scheme combines the KERBEROS authentication protocol with TGS distributed with the threshold ElGamal scheme on elliptic curves.
The second axis is devoted to modeling of security as a parameter in the quality of service. for this, we have proposed a method based on multi-objective optimization which allows to quantify the quality of service (QoS) by compared to deferent levels of security.

Keywords: Authentication, Ad hoc, Kerberos, threshold cryptography, elliptic curves

---

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE DJILLALI LIABES SIDI BEL ABBES

FACULTE DE TECHNOLOGIE

RESUME DE THESE DE DOCTORAT

ملخص

الهدف من هذه الأطروحة هو توفير مصادقة جديدة البنيان تتكيف مع الشبكات اللاسلكية وخاصة الشبكات العشوائية .
لهذا إستخدمنا نموذج يستند إلى بروتوكول المصادقة تحسين الانقسامات الطرف TGS لمخطط قاعدة البيانات KDC باستخدام التشفير بعتبة على المنحنيات الإهليلجية.

يتجنب اقتراحنا نقطة الفشل الواحدة التي عادة ما تحدث في مخططات قاعدة البيانات KDC
الأطروحة المقدمة تركز على المجالات التالية:

أولا، هذه هي المرة الأولى التي يجمع نظام مصادقة بروتوكول المصادقة Kerberos مع توزيع TGS مع مخطط تشفير الجمل بعتبة على المنحنيات الإهليلجية .
ويخصص المحور الثاني لنمذجة الأمن كمعامل في جودة الخدمة لهذا، اقترحنا طريقة تقوم على التحسين المتعدد الأهداف الذي يسمح لقياس كم جودة الخدمة (QoS) من خلال مقارنتها بمستويات الأمن.

الكلمات المفتاحية :
التوثيق، kerberos، عتبة الترميز، المنحنيات الإهليلجية، الشبكات العشوائية