

République Algérienne Démocratique et Populaire  
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa  
Faculté des Sciences et des Sciences de l'Ingénieur

Département d'Informatique  
Ecole Doctorale Réseaux et Systèmes Distribués

## *Mémoire de Magistère*

En Informatique

Option

Réseaux et Systèmes Distribués

Thème

---

# Sécurité de Routage

---

Présenté par

Abdelaziz BABAKHOUYA

Devant le jury composé de :

Pr M. Ahmed Nacer	Président	USTHB, Alger, Algérie
Pr N. Badache	Examineur	USTHB, Alger, Algérie
MC F. Naït Abdesselam	Examineur	USTL, Lille, France
Pr A. Bouabdallah	Directeur de Thèse	UTC, Compiègne, France
Dr Y. Challal	Invité	UTC, Compiègne, France

Promotion 2004 – 2005

## Résumé

Les protocoles de routage assurent la connectivité du réseau et maintiennent des routes afin que les données envoyées par une source puissent atteindre leurs destinations. Les protocoles de routage utilisés actuellement dans l'Internet, comme BGP, OSPF et RIP sont conçus pour opérer dans un environnement sain sans routeurs malicieux. Cependant, avec la croissance importante de l'Internet, un nombre important d'entreprises et services publics sont devenus dépendants de bon fonctionnement de ces protocoles. De ce fait, la sécurisation des protocoles de routage revête d'une importance primordiale.

Nous présentons dans ce mémoire une étude sur la sécurité des protocoles de routage. A partir de cette étude, nous avons constaté la difficulté de sécuriser ces protocoles sans compromettre leurs performances et leur efficacité. Même la simple introduction de mécanismes cryptographiques ne peut pas palier à toutes les attaques possibles sur ces protocoles. Pour cela, nous avons proposé une nouvelle approche appelée S-DV "*Secure Distance Vector Routing Protocols*" permettant de sécuriser les protocoles de routage à base de vecteur de distance. En effet, S-DV favorise le choix d'un chemin plus sûr par rapport à un chemin plus court qui a été sujet à des attaques fréquentes. Ceci est rendu possible via une métrique qui mesure le niveau de sécurité associé à un chemin qui passe par un routeur voisin. Nous avons également proposé un nouveau mécanisme appelé DR "*Distance Request, Distance Reply*" permettant de vérifier la cohérence d'une annonce de route envoyée par un routeur voisin. Notre analyse montre l'efficacité de notre approche à détecter tout type d'annonce mensongère avec un coût très réduit.

**Mots-clés** : Sécurité, Routage, Authentification, Contrôle de Cohérence.

## Abstract

Routing protocols ensure the network connectivity, they maintain routes so that the data sent by a source can reach their destinations. Routing protocols used actually in the Internet, like BGP, OSPF and RIP were designed to operate in a safe environment without malicious routers. Although, with the importance growth of the Internet, a significant number of companies and public services became dependent on its correct operation. So that, securing routing protocols becomes of critical importance.

In this report we review routing protocols security. From this study, we conclude that it is very difficult to secure such routing protocols without compromising their performance and efficiency. The simple introduction of cryptographical mechanisms cannot prevent from all the possible attacks on these protocols. For this reason, we proposed a new approach called S-DV "*Secure Distance Vector Routing Protocols*". S-DV prefers the choice of a secure route than a shortest one which was subject to frequent attacks. This became possible with new metrics that measure the security level associated to a route that passes through a neighbor routers. We proposed also a new mechanism called DR "*Distance Request, Distance Reply*" to check the coherence of an advertised route received from a neighbor router. Our analysis shows the efficiency of our approach to detect all types of misbehaving advertisements with low cost.

**Keywords** : Security, Routing, Authentification, Coherence Check.

# Table des matières

Glossaire	i
Table des matières	ii
Liste des figures	v
Liste des tableaux	vi
Liste des algorithmes	vii
Introduction Générale	1
<b>1 Protocoles de routage dans l'Internet</b>	<b>4</b>
1.1 Introduction	4
1.2 Protocole de routage interne	5
1.2.1 Protocole de routage à base de vecteur de distance	5
1.2.2 RIP ( <i>Routing Information Protocol</i> )	9
1.2.3 Protocole de routage à état des liens	10
1.2.4 OSPF ( <i>Open Shortest Path First</i> )	11
1.3 Protocole de routage externe	12
1.3.1 Protocole de routage à base de Path vector	12
1.3.2 BGP ( <i>Border Gateway Protocol</i> )	13
1.4 Synthèse et comparaison	14
1.5 Conclusion	15
<b>2 Cryptographie et Sécurité</b>	<b>16</b>
2.1 Introduction	16
2.2 Confidentialité	16
2.2.1 Chiffrement symétrique	17
2.2.2 Chiffrement asymétrique	17
2.3 Intégrité des données	18
2.3.1 Fonction de hachage	19
2.3.2 Fonctions de hachage usuelles	19
2.4 Authentification de l'origine des données	20
2.4.1 MAC	20
2.5 Non répudiation avec preuve de l'origine des données	21
2.5.1 La signature digitale	22

2.5.2	Certificat à clé publique . . . . .	23
2.6	Conclusion . . . . .	24
<b>3</b>	<b>Attaques sur les protocoles de routage</b>	<b>25</b>
3.1	Introduction . . . . .	25
3.2	Analyse des protocoles de routage . . . . .	26
3.3	Vulnérabilités liés aux protocoles de routage . . . . .	28
3.3.1	Attaques externes . . . . .	28
3.3.2	Attaques internes . . . . .	28
3.4	Techniques utilisées pour une attaque . . . . .	29
3.4.1	Interception (IP Sniffing) . . . . .	30
3.4.2	IP Spoofing . . . . .	30
3.4.3	Falsification . . . . .	30
3.4.4	Rejoue . . . . .	30
3.4.5	Fausse annonce de préfixe d'origine . . . . .	31
3.4.6	Fausse annonce de la distance ou du chemin . . . . .	31
3.5	Conséquences d'une attaque . . . . .	31
3.5.1	Blackhole . . . . .	31
3.5.2	Gryhole . . . . .	32
3.5.3	Déni de Service . . . . .	32
3.6	Conclusion . . . . .	32
<b>4</b>	<b>Contre-mesures</b>	<b>33</b>
4.1	Introduction . . . . .	33
4.2	Prévention contre des attaques externes . . . . .	34
4.2.1	Authentification à base de clé partagée . . . . .	35
4.2.2	Gestion des clés partagées . . . . .	36
4.2.3	Authentification à base de clé publique . . . . .	37
4.2.4	Vers un standard de sécurité IP (IPsec) . . . . .	39
4.3	Prévention contre des attaques internes . . . . .	40
4.3.1	Prévention contre une annonce mensongère de préfixe . . . . .	41
4.3.2	Prévention contre une annonce mensongère du chemin (S-BGP) . . . . .	42
4.3.2.1	Attestation d'Adresse (AA) . . . . .	43
4.3.2.2	Attestation de Route (RA) . . . . .	43
4.3.2.3	Description de protocole . . . . .	43
4.3.3	Prévention contre une annonce mensongère de la distance . . . . .	45
4.3.4	Contrôle de cohérence d'une annonce de route . . . . .	45
4.3.5	S-RIP . . . . .	47
4.3.5.1	Prévention contre une information de routage non authentique . . . . .	47
4.3.5.2	Prévention contre une annonce mensongère de préfixe . . . . .	48
4.3.5.3	Prévention contre une annonce mensongère de la distance . . . . .	48
4.3.5.4	Réputation des routeurs . . . . .	49
4.3.5.5	Overhead généré par S-RIP et discussion . . . . .	49
4.4	Conclusion . . . . .	52

<b>5</b>	<b>S-DV : Secure Distance Vector Routing Protocols</b>	<b>53</b>
5.1	Motivation . . . . .	53
5.2	Modèle du réseau . . . . .	54
5.3	Généralités sur S-DV . . . . .	55
5.4	Les services de sécurité assurés par S-DV . . . . .	55
5.4.1	Prévention contre une information de routage non authentique . . .	56
5.4.2	Prévention contre une annonce mensongère de préfixe . . . . .	56
5.4.3	Prévention contre une annonce mensongère de la distance . . . . .	57
5.5	S-DV . . . . .	59
5.5.1	Informations de routage . . . . .	59
5.5.2	Lancement de S-DV . . . . .	61
5.5.3	Détails de S-DV . . . . .	63
5.6	Analyse des menaces . . . . .	67
5.6.1	Annonce mensongère de prédécesseur . . . . .	67
5.6.2	Suppression ou modification d'un message DR . . . . .	68
5.7	Conclusion . . . . .	68
<b>6</b>	<b>Mesures de performances de S-DV et Comparaison</b>	<b>69</b>
6.1	Introduction . . . . .	69
6.2	Mesure de l'overhead engendré par S-DV . . . . .	69
6.3	Comparaison . . . . .	72
6.4	Discussion . . . . .	73
6.5	Conclusion . . . . .	74
	<b>Conclusion générale</b>	<b>75</b>
	<b>Bibliographie</b>	<b>77</b>