

Architecture Hiérarchique Distribuée pour Sécuriser les Réseaux Ad hoc Mobiles

Abderrezak RACHEDI Abderrahim BENSLIMANE

LIA/CERI, Université d'Avignon
Agroparc, BP 1228
84911, Avignon, France

8ème Journées Doctorales en Informatique et Réseaux, 17-19
Janvier 2007 Marne la Vallée



Plan

- 1 Problématique et Challenges
 - Problématique
 - Challenges
- 2 Motivation
- 3 Présentation de l'architecture
 - Modèle de confiance
 - Zone Dynamique Démilitarisée (DDMZ)
 - Algorithme distribué d'élection sécurisé (ADES)
- 4 Evaluation de performance : simulations
- 5 Conclusion et Perspectives

Plan

- 1 Problématique et Challenges
 - Problématique
 - Challenges
- 2 Motivation
- 3 Présentation de l'architecture
 - Modèle de confiance
 - Zone Dynamique Démilitarisée (DDMZ)
 - Algorithme distribué d'élection sécurisé (ADES)
- 4 Evaluation de performance : simulations
- 5 Conclusion et Perspectives

Problématique

Comment assurer la sécurité et la maintenir dans les réseaux Ad-Hoc mobiles ?

Plan

- 1 Problématique et Challenges
 - Problématique
 - Challenges
- 2 Motivation
- 3 Présentation de l'architecture
 - Modèle de confiance
 - Zone Dynamique Démilitarisée (DDMZ)
 - Algorithme distribué d'élection sécurisé (ADES)
- 4 Evaluation de performance : simulations
- 5 Conclusion et Perspectives

Challenges

- Réseau ouvert
- Topologie Dynamique du réseau
- Absence d'unité de contrôle centralisée
- Ressources limitées
- Environnement non sûr
- Hétérogénéité des nœuds

Motivation

Dans les réseaux Ad-Hoc mobiles certains nœuds sont :

- Confidents, coopératifs
- Malveillants, égoïstes
- Mobilité relative

Nous utilisons la diversité des niveaux de confiance et la mobilité parmi les nœuds pour sécuriser le réseau.

Le but

- Définir une architecture hiérarchique, basée sur la division du réseau sous forme de groupes (clusters), avec un seul chef par groupe.
- Générer une infrastructure à clé publique (PKI) dans chaque groupe et sécuriser la communication inter-groupes
- Election d'un nœud CA parmi les nœuds qui disposent du niveau de confiance le plus élevé et d'une certaine stabilité
- Maintenir le plus longtemps possible l'architecture

Plan

- 1 Problématique et Challenges
 - Problématique
 - Challenges
- 2 Motivation
- 3 Présentation de l'architecture
 - Modèle de confiance
 - Zone Dynamique Démilitarisée (DDMZ)
 - Algorithme distribué d'élection sécurisé (ADES)
- 4 Evaluation de performance : simulations
- 5 Conclusion et Perspectives

Modèle de confiance (1)

Definition

- Métrique de confiance (T_m) : valeur continue dans $[0 - 1]$
- Seuls les nœuds de confiance ont $T_m = 1$
- Chaque nœud dispose d'une table de confiance, qui sera actualisée a chaque changement de la T_m
- Chaque nœud inconnu commence avec $T_m = 0.1$ (le plus bas niveau de confiance)

Modèle de confiance (2)

Definition

Pour qu'un nœud obtienne la plus grande métrique de confiance ($Tm = 1$) soit :

- 1 Le nœud est connu par les nœuds de confiance et il a échangé une clé sous un canal sécurisé [4][5]
ou
- 2 Le nœud a prouvé sa total coopération (ré-acheminant les paquets, ... etc)

L'idée consiste à obliger les nœuds inconnus à coopérer et bien se comporter

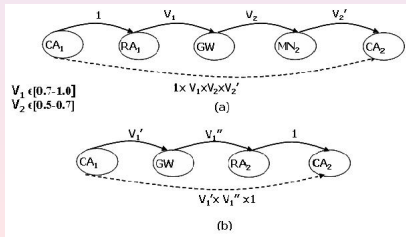
Modèle de confiance (3)

Nous définissons cinq types de rôle pour le nœud :

- **Autorité de Certification** du groupe (CA) avec $T_m = 1$
- **Autorité d'enregistrement** du groupe (RA) avec $T_m = 1$
- **Passerelle** entre deux groupes (GW) avec $T_m \in [0.7 - 1.0]$
- **Membres** (MN) ce sont les nœuds qui appartiennent au groupe et qui disposent de $T_m \in [0.5 - 0.7]$
- **Visiteur** (VN) avec $T_m \in [0.1 - 0.5]$

Chemin de confiance

- La valeur de confiance d'un chemin dépend de la chaîne de confiance de ce chemin.
- L'évaluation de la confiance entre deux nœuds consiste à prendre la valeur minimum entre les deux métriques de confiance.



Plan

- 1 Problématique et Challenges
 - Problématique
 - Challenges
- 2 Motivation
- 3 **Présentation de l'architecture**
 - Modèle de confiance
 - **Zone Dynamique Démilitarisée (DDMZ)**
 - Algorithme distribué d'élection sécurisé (ADES)
- 4 Evaluation de performance : simulations
- 5 Conclusion et Perspectives

Zone Dynamique Démilitarisée

Definition

- C'est l'ensemble des nœuds de confiance à un seul saut du nœud CA
 - Chaque nœud joue le rôle de l'autorité d'enregistrement (RA)
- Le rôle de ces nœuds est de protéger le nœud CA contre les nœuds qui possèdent un faible niveau de confiance

Plan

- 1 Problématique et Challenges
 - Problématique
 - Challenges
- 2 Motivation
- 3 Présentation de l'architecture**
 - Modèle de confiance
 - Zone Dynamique Démilitarisée (DDMZ)
 - Algorithme distribué d'élection sécurisé (ADES)
- 4 Evaluation de performance : simulations
- 5 Conclusion et Perspectives

Algorithme distribué d'élection sécurisé (1/5)

Règles principales de ADES

- Seuls les nœuds de confiance ($Tm(i) = 1$) peuvent devenir candidats au rôle de CA
- Chaque chef de groupe (cluster-head) est le CA d'un seul groupe
- Tous les nœuds de confiance voisins au nœud CA peuvent devenir RA dans le groupe
- Les nœuds qui appartiennent au groupe sont à d sauts de distance maximale du nœud CA

Algorithme distribué d'élection sécurisé (2/5)

Critères de sélection du nœud CA

- 1 **Sécurité** : Pour augmenter le niveau de sécurité dans le groupe, l'algorithme (ADES) sélectionne le nœud de confiance ($T_m = 1$) qui dispose d'au moins un nœud voisin de confiance
- 2 **Stabilité** : Est basée sur la métrique de mobilité [1]. Cette métrique donne une bonne connaissance de la mobilité relative entre deux nœuds voisins

Algorithme distribué d'élection sécurisé (3/5)

Chaque nœud candidat au rôle CA commence d'envoyer un paquet d'élection qui contient les informations suivantes :

- L'identité du nœud au rôle de CA
- Degré de voisins de confiance (DTN)
- Mobilité relative (RM) par rapport au voisins de confiance
- Nombre de saut vers le nœud candidat (Hop-Count)
- Numéro de séquence du paquet d'élection
- "Message Authenticated Code" (MAC) du paquet

$$(MAC_{K-}[CA, Hop - count, DTN, RM, Sq - num])$$

Algorithme distribué d'élection sécurisé (4/5)

Algorithm 1: Algorithme d'élection

```

Quand le nœud (j) reçoit un paquet balise du nœud (i);
begin
  Authentication do If ( $Tm(i) \neq 1$ ) then
    RejectBeacon(); Goto(end);
  else if ( $HopCount \geq d$ ) then
    | No - Competition; Goto(end);
  else if ( $RM_i < RM_j$ ) OR ( $(RM_i == RM_j)$  AND
( $DTN_j < DTN_i$ )) then
    Accepter le nœud (i) comme CA;
    if ( $HopCount == 1$ ) then
      |  $Status(j) = RA$ ;
      |  $HopCount(i) = 1$ ;
    else
      |  $HopCount(i) = HopCount + 1$ ;
      |  $Status(j) = MN$ ;
  else if ( $RM_j < RM_i$ ) OR ( $DTN_j > DTN_i$ ) then
    | Le nœud (j) rest candidat au CA;
  else if ( $RM_i == RM_j$ ) AND ( $DTN_j == DTN_i$ )
  then
    | Exécuter Lowest-ID ;
end

```

Algorithme distribué d'élection sécurisé (5/5)

Algorithm 2: Algorithme exécuté par le nœud si ses RA ou CA ne sont plus disponibles

Si le nœud (i) ne reçoit pas de paquet balise de CA après certain temps pré-définie;

begin

if *Il peut atteindre CA avec un autre RA* **then**

 Garder le CA actuel;

 Mettre à jour le nœud RA et *Hopcount*;

else if *Il peut trouver un autre CA* **then**

 Joindre le nouveau CA;

if ($Tm(i) == 1$) **then**

if ($HopCount == 1$) **then**

$Status(i) = RA_NODE$;

$HopCount(newCA) = 1$;

else

$Status(i) = MN$;

$HopCount(newCA) = HopCount + 1$;

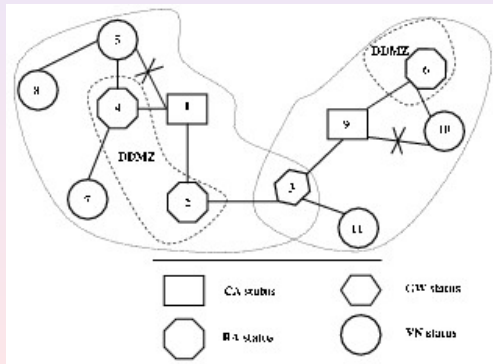
else

 Demande de certification au nœud RA;

end

Exemple

Le cas de 2 sauts de taille de groupe



Modèle de simulation et scénarios

Pour comparer l'algorithme ADES avec d'autre algorithmes de clusterisation comme MOBIC [1] et Lowest-ID [2].

Pour cette raison, nous utilisons le simulateur réseau ns-2 avec les même scénarios.

Parameter	Valeurs
Nombre des nœuds (N)	50
Taille de la surface (mxn)	670x670m ²
Vitesse de mobilité	20 m/sec
Portée de transmission	10 m - 250 m
Interval de diffusion (BI)	0.75-1.25 s
Interval de découverte	10*BI s
Période de contention	3.0 s
Temps de simulation	300 s

Résultats de simulations (1)

Stability

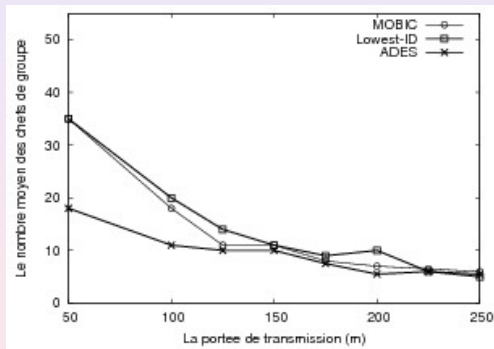


FIG.: Comparison entre les algorithmes de clusterisation ADES, MOBIC and Lowest-ID

Résultats de simulations (2)

Sécurité et robustesse

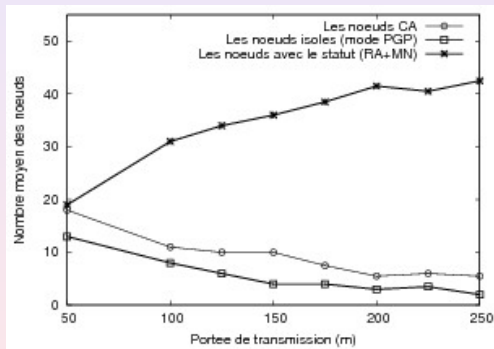


FIG.: Nombre moyen de différents status des noeuds

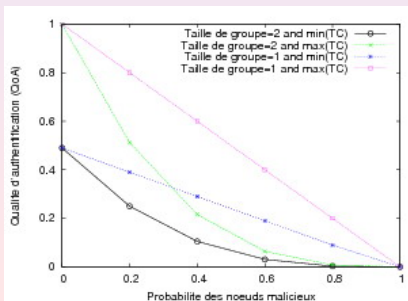
Résultats de simulations (2)

Qualité d'authentification

Dans le but d'évaluer la confiance d'authentification au niveau des nœuds CA, nous calculons la qualité d'authentification (QoA) [3].

$$QoA(V_1 - V_2) = TC(V_1 - V_2) * (1 - p)^{(d-1)} \quad (1)$$

d : la longueur de la chaîne de confiance.



Analyse de Sécurité (1)

- La sécurité de notre architecture dépend du modèle de confiance adopté.
- La présence d'un grand nombre de nœuds de confiance augmente la sécurité du réseau.
- Toutes les communications venant des nœuds ou des groupes malicieux sont ignorées.
- Les attaques de type déni de service (DoS) sont évitées par la DDMZ. (Les nœuds RA filtrent toutes les requêtes venant des nœuds inconnus).
- La robustesse de la DDMZ dépend du nombre de nœuds RA qui collaborent entre eux pour protéger le nœud CA.

Analyse de Sécurité (2)

- Les nœuds malicieux peuvent utiliser l'identité des nœuds légitimes uniquement si leur clé privée est divulguée.
- Si un attaquant tente de compromettre tout le réseau, il doit compromettre tous les nœuds CAs.
- La taille du groupe doit être adaptée au nombre de nœuds de confiance pour bien sécuriser le nœud CA (un compromis entre les nœuds de confiance et les nœuds inconnus doit être trouvé).
- La présence de deux nœuds de confiance est une configuration minimale pour former un groupe.
- Nous pouvons utiliser la cryptographie à seuil dans chaque groupe une fois le CA sélectionné.

Conclusion et Perspectives





Conclusion

- Nous avons proposé une nouvelle architecture hiérarchique pour distribuer l'autorité de certification (CA).
- Combinaison entre la sécurité et la stabilité pour former les groupes dans le but de sécuriser le réseau.
- Introduction du concept de la DDMZ pour éviter les attaques contre les nœuds CA.
- Cette architecture est adaptée au changement de topologie.

Perspectives

- Étudier la DDMZ face aux différentes attaques de type DoS.
- Évaluer et analyser l'architecture avec différents modèles de mobilité.

Références

-  1) P. Basu and N. Khan and T. Little.
A mobility based metric for clustering in MANET.
*In Proceedings of Distributed Computing Systems
Workshop*, :43–51, 2001.
-  2) M. Gerla and J. T.-C. Tsai.
Multicluster, Mobile Multimedia Radio Networks.
Wireless Networks. (1995) 255–256
-  3) S. Yi and R. Kravets.
Quality of Authentication in Ad Hoc Networks.
ACM, MobiCom2004. (2004)
-  4) S. Capkun and J. P. Hubaux and L. Buttyan.
Mobility Helps Peer-to-Peer Security.
IEEE Transactions on Mobile Computing: 5 (2006) 48–60