UNIVERSITE ELHADJ LAKHDER - BATNA
FACULTE DES SCIENCES DE L'INGENIEUR
DEPARTEMENT D'INFORMATIQUE

Mémoire

présenté en vue de l'obtention du diplôme

Magister en Informatique

Option: Ingénierie des systèmes informatiques (ISI)

Présenté et soutenu publiquement par :

Noureddine CHAIB

Titre :

La sécurité des communications dans les réseaux VANET

JURY

M. Abdelmadjid ZIDANI	Président	Maître de conférences, université de Batna.
M. Mohamed BENMOHAMED	Examinateur	Professeur, université de Constantine.
M. Azzedine BILAMI	Examinateur	Maître de conférences, université de Batna.
M. Mohamed YAGOUBI	Rapporteur	Maître de conférences, université de Laghouat.
M. Nasreddine LAGRAA	Invité	Maître de conférences, université de Laghouat.

Table des matières

Résumé

Dans les prochaines années à venir, les réseaux véhiculaires seront capables de réduire significativement le nombre d'accidents via les messages d'alerte échangés entre les véhicules de proximité. La fonction de routage est un élément fondamental pour le système de communication véhiculaire ; par conséquent, il constituera une cible idéale pour les attaques qui pourrait viser à empêcher des messages d'alerte à atteindre leurs destinations, et mettre ainsi en danger les vies humaines. Malheureusement, les protocoles de routage basés seulement sur des techniques cryptographiques ne peuvent pas garantir la sécurité contre tous les attaques et particulièrement les attaques provenant de l'interne. Parmi les solutions qui répond à la contrainte temps réel des applications des VANET, l'utilisation d'un protocole de révocation distribuée conjointement avec un protocole de routage sécurisé afin de détecter et éliminer les nœuds malveillants rapidement. Cependant, la plupart des protocoles proposés sont vulnérables aux attaques de fausses alertes émises par plusieurs nœuds malveillants en coalition afin d'exclure un grand nombre de nœuds honnêtes. Dans ce travail, nous proposons un nouveau protocole de révocation distribuée SEDIREP (SEcure DIstributed REvocation Protocol) destiné aux réseaux VANET, il permet aux nœuds d'un réseau VANET d'éviter d'utiliser les nœuds malveillants comme relais pour l'acheminement des messages liés à la sécurité. Les résultats de simulation montrent que SEDIREP assure un taux de détection élevé et un faible taux de faux positifs même en présence d'un nombre élevé d'attaquants.

Mots clés: Révocation distribuée, Routage sécurisé, SDI, VANET

Abstract

In the next few years, vehicular networks will be able to reduce significantly the number of accidents by way of warning messages exchanged among nearby vehicles. The routing function is a building block for the vehicular communication system, so it will be an ideal target for attacks that could aim to prevent alert messages from reaching their destinations, thus endangering human lives. Unfortunately, routing protocols based only on cryptographic techniques cannot guarantee security against all attacks, especially insider attacks. Among the solutions that meet the real time constraint of VANET applications, using a distributed revocation protocol together with a secure routing protocol to detect and avoid malicious nodes quickly. However, most proposed systems are vulnerable to false alerts issued by several colluding malicious nodes to exclude a large number of honest nodes. In this work, we propose a novel distributed revocation protocol SEDIREP (SEcure DIstributed REvocation Protocol) for VANETs, it allows nodes in a VANET network to avoid using malicious nodes as relays for transmitting safety related messages. The simulation results show that SEDIREP provides a high detection rate and low false positive rate even in the presence of a large number of attackers.

Keywords: Distributed revocation, Secure routing, IDS, VANET