1. **Record Nr.**   UNISOBSOBE00064844

   Autore   *Commissione *europea

   Titolo   6: Glossary of 300 concepts and technical terms / European Commission

   Pubbl/distr/stampa   Luxembourg, : Office for Official Publications of the European Communities, 1999

   Descrizione fisica   135 p. ; 21 cm

   Lingua di pubblicazione   Inglese

   Formato   Materiale a stampa

   Livello bibliografico   Monografia

2. **Record Nr.**   UNINA9910437587303321

   Autore   Du Suguo

   Titolo   Security assessment in vehicular networks / / Suguo Du, Haojin Zhu

   Pubbl/distr/stampa   New York : , : Springer, , 2013

   ISBN   1-4614-9357-9

   Edizione   [1st ed. 2013.]

   Descrizione fisica   1 online resource (xi, 49 pages) : illustrations (some color)

   Collana   SpringerBriefs in Computer Science, , 2191-5768

   Disciplina   58

   Soggetti   Vehicular ad hoc networks (Computer networks) - Security measures
   Computer science
   Data protection
   Data encryption (Computer science)
   Telecommunication

   Lingua di pubblicazione   Inglese

   Formato   Materiale a stampa

   Livello bibliografico   Monografia

   Note generali   "ISSN: 2191-5768."

   Nota di bibliografia   Includes bibliographical references and index.

   Nota di contenuto   Introduction to Vehicular Networks Security -- Security Assessment via Attack Tree Model -- Attack-Defense Tree Based Security Assessment -- A VANETs Attack-Defense Game -- Modelling of Multiple Phased Attack on VANET Security.

Sommario/riassunto   This book presents several novel approaches to model the interaction between the attacker and the defender and assess the security of Vehicular Ad Hoc Networks (VANETs). The first security assessment approach is based on the attack tree security assessment model, which leverages tree based methods to analyze the risk of the system and identify the possible attacking strategies the adversaries may launch. To further capture the interaction between the attacker and the defender, the authors propose to utilize the attack-defense tree model to express the potential countermeasures which could mitigate the system. By considering rational participants that aim to maximize their payoff function, the brief describes a game-theoretic analysis approach to investigate the possible strategies that the security administrator and the attacker could adopt. A phased attack-defense game allows the reader to model the interactions between the attacker and defender for VANET security assessment. The brief offers a variety of methods for assessing the security of wireless networks. Professionals and researchers working on the defense of VANETs will find this material valuable.