

Preface

Vehicular Networks, or Vehicular Ad-hoc Networks (VANETs), is regarded as a promising approach for future intelligent transportation system, and enables a wide range of safety and Infotainment applications. From the safety perspective, the introduction of VANETS greatly increases the safety of passengers by exchanging safety relevant information. From the Infotainment perspective, it exploits the Vehicle-to-vehicle communications and Vehicle-to-Road Side Unit communications to allow ubiquitous Internet Access, Video Streaming, Location-based Service, Content Distribution and Traffic Monitoring. The security and privacy is more than critical for the success of vehicular networks.

This book is designed to introduce some methods such as attack tree, attack-defense tree and attack-defense game from a system view for analyzing the vehicular network security and privacy problems. The existing research on VANETs security and privacy mainly focuses on the preventive techniques. From a system point of view, it lacks a comprehensive yet well-defined security evaluation to allow the system administrator to identify the most critical security threats and thus determine the appropriate defense strategy, which are more than important for the overall success of VANETs deployment. The existing risk analysis schemes include attack tree, attack graph or defense tree based solutions. However, there are several research challenges which make the existing security analysis solutions cannot work well for security and privacy evaluation in VANETs. Firstly, for VANETs security, the defense strategy is directly correlated to the attack strategy and vice versa, which means that the security evaluation should consider both of attack and the defense side rather than any single one. Secondly, most of the existing security solutions only consider how to prevent an attack while fail to consider the costs and gains of the attacker and the defender. In reality, a rational attacker or defender may try to maximize its attack or defense benefits instead of blindly launching an attack or adopting a countermeasure. Lastly, but no less importantly, how to model the mutual interaction between the attacker and defender remains a great challenge for VANETs security evaluation.

This book presents several novel approaches to model the interaction between the attacker and the defender and assess the security of the considered VANETs. The first security assessment approach presented in this book is based on attack tree

security assessment model, which leverages tree based method to model and analysis the risk of the system and identify the possible attacking strategies the adversaries may launch. With the help of the attack tree model, it is convenient to analyze the capability of the attack source and estimate the degree or the impact a certain threat might bring to the system.

To further capture the interaction between the attacker and the defender, we further propose to utilize the attack-defense tree model to express the potential countermeasures which could be used to mitigate the system. The difference between an attack tree and an attack-defense tree is that the front only represents the attack strategies that attackers can launch, while the latter includes the set of countermeasures which can mitigate the possible damages produced by the attackers.

By considering rational participants that aim to maximize their payoff function, we propose a game-theoretic analysis approach to investigate the possible strategies that the security administrator and the attacker could adopt. On one side the VANETs security administrator wants to protect the security of the vehicular networks by adopting countermeasures to thwart the attacks; on the other side, the attacker wants to exploit the vulnerabilities and obtain some profit by attacking the vehicular networks. However, they cannot maximum their utility at the same time because one's action that aims to increase its own benefits will reduce its adversary's utility. Under this setting, we discuss the potential strategies of the defender and the attacker by modeling it as an attack-defense game. We then give a detailed analysis on its Nash Equilibrium.

Since many real world systems operate in multiple phases and, for mission success, all phases must be completed without failure. In practice, the attack strategy will evaluate from simple attack to more advanced yet complicated attacks along with the evolution of the defense strategy. Therefore, defending the attack succeeds if and only if the defense of all of phases succeed. We introduce a phased attack-defense game to model the interactions between the attacker and defender for VANET security assessment.

This book can be used for graduate students who interest in network security and privacy research area in their first year's literatures reviewing phase. This book can be a reference reading material for management science or computer science graduate students. The main mathematical prerequisite are the rudiments of Boolean algebra and game theory.

Finally we would like to thank Mr. Xiaolong Li and Mr. Junbo Du for their devotion to this work.

Shanghai, People's Republic of China
August 2013

Suguo Du
Haojin Zhu



<http://www.springer.com/978-1-4614-9356-3>

Security Assessment in Vehicular Networks

Du, S.; Zhu, H.

2013, XI, 49 p. 9 illus., Softcover

ISBN: 978-1-4614-9356-3