Trust management for Vehicular Networks: An Adversary-Oriented Overview

摘要

> 两大重要防御方法
>
> - 密码学 Cryptography
> - Trust

1. Introduction

- 车载自主网络VANET安全很重要
- 网络安全靠Cryptograpy来保证
  - 证数、签名、公钥、指令检测系统、第三方插件
- 另一些场景：缺乏基础设施的高速移动场景，Cryptography方法表现并不好
  - 一个经过授权与验证的用户被恶意感染了
  - 信任管理Trust Management来补充这一不足
  - Trust可定义为：a subjective belief of a peer about other peers belonging to the same society or geographical zone
  - 信任管理主要源自于经济学
- VANET场景下
  - 信任评估基于历史的直接或间接交互行为
  - 由于基于历史数据计算，不存在延迟
- 信任模型分类
  - entity-oriented trust model
  - data-oriented trust model
  - hybird trust model
- 信任模型分类依据
  - depending on the revocation target
- 信任模型主要关注网络内部攻击 inside attack
- 文章阐述Trust对Cryptography何时更优、更差、或为补充

> 文章结构
>
> - 与车联网相关的Cryptography/Trust Management方法介绍(Section2)
> - 车联网的安全需求与对策(Section3)
> - Cryptography与Trust Management方法特点，区别(Section4)
> - 现有Trust Model性能评估(Section5)
> - 未来Trust Management方向(Section6)
>   - 重点关注哪些能够绕过现有信任模型的威胁
> - 总结(Section7)

2. Related Work

- 本文分类方法
  - Trust-based
  - Cryptography-based
  - combine both strategies

3. VANET安全需求与威胁

- 除了隐私问题外，可分为如下五个需求
  - 可用性 Availability(最重要)
  - 基于加密或信任的方法都允许在基础设施存在的情况下保护网络
  - 基于信任的方法，在分布式场景下是个更好的选择
  - 真实性 Authenticity
  - 包括identification, authentication, and access control
  - 只能通过加密方法来实现
  - 机密性 Confidentiality
  - 公钥传输
  - VANET场景下，safety messages与邻居发现信息仍需透明传输
  - 只能通过加密方法来实现
  - 完整性 integrity
  - 公钥+信任模型
  - 不可否认行 non-repudiation
  - 签名技术，只能通过加密方法来实现
  - 隐私性 Privacy
  - 包括Location与Identification
  - Pseudonym changing技术
- 威胁分类
  - Attacks addressing secure communications
  - certificate replication attack
    - 攻击者使用合法身份伪装自己，躲避检测
  - eavesdropping attack
    - APT(Advanced Persistent Threat)攻击，平日只窃听，不直接攻击
  - identity/location privacy attacks
  - Attacks addressing safety applications: 所有的安全应用都是基于多跳和延迟敏感的信息交换，此类攻击多与信道占用有关
  - Denial of Service attack
    - blocking all possible actions by the target
  - Jamming attack
    - 类似DoS,Target is the shared bandw idth
  - Coalition and platooning attack
  - Betrayal attack
    - 合法节点突然变为恶意节点
  - Attacks addressing infotainment applications: Infotainment applications are all those related to passengers' comfort, and most of them are based on relay selection strategies for message exchanges.
  - Replayed, altered, and injected messages attack
  - Illusion attack
  - Both secure communications and safety applications
  - Masquerading attack
  - Impersonation attack
  - Both secure communications and infotainment applications
  - Sybil attack
    - 类似僵尸攻击，攻击者控制若干个节点，发起恶意行为
  - GPS position faking attack
  - Both safety and infotainment applications
  - Timing attack
  - Blackhole attack
  - Grayhole attack