Artificial Intelligence and Game Theory Based Security Strategies and Application Cases for Internet of Vehicles

Zhiyong Wang[1], Miao Zhang[1], He Xu[3], Guoai Xu[1(✉)], Chengze Li[2(✉)], and Zhimin Wu[2(✉)]

[1] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China
xga@bupt.edu.cn
[2] National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT), Beijing, China
{lichengze,wuzhimin}@cert.org.cn
[3] University College London, London, UK

Abstract. Information security of Internet of Vehicles (IoV) has attracted much attention in recent years. In view of security vulnerabilities existed in automobiles, many countries launch guidelines and cybersecurity standards concerning IoV security and plenty of new techniques have been applied to combat threats. In this paper, a variety of attacks on IoV are summarized and classified, then artificial intelligence and game theory based security countermeasures for IoV are highlighted, and their protection mechanisms are illustrated. Finally, a few application cases of artificial intelligence and game theory based security strategies for IoV is analyzed, aiming to provide helpful reference for the development of IoV security techniques.

Keywords: Internet of vehicles (IoT) · Artificial intelligence(AI) · Game theory · Security · Application

1 Introduction

There are more than 1.2 billion motor vehicles across the globe now, and it is expected to hit two billion by 2035. It is estimated that over 125 million network connected automobiles will be manufactured between 2018 and 2022 [1]. In China, as of 2017, there were more than 17.8 million users of IoV [2]. IoV is regarded as a typical kind of Internet of Things (IoT), and it can ameliorate driving safety, provide convenience information and facilitate traffic management. IoV implements the communications between vehicles and public networks via vehicle-to-road (V2R), vehicle-to-human (V2H), vehicle-to-vehicle (V2V), and vehicle-to-sensor (V2S) interactions.

However, the rapid development of IoV raises concerns about security and privacy problems which can threaten driving safety and driver's lives and invade people's privacy. In 2015, security flaws of BMW vehicles equipped with connected drive were found to enable thieves to unlock doors and steal car data. Following this, more than 1.4 million of Chrysler cars in US were recalled due to network security problems [3].

Q. Liang et al. (Eds.): CSPS 2019, LNEE 571, pp. 322–329, 2020
https://doi.org/10.1007/978-981-13-9409-6_38

In 2016, US National Highway Traffic Safety Administration (NHTSA) launched "Cybersecurity Best Practices for Modern Vehicles", in which cybersecurity standards, principles, and best practices for car industry were described to improve the information security of vehicles. In 2017, "White Papers of Network Security of Internet of Vehicles" was published by China Academy of Information and Communications Technology (CAICT), aiming to promote the safe development of IoV.

Until now, plenty of security strategies have been put forward to ensure the security of IoV, such as encryption, intrusion detection system, secure routing protocols and key management. However, more effective and flexible methods need to be developed to meet the needs of the special features of IoV, including dynamic change of network topology, limited storage capacity and processing capacity of automobile terminal. Artificial intelligence can not only enhance the detection accuracy for threats, but also can find hidden risks by learning from data without explicit programming. Game theory is also an intelligent tool to analyze the interaction process between the attackers and defenders. In this article, we will discuss the structure of IoV, security threats and countermeasures for network security. Meanwhile, artificial intelligence (AI) and game theory based security scheme for IoV will be emphasized, and the application cases of IoV with AI and game theory will be analyzed accordingly.

2 Literature Survey

2.1 Structure of IoV

Vehicle system architecture can be hierarchically grouped into four layers in terms of security, namely, external communication layer (Level 1), vehicle gateway layer (Level 2), in-vehicle network layer (Level 3), and hardware layer (Level 4) (shown in Fig. 1) [4].

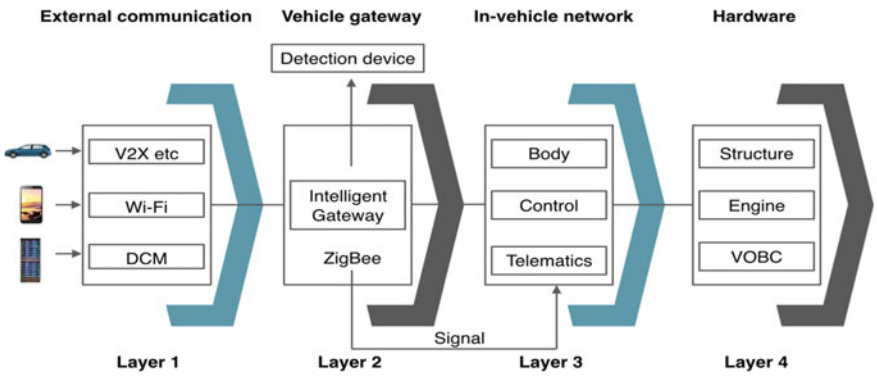

Fig. 1. Structure of IoV

External communication layer achieves the communications between vehicles and outside world by linking on-board communication equipment to V2X systems, Wi-Fi and mobile networks. Vehicle gateway layer regulate automotive systems in a vehicle like the headquarter, in which vehicle gateway connects internal ECUs (Electronic Control Units) to external communication equipment at Level 1 and controls message transfer in the in-vehicle networks. In-vehicle network layer is responsible for transmitting messages among ECUs, and it can be classified into multiple of network subunits in terms of ECU functions, such as body domain, control domain, and telematics domain. CAN (Controller Area Network) or LIN (Local Interconnect Network) is commonly used as communication protocols at this layer. Naturally, hardware layer is comprised of ECUs and various components that perform specific functions related to vehicle [4].

2.2 Attack Classification in IoV

Attacks can be mainly classified into five types in IoV: authentication attacks, attacks on availability, privacy attacks, attacks on routing and attacks of data authenticity. Attacks on authentication include Sybil attack, GPS camouflage, camouflage attack, and wormhole attack. With regard to availability attacks, interference on channel and service denial are two common attacks. Specially, the secrecy attacks steal customer data by interception or eavesdropping. With respect to routing attacks on routing, there are four attack types related to routing, including interception, camouflage, service denial and route modification. In regard to data authenticity attacks, they can be categorized into the masquerading attack, replay attack, illusion attack and information fabrication and falsification (shown in Fig. 2) [5].

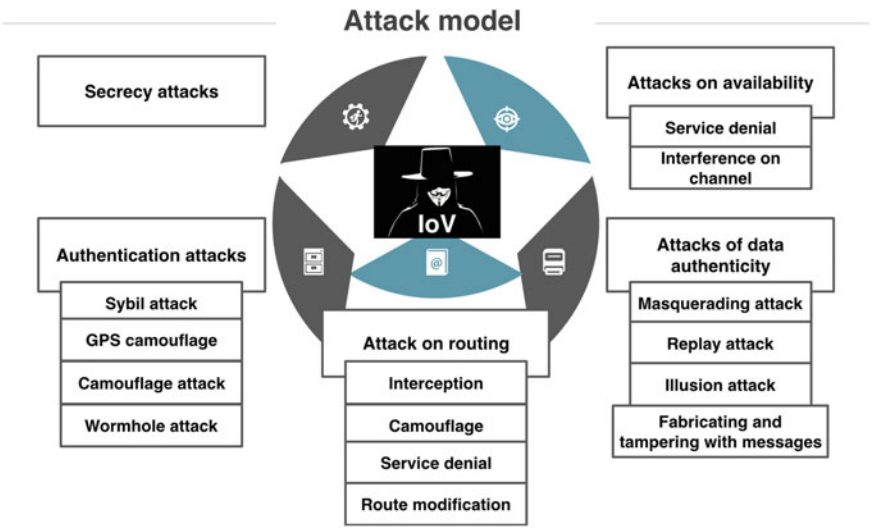

Fig. 2. Attack model

2.3 Countermeasures for IoV Security

A wide range of countermeasures have been proposed to prevent the threats on IoV according to special characteristics of IoV attacks, including establishing suitable model of threat, adopting honeypot system, constructing intrusion monitor system, employing privacy protection mechanism of routing, using reliable routing protocols and key management. With regard to threat model, constructing mathematical model and adopting graph-based methods are two main approaches for simulating threats. Intrusion detection system (IDS) can employ anomaly detection approach and signature detection method to hinder attacks through collecting and analyzing internal system's information. In addition, SVM-based security framework and protocol analysis can offer protection for IoV security as well. Honeypots can realize protection by tempting and hoaxing attackers' attention to avoid invading in vital system data in the context of IoV. Several secure routing protocols can not only perform normal routing functions, but also can restrain attacks on routing such as SAODV, Ariadne, and SRP protocol. Routing privacy protection mechanism contains a few of algorithms to guard against routine nodes data leakage, including SLPD, ALAR, and STAP. Key management is a crucial strategy for IoV security in that encryption is a significant method for information security, and successful encryption relies on suitable key management. Additionally, pseudonym signature and certificateless signature can also provide effective protection (shown in Fig. 3) [5].

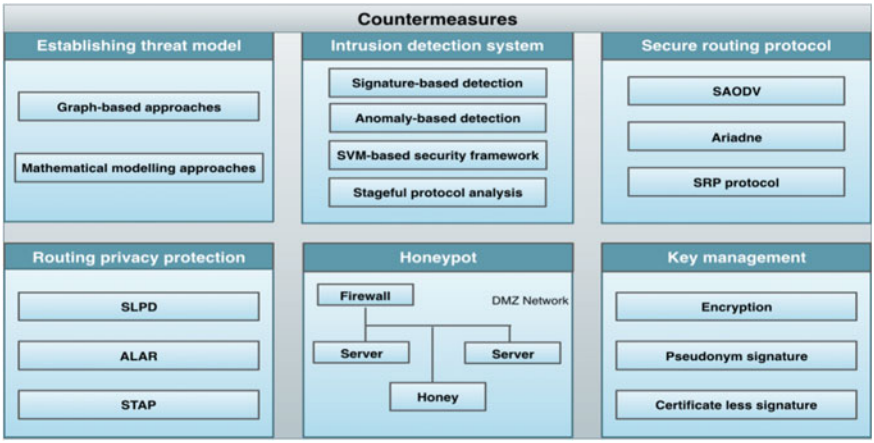

Fig. 3. Countermeasures for IoV security

2.4 Artificial Intelligence and Game Theory Based Security Strategies for IoV

Artificial intelligence (AI) is a kind of ability that a machine simulates human behavior intelligently and carries out specific tasks arranged by humans. Machine learning and deep learning are two main techniques to implement artificial intelligence. Some scholars argued that machine learning, deep learning and reinforcement learning can be

adopted to safeguard the information security in Internet of Things (IoT). For example, AI can build up real-time behavioral modeling for net nodes, servers and equipment, and reduce new malware attacks and APT malware (Phishing, Adware, Trojans, etc.) [6].

Machine learning can defend against threats on IoV via gathering and storing right data, the vehicle's internal network can be monitored by storing and analyzing logs, thereby detecting wicked threats and combating attacks. Once user logs are acquired, machine learning can check anomalies existed in the picture. Thus, machine learning can be able to analyze outside service data and information to detect unusual activities and malware attacks [7].

Loukas put forward a deep learning based intrusion detection approach to prevent cyber-physical attacks in IoV, which can enhance intrusion detection accuracy for vehicles compared with other deep learning and machine learning approaches [8]. Support Vector Machine (SVM) based detection system differentiates normal contents and anomalies by analyzing the training data of normal parts. Naturally, the input space is therefore classified into normal and abnormal parts [9]. Kang developed a Deep Belief Network (DBN) to detect intrusion for in-vehicle network, which ensure 97.8% accuracy and 1.6% false positive rate [10]. Vuong et al. adopted decision tree to search for command injection and denial of service threats on robotic vehicles, indicating the introduction of physical input characteristics can increase detection accuracy and eliminate the false positive rate [11].

Game theory is exploited to find out optimal choices when facing conflicts. It refers to the process which individuals or organizations select strategies from action sets to make best decisions in a specific context [12]. Of these, security games focus on the interaction between malicious attackers and defenders and it is applied to detect intrusion in IoV networks. For instance, Buchegger and Alpcan proposed two-player zero-sum game to generate solutions to security of IoV, in which they defined one player as attacker, and a group of mobile nodes as defender to imitate jamming and Sybil attacks in a vehicular network. The result showed the mobile nodes can improve their safeguard strategy by adopting zero-sum game approach [13].

In the aspect of understanding attack and defense comprehensively, game theory is proven to be an effective analysis tool. Alpan utilized game theory model based on noncooperation approach and provided Nash equilibrium analysis for lots of common network attack detection [14]. Chen mentioned abnormal network attack detection and provided mixed Nash equilibrium analysis [15]. Afterwards, Ismail [16] applied Chen's conclusion into privacy attack detection of ammeter infrastructure data. However, most of conclusions are based on assumption that attacker's identity is known already, and this assumption does not work due to high masquerading of attackers [14–16]. To resolve the unknown identity problem, some scholars employed Bayesian game theory to solve attack detection problem, whose rationale is based on credibility evaluation of attacker's previous behaviors and real-time update by Bayesian theory [17–25]. In terms of features of mobile wireless ad hoc networks of IoV, researchers performed a numbers of studies on intrusion node detection and node communication incentive [26, 27]. Additionally, game theory is also used for intrusion detection of industrial control including networked control system [28] and energy system [29]. Apart from this, game theory is also widely applied in numerous of fields [30–32].

2.5 Case Study of Artificial Intelligence and Game Theory Based Security Strategies for IoV

In the aspect of artificial intelligence, Kang et al. adopted deep neural network method to construct intrusion monitor system for security of IoV. In this system, parameters can be originated by utilizing deep belief networks as a pre-processing step. Following this, high-dimensional packet data can train neural networks to discriminate and analyze hacking and normal data's statistical properties and find out the relevant characteristics [33].

Regarding artificial intelligence's practical application, "learn and prevent" device was developed through machine learning by Miller and Valasek, aiming to detect intrusion in the vehicle. The device is essentially a NXP micro-controller, and its simple board can be plugged into the OBD-II port. It can collect the typical data patterns of vehicle in the beginning of driving as observation mode, and then it changes to detection mode to monitor unusual information. Once any attacks are found, the automobile will be switched into "limp mode" to interrupt the networks and suspend vital functions like steering, then prevention and alert mode will be stimulated when any anomalies are found. The prevention mode enables the vehicle to neglect the malicious attacks and attackers can be inhibited, while alert mode empowers the driver to take actions by sending messages.

With respect to game theory, Raya et al. designed a repudiation protocol for network security based on game theory method. Raya et al. presented three choices that each player can adopt according to the available protocols. Firstly, a player can give up the local repudiation step by choosing A due to mobile node's unwillingness of involving in repudiation step. Secondly, a player can use vote V to fight detected attacker by participating in local voting step. Finally, a player can perform invalidity procedure for attacker's identity and its own identity and commit suicide. By introducing dynamic game, researchers define mobile nodes as players to solve the repudiation problem.

Eventually, Raya et al. applied repudiation procedure based on gme theroy method to resolve practical problems. The protocol realizes quick and best repudiation process through motivating mobile nodes to be involved in repudiation process actively. Realistic simulation in IoV of this game theory method indicated a better tradeoff among various approaches [34].

3 Conclusions

A wealth of countermeasures based on different theory and new techniques have been employed to defend against threats for the security of IoV. Among them, artificial intelligence and game theory based security strategies can prevent IoV from wicked attacks effectively and securely. Along with the occurrence of more application cases based on aforementioned two methods, artificial intelligence and game theory based secure scheme can play a stronger and broader role in cybersecurity of IoV in the future.

With the rapid development of IoV and techniques, more malicious attacks will emerge and more effective techniques can be developed to fight against threats in the future. Given this, any single technique cannot guarantee the absolute security of IoV, thus combined application of multiple of effective techniques may be a better way to prevent from threats of IoV networks. Additionally, the advent of 5G era and the emergence of a great number of innovative and effective techniques definitely bring new methods for IoV security protection and automobile manufacture industry to ensure the safe driving and facilitate the establishment of smart cities.

Acknowledgements. This work is supported by the National Key Research and Development Program of China (Grant No.: 2018YFB0803605), the National Natural Science Foundation of China (Grant No.: 61897069), and the Foundation Strengthening Program for Key Basic Research of China (Grant No.: 2017-JCJQ-ZD-043). Guoai Xu, Chengze Li and Zhimin Wu are the corresponding authors.

References

1. Millman R (2018) Connected cars report: 125 million vehicles by 2022, 5G coming. In: Internet of business. https://internetofbusiness.com/worldwide-connected-car-market-to-top-125-million-by-2022/
2. Analysis of status development of internet of vehicles in China in 2018 (2018) In: RFID world. http://news.rfidworld.com.cn/2018_09/6746f0f84b2cd8cd.html
3. Takefuji Y (2018) Connected vehicle security vulnerabilities. IEEE Technol Soc Mag 37 (1):15–18
4. Tanaka M, Takahashi J, Oshima Y (2017) Cyber-attack countermeasures for cars. NTT Technical Rev 15(5):1–5
5. Sun YC, Wu L, Wu SZ, Li SP, Zhang T, Zhang L, Xu JF, Xiong YP, Cui XG (2017) Attacks and countermeasures in the internet of vehicles. Ann Telecommun 72:283–295
6. Lee GM Artificial intelligence (AI) for development series: report on AI and IoT in security aspects. ITU. 10
7. Causevic D How machine learning can enhance cybersecurity for autonomous cars. Total. https://www.toptal.com/insights/innovation/how-machine-learning-can-enhance-cybersecurity-for-autonomous-cars
8. Loukas G, Vuong T, Heartfield R, Sakellari G, Yoon Y, Gan D (2018) Cloud-based cyber-physical intrusion detection for vehicles using deep learning. IEEE Spec Sect Secur Anal Intell Cyber Phys Syst 6:3491–3508
9. Carlos A, Catania FB (2012) An autonomous labeling approach to support vector machines algorithms for network traffic anomaly detection. Expert Syst Appl 39(2):1822–1829
10. Kang MJ, Kang JW (2016) Intrusion detection system using deep neural network for in-vehicle network security. PLoS ONE 11(6):1–17
11. Vuong TP, Loukas G, Gan D (2015) Decision tree-based detection of denial of service and command injection attacks on robotic vehicles. IEEE Int Work Inf Forensics Secur 1–6
12. Liang XQ, Yan Z (2019) A survey on game theoretical methods in Human-Machine networks. Futur Gener Comput Syst 92:674–693
13. Buchegger S, Alpcan T (2008) Security games for vehicular networks. In: Proceedings of the 46th annual allerton conference on communication, control and computing, pp 244–251

14. Alpcan T, Basar T (2011).Network security: a decision and game-theoretic approach. Cambridge University Press
15. Chen L, Leneutre J (2009) A game theoretical framework on intrusion detection in heterogeneous networks. IEEE Trans Inf Forensics Secur 4(2):165–178
16. Ismail Z, Leneutre J, Bateman D, Chen L (2014) A game theoretical analysis of data confidentiality attacks on smart-grid AMI. IEEE J Sel Areas Commun 32(7):1486–1499
17. Liu Y, Comaniciu C, Man H (2006) A Bayesian game approach for intrusion detection in wireless ad hoc networks. In: ACM international conference proceeding series
18. Nguyen KC, Alpcan T, Basar T (2009) Security games with incomplete information. In: IEEE international conference on communications
19. Zhang Y, Tan XB (2011) Perception method of internet security based on Markov game theory model. J Softw 22(3):495–508
20. Hu H (2011) Strategy model of internet security based on Markov game theory. J Xi'an Jiaotong University 45(4):18–24
21. Fu Y (2009) Study on strategy selection of attacks and defenses of internet. J Beijing Univ Posts Telecommun 32(1):35–39
22. Zhu Q, Tembine H, Basar T (2010) Network security configurations: a nonzero-sum stochastic game approach. In: American control conference
23. Nguyen KC, Alpcan T, Basar T (2009) Stochastic games for security in networks with interdependent nodes. In: International conference on game theory for networks
24. Nguyen KC, Alpcan T, Basar T (2010) Security games with decision and observation errors. In: American control conference
25. Jiang W (2009) Security evaluation and optimal active defense based on game theory model. Chin J Comput 32(4):817–827
26. Sagduyu YE, Berry R, Ephremides A (2009) MAC games for distributed wireless network security with incomplete information of selfish and malicious user types. In: International conference on game theory for networks
27. Zhu Q, Fung C, Boutaba R, Basar T (2012) GUIDEX: a game-theoretic incentive-based mechanism for intrusion detection network. IEEE J Sel Areas Commun 30(11):2220–2230
28. Amin S, Schwartz GA, Sastry SS (2013) Security of interdependent and identical networked control system's. Automatica 49(1):186–192
29. Maharjan S, Zhu Q, Zhag Y, Gjessing S, Basar T (2012) Dependable demand response management in the smart grid: a Stackelberg game approach. IEEE Trans Smart Grid 61 (8):3693–3704
30. Manshaei M, Zhu Q, Alpcan T, Basar T, Hubaux JP (2013) Game theory meets network security and privacy. ACM Comput Surv 45(3):1–39
31. Roy S, Ellis C, Shiva S, Dasgupta D, Shandilya V, Wu Q (2010) A survey of game theory as applied to network security. In: Proceedings of the 43rd Hawaii international conference on system sciences
32. Liang X, Xiao Y (2013) Game theory for network security. IEEE Commun Surv Tutor 5 (1):472–486
33. Kang MJ, Kang JW (2016) A novel intrusion detection method using deep neural network for in-vehicle network security. Proc IEEE VTC Fall 1–5
34. Raya M, Manshaei MH, Felegyhazi M, Hubaux JP (2008) Revocation games in ephemeral networks. In: Proceedings of ACM conference on computer and communications security (CCS)