Advances in Intelligent Systems Research, volume 147
International Conference on Network, Communication, Computer Engineering (NCCE 2018)

Research on Communication Security of VCPS

Meifeng Xiao [a)] and Lichen Zhang [b)]

School of Computer, Guangdong University of Technology, Guangdong 510006, China

[a)] Corresponding author: 2441015805@qq.com
[b)] Zhanglichen1962@163.com

Abstract. VCPS (Vehicular Cyber Physical System) effectively improves road safety and improves driver's driving environment. However, due to the large scale of the VANET network, the predictability of the trajectory, and the open nature of the wireless channel, it is more vulnerable to privacy and security threats. This paper proposes security requirements for VCPS communication, security threats and trust-based security analysis.

Key words: VCPS; VANET; wireless channel; security analysis; trajectory.

INTRODUCTION

When the vehicle uses actual identities, security can be achieved through authentication, but in this case, privacy is a major issue because there is a direct correspondence between the identity of the vehicle and the identity of the driver or car rental person, an attacker may eavesdrop on broadcast messages in wireless channels and track malicious attacks such as vehicles by analyzing data and predicting trajectories [1, 2]. Therefore, VANET for VCPS needs to be able to guarantee security and protect privacy. In VANET, verifying the validity of a received message is challenging when the actual identity of the vehicle is not used to authenticate security. Trust is an important factor in VCPS security. When a fixed roadside infrastructure is used for VCPS communication, trust establishment and maintenance can take a long time, However, because of the dynamic topology change of VANET and the short life cycle of the network, trust management has become a challenging issue. When vehicles are in communication with each other, they can exchange information and communicate, however, when the vehicles are not within the communication range of each other, they will not be able to obtain the first-hand information of the vehicle through single-hop communication. In this case, the vehicle relies on the adjacent vehicles to receive messages through multiple hops. Therefore, in VCPS, if there is no suitable trust management mechanism, VCPS may be subject to malicious attacks that spread false information. VCPS security mechanisms should protect the network from malicious attacks while protecting the privacy of drivers and passengers [3].

VCPS SECURITY REQUIREMENTS

In VCPS, the main function of the vehicle as a terminal is perception, and a large number of electronic control unit ECUs, smart sensors, actuators and other electronic systems are installed inside the vehicle, making the vehicle itself an intelligent sensor network system. Vehicle communication is the pillar of VCPS. However, due to the dynamic topology of the network and the high-speed movement of the vehicle, the vehicle communication process is vulnerable to a series of security issues such as privacy leakage and location tracking. The VANET that ensures the security of VCPS should meet the following requirements:

•Authentication: The vehicle's reaction to events should be based on legitimate messages (that is, generated by legitimate senders). Therefore, we need to authenticate the sender of these messages.

• Verify the consistency of the data: The legitimacy of the message also includes the consistency with the messages generated at close range and adjacent times, because there are cases where the sender is legitimate and the message contains erroneous data. This requirement is sometimes called "rationality".

• Availability: Even assuming a strong communication channel, some attacks (for example, DoS caused by interference) can cause network interruption. Therefore, availability should support alternative methods.

• Non-repudiation: The driver who caused the accident is reliably identified; the sender cannot deny sending information.

• Privacy: Unauthorized driver privacy should be guaranteed.

• Real-time constraints: Vehicles travel at high speeds, network dynamic topology, connectivity may be disconnected in a short period of time, and strict time limits should be observed.

VANET SECURITY THREATS IN VCPS

1) Interference attack VANET (Vehicular Ad-hoc Network) security threats are both from the outside world and internal attacks. Security issues are more complex. Interference attack is an attack method based on the frequency selection, channel listening, modulation and data sending and receiving functions provided by the physical layer of wireless communication. High bit error rate, limited transmission bandwidth, poor communication quality, and poor system security are inherent characteristics of wireless channels. In the ad hoc network, vehicles randomly access or leave the network wirelessly and share wireless channels. Attackers can transmit high-power interference signals to specific areas, disrupt normal communication between vehicles, and cause signal transceiver nodes to lose normal signal transmission and reception capabilities, thereby forming a spectrum jamming attack [4]. The general implementation of spectrum interference attack is when the attacker perceives the communication behavior in the network, generate and transmit continuous high-power wireless signals in the licensed frequency band by increasing their own power spectral density (PSD) to block normal communications. When a node wants to send data, because the channel is busy and cannot obtain effective use of the channel, when the node wants to receive data, the receiving node is also annihilated by a large number of wireless signals from the attack. In VCPS, various types of real-time perception information must be frequently exchanged between vehicles in order to make appropriate judgments and decisions for vehicle safety. However, if such information cannot be transmitted or transmitted normally between nodes, an error may occur, which may cause chaos in the inter-vehicle communication and may even cause a safety accident. Spectrum interference attack is a typical physical layer DoS attack.

2) False information attack false information attack is a kind of active attack method that is realized by sharing the characteristics of open channels among nodes in VANET. In VANET, when the attacker captures the frequency band where the shared channel is located, you can pretend to be a legitimate VCPS node and send false information to the network. You can also falsify, delay forwarding, or discard the information that needs to be forwarded after receiving it, so as to achieve the purpose of the attack. Security is the key to whether VCPS technology can move from theory to application and from lab to large-scale deployment. Traffic safety relies on the cooperation among a large number of nodes in a VCPS, and it is required that the nodes can exchange information in real time and ensure the authenticity, integrity, and availability of data transmission. For this reason, VANET needs to be able to simultaneously defend against internal and external network security threats and form a highly collaborative network environment that is trustworthy, controllable and manageable.

3) The tunnel attack tunnel attack [5] refers to the malicious node in the network concealing the real path between the nodes by creating a hidden communication channel, algorithms involving route information, such as routing and node positioning, fail due to the falsity of the information obtained. There is a covert channel between malicious attack nodes A and B. Attacking nodes using this covert channel can absorb the data traffic of the neighboring nodes, ignoring the existence of the "vehicle A" node. Because some of the real nodes are ignored, the authenticity of the network topology is destroyed, and the topology-based communication cooperation and algorithms are mistaken during execution. The characteristics of active attacks and passive attacks are also reflected in the tunnel attack process. Malicious nodes cooperate with each other to build covert channels to redirect routes. Other attack methods can also use the created tunnel to initiate new attacks. The realization process of the tunnel attack, from monitoring the available frequency band of the network to the generation of attacking peers, the entire process is completely dependent on the normal network protocol and does not tamper with the information of other nodes. Instead, it uses its own advantages in tunnel resources to induce other nodes to choose paths. In VCPS, tunnel attacks mainly exist at the physical layer and network layer, and they mislead the information transmission path, which leads to the error in judging the relative position between vehicles and the traffic safety.

In addition to the above security attacks, VCPS is also subject to black hole problems, DoS attacks (layers distributed in the network architecture, such as network layer DoS attacks, MAC layer DoS attacks, etc.), routing table overflow, and information leakage and other active attacks.

TRUST-BASED VCPS SECURITY METHOD ANALYSIS

Trust-based VCPS security can be divided into two categories: a centralized approach and a distributed approach. In the centralized method, the central unit controls the security of the network through the trust value [6, 7]. The method of abnormal behavior detection is proposed in [6] to improve the trust of VANET. The new certificate revocation mechanism of the Lightweight Directory Access Protocol (LDAP) directory server is provided in [7]. The certificate revocation list issued by the LDAP directory server can be implemented in real time. The literature [8] proposed a centralized method for assigning numbers pseudonyms to regulate the identity of vehicles. The literature [9] proposed an adaptive method to change the car alias in certain areas when many vehicles were in communication, but this method could not work without enough vehicles.

In the distributed method, the trust value is generally used to implement the description of the node's trusted capability. Literature [10, 11] proposes a multi-tiered trust modeling framework that includes role-based trust, experience-based trust, and majority-based trust, and can limit the number of reports received. In [12], a trust-based VANETs privacy protection model was proposed. Using the concept of groups, VANET users were anonymous in their group, but they were identified and responsible for their team leaders. The team leader played a role in the dispute or attack in VANET. The literature [13] discusses the location privacy protection in VANET, proposes a data collection framework based on path reporting, and proves that the trajectory privacy protection based on path reporting is a NP-hard problem, and gives an approximate solution to this problem. The literature [14] analyzes probabilistic and deterministic methods (alone and in combination) to estimate VANET security trust. The trust level is used to determine the legitimacy of the message and is used to determine whether the message will be used for further transmission through the VANET or to discard it. The probability method determines the level of trust of the peer vehicle based on the received information. The deterministic method measures the trust level of the received message by using the distance calculated by the received signal strength (RSS) and the geographical position of the vehicle (position coordinates). The combination of probabilistic and deterministic methods through simulation results provides better results than the individual methods.

Trust is a very important issue in VANET, especially the trust between communication vehicles. Therefore, there is an urgent need for effective trust management in VANET to ensure the safety of in-vehicle network communications. The literature [15] discusses the challenges faced by trust management and existing trust models in VANETs and points out their key issues.

RESEARCH DIRECTION OF VCPS COMMUNICATION SECURITY

As mentioned above, there are many security threats and hidden dangers faced by VCPS communication. Through research and analysis, we can conclude that in the future work, the research on communication security aspects of VCPS can be divided into the following modules:

1) Assessing the credibility of participating VANET nodes and detecting their bad behavior: The evaluation of vehicle reliability in VANET is an important issue. Any malicious attack can endanger people's lives. Then define what is a node's trustworthy standard, how to judge whether it is reliable to rely on it to disseminate key information. Based on these criteria, we can detect vehicle or back-end unfair behavior. What measures should be taken to detect inappropriate behavior and how to define penalties are all research hotspots in this direction.

2) Revocation process and certificate revocation list management and distribution: How to undo misconduct once it is discovered? CRL-based solutions are still under development. The current use of short-lived certificate CRLs and certificate change policies has not yet been defined, and there are still loopholes in the CRL infrastructure.

3) The ability of the network to organize itself through a high mobile network environment: The formation of a group is a trend, but how to achieve cross-partition delivery in VANET is still not clearly defined. In the team, the team leader is the central server that joins all the nodes in this group and passes it for key management and basic communication. Study the solution when the leader leaves the group or cuts off the radio link by integrating the different wireless technologies in VANET and switching between them when a problem occurs.

4) Data Context Trust and Verification: VANET aims to ensure security and cooperation. This provides appropriate information to the driver or vehicle. Therefore, it is very important to check and verify the exchanged

information. Anti-tamper hardware used in vehicles can detect unnecessary information accident warnings. VANET needs further research on data-centric trust and verification. For contextual verification, the vehicle must be able to act as an intrusion detection system to compare the information received about the status and environment with the information available to them. In addition, the concept of passive security needs to be strengthened.

5) Security, privacy, and irreversibility guaranteed cryptography methods: For the key size, there is no recommended key size, authentication delays, and specific protocols. The method of periodically switching certificates to ensure privacy has not yet been defined. At the same time regarding untraceability and privacy, in addition to using mobile IP or changing the IP or MAC address through the vehicle to prevent traceability, there are still more effective methods to be studied.

6) Anti-malware and intrusion detection systems: The embedded anti-malware framework still has problems in VANET. This is an intrusion detection mechanism that must be developed to enhance network security.

CONCLUSION

This article mainly analyzes and summarizes the security of VCPS from the perspective of VCPS communication. First of all, it gives the security requirements in the process of vehicle communication, and at the same time puts forward the security threats in the process of communication, and then analyzes the security based on trust. Finally, the future research direction and content of the security in VCPS communication are summarized.

ACKNOWLEDGMENTS

This work is supported by the national natural science foundation of China under grant (No.61572142), natural science foundation of Guangdong province under grant (No.2015A030313490).

REFERENCES

1. Li Yang, Wang Zhe, Zhang Chuwen et al. “Trajectory Prediction Algorithm in VANET Routing”, Computer research and development, 2017, 54(11):2421-2433.
2. Xia Zhuoqun, Hu Zhenzhen, Luo Junpeng et al. “Adaptive Trajectory Prediction for Moving Objects in Uncertain Environment” Computer research and development, 2017, 54(11):2434-2444.
3. Raya M, Hubaux J P. “The security of vehicular ad hoc networks” ACM Workshop on Security of Ad Hoc and Sensor Networks”. ACM, 2005:11-21.
4. ALNIFIE G, SIMON R. “A multi-channel defense against jamming attacks in wireless sensor networks”. Proceedings of the 3rd ACM workshop on QoS and security for wirelessand mobile networks. NY, USA: ACM Press , 2007 : 95-104.
5. AL-KAHTANI. “Survey on security attacks in Vehicular Adhoc Networks (VANETs)”. Proceeding of the 2012 6th International Conference on Signal Processing and Communication Systems (ICSPCS). QLD, Australia: IEEE Press, 2012: 1-9.
6. Raya M, Papadimitratos P, Aad I, et al. “Eviction of Misbehaving and Faulty Nodes in Vehicular Networks”. Selected Areas in Communications IEEE Journal on, 2007, 25(8):1557-1568.
7. Zhang S, Wang H. “An Improved Delta and Over-Issued Certificate Revocation Mechanism”. 2008:346-350.
8. Tzer F. “Privacy issues in vehicular ad hoc networks” International Conference on Privacy Enhancing Technologies. Springer-Verlag, 2005:197-209.
9. Beresford A R, Stajano F. Mix Zones: “User Privacy in Location-aware Services” Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Conference on. IEEE, 2004:127-131.
10. Minhas U F, Zhang J, Tran T, et al. “Intelligent Agents in Mobile Vehicular Ad-Hoc Networks: Leveraging Trust Modeling Based on Direct Experience with Incentives for Honesty” Ieee/wic/acm International Conference on Web Intelligence and Intelligent Agent Technology. IEEE, 2010:243-247.
11. Minhas U F, Zhang J, Tran T, et al. “Towards Expanded Trust Management for Agents in Vehicular Ad-hoc Networks”. 2010:3–15.
12. Tajeddine A, Kayssi A, Chehab A. “A Privacy-Preserving Trust Model for VANETs” IEEE International Conference on Computer and Information Technology. IEEE Computer Society, 2010:832-837.
13. Wu Xuangou, Wan Pengfei, Zhen Xiao, et al. “Research progress in Internet of vehicles trajectory privacy protection”. Computer research and development. 2017, 54(11): 2467-2474.

14. Rawat D B, Yan G, Bista B B, et al. “Trust on the Security of Wireless Vehicular Ad-hoc Networking”. Ad Hoc & Sensor Wireless Networks, 2014, 24(3-4):283-305.
15. Zhang J. “A Survey on Trust Management for VANETs” IEEE International Conference on Advanced Information NETWORKING and Applications. IEEE Computer Society, 2011:105-112.