Low-Speed Injection Attack Detection on CAN Bus

Chundong Wang[1,2], Chuang Li[1,2](✉), Tongle An[1,2], and Xiaochun Cheng[3]

[1] Key Laboratory of Computer Vision and System, Ministry of Education,
Tianjin University of Technology, Tianjin 300384, China
michael3769@163.com, lyc5117@hotmail.com, luoye_atl@163.com

[2] Tianjin Key Laboratory of Intelligence Computing and Novel Software Technology,
Ministry of Education, Tianjin University of Technology, Tianjin 300384, China

[3] Department of Computer Science, Middlesex University, London NW4 4BT, UK
Xiaochun.cheng@gmail.com

Abstract. The car CAN (Controller Area Network) bus message injection attacks seriously affects various functions of the safety of cars, life and property. However, low-speed injection attack is detection inconspicuous in a majority of existing researches. This paper proposes a self-contained low-speed injection attacks detection system including whole detection process and principle. This paper first analyzes the feasibility of low-speed injection attacks; then we propose to use LOF (Local Outlier Factor) to detect the injection attack, and compare with the previous detection algorithms. Experimental results show that our algorithm has obvious advantages in detection rate over the previous algorithms.

Keywords: Anomaly detection · Controller Area Network · Local Outlier Factor · Periodic error · Data mining

1 Introduction

With the rapid development of intelligent networked vehicles, the safety of automobiles has gradually attracted researchers' attention, especially the safety inside the vehicles [1–6]. When designing the vehicle's internal bus, the researchers being to consider only partial security. However, the threats from external network access have caused serious damage to IOV security. Among them, the most concerned point of the researchers is the intrusion detection of the car bus.

The key equipment (e.g. Brake systems, Engine) in the car are connected by CAN (Controller Area Network) bus. The safety detections inside cars have

Supported by NSFC: The United Foundation of General Technology and Fundamental Research (No. U1536122), the General Project of Tianjin Municipal Science and Technology Commission under Grant (No. 15JCYBJC15600), and the Major Project of Tianjin Municipal Science and Technology Commission under Grant (No. 15ZXDSGX00030).

G. Xu et al. (Eds.): FCS 2020, CCIS 1286, pp. 30–43, 2020.
https://doi.org/10.1007/978-981-15-9739-8_3

Table 1. Data frame format of CAN 2.0 Bs.

SOF	ID	Control	Data	CRC	ACK	EOF
1 bit	11 bits	6 bits	0–64 bits	16 bits	1 bit	1 bit

always focused on the intrusion detection of CAN bus by analyzing physical characteristics or message format of CAN bus (Table 1). Cho et al. [7] proposed a clock-based anomaly Intrusion Detection System (IDS), which measures and uses the time interval for periodically transmitting information as the fingerprint of the ECU (Electronic Control Unit). The resulting fingerprint is constructed by using a Recursive Least Squares (RLS) algorithm to construct the ECU clock behavior. Based on this standard, CIDS uses Cumulative sum (CUSUM) to detect and identify abnormal changes, and its core is still clock-based. Similar to [8] and [9], time intervals are used as features to detect anomalies.

Existing papers based on traffic anomaly detection, including intrusion detection based on bus features and intrusion detection based on machine learning [10–16], can detect high frequency or large data insertion injection attacks, and rarely detect injection data. But this type of attack can also threaten vehicle safety. At this time, the abnormal data are small, and the abnormality detection based on the traffic is generally not detected. In addition, most existing works assume that the period of the message is fixed and used as a fingerprint, but existing research does not consider the situation in which the message period changes due to actual conditions.

In this paper, considering the periodic variation, the injection attacks with less data volume is detected, and finally a good detection effect is achieved. So, we have two contribution:

1) This paper analyzes the feasibility and harm of low-speed injection attacks;
2) This paper proposes a new detection method: it can detect low-speed injection attacks.

The main contents of this paper are as follows. In Sect. 2, we introduce and analyzes different detection methods for injection attacks. In Sect. 3, The article analyzes the possibility of low-speed injection attacks. In Sect. 4, The article proposes a detection model and introduces the detection process. In Sect. 5, We introduce the detection principle for low-speed injection attacks. Further, we use experiments to verify the feasibility of the detection algorithm, conduct comparative experiments and analyze in Sect. 6. Finally, we summarize the article in Sect. 7.

2 Related Work

Recently, machine learning technology has become more and more mature, and many researchers have gradually applied related algorithms to bus intrusion detection. For example, the Kang et al. [15] uses Deep Neural Networks (DNN) to detect intrusion behavior, among which DNN parameters. It is trained by probability-based feature vectors extracted from the in-vehicle network grouping. Literature [16] uses information entropy as a feature structure of the Gradient Lifting Decision Tree (GBDT), and realizes the detection of abnormal messages. Markovitz et al. [17] proposes a semantic perceptual anomaly detection model for CAN bus traffic. In the learning phase, the field is characterized according to the classifier, and the model is built according to the field type. The model can detect the abnormal traffic on the CAN bus very well. The traffic on the port is abnormal. Kang et al. [18] use the voltage of the ECU (Electronic Control Unit) as fingerprint information, which not only achieves a high intrusion detection rate, but also realizes identification of the ECU.

Marchetti et al. [19] propose an anomaly detection algorithm based on CAN bus message ID sequence, which can identify attacks based on malicious injection. However, in the face of one or several malicious message injections, the detection rate depends on the probability distribution. In short, this type of attack has a limited effect. For example, as described in the article, when the insertion rate is low, the anomaly detection rate of the four IDs is relatively low. Marchetti et al. [20] uses the concept of entropy in information theory to calculate the information entropy of the message, and this theory can determine whether the message is forged to achieve the purpose of detecting anomalies. However, this detection method aims at all message injection attacks and only works under high-rate attacks; while the low-speed injection attack with the same ID is effective, this method requires several exception detectors to be executed in parallel (one for each ID). However, the overhead of resource consumption is quite heavy.

3 The Feasibility Analysis of Low-Speed Injection Attacks

3.1 CAN Message

In order to distinguish the independence and uniqueness of each message on the CAN bus, the ID of the message must be unique on a bus; later, the ID of the message is determined by the priority of the message, which also indicates the priority of the message on the bus.

When a message is sent on the CAN, the level on the bus is read and compared to the data that it wants to send when each message sends an ID portion. This is called bus arbitration. If node A sends a recessive bit (usually 1) and reads a dominant bit (usually 0), then A will realize that a message with a higher priority than itself is being sent on the bus, losing its right to send, waiting to send it the next time.

For the bus-based message arbitration mechanism, when message A and message B collide (simultaneous transmission), there will be two cases: A wins or B wins. Considering the presence of an attacker, when malicious message A and normal message B are simultaneously sent, there are generally three cases:

1) A has a high priority, wins arbitration, and B message is sent the next time. That is, message A is injected successfully, and message B is delayed transmission, which does not affect normal message transmission.
2) B has a high priority and wins arbitration. Message injection fails.
3) The IDs of A and B are the same, and they are sent at the same time. An error occurs in the data field, and an increment of the error counter occurs [21].

3.2 Principle of Attack

If an attacker conducts low-speed injection attacks, there are generally two purposes:

(1) Random message injection, to destroy normal communication. First, it listens, collects the data sent on the CAN bus, and then randomly performs message injection. In order to avoid most of the current detection methods, low-frequency, irregular message injection is required. It is called the random injection attack in this article.
(2) In order to control the vehicle, targeted injection of information is carried out. The attacker listens to the target message on the bus and calculates the message period. In the next step, the attacker has two attack methods according to the purpose of the attack:

A. The message is sent on time according to the calculated period. In order to cause the malicious message to collide with the normal message, the message is invalidated, and eventually the normal communication is destroyed.

B. The attacker calculates the time at which the next message is sent, avoiding the point in time for message insertion. The purpose is to stagger the malicious message and the normal message, to make the malicious message take effect, and finally disrupt the normal communication, so that the vehicle performs unexpected actions. For example, send a command to open the door during high-speed driving. This behavior can implement bus-off attack [11].

The success rate of these two attack methods depends on the attacker's understanding of the communication process. In order to achieve the second attack purpose, the attacker needs to have bigger computing power and deeper understanding of the communication process than the first one. With the improvement of hardware (ECU) and the development of the industry, these are not problems. So, the impact of low-speed injection attacks on vehicles has become possible. This paper is useful for the detection of these two kinds of aggression.

4 Detection Model

The detailed flow of data from sending to detection is displayed in the Fig. 1.

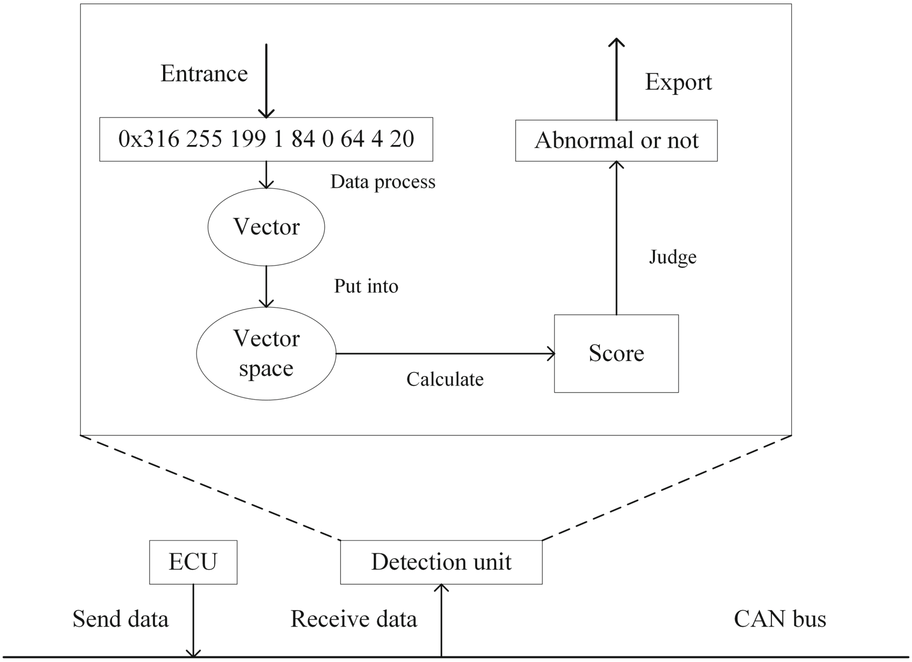


Fig. 1. Detection process.

4.1 Data Process

The data used in this article are all standard data sets [22]. Once the data is available, the data is processed first, so that all data are normalized and formatted. The format of the data collected at the beginning is as follows:

0x123:8:fec05dc05d0708b8

For ease of calculation and analysis, we convert the data to a decimal number:

291:254,192,93,192,93,7,8,184

Among them, the third part of the data field has a total of 64 bits, which is divided into 8 parts, each part is 8 bits, and then converted into a decimal number.

According to the previous section, the CAN bus data in the car can be divided into two parts: The first part the ID number, there are many ECUs on the bus, generally only one ID number can be issued by an ECU, so the ID number can be used as a description dimension of the data point; The second part is the data field, which is the specific content of the message. In this paper, it is divided into eight parts, which are eight other dimensions of the data point. In addition, since the data on the bus is generally sent periodically, the cycle can also be an important dimension. In this paper, the current ID is predicted, and the probability that the ID appears at this time is taken as a reference dimension.

So far, we have obtained data descriptions for 10 dimensions. They are: period T, identifier I and data fields D_1, D_2, D_3, D_4, D_5, D_6, D_7 and D_8.

4.2 Low-Speed Injection Attacks Detection

On the bus, the data transmission is exclusive. The detection unit only needs to read the detection abnormality frame by frame, and the detection result can be obtained before the complete data transmission ends. The detection principle is described in detail later.

5 Detection Principle

The normal communication process on the bus is shown in the Fig. 2.

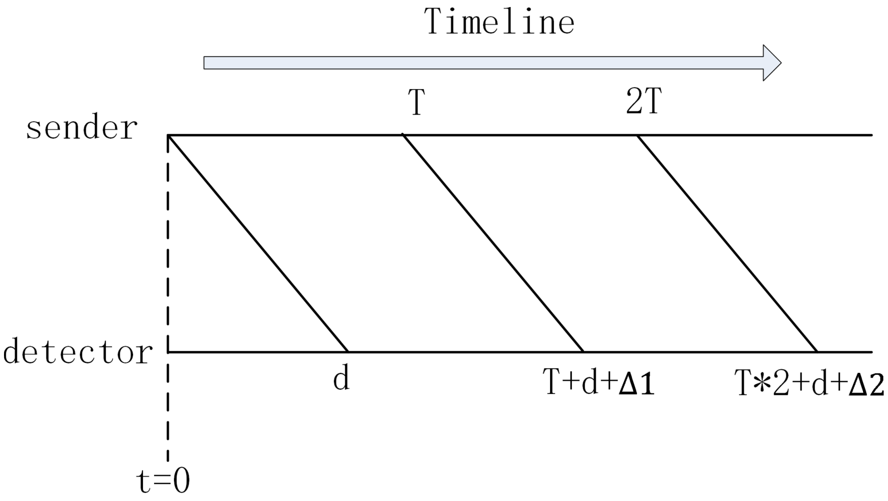


Fig. 2. Message simulation.

In the Fig. 2, $t = 0$ is the first data time point sent by the sender, T is the transmission period, and the d that is the time a message is uploaded from the ECU to the bus is the reception delay, depending on the length of the packet that is generally fixed. When the ECU on the bus sends a message, due to the influence of the transmission environment-such as the transmission speed of the bus and the performance of the ECU, the time when the receiver receives the data and the theoretical time always have a certain discrepancy, which is Δ in the above figure. Although Δ_1 and Δ_2 are not equal in the figure, due to hardware factors, the values of the two variables will always be in a small range.

The attacker is unable to inject data with an abnormal ID number, they will consider injecting data of the same ID for destruction and interference. The general attack process is as follows:

a) The attacker listens and periodically detects the data of an ID number on the bus.
b) Calculate the sending period of the message
c) Calculate the time you want to send based on the time of the last message at the appropriate time
d) Inject packet on time

When an attacker injects a packet in this way, there are two situations: Malicious messages and normal messages are misaligned due to random perturbations in the periodicity of the message; malicious messages and normal messages fail to be sent due to the message collision mechanism of the CAN bus.

A message is misplaced, the following occurs in the Fig. 3.

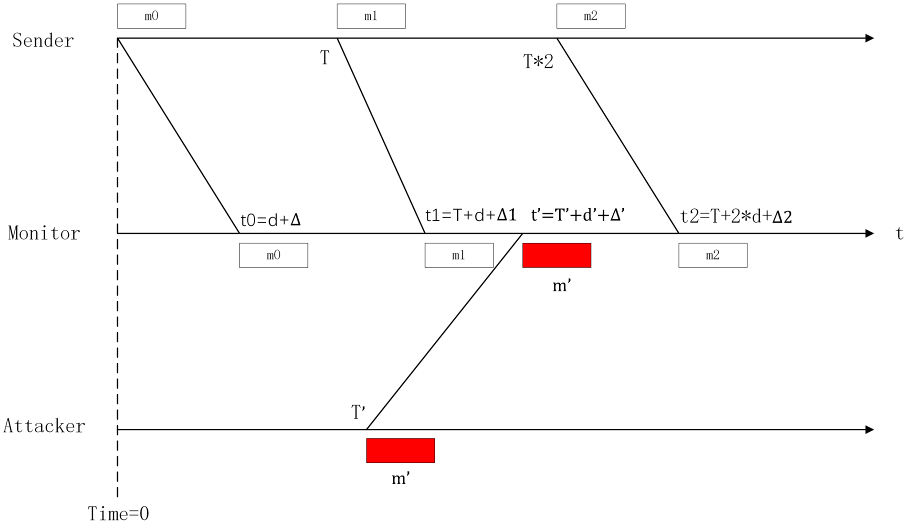


Fig. 3. Message misplacement.

The sender of the normal message has a transmission period of T, the delay of the message that the listener receives the ID is d, and the listener will randomly perturb Δ when it receives each message. When $T = 0$, the attacker has calculated the transmission period T' of the message m according to the previous message, and then sends an attack message at the time T'. The propagation delay of the attacker sending the message is d', and the random disturbance is Δ'. At this point, the listener receives four messages: m_0, m_1, m', m_2, at times t_0, t_1, t', t_2, respectively. For the listener, four messages are sent.

In this way, when the listener detects the message period of this ID, the calculation cycle will be different for the messages m_1 and m': the message m' is close to m_1, so the calculated period is very short; When calculating the period of the message m_2, since the time after the occurrence of m is later, the obtained value will be different from the normal period, that is, it will be smaller. This difference is more pronounced if the period of each message is more stable.

When two messages collide, the following happens in the Fig. 4.

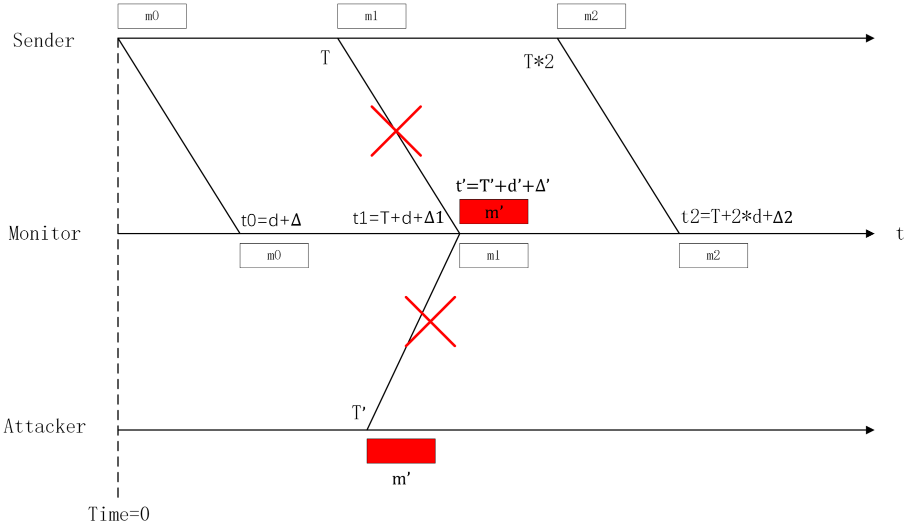


Fig. 4. Message collision.

As shown in the Fig. 4, when messages m_1 and m' collide, both messages fail to be sent. The listener only receives two messages at times t_0 and t_2.

Thus, when the listener detects the message period of the ID, the message m_1 collides with the malicious message m', the m_1 transmission fails, and the existence of m_1 is not detected. The calculated period of m_2 will be twice the normal period.

According to the above detection principle, we use the LOF (Local Outlier Factor) algorithm [23] in the outlier detection algorithm to detect periodic packets. When low-speed injection attacks occur, the cycle of the message has changed, the location of the message in the data space is farther from the normal data points, and the LOF algorithm can find these anomalies accurately and quickly.

6 Experimental Results and Analysis

6.1 Abnormal Insertion

In order to perform anomaly detection experiments, we use two different types of low-speed injection attacks:

a) Random injection attack: Random insert data.
b) Replay attack: The attacker listens for messages on the bus and then sends the packet according to the detected ID period

All the data in this paper comes from the CAN bus when the vehicle is driving normally.

6.2 Abnormal Detection

Using the 20,000 data in the static state as a template, use the LOF algorithm to get the Fig. 5.

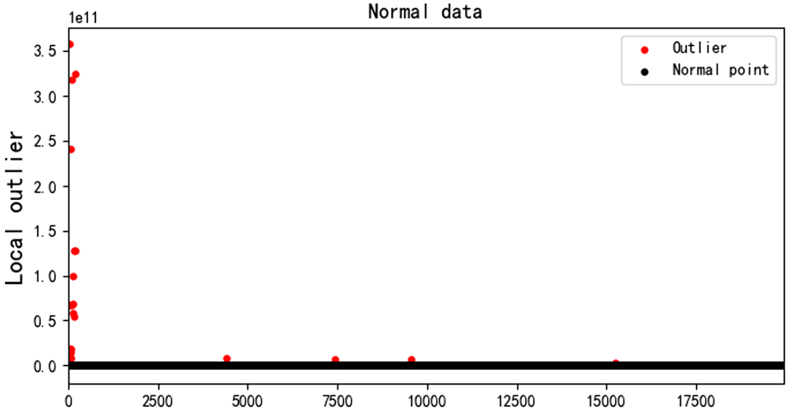


Fig. 5. Normal data outliers.

We have intercepted a piece of data. Each ID number has a small period when it first appears. In this experiment, it is treated as 0, which must be an outlier, so the outliers starting from the figure can be omitted. There are three outliers with small outliers in the middle of the graph, which can be regarded as normal systematic errors with an error rate of 0.015%.

a) randomly extract and insert from the vehicle speed data

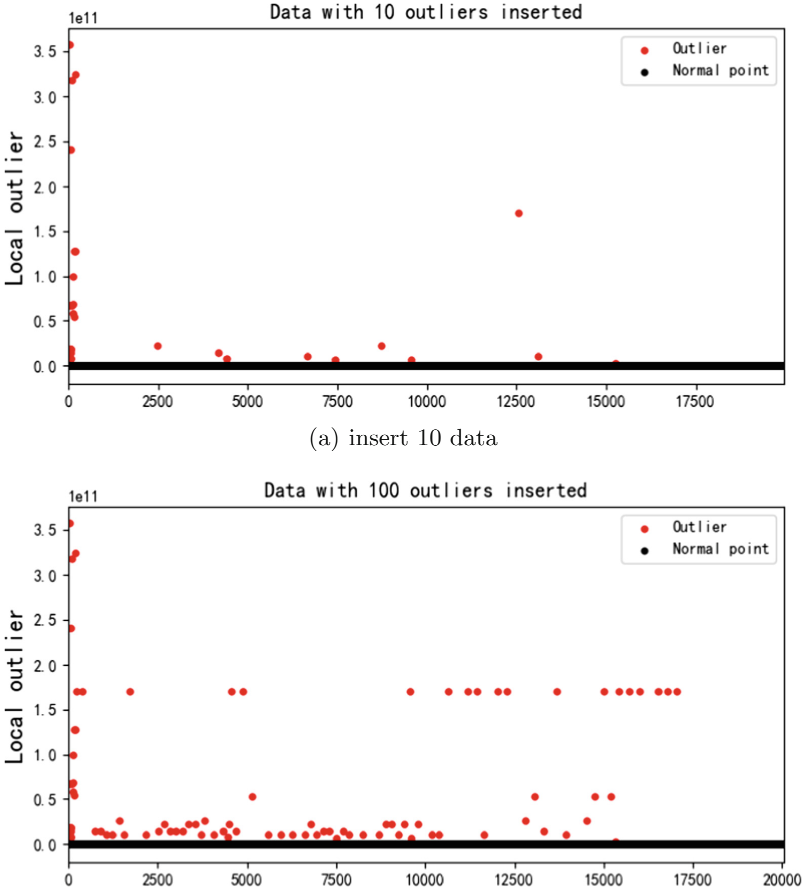
We extract 10 and 100 strips from the vehicle speed data and insert them separately. After running the LOF algorithm, we get the Fig. 6.
There are more outliers in the two graphs. The abnormal rate on the top is about 0.045%, which is 3 times the normal. The abnormal rate on the below is 0.35%, which is 23 times the normal conditions. Therefore, when randomly inserting less data, it is easy to detect whether the data on the bus is abnormal by using the LOF algorithm.

b) perform cycle detection and insert the message

In this experiment, we extract the data of the same ID number in the collected data and then format it. In addition, simulate an attack node for message insertion.

When a malicious message is inserted, the message is misplaced. The LOF algorithm results are in the Fig. 7.
In the Fig. 7, there are two abnormal points, and the above abnormal point ID and the following abnormal point ID are just approaching, which is consistent with our expectation.

When a malicious message is inserted, no misalignment occurs, that is, two messages collide, and the LOF algorithm results are in the Fig. 8.



(a) insert 10 data

(b) insert 100 data

Fig. 6. Outliers after inserting data

In the Fig. 8, only one abnormal point appears, which is also in line with our expectations.

c) brief summary

During the detection of a specific ID message injection, if the normal message and the malicious message do not collide, then two of the messages will become outliers in the LOF algorithm. The local outlier factor of the first point is relatively large, and the second one is relatively small. The value of the second local outlier is largely dependent on the error value (disturbance value) of this message as it travels over the bus. The smaller the error value, the smaller the second local outlier factor. When the error value is small, the probability that a normal message collides with a malicious message is greater. Only when the error value is within a certain range can an attacker escape the detection of the

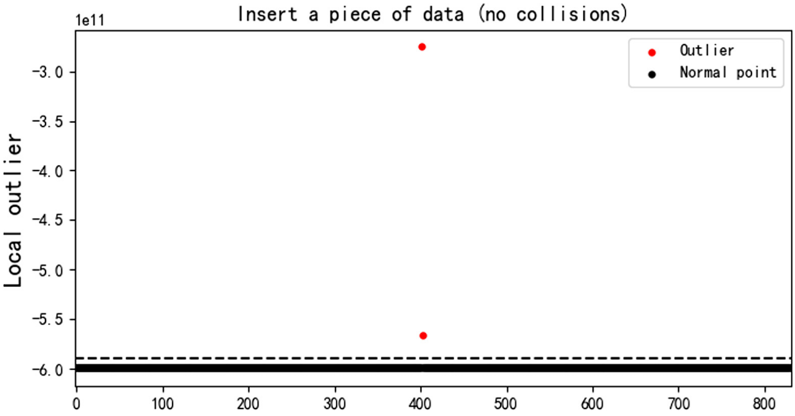


Fig. 7. Outliers after a message misplacement.

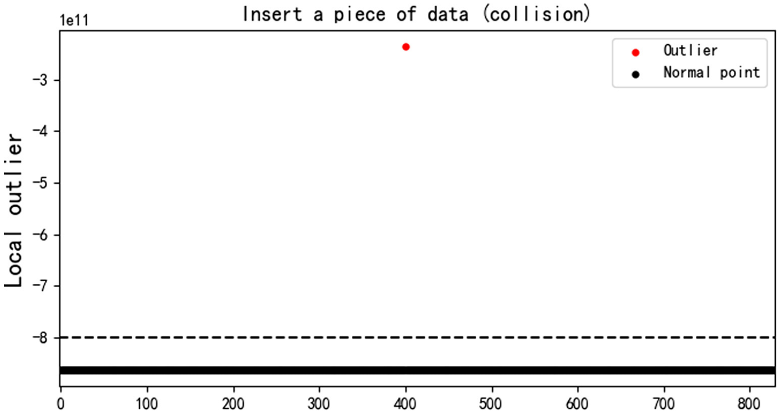


Fig. 8. Outliers after a message collision.

LOF algorithm. But the attacker does not know the error value of a certain message, so it is hard to evade detection.

6.3 Contrast Experiment

In this paper, algorithm based on sequence (AS) [19], information entropy algorithm (IEA) [20] and LOF algorithm are used for comparative experiments. The sequence-based algorithm is to create a two-dimensional array associated with ID Numbers. If adjacent messages appear in normal messages, fill in 1 at the corresponding position in the array. During the detection process, it is judged whether the position of the serial number in the matrix is 1 or not. For example, after serial number A is serial number B., write 1 in column A and row B of the array. Detection based on information entropy is calculating the information entropy of packet within a certain time window.

There are three attack windows in this article: 0.1s, 0.5s and 1s. The selection of the time window has no effect on the detection results of AS and LOF. In this paper, only the detection results with attack window of 1s are displayed for two algorithms. In the experiment, there are seven different levels of data volume for inserting data: 0.1%, 1%, 3%, 5%, 8%, 10% and 20%. The detection results of the three algorithms are shown in Table 2 and Table 3.

Table 2. Random injection attack.

		0.1%	1%	3%	5%	8%	10%	20%
AS	1s	99.2	99	99	99.1	99.1	99	99.1
IEA	1s	100	100	100	100	100	100	100
	0.5s	0	100	100	100	100	100	100
	0.1s	NULL	0	0	0	100	100	100
LOF	1s	90.1	86.7	83.2	80.1	79	78.8	77

Annotate: The number unit in the table is %.

Table 3. Replay attack.

		0.1%	1%	3%	5%	8%	10%	20%
AS	1s	50	51.4	51.6	51.8	51.9	51.9	52
IEA	1s	0	0	0	100	100	100	100
	0.5s	0	0	0	0	100	100	100
	0.1s	NULL	0	0	0	0	0	0
LOF	1s	90.1	86.7	83.2	80.1	79	78.8	77

Annotate: The number unit in the table is %.

As can be seen from Table 2, the detection of the random injection attacks by the LOF algorithm is worse than the other two algorithms. However, as can be seen from Table 3, the LOF algorithm is significantly better than the AS. Compared with the IEA, the LOF algorithm is better when the insertion data is below 3%. When it is higher than 3%, the detection effect of the IEA depends on the detection window. The detection effect of the LOF algorithm is independent of the detection window, so it is better than the IEA.

In general, when the inserted data is less than 20%, the LOF algorithm is superior to the other two algorithms in detecting the replay attack, and is worse than the other two algorithms in detecting the random injection attacks. The data inserted by the random injection attacks have a greater impact on the entire communication process, calculating information entropy and contrasting two-dimensional array are more sensitive to random injection attacks, so the two methods have better detection effects on random injection attacks. The LOF algorithm detection does not depend on the attack behavior, which is only related to the amount of data inserted, so the detection effect of the two attacks is basically the same.

The purpose of the two attack methods is different. The random injection attack is for the communication system, and the replay attack is to achieve certain functions. Detection of replay attacks is more important.

7 Conclusions

This paper describes the low-speed injection attacks from the uniqueness of each state message of the vehicle, and introduces the purpose and principle of the two related attacks: the random injection attack and the replay attack. The density-based outlier detection algorithm LOF algorithm in data mining is used to detect these two attacks. For the replay attack in low-speed insertion attacks, a good detection result is finally obtained.

With the development of attack technology, the attacker's means are more sophisticated. Message anomalies are not only reflected in traffic, but data content can also be forged by attackers. In order to face endless attacks, it is not enough to detect anomalies only from the aspect of traffic. It is also necessary to detect various attacks from the data content. This is our next research goal.

References

1. Malik, K.R., Ahmad, M., Khalid, S., Ahmad, H., Jabbar, S.: Image and command hybrid model for vehicle control using Internet of Vehicles. Trans. Emerg. Telecommun. Technol. **31**(5), e3774 (2020)
2. Sajjad, M., et al.: CNN-based anti-spoofing two-tier multi-factor authentication system. Pattern Recogn. Lett. **126**, 123–131 (2019)
3. Chen, C., Liu, X., Qiu, T., Sangaiah, A.K.: A short-term traffic prediction model in the vehicular cyber-physical systems. Future Gener. Comput. Syst. **105**, 894–903 (2020)
4. Aloqaily, M., Otoum, S., Al Ridhawi, I., Jararweh, Y.: An intrusion detection system for connected vehicles in smart cities. Ad Hoc Netw. **90**, 101842 (2019)
5. Al Ridhawi, I., Otoum, S., Aloqaily, M., Jararweh, Y., Baker, T.: Providing secure and reliable communication for next generation networks in smart cities. Sustain. Cities Soc. **56**, 102080 (2020)
6. Lv, Z., Mazurczyk, W., Wendzel, S., Song, H.: Recent advances in cyber-physical security in industrial environments. IEEE Trans. Ind. Inf. **15**(12), 6468–6471 (2019)
7. Shin, K.G., Cho, K.T.: Fingerprinting electronic control units for vehicle intrusion detection. In: 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, USA (2019)
8. Song, H.M., Kim, H.R., Kim, H.K.: Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. In: 2016 International Conference on Information Networking (ICOIN), pp. 63–68. IEEE, Kota Kinabalu (2016)

9. Gmiden, M., Gmiden, M.H., Trabelsi, H.: An intrusion detection method for securing in-vehicle CAN bus. In: 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), pp. 176–180. IEEE, Sousse (2016)
10. Taylor, A., Sylvain L., Nathalie J.: Anomaly detection in automobile control network data with long short-term memory networks. In: 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA), pp. 130–139. IEEE, Montreal (2016)
11. Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Mostarda, L.: Cyber security threats detection in internet of things using deep learning approach. IEEE Access **7**, 124379–124389 (2019)
12. Amrollahi, M., Hadayeghparast, S., Karimipour, H., Derakhshan, F., Srivastava, G.: Enhancing network security via machine learning: opportunities and challenges. In: Choo, K.-K.R., Dehghantanha, A. (eds.) Handbook of Big Data Privacy, pp. 165–189. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-38557-6_8
13. Mohammadi Rouzbahani, H., Karimipour, H., Rahimnejad, A., Dehghantanha, A., Srivastava, G.: Anomaly detection in cyber-physical systems using machine learning. In: Choo, K.-K.R., Dehghantanha, A. (eds.) Handbook of Big Data Privacy, pp. 219–235. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-38557-6_10
14. Skowron, M., Artur, J., Wojciech, M.: Traffic fingerprinting attacks on internet of things using machine learning. IEEE Access **7**, 20386–20400 (2020)
15. Min-Joo, K., Je-Won, K., Tieqiao, T.: Intrusion detection system using deep neural network for in-vehicle network security. PLoS ONE **11**(6), e0155781 (2016)
16. Tian, D., et al.: An intrusion detection system based on machine learning for CAN-bus. In: Chen, Y., Duong, T.Q. (eds.) INISCOM 2017. LNICST, vol. 221, pp. 285–294. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-74176-5_25
17. Markovitz, M., Avishai, W.: Field classification, modeling and anomaly detection in unknown CAN bus networks. Veh. Commun. **9**, 43–52 (2017)
18. Cho, K.T., Kang, G.S.: Viden: attacker identification on in-vehicle networks. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 815–828. ACM, Dallas (2017)
19. Marchetti, M., Dario S.: Anomaly detection of CAN bus messages through analysis of ID sequences. In: 2017 IEEE Intelligent Vehicles Symposium (IV), pp. 1577–1583. IEEE, Los Angeles (2017)
20. Marchetti, M., Stabili, D., Guido, A., Colajanni, M.: Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms. In: 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), pp. 1–6. IEEE, Bologna (2016)
21. Cho, K.T., Kang G.S.: Error handling of in-vehicle networks makes them vulnerable. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 1044–1055. ACM, Vienna (2016)
22. TU-CRRC. http://tucrrc.utulsa.edu/Publications.html. Accessed 3 Apr 2019
23. Breunig, M.M., Kriegel, H.P., Ng, R., Sander, J.: LOF: identifying density-based local outliers. In: Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, pp. 93–104. ACM, Dallas (2000)