2022 ICEICT

Performance evaluation and ZigBee smart home device security access scheme

厦门理工学院
XIAMEN UNIVERSITY OF TECHNOLOGY

Abstract

This paper proposes a secure access method for Zigbee networks. Install Code is used to pre-configure the entry key when a smart device is connecting to a Zigbee network, thus guaranteeing the security of ZigBee entry and entry efficiency. The hardware based experiment results show that using Install Code encryption in the network has a better defence against sniffing attacks, and has 5% lower packet loss rate compared to Global key entry.

Background

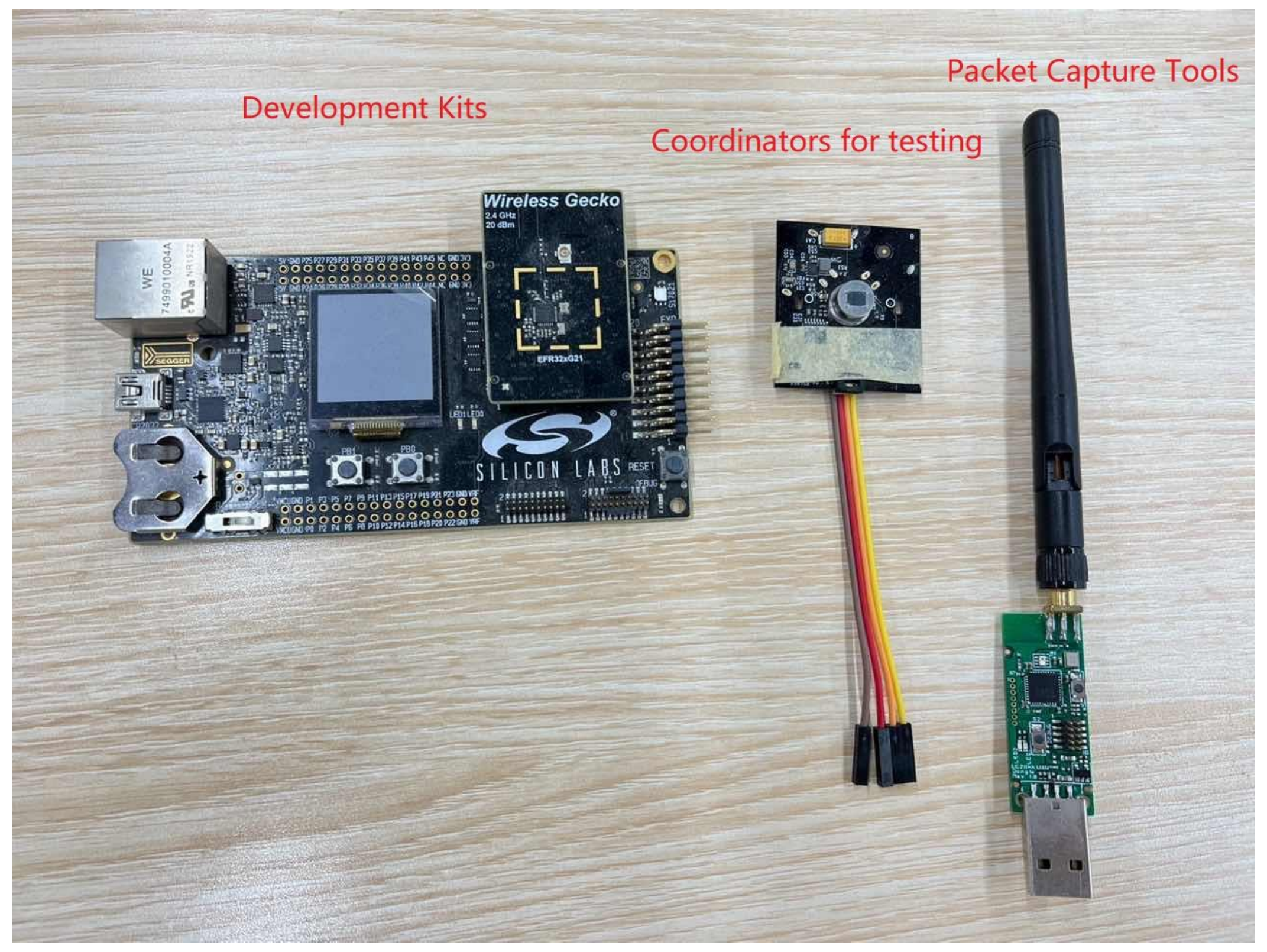
At present, ZigBee smart home devices are mainly connected through the gateway to open the entry channel and the device seeking network for an interactive connection. Since the default key connection is used in the interactive process, such a scheme is easy to be sniffed by hackers in the device seeking network stage, thus destroying the security of the network. Therefore, this paper proposes a sweeping QR code access scheme, which uses the sweeping QR code to establish a communication connection to a designated device, thus eliminating the risk of pen involved being sniffed.

Project Goals

- **Install code converted ID.**
- **Install code to QR code conversion.**
- **Install code based joining Method via internet.**
- **Keys security reinforcement.**

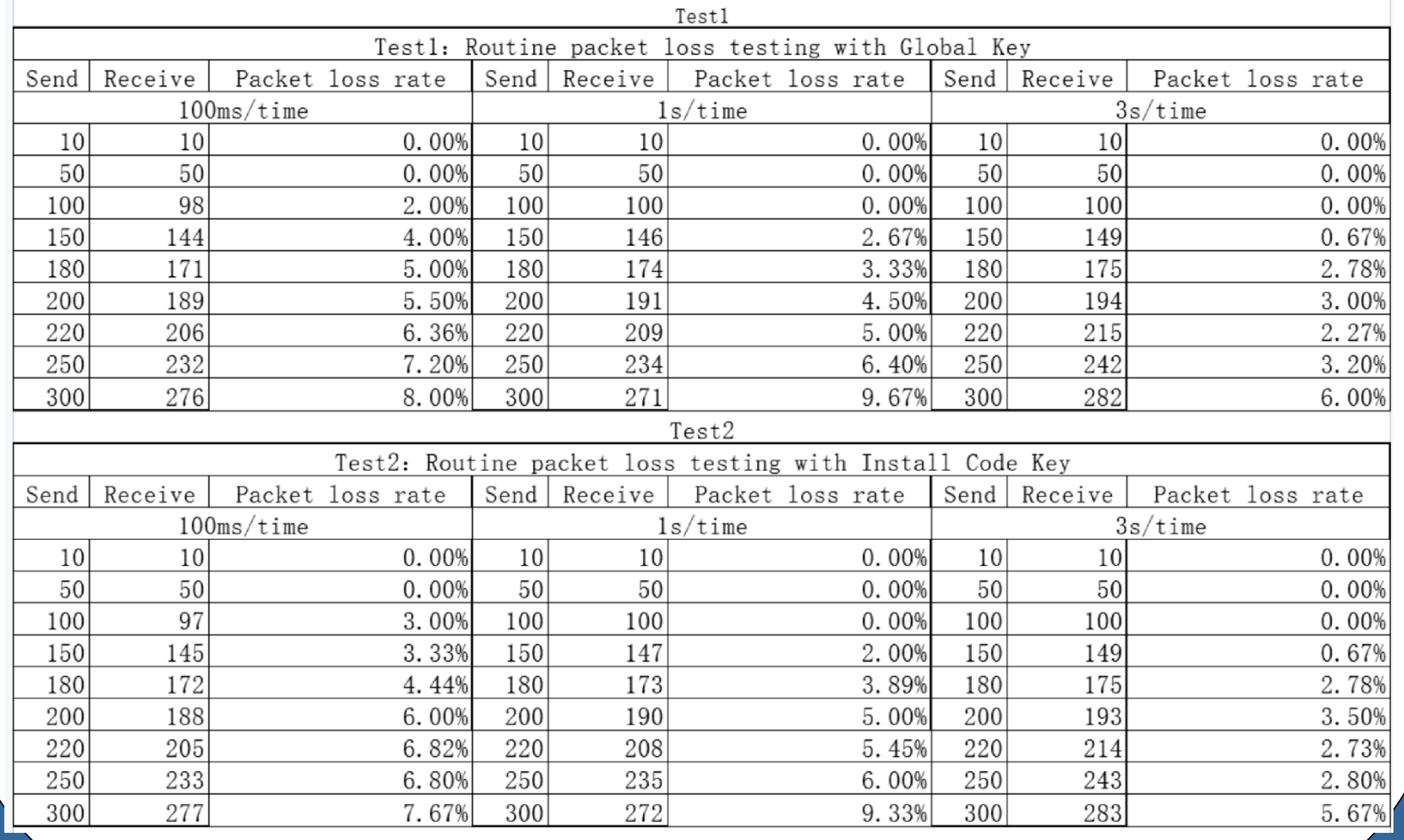
Process

The experiment is based on the software Simplicity Studio v5 development software and the development kit with EFR32xG21, using one kit as a coordinator device (Coordinator) and one as a routing device (Router) to establish the ZigBee network connection. Network analysis and packet capture are performed on the Ubiqua platform using a packet capture tool.



Results

After using Global Key and Install Code Key to send and receive packet loss test, the packet loss rate is similar, but with Install Code Key encryption method, the packet loss rate decreases to a certain extent, about 0.5%.



Test1

Test1: Routine packet loss testing with Global Key

Send	Receive	Packet loss rate	Send	Receive	Packet loss rate	Send	Receive	Packet loss rate
100ms/time			1s/time			3s/time		
10	10	0.00%	10	10	0.00%	10	10	0.00%
50	50	0.00%	50	50	0.00%	50	50	0.00%
100	98	2.00%	100	100	0.00%	100	100	0.00%
150	144	4.00%	150	146	2.67%	150	149	0.67%
180	171	5.00%	180	174	3.33%	180	175	2.78%
200	189	5.50%	200	191	4.50%	200	194	3.00%
220	206	6.36%	220	209	5.00%	220	215	2.27%
250	232	7.20%	250	234	6.40%	250	242	3.20%
300	276	8.00%	300	271	9.67%	300	282	6.00%

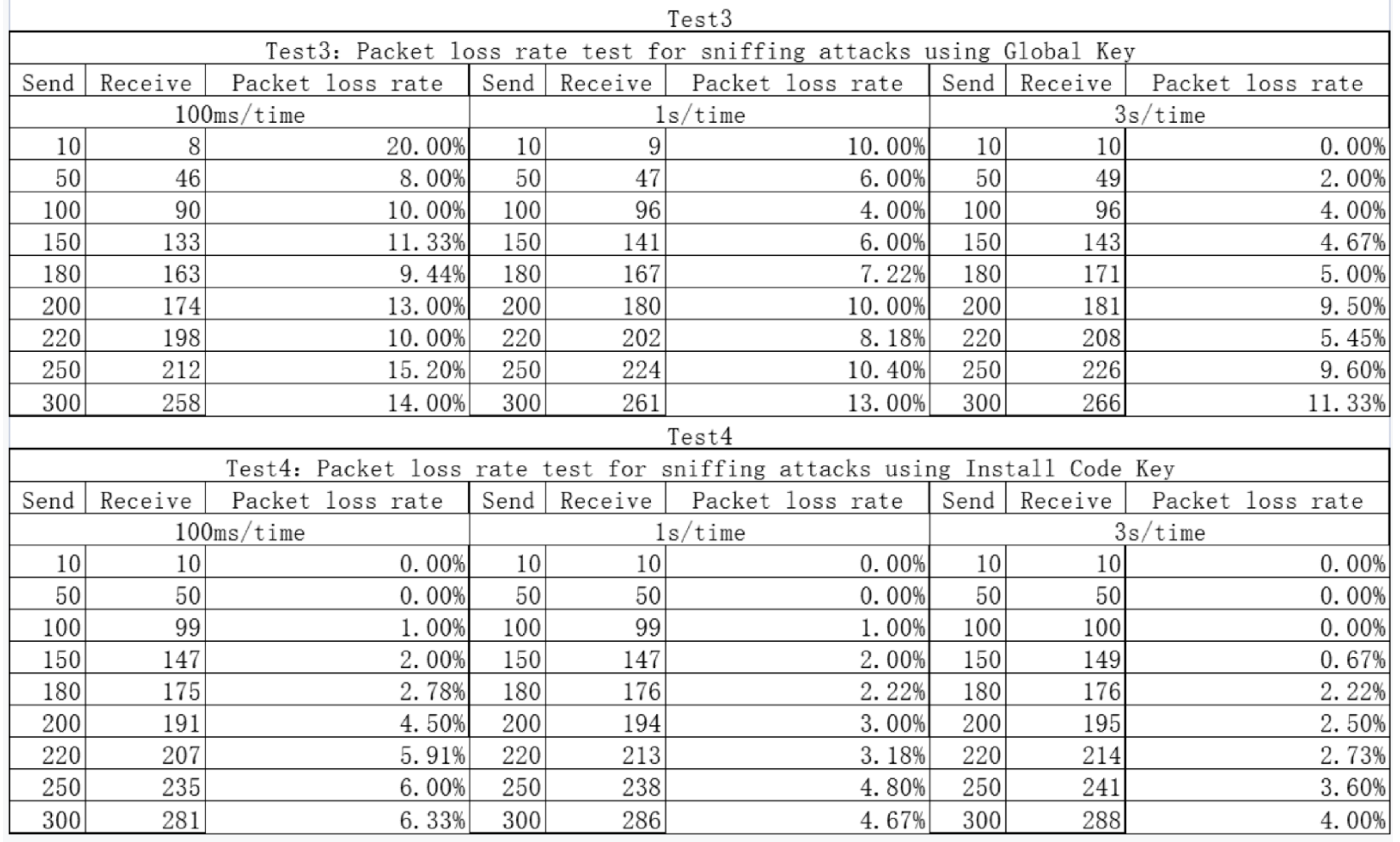
Test2

Test2: Routine packet loss testing with Install Code Key

Send	Receive	Packet loss rate	Send	Receive	Packet loss rate	Send	Receive	Packet loss rate
100ms/time			1s/time			3s/time		
10	10	0.00%	10	10	0.00%	10	10	0.00%
50	50	0.00%	50	50	0.00%	50	50	0.00%
100	97	3.00%	100	100	0.00%	100	100	0.00%
150	145	3.33%	150	147	2.00%	150	149	0.67%
180	172	4.44%	180	173	3.89%	180	175	2.78%
200	188	6.00%	200	190	5.00%	200	193	3.50%
220	205	6.82%	220	208	5.45%	220	214	2.73%
250	233	6.80%	250	235	6.00%	250	243	2.80%
300	277	7.67%	300	272	9.33%	300	283	5.67%

Results

In the test with sniffing attack, the packet loss rate decreases significantly after using Install Code Key encryption, which is 2%-5.5% compared to Global Key. This shows that using Install Code Key is a good defense against sniffing attacks.



Test3

Test3: Packet loss rate test for sniffing attacks using Global Key

Send	Receive	Packet loss rate	Send	Receive	Packet loss rate	Send	Receive	Packet loss rate
100ms/time			1s/time			3s/time		
10	8	20.00%	10	9	10.00%	10	10	0.00%
50	46	8.00%	50	47	6.00%	50	49	2.00%
100	90	10.00%	100	96	4.00%	100	96	4.00%
150	133	11.33%	150	141	6.00%	150	143	4.67%
180	163	9.44%	180	167	7.22%	180	171	5.00%
200	174	13.00%	200	180	10.00%	200	181	9.50%
220	198	10.00%	220	202	8.18%	220	208	5.45%
250	212	15.20%	250	224	10.40%	250	226	9.60%
300	258	14.00%	300	261	13.00%	300	266	11.33%

Test4

Test4: Packet loss rate test for sniffing attacks using Install Code Key

Send	Receive	Packet loss rate	Send	Receive	Packet loss rate	Send	Receive	Packet loss rate
100ms/time			1s/time			3s/time		
10	10	0.00%	10	10	0.00%	10	10	0.00%
50	50	0.00%	50	50	0.00%	50	50	0.00%
100	99	1.00%	100	99	1.00%	100	100	0.00%
150	147	2.00%	150	147	2.00%	150	149	0.67%
180	175	2.78%	180	176	2.22%	180	176	2.22%
200	191	4.50%	200	194	3.00%	200	195	2.50%
220	207	5.91%	220	213	3.18%	220	214	2.73%
250	235	6.00%	250	238	4.80%	250	241	3.60%
300	281	6.33%	300	286	4.67%	300	288	4.00%

Conclusions

we analyze the problem that the default key access mode of smart home may lead to the security risk of network theft by unlawful elements, so as to adopt the more secure Install Code encryption method to access the network. The experiments show that the security and efficiency are higher than the traditional Global Link Key access, which has some practical application value for the development of smart home industry.

Acknowledgments

The work was supported by the Natural Science Foundation of Fujian Province (2022J01130358); Innovation and entrepreneurship training program for College Students (202211062009 and 202211062010).