

## LIST OF FIGURES

2.1	Enablers of IoT [1]. . . . .	4
2.2	Bluetooth Protocol Stacks [2]. . . . .	6
2.3	GATT Transaction in BLE [3]. . . . .	10
2.4	BLE Protocol Stacks [3]. . . . .	11
2.5	BLE Security Phases [4]. . . . .	12
2.6	Token Authentication [5]. . . . .	14
2.7	Scheme of BLE Security Phases using Token Authentication [6]. . .	15
2.8	Packet Sniffing [7]. . . . .	15
2.9	Bluetooth Packet Sniffing. . . . .	16
3.1	Topology of BLE based Temperature Sensor. . . . .	17
3.2	Flowchart of Temperature Sensor. . . . .	18
3.3	Flowchart of BLE based Temperature Sensor. . . . .	19
3.4	Topology of BLE based Temperature Sensor with Packet Sniffing Attack. . . . .	20
3.5	ESP32 Micro-controller . . . . .	22
3.6	Waterproof Ds18b20 Digital Temperature Sensor. . . . .	23
3.7	Character I2C LCD. . . . .	24
3.8	Ubertooth ONE. . . . .	24
3.9	Version of Ubertooth ONE. . . . .	25
3.10	Arduino IDE . . . . .	25
3.11	Android Studio . . . . .	26
3.12	Ubuntu 18.04 . . . . .	27
3.13	Oracle VM VirtualBox . . . . .	27
3.14	Wireshark. . . . .	28
3.15	Flowchart of How the device works. . . . .	29
3.16	The composition of the instrument used as a Temperature Sensor. . .	30
3.17	Configuration of BLE Authentication on ESP32. . . . .	31
3.18	Application Interface. . . . .	33
3.19	Available Bluetooth Connections. . . . .	34
3.20	Token Authentication Process on Android Phone. . . . .	34
4.1	How to capture packet with Wireshark. . . . .	38

4.2	Results of capturing with Wireshark. . . . .	39
4.3	Results of Spectrum Analyzer. . . . .	39
4.4	Scan Response (SCAN_RSP) Packet. . . . .	40
4.5	List of Malformed Packets. . . . .	41
4.6	Packets with Different Combination Numbers of Source. . . . .	42
4.7	14th Packet Differences. . . . .	42
4.8	Results of Packet Statics on Connectivity Analysis. . . . .	43
4.9	Start of process advertising from BLE device. . . . .	44
4.10	Process of connecting between Android Phone and BLE device . . .	45
4.11	Authentication Process on Screen. . . . .	45
4.12	Results of Android Phone already connected with BLE device. . . .	46
4.13	Android Phone exchanging data with BLE device. . . . .	46
4.14	60 <sup>th</sup> Packet Data Information "Control Opcode: LE_VERSION_IND. 47	
4.15	63 <sup>rd</sup> Packet Data Information "Empty PDU" (1). . . . .	48
4.16	63 <sup>rd</sup> Packet Data Information "Empty PDU" (2). . . . .	48
4.17	93 <sup>rd</sup> Packet Data Information "L2CAP Fragment". . . . .	49
4.18	99 <sup>th</sup> Packet Data Information "L2CAP Fragment [Missing Fragment]". . . . .	49
4.19	Temperature read by sensors from BLE device and Android Phone. .	50
4.20	Experiment Scheme for Device Capabilities. . . . .	51
4.21	Results of Graphic Curve of the Delay Average. . . . .	53
4.22	Results of Graphic Curve of the Jitter Average. . . . .	54
4.23	Results of Graphic Curve of the Delay Average at Body Temperature. 55	
4.24	Results of Graphic Curve of the Jitter Average at Body Temperature. 56	
4.25	Results of Graphic Curve of the Delay Average at Extreme Temperature. . . . .	57
4.26	Results of Graphic Curve of the Jitter Average at Extreme Temperature. . . . .	58
3.1	Process Packet Sniffing on Terminal (1). . . . .	1
3.2	Process Packet Sniffing on Terminal (2). . . . .	1
3.3	Process Packet Sniffing on Terminal (3). . . . .	2