

Democratic and Popular Republic of Algeria
Ministry of Higher Education and Scientific Research

Ferhat ABBAS University Setif 1



Faculty of Sciences

DEPARTEMENT : Computer Science
DOMAIN : Mathematics and Computer Science
SPECIALTY : Networks and Distributed Systems

MASTER'S THESIS

Theme

**Security for the Industrial Internet of Things
(IIoTs) "MITM Attack"**

Presented by :
Guechtal Rihab
Merzougui Bessma

Supervised by :
Dr. ZERGUINE Nadia

Jury members :
Dr. CHERBAL Sarra
Dr. KHARCHI Samia

Academic Year: 2024/2025

Abstract

In various applications, Industrial Internet of Things (IIoT) networks have become a fundamental part. These networks rely on the Time Slot Channel Hopping (TSCH) protocol, which provides efficient communication capabilities. However, it is still vulnerable to MITM attacks. This thesis addresses this type of attack and its impact on IIoT networks.

This type of cyberattack involves stealing device identities, injecting fake data, and also using replay attacks to flood the network. We propose a new encryption mechanism based on the dynamic Fibonacci sequence and XOR logic operation to hide the identity of the real sender and protect data.

Simulation results using the Contiki-NG simulator show that our mechanism is highly effective against this attack, preventing identity theft and data decryption, thus enhancing network security.

We take into consideration the devices resource constraints while addressing these security vulnerabilities. therefore, we can say this research advances the protection of IIoT networks, ensures robust security . Achieving maximum security in constrained devices can be achieved through innovative cryptographic approaches.

Keywords: IIoT, TSCH , Fibonacci sequence, Dynamic key , MITM attack, TSCH Security.

Contents

Abstract	ii
Résumé	iv
Dedication	v
Dedication	vi
Acknowledgment	vii
Abbreviations	xiv
General introduction	1
1 Internet of Things (IoT)	3
1.1 Introduction	3
1.2 Definition of Internet of Things(IoT)	3
1.3 Characteristics of the IoT	5
1.4 Deployment	6
1.5 Applications of IoT	6
1.6 Industrial Internet of Things(IIoT)	8
1.6.1 Particularities	9
1.6.2 IIoT application examples	10
1.7 Conclusion	11
2 Time Slotted Channel Hopping (TSCH) protocol	12
2.1 Introduction	12
2.2 Time Slotted Channel Hopping (TSCH)	12
2.2.1 Definition	13

2.2.2	How TSCH works ?	14
2.3	Orchestra	17
2.3.1	Definition	17
2.3.2	Orchestra Timeslot	17
2.3.3	Orchestra Slotframe	18
2.3.4	How Orchestra works ?.....	19
2.4	Comparison between TSCH and Orchestra	19
2.5	Security in TSCH	20
2.5.1	Channel Hopping.....	20
2.5.2	Time Synchronization	21
2.5.3	Slotframe and Schedule Control (Access Control)	21
2.5.4	Link-layer Security	21
2.5.5	Upper-Layer Key Management.....	21
2.6	Security challenges in TSCH	21
2.6.1	Time Synchronization	22
2.6.2	Scheduling Complexity.....	22
2.6.3	Limited Bandwidth.....	22
2.6.4	Join and Key Management.....	23
2.6.5	Interoperability and Standardization	23
2.7	Vulnerabilities of TSCH	23
2.7.1	Jamming attacks	23
2.7.2	Deny of Services(DoS) Attacks	24
2.7.3	Selective forwarding.....	25
2.7.4	Man-In-The-Middle Attack(MITM)	26
2.8	Main Security Methods for IIoT Networks	26
2.8.1	Blockchain.....	26
2.8.2	TLS	27
2.8.3	Multi-Factor Authenticated(MFA).....	27
2.8.4	Certificate Pinning.....	27
2.8.5	IDS and IPS	27
2.8.6	Data Integrity Verification	27
2.9	Conclusion	28

3	The proposed contribution	29
3.1	Introduction.....	29
3.2	Related work	29
3.2.1	TinyDTLS(2013)	29
3.2.2	Decryption Mechanism in the MAKE-IT Protocol(2020) .	30
3.2.3	A Hybrid Fibonacci-Based Affine-Hill Cipher(2020)	30
3.2.4	Protocol Based on Hash Functions and XOR Operations(2017)	31
3.3	MITM Attack.....	31
3.3.1	MITM impact.....	33
3.4	Contribution.....	34
3.4.1	Implemented functions	37
3.5	Conclusion	41
4	Implementation and Results	42
4.1	Introduction.....	42
4.2	Tools.....	42
4.2.1	Contiki-NG.....	42
4.2.2	Wireshark	43
4.2.3	ProVerif.....	44
4.2.4	Overleaf.....	45
4.3	Simulation scenarios	46
4.3.1	Simple scenario	46
4.3.2	Simple scenario with attack	47
4.3.3	Secure Scenario under Attack	48
4.3.4	Secure Scenario under Three Attacks.....	49
4.4	Performance Metrics	50
4.4.1	Average latency.....	50
4.4.2	Throughput	52
4.4.3	Energy consumption	54
4.4.4	Packet Delivery Ratio.....	55
4.5	Security evaluation.....	57
4.6	General discussion	59
4.7	Conclusion	60

