

CONTENTS

APPROVAL PAGE

SELF DECLARATION AGAINST PLAGIARISM

ABSTRAK	i
ABSTRACT	ii
DEDICATION	iii
ACKNOWLEDGMENT	iv
PREFACE	v
CONTENTS	vi
LIST OF FIGURES	ix
LIST OF TABLES	xi
1 INTRODUCTION	1
1.1 Background	1
1.2 Statement of Problem	7
1.3 Research Objectives	8
1.4 Scope of Work	9
1.5 Hypothesis	10
1.6 Research Methodology	10
2 OVERVIEW	12
2.1 Information Hiding in Computer Networks	12
2.2 MQTT	13
2.3 ASCON	15
3 DESIGN AND SIMULATION	16
3.1 System Model	16
3.1.1 MQTT-based Covert Channel	17

3.1.2	ASCON	18
3.1.2.1	ENCIPHERMENT PROCESS	18
3.1.2.2	DECIPHERMENT PROCESS	21
3.1.3	ZERO-WIDTH CHARACTERS (ZWC)	23
3.1.4	ASCON-HASH	24
3.2	Simulation & Analysis	27
3.2.1	Implementation Steps	27
3.2.2	Test	28
3.2.3	Measurement Parameters and Tools	29
4	RESULT & ANALYSIS	30
4.1	Algorithm	30
4.1.1	ASCON	30
4.1.1.1	Latency	30
4.1.1.2	Avalanche Effect	31
4.1.1.3	Computational Overhead	32
4.1.2	AES-GCM	33
4.1.2.1	Latency	34
4.1.2.2	Avalanche Effect	35
4.1.2.3	Computational Overhead	35
4.1.3	ChaCha20 Poly1305	36
4.1.3.1	Latency	37
4.1.3.2	Avalanche Effect	38
4.1.3.3	Computational Overhead	39
4.1.4	ASCON with ZWC	40
4.1.4.1	Latency	40
4.1.4.2	Avalanche Effect	41
4.1.4.3	Computational Overhead	42
4.1.5	AES-GCM with ZWC	42
4.1.5.1	Latency	43
4.1.5.2	Avalanche Effect	43
4.1.5.3	Computational Overhead	44
4.1.6	ChaCha20 Poly1305 with ZWC	45
4.1.6.1	Latency	46
4.1.6.2	Avalanche Effect	46
4.1.6.3	Computational Overhead	47
4.2	Comparison	48
4.2.1	ASCON, AES-GCM, & ChaCha20 Poly1305	49

4.2.1.1	Latency	49
4.2.1.2	Avalanche Effect	50
4.2.1.3	Computational Overhead	52
4.2.2	ASCON+ZWC, AES-GCM+ZWC, & ChaCha20 Poly1305+ZWC	53
4.2.2.1	Latency	53
4.2.2.2	Avalanche Effect	55
4.2.2.3	Computational Overhead	57
4.2.3	ASCON & ASCON + ZWC	58
4.2.3.1	Latency	58
4.2.3.2	Avalanche Effect	60
4.2.3.3	Computational Overhead	62
5	CONCLUSION AND FUTURE WORKS	64
5.1	Conclusion	64
5.2	Future Works	65
	REFERENCES	66