

CONTENTS

APPROVAL	ii
SELF DECLARATION AGAINST PLAGIARISM	iii
ABSTRACT	iv
ABSTRAK	v
DEDICATION	vi
ACKNOWLEDGMENTS	vii
PREFACE	viii
CONTENTS	ix
LIST OF TABLES	xii
LIST OF FIGURES	xiii
LIST OF NOTATIONS	xviii
1 INTRODUCTION	1
1.1 Background	1
1.2 Statement of the Problem	4
1.3 Objective	4
1.4 Research Question	5
1.5 State of the Art	5
1.6 Research Methods	6
1.7 Scope of the Thesis	8
1.8 Structure of Thesis	8
2 LITERATURE REVIEW	9
2.1 Internet of Things	9
2.1.1 Internet of Things Protocol	9
2.1.2 Internet Of Things Protocol Security	13
2.1.3 Internet of Things Security Thread	14

2.1.4	Internet of Things Constraint Device	16
2.2	Related Studies	19
2.2.1	Event-Based Control System	19
2.2.2	Fisher-Yates Shuffle	19
2.2.3	ElGamal Cryptography System	20
2.2.4	TAMARIN PROVER	21
2.2.5	Pseudo-Random Generator	22
2.3	Authentication Security on MQTT Protocol	23
2.3.1	Supported with TLS	23
2.3.2	Without Using TLS	25
2.3.3	Authentication Security on MQTT Protocol Summary	28
3	PROTOCOL DESIGN	33
3.1	Introduction	33
3.2	Assumption	33
3.3	Conceptual Framework/Paradigm	34
3.4	Improvement of MQTT Authentication Mechanism	37
3.4.1	Basic Idea	38
3.4.2	Proposed Method	38
3.5	Protocol Model	45
3.5.1	Existing MQTT Protocol	46
3.5.2	Proposed MQTT Protocol	48
3.6	Validation Model	52
3.6.1	Existing MQTT protocol Validation Model	52
3.6.2	Proposed MQTT protocol Validation Model	54
4	CORRECTNESS OF SECURITY PROTOCOL	57
4.1	Validation Scenario	57
4.2	Existing MQTT Protocol Model Prove	59
4.2.1	Registration Phase	59
4.2.2	Publish Phase	59
4.3	Proposed MQTT Protocol Model Proof	60
4.3.1	Proposed MQTT Protocol Specification	60
4.3.2	Connection Phase	62
4.3.3	Authpublish Phase	68
4.4	Summary Validation Protocol Model	70

5	PROTOCOL IMPLEMENTATION	72
5.1	Pre-conditions	72
5.2	Protocol Rules	72
5.3	Client Algorithm	74
5.4	Broker Algorithm	77
5.5	Broker and Client Implementation	78
5.6	Algorithm Performance	83
5.7	Memory Utilization	84
6	CONCLUSION AND RECOMMENDATIONS	91
6.1	Conclusions	91
6.2	Recommendations	91
6.3	Future Work	92
	BIBLIOGRAPHY	93
	Appendices	98
A	MISCELLANEOUS	100
A.1	Random Test from Proposed Pseudo-random Generator Algorithm . .	100