

# **CONTROLLED LINK ESTABLISHMENT ATTACKS ON DISTRIBUTED SENSOR NETWORKS AND COUNTERMEASURES**

DISSERTATION

Submitted to the University Graduate School  
University of Technology, Sydney



In fulfilment of the requirements for the degree of  
Doctor of Philosophy in Engineering and Information Technology

BY

**THANH DAI TRAN**

B.Eng., Hanoi University of Science and Technology, 2005  
M.Eng., Kyung Hee University, 2007

Sydney, December 2010

## **CERTIFICATE OF AUTHORSHIP/ORIGINALITY**

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Signature of Candidate

.....

*To the memory of my dearest grandmother and grandfather*

## **Abstract**

For over a decade, the boom in research, development, and application of distributed sensor networks (DSNs) has enabled their pervasion in many aspects of human life. In such networks, collaboration among sensor nodes plays a key role in resolving distributed tasks. Typically, traditional cryptographic protections such as encryption and authentication are utilised to secure this collaboration against malicious attacks.

Unfortunately, this secured collaboration is undermined by an attack named Controlled Link Establishment Attack (CLEA). To launch CLEA, the attacker first captures and compromises a limited number of nodes to extract their secret information. Next, the attacker repetitively utilises the compromised nodes and secret information to create overwhelming controlled links with legitimate nodes. These controlled links are then used to subvert network-wide cooperative efforts or gain the control of the network.

This thesis comprises two parts: CLEA investigation and development of new countermeasures against CLEA. The investigation involves (i) identifying and characterising CLEA based on the examination of actual instances (ii) undertaking a literature review of existing key establishment schemes for DSNs and pinpointing their vulnerability to CLEA (iii) performing a comprehensive survey of existing countermeasures applicable to defend against CLEA, and (iv) studying the feasibility of CLEA. The conclusion drawn from this investigation is that although CLEA is a real and serious threat, no sufficiently robust and efficient countermeasures have been found in the literature to defeat the attack.

The development starts with a study of related works that can be used as building blocks for new countermeasures followed by their description. The proposed countermeasures can be classified into either protection-based approach or detection-based approach. Following the first approach, three schemes focusing on protecting key establishment schemes by leveraging a cryptographic one-way hash chain are developed. Following the second approach, three schemes are introduced. The first two schemes are capable

of detecting and stamping out CLEA attempts from the beginning. The final scheme is even more powerful than the previous ones with the ability to identify and revoke the source of the attack.

Finally, thorough evaluations of the proposed schemes in respect of security features and performance overheads are carried out through intensive analyses, simulations, implementation, and extensive comparison with other schemes. The findings from these evaluations indicate that the proposed schemes achieve robust and effective prevention, detection, and revocation capability against CLEA with reasonable overheads. In comparison, the protection-based schemes are more performance efficient but less security effective than the detection-based schemes. They are all suitable for use in the current generation of sensor nodes.

## **Acknowledgements**

A major research project like this is never entirely the work of the author. Over my doctoral candidature, I have been receiving support and encouragement from different people in various ways. My thesis would not have been completed without these support and encouragement.

First and foremost, I wish to express my deepest gratitude towards my supervisor, Dr. Johnson Agbinya, who has been my supervisor since the beginning of my study. Johnson has always been a great mentor and above all good friend, giving me tremendously valuable suggestions, thoughtful guidance, and continuous support. His excellent ideas and feedback from numerous face-to-face discussions and group meetings have assisted me in selecting my thesis topic, formulating research questions, developing new methodology for these questions, publishing my work, and completing this thesis. His research expertise and community network as well as his financing for my publications and conference attendance have been very helpful. His dedication to research and vastness of knowledge have set a standard I long to meet for the years to come. It is my great honour to receive his guidance and direction towards the accomplishment of this dissertation.

My sincere thanks are extended to my co-supervisor, Dr. Adel Ali Al-Jumaily and my previous co-supervisor, A/Prof. Elaine Lawrence, for their advice and support throughout my thesis.

I am indebted to the Faculty of Engineering and Information Technology (FEIT), UTS in general and Prof. Hung Nguyen in particular for having offered me a Faculty of Engineering Postgraduate Research Scholarship. Without this scholarship, my dream of studying in Australia would not have been fulfilled. I would like to extend further my thanks to the Vice Chancellor's Conference Funding and FEIT Travel Funding committees for their generous financial support of my conference trips.

My keen appreciation goes to Ms. Phyllis Agius, Research Administration Officer, for her dedicated assistance. She has always been my first point of contact whenever I had difficulties with paperwork and administrative details.

Moving toward more personal acknowledgments, I owe special gratitude to my closest friend Richard Turnell for his true companionship, unwavering support, and warm encouragement. He has made me feel at home and devoted countless hours to improving my English skills, proofreading my paper drafts, teaching me how to drive cars, and above all helping me absorb and value Australian culture. He has been my point of reference for difficulties I faced in my daily life and acted as my main source of hilarity, vitality, and exhilaration. Without his effort, I would not have concentrated on my study and finished it on time.

My heartfelt gratitude towards my beloved fiancée, Giang, cannot be expressed in words. Her eternal love, understanding, and sharing are always a powerful source of inspiration and energy for my study. She has helped me keep balance in my mind and fetched me happiness in life when I lost track of my research and felt disappointed and stressed. I do not hesitate to say that, with her by my side, I am not alone on this so-called 'lonely journey'.

Last, but most important, is the dedication of this thesis to my dearest parents and younger sister for their never-ending love, unconditional support, and tireless sacrifices. It is no exaggeration to say that I am very lucky to have such marvellous family members. I hope they will read this work some day and be proud of me.

## **Table of Contents**

<b>CERTIFICATE OF AUTHORSHIP/ORIGINALITY.....</b>	<b>ii</b>
<b>Abstract.....</b>	<b>iv</b>
<b>Acknowledgements.....</b>	<b>vi</b>
<b>Table of Contents .....</b>	<b>viii</b>
<b>List of Figures.....</b>	<b>xiii</b>
<b>List of Tables .....</b>	<b>xvi</b>
<b>Chapter 1: Introduction .....</b>	<b>1</b>
1.1 Distributed Sensor Networks .....	1
1.1.1 Characteristics .....	3
1.1.2 Applications .....	5
1.2 Problem Scope and Definition .....	7
1.3 Thesis Objectives .....	11
1.4 Design Challenges.....	12
1.5 Thesis Contributions .....	13
1.6 The Organisation.....	15
1.7 Publications Related to the Thesis .....	15
1.7.1 Book Chapters .....	15
1.7.2 Journal Articles .....	16
1.7.3 Peer Reviewed Conference Papers.....	16
<b>Chapter 2: Models and Assumptions .....</b>	<b>18</b>
2.1 Network Assumption and Model .....	18
2.2 Security Model .....	21
2.3 Adversary Assumptions .....	22
2.4 Notation.....	24
<b>Chapter 3: Literature Review .....</b>	<b>28</b>
3.1 Key Establishment in Sensor Networks.....	28

---

3.1.1 Taxonomy of Key Establishment Schemes.....	28
3.1.1.1 Symmetric Techniques vs. Asymmetric Techniques.....	29
3.1.1.2 Key Transport Protocols vs. Key Agreement Protocols .....	30
3.1.1.3 Static Schemes vs. Dynamic Schemes.....	31
3.1.1.4 Network Topology Dependent Schemes.....	31
3.1.2 Vulnerability of Key Establishment Schemes to CLEA.....	32
3.2 Node Replication Attack.....	33
3.3 Key Swapping Collusion Attack.....	36
3.4 Indirect Countermeasures .....	37
3.5 Direct Countermeasures .....	40
3.5.1 Witness-Based Detection Schemes .....	41
3.5.2 SET: Set Operation Based Detection Scheme .....	46
3.5.3 Bloom Filter Based Detection Scheme .....	49
3.5.4 Randomly Directed Exploration Based Scheme.....	51
3.5.5 Sequential Analysis Based Detection Scheme.....	52
3.5.6 Random-Walk Based Detection Approach.....	53
3.6 Chapter Remark .....	55
<b>Chapter 4: Background.....</b>	<b>56</b>
4.1 Cryptographic Primitives .....	56
4.1.1 Symmetric Key Ciphers .....	57
4.1.2 Cryptographic Hash Functions.....	61
4.2 Message Authentication in DSNs .....	62
4.2.1 Symmetric-Key Approaches .....	63
4.2.2 Public-Key Approaches .....	66
4.3 DoS Prevention for Broadcast Authentication.....	68
4.4 Anti-Jamming Techniques .....	70
4.5 Secure Localisation Algorithms.....	71
4.6 Secure Time Synchronisation Protocols .....	72
4.7 Chapter Remark .....	73
<b>Chapter 5: Feasibility of Controlled Link Establishment Attack .....</b>	<b>74</b>
5.1 Feasibility of Node Compromise .....	74
5.2 Methods for Repetitive Use of Compromised Secret Information .....	76

5.2.1 Secret Information Cloning.....	76
5.2.2 Short-Distance Swapping.....	77
5.2.3 Long-Distance Swapping.....	78
5.2.4 Mixed-Distance Swapping.....	80
5.3 CLEA Prototype Implementation .....	80
5.3.1 Assumptions.....	80
5.3.2 Software Tools and Hardware Devices.....	81
5.3.3 Implemented Applications .....	82
5.3.4 Operation of the Demonstration.....	85
5.4 Chapter Remark .....	88
<b>Chapter 6: Secret Information Protection Based Countermeasures .....</b>	<b>89</b>
6.1 OWHCBS: One-Way Hash Chain Based Scheme.....	89
6.1.1 Overview .....	89
6.1.2 Detailed Description of OWHCBS .....	91
6.1.2.1 System Initialization Phase .....	91
6.1.2.2 First Generation Deployment Phase .....	91
6.1.2.3 Successive Generation Deployment Phase .....	92
6.1.3 Security Analysis .....	93
6.1.3.1 Cascading Impact of CLEA .....	93
6.1.3.2 Probability of the $h$ th Generation Being Vulnerable.....	95
6.1.4 Performance Analysis .....	96
6.1.5 Limitations .....	98
6.2 DOWHCBS: Diversified OWHC Based Scheme.....	98
6.2.1 Overview .....	98
6.2.2 Detailed Description of DOWHCBS .....	99
6.2.2.1 System Initialization Phase .....	99
6.2.2.2 First Generation Deployment Phase .....	100
6.2.2.3 Successive Generation Deployment Phase .....	101
6.2.3 Security Analysis .....	102
6.2.3.1 Analytical Analysis .....	102
6.2.3.2 Further Security Discussion .....	107
6.2.3.3 Simulation Analysis .....	107
6.2.4 Performance Evaluation.....	108

6.2.5	Limitations .....	111
6.3	HOWHCBS: Hidden OWHC Based Scheme .....	112
6.3.1	Overview .....	112
6.3.2	Detailed Description of HOWHCBS .....	113
6.3.2.1	System Setup.....	113
6.3.2.2	Same Generation Key Establishment.....	114
6.3.2.3	Different Generation Key Establishment.....	115
6.3.3	Security Analysis .....	116
6.3.4	Performance Evaluation .....	119
6.3.4.1	Communication Cost.....	119
6.3.4.2	Computational Cost.....	120
6.3.4.3	Storage Cost .....	122
6.4	System Implementation.....	123
6.5	Chapter Remarks .....	126
<b>Chapter 7: Per Node Deployment Based Detection Countermeasures .....</b>		<b>127</b>
7.1	Design Goal and Overview .....	127
7.1.1	Design Goal.....	127
7.1.2	Overview .....	128
7.2	Naïve Detection Scheme .....	128
7.2.1	Assumptions.....	128
7.2.2	Initialisation of Security Server and Sensor Nodes .....	130
7.2.3	Pre-programming of Sensor Nodes.....	131
7.2.4	Detection of CLEA at Sensor Nodes .....	132
7.2.5	Discussion .....	132
7.3	Adaptive Detection Scheme .....	133
7.3.1	Assumptions.....	133
7.3.2	Initialisation of Security Server and Nodes .....	134
7.3.3	Deployment of Sensor Nodes and Detection of CLEA .....	134
7.3.4	Security Analysis and Discussion .....	137
7.4	Extended Adaptive Detection Scheme.....	139
7.4.1	Assumptions.....	139
7.4.2	Detection of CLEA at Sensor Nodes .....	140
7.4.3	Security Analysis and Discussion .....	142

7.4.3.1 Finding Detection Rate .....	142
7.4.3.2 Counteracting Masked-Replication Attack .....	145
7.4.3.3 Thwarting Node Revocation Attack.....	146
7.4.3.4 Other Security Vulnerabilities.....	147
7.5 Evaluations and Further Comparison.....	147
7.5.1 Performance Evaluation.....	148
7.5.1.1 Analytical Evaluation.....	148
7.5.1.2 Simulations.....	149
7.5.2 Further Comparison .....	151
7.6 Chapter Remarks .....	153
<b>Chapter 8: Conclusions and Future Work .....</b>	<b>154</b>
8.1 Conclusions .....	154
8.2 Future Work .....	157
<b>References .....</b>	<b>158</b>
<b>Appendix Glossary .....</b>	<b>175</b>

## List of Figures

Figure 1.1: Basic concept of the thesis objectives .....	11
Figure 2.1: Illustration of local broadcast communication in DSNs.....	20
Figure 2.2: Illustration of connection in a DSN and corresponding key-sharing graph	22
Figure 3.1: Classification of key establishment schemes in sensor networks .....	29
Figure 3.2: Illustration of node replication attack.....	34
Figure 3.3: Line-selected multicast: The attacker is assumed to have created a replica of $r$ , $r'$ . The storage of the replicas' location claims at nodes en route to the witnesses ( $w_i$ s and $w_i'$ s) results in an intersection at $\chi$ .....	43
Figure 3.4: The construction of seven subsets in accordance with the ESMIS algorithm .....	47
Figure 3.5: An illustration of a Bloom filter, representing the set $\{a, b, c\}$ . The arrows show the positions in the bit array to which each set element is mapped. The element $d$ is not in the set $\{a, b, c\}$ , because it hashes to one bit-array position containing 0 ( $m = 12$ , $k = 3$ ).....	50
Figure 3.6: Illustration of random-walk based detection approach.....	54
Figure 4.1: The concept of a symmetric-key block cipher.....	58
Figure 4.2: Illustration of $\mu$ TESLA.....	63
Figure 4.3: Illustration of the basic ALPHA.....	64
Figure 4.4: An illustrative anchor distribution tree for eight sensor nodes.....	65
Figure 4.5: Illustration of dynamic window scheme.....	69
Figure 5.1: An illustration of the short-distance secret information swapping method.	78
Figure 5.2: The illustrations of long-distance collusion attack.....	79
Figure 5.3: The network scenario of the CLEA prototype implementation .....	81
Figure 5.4: The component relationship within RandPKS .....	83
Figure 5.5: The component relationship within CtrlledNode .....	84
Figure 5.6: The hardware devices used in the demonstration.....	86

Figure 5.7: The completion of the hello message exchange between nodes 1(4) and 2(3) with the failure of key establishment .....	87
Figure 5.8: The success of short-distance swapping CLEA .....	87
Figure 6.1: An example of the deployment model.....	90
Figure 6.2: The impact of CLEA in the three scenarios .....	94
Figure 6.3: Probability of the $h$ th generation being vulnerable.....	96
Figure 6.4: Cryptographic energy consumption.....	97
Figure 6.5: Illustration of the KEK diversification .....	99
Figure 6.6: (a) First generation deployment phase flow chart (b) Generation addition phase flow chart .....	100
Figure 6.7: Illustration of the interested attack period .....	104
Figure 6.8: Probability of at least one sensor node of a generation being captured/compromised over the interval $Y_v$ .....	105
Figure 6.9: Probability of capturing a node during the interval $Y_v$ after deployment times .....	108
Figure 6.10: Communication overheads of each sensor node with various settings ....	110
Figure 6.11: Computational overheads per sensor node with varied deployment scenarios .....	111
Figure 6.12: Illustration of node $S_{u,v}$ 's initialisation and setup.....	113
Figure 6.13: Different generation key establishment under HOWHCBS's protection. ....	115
Figure 6.14: The upper bound of the probability of $K_c$ being compromised over the network lifetime .....	118
Figure 6.15: The estimated number of messages sent per node of each generation over the network lifetime .....	120
Figure 6.16: The estimated computational costs per node of each generation over the network lifetime .....	122
Figure 6.17: The component relationship in the implementation of HOWHCBS .....	124
Figure 6.18: The component relationship in RfmToHello.....	125
Figure 6.19: The component relationship in SJCipherC.....	126
Figure 7.1: Counter value increment in sensor nodes following the naïve scheme.....	129

---

Figure 7.2: The counter value increment in sensor nodes following the adaptive detection scheme .....	135
Figure 7.3: Counter value transition in $S_u$ deployed over $\Delta T_i$ .....	136
Figure 7.4: Example of detection of CLEA at sensor nodes.....	141
Figure 7.5: Influence of $r$ on $P_{c_{ib}}$ with different network sizes .....	144
Figure 7.6: Influence of $\alpha$ on $P_{c_{ib}}$ with different network sizes .....	145
Figure 7.7: Average amount of communication per node in three approaches .....	150
Figure 7.8: Average computation overhead per node in three approaches.....	150
Figure 7.9: Average memory storage per node in three approaches.....	151

## **List of Tables**

Table 2.1: List of symbols used in the thesis .....	25
Table 3.1: Classification of key establishment schemes in terms of their vulnerability level to CLEA .....	33
Table 3.2: Summary of scheme costs.....	44
Table 4.1: Common elements in block ciphers [136] .....	60
Table 6.1: Comparison of storage requirements between two schemes .....	109
Table 6.2: Storage cost of HOWHCBS (in byte).....	123
Table 7.1: Summary of performance overheads .....	149
Table 7.2: Comparison with other schemes in terms of security and performance .....	152