UNIVERSITI PUTRA MALAYSIA

OBFUSCATABLE AGGREGATABLE SIGNCRYPTION SCHEME WITH PadSTeg FOR UNATTENDED DEVICES IN IoT SYSTEMS

INYAMA VICTOR UWADIEGWU

FSKTM 2019 19

UNIVERSITI PUTRA MALAYSIA

Obfuscatable Aggregatable Signcryption Scheme with PadSteg for Unattended Devices in IoT Systems (JUNE 2019)

By

INYAMA VICTOR UWADIEGWU

Dissertation Submitted to the School of Graduate Studies, Universiti PutraMalaysia, in Fulfilment of the Requirements for the Degree of

Master of Information Security

June 2019

DEDICATIONS

This project paper is dedicated to my lovely parents for their endless love, support, patience, and encouragement throughout my education carrier. To each of who has taught me or gave me advice...teachers. Dedicate this work ...

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Information Security

Obfuscatable Aggregatable Signcryption Scheme with PadSteg

For Unattended Devices in IoT Systems

By

INYAMA VICTOR UWADIEGWU

JUNE 2019

Supervisor: DR. Azizol Abdullah

Faculty: Computer Science and Information Technology

Abstract

Obfuscatable Aggregatable Signcryption (OASC) is the combination of cryptography technique such as digital signature with data encryption and obfuscation to protect data in the IoT system. It is efficacious to protecting the confidentiality and integrity of communication in Internet of Things (IoT) system. Wireless Sensor Network (WSN) is now an inevitable component of the Internet of Things (IoT), this integration creates new security challenges that exist between the sensor nodes and to the sink or internet host. For instance, when a sensor node is transmitting data from one node to another there is inadequate security mechanism which an intruder or a man in the middle (MITM) attack can capture the ciphertext to get secrete keys in other to decrypt the ciphertext. The aggregatable signcryption that enables special signcryption ciphertexts intended for the same destination be assembled in a compressed single ciphertext while maintaining the same security standards in the system. The procedure is then obfuscated aimed at making information more difficult to be understood by human being for the purpose of security and privacy of the program/information while commonly maintaining its computational

functions. Unfortunately, most of these devices are left unattended or in remote places which gives an attacker a comfortable scenario to not only intercept transmission within range but also have physical access to components without been caught. This leaves some vulnerability during communication. In other to achieve the security enhancement, efficiency and reduce communication overheads by using small security parameter and the effect of such a security complexity trade-off. Motivated by this issue, we propose Signcryption Obfuscatable and Steganography-PadSteg (SOS) algorithm as a solution. Having Signcryption (digital signature and encryption) at each node is the baseline of security but the caveat is that the computational power of these components means both mechanisms will not be of highest security level hence the need to protect the information as it travels for a final process of obfuscation. This is achieved by employing a type of Network Steganography known as PadSteg and hiding these data in padded segments of choice protocols (ARP/TCP/UDP/ICMP) which will not be visible to an observer. At the end of this thesis, we achieved the result to solve the security issues mention above and to enhance the security in IoT system. The simulation result on different nodes showed that the proposed algorithm on Signcryption Obfuscatable and Steganography-PadSteg (SOS) performs 25% reasonably well as expected. The scheme will be useful in a various scenario of IoT environment where data is sent from unattended nodes to the destination known as a sink or receiver.

ACKNOWLEDGMENTS

First and foremost, praise be to God Almighty through whose mercy and favours all good things are accomplished.

I would like to thank my parents. I am deeply indebted to them for their unconditional support and sacrifice for so many years. I would like to express the deepest appreciate and sincerest gratitude to my supervisor, Dr Azizol Abdullah for his patience and truthful guidance through all the steps of research and writing dissertation. I attribute the level of my master's degree to his encouragement and effort he spent for helping me accomplishing this work. I thank and appreciate the valuable effort of my lecturers at Faculty of Computer Science and Information Technology (FSKTM), Universiti Putra Malaysia (UPM), Malaysia.

Finally, I owe many thanks to my friends for their love, dedication, help, and encouragement in those critical moments along this journey. Words are not enough to express my gratitude.

This dissertation was submitted to the Information Security Department, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of **Master of Information Security**.

Dr. Azizol Abdullah
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia

Date:

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.

(Signature)

Inyama Victor Uwadiegwu / GS50350

Date:

TABLE OF CONTENTS

Page

DEDICATIONS i

ABSTRACT ii

ACKNOWLEDGMENTS iv

APPROVAL v

DECLARATION vi

LIST OF TABLES ix

LIST OF FIGURES x

CHAPTER **1**

1.1 INTRODUCTION 1

1.2 Background and Motivation 1

1.3 Problem Statement 3

1.4 Research Objectives 4

1.5 Research Scope 5

1.6 Thesis Structure 5

2 LITERATURE REVIEW 7

2.1 Introduction 7

2.2 Signcryption 7

2.2.1 Digital signature 7

2.2.2 Encryption 8

2.3 Aggregate signature 9

2.3.1 Aggregatable signcryption 10

2.4 Program obfuscation 13

2.5 Steganography Method PadSteg 15

2.6 Summary 18

3 RESEARCH METHODOLOGY 21
3.1 Introduction 21
3.2 Research Process 21
3.3 Research Framework 22
3.4 Experiment Design 25
3.5 Mathematical Structures 27
3.6 Building Blocks Scheme 30
3.7 Summary 31
4 DESIGN AND IMPLEMENTATION 32
4.1 Introduction 32
4.2 Proposed SOS-PadSteg Framework 33
4.3 Commencement 34
4.4 Identification and Preparation 34
4.5 Summary 40
5 RESULTS AND FINDINGS 41
5.1 Introduction 41
5.2 COMPUTATIONAL COST ANALYSIS 43
5.3 Comparative study between OASC technique and proposed SOS-PadSteg techniques with other techniques. 48
6 CONCLUSION AND FUTURE WORK 50
6.1 CONCLUSION 50
6.2 Future Work 51
7 References 52

APPENDICES 57

LIST OF TABLES AND LIST OF FIGURES

1. Figure 2-1 Aggregatable signcryption in the IoT 10
2. Figure 3-1 Research Framework 22
3. Figure 3-2 SOS-PadSteg methodology flowchart 24
4. Figure 3-3 SOS methodology flowchart 25
5. Figure 4-1 Flowchart of proposed solution 33
6. Figure 4-2 Flowchart SOS Algorithm 36
7. Figure 4-3 Data hidden group activation phase in the IoT 38
8. Figure 5-1 Simple Data Analysis in IoT Security 42
9. Figure 5-2 Padding Analysis 43
10. Figure 5-3 Comparison of communication costs with respect to ciphertext 47
11. Figure 5-4 Comparison of communication costs with respect to aggregated ciphertext 48

LIST OF TABLES

12. Table 1 Summary of The Features of SOS-PadSteg 18

CHAPTER 1

1.1 INTRODUCTION

This chapter commences with an overview of the research topic and explains the motivation for this work. The problem statement is then identified followed by the research objectives, and scope. At the end of this chapter the organization of the dissertation is provided.

1.2 Background and Motivation

There are vast varieties of technologies that have a great influence on our daily life, just like the two sides of a coin they offer both advantage and disadvantage which Internet of Things (IoT) is not an exception. In today's modern world, IoT associated with computer resources is increasingly shifting toward Internet of Everything (IOE) which provides transmission using a set of wireless network sensor over the Internet. The Internet of Things (IoT) can be referred to as the interconnectivity of "things"-devices embedded with integrated circuits and other electronic components sensors, and operating software to help achieve their purpose by providing greater value and functionality through communication and resource sharing with vendors, operators, and other interconnected nodes. In the IoT paradigm, most of these IoT components like electronic tag readers, CCTVs traffic cameras, sensors, road-side units are positioned in remote areas and also nontrustable environments, such as roads, highways, countryside, forests, parking spaces, animal reserves and wild fields etc., where their physical security cannot be guaranteed thus operating in an unattended environment and condition making them vulnerable to device capture attack.

As IoT is the leading technology in the world nowadays, it is absolutely important to know that security of IoT devices is highly needed to secure the data during

transmission. it will be also useful to conceptualize IoT security as a spectrum of device vulnerability. As we increasingly connect devices to the Internet in IoT, multiple new opportunities to exploit potential security vulnerabilities grow proportionally. The conventional issue of security breach owing to exposed of confidential information is one of the main security issues among IoT devices when people don't believe that their connected devices such as smart TV's, smart phones, other home appliances and their information are reasonably secure from misuse or harm, the resulting diminution of trust will cause a reluctance from accepting IoT globally. The intrinsic distributed and heterogeneous nature of IoT objects coupled with poorly secured IoT devices could serve as endangered entry points for cyber-attacks such as interception, eavesdropping, modification of confidential data where intruder might re-program a device or cause it to malfunction once gaining access to the interconnected IoT devices thereby resulting in security breach.

Also, it should be noted that these devices communicate and transmit information with one another over wireless communication channels which will be passed on to next devices and so on till eventually the information if deposited at the sinks, such as gateway devices or even drones. For that matter, it is imperative to adopt a secure form of processing and transmitting this valuable information to establish confidentiality and integrity.

The motivation for conducting research on security in IoT environment can be summarized in the following points. IoT is increasingly being deploying to every sector like businesses, Hospitals, industries and government users to transmitting amounts of data from one node to another until it each to sink or cloud for storage. While, IoT applications is increasingly being accessed with mobile electronic devices. Criminals are embracing the opportunity to capture illicit data during the

transmission, which contributes to difficulties in proving IoT security and interaction.

by this issue, Y. Shi et al (2017) explained obfuscatable aggregatable signcryption scheme (OASC) together with an obfuscator for the signcryption algorithm, which has been designed by taking into account that the computational and communication costs should be sufficiently small (light-weighted) to fit applications in resource-constrained embedded devices. The proposed obfuscator can protect signcryption programs from key-extraction attacks by transforming the programs into unintelligible obfuscated programs. The scheme's security features with respect to obfuscation, confidentiality, and unforgeability have been theoretically proved. It motivated us to enhance the security of IoT by applying signscryption obfuscation steganograpgy-PaddStep (SOS) to hardening the security when an intruder or man in the mild attack threatening to capture the data and decipher the signcryption data on unattended devices.

1.3 Problem Statement

According to my research on (Y. Shi et al 2017) the OASC does not meet the security features in IoT during data transmission from one node to another node in IoT system. One solution is introduced by Ria Das and Indrajit Das (2016) called MSB-LSB Substitution to solve these security features however their solution has difficult in implementing because of computational nature of MSB-LSB to execute in IoT system and needs to be analyzed. Since the author Y. Shi et al (2017) has proposed security measures at source nodes (Signcryption) and Destination (Obfuscation). The major limitation in the proposed system is that data coming from nodes still have weak security or inadequate security and are vulnerable since obfuscation takes place after the final aggregation at the sink. It is imperative to understand that these nodes in a WSN are very lightweight both in hardware and software therefore they don't have the computational power to

perform some of the security mechanisms at high level. With that in mind, we expect at every node to have data that has undergone signcryption but as explained above, both encryption and digital signature are not done on a high level so will still be susceptible to cryptanalysis. Secondly, there is security complexity trade-off in IoT environment. Y. Shi et al (2017) OASC methods have the poorest efficiency of any technique, since multiple sensors expend energy on sending data like jamming protocol. In probabilistic signcryption, secure channel, and aggregatable transmission, all the sensors in the IoT system are assumed to be active at once. the comparison of the various node's security schemes. It does not require the exchange of secret encryption matrices that are unknown to eavesdroppers. it does not need a node to waste energy by transmitting dummy or jamming

1.4 Research Objectives

In order to successfully solve the issue of data confidentiality loss in IoT, we offer a security technique based on a combined approach of signscryption Obfuscatable and Steganography-paddSteg (SOS) techniques. This security measures like encryption, steganography and digital signature are essential basic requirements to avoid data leak or manipulation through passive or active attacks. It has become easier to attain a vibrant and scalable composition of both signature and encryption, also coined as signcryption, which has been widely used to protect both the confidentiality and unforgeability of information disseminated over non-trustworthy or open channels as follows below.

1 The objective of this research is to implement an enhancement of secure data communication scheme that will enhance the confidentiality and integrity levels of the data in IoT system.

2 To propose an enhancement of Signcryption Obfuscation and Steganography-PadSteg (SOS) algorithm to solve issues of efficiency, reduce communication overheads and computational in IoT

1.5 Research Scope

One of the important methods to implement security primitive in IoT for attacks on nodes is through SOS, and this method called PadSteg to secure data during transmission between node to node until reach node leaf or workstation, cloud, and techniques they used. Our scope is to protect or harden security between sensors from an intruder

The research was undertaken using WSN from one sensor to another sensor. the research was limited to the most popular simulation tool known as ns2, applied signcryption, obfuscation and steganography-padSteg at the time of undertaking this study. However, any other application may have different results and findings. Additionally, the research was undertaken using the proposed SOS method on the IoT components.

1.6 Thesis Structure

The project consists of an introduction and follows the chapters which describe the research in detail, and finally summarize the findings. The project also includes an overall summary, acknowledgements, table of contents, list of figures, tables, and a glossary of technical terms.

Chapter 1 introduces the overall topic, including background information regarding IoT, Security and the issues faced security in IoT. The problem statement of the research is discussed, and the objectives are listed. To conduct the objectives. Then, the limitation of this research is explained. In the end, the structure of the research is outlined.

Chapter 2 we studied the current literature which focusing on IoT, digital security such as signcryption and steganography. the Issues relating to sensor deployment, security and analysis. Additional issues are generally described, and a summary concludes the chapter.

Chapter 3 The aims are to clarify the research methodology applied to the project. The research methodology for each research question is detailed and answered. Finally, a summary concludes this chapter.

Chapter 4 This section is outlining the proposed solution of security issues in IoT system and the way this can be applied to solve the problem of security. Each step of the algorithm has been explained (Identification & Preparation, Analysis,).

Chapter 5 describes the procedures of the framework for the analysis result obtain and interpretation of the result from SOS. In each case, the data remnants on the sensors are first examined using the proposed framework. Next, the IoT device is examined to further assess the framework and to determine the data. The data regarding on transmission are then explained and listed at the end of each process.

Chapter 6 the conclusion of the overall research. In the first section, the research is outlined, detailing the way how the objectives and contributions achieved. Next, a summary of the research and the areas for future research are then provided.

References

A. Yin and H. Liang, “Certificateless hybrid signcryption scheme for secure communication of wireless sensor networks,” Wireless Pers. Commun., vol. 80, no. 3, pp. 1049–1062, 2015.

A. Newell, H. Yao, A. Ryker, T. Ho, and C. Nita-Rotaru, “Node-capture resilient key establishment in sensor networks: Design space and new protocols,” ACM Comput. Surveys, vol. 47, no. 2, pp. 1–34, 2014.

A. W. Dent, “Aggregate signcryption,” IACR cryptology ePrint archive 2012. [Online]. Available: https://eprint.iacr.org/2012/200.pdf

B. Barak et al., “On the (Im)possibility of obfuscating programs,” J. ACM, vol. 59, no. 2, Apr. 2012, Art. no. 6.

B. Jankowski, W. Mazurczyk, K. Szczypiorski, Information Hiding Using Improper Frame Padding, Submitted to 14th International Telecommunications Network Strategy and Planning Symposium (Networks 2010), 27-30.09.2010, Warsaw, Poland

C. Barak et al., “On the (Im)possibility of obfuscating programs,” in Proc.Adv Cryptol. (CRYPTO), Santa Barbara, CA, USA, 2001, pp. 1–18.

C. Collberg, C. Thomborson, and D. Low, “A taxonomy of obfuscating transformations,” Dept. Comput. Sci., Univ. Auckland, Auckland, New Zealand, Tech. Rep. 148, 1997, pp. 1173–3500.

C. S. Collberg and C. Thomborson, “Watermarking, tamper-proofing, and obfuscation—Tools for software protection,” IEEE Trans. Softw. Eng., vol. 28, no. 8, pp. 735–746, Aug. 2002.

C. Lin, G. Wu, C. Yu, and L. Yao, “Maximizing destructiveness of node capture attack in wireless sensor networks,” J. Supercomput., vol. 71, no. 8, pp. 3181–3212, 2015.

D. H. Yum and P. J. Lee, “Exact formulae for resilience in random key predistribution schemes,” IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1638–1642, May 2012

D. Boneh, C. Gentry, B. Lynn, and H. Shacham, “Aggregate and verifiably encrypted signatures from bilinear maps,” in Proc. Int. Conf. Theory Appl. Cryptograph. Techn., Warsaw, Poland, 2003, pp. 416–432.

D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the Weil pairing,” J. Cryptol., vol. 17, no. 4, pp. 297–319, 2004

D. Kapoor Sarmah and Neha Bajpai “Proposed System for data hiding using Cryptography and Steganography Proposed System for data hiding using Cryptography and Steganography” 2010 International Journal of Computer Applications

E. Souza et al., “End-to-end authentication in under-water sensor networks,” in Proc. ISCC, Guangzhou, China, 2013, pp. 299–304.

F. S. Babamir and Z. Eslami, “Data security in unattended wireless sensor networks through aggregate signcryption,” KSII Trans. Internet Inf. Syst., vol. 6, no. 11, pp. 2940–2955, 2012.

F. Li and P. Xiong, “Practical secure communication for integrating wireless sensor networks into the Internet of Things,” IEEE Sensors J., vol. 13, no. 10, pp. 3677–3684, Oct. 2013

Fisk, G., Fisk, M., Papadopoulos, C., Neil, J.: Eliminating Steganography in Internet Traffic with Active Wardens, In Proc: 5th International Workshop on Information Hiding, Lecture Notes in Computer Science: 2578, 2002, str. 18–35

H. Wang, Z. Liu, Z. Liu, and D. S. Wong, “Identity-based aggregate signcryption in the standard model from multilinear maps,” Front. Comput. Sci., vol. 10, no. 4, pp. 741–754, 2016.

J. Yi, L. Jianping, and X. Anping, “Certificateless aggregate signcryption scheme for wireless sensor network,” Int. J. Advancements Comput. Technol., vol. 5, no. 8, pp. 456–463, 2013

J.-H. An, Y. Dodis, and T. Rabin, “On the security of joint signature and encryption,” in Proc. Int. Conf. Theory Appl. Cryptograph. Techn., Amsterdam, The Netherlands, 2002, pp. 83–107.

K. Xing and X. Cheng, “From time domain to space domain: Detecting replica attacks in mobile ad hoc networks,” in Proc. IEEE Infocom, San Diego, CA, USA, 2010, pp. 1–9.

L. Shen, J. Ma, X. Liu, F. Wei, and M. Miao, “A secure and efficient IDbased aggregate signature scheme for wireless sensor networks,” IEEE Internet Things J., to be published

Lucena N. B., Lewandowski G., Chapin S. J., Covert Channels in IPv6, Proc. Privacy Enhancing Technologies (PET), May 2005, pp. 147–66.

M. R. Alagheband and M. R. Aref, “Dynamic and secure key management model for hierarchical heterogeneous sensor networks,” IET Inf. Security, vol. 6, no. 4, pp. 271–280, Dec. 2012.

N. Bitansky and O. Paneth, “On the impossibility of approximate obfuscation and applications to resettable cryptography,” in Proc. 45th Annu. ACM Symp. Theory Comput., Palo Alto, CA, USA, 2013, pp. 241–250.

P. Tague, M. Y. Li, and R. Poovendran, “Mitigation of control channel jamming under node capture attacks,” IEEE Trans. Mobile Comput., vol. 8, no. 9, pp. 1221–1234, Sep. 2009.

R.L. Rivest, A. Shamir, and L. Adleman “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems” journal Communications of the ACM, 1978 volume 21, pages 120—126

R. Das and Indrajit Das (2016) "Secure Data Transfer in IoT environment: adopting both Cryptography and Steganography techniques" second international conference on research in computeration intelligence communication network (ICRCICN), 2016

S. B. Othman, A. A. Bahattab, A. Trad, and H. Youssef, "Confidentiality and integrity for data aggregation in WSN using homomorphic encryption," Wireless Pers. Commun., vol. 80, no. 2, pp. 867–889, Jan. 2015.

S. S. D. Selvi, S. S. Vivek, J. Shriram, S. Kalaivani, and C. P. Rangan, "Identity based aggregate signcryption schemes," in Proc. 10th Int. Conf. Cryptol. India Progr. Cryptol. INDOCRYPT, New Delhi, India, 2009, pp. 378–397

S. Goldwasser and Y. T. Kalai, "On the impossibility of obfuscation with auxiliary input," in Proc. 46th Annu. IEEE Symp. Found. Comput. Sci., Pittsburgh, PA, USA, 2005, pp. 553–562.

S. Goldwasser and G. N. Rothblum, "On best-possible obfuscation," J. Cryptol., vol. 27, no. 3, pp. 480–505, 2014.

S. Rana, Saddam Hossain, Hasan Imam Shoun, Dr. Mohammod Abul Kashem "An Effective Lightweight Cryptographic Algorithm to Secure Resource-Constrained Devices" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 11, 2018

S. Alharby, Nick Harris, Alex Weddell & Jeff Reeve "The Security Trade-Offs in Resource Constrained Nodes for IoT Application" World Academy of Science, Engineering and Technology International Journal of Electronics and Communication Engineering Vol:12, No:1, 2018

Whitfield Diffie; Martin Hellman (1976). "New directions in cryptography". IEEE Transactions on Information Theory. 22 (6): 644.

Wolf .m, "Covert Channels in LAN Protocols," Proc. Wksp. Local Area Network Security (LANSEC), 1989, pp. 91–101

X. Liu, H. Zhu, J. Ma, Q. Li, and J. Xiong, “Efficient attribute based sequential aggregate signature for wireless sensor networks,” Int. J. Sensor Netw., vol. 16, no. 3, pp. 172–184, 2014

X.-Y. Ren, Z.-H. Qi, and Y. Geng, “Provably secure aggregate signcryption scheme,” ETRI J., vol. 34, no. 3, pp. 421–428, 2012.

Y. Han, D. Fang, Z. Yue, and J. Zhang, “SCHAP: The aggregate signcryption based hybrid authentication protocol for VANET,” in Proc. 1st Int. Conf. Internet Veh. Technol. Services (IOV), Beijing, China, Sep. 2014, pp. 218–226.

Y. Shi, J. Han, J. Gao, and H. Fan “An Obfuscatable Aggregatable Signcryption Scheme for Unattended Devices in IoT Systems” in IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 4, AUGUST 2017

Y. Zheng, “Digital signcryption or how to achieve cost (signature & encryption) cost(signature) + cost(encryption),” in Proc. 17th Annu. Int. Cryptol. Conf. Adv. Cryptol. CRYPTO, Santa Barbara, CA, USA, Aug. 1997, pp. 165–179.