SECURE DATA AGGREGATION PROTOCOL FOR WIRELESS SENSOR NETWORKS

HAMIDREZA GHAFGHAZI

UNIVERSITI TEKNOLOGI MALAYSIA

SECURE DATA AGGREGATION PROTOCOL FOR WIRELESS SENSOR NETWORK

HAMIDREZA GHAFGHAZI

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Science (Electrical-Communcation)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

DECEMBER 2010

Especially for:

My family, who offered me unconditional love and support throughout my life.

ACKNOWLEDGEMENT

I would like to take this opportunity to thank especially my supervisor. DR. DAVID IAN FORSYTH that guides me to fully understand the project title and some basic concept that were new to me.

Secondly, my very special thank goes to my family, that give me their endlessly support so that I could graduate from Universiti Teknologi Malaysia (UTM). It was impossible to study abroad without their help and care.

Special indebtedness goes to all my friends in UTM for their assistance and understanding.

Thank you.

ABSTRACT

In this work, the relationship between security and data aggregation protocols has been investigated. Providing security causes more energy consumption due high computation requirements. Therefore, a method is needed to facilitate energy consumption. Combining security with data aggregation is beneficial because data aggregation protocols decrease the amount of communications that reduce energy expenditure of redundant transmissions. In this project, Data Aggregation and Authentication protocol (DAA) is simplified called SDAA and implemented in order to detect false data along with data aggregation and confidentiality. The main goal of this particular algorithm is to find false data as early as possible to decrease data transmissions. In DAA there are three steps which are: Monitoring node selection, forming pair of nodes and integration of false data detection along with data aggregation and confidentiality as SDFC algorithm. In order to simplify DAA the first two steps have been predefined prior to network deployment. Besides, monitoring nodes are assumed to be sensing nodes which sense plain data. Eight different experiments are performed where in each experiments the number of data aggregators or number of monitoring nodes are varied. TelosB motes were deployed and all of results that relate to this particular sensor node with its constraints are analyzed. Consequently, with the aid of false data detection along with the data aggregation total amount of transmission compared to traditional methods decreased tremendously. Although the number of computations increased, the energy conserved by applying data aggregation and false data detection is more than other similar methods that detects false data at the base station. In this work, the number of transmissions of packets decreases from approximately 4000 to 2500 packets which shows the efficiency of SDAA protocol. However, when number of monitoring nodes increased the amount of packet loss and end-to-end delay also increased. In this project, to facilitate packet loss and end-to-end delay synchronization of monitoring nodes has been utilized. Moreover, with the aid of synchronization the end-to-end delay decreased from 17583 (ms) to 679 (ms) and the amount of packet loss improved from 85% to only 18%.

ABSTRAK

Dalam projek ini, hubungan antara protokol keselamatan dan agregasi data telah kaji. Menyediakan keselamatan menyebabkan pengambilan tenaga lebih keperluan kerana yang lama. Oleh kerana itu, kaedah yang diperlukan untuk memudahkan tenaga. Kebaikan menggabungkan keselamatan dengan agregasi data peoses menjimatkan adalah data protokol agregasi dapat mengurangkan jumlah komunikasi yang mengurangkan pengeluaran tenaga penghantaran berlebihan. Dalam projek ini, data Agregasi dan protokol Authentication (DAA) akan diubah suai dan dilaksanakan untuk mengesan data palsu bersama-sama dengan agregasi data dan sekuriti. Tujuan utama dari algoritma ini adalah untuk mencari data palsu seawal mungkin untuk mengurangkan penghantaran data. Dengan DAA ada tiga langkah iaitu: pemilihan Monitoring node, membentuk sepasang node dan integrasi data pengesanan palsu bersama-sama dengan agregasi data dan kerahsiaan sebagai algoritma SDFC. Untuk memudahkan DAA dua langkah pertama telah diketahui terlebih dahulu. Selain itu, pemantauan node mengandaikan sensing data node ada biasa. lapan percubaan yang berbeza yang dilakukan bahawa dan dalam setiap satu nombor dari pengumpul data atau jumlah node pemantauan diubah. TelosB motes digunakan dan semua keputusan berkaitan dengan ini node sensor tertentu diteliti. Dari analisis, pengesanan data palsu bersama-sama dengan jumlah agregasi data penghantaran berbanding dengan kaedah tradisional sangat menurun. Walaupun masa proses meningkat naik, tenaga yang kekal dengan melaksanakan agregasi data dan palsu pengesanan data jauh lebih daripada kaedah serupa yang lain yang mengesan data palsu pada base station. Dalam projek ini, jumlah penghantaran menurun daripada 4000-2500 yang menunjukkan kecekapan protokol SDAA. Namun, ketika jumlah node pemantauan meningkatkan jumlah pakej loss dan delay end-to-end juga meningkat. Dalam projek ini, untuk memudahkan packet loss dan end-to-end delay penyegerakan pemantauan node telah digunakan. Dalam juga, dengan bantuan penyegerakan penangguhan end-to-end menurun dari 17.583 (ms) untuk 679 (ms) dan jumlah pakej loss meningkat dari 85% menjadi hanya 18%.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

DA	-	Data Aggregator
K	-	XOR Key
AA-Pair	-	Data Aggregator nodes partners
MN-Pair	-	Monitoring nodes Partners
MF-pair	-	Monitoring-Forwarding nodes partners
K_{Group}	-	Group key for XOR
BS	-	Base Station
PC	-	Computer

LIST OF ABBREVIATIONS

WSN	-	Wireless Sensor Network
DAA	-	Data Aggregation and Authentication protocol
SEDAN	-	Secure aggregation for wireless sensor networks
WBA	-	Witness-Based Approach
SDAP	-	Secure hop-by-hop Data Aggregation Protocol
iPDA	-	Integrity-protecting private data aggregation
SRDA	-	Secure Reference-Based Data Aggregation
SDAV	-	Secure Data Authentication
MAC	-	Message Authentication Code
SDAA	-	Simplified Data Aggregation and Authentication
SDFC	-	Secure data aggregation and false data detection
MNS	-	Monitoring node selection
GPL	-	General Public License
OS	-	Operating System
HMAC	-	Hash-based Message Authentication Code
CBC-MAC	-	Cipher Block Chaining Message Authentication Code
CMAC	-	Cipher-based Message Authentication Code

CHAPTER 1

INTRODUCTION

1.1 Background of Study

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion, or pollutants, at different locations. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control. [1,2]

Although WSNs could be applied extensively, they have features and boundaries associated with their nature. The most important constraint in WSN is the lower energy that can be stored in them that causes short lifetime sensor nodes and network itself. Moreover, it is usually impossible to recharge the battery or even change it. Another major problem which the network designers are facing with is accessibility of intruders and attackers to these tiny sensor nodes. In other words, sensor nodes could easily be compromised by adversaries physically and the information might be revealed. Consequently, significant challenges of WSNs which should be taken into account for such application include: limited power they can harvest or store, ability to withstand harsh environmental conditions, ability to cope with node failures, stationary or mobility of nodes, static or dynamic network topology, communication failures, heterogeneity of nodes, large scale of deployment, unattended operation and security [3].

Energy consumption is one the most considerable constraints in WSNs. Batteries in wireless sensor nodes can store only a limited amount of energy and they are irreplaceable. Therefore, efficiency of energy consumption in WSNs is a mission critical task which plays an important role to prolong the network lifetime. One of the significant approaches in order to conserve energy in WSNs is data aggregation. The enormous part of energy consumption is during data transmission. Since sensors are densely deployed in a certain area to gather the particular information, therefore, data redundancy is extremely high. In this respect, data aggregation by reducing the amount of data that needs to be transmitted, effectively decrease energy consumption [4].

Apart from energy consumption, security is another major concern in WSNs which should be investigated. WSNs generally communicate via radio which introduces various problems such as: noise and security. This exposes any recipient with compatible receiver is able to detect the transmitting message. While all networks are subject to common threats, remote wireless sensor networks are more vulnerable to security breaches since they are physically more accessible to possible adversaries.

Many WSNs are employed in critical applications which information has to be confidential security is vital [5]. Moreover, solving security problem might be difficult since security solutions require high computation resources, storage and energy resources which impose additional challenges when working with tiny sensor nodes with limited resources [6].

In this work, the relationship between security and data aggregation protocols will be investigated. To provide security is extremely expensive in term of energy consumption due high computation requirements, thus, combining security with data aggregation is beneficial because data aggregation protocols will be able to decrease the amount of communications. This will decrease energy expenditure of redundant transmissions. As mentioned previously, the main concern in secure data aggregation is to prolong the lifetime of the network, confidentiality and integrity. Although, providing these features will lead to more computation overhead and cause more energy consumption due higher computation requirements, joint operation of security and data aggregation gives better performance for the network. This will not only increase the lifetime of the nodes but the communication overhead will also be decreased.

1.2 Statement of Problem

Wireless Sensor Networks have attracted researcher`s attention recently to many open research issues. Prolonging lifetime of the network is extremely important due to critical applications like battle field surveillance. In this respect, data aggregation technique is vastly applied in order to conserve the energy by reducing communication overhead. Furthermore, putting security on the top of particular data aggregation

algorithm will enhance its performance in terms of trustworthiness of the data and legitimate users authority that have access to the network and critical information.

Although WSNs can be used for different applications and they are extremely beneficial due its low cost and availability as autonomous devices. Energy is a predominant challenge since sensor nodes is able to work for several months or even years with irreplaceable batteries.

Furthermore, these tiny sensors are usually deployed in hostile environment to do critical missions like battle field surveillance; as a result security issues like integrity and confidentiality are significantly important. In addition, they are so accessible to adversaries and they will be compromised easily. For example, intruders may inject false data through data aggregation procedure and waste energy and bandwidth. Therefore, wireless sensor network protocols such as data aggregation protocols, should be designed with security in mind to not only detect false data injection in order to conserve bandwidth which is done by dropping faulty packets but also to provide data integrity and confidentiality which is a major concern.

1.3 Objectives/Purpose of the Study

The objectives of this study are:

i. To develop the simplified version of Data Aggregation and Authentication (DAA) protocol called (SDAA) in WSNs` programming language which is NesC.
ii. To implement SDAA in WSN use TelosB mote by writing NesC codes.

iii. To analyze the performance of SDAA on WSN test bed in terms of the amount of transmissions and computations and energy consumption.

1.4 Scope of the Study

The orientation of the study is secure data aggregation protocols in wireless sensor networks. To achieve objectives that are mentioned above the data aggregation protocol should decrease communication overhead and computation overhead to save energy and prolong lifetime of the network. However, combining security with data aggregation will impose some computation overhead. On the other hand, each secure data aggregation protocol has some redundancies for integrity of the data and endorsement of information which could be omitted so as to decrease computation overhead and increase efficiency of the protocol. In this project, we are going implement DAA because it is simple and practical to implement in the real WSN testbed.

1.5 Thesis outline

In this study, chapter one presents introduction. The general oveview of wireless sensor networks has been discussed and different applications in which WSNs are able to applied has been inroduced.

Literature review is discussed in chapter two. Different approches of secure data aggregation introduced. Those protocols has been compared in a table to elaborate advantages and disadvantages of them. DAA has been presented and explained in detail.

Chapter three highlighted research methodology. The steps that is needed to reach the objectives has brought to a flowchart and discussed.

Source code development is presented in chapter four. The flow charts of writing NesC codes for different kinds of node functionalities has elaborated.

Chapter five discusses testbed implementation. The performance of proposed protocol in terms of number of transmissions and computations and respective energy consumption discussed.

Finally chapter six concludes the study. Future works has introduced and improvements has elaborated.

Reference

1. Jan F. Akyildiz , Tommaso Melodia, Kaushik R.Chowdury "wireless multimedia sensor networks: A survey " IEEE wireless communication vol. 14 No. 6, Dec. 2007.
2. S. Bhatti, J. Carlson, H. Dai, J. Deng, J. Rose, A. Sheth, B. Shucker, C. Gruenwald, A. Torgerson, R. Han,mantis,"An embedded multithreaded oprating system for wireless micro sensor platforms ACM/Kluwer Mobile Networks & Applications (MONET)" Special Issue on Wireless Sensor Networks, vol. 10, no. 4, August 2005**.**
3. Sensor Network Security: A survey, Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, " IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 2, SECOND QUARTER 2009.
4. Afshin Fallahi and Ekram Hossain "QoS provisioning in wireless video sensor networks: A dynamic power management framework " IEEE wireless communication vol.14 No.6 december2007.
5. Ilker Demirkol, Cem Ersoy, and Fatih Alagoz, Bogazici University, "MAC protocols for wireless sensor networks" IEEE Communications Magazine, April 2006.
6. Tanveer Ahmad Zia, "A SECURITY FRAMEWORK FOR WIRELESS SENSOR NETWORKS ", School of Information technology, University of Sydney, February 2008.
7. J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey, Comput. Networks 52 (12) (2008) 2292–2330.
8. K. Akkaya, M. Demirbas, R.S. Aygun, The Impact of Data Aggregation on the Performance of Wireless Sensor Networks, Wiley Wireless Commun. Mobile Comput. (WCMC) J. 8 (2008) 171–193.
9. H. am, S. Ozdemir, Integration of False data detection and secure data aggregation in wireless sensor networks, in: IEEE/ACM TRANSACTIONS ON NETWORKING Editor D. Agrawal, August 14,2009
10. Miloud Bagaa,et. Al, published in "IEEE Local Computer Networks / Workshop on Network Security, Ireland (2007).

11. Y. Yang, X. Wang, S. Zhu, G. Cao, SDAP: a secure hop-by-hop data aggregation protocol for sensor networks, in: Proceedings of the ACM MOBIHOC'06, 2006.

12. W. Du, J. Deng, Y.S. Han, P.K. Varshney, A witness-based approach for data fusion assurance in wireless sensor networks, in: Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '03), 2003, pp. 1435–1439.

13. HE, W., LIU, X., NGUYEN, H., NAHRSTEDT, K., AND ABDELZAHER, T. 2007. PDA: Privacy preserving data aggregation in wireless sensor networks. In *Proceedings of the Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'07)*.

14. H.O. Sanli, S. Ozdemir, H. □am, SRDA: secure reference-based data aggregation protocol for wireless sensor networks, in: Proceedings of the IEEE VTC Fall Conference, Los Angeles, CA, 26–29 September 2004, pp. 4650–4654.

15. A. Mahimkar, T.S. Rappaport, SecureDAV: a secure data aggregation and verification protocol for wireless sensor networks, in: Proceedings of the 47th IEEE Global Telecommunications Conference (Globecom), November 29–December 3, Dallas, TX, 2004.

16. Stallings, W. (2004). *Data and Computer Communications.* Pearson Prentice Hall, Upper Saddle River, NJ, pp. 670-677.

17. D. Kahn, *The Codebreakers: The Story of Secret Writing,* New York: Macmillan Publishing Co., 1967.

18. Mat´uˇs Harvan, "*Connecting wireless Sensor Networks to the internet – a 6lowpan Implementation for TinyOS* 2.0,May 2007.

19. *TinyOS tutorial. Introduction into interfaces and Components*, http://docs.tinyos.net/index.php/Getting_Started_with_TinyOS#Components_and_Interfaces. Accessed on 13th November 2008.

20. David Gay, Philip Levis, David Culler, Eric Brewer *nesC 1.1 Language Reference Manual* May 2003.

21. Sharpe.R, Lamping.U *Wireshark User's Guide 28195 for Wireshark 1.0.0,* NS Computer Software and Services P/L Ed Warnicke.

22. *Chipcon. CC2420 low power radio transceiver,* http://www.chipcon.com. Accessed on 23rd January 2008.

23. *Sensor Node in Wireless Sensor Network TelosB Information* http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/TelosB_Datasheet.pdf. Accessed on 20th August 2008.

24. *Ubuntu Operating system Information, Description and How to download.* http://en.wikipedia.org/wiki/Ubuntu_(Linux_distribution). Accessed on 27th December 2008.

25. B. W. Kernighan and D. M. Ritchie. *The C Programming Language*, Second Edition. Prentice Hall, 1988.

26. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. E. Culler, and K. S. J. Pister. *System Architecture Directions for Networked Sensors. In Architectural Support for Programming Languages and Operating Systems*, pages 93–104, 2000.

27. C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," in *Proc. 2nd ACM Conf Embedded Netw. Sensor Syst.*, 2004, pp. 162–175.

28. A. Prayati, Ch.Antonopoulos, T.Stoyanova, C.Koulamas, G.Papadopoulos, " A modeling approach on the TelosB WSN platform power consumption" The Journal of System and Software, Elsevier Inc 2010, 21 January 2010.

29. J. Lee et al., The price of security in wireless sensor network, Comput. Netw. (2010), doi: 10.1016/j.comnet.2010.05.011