WSN KEY MANAGEMENT SECRECY TECHNIQUE USING LOCAL FM RADIO

AHMAD MOHAMMAD LUTFI AL-ZURAIQI

WSN KEY MANAGEMENT SECRECY TECHNIQUE USING LOCAL FM RADIO

Ahmad Mohammad Lutfi Al-Zuraiqi

(Metric No. 3140094)

Thesis submitted in fulfillment of the degree of

MASTER OF COMPUTER SCIENCE

Via Mixed Mode

INFORMATION SECURITY AND ASSURANCE

Faculty of Science and Technology

UNIVERSITI SAINS ISLAM MALAYSIA

Nilai

December 2015

AUTHOR'S DECLARATION

بسم الله الرحمن الرحيم

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

Date: 20th December 2015

Signature:

Name:

Metric No:

Address:

BIODATA OF AUTHOR

Ahmad Mohammad Lutfi AL-Zuraiqi (3140094), a Jordanian student, was born on the 20th of April 1980 in Riyadh, KSA. He obtained his bachelor degree in computer science from Philadelphia University in Amman, Jordan in 2005. He is a Microsoft Certified Professional (MCP) B877-0357, a Microsoft Certified Systems Administrator (MCSA) B877-0356, a Microsoft Certified Systems Engineer (MCSE), B877-0347, a Cisco Certified Network Associate (CCNA) CSCO11282416, an ICDL Certified UN-01070835 and ICDL Certified Examiner UN-JO-0148. Currently he is a Master's student at USIM University, majoring in Information Security and Assurance.

ACKNOWLEDGEMENTS

Praise be to Allah (SWT) who gave me the courage and power to do this work. I am thankful to my parents for their blessings, care and passion, to my lovely wife for her encouragement and support in tough times, and to my kids, Toleen and Ameen, in whose eyes I see the future. Thanks are also extended to my supervisor Prof. Kamaruzzaman Bin Seman for his direction and vision in the completion of this thesis.

ABSTRACT

Wireless sensor network services rely on two elements, secure communication, and symmetric key distribution. As WSN use symmetric key cryptography to protect data confidentiality, each sensor node has to keep a copy of the secret key to be used in encryption/decryption process. The secret key can be sent wired or wireless, but wire solution is impossible especially in remote areas, while current wireless solutions have either coverage or cost issues or they require a long implementation time. Most studies try to find solutions for remote WSN network reachability by using solutions like satellite connections, others turn out to use other wireless solutions to create point-to-point connection. But such solutions lack durability in bad weather or require a long time and effort in addition to high cost to setup. This research will solve the issue of sending secret key securely to WSN nodes in remote areas using commercial FM stations. Since WSN node lacks processing power, memory and energy capacity, Elliptic Curve Cryptography (ECC) will be used to encrypt the secret key, as it has fast computational time and smaller key size that can be transmitted easily through FM radio. The encrypted spread has simple XOR encryption before modulating it to the 80 kHz, then it is embedded in the commercial FM band and broadcasted using commercial FM stations, to hide the key within the FM band. This research seeks to solve key management issues by providing multi-layers of security, to make certain that key is delivered without being sniffed or compromised. Through the implementation, we have tested that the technique being tested is successful in sending the secret key to WSN base station.

ABSTRAK

Perkhidmatan rangkaian sensor tanpa wayar ataupun Wireless sensor network (WSN) bergantung pada dua elemen, komunikasi yang selamat dan pengedaran kunci simetri. WSN menggunakan kriptografi kunci simetri untuk melindungi kerahsiaan data, setiap nod sensor perlu menyimpan salinan kunci rahsia yang akan digunakan dalam proses penyulitan / penyahsulitan. Kunci rahsia ini boleh dihantar melalui wayar atau tanpa wayar, akan tetapi penyelesaian melalui wayar adalah mustahil terutama di kawasan pedalaman. Isu penggunaan tanpa wayar pula berkaitan liputan rangkaian, kos atau memerlukan masa pelaksanaan yang panjang. Kebanyakan kajian cuba untuk mencari penyelesaian bagi masalah capaian rangkaian WSN dengan menggunakan penyelesaian seperti sambungan satelit, manakala sesetengah pihak mula menggunakan penyelesaian tanpa wayar dengan mewujudkan sambungan titik-ke-titik. Tetapi penyelesaian ini tidak mempunyai ketahanan dalam keadaan cuaca buruk atau memerlukan usaha dan masa yang panjang dan di samping kos yang tinggi untuk penyediaan WSN. Kajian ini akan menyelesaikan isu menghantar kunci rahsia dengan selamat ke nod WSN di kawasan pedalaman dengan menggunakan stesen FM komersial. Oleh kerana nod WSN tidak mempunyai kuasa pemprosesan, memori dan tenaga keupayaan, Eliptik Curve Kriptografi (ECC) akan digunakan untuk menyulitkan kunci rahsia, kerana ia mempunyai masa pengiraan cepat dan saiz kekunci yang lebih kecil yang boleh dihantar dengan mudah melalui radio FM. Proses mudah penyulitan XOR ini digunakan sebelum modulasi kepada 80 kHz. Kemudian ia disatukan dalam jalur FM komersial dan disiarkan menggunakan stesen FM komersial bertujuan menyembunyikan kunci dalam jalur FM. Kajian ini bertujuan untuk menyelesaikan isu-isu pengurusan mengenai kunci dengan menyediakan pelbagai lapisan keselamatan agar kunci ini dapat dihantar tanpa berjaya dikesan atau tolak ansur. Melalui

pelaksanaan kajian yang dijalankan , teknik yang kami uji ini berjaya dalam menghantar kunci rahsia ke stesen pangkalan WSN.

CONTENT PAGE

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CDMA	Code division multiple access
DARC	Data Radio Channel
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ETA	Estimated Time of Arrival
FM	Frequency Modulation
GMSK	Gaussian Minimum Shift Keying
GPS	Global Positioning System
GSM	Global System for Mobile
KMS	Key Management Service
MSN	Microsoft Network
PSTN	Public Switched Telephone Network
RDS	Radio Data System
RX	Receive State
SPOT	Smart Personal Object Technology
TX	Transmit State
UHF	Ultra high frequency
VHF	Very high frequency
WSN	Wireless Sensor Network

Research	Year	Technique	Coverage	Advantages	Disadvantages
Li	2009	SDR	In Lab	Used USRP with GNURadio to overcome the shortage of low throughput and coverage. The researchers have used narrow-band to communicate with a range of WSN platforms using SDR, because using SDR has no specific standard of hardware design constrains, as the biggest part of the hardware implementation are done on the software side (GNURadio) while USRP used for communication	No specific standard, though because of regulations SDR must be only used in a secure lab to not overlap with other frequencies.