JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

PERFORMANCE ANALYSIS OF MISTY1 CIPHER AND OCB BLOCK CIPHER MODE IN TINYSEC LIBRARY FOR WIRELESS SENSOR NETWORK SECURITY

KanchanThool & Dr. Umesh K Singh

School of Engineering & Technology and Institute of Computer Science,Vikram University, Ujjain

kanchanthool7@gmail.com, umeshsingh@rediffmail.com

ABSTRACT:

This paper describes the link layer architecture and block cipher. The Tinysec library implementation was provided with 2 ciphers (skipjack and RC5) and block cipher mode(CBC) . The Tinysec library provides opportunity to replace the cipher and block cipher mode with one of our choice. In our analysis we used Misty1 as block cipher and OCB as block cipher mode. Misty1 is a block cipher based on nested Feistel network with variable number of rounds (typically 8). It uses a 128 bits sized crypto variable and block size of 64 bits. In this paper, we emphasis on energy requirement, RAM requirement and throughput by misty1 block cipher and OCB block cipher mode in Tinysec link layer architecture. A Wireless Sensor Network (WSN) consists of sensors to monitor physical or environmental conditions and pass their data through the network through switch station to main station and basically deployed in non accessible area. The WSN is built of several no. of nodes connected to one or several sensors. Node consists of radio transceiver with antenna, energy source and microcontroller. Wireless sensor network is only option to study the remote area where human access is not possible and gives opportunity to explore more area. Contributions of this work are as follows: Implementation of Misty1 cipher and Ocb block cipher mode in tinysec library to decrease the energy consumption, increases throughput and provide more security. We simulated the ciphers and modes implemented in NesC, Tinysec library. We used TOSSIM and AVRORA as the WSN simulator. The NesC compiler gives us output, the RAM requirement.. AVRORA allows us to analysis more details of execution of program and diagnoses of performance and problems before deployed on the target hardware. From AVRORA, we get result of energy consumption and throughput of for cipher and block cipher used.

KEYWORDS:

Wireless Sensor Networks, Link Layer Security, Block Cipher, Encryption, Authentication, Misty1 cipher, OCB block cipher mode, energy requirement, throughput, tinysec library, wireless sensor network security, link layer architechture.

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of sensors to monitor physical or environmental conditions and pass their data through the network through switch station to main sttaion and basically deployed in non accessible area. The WSN is built of several no. of nodes connected to one or several sensors. Node consists of radio transceiver with antenna, energy source and microcontroller. Wireless sensor network is only option to study the remote area where human access is not possible and gives opportunity to explore more area. Deployment of nodes in remote area, changing of battery is not an option.

Depends on a battery, not only limits the sensors lifetime but also makes design & management of wireless sensor network a challenge. So different type of energy harvesting is used and Lowering the energy consumption in data processing at the node increases life time of sensor node.

Tinysec library is an open source and popular TinyOS which provide a platform designed for wireless sensor network. The basic designing goal of Tinysec link layer architecture is security and performance.

i. Security: 3 major concerns are access control, integrity and confidentiality.
   - a> Access control: it means to stop the access of unauthorized node in particular network. Also detect message from unauthorized node and reject them.
   - b> Integrity: it means message is come from authorized node.
   - c> Confidentiality: it means keeping information secret from unauthorized nodes.

ii. Performance: basics concerns are RAM and ROM requirement of the application at the time of compilation, the throughput in bits/sec, energy requirement and time of simulation.

II. MOTIVATION

Security services provided by the link layer security protocol depend on the requirement. These link layer security protocols like Tinysec, Sensec, Minisec has open ended design so as to enable the use of any block cipher with appropriate mode of operation. Tinysec is 1st lightweight and link layer security protocol. Sensec: it does not support replay protection. Minisec it offers all the basic desired link layer security like Data encryption, message integrity and replay protection. But it does not provide configurability. Zigbee: it offering high security at high overhead. So it's suitable for higher end devices and not the low end WSN nodes. None of these offer any choice in selection cipher as well as the selection of the MAC sizes.

PROPOSED MODEL

These tinysec library have an open-ended design. the open ended design allow us to use different cipher with other block cipher mode which is appropriate for tinyOS. Tinysec library has 2 block cipher named skipjack and RC5 with CBC block cipher mode.

The proposed model is to replace Skipjack block cipher model with Misty1 block cipher with two block cipher mode cbc and obc.

Encryption scheme[3]:.

TinySec uses single and symmetry key which is used to share between all the sensor network nodes.

All node encrypted the data and add MAC (message authentication code) for data integrity than transmit packet . At the receiving end , receiver verifies the packet using MAC to check weather the packet is modified or not than decrypt the packet.

MISTY1 CIPHER

MISTY1 is a Feistel network with a n number of rounds ,where n is the multiple of 4,8 are recommended with recursive structure. The cipher operates on 64-bit blocks and has a key size of 128 bits. MISTY1 claims to be provably secure against linear and differential cryptanalysis.

IV.TOOLS FOR IMPLEMENTATION

1. TINYOS: TINYOS is an operating system specially design for sensor network to reduce the energy and ram requirement of node to increases the life of node.It is based on event driven programming. TinyOS content the tinysec library where security code is define. TOSSIM is a simulator used in TinyOS. TOSSIM can simulate hundreds of nodes at the same time. TOSSIM is used to measure the RAM requirement for different nodes.
2. AVRORA: AVRORA is used to measure the energy consumption, throughput in bits/sec and time of simulation.

V.METHODOLOGY

. We used TOSSIM as the WSN simulator.We simulated the performance of the misty1 ciphers and different modes named OCB & CBC block cipher mode implemented in NesC. The NesC compiler will give RAM requirement of the sensor node.

Interface

Commands are the set of function specifying by interface and event is known as when commands are implemented interface's provider to implement by interface's user. We have change Block Cipher Mode interface file in original TinyOS version to incorporate our mode of operation.

Configuration

A NesC component is either a module or a configuration. Configuration file is responsible for wiring between different modules. We make changes in configuration file of Tinysec viz. TinySecC. In this file implementation clause specifies a list of C declarations and definitions called translation-unit.

Modules

As we have discussed, commands defined in interface must be implemented by provider of the interface.

III. RESULT & DISCUSSION

Some are very important issues when we design tiny operating system. Memory management, energy management performance and security.

When we discuss about memory management we have very small amount of memory only some kbs. Memory of sensor divided into 3 parts mainly. RAM, internal flash and EEPROM. RAM is used to store and access application data temporarily to work faster. As we have RAM in few kbs, so it limits the computing power and communication capabilities. RAM is important part of memory for sensor to compute and communicate the processed data. To install or upgrade application we need more RAM memory. RAM requirement for CBC mode with skipjack (original configuration), CBC mode with Misty1, OCB mode with skipjack and OCB with misty1 cipher for mica, mica2 and mica2dot platform. RAM usage is decreases when we are using Misty1 cipher with CBC mode and OCB mode. RAM usage is high in original configuration. Misty1 cipher is more secure than skipjack cipher. Decreases in RAM usage decreases energy usage

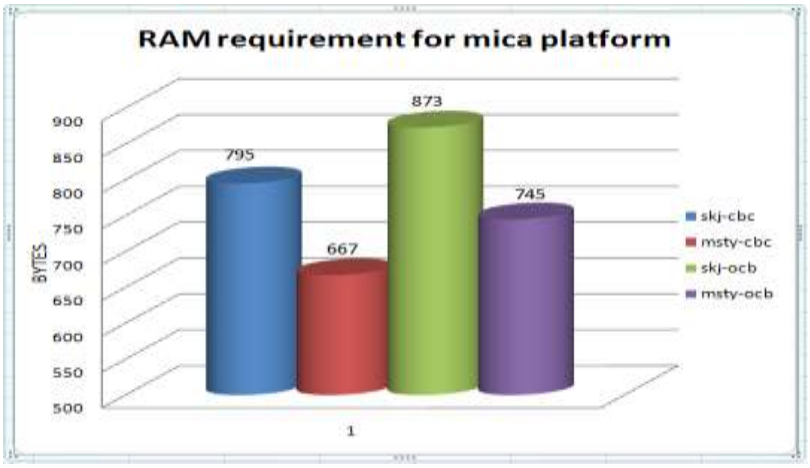

Figure 1: RAM requirement for mica platform

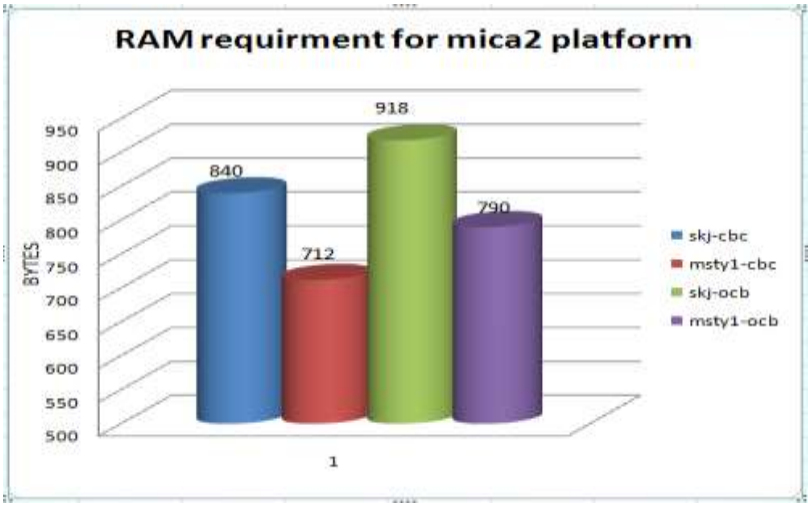

Figure 2: RAM requirement for mica2 platform

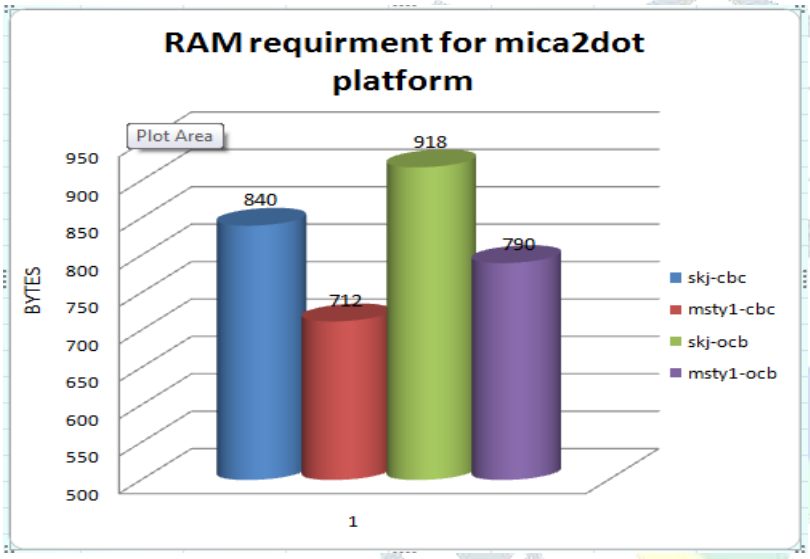

Figure 3: RAM requirement for mica2dot platform.

Energy requirement is second important issue for WSN. As we have very limited energy. So it's very important to manage energy for long lasting and proper processing of data and proper communication of data. As sensors nodes are non-rechargeable so when we deploy in remote area, always more than required nodes. It will increase all over all system cost. The main reason of energy consumption is transmission and reception of data which can't be cut down so we have only option is to reduce processing energy requirement by using light weight applications for security and computing the data. In our suggested combination, Misty1 cipher with ocb block cipher mode energy requirement is .0032 joules and in previous combination skipjack with CBC block cipher mode is 2.447 joules. By using MISTY1 cipher with ocb block cipher mode processing energy requirement is reduced.

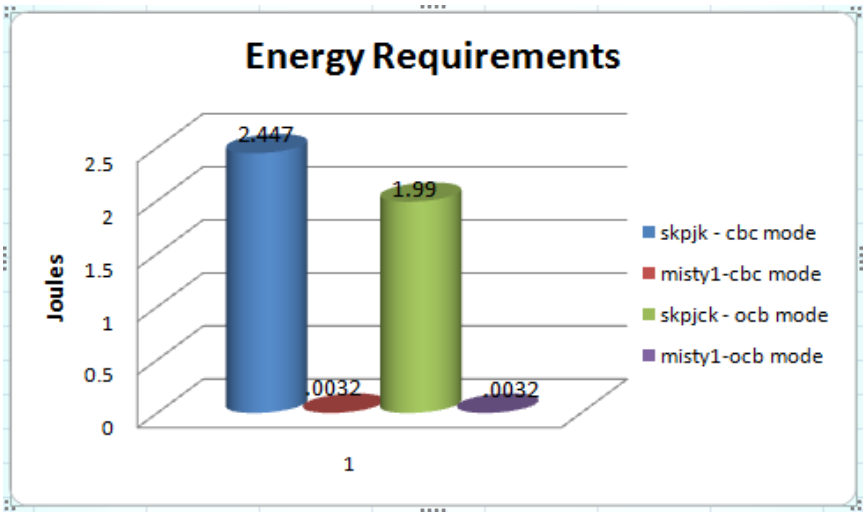

Figure 4: Energy Requirement for block cipher & with different mode combination.

Performance is another issue. Performance can be calculated by throughput. Throughput means number of successful massage send and receive in particular time interval. In previous combination skipjack and CBC Cipher mode it is 8.106. We calculated throughput with different combination we get different results. When we combine skip jack with ocb block cipher mode, it is 6.784. By using Misty 1 cipher with CBC mode, it will increase upto 63.08 and misty 1 cipher with OCB mode; it gives best results with 65.33.

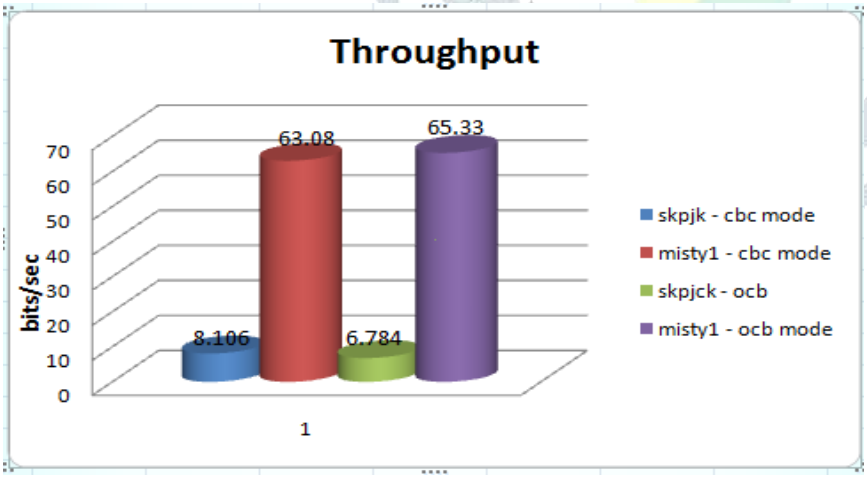

Figure 4: throughput for block cipher & with different mode combination.

VII.CONCLUSION

In this paper, we investigate Misty1 cipher with CBC mode and OCB mode in Tinysec library for wireless sensor network. As per the experimental result that we obtain, RAM usage is decreases when we are using Misty1 cipher with CBC mode and OCB mode. RAM usage is high in original configuration. Misty1 cipher is more secure than skipjack cipher. Decreases in RAM usage decreases energy usage. Energy requirement decreases and throughput increases in Misty1 cipher with OCB mode.

In future, Misty1 block cipher can be used with other mode of block cipher to improve security in Tinysec security architecture.

REFERENCES

[1] I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci "Wireless sensor networks: a survey" Broadband and Wireless Networking Laboratory, School of Electrical andComputer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA Received 12 December 2001; accepted 20 December 2001.

[2] NasrinSultana, Tanvir Ahmed and Professor Dr. ABM Siddique Hossain"Study of a new link layer security scheme in a wireless sensor network" The AIUB Journal of Science and Engineering (AJSE), Vol. 10, No. 1, August 2011.

[3] Chris Karlof, Naveen Sastry, and David Wagner," TinySec: A link layer security architecture for wireless sensor networks", in Proc. of the Second ACM Conference on Embedded Networked Sensor Systems (SenSys 2004), November 2004.

[4] David Gay, Phil Levis, Rob von Behren, Matt Welsh, Eric Brewer, and David Culler. The nesC language: A holistic approach to network embedded systems. In Programming Language Design and Implementation (PLDI), June 2003.

[5]Philip Levis and Nelson Lee. "TOSSIM: A Simulator for TinyOS Networks Version 1.0 June 26, 2003"

[6] Devesh Jinwala, Dhiren Patel, Kankar Dasgupta, " Optimizing the block cipher and modes of operation overhead at the Link Layer Security framework in Wireless Sensor Networks ", in Proceeding of ICISS 2008, LNCS 5352, pp. 258-272,2008, Springer – Verlag , Berlin Heidelberg 2008.

[7] M.matsui,"New Block Encryption Algorithm MISTY", In Proceedings of fourth International Workshop of Fast Software Encryption, jan 1997

[8] M.matsui, "Supporting Document of MISTY1 – version 1.10", Mitsubishi electric corp,September 2000.

[9]http://en.wikipedia.org/wiki/skipjack_(cipher)

[10]https://en.wikipedia.org/wiki/MISTY1