

Internetworking Indonesia Journal

Volume 1
Number 1
Spring 2009

Editors' Introduction	1
The Overhead and Efficiency Analysis on WiMAX's MAC Management Message <i>by Ardian Ulwan, Vit Andriik & Robert Bestak</i>	3
Loop-back Action Latency Performance of an Industrial Data Communication Protocol on a PLC Ethernet Network <i>by Endra Joelianto & Hosana</i>	11
"Wayang Authoring": A Web-based Authoring Tool to Support Media Literacy for Children <i>by Wahyu Agung Widjajanto, Michael Lund, & Heidi Schelhowe</i>	19
Studi atas Prilaku Pengguna Layanan Wide Area Network (WAN) BPKP <i>by Desi Nelvia & Rudy M. Harahap</i>	25
Issues in Elliptic Curve Cryptography Implementation <i>by Marisa W. Paryasto, Kuspriyanto, Sarwono Sutikno & Arif Sasongko</i>	29

ISSN: 1942-9703
IJ © 2009
InternetworkingIndonesia.org

Internetworking Indonesia Journal

The Indonesian Journal of ICT and Internet Development
ISSN: 1942-9703

Internetworking Indonesia is a semi-annual electronic journal devoted to the timely study of the Information and Communication Technology (ICT) and Internet development in Indonesia. The journal seeks high-quality manuscripts on the challenges and opportunities presented by information technology and the Internet in Indonesia.

Journal mailing address: Internetworking Indonesia Journal, PO Box 397110 MIT Station, Cambridge, MA 02139, USA.

Co-Editors

Thomas Hardjono, PhD
(MIT Kerberos Consortium, MIT, USA)

Budi Rahardjo, PhD
(ITB, Indonesia)

Kuncoro Wastuwibowo, MSc
(PT. Telkom, Indonesia)

Editorial Advisory Board

Prof. Edy Tri Baskoro, PhD (ITB, Indonesia)

Mark Baugher, MA (Cisco Systems, USA)

Lakshminath Dondeti, PhD (Qualcomm, USA)

Prof. Svein Knapskog, PhD (NTNU, Norway)

Prof. Merlyna Lim, PhD (Arizona State University, USA)

Prof. Bambang Parmanto, PhD (University of Pittsburgh, USA)

Prof. Wishnu Prasetya, PhD (Utrecht University, The Netherlands)

Prof. Jennifer Seberry, PhD (University of Wollongong, Australia)

Prof. Willy Susilo, PhD (University of Wollongong, Australia)

Prof. David Taniar, PhD (Monash University, Australia)

Focus & Scope: The Internetworking Indonesia Journal aims to become the foremost publication for practitioners, teachers, researchers and policy makers to share their knowledge and experience in the design, development, implementation, and the management of ICT and the Internet in Indonesia.

Topics of Interest: The journal welcomes and strongly encourages submissions based on interdisciplinary approaches focusing on ICT & Internet development and its related aspects in the Indonesian context. These include (but not limited to) information technology, communications technology, computer sciences, electrical engineering, and the broader social studies regarding ICT and Internet development in Indonesia. A list of topics can be found on the journal website at www.InternetworkingIndonesia.org.

Open Access Publication Policy: The Internetworking Indonesia Journal provides open access to all of its content on the principle that making research freely available to the public supports a greater global exchange of knowledge. This follows the philosophy of the Open Journal Systems (see the Public Knowledge Project at pkp.sfu.ca). The journal will be published electronically and there are no subscription fees. Such access is associated with increased readership and increased citation of an author's work.

Manuscript Language: The Internetworking Indonesia Journal accepts and publishes papers in Bahasa Indonesia and English.

Manuscript Submission: Manuscripts should be submitted according to the IEEE Guide for authors, and will be refereed in the standard way. Manuscript pages should not exceed 7 pages of the IEEE 2-column format preferably in a MS-Word file format. Links to the IEEE style files can be found at www.InternetworkingIndonesia.org. Manuscripts submitted to Internetworking Indonesia must not have been previously published or committed to another publisher under a copyright transfer agreement, and must not be under consideration by another journal. Authors of accepted papers are responsible for the Camera Ready Copy (CRC) in the IEEE 2-column format (delivered in an MS-Word file). Authors are advised that no revisions of the manuscript can be made after acceptance by the Editor for publication. The benefits of this procedure are many, with speed and accuracy being the most obvious. We look forward to working with your electronic submission which will allow us to serve you more efficiently. Please email manuscripts or inquiries to the editors at the following address: editor@InternetworkingIndonesia.org.

Submission Guidelines: Internetworking Indonesia accepts a variety of manuscripts in either English or Bahasa Indonesia. Please review the descriptions below and identify the submission type best suited to your intended submission:

- *Research Papers:* Research papers report on results emanating from research projects, both theoretical and practical in nature.
- *Short papers:* Short research papers provide an introduction to new developments or advances regarding on-going work.
- *Policy Viewpoints:* Policy Viewpoints explore competing perspectives in the Indonesian policy debate that are informed by academic research.
- *Teaching Innovation:* Teaching Innovation papers explore creative uses of information technology tools and the Internet to improve learning and education in Indonesia.
- *Book Reviews:* A review of a book, or other book-length document, such as a government report or foundation report.

Editors' Introduction

WELCOME to the inaugural issue of the *Internetworking Indonesia Journal* (IJ). It has been a year-long effort to get the journal off the ground, and we are tremendously pleased that we have reached this important milestone.

The original conception for the IJ was rooted in a question posed by a colleague concerning the flagship Indonesian journal on computer science. This academic person was interested in learning more about work being done by researchers in Indonesia in the field of Information and Communications Technology (ICT), and about the Internet infrastructure development in Indonesia. This simple question led to the realization of the lack of an Indonesia-wide professional journal in the area of ICT, which includes the development of the Internet and its infrastructure in Indonesia.

Currently in Indonesia there are a number of small journals in the area of ICT that are university-related or university-sponsored. Many of these have as their sole purpose the task of reporting research work within their university or institution, and as such do not typically accept papers from other institutions. Additionally, many of these journals do not publish on a stable regular basis. Among those academics who are able to author papers, many feel compelled to publish in their own university journals for career development reasons.

There is therefore a gap that needs to be addressed: on one hand there are very few authors and academics from Indonesia who publish in ICT journals overseas, yet on the other hand there are multiple university-sponsored journals that are narrow in its scope and which often do not have a sufficient number of papers to appear on a regular basis.

The IJ hopes to fill this gap, and in doing so become the Indonesian flagship publication for the field of ICT and Internet development in Indonesia, with accessibility to readers worldwide through electronic publication.

The IJ has a number of broad aims:

- Provide an Indonesia-wide independent journal on ICT and Internet development in Indonesia. The IJ is not sponsored by or tied to any university or institution, and is open to receiving papers from Indonesian and international authors.
- Provide a publishing avenue for graduate students in the broad field of ICT and Internet development, both for students from Indonesia and abroad.
- Provide access to academics and professionals overseas

through the establishment of an *Editorial Advisory Board* (EAB) with an international membership. The composition of the EAB has intentionally been that of professionals from the ICT industry and academics from various organizations around the world.

- Promote the culture of writing and excellent authorship for students, academics and professionals in Indonesia. The editors and EAB members of the IJ understand that the habit of writing scientific papers needs to be encouraged at a very early age in a student's life. As such the IJ is very supportive and helpful of papers authored by Masters (S2 level) and PhD (S3 level) students in Indonesia, albeit their writing quality often being not on-par with their peer-students from universities abroad. The IJ decided to be bilingual in its publication of papers to support this aim, thereby broadening the scope of its readership in Indonesia.

This inaugural issue of the *Internetworking Indonesia Journal* carries five papers. Two of these papers were developed from related research papers presented at the *Wireless and Optical Communications Networks* (WOCN) 2008 conference in Surabaya. The third paper was developed from a conference paper presented at the *iiWAS2008 (Information Integration and Web-Based Applications and Services)* conference. The fourth paper written in Bahasa Indonesia reports some research results on WAN performance found within the BKKP institution in Indonesia. The fifth and last paper discusses issues relating to implementing public-key cryptosystems in hardware and software.

It is worthwhile to note that three of the papers in this inaugural issue are in fact written by graduate students, which to a significant degree fulfils one of the core aims of the journal. We also note that one of the papers is written in Bahasa Indonesia, which again goes to support one of the aims of the journal.

We hope this inaugural issue of the *Internetworking Indonesia Journal* can be the starting point of a successful journal that can one day become the flagship journal for the area of ICT and Internet development in Indonesia.

Thomas Hardjono
Budi Rahardjo
Kuncoro Wastuwibowo

The co-editors can be reached either at the IJ email address (editor@InternetworkingIndonesia.org) or at their private email addresses. Thomas Hardjono is at thardjono@yahoo.com. Budi Rahardjo is at rahardjo@gmail.com, while Kuncoro Wastuwibowo can be reached at kuncoro@kuncoro.com.

The Overhead and Efficiency Analysis on WiMAX's MAC Management Message

Ardian Ulvan^{1,2}, Vit Andrlík² and Robert Bestak²

¹Dept. of Electrical Engineering, The University of Lampung, Indonesia.

²Dept. of Telecommunication Engineering, Czech Technical University in Prague, Czech Republic.

Email: ulvan@unila.ac.id, (ulvana1, andrlík1, bestar1[@fel.cvut.cz])

Abstract—This paper presents the overhead analysis on MAC Management Messages of WiMAX based on IEEE802.16 standard. The efficiency on the MAC layer is derived for Point to Multipoint (PMP) topology. The influence of several parameters is examined. The parameters, such as the number of subscriber stations in the network, various modulation and coding, and length of MAC message's PDUs, are assigned as the overhead parameters. The results show the specified parameters have significant impact on the efficiency of MAC layer. Finally, some recommendations to reduce the overhead are put forward.

Index Terms — WiMAX, IEEE802.16; MAC efficiency; MAC overhead

I. INTRODUCTION

The Worldwide Inter-operability for Microwave Access (WiMAX) is a telecommunication technology based on IEEE802.16 standard [1]. WiMAX network overcome some of the limitations of IEEE 802.11, e.g. limited range or insufficient Quality of Service support, and also introduce full mobility [2]. Using their conjunction it is possible to create a solution for metropolitan and local area networks.

WiMAX supports two types of network topologies i.e. Point to Multipoint (PMP) and Mesh. In PMP, the link connection is only between Base Station (BS) and Subscriber Station (SS). A connection, used for the purpose of transporting Medium Access Control (MAC) management messages, required by the MAC layer.

The overhead caused by the MAC layer of the network is an important performance indicator, because it significantly influences the throughput. It is interesting to make an analysis how the MAC efficiency is dependent on the physical and logical setups of the network. Performance of a networking protocol is commonly evaluated by means of the net throughput, especially on MAC layer, and delay. The focus of this paper is the MAC layer efficiency.

Many papers evaluate MAC performance of the IEEE 802.11 standard. In [3] the authors study the influence of

MAC overhead in IEEE 802.11 ad-hoc networks. The analysis in [4] investigates MAC performance of the IEEE 802.16 and the amendment IEEE 802.16a. The focus is on the PMP topology and for a simple scenario, using one base station and one subscriber station, the net bit rate on the MAC level is calculated.

The authors in [5] analyze the MAC efficiency dedicated to multi-hop wireless networks based on IEEE 802.16a standard. The IEEE 802.16a air interface is described and a multi-hop approach for PMP mode is defined. Net throughput on MAC layer is then presented for one chosen multi-hop scenario. The number of hops is carried out as the parameter.

The remainder of this paper is organized as follows: In Section II, the IEEE802.16 reference model mainly for the PMP mode is described. Section III determines the MAC messages overhead as well as the efficiency of MAC layer. The net throughput analysis is also carried out in this section. Results of MAC overhead and the efficiency are shown in section IV. We also discussed the simulation results. The last section provides our conclusions.

II. IEEE802.16 REFERENCE MODEL

A. MAC Layer Functionality

The reference model is shown in Figure 1. It can be seen that the MAC consists of three sub-layers [6][7].

The Service-Specific Convergence Sub-layer (CS) is used for mapping of external network data into MAC service data units (SDUs) received by the MAC common part sub-layer (CPS). The MAC CPS isn't required to parse any information from the CS payload.

The MAC CPS provides the core MAC functionality of system access, bandwidth allocation, connection establishment, and connection maintenance. The separate security sub-layer provides authentication, secure key exchange and encryption. The MAC management messages are part of MAC CPS.

This research work was supported by Czech Technical University's grant no. CTU0715013. It also been performed in the Framework Programme 6 (FP6) project FIREWORKS IST-27675 STP, which is funded by the European Commission.

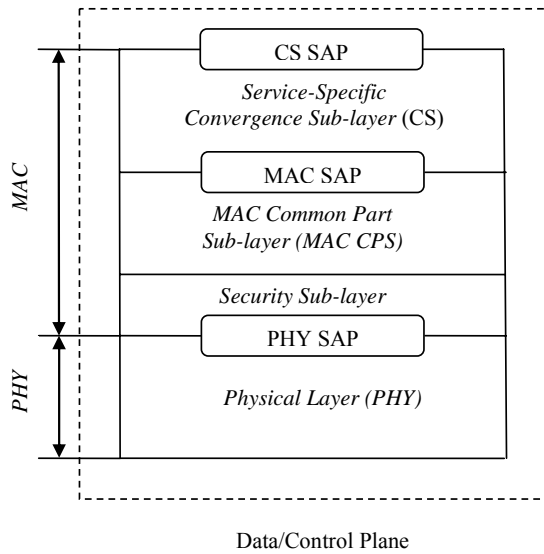


Fig. 1. IEEE 802.16 – layer model – data/control plane

B. PMP Topology

In this topology a central BS operates with a sectorized antenna capable of handling multiple independent sectors simultaneously. Within a given frequency channel and antenna sector, all stations receive the same transmission. The subscriber stations communicate only with the BS and not with each other. This scenario is shown in Figure 2.

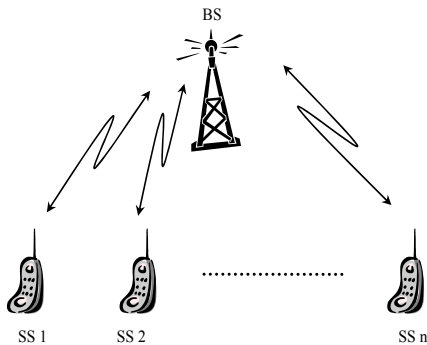


Fig. 2. Point to Multipoint topology

In downlink, the BS is the only transmitter, so that it doesn't have to coordinate with other stations, except for the overall time division duplexing (TDD) when time is divided into uplink and downlink transmission periods. In the uplink direction, SSs transmit on a demand basis. A SS may have continuing rights to transmit, or the rights may be granted by the BS after receipt of a request.

The MAC operates in a connection-oriented mode. After SS registration, connections are associated with service flows to provide a reference against which to request bandwidth. Service flows provide a mechanism for uplink and downlink quality of service (QoS) management. In addition, bandwidth is granted by the BS to an SS as an aggregate of grants in response to per connection requests from the SS.

Once the connections are established, they may be

maintained during their existence, and may be terminated. The maintenance requirements depend on the type of selected service.

C. Physical OFDM Symbols Parameters

According to the standard, four primitive parameters are defined to characterize the OFDM symbol:

- BW – nominal channel bandwidth,
- N_{used} – number of used subcarriers,
- n – sampling factor, in conjunction with BW and N_{used} determines the subcarrier spacing and the useful symbol time,
- G – ratio of CP time to useful time.

Using these primitive parameters another derived parameters are identified:

- N_{FFT} – smallest power of two greater than N_{used} ,
- Sampling frequency; $F_s = \lfloor n \cdot BW / 8000 \rfloor \cdot 8000$,
- Subcarrier spacing; $\Delta f = F_s / N_{FFT}$,
- Useful symbol time; $T_b = 1 / \Delta f$,
- CP Time; $T_g = G \cdot T_b$,
- OFDM symbol time; $T_s = T_b + T_g$,
- Sampling time; T_b / N_{FFT} .

Possible values of G are 1/4, 1/8, 1/16 and 1/32. The sampling factor has different values for bandwidths that are being multiples of different frequencies.

N_{used} is specified as 200 which mean that N_{FFT} is 256. Therefore the number of lower frequency guard subcarriers is equal to 28, the number of higher frequency guard subcarriers is 27. Thus, together with the DC carrier, the number of null subcarriers is 56 [2]. After subtracting 8 pilot subcarriers, there are 192 subcarriers available for data transmission.

D. Channel Coding/Modulations

The channel coding process is composed of three steps: randomizing, forward error correction (FEC) and interleaving. During transmission they are applied in this order, during reception their order is reversed. The mandatory channel coding with different modulations used in this paper can be seen in table 1.

Encoded data bits are then interleaved by an interleaving block with a block size corresponding to the number of coded bits per the allocated subchannel per OFDM symbol (N_{cbps}). For BPSK, QPSK, 16-QAM and 64-QAM, this number is 1, 2, 3 and 6, respectively.

III. THE EFFICIENCY ON MAC LAYER

The MAC overhead can be evaluated by means of determining the efficiency of the MAC layer. According to [5] the MAC efficiency can be defined as the ratio of the net throughput on MAC layer and the throughput per OFDM symbol.

$$\eta = \frac{\Theta_{MAC \ net}}{\Theta_{OFDM \ symbol}} \quad (1)$$

TABLE I.
MANDATORY CHANNEL CODING/MODULATION

Modulation	Uncoded block size (bytes)	Coded block size (bytes)	Overall coding rate
BPSK	12	24	1/2
QPSK	24	48	1/2
QPSK	36	48	3/4
16-QAM	48	96	1/2
16-QAM	72	96	3/4
64-QAM	96	144	2/3
64-QAM	108	144	3/4

The net throughput on the MAC layer is defined by equation 2. It is the ratio of the total number of payload bits, i.e. without all MAC overhead, in a frame to the frame duration T_{frame} .

$$\Theta_{MAC\ net} = \frac{\sum \text{Payload bits}}{T_{frame}} \quad (2)$$

The throughput of an OFDM symbol is given by:

$$\text{data rate} = \frac{\text{number of uncoded data bits per OFDM symbol}}{\text{OFDM symbol duration}} \quad (3)$$

Equation 4 shows the calculation in a more symbolic way, where N_{used} is the number of used OFDM subcarriers, N_{pilot} is the number of OFDM pilot subcarriers, N_{cbps} is the number of coded bits per allocated symbol (e.g. $N_{cbps} = 6$ for 64-QAM) and C is the code rate.

$$\Theta_{OFDM\ symbol} = \frac{(N_{used} - N_{pilot}) \cdot N_{cbps} \cdot C}{T_{symbol}} \quad (4)$$

The number of uncoded bytes per symbol is given as:

$$BpS = \frac{(N_{used} - N_{pilot}) \cdot N_{cbps} \cdot C}{8} \quad (5)$$

Higher modulation used for individual OFDM subcarriers, which results in higher N_{cbps} , together with higher code rate affect both $\Theta_{MAC\ net}$ and $\Theta_{OFDM\ symbol}$. Therefore we propose to evaluate the MAC layer efficiency as the ratio of OFDM symbols used for payload transmission in a frame to the total number of OFDM symbols in a frame. Letter L in the following equation always means length expressed as a number of OFDM symbols.

$$\eta = \frac{L_{net\ payload}}{L_{frame}} \quad (6)$$

The number of symbols in a frame does not depend on the modulation nor coding, as defined by equation 7.

$$L_{frame} = \left\lfloor \frac{T_{frame}}{T_{symbol}} \right\rfloor \quad (7)$$

A. MAC Efficiency in PMP Topology

In this section the MAC layer efficiency of the PMP topology is assessed. Our goal is to express the $L_{net\ payload}$ value. The uplink sub-frame consists of symbols used for ranging (L_{RNG}) and bandwidth requests (L_{BW}) and then of symbols containing UL physical layer PDUs. The length of the frame in OFDM symbols, when assuming one UL PHY PDU per subscriber station, can be written as:

$$\begin{aligned} L_{frame} &= L_{DL\ subframe} + L_{UL\ subframe} = \\ &= L_{DL\ PHY\ PDU} + L_{RNG} + L_{BW} + \sum_{i=1}^{N_{SS}} L_{UL\ PHY\ PDU\ i} \end{aligned} \quad (8)$$

1) Downlink Subframe

The DL sub-frame contains only one DL PHY PDU, which consists of the two-symbol long preamble and one-symbol Frame Control Header (FCH), then followed by the DL bursts. The DL burst #1 is different from other DL bursts (if present), since it contains broadcast MAC messages.

These broadcast messages comprise DL-MAP, UL-MAP, DCD and UCD messages. Their presence means less space for payload transmission, which means that longer broadcast messages decrease the MAC layer efficiency. The overhead in bytes introduced by them when assuming that all of them are present in the frame is given by equation 9.

$$OH_{DL\ burst\ \#1} = OH_{DL-MAP} + OH_{UL-MAP} + OH_{DCD} + OH_{UCD} + 4 \cdot OH_{MAC\ PDU} \quad (9)$$

For our purposes it is necessary to express the length of the overhead in DL burst #1 in OFDM symbols, which can be done by using equation 10, where BpS is the number of uncoded bytes per OFDM symbol, as specified by equation 5.

$$L_{DL\ burst\ \#1} = \frac{OH_{DL\ burst\ \#1}}{BpS} \quad (10)$$

The resulting number of bytes available for transmission of data MAC PDUs can be calculated using equation 11.

$$L_{DL\ data} = L_{DL\ subframe} - L_{LP} - L_{FCH} - L_{DL\ burst\ \#1} \quad (11)$$

L_{LP} (long preamble) is 2 symbols and L_{FCH} is 1 symbol.

2) DL-MAP MAC Management Message

The DL-MAP message defines the access to the downlink information. It is a fixed part that is created by 8 bytes at the beginning. After this fixed part, several information elements (IEs) defining the fifth and further DL bursts are present.

The first four DL burst are specified in the DLFP burst. Another IE is at the end of the DL-MAP message, the DL-MAP end IE. Each of these IEs is 4 bytes long. The overhead in bytes introduced by the DL-MAP message is described by equation 9.1. $N_{DL\ burst}$ is the number of downlink bursts in the frame.

$$OH_{DL-MAP} = 8 + 4 \cdot (N_{DL\ burst} - 3) \quad (9.1)$$

3) UL-MAP MAC Management Message

The UL-MAP message allocates access to the uplink channel. The length of the fixed part is for this message 7 bytes. The following IEs are 6 bytes long. One IE is used for every UL burst, i.e. for every subscriber station. The resulting overhead in bytes can be found in equation 9.2. N_{SS} is the number of transmitting subscriber stations.

$$OH_{UL-MAP} = 7 + 6 \cdot (N_{SS} + 2) \quad (9.2)$$

4) DCD MAC Management Message

The DCD message is transmitted periodically by the MBS to define the characteristics of a downlink physical channel. Three bytes construct the fixed part of the message, the rest of the message is formed by the TLV tuples. Numerous TLV encodings are defined to describe the downlink channel properties and the burst profiles. Each burst profile definition occupies 9 bytes.

The resulting overhead caused by the DCD message is defined by equation 9.3. $N_{DL\ burst\ profiles}$ represents the number of downlink burst profiles used.

$$OH_{DCD} = 68 + 9 \cdot N_{DL\ burst\ profiles} \quad (9.3)$$

5) UCD MAC Management Message

The UCD message is similar to the DCD, but it describes the uplink physical channel. The fixed part comprises 6 bytes. TLV part without definition of burst profiles is 32 bytes long and each burst profile used occupies additional 12 bytes [1]. The UCD overhead can be evaluated as in equation 9.4. $N_{UL\ burst\ profiles}$ represents the number of uplink burst profiles used.

$$OH_{UCD} = 38 + 12 \cdot N_{UL\ burst\ profiles} \quad (9.4)$$

6) Uplink sub-frame

The uplink sub-frame contains slots for ranging, which are mainly used during the initial network entry or re-entry during handover. The number of bytes used for bandwidth requests

can be calculated according to equation 12. N_{SS} is the number of subscriber stations. We assume that every SS sends one BW request every frame.

$$OH_{BW} = N_{SS} \cdot OH_{MAC\ PDU} \quad (12)$$

Expressed in OFDM symbols, equation 12 can be written as:

$$L_{BW} = \frac{N_{SS} \cdot OH_{MAC\ PDU}}{BpS} \quad (13)$$

We obtain the resulting number of OFDM symbols available for transmission of data MAC PDUs from the following equation.

$$L_{UL\ data} = L_{UL\ subframe} - L_{BW} - N_{SS} \cdot L_{SP} \quad (14)$$

B. Total Efficiency

Using equations 8, 11 and 14 it is possible to obtain the total number of OFDM symbols available for MAC PDUs as given by equation 15.

$$L_{data} = L_{frame} - L_{LP} - L_{FCH} - L_{DL\ burst\ \#1} - L_{BW} - N_{SS} \cdot L_{SP} \quad (15)$$

Another important overhead introduced by the MAC layer are the generic MAC headers and CRCs of the data PDUs. We suppose that the frame is fully used, the number of MAC PDUs which without considering fragmentation fit into one frame is given by equation 16, where k is the length including the generic MAC header and CRC of the MAC PDU in bytes. Applicable lengths are from 11 bytes (1 byte of payload) to 2047 bytes. The maximum length is restricted by the capacity of the Length field of the generic MAC header, which is 11 bits.

$$N_{MAC\ PDU} = \left\lfloor \frac{L_{data}}{k} \right\rfloor \quad (16)$$

Using the number of MAC PDUs in a frame, the number of OFDM symbols utilized for the data MAC PDUs overhead can be calculated, as given by equation 17.

$$L_{data\ MAC\ PDU\ OH} = \frac{N_{MAC\ PDU} \cdot 10}{BpS} \quad (17)$$

The number of OFDM symbols usable for the payload of the data MAC PDUs – SDUs from higher layers is given by equation 18.

$$L_{net\ payload} = L_{data} - L_{data\ MAC\ PDU\ OH} \quad (18)$$

Using the equation 6, efficiency on the MAC layer can be finally calculated. Results for various parameters will be presented in the next section.

IV. RESULTS IN MAC EFFICIENCY

The numerical values of the OFDM parameters, which are used to obtain the resulting efficiencies and haven't been presented before, are T_{frame} and T_{symbol} . T_{frame} defined by the standard IEEE802.16e-2005 [2], can have values from 2.5 ms to 20 ms. The third highest value, $T_{frame} = 10$ ms, is chosen for the calculations. T_{symbol} can be calculated using equation 19, with substituting the following: $G = 1/4$, $BW = 20$ MHz and $n = 144/125$. These values are allowed by the standard for license-exempt bands. Bandwidth of 20 MHz and the ratio of the cyclic prefix to the useful symbol time are both the largest allowed. The final symbol duration is then 13.89 μ s.

$$\begin{aligned} T_s &= T_b + T_g = (1/\Delta f) + G \cdot T_b = (1/\Delta f) \cdot (1+G) = \\ &= (N_{FFT} / F_s) \cdot (1+G) = \left[N_{FFT} / (\lfloor n \cdot BW / 8000 \rfloor \cdot 8000) \right] \cdot (1+G) \quad (19) \end{aligned}$$

Besides the main parameter, which is the number of subscriber stations (N_{ss}), other variables are chosen for the evaluated efficiency. These are the length of the data MAC PDUs, modulation/coding used, and number of burst profiles.

A. MAC PDU length

The length of the data MAC PDUs plays an important role for the efficiency value. The shorter the PDU is, the bigger part of it is occupied by the generic MAC header and CRC bytes, which for lower lengths significantly decreases the efficiency. The modulation QPSK 1/2 is assumed in the simulation. 1 DL burst profile and 1 UL burst profile is also considered.

In Figure 3, results for different number of subscriber stations (N_{ss}) are shown. It can be seen that the efficiency rises rapidly for smaller k values (approx. up to 100 bytes). After this point, the efficiency increases only gradually and for k values of 1000 bytes and more it is almost constant. At the same time it can be seen that for a certain MAC PDU length the largest number of subscriber stations has the lowest efficiency.

For higher number of subscriber stations, it obviously comes into effect for a lower initial PDU length. Nevertheless, the higher number of subscriber stations means lower efficiency.

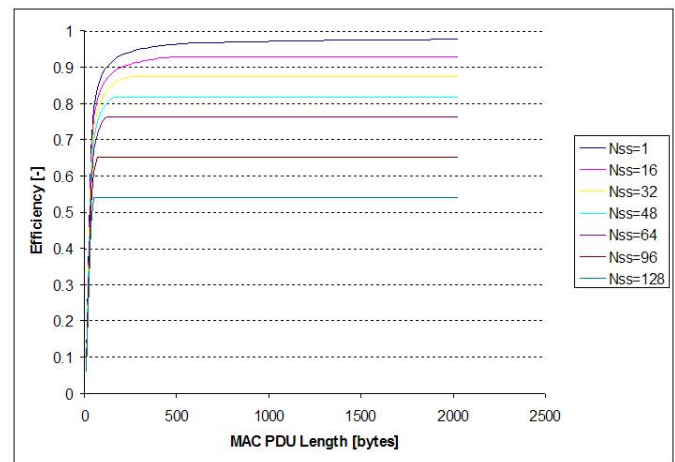


Fig.3. PMP efficiency – Parameter PDU length, parameter N_{ss}

B. Various modulation and coding

The influence of modulation and coding is presented when using 1 DL burst profile, 1 UL burst profile and fixing the MAC PDU length to 1024 bytes. When assuming this length or higher, the influence of the number of subscriber stations is much more noticeable than the influence of the PDU length.

Based on table 1, the efficiencies are calculated for six most common modulations/coding of them, omitting only the most robust BPSK 1/2 modulation. The modulation/coding types are numbered as in table 1.

Figure 4 shows that higher modulations usage means lower MAC overhead. That is due to the fact that the PMP broadcast messages don't have to be transmitted by the most robust modulation/coding. When a modulation/coding with a higher,

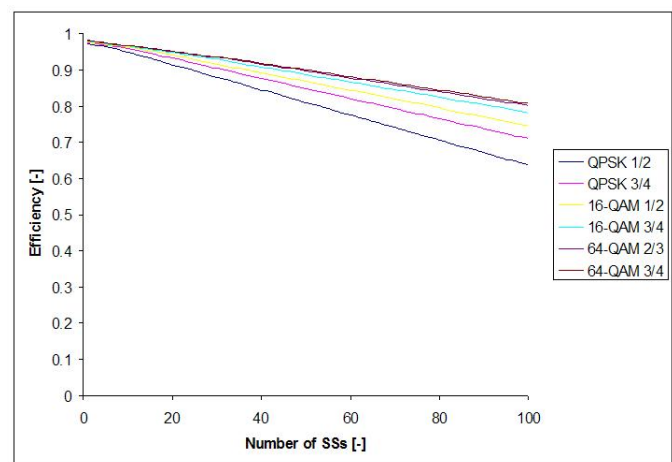


Fig.4. PMP efficiency – various modulations/coding, parameter modulation type

number of bytes per symbol is used the messages occupy a smaller portion of the PMP frame. For a higher number of subscriber stations the difference in efficiency for different modulations increases, because the more SSS are connected, the more OFDM symbols are used to send them and the more

is consequently saved.

It is obvious that lower modulations mean lower efficiency variations when assuming different number of subscriber stations. The higher modulation is able to keep the efficiency high. That is caused by the fact that higher modulations slightly compensate the influence of growing broadcast messages.

C. Various number of burst profiles

Another parameter, which affects performance on the MAC layer, is the number of burst profiles (BP). We assume that the MAC PDU length is 1024 bytes and more uplink and downlink burst profiles are specified. For UL/DL burst profile 1 modulation/coding 1 is used, for UL/DL burst profile 2 modulation/coding 2 is used, etc. Maximum number of burst profiles is 6, since 6 most common modulations are used.

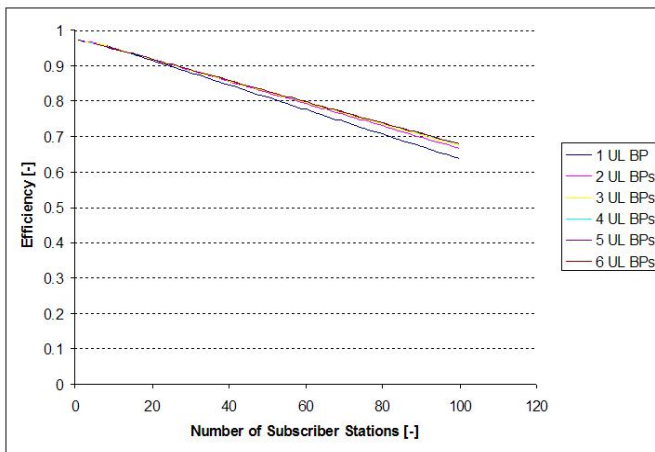


Fig.5. PMP efficiency – various number of N_{ss} , parameter BPs

Since the broadcast messages are assumed to be always transmitted using QPSK 1/2 modulation, using more burst profiles has only the influence of decreasing the efficiency because of additional overhead to define these BPs. This extra overhead is relatively small (approx. 6% between 1 BP and 6 BPs).

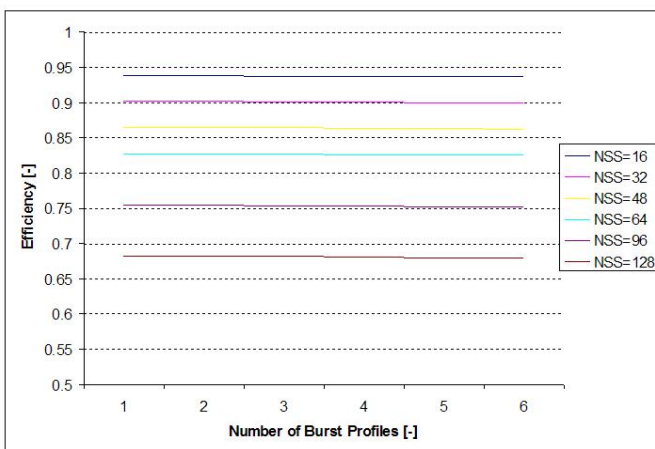


Fig.6. PMP efficiency – various number of burst profiles, parameter NSS

Figure 5 shows that the lower number of burst profile gives the lowest efficiency when N_{ss} is higher. On the other hand, Figure 6 depicts the fact that the BPs has a minor impact on MAC efficiency for particular number of subscriber stations. When the network has a lower number of subscriber stations then they will have a better efficiency.

V. CONCLUSIONS

Performance on the MAC layer of the IEEE 802.16 WirelessMAN standard has been analyzed. The Point to Multipoint mode is well suited for higher number of subscriber stations. Using the QPSK 1/2 modulation and MAC PDU length of 1024 bytes, the efficiency on the MAC layer is for 100 subscriber stations connected to the base station around 75%.

The data MAC PDU length is the parameter that highly influences the MAC layer performance. Obviously longer PDUs mean less MAC overhead. Another way of reducing the MAC overhead is usage of a higher modulation/coding. Especially for the PMP mode, transmitting the broadcast message with higher number of bytes per symbols gives more space to the data MAC PDUs transmission.

Introducing some changes to the IEEE 802.16 standard, for example defining more space saving TLV tuples for some of the management MAC messages could also bring some minor savings, but as the standard already experienced a gradual evolution and being implemented in many real-life applications, it doesn't make any sense to call for its change.

ACKNOWLEDGMENT

The authors would like to acknowledge the contributions of both Czech Technical University and their colleagues from IST-EU FIREWORKS project consortium.

REFERENCES

- [1] "802.16-2004, IEEE Standard for Local and Metropolitan Area Networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems," New York, USA: The Institute of Electrical and Electronics Engineers, 2004. ISBN 0-7381-4070-8
- [2] "802.16e-2005, IEEE Standard for Local and Metropolitan Area Networks – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems – Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1," New York, USA: The Institute of Electrical and Electronics Engineers, 2006. ISBN 0-7381-4857-1.
- [3] M. K. Marina and S. R. Das, "Impact of Caching and MAC Overheads on Routing Performance in Ad Hoc Networks," *Computer Communications*, vol. 27, no. 3, pp. 239-252, February 2004.
- [4] G. R. Hiertz, L. Stibor, J. Habetha, E. Weiss, and S. Mangold, "Throughput and Delay Performance of IEEE 802.11e Wireless LAN with Block Acknowledgements," in *European Wireless 2005*, Nicosia, Cyprus, pp. 246-252, April 2005.
- [5] S. Redana, "Advanced Radio Resource Management Schemes for Wireless networks," Ph.D. dissertation, Politecnico di Milano, Milano, Italy, 2005.
- [6] F. Ohrtmann, "WiMAX Handbook: Building 802.16 Wireless Networks," New York, USA: McGraw-Hill, 2005. ISBN 0-07-145401-2.
- [7] L. Nuaymi, *WiMAX: Technology for Broadband Wireless Access*, Chichester, England: John Wiley & Sons, 2007. ISBN: 0-470-02808-4.



Ardian Ulvan received the B.Eng degree in electrical engineering in 1997 from The University of North Sumatra, Indonesia, and MSc in Networks Engineering from Sheffield Hallam University, UK in 2001. In 2006 he received the accredited Engineering (Ing.) acknowledgement from Czech Technical University in Prague, Czech Republic. His PhD degree in Telecommunication Engineering is awarded in 2009 from CTU in Prague. In 1999-2005 periods he worked as a Senior Lecturer in Department of Electrical Engineering, The University of Lampung, Indonesia. He is currently working as researcher at wireless networks research group Department of telecommunication engineering, CTU in Prague. His research interests include MAC functionalities on broadband and gigabit wireless based on standards IEEE802.16d/e/j/m and 3GPP LTE/LTE-A, multihops-multicells wireless networks and the IP Media Subsystem (IMS). He involves in European research projects FIREWORKS (IST-FP6) and ROCKET (IST-FP7) and several projects at CTU R&D Centre.



Robert Bestak received his engineering degree from the Czech Technical University in Prague, Faculty of Electrical Engineering, in 1999. Within 1999/2000, he did one-year engineering program in telecommunications and computer networks at the Institute EERIE de l'Ecole des Mines d'Alès, Nimes, France. In 2003, he received his Ph.D. degree in computer science from ENST Paris, France. Since 2004, he works as a researcher at the Department of telecommunication engineering, CTU in Prague. Since 2006, he heads wireless research group at the department. His research interests include RRM techniques in HSPA/LTE systems and multi-hop networks. He participated in EU FP projects ALLIPRO, FIREWORKS and he currently participates in EU FP7 project ROCKET. He has been involved in several R&D Centre projects.

Vit Andrlík received his engineering diploma from the Czech Technical University in Prague, Faculty of Electrical Engineering, in 2008. He did some researches on MAC functionalities of WiMAX 1.0 and WiMAX 2.0. He is currently works as a solution engineer at Siemens Enterprises Communication.

Loop-back Action Latency Performance of an Industrial Data Communication Protocol on a PLC Ethernet Network

Endra Joelianto, *Member IEEE*, and Hosana

Abstract—One of the well known industrial data communication protocols is Modbus which is widely used in industrial automation due to its availability. Modbus protocol can be implemented in many ways according to its network. Network using serial RS485 is well known in industry especially for long range communication, but realtime input/output (I/O) communication over ethernet is fairly new in the industrial environment. There are many questions about the reliability and performance of the Modbus for its optimization especially in its networking.

Performance metrics and tests for IT infrastructure equipment have been used for many years, but now with realtime communication being used more, users are asking whether their desktop, laptop, or palm computer can handle the performance requirements of these network intensive applications. These same questions can be asked for industrial equipments as well, such as Programmable Logic Controller (PLC) ethernet networks. In this paper, serial communication RS 485 and TCP/IP are used as physics of Modbus data communication protocol. Action latency performance of this protocol will be tested on the ethernet network. An extension of the ethernet network with serial RS485 network will also be considered in relation with two different network topologies. The algorithm that used to test Modbus is the Media Access Control (MAC) algorithm, which mainly determines the performance of a network.

Index Terms— Industrial ethernet networking, Modbus, TCP/IP, MAC, programmable logic controller.

I. INTRODUCTION

Conventional industrial sequential control systems adopt a master-slave centralized control approach. A central controller (master) makes major control decisions and controls low-level I/O devices via point-to-point connections. Although it is reliable, this control architecture is inflexible

for long implementation and reconfiguration time. Industrial equipment vendors and users were primarily concerned with inherent nondeterministic performance of industrial communication network characteristics. In general, there is no guarantee the data transmitted over wire by the source will reach the destination. This is unacceptable in the industrial world. Therefore, new protocols and methods have been developed to overcome these limitations [1].

With the development of the computer network technology and intelligent sensors and actuators, Modbus technology is being used more and more widely nowadays. Modbus is a network for connecting field devices: sensors, actuators and field controllers such as PLCs, regulators, driver controllers and so on. It is a kind of realtime communication systems and is based on a layered structure deduced from the seven layers OSI model. For time-critical control systems such as realtime control system, to reduce message delay is one of the major considerations. While for safety-critical systems such as fire alarm systems, to avoid data loss is of high importance. For different control systems, different approaches are adopted according to the requirements of the system [2].

The enterprise performance management of data network is becoming more important as computer networks grow in size and complexity. An increase in frequency, type and severity of faults occurring on these networks has been linked to this growth. Monitoring changes in topology and traffic flow is essential for management of dynamic communication networks. For automation users, deterministic performance of the Modbus is essential for control, messaging and large data acquisition applications. Simply deploying the latest switching technologies may not ensure determinism if those features are not carefully designed.

A comprehensive examination of the network communications matrix, message traffic, host protocols used, and capabilities of the infrastructure can lead to greater performance and reliability for investment. Schneider Automation NCSE's has identified those inefficiencies that rob performance such as reported in [3]: (1) System bottlenecks and congested message queues, (2) Unauthorized hosts or devices on networks, (3) Unnecessary Protocol in use, (4) Excessive collisions, errors and delays, (5) Excessive broadcast or multicast traffic from switches, routers and PC's. Identifying and correcting problems in these areas will

Manuscript received March 27, 2009. This work was partially supported by the Incentive Research Program, State Ministry of Research and Technology, Indonesia under Grant 97M/Kp/XI/2007.

E. Joelianto is with the Instrumentation and Control Research Group, Department of Engineering Physics, Bandung Institute of Technology, Bandung 40132, Indonesia (corresponding author phone: +62-22-2504424; fax: +62-22-2506281; e-mail: ejoel@tf.itb.ac.id).

Hosana was with the Instrumentation and Control Research Group, Department of Engineering Physics, Bandung Institute of Technology, Bandung 40132, Indonesia.

produce a cleaner, faster and more effective network.

One example of Modbus that functions well at this moment and is able to solve a few problems that have not been solved before is Modbus TCP application on a ship [4]. The main control system is able to manage generation and distribution energy in the ship and also to manage the cargo. Modbus TCP in the ship is used to manage and control all the main system, such as propulsion system, electricity distribution, heating, air conditioning, pump, technical equipment, security, state monitoring, etc.

This project was started in 2002 where Aker Kaerner proposed implementation of a Modbus TCP based *Transparent Ready* solution for the Viking Dynamic, a platform supply vessel managed by Eidesvik AS. The system uses web-enabled architecture that transmits data directly to the ship owner via the ship's satellite connection. The use of remote diagnostics also generates savings because maintenance can be planned in advance and new parts can be ordered before the ship gets back to its home port. This is good news as the vessel spends less time at dock which reduces port fees.

There were several reasons that contributed directly to the success of the project. First, because of the open nature of the architecture, it facilitated collaboration between people, system, and products. Second, it permitted easy access to data using universal technologies, i.e. ethernet TCP/IP via Modbus and the Internet that people were already familiar and comfortable with. Security problems were solved by building the architecture through the use of dedicated components such as routers, firewalls, and virtual private networks for the Modbus TCP application. The architecture allowed remote appraisals or diagnostics of installations, machines, panel boards and other equipment at less costs and without special training since most encounters with these things are no more than looking at a web page. Moreover, human machine interface (HMI) could be located in a computer anywhere with easy and secure access to a network, public or private. This application shows that by using Modbus TCP many problems in automation can be solved and brings a new way to develop automation projects [4].

Our research is focused on the performance of Modbus protocols in PLC. In this research, a widely used Modbus, serial RS485 and TCP will be tested on a PLC Twido network. Mathematical analysis is taken to evaluate the realtime performance of the system with respect to the throughput as well as the message delay. The remainder of the paper is organized as follows. In section 2, we describe the basic theory of Modbus, PLC, Topology, MAC algorithm and performance testing methodology. In section 3, we describe the experiment that have been done, simplify the model and give some assumptions. In section 4, we analyze the Modbus performance and section 5 will give the conclusion.

II. BASIC THEORY

A. Modbus Protocol

Modbus is an application layer messaging protocol, positioned at level 7 of the OSI model that provides client/server communication between devices connected on different types of buses or networks. Modbus has been known as industry's serial de facto standard since 1979 and continues to enable millions of automation devices to communicate. The Internet community can access Modbus at a reserved system port 502 on the TCP/IP stack. Modbus is a request/reply protocol and offers services specified by function codes. Modbus function codes are elements of Modbus request/reply Protocol Data Units (PDUs). Fig. 1 shows the Modbus communication stack.

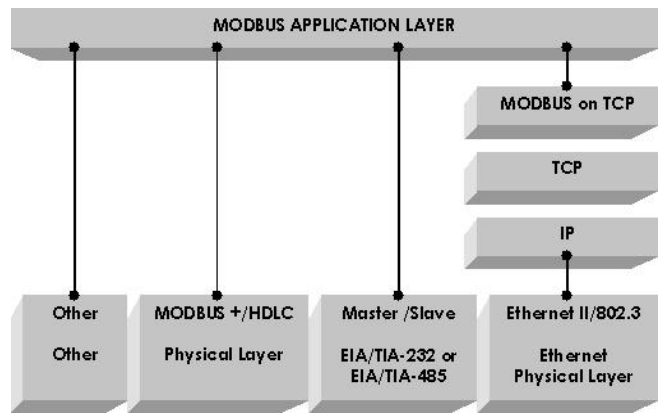


Fig. 1. Modbus communication stack.

The Modbus protocol allows an easy communication within all types of network architectures. Every type of devices (PLC, HMI, Control Panel, Driver, Motion control, I/O Device, etc) can use Modbus protocol to initiate a remote operation [5]. A networking example of Modbus is shown in Fig. 2.

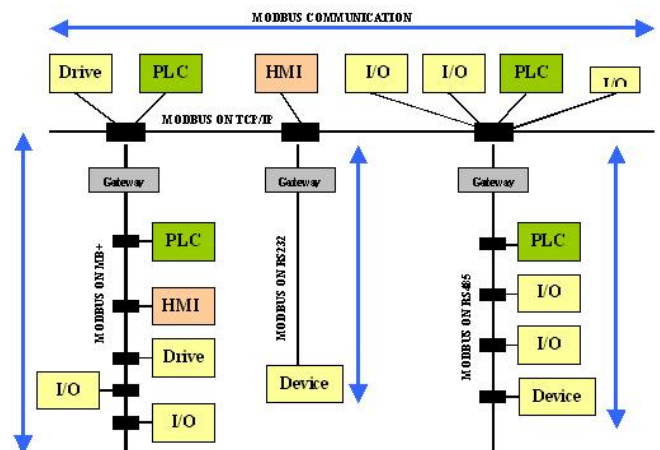


Fig. 2. The architecture of Modbus networking example.

B. Modbus Serial

Modbus Serial Line protocol is a Master-Slave protocol. This protocol takes place at level 2 of the OSI model. A master-slave type system has one node (the master node) that issues explicit commands to one of the slave nodes and processes responses. Slave nodes will not typically transmit data without a request from the master node, and do not communicate with other slaves. The mapping of Modbus protocol on a specific bus or network introduces some additional fields on the Protocol Data Unit (PDU) is shown in Fig. 3. The client that initiates a Modbus transaction builds the Modbus PDU, and then adds fields in order to build the appropriate communication PDU.

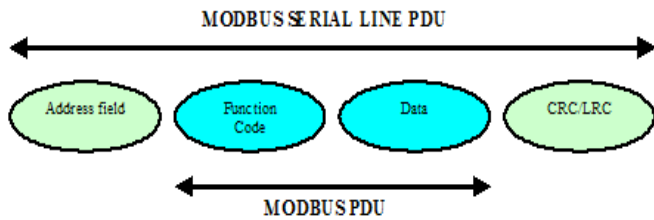


Fig. 3. Modbus mapping.

The Modbus data link layer comprises two separate sub layers:

- The master/slave protocol
- The transmission mode (RTU vs ASCII modes)

The behavior of Modbus master and slave are shown in Fig. 4 and 5 respectively.

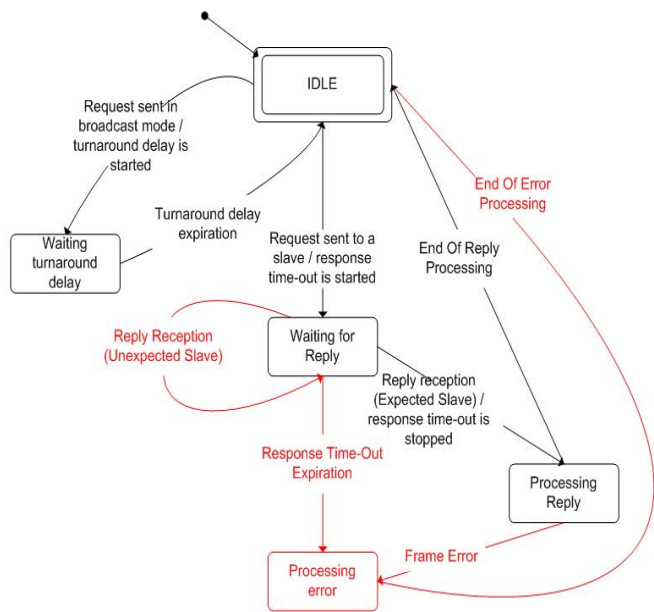


Fig. 4. Master behavior of Modbus.

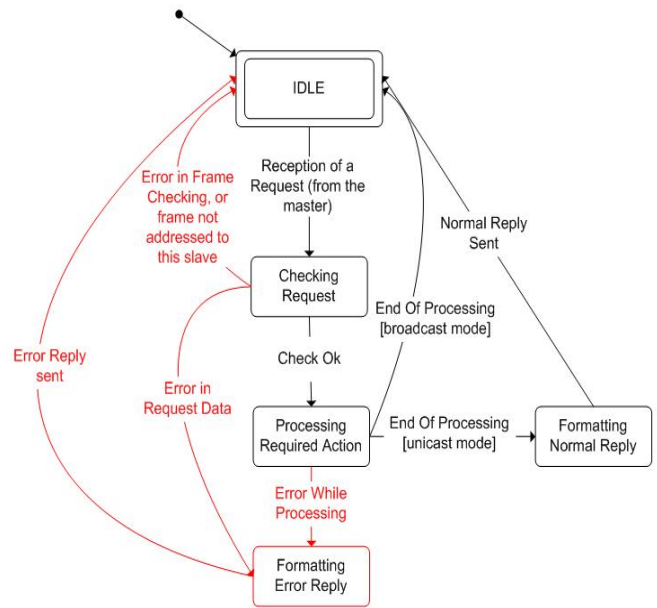


Fig. 5. Slave behavior of Modbus.

This following figure shows the time diagram of 3 typical scenarios of Master/Slave communications [6].

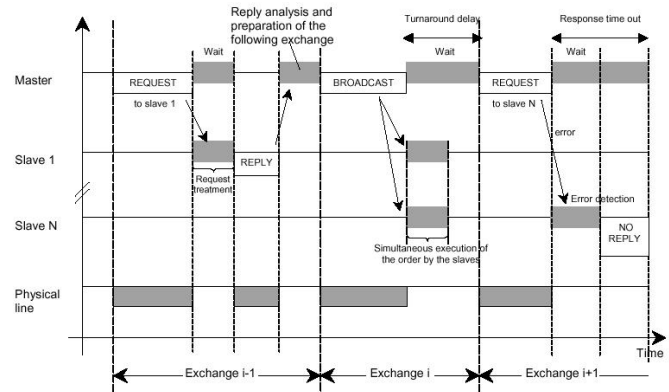


Fig. 6. Time diagram of Modbus Master/Slave communication.

C. Ethernet & Modbus TCP

Ethernet/IP uses a peer-to-peer and producer/consumer architecture for its data exchange versus a master/slave or command/response architecture. This allows for greater flexibility in the network and system designs, which fits better into the Ethernet networking model. In addition, Ethernet/IP splits its communication into configuration and management traffic (implicit messaging). Configuration and management traffic uses TCP/IP, and realtime I/O traffic uses UDP/IP.

The producer/consumer model for Ethernet/IP allows multiple modes of communication to be chosen for realtime data exchange. The most common mode for producing data is called cyclic production. During cyclic production, the producer will send data at a particular rate called the Requested Packet Interval (RPI). The RPI and corresponding Accepted Packet Interval dictates the speed of the data

produced over the network regardless of the rate at which the actual data values change.

Ethernet/IP also uses an object-oriented model. Some objects, such as the Identity object, TCP/IP object, and the Ethernet link object, are required by all Ethernet/IP devices. These map basic information about the device into the object model. Other objects are device specific, and while basic definitions of them may exist in the specification, the exact information recorded in the object is specific to the device and application [7][8].

A communicating system over Modbus TCP may include different types of device:

- A Modbus TCP Client and Server devices connected to a TCP/IP network
- The Interconnection devices like bridge, router or gateway for interconnection between the TCP/IP network and a serial line sub-network which permit connections of Modbus Serial line Client and Server end devices.

The architecture of the Modbus TCP can be described as the Fig. 7. The response of Modbus TCP is non-deterministic with the best reaction time is 20 ms. To improve performance, realtime with RTPS (Realtime Publisher Subscriber) that utilizes UDP/IP but this is not really realtime standard. The available bandwidth for TCP/IP is 90%-100% [9].

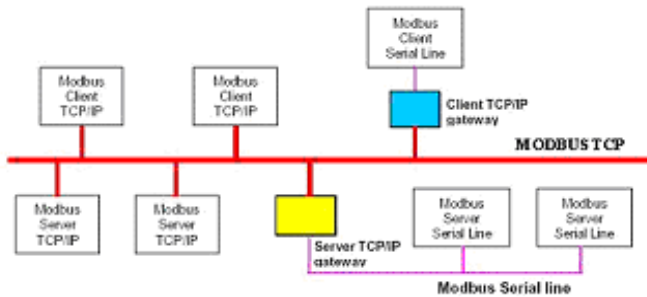


Fig. 7. Modbus TCP communication architecture.

D. Programmable Logic Controller

By definition, a Programmable Logic Controller (PLC) is a solid state control system that continuously monitors the status of devices connected as inputs. Based upon a user written program, stored in memory, it controls the status of devices connected as outputs. PLC that used in this research is PLC Twido. PLC Twido is a PLC that made by Schneider-Telemecanique and it is included into PLC nano category.

PLC is able to make network, the typical architecture of the industrial network is shown in Fig. 8. Level 0 consists of sensors and actuators. Level 0.5 consists of smart devices which have capability to perform simple control actions. PLC and Human Machine Interface (HMI) are located in Level 1. Level 2 is called Host, it links industrial automation networks with the office automation networks.

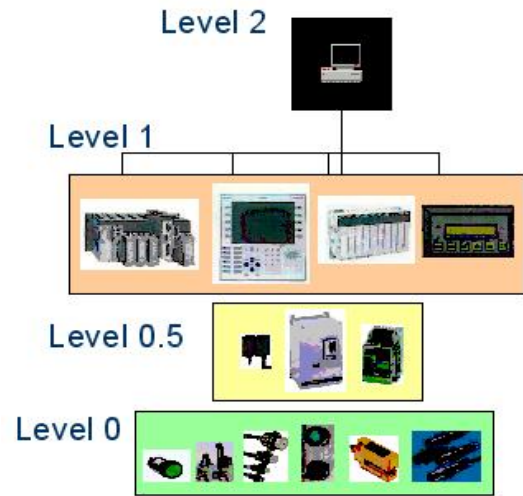


Fig. 8. PLC networking.

Level 1 in the Fig. 8 consists of PLC that can communicate with the highest level (Level 2) and the lowest level (Level 0). Hence communication is an important factor in the industrial automation implementation. PLC Twido supports communication in Modbus, ASCII and Remote Link. In this experiment the evaluated communication is Modbus, either TCP or serial RS485.

E. Predictive P-Persistent CSMA Protocol

MAC algorithm shown in Fig. 9 is used to control the access of a node to the shared media. To reduce the message delay, LonWork uses an enhanced algorithm which belongs to the family of Carrier Sense Multi Access (CSMA). It is a variant of *p*-persistent CSMA with the difference that the parameter *p*, the probability with which a message is transmitted when the channel is idle, varies according to the traffic condition.

When the traffic is high, *p* is small. When the traffic is low, *p* rises. Such a strategy decreases the collision during heavy traffic and improves the utilization of the channel when the traffic is low. For such a protocol, a ready node, the one that has message to send, will sense the channel before transmission. If the channel is detected idle, with the probability *p* varies with the current backlog (i.e. the number of ready nodes), it will transmit the message. With the probability $1 - p$, it will delay the transmission by one slot time. If at this new point, the channel is detected idle, it will repeat the same process. If the channel is sensed busy, this node will reschedule the transmission according to a random delay time [2].

The implementation of this algorithm in the MAC layer is shown in the Fig. 10. The probability *p* is given by $p = 1/(16BL)$, where *BL* is the estimated number of ready nodes ($1 \leq BL \leq 63$). Then, the Random Delay Time (RDT) is calculated according to *p* and the RDT timer is started. If the

channel is always sensed idle during the period of this RDT. This node will start transmission when the RDT is expired. If before the end of the RDT, the channel is detected busy, the same process will be repeated. A ready node monitors the state of the channel and determines the channel to be idle if it senses no transmission during the β_1 period. Nodes without a ready message during this period will remain in synchronization for the duration of the followed random delay time. And if the message is ready after the end of β_1 period, it will be scheduled to transmit in one of the $(0 \dots 16 \cdot BL - 1)$ slots during this random delay time.

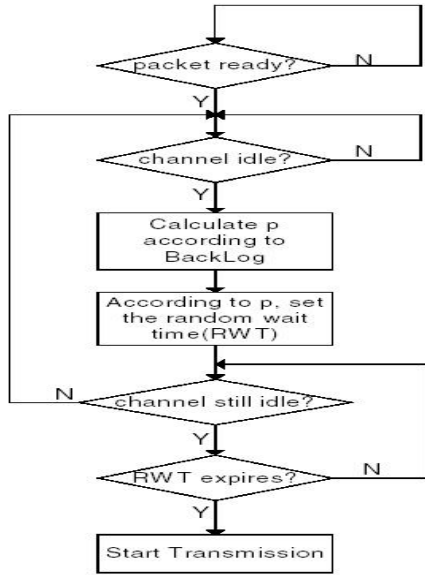


Fig. 9. MAC algorithm.

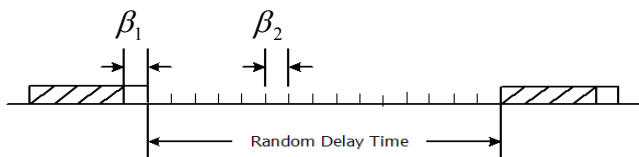


Fig. 10. Random delay time.

F. Performance Testing Methodology

Latency is defined as the time interval between a message being sent to a device and a corresponding event occurring. Action Latency tests the ability for a device to either cause or measure a physical action and determine the time between the action and the associated network packet. If the device is being commanded to act, it is the time between the device receiving the network packet and the action happening. If the device is producing data, it is the time between the physical action and the device sending the network packet. These tests will be highly device specific, and require application level programming on the part of the tester. These tests will also be affected by multiple error sources, since the test equipment may consist of more than one device [10][11]. Latency approach to test the performance of Ethernet/IP devices

carried out by the Open DeviceNet Vendor Association (ODVA) can be found in [12].

In order to eliminate the need for multiple devices to execute the test, it may be possible to construct a loop-back test. This loop-back test would connect an output on the device to an input, and then command the device to send an output and wait for the input to be measured by the device. While not all devices will have both inputs and outputs, many of the test equipment to one device, since the test equipment would only have to measure the time delay between networks packets.

The loop-back test would be subject to many different types of errors and latencies. This test will be much more valuable to users than to developers, since it will not show the affects of the individual errors of latencies. The major sources of error and latency will probably be from the physical energy conversion creating an output signal and reading the input. These numbers are usually well known by the vendor and can be accounted for in the performance analysis. Another source of error and latency would be due to the processing overhead and network protocol stack. A time analysis of the action latency loop-back test procedure is shown in Fig. 11. and equations (1) as follows [10]:

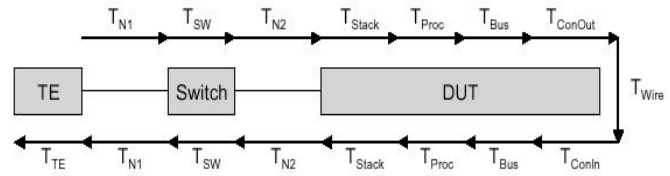


Fig. 11. Time analysis for action loop-back test.

$$T_{DUT_ALLB} = 2 \times T_{stack} + 2 \times T_{Proc} + 2 \times T_{Bus} + T_{ConOut} + T_{Wire} + T_{ConIn} \tag{1}$$

$$T_{ALLB} = 2 \times T_{Network} + T_{DUT_ALLB} + T_{TE} \tag{2}$$

where:

- T_{DUT_ALLB} : Latency Time for the Device Under Test for the Action latency Loop-Back Test
- T_{Bus} : Latency Time for the internal device bus, may be zero if device does not use a bus
- T_{ConOut} : Latency Time to perform the output energy conversion
- T_{Wire} : Latency Time for the signal to travel along the wire
- T_{ConIn} : Latency Time to perform the input energy conversion
- T_{ALLB} : Latency Time for the Action Latency Loop-Back Test
- $T_{Network}$: Latency time due to network overhead
- T_{TE} : Latency time due to the test equipment
- T_{Stack} : Latency time due to the DUT's network protocol stack

III. MEASUREMENT OF THE APPLICATION RESPONSE TIME

A. Modbus Experiment Configuration on PLC Network

Important requirements in realtime applications are the application response time and throughput. The application response time is the time measured from the moment, when the application calls the middleware to send a publication through the network layers, to the time, when the subscribed applications get this publication. The application response time can be affected by the network load, the network bandwidth, the implemented network stack, the processor speed, and in most case by the operating system.

The experiment that has been done is an experiment to test the packet delay between the HMI through TCP/IP connection into PLC Twido. Another experiment tests packet delay between the HMI through TCP/IP connection into PLC Twido and then the data goes into another PLC through Modbus serial RS485. The second experiment uses two network topologies, i.e. star and ring topology. The 1st, 2nd, and 3rd experiment configurations are shown in the following figures.



Fig. 12. 1st Experiment configuration.

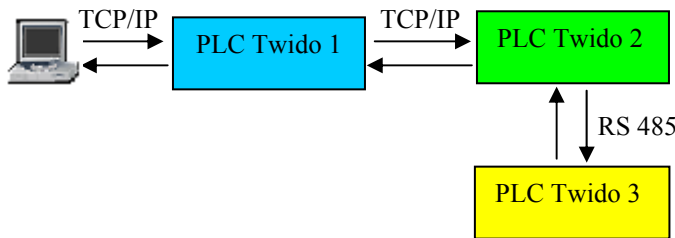


Fig. 13. 2nd Experiment configuration.

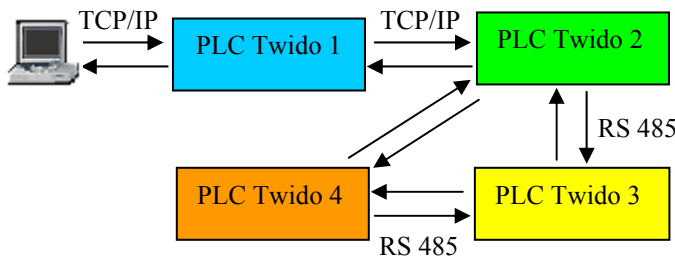


Fig. 14. 3rd Experiment configuration.

From all of these experiments, it is calculated the time required by the transmitted packet sent from the HMI via PLC network and then returned to the HMI again. One packet contains 100 words of data. The experiment is carried out 50 times. The 2nd experiment can be said as a star topology and the 3rd experiment is a ring topology [13]. The algorithms of the developed ladder program in the experiments are shown in Figure 15, 16 and 17.

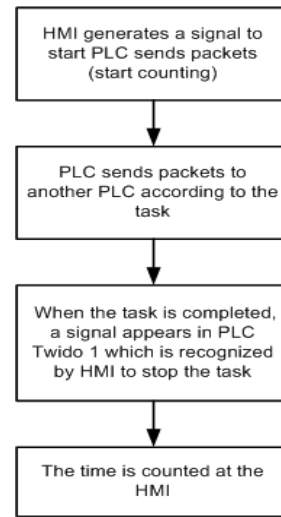


Fig. 15. Counting algorithm.

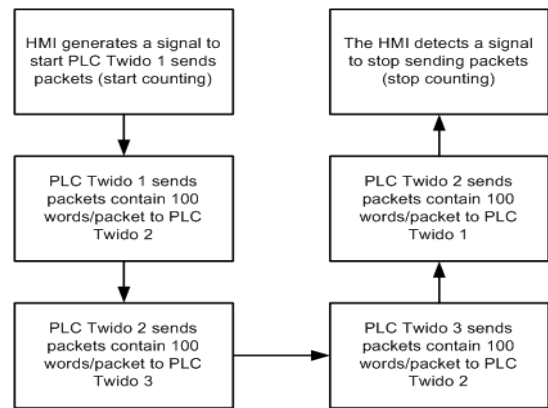


Fig. 16. Block diagram of 2nd experiment algorithm (star topology).

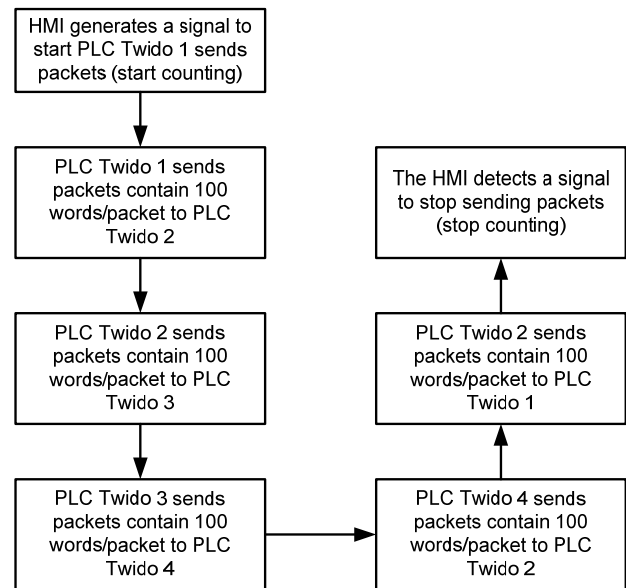


Fig. 17. Block diagram of 3rd experiment algorithm (ring topology).

B. Results

The response time of 1st experiment varies from 12 to 20 ms, the 2nd experiment varies from 98 to 106 ms and the 3rd experiment varies from 92 to 106. The mean time value of the 1st experiment is 17.75862 ms, the 2nd experiment is 101.667 ms and the 3rd experiment is 101.72 ms.

The result of the experiments can be seen in the graphics shown below.

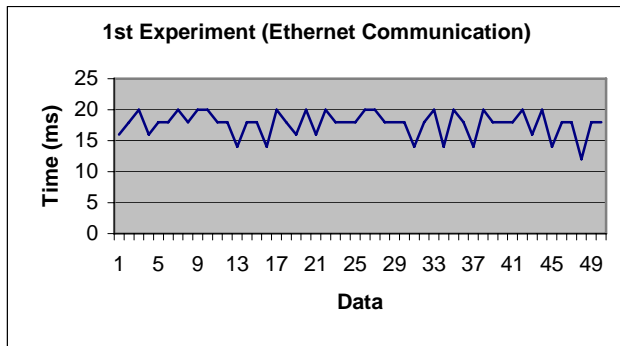


Fig. 18. The result of 1st experiment.

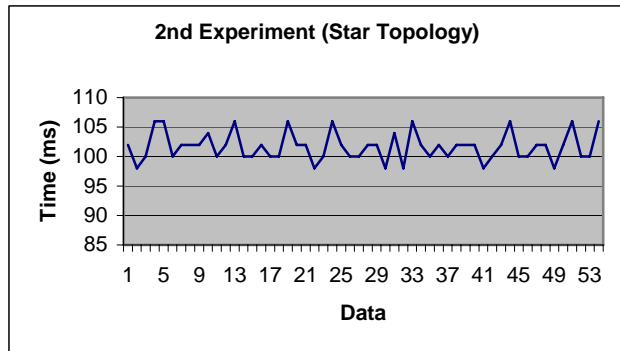


Fig. 19. The result of 2nd experiment.

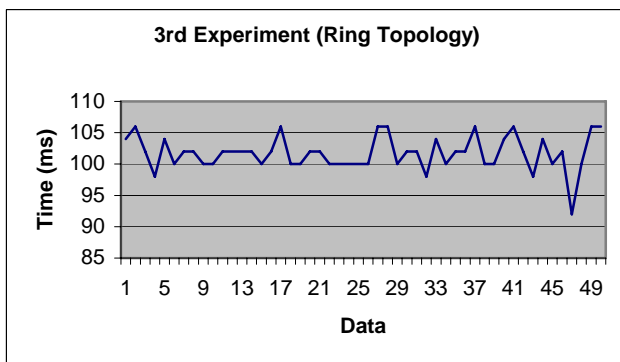


Fig. 20. The result of 3rd experiment.

IV. ANALYSIS

A. Topology, Network and Frame Analysis

Network topology usually gives big different on the performance of a protocol. In these experiments, we only use 2 simple network topologies, i.e. star and ring. From the results of the experiment, it can be seen that there is no big different between the response time of the star topology and the ring topology. The mean of the star topology response time is 101.667 ms and the ring topology response is 101.72 ms. If the analysis is based on the network that is used, it gives very big different. Communication through Ethernet is faster than using serial RS485 because the communication that occurs in Ethernet is full-duplex while communication using serial RS485 is half-duplex. The mean of Ethernet communication response time is 17.75862 ms while the experiment that uses serial RS485 is 101.667 ms for star topology and 101.72 ms for ring topology. Although the experiments that use serial RS485 are also through the Ethernet communication but it still slower than the Ethernet communication only.

B. Action Latency Analysis

The experiment is tested under action latency methodology. According to Fig. 11, the experiments in Fig. 12-14 could also be described as that figure. The test equipment (TE) in this experiment is the PC and the Device Under Test (DUT) in this experiment is PLC. In connection with latency methodology, the experiments could be drawn as in Fig. 21, 22 and 23.

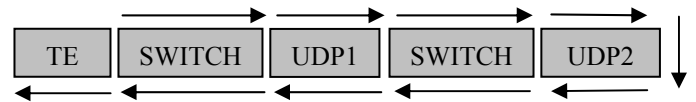


Fig. 21. Action latency configuration of 1st experiment.

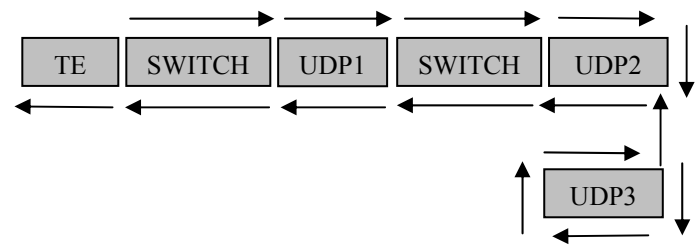


Fig. 22. Action latency configuration of 2nd experiment.

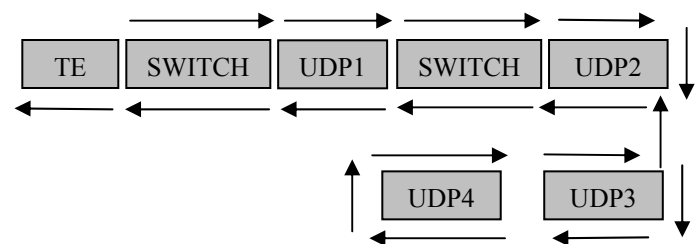


Fig. 23. Action latency configuration of 3rd experiment.

If the figures of action latency configuration for each experiment above are compared with the Figure 11, the response time result can be said as the result of T_{ALLB} for each experiment. The length of Ethernet cable from TE to switch and UDP to switch is about 5 meter and the length of serial RS485 cable from every UDP to UDP is about 3.6 meter. From this experiment can be said that cable length gives little effect to data communication.

C. Delay Analysis

According to the result of all the experiments, transmitting and receiving packets produce delay time. There is uncertainty in the delay time, as there is fluctuation in the measured time. This happens because of message delay phenomenon that usually occurs in the network communication. There are mainly three factors that contribute to the message delay.

1. Waiting delay: the delay between the time when the message arrives and the time when the channel is successfully caught by the message.
2. Transmission delay: the delay between the times that the first and last bits of the message are transmitted.
3. Propagation delay: the delay between the time that the last bit is transmitted at the source node and the time that it is received by the destination node.

In addition, when a message enters the OSI model, it passes through it with different processes by different layers. These processes produce delay. However, when it is compared with above delays, it is negligible [2] and it will not be considered here.

V. CONCLUSION

The paper has shown the loop-back action latency performance comparison of Modbus in PLC network by using Ethernet, serial RS485 and also using two different topologies, ring and star topology. From the experiment and the analysis that have been discussed in the paper, it can be summarized as follow:

- Communication through Ethernet is faster than through serial RS485 in PLC Twido Network
- Different topologies give little effect on the performance of Modbus in PLC Twido
- The cable length also gives little effect on the performance of Modbus in PLC Twido

Further research direction is as suggested in [14].

- The three factors that contribute to the message delay need to be tested in order to find out the value of those delays.
- For RS485 networks, efforts should focus on reducing delay.
- For Ethernet networks, research needs to address the throughput limitations and fairness problems, while preserving the small delays.

REFERENCES

- [1] J. Hops, B. Swing, B. Phelps, B. Sudweeks, J. Pane, and J. Kinslow, "Non-deterministic DUT behavior during functional testing of high speed serial busses: Challenges and Solutions," in *2004 Proc. International Test Conference*.
- [2] X. Chen, and G. S. Hong, "Real-time performance analysis of a fieldbus-based network," in *2002 Proc. Information Decision and Control (IDC)*, Adelaide, Australia.
- [3] *Optimizing Ethernet Network*, Schneider Automation Network Certification Services Team, North Andover, MA, USA, 2001. Available: <http://www.us.telemecanique.com>.
- [4] "Modbus sails along on powered by ethernet," *The Industrial Ethernet Book*, 28, pp. 38-39, Sept. 2005.
- [5] *MODBUS Application Protocol Specification*, May 2002. <http://www.MOBBUS.org>.
- [6] *MODBUS over Serial Line Specification and Implementation Guide*, Feb. 2002. Available: <http://www.MOBBUS.org>.
- [7] O. Dolejs, P. Smolik, and Z. Hanzalek, "On ethernet use for real-time publish-subscribe based applications," *IEEE*, 2004. Available: <http://dce.fdk.cvut.cz/hanzalek/publications/Hanzalek04.pdf>.
- [8] W. Stallings, *Data and Computer Communication*, 6th ed., Prentice Hall, 2000.
- [9] L. Larsson, "Fourteen industrial ethernet solutions under spotlight," *The Industrial Ethernet Book*, 28, pp. 16-23, Sept. 2005.
- [10] J. D. Gilsinn, "Industrial ethernet takes the test," *ISA-InTech*, Sept. 2005. Available: <http://www.isa.org/InTechTemplate.cfm>.
- [11] J. D. Gilsinn, "Real time I/O performance metrics and tests for industrial ethernet," *ISA Automation West*, 2004. Available: <http://www/isa.org>.
- [12] "Performance Test Methodology for EtherNet/IP Devices version 1.0," *EtherNet/IP Implementors Workshop*, ODVA, 2005.
- [13] Y. Song, A. Koubaa, and F. Simonot, "Switched ethernet for realtime industrial communication: modelling and message buffering delay evaluation," in *2002 Proc. 4th IEEE WFCS*, Vasteras, Sweden.
- [14] H. S. Yang, M. Reisslein, M. Herzog, M. Maeir, and. Wolisz, *Metro WDM networks: comparison of ring and star topologies*. Available: <http://www.tkn.tu-berlin.de/publications/papers/gc5.pdf>.

Endra Joelianto (M'01) received the B.Eng. degree in Engineering Physics from Bandung Institute of Technology, Indonesia in 1990, and Ph.D. degree in Engineering from The Australian National University (ANU), Australia in 2002.

He was a Research Assistant with Instrumentation and Control Laboratory, the Department of Engineering Physics, Bandung Institute Technology, Indonesia from 1990-1995. Since 1999, he has been with the Department of Engineering Physics, Bandung Institute of Technology, Bandung, Indonesia, where he is currently an Assistant Professor. His research interest includes hybrid control systems, discrete event systems, artificial intelligence, robust control and intelligent automation. He has edited one book on intelligent unmanned systems published by Springer-Verlag, 2009 and published more than 50 research papers.

Dr. Joelianto currently is an Editor of the International Journal of Artificial Intelligence (IJAI). He is the Chairman of Society of Automation, Control & Instrumentation, Indonesia.

Hosana was born in Jakarta, Indonesia on January 12th, 1983. He received the B.Eng. degree in Engineering Physics from Bandung Institute of Technology, Indonesia in 2005.

After graduated, he worked as a Research Assistant with Programmable Logic Controller-Research Group (PLC-RG), Bandung, Indonesia in the areas of instrumentation and control such as PLC, HMI, DCS, etc. From 2006-2007, he worked at PT. Wifgasindo Dinamika Instrument Engineer, Indonesia as a system integrator and EPC (Engineering, Procurement and Construction) company. At PT. Wifgasindo, he developed a system for ConocoPhillips-Indonesia called Puyuh Load Shedding System. This system was design to avoid blackout that could happen in power systems. Since June 2007, he has been with PT. Scada Prima Cipta also as a system integrator and EPC company. He is responsible in designing and developing new systems in instrumentation and control.

“Wayang Authoring”: A Web-based Authoring Tool to Support Media Literacy for Children

Wahju Agung Widjajanto, Michael Lund, and Heidi Schelhowe

Abstract—In our web-based platform “Wayang Authoring” children with different cultural backgrounds can share stories and make experiences in culturally different storytelling styles. The idea of Wayang Authoring is based on the Indonesian ancient art form Wayang. In Wayang Authoring children are able to compose a story by using digital puppets, saving, and sharing it. The research question focuses on if and how the design of our system can support media literacy for children, enhance creative storytelling and self-expression as well as help to share cultural diversity. In this article the Wayang Authoring platform and its background is presented.

Index Terms—authoring tool, literacy, media, storytelling, wayang

I. INTRODUCTION

THROUGHOUT the world puppet show is a popular form of entertainment. Sometimes it is an ancient heritage, a reminder of an age long past; sometimes a medium for contemporary artist’s experiments with shape, color and movement. For centuries it has been used to relate myth and legend and enact simple traditional farces. Now, as well as undergoing a tremendous revival as entertainment for both adults and children, it is becoming more and more widely used in education and also in therapy.

In our project Wayang Authoring we want to use the Web to revive traditional story telling with puppets. We aim at educational use of virtual storytelling to improve media literacy for young people all around the world through an interesting and challenging application and an intercultural exchange. We want to enable children to express themselves in creating own stories and to share them with others.

Virtual worlds cannot substitute the rich experience of performing with real puppets and a face-to-face-audience. But we want to ponder the potentials of Web design and usage for the field. New possibilities may arise from a worldwide availability and from intercultural exchange of local

Manuscript received January 30, 2009.

Wahju Agung Widjajanto is member of Digital Media in Education (dimeb) Research Group, Faculty of Mathematics/Informatics, University of Bremen, Germany (e-mail: wahju@tzi.de).

Michael Lund is member of Digital Media in Education (dimeb) Research Group, Faculty of Mathematics/Informatics, University of Bremen, Germany (e-mail: mlund@tzi.de).

Heidi Schelhowe is Professor and Head of Digital Media in Education (dimeb) Research Group, Faculty of Mathematics/Informatics, University of Bremen, Germany (e-mail: schelhow@tzi.de).

knowledge on storytelling. Web software can alleviate own construction and design activities. The popularity of client-side scripting allows extended functionality and new kind of interactivity in web applications. The Web offers new and amazing communication and cooperation possibilities all over the world, especially with the rise of social networking sites and the semantic web.

The idea of Wayang Authoring is based on the Indonesian ancient art form Wayang. We will explain more about it in the second chapter. Wayang as a traditional art form offers a space and power to be explored. The third and fourth chapter will tell about digital media and literacy. The field of storytelling and digital story telling will be explained in the fifth chapter. In our project that is portrayed in the seventh chapter we combine the tradition of Wayang storytelling with digital media in order to create a new type of performance possibilities without obstructing the role of the original art itself. Wayang Authoring is designed as a multimedia web-based application for children to create stories and a virtual community of storytellers. At least we will refer to Jenkins notion of media literacy in order to reflect on how these competences could be encountered by Wayang Authoring. We estimate the understanding of audio-visual codes become a major literacy factor in a media based society because it changes the way to read and write.

II. PUPPETS, SHADOW PUPPETS

Puppetry is understood differently depending on whether the explanation comes from the artist or the audience [22]. Upon the artist, the puppet is understood as a medium under his control that frees him of any responsibility, being free to act in unreal world as the consequences are only in that world [2].

Tilis defined the puppet as a theatrical figure perceived by an audience to be an object, that is, given design, movement and frequently speech, so that it fulfills the audience’s desire to imagine it as having life, by creating a double vision perception and imagination, the puppet pleurably challenges the audience’s understanding of the relationship between object and life [22].

Puppets are shadow, hands, dolls, figures and figurines. Wayang is the general word to many kinds of traditional theatre in Java, Bali, Lombok, and some other parts of Indonesia and Southeast Asia, both puppet theatre and actor’s

theatre. *Wayang Kulit*, the most widespread *Wayang*, is an ancient form of storytelling that originated from the Indonesian island of Java. Over the centuries its religious character has increasingly developed into a distinct art form; foreign influences introduced new stories, characters were added, and new refined styles were developed at the courts.

Wayang Kulit consists of two words, *Wayang* and *Kulit*. *Wayang* is a Javanese word meaning shadow or ghost, *kulit* means leather, and added together it translates as 'shadow from leather'. The *Wayang Kulit* is a two-dimensional puppet, made of buffalo or goat leather; like paper dolls, but with arms that swivel (see Figure 1). A *Wayang Kulit* puppet is a representation of mainly human characters and the physical world. Every part of the puppets' design has symbolic significance.



Fig. 1. Example of *Wayang* puppets.

Wayang Kulit employs a white translucent screen made of cloth with an electric lamp hung near the centre of the screen (see Figure 2). At the lower edge of the screen, there are two banana trunks placed horizontally, into which the sharp points of the central controlling stick of the puppets can be stuck. The puppets are moved or fixed on or near the illuminated screen so they cast shadows on the screen. The puppets, the puppeteer, and the musicians can be watched from one side of the screen, and the shadows cast by puppets from the other. The audience can usually watch from both sides [12].



Fig. 2. View of *Wayang* performance space.

Wayang has the functions of entertainment as well as moral guidance, and is a combination of five arts, namely *seni widya* (arts of philosophy and education), *seni drama* (performing and *karawitan* musical arts), *seni gatra* (leather cutting and painting arts), *seni ripta* (thematic and literally arts), and *seni cipta* (conceptual and creative arts).

UNESCO proclaimed the *Wayang* Puppet Theatre as a Masterpiece of Oral and Intangible Heritage of Humanity on

7th November 2003 [23].

Wayang belongs to the Asian and Middle Eastern tradition of shadow theatre with puppets. Traditionally Western shadow theatre uses human actors and Eastern tradition uses puppets, but today there is an intercultural exchange between both traditions. The difference between the two kinds of shadow theatre becomes smaller. The mappings of a 3 dimensional object to a 2 dimensional silhouette hides and articulates specific aspects at the same time [37]. Some approaches use shadow play for educational targets. For example according to Reggio pedagogic the shadow is the first immaterial phenomenon a child is faced. The playful confrontation with shadows enables the comprehension the world of abstraction and concepts. In this view shadow theater could enhance the development of intelligence [30].

III. DIGITAL MEDIA AND LITERACY

Media evolves from oral to digital (see Figure 3). The most important recent milestones in this communicative and technological development are: a) the appearance of electronic media (telephone, film, radio and television) paving the way for mass communication – dominant since the 1950s – and the later emergence of digital media, especially the Internet – since the 1980s [5].

The concept of literacy was traditionally linked to an alphabet or a language code, that is, through reading, writing and understanding and this has been linked with print media. However, today, the term literacy has been extended to cover the skills and competencies involved in using computers competently, also in finding, selecting, analyzing, evaluating and storing information through the internet, in its treatment and its use, independently of the codes or techniques involved [5].

But what is literacy? According to Wendy Earle literacy means more than reading and writing. It means how we respond and understand our world. There is a huge range of definitions of particular and diverse literacies, such as computer literacy, game literacy or emotional literacy (that means to be able to decode certain signs of social communication). The aim of all these competences is to become able to interpret and interact with a range of sources of information and cultural forms [31],[32].

Sandra Calvert and colleagues have looked at the capacity of digital media to support active learning, metacognition, and verbal memory. They report that digital experiences allow children to take active control of their own learning, adjusting the pace and the level of difficulty of the material [9].

According to Jenkins paper which he published with the Mc Arthur Foundation in 2005 more than one-half of all teens in the US have created media content, and roughly one third of teens that use the Internet have shared content they produced. He summarized that (and other) trends under the term "participatory culture" that should become the center of modern media education [10].

21st century literacy is the set of abilities and skills where

aural, visual and digital literacy overlap. These include the ability to understand the power of images and sounds, to recognize and use that power, to manipulate and transform digital media, to distribute them pervasively, and to easily adapt to new forms.

Media literacy means learning a new grammar with its own rules of construction, implies the ability to use media to evoke emotional responses, and has potentials for the way we learn [21]. *Wayang* Authoring can be such a context. It incorporates aspects of storytelling, literature, theater, cinema and digital media.

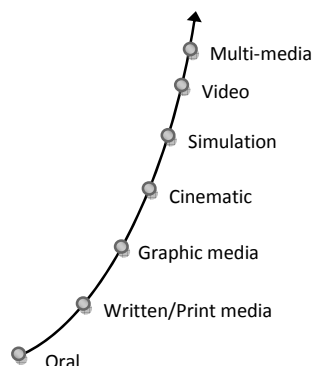


Fig. 3. Media evolution [21].

IV. VISUAL vs. TEXT

Digital media offer high production values, with exciting images, color, and movement that captivate kids' attention.

Researchers suggest that the visual element is especially important for young children, who often think in iconic, visual forms, as well as for poor readers who rely more on visualization of thoughts to scaffold memory skills [9].

Researchers have also associated digital media use with a tendency to focus on graphics first and texts second as children are used to pick up new information. The text illustrates the image – not the other way around [7].

The work of Allan Paivio indicated with his dual-coding theory that learners are far more likely to understand concrete (non-abstract) words when they are accompanied by referent pictures than when only pronounced [14].

The rich visual tradition of Javanese shadow theatre adapted a huge range of archetypical images. Often the visual appearance is an abstraction of a human characteristic, a specific emotion or behavior. This has an expressive and symbolic character, composed by reduction and a contrast of detailed ornamentation that makes them to an aesthetic object. The shadow enhances the evocative character [33],[34]. The figures become alive. The psychologist Fritz Heler created an animation movie, where abstract shapes like triangles and dots become actors. The audience gives those shapes intentions, wishes and personality. He suggests that the ability to create and understand stories is a human ability that helps us to get orientation in the social world and to understand others. Stories are fields for experiments, to try out relation and to develop empathy [35].

V. STORYTELLING

Storytelling is an ancient art form where experiences, events and actions are conveyed in words, images and sounds. This art form is traditionally an oral performance with an interactive relation between storyteller and audience. The storyteller uses often a set of incidents or fragments of plots that are mixed and composed in an improvisational manner [11].

In short words, in stories always a character acts upon a starting question or situation and reacts on events. The gap between his/her aim and the result of his/her acting, the gap between his/her vision and his/her personality creates the dramatic tension [11]. A character is a whole cosmos with diverse attributes and qualities.

Storytelling and the development of media influenced each another alternately, and each new medium established a new kind of storytelling. In theatre and film the storyline of the plot is redefined and becomes an extended aspect of this genre. According to the specific needs of literature or cinema the complexity of characters is defined. With digital media as a major medium nowadays several new kind of storytelling are created, such as text adventure, interactive fiction, role-plays and games with story elements. In an interactive story the user becomes the protagonist (the main and active character of a story) travelling through a universe of possibilities [4].

Digital storytelling is combining the art of telling stories with a mixture of digital graphics, text, recorded audio narration, video and music to present information on a specific topic [18].

Digital storytelling can enable ordinary people to tell their own lives. In the last eight years a new genre of storytelling was developed out of computer games, carrying the tradition of cinema narration into this new media. The environment, the characters and the action can be produced, individually or cooperative [24]. Here the concept of telling is more important as the idea of action.

A story can be created by an individual or by a group. The members of a group - distributed or in the same place - collaborate on the creation of a story, which may be done synchronously or asynchronously using different media [15]. This collaborative storytelling has the capacity to build social interaction and to facilitate communication among the members of a community.

Stories provide a sense of direction. Most often, they have a beginning, middle, and an end. Of course, the advent of hypertext has abolished assumptions about sequencing, but even when there are multiple pathways through a story; narratives ask to deal with notions of ordering that can help to organize thinking. Stories also bring focus to remixed or seemingly chaotic productions by grounding them in emotion. They can help find wholeness in a fragmented world [19].

A simple web-based medium with functionalities for sharing and composing stories might encourage children to engage in co-operative storytelling. This kind of media

concept fits to some main aspects of the ancient art form of *Wayang*. As an ancestor of cinema in *Wayang* the story is more important than acting and the interaction with the audience demands a social embedding of the interactivity. Sharing story fragments and composing stories, recording and viewing can be supported by the possibilities of a medium that are close to the *Wayang* culture.

VI. RELATED WORK

In the following we refer shortly to some examples of digital storytelling and platforms for sharing user-generated content.

TellStory is a web application system that supports the collaborative construction of stories. One of the most important issues of TellStory consists in the user's possibility to use a template in order to address the elaboration of the story through the typical characteristics of a narrative structure [15].

KidPad is a collaborative story authoring tool for children. KidPad provides drawing, typing and hyperlinking capabilities in a large two-dimensional zoomable screenspace. By these functionalities children can create stories by scenes and link them together in a virtual space. Collaborative storytelling helps children develop interpersonal and story-related skills [8]. KidPad supports collaborative storytelling with one computer only, but not in computer networks.

KidStory proposes to build systems that support collaborative learning which itself may underpin the development of storytelling and visualization skills along with the development of multiple forms of literacy [20].

Technology offers an opportunity to support and facilitate collaboration in many respects [1]. Today's technology can be used to support either one individual at one computer, or one individual collaborating with others at different computers using internet technology.

YouTube [27] and Flickr [28] are well known platforms for sharing content; videos and pictures respectively. In these systems users can share contents and find inspirational ideas by looking at other user's creations. However, these are not platforms that support the creation of content. Users need other tools to produce pictures or videos. And also none of them addresses children as a special target group.

Animation tools like Flash [29] are popular and very good tools to make designs, animations, and user interfaces across all browsers and platforms. But this tool is too complex for children to create an animation product.

Building *Wayang* Authoring we learned from existing approaches and decided to use digital media and the Web not only to support children to create stories either individually or collaboratively with others, but at the same time helping children to understand 'the grammar of stories' in general and in a specific culture by composing and arranging stories according to a story line. Children can produce a visual story and combine it with other stories, even from other children easily without using another tool. At the same time this is

supposed to support media education in a general sense.

VII. WAYANG AUTHORIZING

Wayang Authoring is designed as a web-based authoring tool for visualizing storytelling with *Wayang* via the Internet. As it is interactive, users who author the stories can specify the behavior of each object. *Wayang* Authoring is also a choice to create a community and a social network of *Wayang* storytellers to share and to exchange their stories.

A. Target Group

Our target groups are children in the age span from 6 to 11. According to [19],[3],[17],[13], typically children in this age span have a set of psychological, social/emotional, moral, and environmental concerns that is all their own, such as:

Cognitive

- Strengthen their capacity for remembering, imaging, logical reasoning, problem solving, and critical thinking.
- Become more reflective – that is, better able to access, reflect upon, and talk about their own thoughts and feelings, and to describe themselves in complex ways.
- Communicate easily, using language effectively in a wide variety of situation.
- Gain ability to write and understand text.

Social/Emotional

- Form stronger, more complex relationships, particularly with peers of the sex, and grow in their desire to be liked and accepted by friends.
- Gain the ability to play and learn in teams or groups.
- Begin to create social hierarchies and sense of 'groupness'.

We expect that *Wayang* Authoring tool support the ability mentioned above.

B. System Architecture

Authoring tools can be roughly categorized into five basic approaches for programming: script-based, card-based, icon-based, timeline-based and object-based [16]. *Wayang* Authoring treats the application as a collection of objects. Children choose some objects and define properties of these objects.

The architecture of *Wayang* Authoring is shown in Figure 5. The user interacts with the system using a web-based

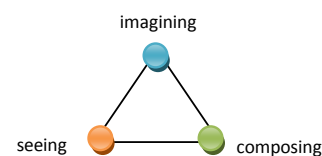


Fig. 4. Creative process

Graphical User Interface. The Story Manager maintains the story, composed by users.

Wayang Authoring is composed of three elements: the

imagination building element, the creative working element and the social interaction element (see Figure 6). Children can get an idea or an inspiration from the tutorial or from stories that are built, stored and shared by other users. This creative process is illustrated in Figure 4. They can also give comments and rank other children's stories. A child as a member of the *Wayang* Authoring community can compose a story, save it and share it. This process is supporting children to get friends and to connect with friends in the context of the

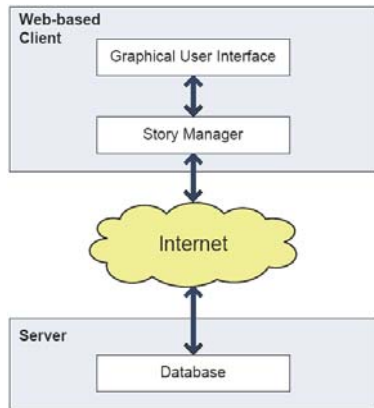


Fig. 5. *Wayang* Authoring's architecture.

social network. A story is composed by using an interactive, simple and easy-to-use tool.

C. The Prototype and Tool Features

The prototype is implemented by utilizing the most important recent feature of the Web that is the ability to run scripts on a client (generally through Javascript). Combined with the ability to access and to modify client-side Document Object Models (DOM) [26] of the browser, and the ability to add asynchronous background requests at the Web, these concepts together are commonly referred to as Asynchronous JavaScript and XML (AJAX) [6]. AJAX allows applications to provide rich client-side interfaces, and allows the browser to communicate with the Web without forcing page refreshes; both fundamental features of Rich Internet Applications (RIAs) [25].

In summary, the main features of *Wayang* Authoring are composing a story or a story list, playing a story or a story list, sharing a story, rating and commenting a story, and creating groups of story.

The tool focuses to create a story by moving the *wayang* figures. The web-based GUI of *Wayang* Authoring tool for composing a story allows for recording the movements of objects. The user can define the movement of an object using the dragging capability of that object. Direction and speed of the movement are automatically recorded, so that the user can record all movements very easily without defining a time line.

The user can also change the sequence of a story to get a different meaning out of the story. By this way, the children can learn about 'story grammar'.

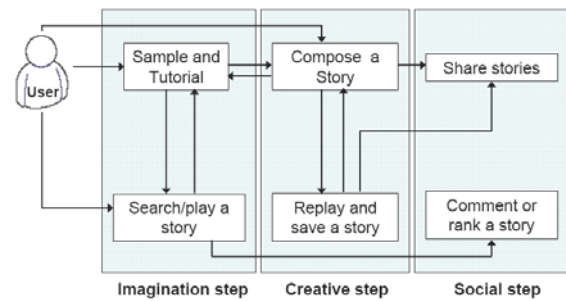


Fig. 6. Basic elements of *Wayang* Authoring.

User can create an individual and also a collaborative story. The tool "individual and collaborative stories" enables to combine different individual, maybe partial stories (that are in the "shared" modus) to one whole story. They also pay attention to other users by commenting or ranking a story.

Wayang Authoring serves all three kind of a participatory culture described by Jenkins:

- 1) Affiliation - through creating a user profile and joining a group centered on its favorite character.
- 2) Expression - through creating a new story with the authoring tool.
- 3) Collaboration - through rating and commenting other children's stories.

As the software is supposed to attract mainly the attention of younger children age 6-11, the social software tool shouldn't have too many functions. We have to avoid that it



Fig. 7. Screen shot of *Wayang* Authoring.

becomes confusing and takes away the attention from being a designer of creative content.

VIII. EVALUATION AND FUTURE WORK

We conducted a workshop with eight children with different cultural background at the International School Bremen. This workshop has been focused on usability and functionality of the prototype. We collected feedback from the participants regarding their opinion about the prototype.

Most of them had no difficulties to use the prototype without guidance. They enjoyed using this tool and could compose a story, playing and sharing it.

We will conduct other workshop to observe the participants, whether they really engage in composing a story

using this prototype, whether they use the online community feature, and pay attention to other users by commenting or ranking a story.

IX. SUMMARY

In summary, we propose a new approach to design story authoring that is intended to support media literacy for children. *Wayang* Authoring, a simple web-based medium, with functionalities for sharing and composing stories is supposed to encourage children to co-operative storytelling. This media concept fits to some main aspects of the ancient art form of *Wayang*. *Wayang* Authoring combines the world of computer games with this traditional art context. It could be an evocative medium alike the learning materials based on concepts of Maria Montessori. Like those materials it attracts attention, is reduced to certain aspects, and allows taking control and finding mistakes. It supports to focuses on quality. In brief it helps to develop language and thinking but it is also about crucial principles in culture and society [36].

REFERENCES

- [1] S. Benford, B. B. Bederson, K. P. Akesson, Bayon et al., "Designing Storytelling Technologies to Encourage Collaboration between Young Children", *Proceedings Human Factors in Computing Systems (CHI 2000)*, ACM Press, 2000, pp. 556-563.
- [2] E. H. Calvillo-Gómez, P. Cairns, *Pulling the Strings: A Theory of Puppetry for the Gaming Experience*, London, 2008.
- [3] Cognitive Skills Group, *Development Overview. Harvard Project Zero*, Presented on T-543 Web site at Harvard Graduate School of Education, 1997.
- [4] C. Crawford, *Chris Crawford on Interactive Storytelling*, New Riders Games, Berkeley, 2004.
- [5] European network on information literacy, *Study on the Current Trends and Approaches to Media Literacy in Europe*, 2007. (January 24, 2009). http://ec.europa.eu/avpolicy/media_literacy/docs/studies/study.pdf
- [6] J. J. Garrett, *Ajax: A New Approach to Web Applications*, Technical report, 2005. (12 June 2008). www.adaptivepath.com/ideas/essays/archives/000385.php
- [7] B. Gros, *The impact of digital games in education*, First Monday, 2004. (December 22, 2007), from www.firstmonday.org/issues/issue8_7/xyzgros/index.html.
- [8] J. P. Hourcade, B.B. Bederson, A. Druin, G. Taxen, "KidPad: Collaborative Storytelling for Children", *Proceedings Human Factors in Computing Systems (CHI 2002)*, ACM Press, 2002, pp. 500-501.
- [9] D. A. Huffaker, and S. L. Calvert, "The new science of learning: Active learning, metacognition, and transfer of knowledge in e-learning applications", *Journal of Educational Computing Research*, 2003, 29, pp. 325-34.
- [10] H. Jenkins, *Confronting the challenges of participatory culture: Media education for the 21st century*, MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital, 2005.
- [11] R. McKee, *Story: Substance, Structure, Style and the Principles of Screenwriting*, HarperCollinsPublisher, New York, 1998.
- [12] J. Mrazek, *Phenomenology of a Puppet Theatre: Contemplations on the Art of Javanese Wayang Kulit*, Kitlv Press, 2006.
- [13] National Center on Birth Defects and Developmental Disabilities, *Middle childhood (6 to 8 years old) and middle childhood (9-11 years old)*, 2005 (January 19, 2009). <http://www.cdc.gov/ncbddd/child/default.htm>.
- [14] A. Paivio, *Mental representations: A dual-coding approach*. New York: Oxford University Press, 1986.
- [15] R. Perret, M. R. S. Borgers, F. M. Santoro, "Applying Group Storytelling in Knowledge Management", *Springer (LNCS 3198)*, 2004, pp. 34-41.
- [16] M. D. Rabin, M. J. Burns, "Multimedia Authoring Tool. In Conference Companion on Human Factors in Computing Systems: Common Ground" (Vancouver, British Columbia, Canada, April 13 - 18, 1996). M. J. Tauber, Ed. *CHI '96*, ACM, New York, 1996, pp. 380-381.
- [17] V. Rideout, D.F. Roberts, U. G. Foehr, *Generation M: Media in the lives of 8-18-year-olds*, Menlo Park, CA: The Henry J. Kaiser Family Foundation, 2005.
- [18] B.R. Robin, *The Educational Uses of Digital Storytelling*, University of Houston, 2006. (10 April 2007). <http://fp.coe.uh.edu/brobin/SITE2006/site-paper-2006.htm>
- [19] R. Shore, *The Power of Pow! Wham!: Children, Digital Media & Our Nation's Future. Three Challenges for the Coming Decade*, New York: The Joan Ganz Cooney Center at Sesame Workshop, 2008.
- [20] Swedish Institute of Computer Science, *KidStory*, 2008. (7 May 2008). http://www.sics.se/kidstory/research/research_summary.html
- [21] The New Media Consortium, *A Global Imperative: The Report of the 21st Century Literacy Summit*, Stanford, California, 2005.
- [22] S. Tillis, *Towards an aesthetics of the puppet: puppetry as a theatrical art*, Greenwood Press, London, 1992.
- [23] UNESCO Jakarta Office, *Wayang Puppet Theatre*, 2005. (22 May 2008). www.unesco.or.id/activities/culture/programme/259.php
- [24] K. When, *Machinima - Was Ego-Shooter und Puppentheater gemeinsam haben*, Telepolis, 2004. (15 August 2008). <http://www.heise.de/tp/r4/artikel/17/17818/1.html>
- [25] J. Wright, and J. Dietrich, "Survey of existing languages to model interactive web applications", in *Proceedings of the Fifth on Asia-Pacific Conference on Conceptual Modelling - Volume 79* (Wollongong, NSW, Australia, January 01 - 01, 2008), 2008.
- [26] W3C Group, *Document Object Model (DOM) Level 3 Core Specification*, Technical report, W3C Recommendation 07 April 2004. (12 June 2008). <http://www.w3.org/TR/DOM-Level-3-Core/>
- [27] YouTube at <http://www.youtube.com>
- [28] Flickr at <http://www.flickr.com>
- [29] Flash at <http://www.macromedia.com/software/flash/about/>
- [30] G. Roderi, J. D. Zipes, *The Grammar of Fantasy: An Introduction to the Art of Inventing Stories*, Teachers and writers Collaborative, New York, 1996.
- [31] W. Earle, *Literacy or Literacies. Education Forum*, 4th April 2005. (20 January 2009) <http://www.instituteofideas.com/transcripts/edforumliteracy.pdf> ,
- [32] C. Bazalgette, *Literacy and the Media*, Skillsset, 2007. (24 January 2009) http://www.qca.org.uk/libraryAssets/media/11466_bazalgette_literacy_and_media.pdf
- [33] F. J. Röhl, *Pädagogik der Navigation*, Köpäd Verlag, München, 2003.
- [34] F. J. Röhl, *Mythen und Symbole der populären Medien*, GEP Verlag, Frankfurt am Main, 1998.
- [35] S. Pinker, *Toward a Consilient Study of Literature*, 2007. (25 January 2009). http://muse.jhu.edu/journals/philosophy_and_literature/v031/31.1pinker.html
- [36] M. Montessori, *Die Entdeckung des Kindes*, Freiburg im Breisgau, Herder, 2001.
- [37] G. Spitzing, *Schattenwelten Indonesiens*, Verlag Asu Poleng E. K., Hamburg, 2002.

Studi atas Prilaku Pengguna Layanan *Wide Area Network* (WAN) BPKP

Desi Nelvia dan Rudy M. Harahap

Email: desi.nelvia@bpkp.go.id dan rudy.m.harahap@bpkp.go.id

Abstrak— Keberhasilan implementasi teknologi informasi (TI) sangat bergantung kepada penerimaan teknologi oleh penggunaannya. Penelitian ini membahas tingkat penerimaan layanan jaringan komunikasi data dan suara yang dideteksi dari persepsi dan perilaku pengguna dalam menggunakan layanan tersebut. Penelitian ini bertujuan untuk mengetahui faktor-faktor yang mempengaruhi diterima atau tidaknya layanan jaringan komunikasi data dan suara oleh pengguna. Selain itu, penelitian ini juga mengungkapkan hubungan antara faktor-faktor yang mempengaruhi penerimaan terhadap layanan tersebut. Model yang digunakan untuk mengetahui penerimaan layanan ini adalah *Technology Acceptance Model* (TAM). Model TAM menjelaskan penerimaan TI dengan dimensi-dimensi tertentu yang dapat mempengaruhi penerimaan teknologi oleh pengguna. Model ini menempatkan faktor sikap dan tiap-tiap perilaku pengguna dengan menggunakan dua variabel utama, yaitu kemanfaatan (*usefulness*) dan kemudahan penggunaan (*easy of use*). Dari penelitian ini, ditemui bahwa penerimaan layanan jaringan komunikasi data dan suara juga dipengaruhi oleh faktor lain, antara lain *intention to use* (ITU) atau niat untuk menggunakan dan *actual usage behavior* (AUB) atau perilaku penggunaan.

Kata Kunci—Prilaku, TAM, dan WAN

I. PENDAHULUAN

Teknologi informasi dan komunikasi sudah menjadi kebutuhan organisasi. Berbagai bentuk aplikasi teknologi informasi dan komunikasi telah diimplementasikan, seperti aplikasi perkantoran (pengolah data, *spreadsheet*, grafis) dan layanan komunikasi (*email*, *chatting*, *teleconference*, dan *VOIP*). Begitu juga dengan BPKP, yang telah mengimplementasikan *wide area network* (WAN)—atau kadang diterjemahkan sebagai

jaringan komunikasi data dan suara (Jarkomdara)—guna menghubungkan kantor pusat BPKP dengan seluruh unit kerja BPKP yang tersebar di seluruh Indonesia. Implementasi WAN ini diharapkan akan menunjang kinerja seluruh pegawai BPKP dalam melaksanakan tugas mereka sebagai aparatur pengawasan. Dengan WAN, tidak hanya komunikasi data yang bisa dilakukan, tetapi juga komunikasi suara berbasis *internet protocol* (IP) atau biasa dikenal sebagai *voice over internet protocol* (VOIP). Untuk kepentingan komunikasi suara berbasis IP, BPKP telah mengimplementasikan produk yang umumnya keluaran Cisco atau biasa dikenal dengan IP-Phone. Di sisi lain, untuk kepentingan *electronic mail system*, BPKP telah mengimplementasikan produk Domino/Lotus Notes yang merupakan keluaran IBM.

Di lingkungan BPKP, ditengarai masih banyak pegawai yang menggunakan *email* non-kedinasan sebagai sarana berkirim *file* di lingkungan BPKP (seperti melalui *email* yahoo.com, telkom.net, hotmail.com, dan sebagainya). Padahal, *file-file* yang dikirimkan tersebut sebagian besar berisi data/informasi hasil pengawasan yang sifatnya sangat rahasia. Penggunaan *email* non-kedinasan tersebut juga tidak terjamin keamanannya jika dilihat dari sisi kepentingan nasional.

Penggunaan IP-Phone sebagai sarana komunikasi suara di lingkungan BPKP juga masih rendah. Masih sering ditemui penggunaan telepon PSTN sebagai sarana komunikasi antar unit BPKP. Padahal, dengan menggunakan IP-Phone, BPKP tidak lagi dikenakan biaya pulsa karena semua biaya sudah di-cover dalam biaya sewa koneksi Internet. Selain itu, di lingkungan kantor BPKP, IP-Phone sudah diintegrasikan dengan PABX yang telah terpasang sebelumnya di seluruh kantor BPKP. Dengan demikian, pegawai yang tidak memiliki IP-Phone pun tetap dapat menggunakan fasilitas WAN untuk berkomunikasi dengan biaya murah dengan rekan kerjanya di seluruh unit BPKP yang berada di hampir seluruh provinsi di Indonesia.

Berdasarkan latar belakang tersebut, dipandang perlu untuk melakukan penelitian ini, yaitu untuk mengetahui faktor apa saja yang mempengaruhi penerimaan pengguna di lingkungan BPKP terhadap implementasi WAN BPKP, khususnya pemanfaatan aplikasi Lotus Notes dan IP-Phone, yang diidentifikasi melalui persepsi dan perilaku pengguna. Pengukuran persepsi dan perilaku pengguna penting dilakukan sebagai tolak ukur keberhasilan implementasi WAN BPKP. Hasil penelitian ini diharapkan dapat dijadikan alat evaluasi dalam mengukur kinerja atas produk, layanan, dan penggunaan teknologi informasi di BPKP sehingga secara khusus dapat dijadikan sebagai acuan dalam

Desi Nelvia adalah alumni Program Studi Magister Ilmu Komputer Universitas Budi Luhur. Saat ini bekerja di Pusat Informasi Pengawasan, BPKP pada Sub Bidang Pengembangan Teknologi Informasi.

Rudy M. Harahap sebelumnya adalah Kepala Sub Bidang Pengembangan Teknologi Informasi, Pusat Informasi Pengawasan, Badan Pengawasan Keuangan dan Pembangunan (BPKP). Saat ini menjabat Kepala Bagian Penyusunan Rencana, Biro Perencanaan Pengawasan. Selain menduduki jabatan formal tersebut, penulis adalah pengajar pada Universitas Bina Nusantara dan anggota Dewan Pengawas Ikatan Audit Sistem Informasi Indonesia (IASII) dan salah satu anggota Kelompok Kerja Evaluasi Teknologi Informasi (Pokja Evatik) pada Dewan Teknologi Informasi Nasional (Detiknas). Penulis memperoleh ijazah Akuntan dari Sekolah Tinggi Akuntansi Negara (1996), Master Manajemen (Sistem Informasi) dari Universitas Bina Nusantara (1999), dan Master of Commerce (Information System) dari Curtin University of Technology (2000). Penulis dapat dihubungi melalui email rudy.m.harahap@bpkp.go.id. Pandangan dan informasi tentang penulis dapat diakses pada <http://rudymh.blogspot.com> dan <http://www.rudymh.8m.com>.

pengembangan teknologi informasi lebih lanjut di lingkungan BPKP dan secara umum di seluruh instansi pemerintah di Indonesia.

II. TINJAUAN PUSTAKA

Iqbaria [15] menyatakan bahwa secara individu maupun kolektif penerimaan teknologi dapat dijelaskan dari variasi penggunaan suatu sistem, karena diyakini bahwa penggunaan suatu sistem yang berbasis TI dapat meningkatkan kinerja individu atau kinerja organisasi. Untuk mengetahui indikator penerimaan TI, secara umum diketahui bahwa penerimaan TI dapat dilihat dengan adanya indikator penggunaan sistem dan frekuensi penggunaan komputer, atau dari aspek kepuasan pengguna dan ada juga yang menjadikan penggunaan sistem sebagai indikator utama penerimaan teknologi oleh penggunanya.

Menurut Syam [17], penggunaan teknologi informasi ditentukan oleh banyak faktor, salah satunya adalah karakteristik pengguna TI. Perbedaan karakteristik pengguna TI ditentukan oleh persepsi, sikap, dan perilaku dalam menerima penggunaan TI. Pengguna suatu sistem adalah manusia yang secara psikologis memiliki perilaku (*behaviour*) tertentu yang melekat pada dirinya, yang menyebabkan aspek perilaku dari pengguna TI menjadi faktor penting bagi setiap orang yang menggunakan TI.

Hasil penelitian yang dilakukan Guimares (tahun 1996), Lee (tahun 1986), Strassman (tahun 1985) dalam Nur [24], menemukan bahwa penerapan TI dalam suatu organisasi mendorong terjadinya revolusi terhadap perilaku bekerja individu dalam konteks penggunaan PC dan kemungkinan seseorang mempunyai keyakinan bahwa penggunaan komputer akan memberikan manfaat bagi dirinya dan pekerjaannya.

Dengan demikian, dapat dipahami bahwa aspek perilaku dalam penerapan TI merupakan salah satu aspek yang penting diperhatikan karena berhubungan langsung dengan pengguna. Sebab, interaksi antara pengguna dengan perangkat komputer yang digunakan sangat dipengaruhi oleh persepsi, sikap, dan afeksi sebagai aspek keprilaku yang melekat pada diri manusia sebagai *user*. Oleh karena itu, sistem yang dikembangkan haruslah berorientasi kepada penggunanya.

Beberapa model telah dibangun untuk menganalisis dan memahami faktor-faktor yang mempengaruhi diterimanya penggunaan teknologi. Model Penerimaan Teknologi (*Technology Acceptance Model* –TAM) pertama kali dikenalkan oleh Davis pada tahun 1989. Model ini sebenarnya diadopsi dari model *The Theory of Reasoned Action* (TRA), yaitu teori tindakan yang beralasan yang dikembangkan oleh Fishbe dan Ajzen [10], dengan suatu premis bahwa reaksi dan persepsi seseorang terhadap sesuatu hal akan menentukan sikap dan perilaku orang tersebut. Teori ini membuat model perilaku seseorang sebagai suatu fungsi dari tujuan perilaku.

Reaksi dan persepsi pengguna TI akan mempengaruhi sikapnya dalam penerimaan penggunaan TI. Salah satu faktor yang dapat mempengaruhi adalah persepsi pengguna atas kemanfaatan dan kemudahan penggunaan TI sebagai suatu tindakan yang beralasan dalam konteks penggunaan TI sehingga alasan seseorang dalam melihat manfaat dan

kemudahan penggunaan menjadikan dasar tindakan orang tersebut dapat menerima penggunaan TI. Model TAM yang dikembangkan dari teori psikologis menjelaskan perilaku pengguna komputer, yaitu berlandaskan pada kepercayaan (*belief*), sikap (*attitude*), intensitas (*intention*), dan hubungan perilaku pengguna (*user behaviour relationship*). Model ini menempatkan faktor sikap dan perilaku dari setiap pengguna dengan dua variabel, yaitu kemanfaatan (*usefulness*) dan kemudahan penggunaan (*ease of use*). Secara empiris, model ini telah terbukti memberikan gambaran pada aspek perilaku pengguna PC, di mana banyak pengguna PC dapat dengan mudah menerima TI karena sesuai dengan apa yang diinginkannya [Iqbaria, 16].

Fred D. Davis [9] menjelaskan bahwa model TAM menggambarkan hubungan antara komponen: (a) *Perceived ease of use* (PEOU), yaitu menunjukkan tingkat kepercayaan bahwa teknologi baru akan mudah untuk dipakai dan terbebas dari usaha yang menyulitkan; (b) *Perceived usefulness* (PU), yaitu menyatakan tingkat kepercayaan bahwa penggunaan teknologi baru akan meningkatkan capaian; (c) *Attitude toward using* (ATU), yaitu sikap pengguna ke arah menggunakan teknologi baru; (d) *Behavioral intention to use* (ITU), yaitu perilaku pengguna ke arah berlanjutnya penggunaan sebuah teknologi baru yang dianggap memberikan manfaat; dan (e) *Actual system usage* (ASU), yaitu pengguna benar-benar menggunakan teknologi baru secara nyata karena merasakan manfaatnya.

Penelitian dengan menggunakan TAM juga dilakukan oleh William Money [20] dalam penelitiannya tentang "*Application of the Technology Acceptance Model to a Knowledge Management System*" yang menggambarkan hubungan *perceived ease of use*, *perceived usefulness*, *behavioral intention to use*, serta *actual system usage*. Dari penelitiannya, dapat disimpulkan bahwa *perceived ease of use* dan *perceived usefulness* dapat langsung berhubungan dengan *actual system usage*.

Keberhasilan implementasi WAN BPKP jika ditinjau dengan menggunakan pendekatan TAM akan ditentukan oleh *perceived ease of use* (PEOU) atau kemudahan dan *perceived of usefulness* (PU) atau kemanfaatan. Jika kedua faktor tersebut memberikan nilai yang positif, maka dapat diperkirakan bahwa implementasi WAN BPKP diterima baik oleh penggunanya. Selanjutnya, ada faktor-faktor lain yang diperkirakan dalam penelitian ini juga berpengaruh pada implementasi WAN BPKP, yaitu *intention to use* (ITU) atau niat untuk menggunakan dan *actual use behaviour* (AUB) atau perilaku nyata pengguna.

III. METODOLOGI PENELITIAN

Penelitian ini merupakan penelitian eksplanatori mengenai hubungan sebab-akibat (kausal) dari variabel-variabel yang akan diteliti sehingga dari penelitian ini diharapkan dapat diketahui bagaimana dan apa saja faktor-faktor yang turut mendukung keberhasilan implementasi WAN BPKP.

Responden yang dijadikan sampel dalam penelitian ini adalah beberapa pegawai dan pejabat, baik struktural maupun fungsional, yang tersebar di beberapa unit-unit kerja di lingkungan Kantor Pusat BPKP, yang telah

menggunakan layanan WAN BPKP, khususnya Lotus Notes atau IP Phone.

Teknik sampling yang digunakan dalam penelitian ini adalah *purposive*, di mana sampel sengaja dipilih yang sesuai dengan yang diinginkan agar maksud penelitian bisa tercapai.

Metode penelitian ini adalah metode survey dan data yang digunakan adalah data kuantitatif. Tujuan dilakukannya survey adalah untuk mendapatkan gambaran dari para pengguna di lingkungan BPKP mengenai pendapat mereka tentang pernyataan yang diajukan dalam kuisioner. Penelitian dilakukan pada tahun 2007.

IV. HASIL PENELITIAN DAN PEMBAHASAN

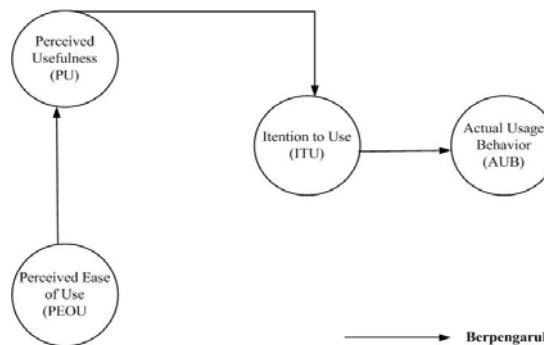
Berdasarkan uji hipotesis pada penelitian ini, diketahui bahwa penggunaan layanan jaringan komunikasi data dan suara di BPKP dipengaruhi oleh 4 variabel laten, yaitu *Perceived Ease of Use* (PEOU) atau kemudahan penggunaan, *Perceived Usefulness* (PU) atau kemanfaatan, *Intention to Use* (ITU) atau niat untuk menggunakan dan *Actual Usage Behavior* (AUB) atau perilaku penggunaan.

Dengan Model TAM, diketahui dari penelitian ini bahwa variabel PEOU (*perceived easy of use*) atau kemudahan berpengaruh terhadap variabel PU (*perceived usefulness*) atau kemanfaatan, variabel PU (*perceived usefulness*) atau kemanfaatan berpengaruh langsung terhadap variabel ITU (*intention to use*) atau keinginan untuk menggunakan dan variabel ITU (*intention to use*) atau keinginan untuk menggunakan berpengaruh terhadap variabel AUB (*actual usage behaviour*) atau perilaku nyata penggunaan. Dalam penelitian ini, variabel PEOU (*perceived easy of use*) atau kemudahan tidak berpengaruh terhadap variabel ITU (*intention to use*) atau keinginan untuk menggunakan.

Dapat dikatakan, penggunaan layanan jaringan komunikasi data dan suara di BPKP dipengaruhi oleh variabel kemanfaatan (PU), yang berdampak kepada variabel keinginan untuk menggunakan (ITU). Setelah pengguna merasakan kemanfaatan Lotus Notes atau IP-Phone, maka akan timbul keinginan untuk menggunakan, yang akhirnya berpengaruh pada perilaku nyata dalam menggunakan Lotus Notes atau IP-Phone. Kemanfaatan yang diperoleh dari Lotus Notes atau IP-Phone antara lain lebih cepat dan meningkatkan efisiensi biaya komunikasi. Adanya manfaat dari Lotus Notes atau IP-Phone menimbulkan keinginan untuk menggunakan.

Variabel perilaku nyata dalam menggunakan (AUB) Lotus Notes atau IP-Phone dipengaruhi oleh variabel keinginan untuk menggunakan (ITU). Perilaku penggunaan nyata dalam menggunakan Lotus Notes atau IP-Phone muncul karena adanya keinginan untuk menggunakan. Pada penelitian ini, perilaku yang positif dalam menggunakan Lotus Notes atau IP-Phone antara lain terlihat dari frekuensi dalam menggunakan dan menjadikan Lotus Notes atau IP-Phone sebagai pilihan utama dalam berkomunikasi antar unit di BPKP.

Berdasarkan modifikasi model dan hasil pengujian hipotesis, maka dapat dijelaskan bahwa model yang didapatkan pada penelitian tampak pada Gambar 1.



Gambar 1 Hasil Akhir Model Penelitian

Implikasi dari hasil penelitian ini adalah bahwa Lotus Notes atau IP-Phone sebagai fasilitas komunikasi data dan suara dapat diterima oleh para pejabat dan pegawai BPKP sebagai sistem yang memiliki nilai kemanfaatan. Namun, untuk mengoptimalkan penggunaan Lotus Notes atau IP-Phone diperlukan adanya dukungan dari pimpinan unit organisasi dan perubahan budaya kerja di masing-masing unit.

V. PENUTUP

Berdasarkan pengujian-pengujian yang dilakukan, maka dapat disimpulkan bahwa (a) Model akhir yang diperoleh pada penelitian ini sesuai dengan penelitian Money & Turner (2004). Di mana variabel yang mempengaruhi penggunaan layanan sebagai fasilitas komunikasi data dan suara pada penelitian ini meliputi PU (*perceived usefulness*), PEOU (*perceived easy of use*), dan ITU (*intention to use*); (b) Variabel PEOU (kemudahan dalam menggunakan layanan) berpengaruh terhadap variabel PU (kemanfaatan dengan menggunakan layanan); (c) Variabel PEOU (kemudahan dalam menggunakan layanan) tidak berpengaruh terhadap variabel ITU (keinginan untuk menggunakan layanan); dan (d) Variabel PU (kemanfaatan dengan menggunakan layanan) berpengaruh terhadap variabel ITU (keinginan untuk menggunakan layanan); dan (e) Variabel ITU (keinginan untuk menggunakan layanan) berpengaruh terhadap variabel AUB (perilaku nyata dalam menggunakan layanan).

Mengingat responden penelitian ini terbatas pada pegawai/pejabat BPKP yang berada di kantor pusat BPKP, simpulan atas penelitian ini dapat berbeda jika responden diperluas ke seluruh kantor BPKP. Simpulan ini juga dapat berbeda jika responden diperluas ke seluruh pegawai/pejabat instansi pemerintah. Karena itu, disarankan: (a) Adanya penelitian lebih lanjut dengan memperluas responden dengan menambahkan variabel-variabel lain selain yang telah ada dalam penelitian ini; (b) Pada penelitian selanjutnya sebaiknya tidak dimasukkan hipotesis bahwa PEOU berpengaruh terhadap ITU; dan (c) Layanan jaringan komunikasi data dan suara melalui IP-Phone dan Lotus Notes harus terus dipelihara dan dioptimalkan penggunaannya di lingkungan BPKP karena dapat meminimalisasi biaya komunikasi dan transfer data antar unit BPKP lebih cepat dan aman.

UCAPAN TERIMA KASIH

Ucapan terimakasih disampaikan kepada pihak-pihak yang telah membantu sehingga dapat diselesaikannya penelitian ini, terutama kepada Dr. Ir. Prabowo Pudjo Widodo, MS dan Dr. Moedjiono, M.Sc dari Universitas Budi Luhur, Tahria Syafrudin dan Daryanto dari Pusat Informasi Pengawasan, BPKP, serta Eni Heni Hermaliani, M. Ikkal, dan Sofyan Hadi.

DAFTAR PUSTAKA

- [1] Adam Denis, Nelson Ryan, dan Todd Peter, 1992, "*Perceived Usefulness, Ease of Use, and Usage of Information Technology : A Replication*", Management Information System Quarterly, Ghozali, Vol.2, Jakarta
- [2] Alavi, M. & Leidner, D.E., 1999, "*Knowledge Management Systems: Issue, Challenges, and Benefits*", Communications of the Association for the Information System, vol.1 no.7
- [3] Ajzen, I., 1991, "*The Theory of Planned Behaviour*", Organizational Behaviour and Human Decision Process 50 : 179-211
- [4] Bodnar H. G., dan Hopwood S, Accounting Information System, Salemba Empat, Jakarta, 1995.
- [5] Bourdon, I., Vitari, C., Moro, J., Ravarini, A., 2004, "*The Key Success Factor Affecting Knowledge Management System*", Liuc Papers n. 155, Serie Tecnologia, 8
- [6] www.bpkp.go.id, "*Sejarah BPKP*", diakses Juli, 2007
- [7] www.bpkp.go.id, "*Struktur Organisasi*", diakses Juli, 2007
- [8] Chin W., dan Todd Peter, 1991. "*On The Use Usefulness, Ease of Use of Structural Equation Modeling in MIS Research: A note of Caution*", Management Information System Quarterly,
- [9] Davis F. D. , 1989 "*Perceived Usefulness, Perceived ease of use of Information Technology*", Management Information System Quarterly
- [10] Fishbein, M and I. Ajzen., 1975, "*Belief, Attitude, Intention and Behaviour. An Introduction to Theory and Research*", Reading MA, Addison-Wesley
- [11] Ghozali, Imam A., 2005, "*Model Persamaan Struktural: Konsep dan Aplikasi dengan Program AMOS Ver. 5.0*", Badan Penerbit Universitas Diponegoro, Semarang
- [12] Hair, J. F., 1998, "*Multivariat Data Analysis*", Prentice Hall, New Jersey,
- [13] Haavelmo, T, 1944, "*The Probability Approach in Econometrica*", Econometrica.
- [14] Hartwick, J. and Barki., 1994, "*Explaining the Role of User Participation in Information System Use*", Management Science, vol. 40, no.4, pp.440-465
- [15] Iqbaria, M, 1994, "*An Examination of the Factors Contributing to Micro Computer Technology Acceptance*", Journal of Information System, Elsevier Ecience.
- [16] Iqbaria, Zinatelli, 1997 "*Personal Computing Acceptance Factors in Small Firm: A Structural Equation Modelling*", Management Information System Quarterly.
- [17] Joreskog, K. G, 1967, "*Some Contribution to Maximum Likelihood Factor Analysis*", Psychometrika
- [18] Joreskog, K. G, 1973, "*Non-Linear Structural Equation Models: The Kenny Judd Model eith Interaction Effects*", Advanced Structural Equation Modeling. Mhwh.NJ: Erlbaum.
- [19] Mathieson, K, 1992, "*Predicting User intention: Comparing the Technology Acceptance Model with the Theory of Planned Behavior*", Information System Research
- [20] Money, W., Turner, A., 2004, "*Application of the Technology Acceptance Model to a Knowledge Management System*", In Proceedings of the 37th Hawaii International Conference on Systems Sciences
- [21] Moore, G.C. & Benbasat, A., 1991, "*Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation*", Information System Research, vol.2, no.3, pp. 192-222
- [22] Malhotra, Y., Galetta, D.F., 1999, "*Extending the Technology Acceptance Model to Account for Social Influence*"
- [23] Neuman, W.L., 2000, "*Social Research Method*", 4th edition, Allyn & Bacon, United States of America
- [24] Nur Indriantoro, 2000, "*Pengaruh Computer Anxiety terhadap Keahlian Dosen dalam Penggunaan Komputer*", Jurnal Akuntansi dan Auditing (JAAI) Vol.3 No.1, FE UII, Yogyakarta.
- [25] Ruggles, R. 1998, "*The State of the Notion: Knowledge Management in Practices*", California Management Review, vol.40, no.3, pp.80-89
- [26] Sitinjak, Tumpal, J. R. ., dan Sugiarto, 2006, "*Lisrel*", Graha Ilmu, Yogyakarta
- [27] Szajna, B, 1996, "*Empirical Evaluation of the Revised Technology Acceptance Model*", Management Science
- [28] Syam Fazli, 1999, "*Dampak Kompleksitas Teknologi Informasi bagi Strategi dan Kelangsungan Usaha*", Jurnal Akuntansi dan Auditing (JAAI) Vol.3 No.1, FE UII, Yogyakarta
- [29] Taylor, S. & Todd, P.A., 1995, "*Understanding Information Technology Usage: a Test of Competing Models*", Information System Research, vol.6, no.2, pp. 145-177
- [30] Trisnawati, Rina., 1998. "*Pertimbangan Perilaku dan Faktor Penentu Keberhasilan Pengembangan Sistem Informasi*", Jurnal Kajian Bisnis, Yogyakarta,
- [31] Thomson, R., Higgin, C. A., dan Howell, J. M, 1991, "*Personal Computing: Toward a Conceptual Model of Utilization*", MIS Quarterly
- [32] Venkatesh, V., dan Davis F. D, 2000, "*A Theoretical Extention of the Technology Acceptance Model: for Longitudinal Field Studies*", Management Science
- [33] Widodo, Prabowo, P, 2006, "*Statistika : Analisis Multivariat. Seri Metode Kuantitatif*", Universitas Budi Luhur, Jakarta. 2006
- [34] <http://id.wikipedia.org/>, "*Wide Area Network*", diakses Juli, 2007.
- [35] Xu, J., Quaddus, M., 2000, "*Exploring the Factors Influencing the Adoption and Diffusion of Knowledge Management System in Organisations*"

Issues in Elliptic Curve Cryptography Implementation

Marisa W. Paryasto, Kuspriyanto, Sarwono Sutikno and Arif Sasongko
School of Electrical Engineering and Informatics
Institut Teknologi Bandung (ITB), Indonesia

Abstract—This work discusses issues in implementing Elliptic Curve Cryptography (ECC). It provides a brief explanation about ECC basic theory, implementation, and also provides guidance for further reading by referring each sub topics with more specific papers or books. The future and research topics in ECC will also be discussed.

Index Terms—cryptography, security

I. INTRODUCTION

THE rapid growth of computer applications for exchanging information electronically has resulted in the elimination of physical ways for providing security through locks, sealing and signing documents. This has thus resulted in the need for techniques for securing electronic document transactions. The techniques used are usually encryption and digital signatures.

The science of keeping messages secure is called cryptography. Cryptography involves encryption and decryption of messages. Encryption is the process of converting a plaintext into cipher text by using an algorithm, while decryption is the process of getting back the encryption message. A cryptographic algorithm is the mathematical function used for encryption and decryption.

Implementing cryptography involves extensive math and effective engineering and also good algorithm to integrate both. Deep math knowledge without efficient implementation techniques and effective implementation without solid foundation on math would not result in a product that can be delivered to solve problem [14].

Cryptographic systems can be broadly divided into two kinds: *symmetric-key cryptography* and *asymmetric-key cryptography* (public-key cryptography). The major advantage of symmetric-key cryptography is high efficiency, but it has a number of significant drawbacks, namely key distribution, key management, and the provision of non-repudiation.

Public-key cryptography provides an elegant solution to the problems inherent in symmetric-key cryptography.

Marisa W. Paryasto is a PhD candidate (S3) at the School of Electrical Engineering and Informatics at ITB in Bandung, Indonesia. She can be reached at marisa@stei.itb.ac.id. Kuspriyanto (kuspriyanto@yahoo.com), Sarwono Sutikno (ssarwono@gmail.com) and Arif Sasongko (asasongko@gmail.com) are faculty members within the School of Electrical Engineering and Informatics at ITB.

Unfortunately, public-key operations are usually significantly slower than symmetric key operations. Hence, hybrid systems that benefit from the efficiency of symmetric-key algorithms and the functionality of public-key algorithms are often used.

The notion of public-key cryptography was introduced in 1975 by Diffie, Hellman and Merkle [3] to address the aforementioned shortcomings of symmetric-key cryptography. In contrast to symmetric-key schemes, public-key schemes require only that the communication entities exchange keying material that is authentic (but not secret). Each entity selects a single key pair (e, d) consisting of a public-key e , and a related private-key d (that the entity keeps secret). The keys have the property that it is computationally infeasible to determine the private key solely from knowledge of the public key.

Elliptic curve cryptography (ECC) [7][11] is an emerging type of public key cryptography that presents advantages compared to other public key algorithms.

Currently ECC is the most efficient public key cryptosystem that uses shorter keys while providing the same security level as the RSA cryptosystem [16]. The use of shorter keys implies lower space requirements for key storage and faster arithmetic operations. These advantages are important when public-key cryptography is implemented in constrained devices, such as in mobile devices.

ECC is more complex than RSA. Instead of a single encryption algorithm (as in RSA), ECC can be implemented in different ways. ECC uses arithmetic algorithms as the core operations for high level security functions such as encryption (for confidentiality) or digital signatures (for authentication).

Cryptography implementation of this kind imposes several challenges, which may require a trade-off in performance, security and flexibility. ECC can be implemented in software or hardware. Software ECC implementations offers moderate speed and higher power consumption compared to custom hardware. Additionally, software implementations have very limited physical security, specially with respect to key storage.

If security algorithms are implemented in hardware, a gain in performance is obtained at cost of flexibility. Dedicated hardware implementations of cryptographic algorithms with low power consumption are expected to outperform the software implementations due to the fact that the instruction set of a processor does not directly implement specific cryptographic functions.

In addition, hardware implementations of cryptographic algorithms are more secure because they cannot be easily read

or modified by an outside attacker. ASIC (Application Specific Integrated Circuit) implementations show lower price per unit, reach high speeds and have low power dissipation. However, ASIC implementations lack flexibility with regards to the algorithms and parameters. This leads to higher development costs when switching algorithms or schemes.

ECC interoperability is better achieved by software implementations. Software has the flexibility of allowing the switching among different ECC schemes with several security levels. However, the downside is that the performance of software implementations is lower. An approach studied in recent years combines the advantages of software (flexibility) and hardware (performance) in a new paradigm of computation referred to as *reconfigurable computing* (RC)[12]. RC involves the use of reconfigurable devices for computing purposes. The concept can be used to implement several applications but the general design methodology is not applicable to all cases.

II. ELLIPTIC CURVE CRYPTOGRAPHY FOUNDATION

ECC has a very unique mathematical structure that enables the process of taking any two points on a specific curve, of adding the two points and getting as a result another point on the same curve. This special feature is advantageous for cryptography due to the inherent difficulty of determining which original two points were used to get the new point. The choice of various parameters in the equation will set the level difficulty exponentially as compared to the key length.

Breaking encryption with ECC must use very advanced mathematics. However, ECC itself only require small increase in the number of bits in its keys in order to achieve a higher security.

ECC consists of a few basic operations and rules that define how addition, subtraction, multiplication, and doubling are performed.

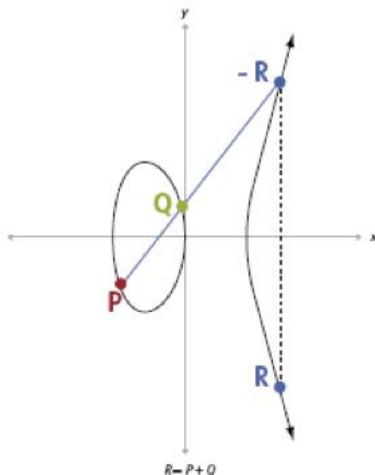


Figure 1 ECC Point Addition

Figure 1 illustrates one particular operation in ECC using real numbers. ECC point addition is defined as finding the line between two points, in this case P and Q. The result is a third point R. Point multiplication kP is accomplished by

performing multiple additions. An example is the repeated point addition and doubling for $9P = 2(2(2P)) + P$.

The public-key operation is $Q(x, y) = kP(x, y)$, with:

Q = public key

P = base point (curve parameter)

k = private key

n = order of P

Thus, the elliptic curve discrete logarithm is the following: given public key kP , find the private key k . The work of [6] gives a comprehensive explanation about elliptic curve mathematical foundation and its implementation.

III. ECC IMPLEMENTATION ISSUES

The most time consuming operation in ECC cryptographic schemes is the scalar multiplication. Efficient hardware/software implementations of the scalar multiplication kP have been the main research topic on ECC in recent years. This costly elliptic curve operation is performed according to the three layers shown in Figure 2 [12].

The scalar k can have different representation, and in the upper layer there are several algorithms to perform the multiplication. In the middle layer, there are several combinations for finite field representation and coordinates system. This layer covers curve operations, while the lower level is about finite field operations/arithmetic.

There are many algorithms can be applied for each layers, and the combination of algorithm used in each layer can significantly affect the performance of the scalar multiplication.

Figure 3 shows an example selection for the middle layer. An elliptic curve can be defined with different underlying fields.

An efficient implementation of an ECC over binary Galois fields in normal and polynomial bases has been proposed by Estes and Hines [4].

Other implementations and analysis over polynomial basis and ONB have also been done earlier by Choi *et al.* [2]. A non-conventional basis of finite fields for implementing a fast communication between two elliptic curve cryptosystems in software and hardware has been proposed by Sang Ho Oh *et al.* in [13]. This was done to address the problem of different choices of the basis. Sunar, Savas and Koc have constructed composite field representations for efficient conversion between binary and composite fields by deriving the change of the basis matrix [19].

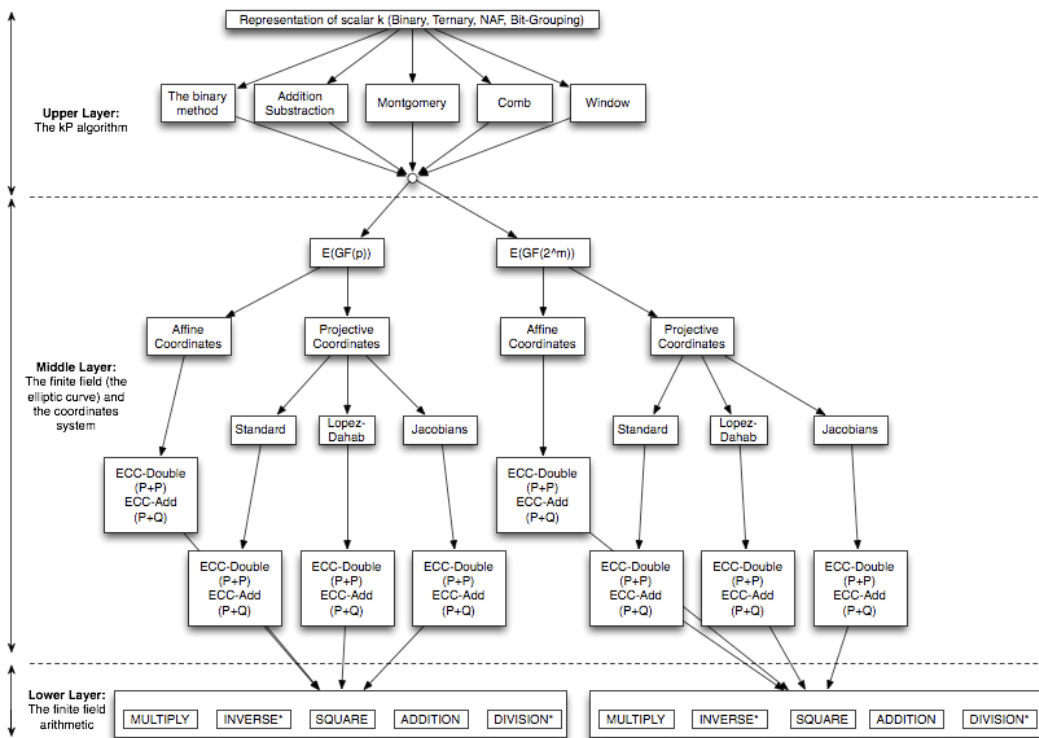


Figure 2 Various Methods of Scalar Multiplication kP

For the lower layer multiple works have been reported: efficient multiplication beyond optimal normal bases [15], Montgomery multiplication in $GF(2^m)$ [9], Mastrovito multiplier for all trinomials [8], hardware implementation of $GF(2^m)$ arithmetic using normal basis [20] and systematic design of original and modified Mastrovito multipliers for general irreducible polynomials [21].

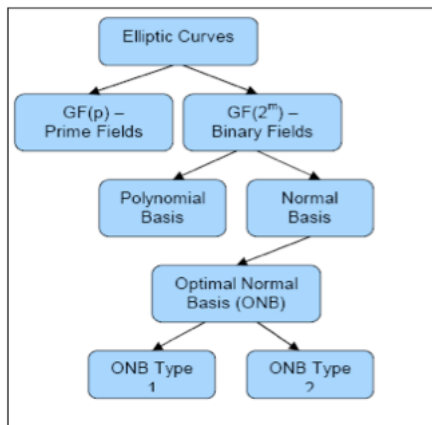


Figure 3 Taxonomy of Elliptic Curves

A. Software Implementations

ECC implementations in general purpose processor and embedded systems can meet some security requirements in some applications, but on the other hand hardware implementations are needed due to the application requirements such as throughput, power consumption, area constrains and physical security.

One of the comprehensive software implementations of ECC is [17]. Other ECC software implementation has been done by [18]. Software implementation in prime fields has been done by [1], while implementation in binary fields has also been done by [5].

B. Hardware Implementations

ECC hardware implementations are aimed to optimize each stage of scalar multiplication kP in Figure 2:

- (1) Field optimization is performed by choosing fields with fast multiplication and inversion;
- (2) Coordinates and scalar multiplication optimizations are performed by reducing the number of field inversions (projective coordinates), reducing the number of point additions (windowing) and by replacing point doubles (endomorphism methods).

Several works reported in the literature have used reconfigurable devices, FPGAs, to implement ECC algorithms. To compute the scalar multiplication kP as fast as possible is the main objective of these works. Hardware architectures for computing kP reported in the literature can be divided into processor or co-processor approaches. In the former, there exist a number of specialized instructions which the processor decodes and executes; most of them are for

elliptic curve and finite field arithmetic. In the latter, there are no such instructions because the algorithms are implemented directly on specialized hardware. In general, both kinds of implementations are based on a regular structure.

Many considerations must be taken into account when these blocks are implemented in hardware, especially for wireless applications where area/performance trade off is important. While a custom implementation can perform the operation kP faster, such custom work is difficult to change in order to support a different algorithm.

There is a diversity of technologies used to implement elliptic curve cryptography in hardware. So far a generic architecture suitable for mobile devices has not been reported. What has been reported are the differences regarding resources and timing achieved for different selections of the ECC parameters [12].

Recent works also show different approaches to implementing the three layers of kP computation. It has been reported that several multipliers have been used at different levels of parallelism. It is not clear how these choices will impact the resources of the coprocessor and the advantages gained by using one of the reported multipliers (namely Karatsuba, LFRS, Massey Omura, and D-serial). The same is also true for the inversion and square algorithms.

IV. FUTURE OF ECC AND RESEARCH TOPICS

The implementation of cryptographic systems presents several requirements and challenges, particularly for constrained environments (memory and area requirements). An important aspect is the power and energy consumption relating to public key algorithms. This is especially a challenge in pervasive devices running on their own energy storage and which are placed in the field for long periods of time without any maintenance or possible physical access. For example, devices like RF-ID makes replacing the batteries a highly cumbersome process. RF-ID tag applications derive the required power from the electromagnetic field of the reader to run its applications. Such systems also have to be extremely power efficient. Therefore, real world estimates of the power requirements for cryptographic processes are extremely important. This includes systems running public-key cryptography on processors with extensions. The underlying arithmetic algorithms could then be chosen and fine-tuned more efficiently for a low power ECC design.

Unlike traditional systems that cannot be physically accessed by an attacker, pervasive systems must also consider physical security as they are placed in insecure surroundings easily accessible for tampering. Therefore, storing the private key securely on such devices remains a big challenge, with the usual solutions remaining too expensive for such low-cost devices.

Even when physically secure, these devices can be passively attacked using side-channel (time and power) methods. Well know side-channel resistant algorithms normally require almost double the execution time, with larger memory and hardware resources. These measures are unsuitable for such low-end devices that require highly

optimized implementation (in time, memory and power) and therefore are an open problem that need further investigation [10].

V. CONCLUSION

ECC is a promising candidate for the next generation public key cryptosystem. Although ECC's security has not been completely evaluated, it is expected to come into widespread use in various fields in the future because of its compactness and high performance when it is hardware-implemented. In general we can conclude that the reliability, maturity and difficulty of a mathematical problem are very important factors.

ECC has been proven to involve much less overheads when compared to RSA. The ECC has been shown to have many advantages due to its ability to provide the same level of security as RSA yet using shorter keys. However, its disadvantage – which may lessen its attractiveness – is its lack of maturity, as mathematicians believe that not enough research has been done in the ECDLP.

REFERENCES

- [1] M. Brown, D. Hankerson, J. Lopez, and A. Menezes. Software Implementation of the NIST Elliptic Curves over Prime Fields.
- [2] Yong-Je Choi, Moo-Seop Kim, Hang-Rok Lee, and Ho-Won Kim. Implementation and analysis of elliptic curve cryptosystems over polynomial basis and onb. In Proceedings of World Academy of Science, Engineering and Technology, volume 10, December 2005.
- [3] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. IEEE International Symposium on Information Theory, June 1976.
- [4] Matthew Estes and Philip Hines. Efficient implementation of an elliptic curve cryptosystem over binary galois fields in normal and polynomial bases. Technical Report GMU EE-746 Fall 2006, George Mason University, 2006.
- [5] Darrel Hankerson, Julio Lopez Hernandez, and Alfred Menezes. Software Implementation of Elliptic Curve Cryptography Over Binary Fields.
- [6] Darrel Hankerson, Alfred Menezes, and Scott Vanstone. Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc., 2004.
- [7] Neal Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48(177): 203–209, January 1987.
- [8] C. K. Koc and Berk Sunar. Mastrovito multiplier for all trinomials. IEEE Transactions on Computers, 1999.
- [9] Cetin K. Koc and Tolga Aca. Montgomery Multiplication in GF(2k), volume 1, pages 57–69. Kluwer Academic Publishers, Boston, April 1998.
- [10] Sandeep S. Kumar. Elliptic Curve Cryptography for Constrained Devices. Verlag Dr. Muller, 2008.
- [11] Victor S. Miller. Use of elliptic curve cryptography. Technical report, Exploratory Computer Science, IBM Research, P.O. Box 218, Yorktown Heights, NY 10598.
- [12] Miguel Morales-Sandoval. An interoperable and reconfigurable hardware architecture for elliptic curve cryptography. PhD thesis, National Institute for Astrophysics, Optics and Electronics - Tonantzintla, Puebla - Mexico, September 2006.
- [13] Sang Ho Oh, Chang Han Kim, Joong Chul Yoon, Hee Jin Kim, and Jong In Lim. Non-conventional basis of finite fields - implementing a fact communication between two elliptic curve cryptosystems in software and hardware.
- [14] Marisa W. Paryasto, Kuspriyanto, Sarwono Sutikno, and Arif Sasongko. ECC implementation: towards math and engineering integration. To be published, March 2009
- [15] Arash Reyhani-Masoleh and M. Anwar Hasan. Efficient multiplication beyond optimal normal bases. IEEE, 52(4), April 2003.

- [16] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21 (120–126), 1978.
- [17] Michael Rosing. *Implementing Elliptic Curve Cryptography*. Manning Publications Co., 1999.
- [18] Zhijie Jerry Shi and Hai Yan. Software implementations of elliptic curve cryptography. *International Journal of Network Security*, 7(2): 157–166, September 2008.
- [19] Berk Sunar, Erkay Savas, and Cetin K. Koc. Constructing composite field representations for efficient conversion. *IEEE Transactions on Computers*, 52(11): 1391, November 2003.
- [20] Alaaeldin Amin Turki F. Al-Somani. Hardware implementation of $gf(2^m)$ arithmetic using normal basis. *Journal of Applied Sciences* 6, 6:1362–1372, 2006.
- [21] Tong Zhang and Keshab K. Parhi. Systematic design of original and modified mastrovito multipliers for general irreducible polynomials. *IEEE Transactions on Computers*, 50(7), July 2001.

Internetworking Indonesia Journal

The Indonesian Journal of ICT and Internet Development
ISSN: 1942-9703

About the Internetworking Indonesia Journal

The Internetworking Indonesia Journal (IJ) was borne out of the need to address the lack of an Indonesia-wide independent academic and professional journal covering the broad area of Information and Communication Technology (ICT) and Internet development in Indonesia.

The broad aims of the Internetworking Indonesia Journal (IJ) are thus as follows:

- **Provide an Indonesia-wide independent journal on ICT:** The IJ seeks to be an Indonesia-wide journal that is independent from any specific institution in Indonesia (such as universities and government bodies). Currently in Indonesia there are a number of university-issued journals that publish only papers from those respective universities. Often these university journals experience difficulty in maintaining sustainability due to the limited number of internally sourced papers. Additionally, most of these university-issued journals do not have an independent review and advisory board, and most do not have referees and reviewers from the international community.
- **Provide a publishing venue for graduate students:** The IJ seeks also to be a venue for publication for graduate students (i.e. Masters/S2 and PhD/S3 students) as well as working academics in the broad field of ICT. This includes graduate students from Indonesian universities and those studying abroad. The IJ provides an avenue for these students to publish their papers to a journal that is international in its reviewer scope and in its advisory board.
- **Improve the quality of research & publications on ICT in Indonesia:** One of the long term goals of the IJ is to promote research on ICT and Internet development in Indonesia, and over time to improve the quality of academic and technical publications from the Indonesian ICT community. Additionally, the IJ journal seeks also to be the main publication venue for various authors worldwide whose interest include Indonesia and its growing area of information and communication technology.
- **Provide access to academics and professionals overseas:** The Editorial Advisory Board (EAB) of the IJ is intentionally composed of international academics and professionals, as well as those from Indonesia. The aim here is to provide Indonesian authors with access to international academics and professionals within the context of a publication that is aware of the issues facing a developing nation. Similarly, the IJ seeks to provide readers worldwide with easy access to information regarding ICT and Internet development in Indonesia.
- **Promote the culture of writing and authorship:** The IJ seeks to promote the culture of writing and of excellent authorship in Indonesia within the broad area of ICT. It is for this reason that the IJ is bilingual in that it accepts and publishes papers in either English or Bahasa Indonesia. Furthermore, the availability of an Indonesia-wide journal with an international advisory board may provide an incentive and impetus for young academics, students and professionals in Indonesia to develop writing skills appropriate for a journal. This in-turn may encourage and train them to subsequently publish in other international journals.