ISSN 2313-1527 (PRINT)
ISSN 2313-1535 (ONLINE)

IJEIE

International Journal of Electronics
and Information Engineering

Vol. 5, No. 2 (Dec. 2016)

INTERNATIONAL JOURNAL OF ELECTRONICS & INFORMATION ENGINEERING

PUBLISHING OFFICE

Min-Shiang Hwang
Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan, R.O.C.
Email: mshwang@asia.edu.tw

International Journal of Electronics and Information Engineering is published both in traditional paper form (ISSN 2313-1527) and in Internet (ISSN 2313-1535) at http://ijeie.jalaxy.com.tw

PUBLISHER: Candy C. H. Lin

23-75, P.O. Box, Taichung, Taiwan 40199, R.O.C.

International Journal of Electronics and Information Engineering

Vol. 5, No. 2 (Dec. 1, 2016)

Congestion Control Schemes in ATM Networks for ABR Services: An Overview

Sanyam Agarwal[1], Tulika Kansal[2]
(Corresponding author: Sanyam Agarwal)

ACE College of Engineering & Management, Agra
7 Km. Stone, NH-2, Opp. Budia ka Taal, Agra - Kanpur Road, Etmadpur,
Agra, Uttar Pradesh 282002, India[1]
NTL Lemnis india, Pvt. Ltd.
Office No 17,18,19, 20, 1st Floor, Satyam Arcade, Near Hotel Novotel,
Viman Nagar, Pune-Nagar Road, Pune, Maharashtra 411014, India[2]
(E-mail: sanyamagarwal@hotmail.com)

(Received Oct. 10, 2016; revised and accepted Nov. 12 & 15, 2016)

Abstract

This article summarizes the advantage and disadvantages of various congestion control schemes for available bit rate (ABR) services in ATM networks. It will help network designers to realize the limitations of the various approaches in order to make informed decisions when considering ATM networks.

Keywords: ABR, ACR, ATM, BECN, CCR, CUP, EAMSA, EFCI, EPRCA, ER, FECN, GMA, MACR, PRCA, RM, RMA, VC, VP

1 Introduction

Broadband integrated services digital network (B-ISDN) efforts are driven by the emerging needs for high-speed communications and enabling technologies to support new integrated services. Among the available technologies, asynchronous transfer mode (ATM) has emerged as a standard for supporting B-ISDN.

ATM uses short, fixed-size cells consisting of 48 bytes of payload and 5 bytes of header to transmit information. The fixed size allows fast processing of cells and reduces delay variance and makes the network suitable for integrated traffic consisting of voice, video, and data. Providing the desired QOS for these various traffic types is much more complex than what is performed in data networks today.

Capability of ATM networks to provide large bandwidth and multiple quality service (QOS) guarantees will realized when equipped with effective traffic management mechanisms. Traffic management includes congestion control, cell admission control, and virtual path/virtual channel (VP/VC) routing. More challenging issues arise in the congestion control of ATM networks for available bit rate (ABR) traffic-data traffic-because it cannot be predicted in advance. The objective of ABR service is to use the unused capacity of the network.

A cell consists of 5 bytes of header information and 48-byte payload. ATM breaks all traffic into these 53-byte cells. The header contains control information such as identification, cell loss priority, routing, and switching information. The Protocol reference model has divided into three layers: The ATM adaptation layer (AAL), the ATM layer, and the physical layer. The physical layer defines a transport method for ATM cells between two ATM entities. The ATM layer mainly performs switching and multiplexing functions. The AAL defines a set of service classes to fit the needs of different user requests & converts incoming user requests for services into ATM cells for transport.

2 Congestion Control Schemes

2.1 Fast resource Management

A fast resource management method proposed by France Telecom. Before actually sending data cells, a source sends a resource management (RM) cell in order to request the desired bandwidth. When a switch receives a RM cell from the source it passes the RM cell on to the next switch if it can satisfy the request. A switch simply drops the RM cell if it cannot grant the request. The source then resends a request as it times out. Upon receiving an RM cell, the destination returns the RM cell back to the source, which can then transmit the data cell. The main problem in this method is excessive delay during normal operation or excessive loss during congestion.

2.2 Early packet Discard

The method uses a bit in the cell header to indicate end of message (EOM). A switch looks for the EOM marker and drops all future cells of the VC until the EOM marker finds again when its queues start getting full because it is better to drop all cells of one packet than randomly drop cells belonging to different packets. This method does not require any inter switch or source-switch communication. This method is not fair in the sense that the cell arriving at a full buffer may not belong to the VC causing the congestion.

2.3 Delay-based Rate Control

In this method, a source periodically sends an RM cell that contains a times tamp. When a destination receives an RM cell from the source, it returns it to the source. Upon receiving RM cell from destination, the source uses the timestamp in the RM cell to measure the round trip delay and to deduce the level of congestion. This approach has the advantage of no explicit feedback from the network.

2.4 Link Window with End-to-End Binary Rate

This method uses window flow control on every link and explicit forward congestion indication (EFCI)-based binary end-to-end rate control. The method is a merger of a rate-based scheme with a credit-based scheme. It is scalable in terms of number of VCs because the window control is per-link and not per-VC. It also guarantees zero cell loss as in credit-based scheme. However, neither the credit based nor the rate-based camp found it acceptable because it contained elements from both camps.

2.5 Fair Queuing with Rate and Buffer Feedback

This method requires that the switches compute a fair share of VCs and monitor each VC's queue length. A source periodically sends an RM cell to determine the bandwidth and buffer usage at its bottleneck. Upon receiving an RM cell from the source, a switch computes a fair share of VCs, which was computed as inverse of interval between the cell arrival and its transmission. Then, the switch assigns the minimum of the fair share and monitors each VC's queue length and assigns the maximum of queue length. Thus, each switch implements fair queuing, which consists a separate queue for each VC and computing the time at which the cell would finish transmission if the queue were to be served round-robin, one bit at a time. The cells scheduled to transmit in this computed time order. The main problem is that the method requires fair queuing in the switches, which is expensive with current hardware technology.

3 Credit Based Approach

As shown in Figure 1 [2, 3, 5, 8] before forwarding any data cell over the link, the sender needs to receive credits for the VC from the receiver. At various times, the receiver sends credits to the sender indicating availability of buffer space for receiving data cells of the VC. After having received credits, the sender is eligible to forward some number of data cells of the VC to the receiver according to the received credit information. Each time the sender forwards a data cell of the VC, it decrements its current credit balance for the VC by one.

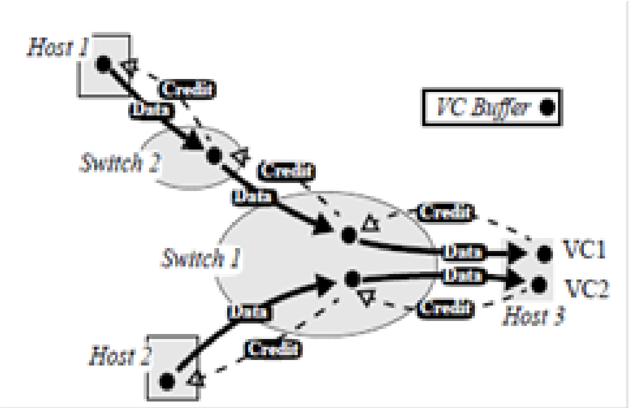

Figure 1: Credit-based flow control applied to each link of a VC

There are two phases in flow controlling a VC. In the first buffer allocation phase, the VC is given an allocation of buffer memory, Buf_Alloc, in the receiver. In the second credit control phase, the sender maintains a non-negative credit balance, Crd_Bal, to ensure no overflow of the allocated buffer in the receiver.

The credit update protocol (CUP) [2] is an efficient and robust protocol for implementing credit control over a link. As shown in Figure 2 for each flow-controlled VC the sender keeps a running total TX cont of all data cells it has transmitted, and the receiver keeps a running total Fwd_cnt of all the data cells it has forwarded. When the sender receives the credit record with value Fwd_cnt, it will update the credit balance, Crt_Bal, for the VC.

$$Crt\_Bal = Buf\_Alloc - (TX_cnt - Fwd\_cnt). \tag{1}$$

A credit based flow control is static or adaptive, if buffer-allocation is static or adaptive. In a static credit control a fixed value of Buf_Alloc will be used for the lifetime of a VC. Adaptive buffer allocation allows multiple VC's to share the same buffer pool in the receiver node adaptively. That is Buf_Alloc of a VC will automatically decrease, if the VC does not have sufficient data to forward, cannot get sufficient scheduling slots, or is back-pressured due to downstream congestion. The freed up buffer space will automatically be assigned to other VC's which have data to forward and are not congested downstream. Adaptive buffer allocation can be implemented at the sender or receiver node.

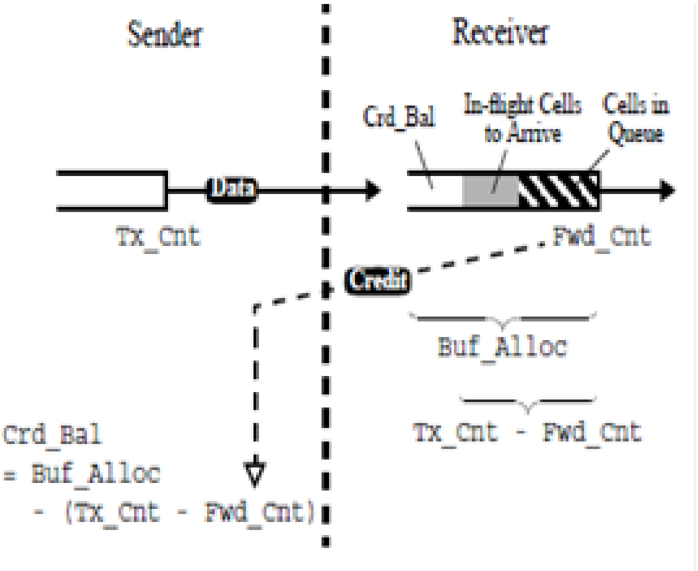

Figure 2: Credit update protocol (CUP)

4 Rate Based Control Schemes

Several proposals contributed in the rate-based congestion control framework to the ATM forum. This approach is a closed loop approach, in which case sources can change their rates based on the networks status. This scheme controls the congestion using the current network information. The control cells sent in the reverse direction, which has information about the rate at which the sources should emit the cells. Following types of rate-based schemes have suggested which described in detail at [4, 5, 7, 11].

4.1 Forward Explicit Congestion Notification (FECN)

This is an end-to-end scheme when a switch gets congested the switch marks Explicit Forward Congestion Indication bit "EFCI" bit in all the data cells passing through the switch on that path in the forward direction which indicates the congested switch status. When these cells reach the destination, the destination sends congestion notification cells in the reverse direction to notify the source regarding congestion. The source uses this cell information to adjust their rate appropriately.

A Queuing model [8] developed to analyze the congestion control based on FECN scheme, where reactive congestion control based upon two thresholds analyzed. Figure 3 shows the model. Under congestion, at the transit node, there are two thresholds with respect to the Queue length: High-level threshold H and low-level threshold L. The node transmits two kinds of control cells i.e., choking cell and relieving cell. When the Queue length at the node reaches the high-level threshold it recognizes congestion occurring at its own buffer, and transmits choking cells to all of the sources. The choking cells will arrive at the source after a constant backward propagation delay Db, which is also assumed to be the same for all sources. The round-trip propagation delay denoted by D slots, between each source and the node is then obtained as follows,

$$D = Df + Db + 1, \tag{2}$$

where 1 represents the transmission time of a control cell in node.

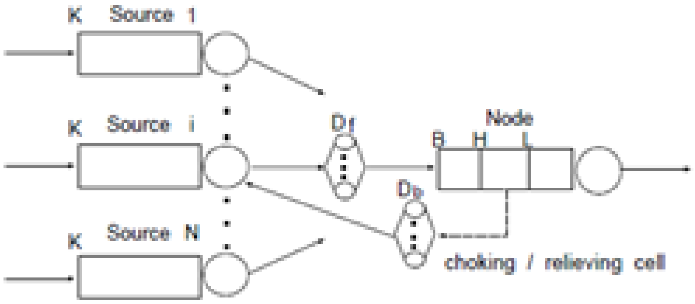

Figure 3: Analytical model

The above model was analytically approached. Through the analysis, the cell loss probability at the sources and the node have derived.

4.2 Backward Explicit Congestion Notification (BECN)

In this scheme, congestion notification cells generated by the switches, when they get congested. Thus congestion control cells are generated from the point where congestion occurs. The sources adjust their rate based on the control cell information. This scheme reacts to congestion immediately. Its response to congestion is much faster than the FECN scheme because it avoids the round-trip delay.

One of congestion control scheme using backward propagation of control cells and dropping off of ATM cells based on priorities in case of buffer overflow in the peak level control.

In peak level control [5] each output buffer has a peak buffer value set by the switch. If any of the output of buffers reaches its peak value (in terms of cells), the ATM switch will generate control cells for each source sending cells to this buffer. The control cells have a special field called Backward Explicit Congestion Notification (BECN) to specify congestion notification from the congested switch. These control cells called reverse mode(RM) cells, sent in the reverse direction ie., towards the source with BECN field set to 1. The sources receiving control cells will reduce their speed based on explicit cell rate of control cells. The Explicit call rate for any call, calculated by the switch as follows,

$$\begin{aligned} \text{Load factor} &= 1 - \text{bandwidth used by the source/total bandwidth of the link.} && (3)\\ \text{Explicit cell rate} &= \text{load factor} \times \text{current call rate.} && (4) \end{aligned}$$

Thus, the sources will reduce their current call rate proportionately to their actual load. When a source receives control cells, it will note down the current time and reduce the current cell rate as shown above. The recovery will resume to its original rate after a period called recovery period. The recovery period is also based on source's peak call rate.

$$\text{Recovery period} = \text{peak call rate} \times 100(\text{ms}). \tag{5}$$

The recovery period based on the peak call rate. The limitation of the proposed scheme is, in case of congestion, if any of the source is having very low call rate, the number of control cells generated are high. This is because the control cells are generated by the switch after certain fixed period. Also, if, the sources, once reduced, will ignore all the control cells coming from all the switches. If some other switch gets congested, it may happen that the sources may not respond to the control cells sent by it which may incur in the cell loss.

5 Selective BECN schemes

The BECN scheme used for comparison characterized by a threshold in the buffer filled by ABR sources. By exceeding this limit there is a risk of congestion because the sources are transmitting at a speed which will fill up the buffer causing a cell loss [13]. According to such a scheme, called No Filter (NF) scheme, see Figure 1, once beyond the threshold for every incoming cell one BECN cell is created, which will be sent to the source that transmitted the incoming cell.

This mechanism implemented by latching the VPI/VCI of the incoming cell, copying it into the BECN cell header and inserting that cell in the reverse direction stream. The BECN cell will go back to the source because the VPI/VCI identifiers are identical in both directions on a virtual connection. The source which receives a BECN cell must reduce its transmission rate for the virtual connection indicated.

When a transmitter receives a BECN cell it will reduce its cell transmission rate to half the current one. If other BECN cells received,it will be ignored until at least one cell transmitted in the forward direction. Consecutive BECN cells will cause decrease in the transmission rate to 50%, then to 25%, 12% and 6%. The another BECN cell will cause the source to stop its transmission: Therefore, six levels are possible on which the transmission rate will be positioned. Within each transmitter there is a transmission rate recovery mechanism. If recovery time is over, no BECN cells received, the transmission rate be doubled and restored to the previous level. This increment takes place at each recovery time, until peak rate is reached. Under the NF scheme it can be generated more BECN traffic than is needed since the sources treated in the same way. Actually, not all the sources will be slowed down in the same way, but only the most dangerous sources, that is a selective back pressure will be exercised. For penalizing sources that transmit more cells. The methods consider subdivision of the buffer as against the individual virtual connections. Using as a reference a transmission delay of 50 cell times, the filter schemes allow for a decrease in the BECN generated of 65% and, if they will optimized, they reach 75% as against the no filter one. Besides, an optimal recovery time of 256 cell times has been found. These schemes allow best effort traffic be kept under control using a limited BECN cell overhead.

5.1 BECN with Output Buffer Switches Proportional Rate Control Algorithm (PRCA)

The proportional rate control algorithm (PRCA) intended to remedy the problem of network congestion collapse with two major modifications: The positive polarity feedback approach and the counter-based approach (i.e., no interval timers). In PRCA, the feedback mechanism uses the EFCI state of the data cells. A source marks the EFCI bit in all data cells except for the first of every N RM cells and continually decreases its cell rate for every data cell transmitted.

The parameter N is predetermined and will affect the response time to congestion and backward link utilization. When a destination receives a data cell with EFCI= 0, it instantly sends an RM cell to the source.

The destination takes no action when the EFCI bit is set by an intermediate switch because of the congestion. A source only increases its cell rate for a VC when it receives an RM cell from the destination. Otherwise, it will continually reduce its cell rate because no source can increase its cell rate unless it has an RM cell from the destination. The increments & decrements in the cell rate of each VC are proportional to the current cell rate, thus eliminating the need for timers and timer value selection in previous rate-based proposal.

PRCA allows both FECN-like operation and BECN-like operation because a switch experiencing congestion can change the state of EFCI = 0 to EFCI = 1 or remove RM cells in the backward direction.

The RM cells in the backward direction. The problem of network congestion collapse associated with the FECN and BECN schemes solved in PRCA.

5.2 Extended Active Multicast Service Architecture (EAMSA)

This scheme is particularly useful and effective for congestion control of video and audio streams, which expected to be the main bulk of data in multimedia enabled networks such as ATM. The concept is based on an active network [1] concept in which network switches support the injection of user codes. EASMA [13] is functionally divided into two levels. Level one provides the basic services of multicast connection setup and management. Level 2 provides means to program the network. These include injection of customized programs into specific nodes of the network. EASMA uses a Multicast Broker Agency(MBA) to perform most of the operations as in Figure 3. The MBA consists of four agents:

1) The Resource Monitoring Agent(RMA) which collects link state and topology information of the network;

2) The Group Management Agent(GMA) which maintains the group membership status, manages the joining or leaving of members and negotiates agreements between the source and the members;

3) The Routing Agent(RM) computes a multicast tree that connects sources and receives, deciding where to inject a customization program, and generates contracts;

4) The connection Management Agent(CMA) which setups the actual multicast tree by sending contracts to the designated virtual switches via the links between MBA and the switches.

EAMSA allows dynamic leave initiated joining and leaving of members. The MBA is capable of supporting point-to-point, point-to-multipoint connections and multipoint-to-multipoint connections, as well as QOS negotiation. A new member joins an existing multicast session through a joint operation. MBA receives this request and processes it (See Figure 4).

GMA updates its group membership table. After which, processing involves computing a bi-directional route from the source to the joining host by RA. The path is merged with the existing multicast tree.

5.3 Explicit Rate Control Algorithm (ERCA)

An explicit rate control algorithm (ERCA) was proposed to address the problems of previous binary feedback schemes. In binary feedback schemes, a single-bit is used only to tell the source whether it should go up or down. It was designed in 1986 for connectionless networks in which the intermediate nodes had no knowledge of flows or their demands.

In connection-oriented ATM, however, the switches know exactly who is using the resources and flow paths. The binary feedback schemes were also designed for window-based controls and are too slow for rate-based controls in high-speed networks. In window-based control, a slight difference between the current window and optimal window will show up as a slight increase in queue length. In rate-based control, a slight difference in current rate and optimal rate will show up as continuously increasing queue length. The reaction times should be fast. ERCA can ensure the source gets to the optimal

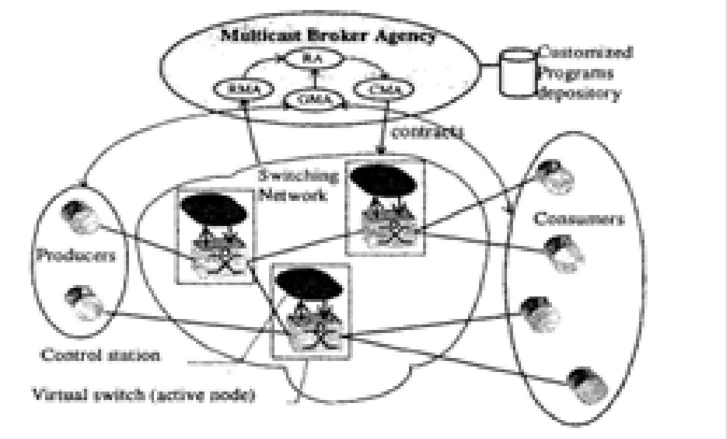

Figure 4: Active multicast service architecture

operating point within a few round trips. ERCA uses a positive feedback approach, and it is based on counter-based approach as in PRCA.In ERCA, each source periodically sends an RM cell containing its current cell rate (CCR),desired rate (DR), and a reduced (R) bit. When a switch receives an RM cell from the source, it monitors the VC's rate and computes a fair share using an iterative RM format procedure. The fair share is computed as follows.

If a VC's DR is more than the fair share, the switch will reduce the DR field and set a reduced bit in the RM cell. However, any VC can grant the DR if its DR is less than the fair share. Upon receiving an RM cell from the source, the destination returns the RM cell to the source. A source then adjusts its rate to that indicated in the RM cell. If the reduced bit is clear, the source could demand a higher desired rate in the next RM cell. If the bit is set, the source uses the current rate as the desired rate in the next RM cell.

The VC1's DR is more than the fair share at switch 2. In this scenario, ERCA has several advantages:

- Policing is straightforward because the entry switches can monitor the returning RM cells and use the rate directly in their policing algorithm.

- The system reaches the optimal operating point quickly because of fast convergence time the initial rate has less impact.

ERCA is robust against errors or loss of RM cells because the next correct RM cell will bring the system to the correct operating point. However, ERCA still employs per-VC accounting, which is very expensive with current hardware technology.

5.4 Enhanced Proportional Rate Control Algorithm (EPRCA)

An enhanced proportional rate control algorithm (EPRCA) is intended to solve the ACR beat down problem & to combine the previous separated rate-based schemes with two enhancements as intelligent marking & explicit rate setting. Fair share=Link Bandwidth - ?Bandwidth of Underloading VCs. If a VC's DR is more than the fair share, the switch will reduce the DR field and set a reduced bit in the RM cell. However, any VC can grant the DR if its DR is less than the fair share. Upon receiving an RM cell from the source, the destination returns the RM cell to the source. A source then adjusts its rate to that indicated in the RM cell. If the reduced bit is clear, the source could demand a higher desired rate in the next RM cell. If the bit is set, the source uses the current rate as the desired rate in the next RM cell.

The VC1's DR is more than the fair share at switch 2. In this scenario, ERCA has several advantages:

- Policing is straightforward because the entry switches can monitor the returning RM cells and use the rate directly in their policing algorithm.
- The system reaches the optimal operating point quickly because of fast convergence time-the initial rate has less impact.

ERCA is robust against errors or loss of RM cells because the next correct RM cell will bring the system to the correct operating point. However, ERCA still employs per-VC accounting, which is considered very expensive with current hardware technology.

5.5 The Intelligent Congestion Control Algorithm

The intelligent congestion control algorithm was proposed to resolve the ACR beat down problem. The key idea of this scheme is for each congested switch to estimate the optimal cell rate on each VC with a small number of computations and without the need of per-VC queuing or accounting.

This estimated rate is used to adjust the cell rates of the sources using positive feedback mechanisms. More specifically, each source periodically sends an RM cell containing its current allowed cell rate (ACR) and explicit rate (ER), which is the maximum allowed cell rate of the source.

For every data cell transmitted, a source continually decreases its ACR by additive decrease rate (ADR) until it receives an RM cell from the destination. A variable modified allowed cell rate (MACR) is defined in order to contain the value of the estimated optimal cell rate for each queue of a switch. When a noncongested switch receives an RM . When a congested switch receives an RM cell from the source, it replaces MACR by ACR - MACR, only if ACR is smaller than MACR. Using a first order filter, an intermediate switch that is congested or non-congested iteratively estimates the optimal cell rate for each VC given the ACR of each VC. When a destination receives an RM (ACR, ER) cell, it returns the RM cell to the source. When a congested switch receives an RM (ACR, ER),it takes one of two actions depending on congestion status. One possible action is the switch replacing ER in the RM cell by min (ER, * MACR) if the current queue length is greater than a certain threshold.

The other possibility is the switch replacing ER in the RM cell by min (ER, MACR) if ACR is greater than MACR. Upon receiving an RM (ACR, ER) cell from the destination, a source computes new ACR according to the rate information in the RM cell. The data and control traffic of the scheme in a congested network.

6 Conclusions

In this paper, an overview is presented on the parameters of quality of services in ATM network, together with the congestion control mechanism that support the QOS guarantee. Today,a number of concepts and mechanisms are specified such as rate based flow control and credit based flow control schemes for ABR traffic.

Significant differences separate credit and rate flow control. Credit provides precise control over buffer use, and can stop transmission automatically to avoid buffer overrun. Typical rate control methods provide no similar guarantee, partially to avoid some of the expense involved in implementing credit hardware. However, in the long run rate-based switches will probably need similarly complex hardware anyway, to enforce fairness and shape traffic at each switch.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] V. Bemme1 and M. Ilyas, "A unified congestion control strategy in ATM networks," in *IEEE International Conference on Serving Humanity Through Communications*, pp. 1600-1604, 1994.

[2] C. Blondia and O. Casals, "Traffic management in ATM networks: An overview," *Performance Evaluation and Applications of ATM Networks*, pp. 83–112, Springer US, 2002.

[3] J. Cox, M. Gaddis and J. Tumer, "Project zeus," *IEEE Network Magazine*, pp. 20–30, Mar. 1993.

[4] R. Jain, "Congestion control in computer networks: Issues and trends," *IEEE Network Magazine*, vol. 4, no. 3, pp. 24–30, May 1990.

[5] M. Kato, Y. Qie, M. Murata, H. Miyahara, "Performance analysis of reactive congestion control based upon queue length threshold values," *Performance Evaluation*, vol. 29, no. 2, pp. 105–125, 1997.

[6] A. Koyama, L. Barolli, S. Mirza, S. Yokoyama, "An adaptive rate based congestion control scheme for ATM Network," in *Proceedings of IEEE Twelfth International Conference on Information Networking (ICOIN'98)*, pp. 14–19, Jan. 1998.

[7] A. Kumar, A. Maniar, A. S. Elmaghraby, "A fair backward explicit congestion control scheme for ATM network," in *Proceedings of IEEE International Symposium on Computers and Communications*, 1999. **(DOI: 10.1109/ISCC.1999.780945)**

[8] H. T. Kung and R. Morris, "Credit-based flow control for ATM networks," *IEEE Network Magazine*, pp. 1–11, Mar. 1995.

[9] P. Newman, "Backward explicit congestion notification for ATM local area networks," in *IEEE Global Telecommunications Conference (GLOBECOM'93)*, 1993. **(DOI: 10.1109/GLOCOM.1993.318176)**

[10] M. Sreenivasulu, "Enhanced EFCI congestion control scheme for ATM networks," *International Journal of Computer Technology and Applications*, vol. 2, no. 5, Oct. 2011.

[11] G. Woodruff and R. KsitPaiboon, "Multimedia traffic management principles for guaranteed ATM network performance," *IEEE Journal on Selected Areas in Communications*, vol. 8, pp. 437–446, Apr. 1990.

[12] C. Woodworth, R. D. Gaglianello and R. D. Gitlin, "Congestion control in ATM networks," in *IEEE Global Telecommunications Conference (GLOBECOM'91)*, 1991. **(DOI: 10.1109/GLOCOM.1991.188543)**

[13] P. Yegani, M. Krunz and H. Hughes, "Congestion control schemes in prioritized ATM networks," in *IEEE International Conference on Serving Humanity Through Communications*, pp. 1169-1173, 1994.

Biography

Sanyam Agarwal is currently working as Professor in the Department of Electronics and Communication Engineering, at ACE College of Engineering and Management, Agra, India. His area of interest is ATM communication networks. He published many papers in National and International Journal and Conference.

Tulika Kansal is currently working as R & D engineer in Lighting divison of NTL Lemnis pvt. Ltd., Noida. She has completed her B.tech in Electronics and Communication engineering Branch From JPIET Noida in year 2014.

Analysis of One Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud

Zhengjun Cao[1], Chong Mao[1], Lihua Liu[2]
(Corresponding author: Lihua Liu)

Department of Mathematics, Shanghai University[1]
No.99, Shangda Road, Shanghai 200444, China
Department of Mathematics, Shanghai Maritime University[2]
No.1550, Haigang Ave, Pudong New District, Shanghai, China
(Email: liulh@shmtu.edu.cn)

(Received Sept. 6, 2016; revised and accepted Oct. 11 & 25, 2016)

Abstract

We show that the scheme [IEEE TPDS, 27(1), 2016, 40-50] is flawed because the group manager cannot complete his computational task in the registration phase. Actually, the designers of the scheme have misunderstood the concept of public key which is usually associated with an asymmetric encryption algorithm. Besides, the mechanism that the group manager has to re-encrypt all data stored in the cloud after a member is revoked, is somewhat infeasible because of its inefficiency.

Keywords: Accessibility, cloud computing, creditability, durability, data sharing, key distribution

1 Introduction

Cloud computing supports a paradigm shift from local to network-centric computing and network-centric content [8], and benefits scientific and engineering applications, such as data mining, computational financing, and many other computational and data-intensive activities. It enables customers with limited computational resources to outsource large-scale computational tasks to the cloud, including linear equations (LE) and linear programming (LP).

In 2010, Kamara and Lauter [4] discussed the security problem of cloud storage. Yu et al. [11] investigated the possibility of data access control in cloud computing. In 2013, Liu et al. [7] explored the problem of multiowner data sharing for dynamic groups in the cloud. Chen et al. [2, 12] investigated on achieving secure role-based access control on encrypted data in cloud storage. Nabeel et al. [9] designed a scheme with privacy preserving policy based content sharing in public clouds.

In 2016, Khaleel et al. [5, 10] discussed the possibility of using caching search engine for files retrieval system, and using cloud based technique for blog search optimization. Hsien et al. [3, 6] have presented two surveys on public auditing for secure data storage in cloud computing.

Very recently, Zhu and Jiang [13] have proposed a data sharing scheme for dynamic groups in the cloud. It claims that the proposed registration method is a secure way for key distribution without any secure communication channels, which enables the users can securely obtain their private keys from group manager.

In this note, we show that in the Zhu-Jiang scheme the group manager cannot complete his computational task in the registration phase. We stress that, from the practical point of view, the mechanism that the group manager has to re-encrypt all data after a member is revoked, is not generally acceptable because it is very inefficient.

2 Review of the Registration Method in Zhu-Jiang Scheme

In the scheme [13] there are three entities, the cloud, a group manager and a number of users.

The manager generates a bilinear mapping system $S = (q, G_1, G_2, e(\cdot,\cdot))$. He then picks $P, G \in G_1$, $\gamma \in Z_q^*$ and computes

$$W = \gamma \cdot P, Y = \gamma \cdot G, Z = e(G, P).$$

He publishes $(S, P, W, Y, Z, f, f_1, Enc())$, where f is a hash function: $\{0,1\}^* \to Z_q^*$, f_1 is a hash function: $\{0,1\}^* \to G_1$, and $Enc()$ is a symmetric encryption system. The manager keeps (γ, G) as the secret master key.

Let ID_i be the identity of a user, $\underline{pk \text{ be the public key of the user}}$ that needs to **be negotiated with** the manager, ac be the user's account for paying. The registration phase can be described as follows.

— The user picks $v_1 \in Z_q^*$ and sends (ID_i, pk, ac, v_1) to the manager.

— The manager picks $r \in Z_q^*$, computes

$$R = e(P,P)^r, U = (r + \gamma\, v_1\, f(pk\|ac\|ID_i)) \cdot P$$

and sends U, R to the user.

— The user checks

$$R \cdot e(v_1\, f(pk\|ac\|ID_i) \cdot P, W) \stackrel{?}{=} e(U, P).$$

If it holds, he picks $v_2 \in Z_q^*$ and sends

$$ID_i, v_2, AENC_{sk}(ID_i, v_1, ac)$$

to the manager, where $AENC()$ is an asymmetric encryption system and sk is the private key corresponding to the public key pk.

— The manager compares the received ID_i with the identity ID_i computed by **decrypting**

$$AENC_{sk}(ID_i, v_1, ac).$$

He also verifies if the decrypted number v_1 is equal to the random number v_1 in the first step. The other description in this step is omitted. We refer to the original for full details.

— The user decrypts $AENC_{pk}(KEY, v_2)$ to obtain his private key $KEY = (x_i, A_i, B_i)$.

In the registration phase, the interactions between the user and the manager can be depicted in the following Figure 1 (see Figure 3 in [13]).

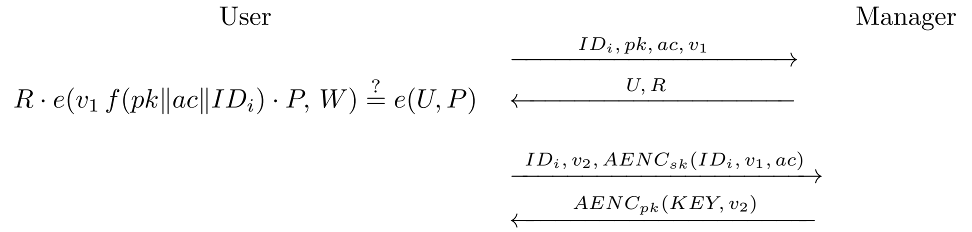
User
Manager
ID_i, pk, ac, v_1
U, R
$R \cdot e(v_1\, f(pk\|ac\|ID_i) \cdot P, W) \overset{?}{=} e(U, P)$
$ID_i, v_2, AENC_{sk}(ID_i, v_1, ac)$
$AENC_{pk}(KEY, v_2)$

Figure 1: Interactions between the user and the manager in the registration phase

3 The weaknesses of Zhu-Jiang Scheme

In this section, we show that Zhu-Jiang scheme [13] have three drawbacks, which make it impossible to be practically implemented.

1) *The manager cannot complete his computational task* in the registration phase because the manager **cannot decrypt** $AENC_{sk}(ID_i, v_1, ac)$, where sk is just the user's secret key. In order to ensure that the manager can decrypt a ciphertext, the user must use the manager's public key pk_M to encrypt data. That is to say, the user has to compute $AENC_{pk_M}(ID_i, v_1, ac)$ and send it to the manager. But we find the scheme does not assign the manager's public key pk_M at all.

2) The scheme stresses that the user's public key pk needs to be negotiated with the manager, and the user can securely obtain the private key from the group manager without any Certificate Authorities. The authors [13] have misunderstood the concept of public key which is associated with an asymmetric encryption algorithm. We here want to point out whether the negotiation is by online or offline interactions, the manager can assign the user's private key (x_i, A_i, B_i) as well as pk simultaneously. In such case, *the registration phase is totally unnecessary.*

   Notice that in order to bind the identity of an entity to its public key, it is usual to introduce a trusted third party (TTP). The TTP is generally assumed to be honest and fair but it does not have access to the secret or private keys of users. Before creating a public-key certificate for Alice, the TTP must take appropriate measures to verify the identity of Alice and that the public key to be certificated actually belongs to Alice.

   To this end, it is conventional that *Alice has to appear before the TTP with a passport as proof of identity*, and submit her public key along with evidence that she knows the corresponding private key.

   Explicitly, a user's public key satisfies [1]:

   - Creditability — it should be authenticated by a certification authority.
   - Accessibility — it should be easily accessible to any user.
   - Durability — it should be repeatedly usable in the life duration because the cost to generate and distribute a user's public key is somewhat expensive.

3) The scheme adopts the mechanism that *the group manager has to re-encrypt all data stored in the cloud after a member is revoked* (see page 44 in [13]). The mechanism, from the practical point of view, is really infeasible because of its inefficiency.

4 Conclusion

We show that Zhu-Jiang scheme is flawed. We would like to stress that the generation and authentication of a user's public key takes a lot of work. We specify that when Bob wants to encrypt a message and send it to Alice, Bob needs to invoke her public key, instead of his public key or secret key.

Acknowledgments

The authors would like to thank the National Natural Science Foundation of China (Project 61303200, 61411146001). The authors gratefully acknowledge the reviewers for their valuable suggestions.

References

[1] Z. Cao, "A note on gottesman-chuang quantum signature scheme," *eprint.iacr.org/2010/317*, 2010.

[2] T. Y. Chen, C. C. Lee, M. S. Hwang, and J. K. Jan, "Towards secure and efficient user authentication scheme using smart card for multi-server environments," *The Journal of Supercomputing*, vol. 66, no. 2, pp. 1008–1032, 2013.

[3] W.F. Hsien, C.C. Yang, and M.S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016.

[4] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Proceedings of 14th International Conference on Financial Cryptography Data Security (FC 2010)*, pp. 136–149, Canary Islands, Spain, January 2010.

[5] M. Khaleel, H. El-Bakry, and A. Saleh, "A new efficient files retrieval system using caching search engine," *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 22–31, 2016.

[6] C.W. Liu, W.F. Hsien, C.C. Yang, and M.S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing," *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.

[7] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 6, pp. 1182–1191, 2013.

[8] D. Marinescu, *Cloud Computing Theory and Practice.* USA: Elsevier, 2013.

[9] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 11, pp. 2602–2614, 2013.

[10] J. Singh, "Cloud based technique for blog search optimization," *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 32–39, 2016.

[11] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proceedings of 29th IEEE International Conference on Computer Communications,INFOCOM 2010*, pp. 534–542, San Diego, CA, USA, March 2010.

[12] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1947–1960, 2013.

[13] Z. Zhu and R. Jiang, "A secure anti-collusion data sharing scheme for dynamic groups in the cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 1, pp. 40–50, 2016.

Biography

Zhengjun Cao is an associate professor of Department of Mathematics at Shanghai University. He received his Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He served as a post-doctor in Computer Sciences Department, Université Libre de Bruxelles, from 2008 to 2010. His research interests include cryptography, discrete logarithms and quantum computation.

Chong Mao is currently pursuing his M.S. degree from Department of Mathematics, Shanghai university. His research interests include information security and cryptography.

Lihua Liu is an associate professor of Department of Mathematics at Shanghai Maritime University. She received her Ph.D. degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics, cryptography and information security.

Data-Aided Joint Timing-Channel Estimation and Interference Suppression in Multiuser UWB System

Wei-Chiang Wu
Department of Electrical Engineering, Da Yeh University
168, University Rd., Da-Tsuen, Changhua, Taiwan 515, R.O.C.
(E-mail: wcwm53@mail.dyu.edu.tw)

(Received July 2, 2016; revised and accepted Aug. 3 & Aug. 10, 2016)

Abstract

Ultra wideband (UWB) impulse radio (IR) system has currently being considered for several applications due to its attractive features that include low-power carrierless and ample multipath diversity. However, accurate timing offset (propagation delay) acquisition and channel estimation are critical for reliable operation. In this paper, we show the feasibility of using small training data set to jointly estimate timing and channel information in a multipath environment and in the presence of multi-user interference (MUI). Moreover, we exploit the training data set to design two types of constrained minimum output energy (C-MOE) mobile station (MS) receivers that effectively suppress MUI and extract the desired signal. Simulation results demonstrate that both the proposed timing-channel estimator and C-MOE based detectors are robust to MUI and near-far problems.

Keywords: Minimum Output Energy (MOE); Multi-user Interference (MUI); Near-far Problem; Time-hopping (TH); Ultra Wideband (UWB)

1 Introduction

Recently, a lot of attention was paid to ultra-wideband (UWB) radio systems since it is a promising technique for low-complexity low-power short range indoor wireless communications [1, 3, 12, 13, 14]. The basic structure of UWB radio stems from transmitting a stream of pulses of very short duration (on the order of nanosecond or less) and with very low duty cycle. When such transmissions are applied in multiple access system, time-hopping (TH) spreading codes are a plausible choice to separate different users [5, 7, 16]. Modulation of TH impulse radio is accomplished by assigning user-specific pattern of time shifting of pulses. However, the above benefits vanish without accurate timing (propagation delay) acquisition. Moreover, multipath fading induced signature waveform distortion severely degrades system performance.

Several data-aided timing acquisition schemes have been proposed [9, 17] for UWB transmission through dense multipath channels. However, [9] relies on a judiciously designed training pattern and [17] only considers single-user AWGN environment. Non-data aided (blind) timing-acquisition schemes have also been developed [4, 10, 18]. Based on the maximum likelihood criterion, channel parameters' estimation for UWB operating in multipath environments has been investigated in [4]. The method proposed in [4] is computationally prohibitive since it requires multi-dimensional search to maximize the log-likelihood function. The work of [10] exploits the second-order cyclostationarity in the UWB signal to perform timing acquisition and tracking. The work of [18] proposes simple integrate-and-dump operations over adjacent symbol-long segments of the received waveform. However, channel estimation is not considered in both algorithms. In [11], first-order cyclostationarity in the UWB pulse-position-modulation (PPM) signal is exploited to perform channel estimation and synchronization. The algorithm proposed in [11] is blind and the complexity is extremely low. However, [11] assumes the multiuser interference (MUI) to be zero-mean, thus cancelled out after averaging over the received signal. Whereas, zero-mean assumption is obviously not satisfied for the considered PPM signal. In the work of [8], both the first and second order statistics of the received signal are employed to blindly estimate multiuser channel impulse responses. The timing estimation (synchronization) problem is not considered in [8].

The first aim of this paper is to develop a data-aided, low-complexity, joint timing and channel estimation algorithm in TH UWB IR system employing binary (antipodal) pulse amplitude modulation (PAM). The rationale of the estimation algorithm is based on the first-order statistic (sample mean) of the training data set, then making use of the characteristics of discrete Fourier transform (DFT). More specifically, our proposed algorithm is computationally feasible such that only relatively small training data set is required. Simulation examples are carried out to evaluate its performance (in terms of root-mean-squared error (RMSE)) under different scenario.

Upon the timing estimation is completed, we can synchronize the observation window at the bit epoch. Employing the same training data set that has been aligned bit-by-bit, we can further estimate the desired user's effective signature vector and the correlation matrix of the observation data. In what follows, two types of constrained minimum output energy (C-MOE) [2, 15] mobile station (MS) receivers are developed for desired signal extraction and interfering signals suppression. The first scheme operates directly on the chip-rate sample data to derive the C-MOE based weight vector. While the second scheme first exploits the desired user's TH sequence to despread the received signal in each resolvable path, thereby, combines the outputs by the C-MOE based weights. From the computational complexity point of view, Scheme 2 is much simpler since the size of data and/or weight vector is extensively reduced. Both schemes exploit relatively small training data set and the performance is comparable to the optimum MOE receiver.

The remainder of this paper is organized as follows. In Section 2, we formulate the transmitting and receiving signal models of the time-hopping UWB multiple access communication system using binary antipodal PAM modulation. The first part of Section 3 describes the rationale of the proposed joint timing-channel estimator. There then, highlights the design of two types of MOE-based receiver. Simulation results are presented in Section 4. Concluding remarks are finally made in Section 5.

Notations 1. *Following common practice, vectors and matrices are represented by boldface, $[\cdot]^T$, $[\cdot]^H$ stand for matrix or vector transpose and complex transpose, respectively. We will use $E\{\}$ for expectation (ensemble average), and $\equiv$ for "is defined as". $\odot$ denotes Hadamard product (element-wise multiplication), $\star$ and $\otimes$ denotes linear and circular convolution, respectively. I_M denotes an identity matrix with size M, diag$\{\}$ denotes a diagonal matrix. hatx indicates the estimate of parameter x.*

2 Signal Model

In UWB-IR system, every information symbol (bit) is conveyed by N_f data modulated ultra short pulses over N_f frames. There is only one pulse in each frame and the frame duration is T_f. The pulse waveform is referred to as a monocycle [13], which typically is a doubly differentiated Gaussian pulse [7], with ultra-short duration at the nano-second scale. We assume the monocycle pulse waveform, $p(t)$, is normalized within a chip, T_c. Note that T_f is usually a hundred to a thousand times of T_c, which accounts for very low duty cycle. When multiple users are simultaneously transmitted and received, signal separation can be accomplished with user-specific pseudo-random sequences.

In downlink side, all users are synchronously transmitted, we may establish the data model of the transmitted signal as

$$x(t) = \sum_{k=1}^{K} \sum_{i} d_k(i) \sum_{j=0}^{N_f-1} a_k p(t - iN_fT_f - jT_f - c_j^k T_c) \tag{1}$$

where t is the clock time of the transmitter. K is the number of active users. a_k is the amplitude of the k^{th} user. The i^{th} bit transmitted by k^{th} user is given by $d_k(i)$, which takes on ± 1 with equal probability. Denoting T_b as the duration of the N_f repeated bits, then $T_b = N_fT_f$. Suppose each frame is composed of N_c time slots each with duration T_c, thus, $T_f = N_cT_c$. User separation is accomplished by user-specific pseudo-random TH code. $\{c_j^k\}_{j=0,1,\cdots,N_f-1}$ accounts for the k^{th} user's TH code with period N_f. Thereby $c_j^kT_c$ is the time-shift of the pulse position imposed by the TH sequence employed for multiple access. $c_j^kT_c \leq T_f$, or equivalently, $0 \leq c_j^k \leq N_c - 1$. To simplify the notation, we define the kth user's pulse train waveform as $p_k(t) \equiv \sum_{j=0}^{N_f-1} p(t - jT_f - c_j^kT_c)$. Thus, we may rewrite Equation (1) as a more compact form

$$x(t) = \sum_{k=1}^{K} \sum_{i} a_k d_k(i) p_k(t - iT_b) \tag{2}$$

In downlink channel, signals are subject to the same fading. In this paper, the multipath channel is modelled as a tapped-delay line with (L+1) taps, thus the time-invariant channel impulse response with (L+1) resolvable paths can be modelled as

$$h(t) = \sum_{l=0}^{L} \alpha_l \delta(t - lT_c) \tag{3}$$

where the tapped-delay line model as depicted in Equation (3) implies (L+1) resolvable paths. α_l denotes the attenuation coefficient along the l^{th} resolvable path. In writing Equation (3), we have assumed the channel parameters are essentially constant over observation interval. The average channel energy is normalized to one, $\sum_{l=0}^{L} |\alpha_l|^2 = 1$. Evidently, by selecting $c_{N_f-1}^k = 0$; $\forall k$ and $T_f > LT_c$ (or equivalently, $N_c > L$), we can guarantee no inter symbol interference (ISI).

Without loss of generality, we assume that the propagation delays between the desired user and the base station is within T_b, $0 \leq \tau < T_b$. Hence, the received composite waveform, which is made up of a weighted sum of attenuated and delayed replicas of the transmitted signal, can be formulated as

$$\begin{aligned} r(t) &= x(t) \star h(t) + v(t) \\ &= \sum_{k=2}^{K} a_k \sum_{i} d_k(i) \sum_{i=0}^{L} \alpha_l p_k(t - iT_b - lT_c - \tau) + n(t) \end{aligned} \tag{4}$$

where $n(t)$ is assumed to be zero-mean AWGN noise process with variance σ.

At the receiver front end, the received signal is first passed through a chip-matched filter (CMF) that matched to the monopulse, $p(t)$. If the time delay τ has been perfectly estimated, thus, offset (synchronized) at the front end of the receiver. Then, the N_fN_c-vector containing samples at the output of a CMF during the ith transmitted symbol can be formulated as

$$\begin{aligned} r(i) &= \sum_{k=1}^{K} a_k d_k(i) \widetilde{c} + n(i) \\ &= \widetilde{C} A d(i) + n(i) \end{aligned} \tag{5}$$

where $\widetilde{C} \equiv [\widetilde{c_1}\widetilde{c_2} \cdots \widetilde{c_K}]$ is a $N_f N_c$-by-K matrix, A is a diagonal matrix, $A \equiv diag\{a_1 a_2 \cdots a_K\}$, $d(i) \equiv [d_1(i) d_2(i) \cdots d_K(i)]^T$. $n(i)$ is the vector of noise samples, which is white with covariance matrix $\sigma^2 I_{N_f N_c}$. Please note that the $N_f N_c$-vectors, $\{\widetilde{c_k}\}_{k=1}^{K}$, represent the effective signature vectors for each user. We can obtain from Equation (5) that it arises from the CMF output's samples within a bit of the composite waveform, $\int_{t=nT_c}^{(n+1)T_c} p(t) \sum_{l=0}^{L} \alpha_l p_k(t - lT_c) dt$; $n = 0, 1, \cdots, N_c N_f - 1$, Denoting $q_{k,l}$ as the samples at the output of CMF of the received waveform coming from the lth path, $\int_{t=nT_c}^{(n+1)T_c} p(t) p_k(t - lT_c) dt$; $n = 0, 1, \cdots, N_c N_f - 1$, thereby it is evident that $\widetilde{c_k}$ can be expressed as

$$\begin{aligned} \widetilde{c_k} &= \sum_{l=0}^{L} \alpha_l q_{k,l} \\ &= C_k \alpha; \quad k = 1, 2, \cdots, K \end{aligned} \tag{6}$$

where $C_k \equiv [q_{k,0} q_{k,1} \cdots q_{k,L}]$, $\alpha \equiv [\alpha_0 \alpha_1 \cdots \alpha_L]^T$.

Without loss of generality, we assume user 1 is the desired user hereafter. In order to facilitate the design of data-aided joint timing and channel estimator, we firstly apply the training sequences, $d_1(i) = 1$; $i = 0, 1, \cdots, M - 1$. Hence, during the training period, we may express $r(t)$ as

$$r(t) = \sum_{i=0}^{M-1} [a_i \widetilde{p_i}(t - iT_b - \tau) + \sum_{k=2}^{K} a_k d_k(i) \widetilde{p_k}(t - iT_b - \tau)] + n(t) \tag{7}$$

where $\widetilde{p_k}(t)$ is the composite waveform of $p_k(t)$ and the multipath channel

$$\widetilde{p_k}(t) \equiv p_k(t) \star h(t) = \sum_{l=0}^{L} \alpha_l p_k(t - lT_c). \tag{8}$$

The problem addressed in this paper is the design of joint timing-channel estimator, based solely on the first-order statistics of the observation process $r(t)$.

3 Proposed Data-aided Linear Detector

3.1 Stage 1: Joint Timing-channel Estimator

To simplify the analysis, we assume τ is integer-multiples of T_c, that is $\tau = \epsilon T_c$; $\epsilon \in [0, 1, \cdots, N_f N_c - 1]$, though generalization to non-integer ϵ is without conceptual difficulty. Without the information of τ, the chip-rate samples during one bit interval in general conveys two adjacent bits. We denote the previous bit and current bit by $d_k(i-1)$ and $d_k(i)$, respectively. Let $\check{c_k}$ be a circular-shifted version of the effective signature vector, $\widetilde{c_k}$, thus it can be written by

$$\begin{aligned} \check{c_k} &= \Gamma(\epsilon) \widetilde{c_k} \\ &= \begin{bmatrix} 0_{(N_f N_c - \epsilon) \times \epsilon} & I_{N_f N_c - \epsilon} \\ I_\epsilon & 0_{\epsilon \times (N_f N_c - \epsilon)} \end{bmatrix} \widetilde{c_k} \\ &= \check{c_{k,-1}} + \check{c_{k,0}} \end{aligned} \tag{9}$$

where $\Gamma(\epsilon)$ is a permutation matrix with respect to the unknown propagation delay ϵ. It is easy to derive that $\Gamma(\epsilon)$ is an orthogonal matrix since

$$\begin{aligned} & \Gamma(\epsilon)\Gamma^T(\epsilon) \\ = & \ \Gamma^T(\epsilon)\Gamma(\epsilon) \\ = & \ I; \forall \epsilon \in \{0, 1, \cdots, N_c N_f - 1\}. \end{aligned}$$

Evidently, $\Gamma(\epsilon)$ circularly shifts the elements in $\widetilde{c_k}$ by ϵ.

$$\begin{aligned} c_{\check{k,}-1} & \equiv [\widetilde{c_k(\epsilon)} \ \cdots \ \widetilde{k}(N_f N_c - 1) \ 0 \ \cdots \ 0]^T, \\ c_{\check{k},0} & \equiv [0 \ \cdots \ 0 \ \widetilde{c_k(0)} \ \cdots \ \widetilde{c_k}(\epsilon - 1)]^T \end{aligned}$$

are the signature vectors associated to the kth user that $d_k(i-1)$ and $d_k(i)$ are modulated onto, respectively. Thereby, during the training interval, the $N_f N_c$-vector containing samples at the output of a CMF for ith symbol can be expressed as

$$r(i) = a_l \check{c_1} + \sum_{k=2}^{K} a_k (d_k(i-1) c_{\check{k,}-1} + d_k(i) c_{\check{k},0}) + n(i). \tag{10}$$

Since $\{d_k(i-1), d_k(i)\}_{k=2,\cdots,K}$ and n are zero-mean, the first-order statistics (ensemble average) can be approximated by the sample mean estimator provided that M is sufficiently large

$$\bar{r} = \frac{1}{M} \sum_{i=1}^{M} r(i) \cong a_1 \check{c_1} \tag{11}$$

Let c_1 be the $N_f N_c$-vector of the desired user's signature vector (undistorted), $h \equiv [\alpha_0 \alpha_1 \cdots \alpha_L 0 \cdots 0]^T$ accounts for the vector of channel IR (padding by $N_f N_c - L - 1$ zeros), and h_ϵ represents the vector that circularly-shifted h by ϵ. It is easy to deduce that

$$\check{c_1} = c_1 \otimes h_\epsilon \tag{12}$$

where $\otimes$ denotes circular convolution [6]. Since in general, c_1 is well-known to the desired mobile receiver, Equation (12) has implicitly separated $\bar{r}$ into a well-known term, c_1, and an unknown term, h_ϵ, which is determined by ϵ and α. Let $\bar{R}$, P_1, H, be the Discrete Fourier Transform (DFT) of $\bar{r}$, c_1, and h, respectively. Upon defining the DFT matrix with block size $N_f N_c$ as

$$\mathrm{w} = \frac{1}{\sqrt{N_f N_c}} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \exp[-j\frac{2\pi}{N_f N_c}] & \cdots & \exp[-j\frac{2(N_f N_c - 1)\pi}{N_f N_c}] \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \exp[-j\frac{2(N_f N_c - 1)\pi}{N_f N_c}] & \cdots & \exp[-j\frac{2(N_f N_c - 1)^2 \pi}{N_f N_c}] \end{bmatrix}$$

Then, we have

$$\begin{aligned} \bar{R} & = W\bar{r} \\ P_1 & = W c_1 \\ H & = W h. \end{aligned} \tag{13}$$

Since time-domain convolution is equivalent to frequency-domain multiplication [6], hence, we can obtain from Equation (11), Equation (12), and Equation (13)

$$\begin{aligned} \bar{R} &= W\bar{r} \cong a_1 W\check{c_1} = a_1 W(c_1 \otimes h_\epsilon) \\ &= a_1\sqrt{N_f N_c} P_1 \odot \phi(\epsilon) H \end{aligned} \qquad (14)$$

where

$$\phi(\epsilon) \equiv diag\{1 \exp[-j\frac{2\pi\epsilon}{N_f N_c}] \cdots \exp[-j\frac{2\pi(N_f N_c - 1)\epsilon}{N_f N_c}]\}$$

Note that in writing Equation (14), we have applied the fact that time-domain circular-shift is equivalent to phase shift in frequency-domain, $Wh_\epsilon = \phi(\epsilon)Wh = \phi(\epsilon)H$. Since P_1 can be calculated *a* priori, we may perform element-wise division from Equation (14), which yields

$$\begin{aligned} R(\hat{m}) &\equiv \frac{R(\hat{m})}{\sqrt{N_f N_c} P_1(m)} \\ &= a_1 H(m) \exp[-j\frac{2\pi m\epsilon}{N_f N_c}]; \quad m = 0, 1, \cdots, N_f N_c - 1. \end{aligned} \qquad (15)$$

Upon defining $\hat{R} \equiv [\hat{R}(0)\hat{R}(1) \cdots \hat{R}(N_f N_c - 1)]^T$, Equation (15) can be written in vector form

$$\hat{R} = a_1 \phi(\epsilon) H. \qquad (16)$$

Toward this end, performing Inverse Discrete Fourier transform (IDFT) on $\hat{R}$, we can obtain the impulse response of the channel circularly-time-shifted by ϵ.

$$\begin{aligned} W^H \hat{R} &= W^H a_1 \phi(\epsilon) H \\ &= a_1 \begin{bmatrix} 0_{\epsilon \times N_f N_c - \epsilon} & I_\epsilon \\ I_{N_f N_c - \epsilon} & 0_{N_f N_c - \epsilon \times \epsilon} \end{bmatrix} h \\ &= a_1 \Gamma(\epsilon) h \end{aligned} \qquad (17)$$

Since $\Gamma(\epsilon)$ is an orthogonal matrix, hence we develop the object function as

$$\hat{h}(\hat{\epsilon}) \equiv \Gamma(\epsilon) W^H \hat{R}.$$

Let us define $\hat{h}(0 : L)$ be the subvector truncated from the first $(L + 1)$ elements of $\hat{h}(\hat{\epsilon})$, we propose to estimate ϵ by maximizing the square norm (energy) of $\hat{h}(0 : L)$

$$\hat{\epsilon} = \arg \max_{0 \leq \epsilon \leq N_f N_c - 1} ||h(0 \hat{:} L)||^2 \qquad (18)$$

Once Equation (18) is evaluated, both ϵ and h ban be jointly estimated. Moreover, it is evident that the maximum value of $||h(0 \hat{:} L)||^2$ corresponds to a_1^2 since $\sum_{i=0}^{L} |\alpha_l|^2 = 1$.

We may summarize the above channel and timing estimation algorithm as the following steps:

Step 1: Construct W and calculate the frequency-domain counterpart of c_1, $P_1 = Wc_1$.

Step 2: Performing time-average during training period on the observation vectors,

$$\bar{r} = \frac{1}{M} \sum_{i=1}^{M} r(i) \cong a_1 \check{c_1}.$$

Step 3: Perform DFT on $\bar{r}$, to obtain $\bar{R}$, $\bar{R} = W\bar{r}$.

Step 4: Using Equation (15) to calculate $R(\hat{m})$, then construct $\hat{R}$.

Step 5: Calculate $\hat{h}(\hat{\epsilon}) \equiv \Gamma(\epsilon)W^H\hat{R}$ for every possible $\epsilon = 0, 1, \cdots, N_fN_c - 1$.

Step 6: Using Equation (18) to determine ϵ, h, and a_1^2.

3.2 Stage 2: Design of Constrained Minimum Output Energy (C-MOE) Receivers

Once ϵ has been estimated, we may offset the observation vectors to align with each bit. Thereby, the data model of Equation (10) becomes

$$\begin{aligned} r(i) &= a_1\tilde{c_1} + \sum_{k=2}^{K} a_k d_k(i)\tilde{c_k} + n(i) \\ &= a_1\tilde{c_1} + u(i); i = 1, 2, \cdots, M \end{aligned} \tag{19}$$

where $u(i) \equiv \sum_{k=2}^{K} a_k d_k(i)\tilde{c_k} + n(i)$ denotes the MUI plus noise vector. Employing the above M training data set, $\{r(i)\}_{i=1}^{M}$, we may estimate the correlation matrix of r by

$$\check{R_r} = \frac{1}{M}\sum_{i=1}^{M} r(i)r^H(i). \tag{20}$$

The rationale of the C-MOE receiver, also referred to as minimum variance distortionless response (MVDR) receiver, is to minimize the output energy, $E\{|w^H r(i)|^2\} = w^H\hat{R_r}w$, corresponds to the constraint that the desired signal should be distortionlessly passed.

$$\begin{array}{ll} \arg\min_w & w^H\hat{R_r}w \\ \text{subject to} & w^H\hat{\tilde{c_1}} = 1 \end{array} \tag{21}$$

where $\hat{\tilde{c_1}} = C_1\hat{\alpha}$, and $\hat{\alpha}$ is obtained from the proposed joint timing and channel estimator. Using Lagrange multiplier, the solution of the constraint optimization problem of Equation (21) can be obtained as

$$w_1 = \frac{\hat{R_r}^{-1}\hat{\tilde{c_1}}}{\hat{\tilde{c_1}}^H\hat{R_r}^{-1}\hat{\tilde{c_1}}} \tag{22}$$

After the training period, information bits can then be extracted by

$$d_1\hat{(}l) = sgn(w_1^H r(l)); l = M + 1, \cdots \tag{23}$$

Therefore, the output signal-to-interference-plus-noise power ratio (SINR) can be obtained as

$$\gamma_1 = a_1^2\frac{|w_1^H\tilde{c_1}|^2}{w_1^H R_u w_1} \tag{24}$$

where we may easily derive R_u from Equations (5) and Equation (19) as

$$\begin{aligned} R_u &\equiv E\{u(i)u^H(i)\} \\ &= \widetilde{C_1}A_1^2\widetilde{C_1}^H + \sigma^2 I_{N_cN_f} \end{aligned} \tag{25}$$

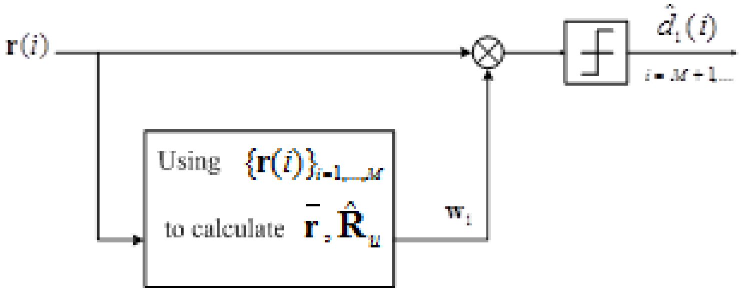
r(i)
$\hat{d}_1(i)$
$i = M+1,...$
Using $\{\mathbf{r}(i)\}_{i=1,...,M}$
to calculate $\bar{\mathbf{r}}$, $\hat{\mathbf{R}}_y$
$\mathbf{w}_1$

Figure 1: Block diagrams of the proposed data-aided joint timing-channel estimation and interference suppression in PAM UWB IR system

where $\widetilde{C_1} \equiv [\widetilde{c_2}\widetilde{c_3}\cdots\widetilde{c_k}]$ is a N_cN_f-by-$(K-1)$ matrix, A_1 is a diagonal matrix, $A_1 \equiv diag\{a_2 \cdots a_k\}$. The schematic block diagram is shown in Figure 1.

Unfortunately, to derive w_1 as depicted in Equation (23) needs to perform inverse of a matrix with size N_cN_f, which is in general computationally prohibitive. Hence from the complexity point of view, we attempt to exploit the known desired user's TH sequence to develop an efficient detection algorithm. In the second scheme, $r(i)$ is first partially spread by a bank of correlators each matched to a different resolvable path of the desired user. Thereby the outputs of the $(L+1)$ correlators yield

$$\begin{aligned} y(i) &= C_1^T r(i) \\ &= a_1 C_1^T \widetilde{c_1} + C_1^T \sum_{k=2}^{K} a_k d_k(i)\widetilde{c_k} + C_1^T n(i) \\ &= a_1 \check{c_1} + \sum_{k=2}^{K} a_k d_k(i)\widetilde{c_k} + v(i) \\ &= a_1 \check{c_1} + u_1(i) \end{aligned} \tag{26}$$

where $\check{c_k} \equiv C_1^T \widetilde{c_k}$, $v(i) \equiv C_1^T n(i)$, $u_1(i) = \sum_{k=2}^{K} a_k d_k(i)\widetilde{c_k} + v(i)$ denotes the MUI plus noise vector. We can deduce that the noise vector $v(i)$ is still jointly Gaussian with zero-mean and covariance (correlation) matrix $E\{C_1^T n(i) n^H(i) C_1\} = \sigma^2 C_1^T C_1$. In short, the original N_cN_f-by-1 observation data vectors, $\{r(i)\}$, after linear transformed by C_1, have been reduced to $\{y(i)\}$ with much smaller dimension. Following the rationale in the first scheme, the first-order statistics of $y(i)$ can be obtained by the sample mean estimator

$$\bar{y} \equiv \frac{1}{M} \sum_{i=1}^{M} y(i) \cong a_1 \check{c_1} \tag{27}$$

where the MUI plus noise term vanishes due to zero-mean characteristics of $u_1 i$. Upon evaluating the correlation matrix of $y(i)$ by

$$\hat{R_y} \equiv \frac{1}{M} \sum_{i=1}^{M} y(i) y^H(i). \tag{28}$$

We can deduce the weight vector for the second C-MOE receiver.

$$w_2 = \frac{\hat{R_y}^{-1}\bar{y}}{\bar{y}^H\hat{R_y}^{-1}\bar{y}} \tag{29}$$

The information bits can then be determined by $\hat{d_1(l)} = sgn(w_2^H y(l))$; $l = M+1, \cdots$. The output SINR can be obtained as

$$\gamma_2 = a_1^2 \frac{|w_2^H \widetilde{c_1}|^2}{w_2^H R_{u1} w_2} \tag{30}$$

where

$$\begin{aligned} R_{u1} &\equiv E\{u_1(i)u_1^H(i)\} \\ &= \widetilde{C_1} A_1^2 \widetilde{C_1}^H + \sigma^2 C_1^T C_1; \end{aligned}$$

$\widetilde{C_1} \equiv [\widetilde{c_2}\widetilde{c_3}\cdots\widetilde{c_k}]$ is a $(L+1)$-by-$(K-1)$ matrix.

4 Performance Analysis

In this section, we present numerical results to evaluate the performance of the proposed joint timing-channel estimator. Moreover, the performances of the two types of C-MOE UWB MS receivers are also comprehensively compared.

4.1 Evaluation of the Joint Timing and Channel Estimator

A plausible criterion to measure the estimation accuracy is root mean-squared-error (RMSE) that is defined as

$$RMSE \equiv \sqrt{\frac{1}{N_s}\sum_{n=1}^{N_s} ||\frac{1}{a_l}\hat{h(n)} - h||^2} \tag{31}$$

where N_s is the Monte-Carlo trial number. Unless otherwise specified, we have set the parameters $N_s = 100$, $N_f = 16$, $N_c = 16$, $K = 10$, $L = 10$ and all the active users' SNR are set to be 15 dB throughout all the simulation examples.

In Figure 2, we present the averaged RMSE with respect to the training length (M). As depicted in the figure, RMSE decreases as M increases. This demonstrates the fact that $\bar{r}$ is asymptotically (according to the window size M) approaches to $a_1\check{c_1}$.

In the second simulation example, RMSE is measured with respect to the desired user's SNR, which is defined as $SNR_1 \equiv (\frac{a_1}{\sigma})^2$ (in dB). As shown in Figure 3, larger SNR offers significantly better estimation performance (smaller RMSE).

In the last simulation example, we attempt to measure the near-far resistant characteristics of the proposed estimator. We first set the interferers' amplitudes to be the same, $a_2 = a_3 = \cdots = a_K = \eta$, and define the near-far ratio (NFR) as the interferer-to-desired user's power ratio, $NFR \equiv (\frac{\eta}{a_1})^2(dB)$. Varying NFR from $0dB$ to $15dB$, the resulted RMSE is shown in Figure 4. As shown in Figure 4, RMSE for the proposed estimator is insensitive (only slightly increases) to the increase of NFR.

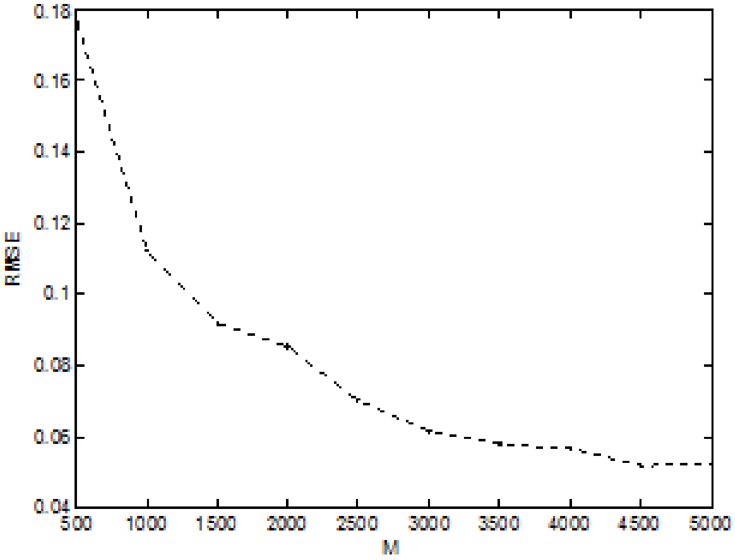

Figure 2: RMSE with respect to M

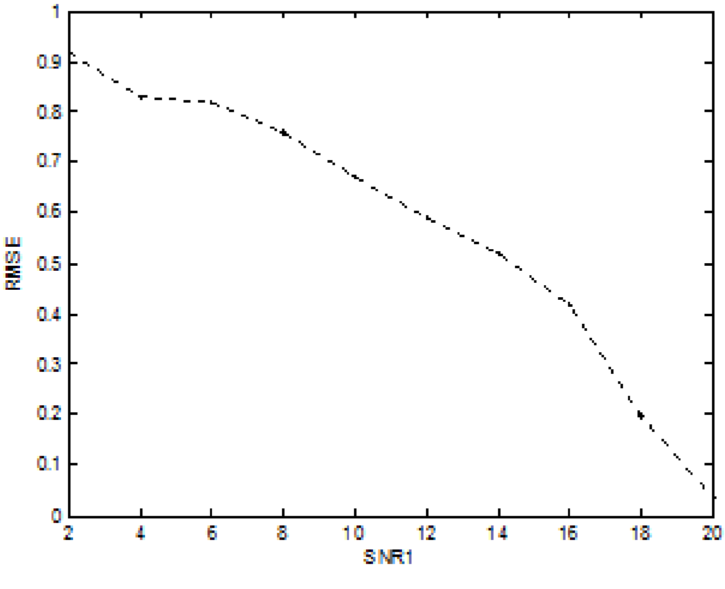

Figure 3: RMSE with respect to SNR_1

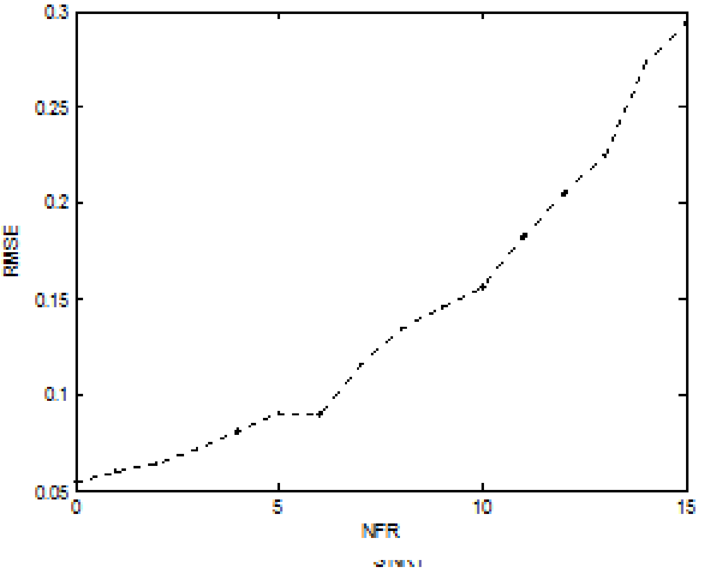

Figure 4: RMSE with respect to NFR

4.2 Evaluation of the Two Types of C-MOE Receivers

Figure 5 presents the SINR (in dB) with respect to the training data length, M. The performance of the ideal (with perfect channel information) MVDR based receiver is also provided as an optimum bound. We can verify from Figure 5 that both schemes converge to the steady state for small training data set. Note that Scheme 2 converges much faster than Scheme 1 since the data size is comprehensively reduced. We set $M = 800$ for the simulation examples hereafter.

Figure 6 presents the SINR with respect to SNR_1. As expected, the SINR of both schemes increases for larger SNR_1. More specifically, though Scheme 1 outperforms Scheme 2 in ideal case, it is worse than Scheme 2 in practical scenario. This demonstrates the fact that the weight vector with larger size is more sensitive to the estimation error (including correlation matrix and effective signature vector).

To characterize the near-far performance, the SINR performance with respect to NFR is revealed in Figure 7. As verified in Figure 7, both schemes are essentially near-far resistant. Furthermore, it is also verified that Scheme 2 outperforms Scheme 1 in practical situation.

Figure 8 presents SINR versus the number of simultaneous users, K. Though both schemes are insensitive to the variation of K, nevertheless, SINR of Scheme 2 degrades rapidly as K exceeds $(L+1)$. This is due to the fact that the weight vector size of Scheme 2 is only $(L + 1)$.

5 Conclusions

In this paper, we have developed a data-aided joint timing-channel estimator in multiuser TH UWB communication system. Moreover, exploiting the same training data set, two types of C-MOE MS receivers are proposed. The timing-channel estimator is computationally efficient since it depends sorely on the first-order statistics of the received data. Exploiting the desired user's TH sequence, the

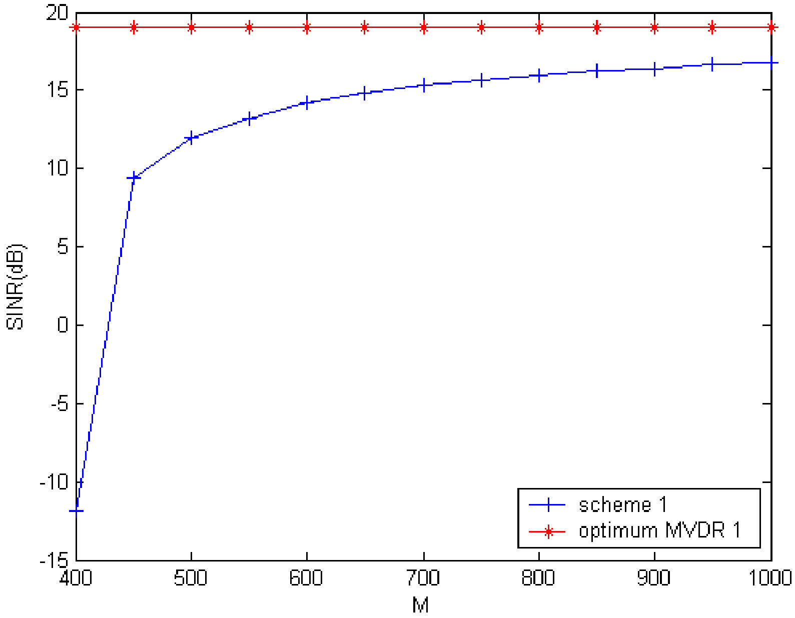

Figure 5: SINR performance with respect to the training data length, M

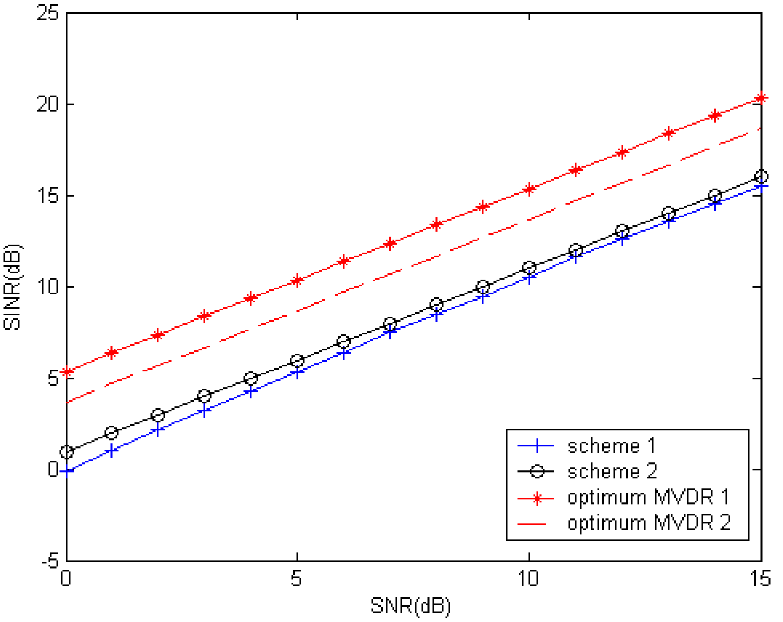

Figure 6: SINR performance with respect to the desired user's SNR

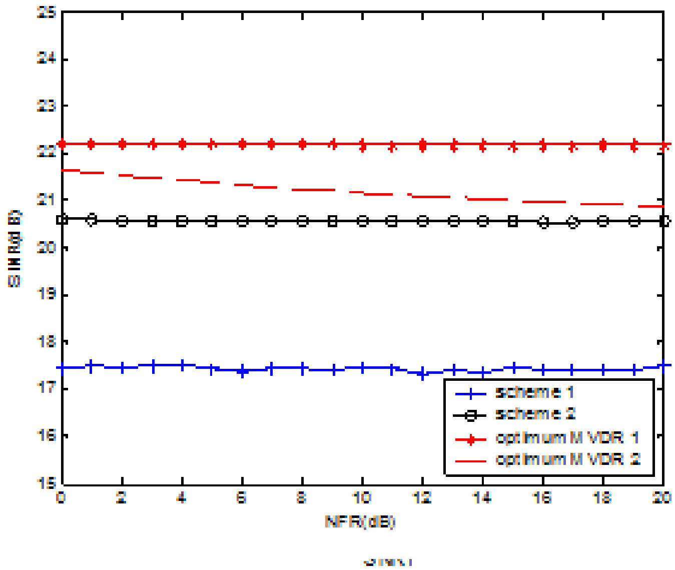

Figure 7: SINR performance with respect to NFR

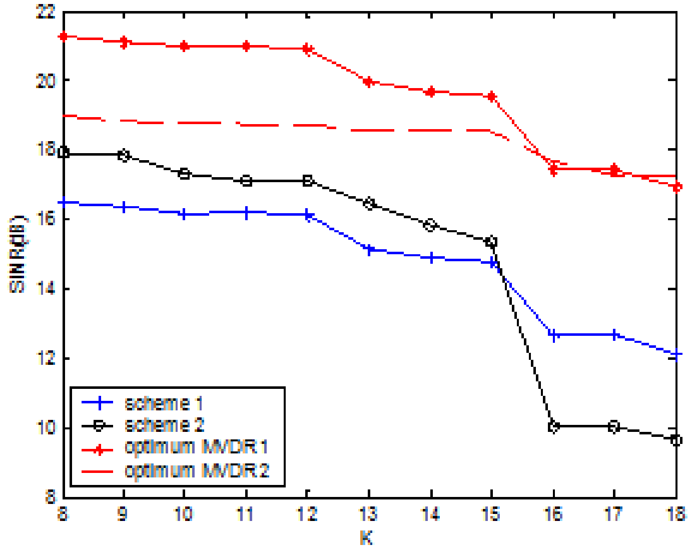

Figure 8: SINR performance with respect to the number of simultaneous users, K

complexity of the second C-MOE receiver is comprehensively reduced as compared to Scheme 1. Several simulation examples of the data-aided estimator and detector were carried out in a multiuser, multipath channel environment. We have demonstrated from the simulation results that Scheme 2 outperforms Scheme 1 in practical situation, nevertheless, the capability to mitigate MUI and near-far problems of Scheme 2 is limited by the number of resolvable paths. It is also verified that the proposed estimator is near-far resistant. More specifically, both the estimator and C-MOE MS receivers are shown to converge to the steady state for reasonably small training data set, thereby gives rise to practical use.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] T. Agrawal, V. Lakkundi, A. Griffin, et al., "Compressed sensing for OFDM UWB systems," in *Proceeding of the IEEE Radio and Wireless Symposium (RWS'11)*, pp. 190–193, Phoenix, AZ, USA., Jan. 16-19, 2011.

[2] M. L. Honig, U. Madhow, and S. Verdu, "Blind adaptive multiuser detection," *IEEE Transactions on Information Theory* vol. 41, no. 4, pp. 944–996, 1995.

[3] S. Y. Jung, "Design of a preamble signal for synchronization in ultra-wideband noncoherent energy detection receivers," *International Journal of Communication Systems*, vol. 26, Issue 4, pp. 465–480, Apr. 2013.

[4] V. Lottici, A. D'Andrea and U. Mengali, "Channel estimation for Ultra-wideband communications," *IEEE Journal on Select Areas Communications*, vol. 20, pp. 1638–1645, Dec. 2002.

[5] F. R. Mireles, "Performance of ultrawideband SSMA using time hopping and M-ary PPM," *IEEE Journal on Select Areas Communications*, vol. 19, no. 6, pp. 1186–1196, June 2001.

[6] S. Salivahanan, A. Vallavaraj, and C. Gnanapryia, *Digital Signal Processing*, Chap. 6, Tata McGraw-Hill, 2000.

[7] R. A. Scholtz, "Multiple access with time-hopping impulse modulation," in *Proceedings of MILCOM'93*, vol. 2, pp. 447–450, 1993.

[8] J. Tang, Z. Xu, and P. Liu, "Mean and covariance based estimation of multiple access UWB channels," in *IEEE Conference on Ultra Wideband Systems and Technologies*, pp. 458–462, 2003.

[9] Z. Tian and G. B. Giannakis, "Data-aided ML timing acquisition in ultra-wideband radios," in *IEEE Conference on Ultra Wideband Systems and Technologies*, pp. 142–146, 2003.

[10] Z. Tian, L. Yang and G. B. Giannakis, "Non-data-aided timing acquisition of UWB signals using cyclostationarity," in *Proceedings of ICASSP'02*, pp. IV.121–124, Apr. 2003.

[11] Z. Wang and X. Yang, "Ultra wideband communications with blind channel estimation based on first-order statistics," in *ICASSP'04*, pp. IV-529–IV-532, 2004.

[12] M. L. Welborn, "System considerations for ultra-wideband wireless networks," in *IEEE Radio and Wireless Conference*, pp.5–8, 2001.

[13] M. Z. Win and R. A. Scholtz, "Ultra wide bandwidth time-hopping spread-spectrum Impulse Radio for wireless multiple access communications," *IEEE Transactions on Communications*, vol. 48, no. 4, pp. 679–691, Apr. 2000.

[14] M. Z. Win and R. A. Scholtz, "Impulse radio: How it works," *IEEE Communications Letters*, vol. 2, no. 1, Jan. 1998.

[15] W. C. Wu, "Blind Signal Reception in Downlink Time-Hopping Ultrawideband Communication System," *European Transactions on Telecommunications*, vol. 19, no. 1, pp. 77–84, Jan./Feb. 2008.

[16] W. C. Wu, "A decorrelating-MRC based space-time multiuser receiver for time-hopping UWB system," *Wireless Personal Communications*, vol. 50, no. 3, pp. 275–289, 2009.

[17] L. Yang and G. B. Giannakis, "Low-complexity training for rapid timing acquisition in ultra-wideband communications," in *Proceedings of Global Telecommunications Conference*, San Francisco, CA. USA, pp. 769–773, Dec. 1-5, 2003.

[18] L. Yang and G. B. Giannakis, "Blind UWB timing with a dirty template," in *Proceedings of ICASSP'04*, pp. IV.509–512, Apr. 2004.

Biography

Wei-Chiang Wu was born in Miaoli, Taiwan, in 1964. He received the B.S. degree in electrical engineering from Chung Cheng Institute of Technology, Taiwan, in 1986, and the M.S. and Ph.D. degrees both in electrical engineering from the National Tsing Hua University, Hsin-chu, Taiwan, in 1992 and 1998, respectively. From 1992 to 1994, he was an assistant researcher in the Communication Department at Chung Shan Institute of Science and Technology (CSIST), Taiwan. From 1998 to 2000, he was in the Army of Taiwan, where he conducted the research of Integrated Logistic Support (ILS). Since 2011, he has been a Professor at the Department of Electrical Engineering, DaYeh University, Changhua, Taiwan. His current research interests are in multiuser detection, smart antenna technology, cognitive radio and ultra-wideband (UWB) impulse radio (IR) technology.

A Note on Design Flaws in One Aggregated-Proof Based Hierarchical Authentication Scheme for The Internet of Things

Lihua Liu[1], Zhengjun Cao[2], Olivier Markowitch[3]
(Corresponding author: Zhengjun Cao)

Department of Mathematics, Shanghai Maritime University[1]
No.1550, Haigang Ave, Pudong New District, Shanghai, China
Department of Mathematics, Shanghai University[2]
No.99, Shangda Road, Shanghai 200444, China
Computer Sciences Department, Université Libre de Bruxelles[3]
Boulevard du Triomphe - CP 212, 1050 Bruxelles, Belgium
(Email: caozhj@shu.edu.cn)

(Received Sept. 23, 2016; revised and accepted Nov. 1 & 12, 2016)

Abstract

Internet of Things (IoT) aims to integrate physical perceptions, cyber interactions, and social correlations, with the embedded intelligence. Recently Ning et al. have proposed an aggregated-proof based hierarchical authentication scheme for IoT. In this note, we show that Ning et al.'s scheme [IEEE TPDS, 26(3), 2015, 657-667] cannot be practically implemented because of design flaws in the underlying homomorphic encryption.

Keywords: Authentication protocol, cloud computing, homomorphic encryption, internet of things

1 Introduction

In the scenario of IoT, physical objects, cyber entities and social attributes are required to achieve interconnections with the embedded intelligence [11]. Since the integrated network is very complicated, it is inevitable to suffer from many security challenges on the aspects of system models, service platforms, infrastructure architectures and standardization [16, 17, 20].

Homomorphic encryption can translate an operation on ciphertexts into an operation on underlying plaintexts. The property is very important for many applications, such as e-voting, threshold cryptosystems, watermarking and secret sharing schemes.

In 1984, Goldwasser and Micali [10] proposed the first probabilistic encryption scheme which was also homomorphic. In 1999, Paillier [19] presented a novel additively homomorphic encryption. At PKC'01, Damgård and Jurik [7] put forth a generalization of Paillier's encryption. The elliptic curve variant of Paillier's cryptosystem is due to Galbraith [8].

At Eurocrypt'06, Schoenmakers and Tuyls [21] have considered the problem of converting a given Paillier's encryption of a value $x \in \mathbb{Z}_n$ into Paillier's encryption of the bits of x. At Eurocrypt'13, Joye and Libert [13] obtained another generalization. In 2013, Boneh et al. [1] considered the problem of private database queries using Paillier's homomorphic encryption. Recently, Cao and Liu [3] have presented a survey on the Paillier's cryptosystem and its variations.

At Asiacrypt' 14, Catalano et al. [5] presented an instantiation of publicly verifiable delegation of computation on outsourced ciphertext which supports Paillier's encryption. In 2015, Castagnos and Laguillaumie [4] designed a linearly homomorphic encryption scheme whose security relies on the hardness of the decisional Diffie-Hellman problem. The Gentry's fully homomorphic encryption scheme [9] relies on hard problems related to lattices. But Paillier's cryptosystem based on the problem of factoring RSA integers is still more competitive for applications that need only to add ciphertexts. Recently, Hsien et al. have investigated the possible usage of homomorphic encryption in client-server scenario [6, 12, 14, 15]. Note that a misapplication of a homomorphic encryption for numerical calculations can give rise to errors like the ones in [22] (see [2] for details).

Very recently, Ning et al. [18] have proposed a hierarchical authentication scheme for the Internet of Things. The scheme is based on two main cryptographic primitives: a homomorphic function and Chebyshev polynomials. Concretely, the homomorphic function is applied to describe the relationships of the directed path descriptors. However, we find flaws in the homomorphic encryption that cause the scheme failing.

2 Review of The Underlying Homomorphic Encryption

The homomorphic encryption is due to Zhang et al. [23]. It needs the following two functions:

$$f(t) := \begin{cases} t, & 0 \le t \le (p-1)/2 \\ p+t, & -(p-1)/2 \le n < 0 \end{cases}$$

$$f^{-1}(t) := \begin{cases} t \mod p, & 0 \le t \mod p \le (p-1)/2 \\ -(p - t \mod p), & (p+1)/2 \le t \mod p < p \end{cases}$$

For convenience, we list here the two descriptions, respectively. See Table 1 for details.

Table 1: The underlying homomorphic encryption

	Description in [18]	Description in [23]
Setup	Pick two large primes p, q. Set $n = pq$ and publish it. Keep p, q as the secret key.	See the left column.
Enc.	For $x \in \mathbb{R}$ with d effective decimal digits, compute $g_1(x) = 10^d x$. If $\lvert g_1(x)\rvert \le (p-1)/2$, $g_2(g_1(x)) \in \mathbb{Z}_p$, $\mathcal{F}(x) := g_2(g_1(x))^{k(p-1)+1} \mod n = c$.	For $x \in \mathbb{R}$ with d effective decimal digits, compute $g(x) = 10^d x$. If $\lvert g(x)\rvert \le (p-1)/2$, $f(g(x)) \in \mathbb{Z}_p$, $\mathcal{E}(x) := f(g(x))^{k(p-1)+1} \mod n = c$.
Dec.	$\mathcal{F}^{-1}(\mathcal{F}(x)) := g_2^{-1}(c \mod p)/10^d = x$.	$\mathcal{D}(\mathcal{E}(x)) := f^{-1}(c \mod p)/10^d = x$.

3 The Weaknesses of Underlying Homomorphic Encryption

The encryption system is directly defined over the field $\mathbb{R}$ of real numbers. We found several flaws in the proposed scheme. The definition of the encryption function is not complete. Indeed, it cannot work at all.

1) The authors have forgotten to specify the function $g_2(\cdot)$ and $g_2^{-1}(\cdot)$ (see page 660 in [18]). Moreover, both two descriptions have not specified the value k.

2) Given $x \in \mathbb{R}$ with d effective decimal digits, compute $g(x) = 10^d x$. If $|g(x)| > (p-1)/2$, then *the encryptor cannot complete the computational task* of $f(g(x))$ (see the definition of the function $f(\cdot)$).

3) *The encryption system is not of additive homomorphic property* even though the converted inputs are constrained to the upper bound $(p-1)/4$ (see Theorem 4, page 168 in [23]).

   For example, take $p = 29, q = 13, n = 377, k = 1,\ x = 1, y = 0.1$. We have

$$g(1) = 10^0 \times 1 = 1, g(0.1) = 10^1 \times 1 = 1$$

$$\mathcal{E}(x) = \mathcal{E}(1) = f(g(1))^{28+1} = 1 \mod 377,$$
$$\mathcal{E}(y) = \mathcal{E}(0.1) = f(g(1))^{28+1} = 1 \mod 377,$$
$$\mathcal{E}(x+y) = \mathcal{E}(1+0.1) = f(g(1.1))^{28+1} = 11^{29} = 98 \mod 377.$$

   Clearly, $\mathcal{E}(x+y) \neq \mathcal{E}(x) + \mathcal{E}(y)$.

4) Given $x \in \mathbb{R}$ with d effective decimal digits, in order to mask it, the encrypter has to compute $f(g(x))^{k(p-1)+1} \mod n$. It means "the secret key p must be known to the encrypter". To recover it, the decrypter has to compute $f^{-1}(c \mod p)/10^d$. It means "the secret key p must be known to the decrypter, too". In such case, *it is totally unnecessary to design the **asymmetric** encryption system.*

4 Conclusion

We show that Ning et al.'s scheme is flawed because it is based on a false encryption system. We would like to stress that it is impossible to design a homomorphic encryption system mapping a practical floating-point number system into any finite domain, because it is impossible to find an invertible encoding transformation associated with it.

Acknowledgments

The work is supported by the National Natural Science Foundation of China (61303200, 61411146001), the Brussels Region (Innoviris) and the SeCloud Project.

References

[1] D. Boneh, C. Craigentry, S. Halevi, F. Wang, and D. Wu, "Private database queries using somewhat homomorphic encryption," in *Proceedings of Applied Cryptography and Network Security (ACNS'13)*, pp. 102–118, Banff, AB, Canada, June 2013.

[2] Z. J. Cao and L. H. Liu, "Comment on 'harnessing the cloud for securely outsourcing large-scale systems of linear equations'," *IEEE Transaction on Parallel Distributed Systems*, vol. 27, no. 5, pp. 1551–1552, 2016.

[3] Z. J. Cao and L. H. Liu, "The paillier's cryptosystem and some variants revisited," *International Journal of Network Security*, vol. 19, no. 1, pp. 89–96, 2017.

[4] G. Castagnos and F. Laguillaumie, “Linearly homomorphic encryption from ddh,” in *Proceedings of the Cryptographer’s Track at the RSA Conference (CT-RSA’15)*, pp. 487–505, San Francisco, CA, USA, April 2015.

[5] D. Catalano, A. Marcedone, and O. Puglisi, “Authenticating computation on groups: New homomorphic primitives and applications,” in *Proceedings of Advances in Cryptology (ASIACRYPT’14)*, pp. 193–212, Kaoshiung, Taiwan, R.O.C., December 2014.

[6] T. Y. Chen, C. C. Lee, M. S. Hwang, and J. K. Jan, “Towards secure and efficient user authentication scheme using smart card for multi-server environments,” *Journal of Supercomputing*, vol. 66, no. 2, pp. 1008–1032, 2013.

[7] I. Damgård and J. Jurik, “A generalisation, a simplification and some applications of paillier’s probabilistic public-key system,” in *Proceedings of Public Key Cryptography (PKC’01)*, pp. 119–136, Cheju Island, Korea, February 2001.

[8] D. Galbraith, “Elliptic curve paillier schemes,” *Journal of Cryptology*, vol. 15, no. 2, pp. 129–138, 2002.

[9] C. Gentry, “Fully homomorphic encryption using ideal lattices,” in *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC’09)*, pp. 169–178, Bethesda, MD, USA, May 2009.

[10] S. Goldwasser and S. Micali, “Probabilistic encryption,” *Journal of Compter and System Sciences*, vol. 28, no. 2, pp. 270–299, 1984.

[11] B. Guo, D. Zhang, Z. Yu, Y. Liang, Z. Wang, and X. Zhou, “From the internet of things to embedded intelligence,” *World Wide Web Journal*, vol. 16, no. 4, pp. 399–420, 2013.

[12] W. F. Hsien, C. C. Yang, and M. S. Hwang, “A survey of public auditing for secure data storage in cloud computing,” *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016.

[13] M. Joye and B. Libert, “Efficient cryptosystems from 2k-th power residue symbols,” in *Proceedings of Advances in Cryptology (EUROCRYPT’13)*, pp. 76–92, Athens, Greece, May 2013.

[14] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, “A survey of public auditing for shared data storage with user revocation in cloud computing,” *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.

[15] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, “A survey of attribute-based access control with user revocation in cloud data storage,” *International Journal of Network Security*, vol. 18, no. 5, pp. 900–916, 2016.

[16] F. V. Meca, J. H. Ziegeldorf, P. M. Sanchez, O. G. Morchon, S. S. Kumar, and S. L. Keoh, “Hip security architecture for the ip-based internet of things,” in *Proceedings of 27th Int. Conf. Adv. Inform. Netw. Appl. Workshops*, pp. 1331–1336, 2013.

[17] H. Ning, H. Liu, and L. T. Yang, “Cyberentity security in the internet of things,” *Computers*, vol. 46, no. 4, pp. 46–53, 2013.

[18] H. Ning, H. Liu, and L.T. Yang, “Aggregated-proof based hierarchical authentication scheme for the internet of things,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 3, pp. 657–667, 2015.

[19] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in *Proceedings of Advances in Cryptology (EUROCRYPT’99)*, pp. 223–238, Prague, Czech Republic, May 1999.

[20] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, “Lithe: Lightweight secure coap for the internet of things,” *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3711–3720, 2013.

[21] B. Schoenmakers and P. Tuyls, “Efficient binary conversion for paillier encrypted values,” in *Proceedings of Advances in Cryptology (EUROCRYPT’06)*, pp. 522–537, St. Petersburg, Russia, May 2006.

[22] C. Wang, K. Ren, J. Wang, and Q. Wang, “Harnessing the cloud for securely outsourcing large-scale systems of linear equations,” *IEEE Transaction on Parallel Distributed Systems*, vol. 24, no. 6, pp. 1172–1181, 2013.

[23] T. Zhang, Q. Wu, W. Liu, and L. Chen, "Homomorphism encryption algorithm for elementary operations over real number domain," in *Proceedings of Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov.*, pp. 166–169, 2012.

Biography

Lihua Liu is an associate professor with Department of Mathematics at Shanghai Maritime University. She received her Ph.D. degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics, cryptography and information security.

Zhengjun Cao is an associate professor with Department of Mathematics at Shanghai University. He received his Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He served as a post-doctor in Computer Sciences Department, Université Libre de Bruxelles, from 2008 to 2010. His research interests include cryptography, discrete logarithms and quantum computation.

Olivier Markowitch is an associate professor with Computer Sciences Department at the Universite Libre de Bruxelles. He is also information security advisor of his University. He is working on the design and analysis of two-party and multi-party cryptographic protocols as well as on the design and analysis of digital signature schemes.

A Proposed E-government Framework Based on Cloud Service Architecture

Ahmad Mosa[1], Hazem M. El-Bakry[1], Samir M. Abd El-Razek[1], Sajjad Q. Hasan[2]

(Corresponding author: Ahmad Mosa)

Information Systems Department, Faculty of Computer and Information Sciences, Mansoura University[1]
El Gomhouria St, Mit Khamis WA Kafr Al Mougi, Mansoura, Dakahlia Governorate 35516, Eygpt
University of Baghdad, Iraq[2]
(Email: ahmed.mosa706@yahoo.com)

(Received Feb. 20, 2016; revised and accepted Mar. 30 & Apr. 10, 2016)

Abstract

E-government has a lack of investment over financial and organizational perspectives regards to the mechanism provided for supporting government services. There are many key challenges such as integrated database centers, interoperability, and quality of service. The proposed framework has great enhancement impact over investment including financial and organizational issues. Furthermore, the proposed framework setups different impacts to handle quality of service, service level agreement and pas as use based on cloud infrastructure. It is fully private for the government itself. In addition, it provides services to the general public through the instances. This results in a speedy and easy access to the services provided by the government at the lowest possible error ratio. Moreover, it allows various government units to increase efficiency, reduce costs, and provide potentially better customer service.

Keywords: Cloud computing, cloud service, E-government, E-service, service oriented architecture

1 Introduction

E-government is a suite of services which have range of consumers range from selected people to reach big number of public people as service consumers. These consumers have to be satisfied with service performance, integrity, interoperability, security, notification and much more. General pattern in e-government improvement works for signed up administrations that are compelling, easy to utilize, formed around and reacting to the requirements of the resident, and not only orchestrated the supplier's accommodation [12]. Thusly, the clients need have no information of - nor direct collaboration with - the administration elements included [15]. Thus, services need to consider information and data to be traded and handled flawlessly crosswise through the process of advancement of current e-government services. Interoperability is considered as a key issue. Still in ref. [8], three levels of interoperability were divided into: technical, semantic and organizational which confirmed it's role, not just as a specialized matter worried about connecting up PC systems, additionally as a basic necessity to share and re-use information in the middle of systems, and redesign authoritative procedures to better backing the administrations themselves [6].

Technical interoperability refers to the subjects of defining standard protocols connecting systems and data formats. Semantic interoperability interested in the trading of data in a reasonable route, whether inside or between organizations, either local or crosswise over nations and the endeavor area [8]. The third one alludes to empowering procedures to co-work, by revising rules for how Public Administrations (PAs) work inside, participate with their clients, and utilize Information and Communication Technologies (ICT). Containing set of service into a single portal is a key success feature that is known as integration. a basic requirement of PA portals is integration of services, which aims to assemble and change procedures that required for a specific resident's life occasion into one single administration and the comparing back-office rehearses. A promising arrangement is given by the one-stop portals of government [6, 23, 27, 28, 29, 30, 37] that are united on-line access points, where several PAs collaborate for the provision of integrated services.

The main goal of current paper is to propose a framework of e-government services that based on using pros of cloud computing environment. Which supports many features of quality of service, pay as you use, reliability, integration, notification etc. The proposed framework is evaluated on deep discussion relative to interoperability and integration. Next section explains basic information of most known service based system techniques of e-government which are used perfectly to provide services for citizens in e-government applications. In Section three, short term survey of recent researcher's activities and publications over service providing systems and applications especially based on cloud computing besides related applications. Section four is the presentation and discussion of the proposed systems and how can be applied and used. In turn a comprehensive discussion is maintained to evaluate the performance, explaining the impact of the proposed framework comparing their impact against other proposed systems via a strong discussion. Finally, paper is concluded with contribution statement rather than future works.

2 Preliminaries

Different common service architecture are used for providing e-service applications differ based on their mapping strategies and allocation techniques. The key mechanisms of service architecture are discussed because of their importance to derive the proposed system.

2.1 Web Service (WS) Based Architecture

Presently, there is no agreement on a definition of ”e-government Web-based services”. However, communication [18], “e-government” is known as ”online government services”, which can use interaction between users and government. If a meaning of ”e-government Web-based services ”is needed, according to this literatures, it can be known also as the services and information supplied to the citizen through government Web sites. In turn, it could be put a definition according to its several uses in this literature. McClure [14] defined e-government as government's utilization of innovation, especially Web-based Internet applications, to improve the entrance to and conveyance of government data and administration to nationals, business accomplices, and workers, different offices, and government elements [36]. Whereas, Golden et al. [21] argued that, electronic government comprises of utilizing innovation, especially the Internet, as a way to convey administrations to subjects, organizations and different substances with the reason for giving helpful access to administrations and government data. In a report came from the Momentum Research Group of Cunningham.

In order to provide services of e-government using web service architecture leads to many benefits which can be ensured. To provide services to the general public through the online might cause quicker and additional adequate access to government services with slight errors [32]. Additionally it implies that the units of government might notice exaggerated efficiencies, value reductions and probably higher client service. Attractiveness of those edges has been with success incontestable by numerous e-commerce initiatives within the non-public sector. Success in business surroundings doesn't mean that government agencies may have the benefit of the same initiatives by merely loading their services and data on the online. Web service systems have a key feature to facilitate interactions between the government agencies area unit and general public the directly associated with the come back on government's investment in delivering services on-line and developing websites. At a minimum, assume that the cost of delivered service is a smaller amount on a Website than several ancient ways, so every net interaction they put in their mind a value savings, even while not value savings to the government agencies, so the value of access by voters are often the supply of profit, usually in reduced travel value. Therefore, to get the pursued advantages, government agencies ought to move their customers - voters - from the recent service delivery system (i.e. ancient service delivery methods) to the new net based mostly one. Since this kind of advantages area unit based mostly upon the dimensions of use, a lot of individuals use it, a lot of potential potency and price reduction are gained.

If a government computing machine fails to help the interaction between the government and general public, the service delivery completed during this way won't be advantageous whereas competitor with the standard ways in which of service delivery. Such trade off of investment requires deep evaluation activity for guaranteeing returns from investments over time [24]. Monetary investment involves defrayal on instrumentation and technology necessary to deliver e-government Web-based services. Wherever government investments on delivering e-government Web-based services area unit sometimes monumental. For instance, the monetary investment for implementing ten to fifteen services on associate degree integrated portal will simply run to $100 million [1]. So as to form such investments worthy, government agencies should be able to justify some style of come back on investment, which usually needs analysis of the e-government Web-based services. Structure investment, on the opposite hand tends to be unperceivable, and contains the energy and time that government agencies ought to reorganizing, streamlining, and rethinking the service delivery system for the e-government initiatives.

The required raise in citizen's utilization of the Web-based services; either via iterate visit of a citizen, or via citizens' recommendation from one to another citizen concerning the new kind services. As a consequence, not solely the pursued interests can't be attained, investment created by government agencies won't pay off, too. it's visible that, via the analysis of e-government web-based services doesn't generate the value saving impact directly, it is substantial to ensure that the wanted cost-saving impact happens [20]. The presently enforced design of the database relies on replicating subsets of the government institutions databases into the Integrated Central Database. The main functionalities of the Integrated Central Database are replication and accessibility [5]. Both functionalities suffer from the lack of vital features which are: interoperability, flexibility and manageability. Which appears when work on replicating a government institution database with a different type database of the Integrated Central Database. The problem also appears when clients trying to access the Integrated Central Database over a transport, driver, or an API that is not natively supported by the Integrated Central Database. Another problem emerges from the inability to attain a central point of management for the operation of the Integrated Central Database. Service Oriented Architecture (SOA) is considered as technological solution adopted for integration purposes which enables combined use of preexisting applications, the standardized description, invocation, and retrieval [32].

2.2 Service Oriented Architecture

SOA gives an answer for shared and disseminated administrations and it accomplishes high interoperability, adaptability, and institutionalization by using the portrayal, disclosure, and conjuring of administrations [22]. To understand the concept of SOA model, one would utilize the (ESB) Enterprise Service Bus [25, 33]. ESB represents the middleware paste foundation that holds SOA parts together and incorporates and deals with the correspondence among various Web Services, applications, and sources of data. The three elements: Web Services, SOA and ESB considered as the foundation for understanding the e-Government Central Database. In turn, SOA becomes able to architect framework for e-government integrated central database that achieves interoperability, flexibility, and manageability. In which, researchers have overcome above short comings by transforming WS architecture into a SOA. Although, SOA have overcome major problems of the web service based applications for e-government, SOA have lack of many benefits of cloud computing architectures including save time, cost, scale etc. Next, cloud computing service basis is discussed explaining pros key features [5].

2.3 Cloud Computing Architecture

A cloud-based service provides through a shared pool of computing resources on-demand delivery of Information and Communication Technologies (ICT) services over a network, commonly over the internet, from. Cloud services are generally grouped into three types of offerings [11]:

- Infrastructure as a Service (IaaS), where storage, computing power, and networking are provided.
- Platform as a Service (PaaS), where applications can be developed and executed.
- Software as a Service (SaaS), where software application are delivered.

These services are generally standardized and configured by the provider to maximize economies of scale, and are delivered through four basic models: private, public, hybrid and community cloud. The differences relate to who provides the cloud services and how they are provided. Private cloud services are provided solely for the use of one organization, and are managed by that organization or a third party. Public cloud services can be used concurrently by a number of unrelated users, while the hybrid model shares attributes of both private and public cloud models. An example would be data stored in a private cloud or agency database that is manipulated by a program running in the public cloud. Community cloud services are shared by a number of organizations and support shared objectives, such as service delivery, security, policy, or compliance considerations [11, 20].

Cloud-based ICT services provide opportunities for agencies to achieve better value, flexibility and reliability, and make sustainable service delivery improvements [9, 10, 16, 17, 31, 34, 39]:

1) Cost - Moving from customizing and operating in house ICT to using the best available 'off the shelf' commodity solutions will reduce the total cost of ownership. Flexible, on-demand services enable solution testing without significant capital investment and provide transparency of usage charges to drive behavioral changes within agencies.

2) Consumption based pricing - The benefits of consumption based, pay as you go pricing enables an agency to move to a model that is aligned to actual demand.

3) Agility - On-demand, scalable and flexible services that can be implemented quickly provide agencies with the ability to respond to changing requirements and peak periods.

4) Innovation - Innovation will be facilitated by rapid and continuous system development.

5) Resilience - A large, highly resilient environment reduces the potential for system failure. The failure of one component of a cloud-based system will have less impact on overall service availability and reduce the risk of downtime.

6) Standardization - Adoption of cloud solutions by agencies will increase procurement of standard service offerings, providing opportunities for standardization and improved interoperability.

7) In-built upgrades - Future upgrades are removing the need for costly and lengthy upgrade cycles.

3 Literature Review

Many proposals of net services composition ways have been discussed in last years. For a closed survey, we have a tendency to discuss with [2, 26]. In current section, we introduce a summarized overview of some different techniques that deal with automatic web service composition. We take into consideration only techniques that utilize service dependency information, graph models, and semantics. The plain concept beyond dependency is that whenever a web service receives several inputs and returns several outputs, the outputs is somehow correlating or dependent on the specified inputs. By utilizing a graph model, the attitude of obtainable web services is appeared in terms of their input-output information, as well as semantic information about the web data. A graph is represented by a set of vertices or 'nodes' and a set of edges that link pairs of vertices. A graph might be undirected, significance that there is no variance between the two vertices connected with every edge, or its edges might be directed from one vertex to another. A weighted graph is a graph where every edge has a weight (some real number) connected with it. The dependency graph is utilized in finding a combined service to fulfill a specific request. The majority of composition graph-based styles or methods construct web services dependency graphs during runtime. They utilize a seeking algorithm for navigating dependency graphs for composing services. The major distinctions between these styles are Attributable to how they seek the dependency graph. A*, Dijkstra, Floyd, the mostly popular search techniques used were backward chaining, Forward chaining, and bidirectional search algorithms .

Hashemian et al. [34] save output and input dependencies among obtainable Web services in their dependency graph, and then construct composite services by using a graph seeking algorithm. In their graph, every service and Output and Input parameter is demonstrated by a vertex, service's Output and Input are demonstrated by outgoing and incoming edges, respectively. The authors take into account only the matching and dependencies among Output and Input parameters with the lack of focus on functional semantics, thus they can't warranty that the created composite services Responds to the requested functionality well.

Gekas et al. [13] developed a service composition registry as a hyperlinked graph network, dynamically analyzed its structure and with no size restrictions to conclude helpful heuristics to guide the composition process. Services are performed in a graph network and this graph was produced and explored during the composition process to find a potential path from the initial state to a final state. In order to minimize the time of searching, a group of heuristics were used. But according to the authors, creating the graph at the time of composition costs a lot from where of computation and limits the applicability of graph-based approaches to the problem of web service composition.

In [4], the authors utilize the backward chaining method in combined to depth initial search to obtain the needed services for a composite task. the author presented a summarized solution and they did not discuss a fulfillment plan generation algorithm obviously . Arpinar et al. [3] the authors used an approach which utilized semantic similarity and graphs for web service composition as we planned to do in this work. They took into consideration edges with weights and deploy a shortest-path dynamic programming algorithm according to Bellman- Ford's algorithm for computing the shortest path. concerning cost, the authors considered the output and Input and fulfillment time of each service likeness but they did not consider the services' nonfunctional attributes.

Talantikite et al. [35] they proposed to pre-compute and store a network of services that are connected by their Output and Input parameters. The link was built by utilizing semantic likeness functions based on ontology. They represented the service network utilizing a graph structure. Their approach utilized depth-first search algorithms and backward chaining to find sub-graphs that include services to accomplish the requested task. They proposed a way to choose an optimum plan in case of discover more than one plan. However, they also created the graph at the same time of composition which incurs substantial overhead.

On the investigation for the e-Government data integration, the authors in [35] propose a conceptual SOA-based framework for the Palestinian e- Government Central Database. In this paper we present the realization of that framework.

A SOA-based approach to data integration achieves interoperability. Works such as [7, 19] have stressed the importance of interoperability for the data integration process where database accessibility should be according to neutral mechanisms and will be freelance of the underlying implementation.

A technical construct that employs SOA as AN IT platform to handle totally different modalities, information streams, and devices within the operation space is conferred in [38]. They propose SOA for integration inheritance medical devices on networked medical devices. It is a model for a service-oriented e-Government support platform for the mixing of both information and application referred to as (SoGoSP) is projected in [34]. It integrates information and applications from varied business systems deployed in both e-Government external and internal networks. The model consists of 4 item layers that embrace application layer, common service layer, service support layer and service integration layer.

A solution to information integration downside between heterogeneous databases is conferred in [4]. The answer is predicated on constructing information center with XML schema and internet Service technique which might gives a sensible solution to issues with business logic technique invocation and obvious information exchange in low layer. The wants of abstracting, sharing and integration multiple heterogeneous info management systems in e-Government square measure self-addressed in [38]. They introduce design of e-Government info management platform supported SOA framework.

4 The Proposed Algorithm

Today, different governments are going to provide services that are suitable for citizen's capacity rather than stability. E-government application suites become principle concept to conduct wide range of clients/citizens. These applications suites suffer from many different challenges that were addressed in many researches before. Challenges include different information management systems, central database, robust infrastructure, interoperability, integrity and much more. In case, services are not satisfied perfectly the citizens of government, the country will have extreme challenge with cover the flow of work requests at their sites. Quality of service will be decreased rapidly to be insufficient. Delay of delivery, work overhead, inconsistent, and structure and semantics conflicts rather much more are subject of side effect to work performance rates. The problem of the proposed is focused on handling quality of service, integrity, delivery status, workflow notification, cost, security and interoperability between different organizations under approved unified government umbrella.

The proposed system based on solving the key problem of e-government service architecture based on web service architecture, see Figure 1 using cloud based service architecture. These shorts are listed as technical issues and functional challenges. In technical issues, the web service based model have single user profiling strategy, weak synchronization mechanism and have restricted user interface panel comparing to available hardware possible screen in current days. In single user profiling, e-government application have single entry point for every user which is represented by client web browser. These constraints restricts the user to be stand at his laptop if not his workstation computer. Single point of user profiling makes the user disable to consume his service on the go that limits his satisfaction and usages about service available by government. Synchronization is ancient challenges that forces applications to be solid against possible ways of system dynamicity. Synchronization works on consisting data, actions and flows of client's requests. Although, clients have verities of their terminal such as tablets, smart phones and on go transformable laptops as MS surface to access internet, but still web based e-government designs have only basis on computer, laptops stations. Always, user interface plays an important roles that increase human interactivity with the applications and system, in turn user interface represent shorten of web based service solutions. Whereas, functional shorts includes missing features as well detailed and descriptive workflow, status notification and sharing work packages.

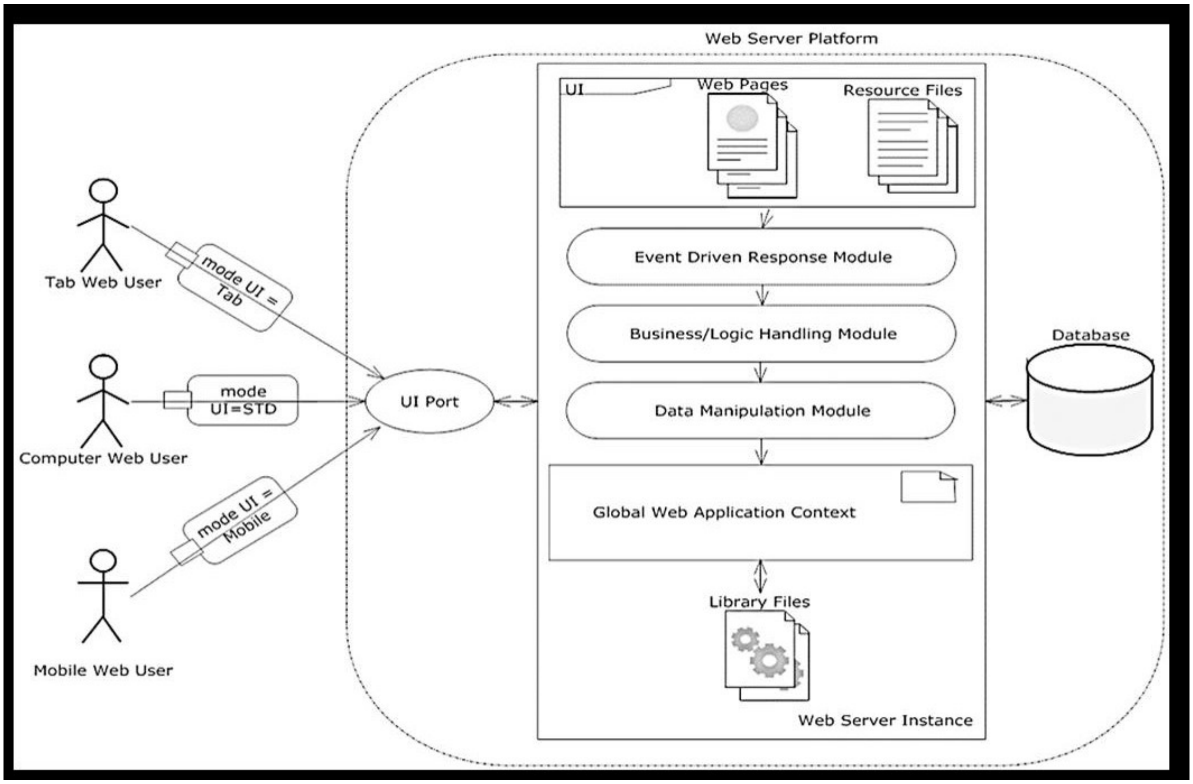

Figure 1: Web Service based e-government framework

The functional features are subject for being solved using work around strategies which may act as fit solution and may not rather than cost challenges. The functional requirements are elementary points in the proposed cloud based e-government framework. In the cloud based e-government architecture, there exists three basic blocks including user interface, data storage and back end block, see Figure 2. The user interface block containing different items related to user interaction ranging from humanity interaction to verities of computing terminals. In the user interface, there is ability to provide native interface for mobile handheld devices, tablets, transformable laptops also have ability to provide basic entry point as web page. On other hand, within block, cross platform development todays are fully supported depending on different technologies. All of these types of user interface support share global resources, preference, setting etc. In turn, user have many entry points to interact with applications services. Based on verities of interactions types, synchronization and central data storage becomes spot points of interest.

In order to handle central data storage, data storage block contains ability to insatiate one or more instance of database. These instances are transparent from user via transparency management layer. Transparency features include modules for data integrity checks, consistency and consolidation. These management operation is performed through handling transactions. Transactions can be online, offline or batch package. Synchronization layer is responsible for making data up to date between online and offline and visa verse. Such features are enabled through supporting specialized framework per development technology such as dot net framework have it's own compatible software development kit, android platform have mainly android sdk, also iOS, etc. These frameworks support high precision of application development, integrity and compatibility. The back end have scope covering verity of services as workflow and document management, user management, notification service and business logic of government system. In user management is a service based module focus on enabling user authentication and data storage for user accounts. The module provides a set of APIs facilitating user registration process, authentication, password management and user profile editing. The proposed module provides a choice between internal authentication or integration with social networks like Face book, Twitter or Google+ accounts. The module allows developers to manage all aspects of users' accounts, change user properties, reset password, enable or disable users.

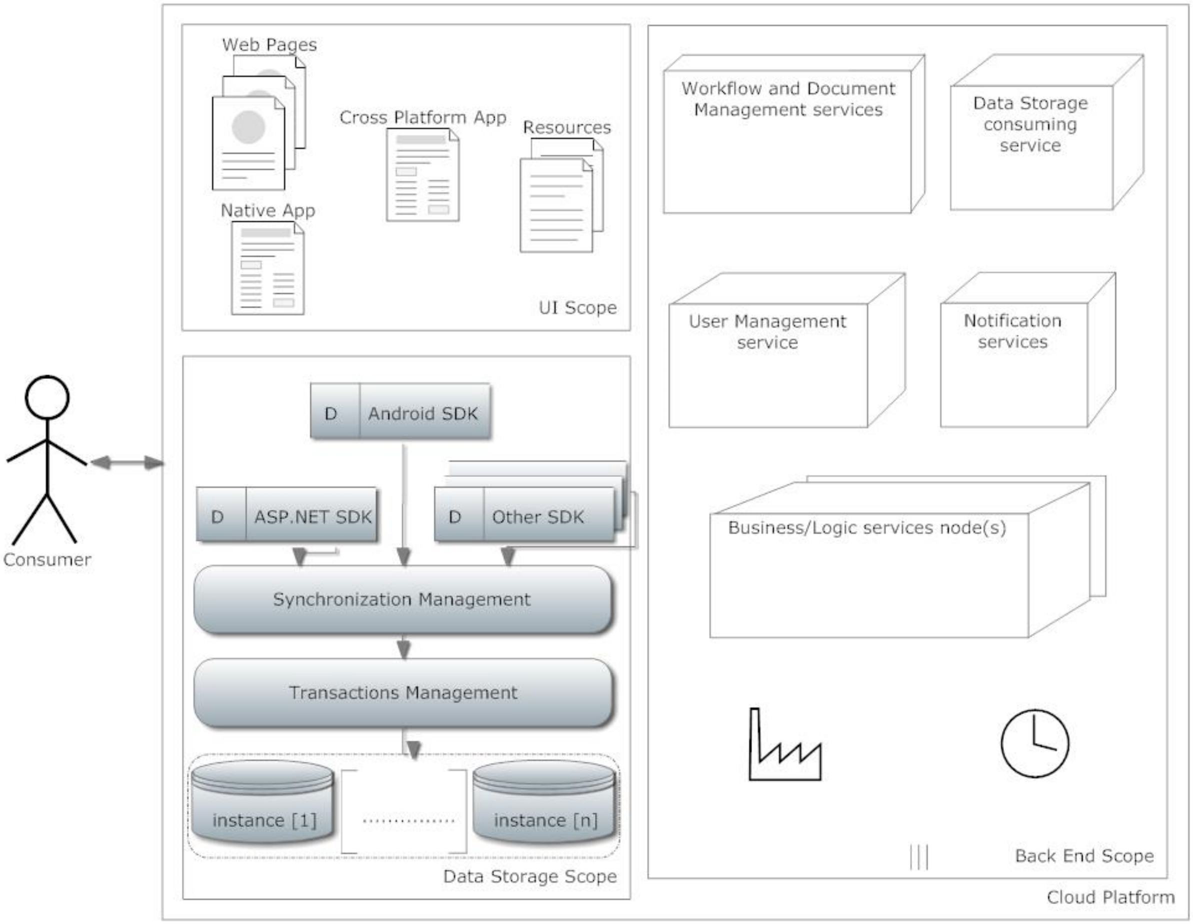

Figure 2: The proposed Cloud based e-government framework

The proposed user management service is designed to be orthogonal design. another services can be used independently, they are not dependent or connected. The proposed user management module should also be able to integrate with existing LDAP, Active Directory, CRM etc. also This module can work in conjunction with engine which provides comprehensive actionable analytics on user's behavior and the ability to take action, e.g. lead generation, survey, coupon, email, push notification, coupon, social post etc. workflow management service provides an infrastructure to setup, execute, and monitor scientific workflows and works on coordination of operation of individual components that constitute the workflow, i.e. orchestration. As research becomes more data-intensive and more reliant on the use of computers, larger volumes of experimentation data are recorded quicker and with greater precision. This trend has encouraged significant increase in complexity of scientific simulation software.

Additional difficulties arise from the need to deal with the mismatched data formats that various services produce or consume. Workflow management service have emerged to solve these problem and provide an easy-to-use way of specifying the tasks that have to be performed during a specific cycle. Whereas document management module focus on handling file creation, access, audit, share etc. The module have different capabilities including find files and documents in seconds instead of hours, share files in order to allow more than one worker to access the same file at the same time, version control where consumers are able to manage document changes and revisions including going back to a past version of a document, configure document security for who could see and make changes on files and enable auditing to emphasize who saw and made updates to documents and archiving documents via retention periods for documents.

Today, every applications should have notification facility to announce about details, services, policies, laws or any new flyer for his wide range consumers. The proposed allows e-government suite to reach their consumers from notification service module to keep them touch for supervision, their service status report, feedback about their consumers and monitor and control quality of service regards service consumer perspectives. In turn, notification service enforce consumer to be informed with details and status about his enquiry. Under, business logic service nodes, e-government applications are going to provide wide unlimited range of services for the public. Based on service node, there are many constrains of support are satisfied including cloud quality of service (QoS), service level agreement (SLA), pay as you use and use on the go principles. QoS includes two sides of service quality, side for the service quality during consuming e-government service from the citizen and other side from the government investor to achieve level of service demanding during provide the e-government service for the public. Same as QoS, SLA have two sides of participators, end user, citizen and investor, government.

During satisfying, QoS and SLA, the citizen can consume different services from various terminals on the go of his way. Also, investor pays only per use of his covered range of citizens not based on resources allocated as SOA and WS. The proposed framework offers facility to be central and dynamic center satisfying interoperability, integrity and transparency. The proposed framework should have minimum total cost of maintenance, configurations and other regular operations which are successive operations of installation and setup. These operations are subject to be role for the government private cloud provider. Generally, the proposed system have covered different key points of e-government service suites including interoperability, integration, integrated central database with replication and accessibility, flexibility and manageability which keep investment safe over different perspectives; financial and organizational investment.

5 Conclusion

A professional e-government framework that saves financial and organizational investment has been proposed. Such framework has been designed based on cloud benefits. Furthermore, it has kept away the limitations and cloud constrains via implementing government private cloud. In addition, it has the ability to migrate, imitate, develop and maintain e-government services. Moreover, it has awareness about interoperability, integration features, replication, manageability, flexibility and accessibility of integrated database centers.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] G. Al-Kibsi, K. de Boer, N. P. Rea, M. Mourshed, "Putting citizens on-line, not in line," *The McKinsey Quarterly*, 2001.

[2] A. Alamri, M. Eid, A. El Saddik, "Classification of the state-of-the-art dynamic web services composition," *International Journal of Web and Grid Services*, vol. 2, pp. 148–166, 2006.

[3] I. B. Arpinar, R. Zhang, B. Aleman-Meza, A. Maduko, "Ontology-driven web services composition platform," *Information Systems and E-Business Management*, vol. 3, no. 2, pp. 175–199, 2005.

[4] R. Aydogan and H. Zirtiloglu, "A graph-based web service composition technique using ontological information," in *IEEE International Conference on Web Services (ICWS 2007)*, pp. 1154-1155, 2007.

[5] R. S. Baraka, S. M. Madoukh, "A conceptual SOA-based framework for e-government central database," in *International Conference on Computer, Information and Telecommunication Systems (CITS'12)*, 2012.

[6] A. Bouguettaya, B. Medjahed, "Webdg - a platform for e-government web services," *Lecture Notes in Computer Science*, vol. 3289, pp. 553–565, 2004.

[7] D. Chen, N. Daclin, "Framework for enterprise interoperability," in *Proceedings of IFAC Workshop (EI2N'06)*, pp. 77–88, 2006.

[8] Commission of the European Communities, "Linking up europe: the importance of interoperability for e-government services," 2003. (`http://ec.europa.eu/idabc/servlets/Doc2bb8.pdf?id=1675`)

[9] N. S. Abu El-Ala, W. A. Awad and H. M. El-Bakry, " Cloud computing for solving e-learning problems," *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 12, pp. 135-137, Dec. 2012.

[10] N. S. Abu El-Ala, H. M. El-bakry, S. A. Abd El-Hafeez, "Personal cloud-based learning environment," *International Journal of Computer Science and Engineering*, vol. 8, no. 4, pp. 122–127, Apr. 2016.

[11] D. C. H. Elmaghraoui, I. Zaoui and L. Benhlima, "Graph based e-government web service composition," *International Journal of Computer Science*, vol. 8, no. 5, pp. 103–110, 2011.

[12] J. Gamper, N. Augsten, "The role of web services in digital government," *Lecture Notes in Computer Science*, vol. 2739, pp. 161–166, 2003.

[13] M. F. J. Gekas, "Automatic web service composition based on graph network analysis metrics," in *International Conference on Ontology, Databases and Applications of Semantics (ODBASE'05)*, pp. 1571–1587, 2005.

[14] W. E. A. Golden, "The role of process evolution in achieving citizen centered e-government," in *Ninth Americas Information Systems*, pp. 801–810, 2003.

[15] A. Gugliotta, L. Cabral, J. Domingue, V. Roberto, M. Rowlatt, E. C. Council, and R. Davies, "A semantic web service-based architecture for the interoperability of e-government services," *WISM'05*, 21, 2005.

[16] R. Izzat, B. T. Shabana A. M. Riad and H. M. El Bakry, "Spatial query performance for GIS cloud," *International Journal of Electronics Communication and Computer Engineering*, vol. 5, no. 8, pp. 56–65, Aug. 2015.

[17] M. Khaleel, H. M. El Bakry, and A. A. Saleh, "Developing e-learning services based on cache strategy and cloud computing," *International Journal of Information Science and Intelligent System*, vol. 3, no. 4, pp. 45–52, Oct. 2014.

[18] R. Klischewski, “Semantic web for e-government,” *Lecture Notes in Computer Science*, vol. 2739, pp. 288–295, 2003.

[19] H. Ma, “A service-oriented e-government support platform for integration of application and data,” in *Second International Conference on Information Technology and Computer Science (ITCS’10)*, pp. 398–401, 2010.

[20] S. Madoukh and R. Baraka, “A soa-based e-government data integration,” *International Arab Journal of e-Technology*, vol. 3, pp. 138-145, Jan. 2014.

[21] D. McClure, “Electronic government: Federal initiatives are evolving rapidly but they face significant challenges,” in *Statement of David L. McClure, U.S. General Accounting Office, before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives*, 2000. (`http://www.gao.gov`)

[22] B. Medjahed, A. Rezgui, A. Bouguettaya, M. Ouzzani, “Infrastructure for e-government web services,” *IEEE Internet Computing*, vol. 7, no. 1, pp. 58- 65, 2003.

[23] A. Mosa, H. M. El Bakry, and M. Abuelkhir ”Cloud computing in e-Government: A survey,” *International Journal of Advanced Research in Computer Science & Technology*, vol. 3, no. 2, pp. 132–139, 2015.

[24] E. Mugellini, M. C. Pettenati, “Egovernment service marketplace: Architecture and implementation,” in *Proceedings of the 2005 international conference on E-Government: towards Electronic Democracy (TCGOV’05)*, pp. 193–204, 2005.

[25] M. P. Papazoglou, P. Traverso, S. Dustdar, F. Leymann, “Service-oriented computing research roadmap,” *International Journal of Cooperative Information Systems*, vol. 7, no. 2, pp. 223–255, 2008.

[26] X. S. J. Rao, “A survey of automated web service composition methods,” in *Semantic Web Services and Web Process Composition (SWSWPC’04)*, pp. 43–54, 2004.

[27] A. M. Riad, G. H. El-Adl, M. H. Manoun and H. M. El-Bakry, “A decision support system framework for E-government,” *International Journal of Computational Linguistics and Natural Language Processing*, vol. 1, no. 3, pp. 75–84, 2012.

[28] A. M. Riad, G. H. El-Adl, M. H. Manoun and H. M. El-Bakry, “Effective and secure DSS for e-Government,” in *Proceedings of the 1st WSEAS International Conference on Information Technology and Computer Networks (ITCN’12)*, pp. 243–255, Vienna, Austria, Nov. 2012.

[29] A. M. Riad, H. M. El-Bakry, and Gamal H. El-Adl, “E-government frameworks survey,” *International Journal of Computer Science*, vol. 8, no. 3, pp. 319–323, 2011.

[30] A. M. Riad, H. M. El-Bakry, and Gamal H. El-Adl, “A novel service for e-Government,” *International Journal of Computer Science and Information Security*, vol. 9, no. 1, pp. 193–200, 2011.

[31] A. M. Riad, H. M. El-Bakry, and G. H. El-Adl, “A new developed DSS framework for complicated services of e-Government,” in *Proceedings of 13th WSEAS International Conference on MATHEMATICAL and COMPUTATIONAL METHODS in SCIENCE and ENGINEERING (MACMESE’11)*, pp. 124–129, Jakarta, Indonesia, Dec. 1-3, 2011.

[32] J. Shutter and E. de Graffenreid, “Benchmarking the egovernment revolution,” *tech. rep., Report on Citizen and Business Demand*, Momentum Research Group, July 2000.

[33] M. Strahle, M. Ehlbeck, V. Prapavat, K. Kuck, F. Franz, J. U. Meyer, “Towards a service- oriented architecture for interconnecting medical devices and applications,” in *IEEE High Confidence Medical Devices, Software, and Systems and Medical Device Plug-and-Play Interoperability (HCMDSS-MDPnP’07)*, pp. 153–155, June 2007.

[34] S. Hashemian and F. Mavaddat, “A graph-based framework for composition of stateless web services,” in *ECOWS’06*, IEEE Computer Society (D. Washington, ed.), pp. 75–86, 2006.

[35] H. N. Talantikite, D. Aissani, N. Boudjlida, “Semantic annotations for web services discovery and composition,” *Computer Standards Interfaces*, vol. 31, no. 6, pp. 1108–1117, 2009.

[36] S. B. Lili Wang and J. Gant, "Evaluating web-based e-government services with a citizen-centric approach," in *38th Hawaii International Conference on System Sciences*, 2005.

[37] M. A. Wimmer, "European development towards online one-stop government: The eGOV project," in *ICEC'01*, 2001. (`https://pdfs.semanticscholar.org/ef79/248e5ae739a957f7948fe662c52d6a620dfc.pdf`)

[38] J. Yunliang, Z. Xiongtao, S. Qing, F. Jing, Z. Z. Ning, "Design of e-government information management platform based on soa framework," in *First International Conference on Networking and Distributed Computing (ICNDC'10)*, Hangzhou, pp. 165–169, Oct. 2010.

[39] S. Ziad, H. M. El Bakry, and I. M. Abdelhady, "A proposed framework for ranking and reservation of cloud services based on quality of service," *International Journal of Advanced Research in Computer Science & Technology*, vol. 3, no. 2, pp. 195–199, April-June 2015.

Guide for Authors

International Journal of Electronics and Information Engineering

International Journal of Electronics and Information Engineering (IJEIE) will be committed to the timely publication of very high-quality, peer-reviewed, original papers that advance the state-of-the art and applications of Electronics and Information Engineering. Topics will include, but not be limited to, the following: Algorithms, Bioinformatics, Computation Theory, AI, Fuzzy Systems, Embedded Systems, VLSI/EDA, Computer Networks, Information Security, Database, Data Mining, and Information Retrieval, Digital Content, Digital Life, and Human Computer Interaction, Image Processing, Computer Graphics, and Multimedia Technologies, Information Literacy, e-Learning, and Social Media, Mobile Computing, Wireless Communications, and Vehicular Technologies, Parallel, Peer-to-peer, Distributed, and Cloud Computing, Semiconductor, Software Engineering and Programming Languages, Telecommunication, etc.

1. Submission Procedure

Authors are strongly encouraged to submit their papers electronically by using online manuscript submission at http://ijeie.jalaxy.com.tw/.

2. General

Articles must be written in good English. Submission of an article implies that the work described has not been published previously, that it is not under consideration for publication elsewhere. It will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.

2.1 Length Limitation:

All papers should be concisely written and be no longer than 30 double-spaced pages (12-point font, approximately 26 lines/page) including figures.

2.2 Title page

Title page should contain the article title, author(s) names and affiliations, address, an abstract not exceeding 100 words, and a list of three to five keywords.

2.3 Corresponding author

Clearly indicate who is willing to handle correspondence at all stages of refereeing and publication. Ensure that telephone and fax numbers (with country and area code) are provided in addition to the e-mail address and the complete postal address.

2.4 References

References should be listed alphabetically, in the same way as follows:

For a paper in a journal: M. S. Hwang, C. C. Chang, and K. F. Hwang, ``An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445--446, 2002.

For a book: Dorothy E. R. Denning, *Cryptography and Data Security*. Massachusetts: Addison-Wesley, 1982.

For a paper in a proceeding: M. S. Hwang, C. C. Lee, and Y. L. Tang, ``Two simple batch verifying multiple digital signatures," in *The Third International Conference on Information and Communication Security (ICICS2001)*, pp. 13--16, Xian, China, 2001.

In text, references should be indicated by [number].

2.5 Author benefits

No page charge is made.

Subscription Information

Individual subscriptions to IJEIE are available at the annual rate of US$ 200.00 or NT 6,000 (Taiwan). The rate is US$1000.00 or NT 30,000 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Jalaxy Technique Co., LTD." For detailed information, please refer to http://ijeie.jalaxy.com.tw or Email to ijeieoffice@gmail.com.