行政院國家科學委員會專題研究計畫 成果報告

嵌入式系統平台多媒體影音播放的電力效能分析
研究成果報告(精簡版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 98-2221-E-029-028-
執 行 期 間 ：98 年 08 月 01 日至 99 年 07 月 31 日
執 行 單 位 ：東海大學資訊工程與科學系

計畫主持人：劉榮春
共同主持人：林祝興
計畫參與人員：碩士班研究生-兼任助理人員：鐘蓉蓉
碩士班研究生-兼任助理人員：徐煒程
碩士班研究生-兼任助理人員：左浩天
碩士班研究生-兼任助理人員：吳家維
大專生-兼任助理人員：賴信斌
博士班研究生-兼任助理人員：李鎮宇

報 告 附 件 ：出席國際會議研究心得報告及發表論文

處 理 方 式 ：本計畫可公開查詢

中 華 民 國 99 年 09 月 30 日

目錄

目錄	1
第一章 前言	2
第二章 研究目的	3
第三章 文獻探討	4
第四章　研究方法	6
第五章 結果與討論	7
第六章 計畫成果自評	10
參考文獻	12

第一章 前言

在現代的無所不在計算環境裡，以嵌入式系統建置的裝置出現於日常生活的各個角落與應用中，並且使用者常常不知不覺地使用它們，例如在通信時網路的電話交換機與使用者的行動電話，聽音樂時的mp3播放器，看視訊的PDA或DVD播放器，玩遊戲的遊戲機，作導航的GPS接收器，廚房與客廳的各項家電例如微波爐與洗衣機等等，嵌入式系統建置的設備與我們的食衣住行息息相關，也增進了現代生活的便利性，但也更突顯了另一個議題，亦即節能問題。

不管是考慮建置嵌入式系統手持行動裝置裡有限的電池壽命與電力管理，或是普遍使用的各項建置嵌入式系統電子裝置的節能技術，如何靈活地運用科技產品，又不至於對全球環境造成衝擊，是一個不可忽視的議題。嵌入式系統的應用廣泛，全球微控制器的出廠量在2010年時每一年預估會超出200億個，這個驚人的數字告訴了我們對嵌入式系統使用時的電力效能的重要性。消費性電子及其服務在娛樂、行動、和通信上的需求，對全球能源造成相當大的壓力，對全球資源與環境造成非常大的衝擊，因此降低電子產品能源耗損的衝擊，明智的節約電能的策略將非常重要！

近來最熱門的智慧型手機、PDA、膝上型電腦、掌上型遊戲機及各類型行動撥放裝置，因為電腦與網路的普遍化使得各種類型多媒體資料的蓬勃發展，在這個資訊化的時代，各種類型多媒體資料必須能被快速的傳播與交流。而聲光影音是最直接的溝通工具、也是最常使用的工具，所以我們將在各種嵌入式系統平台上做影音播放的電力效能分析，以便未來各種影音播放格式的發展參考。

此報告接下來的第二章將介紹研究目的，第三章為相關文獻探討，第四章為研究方法，接著第五章為實驗結果與討論，第六章總結整個研究計畫與自評。

第 2 章 研究目的

近年來，嵌入式裝置的日益普，人們的生活已與嵌入式裝置息息相關。嵌入式裝置上的使用除了一般的功能外，也多了些許趣味性。影音功能現在已是大多數嵌入裝置的基本設備了，多數廠商所生產的行動裝置將影音功能列為不可或缺的功能；消費者在選擇行動裝置上也會考量到影音功能。因此多數人都使用過嵌入式裝置上的影音功能，利用來播放多媒體的資訊。

由於多數的嵌入式裝置限制在電池容量的大小，較大容量的電池能提供較長的使用時間，但是卻不適合攜帶。因此，如何在有限的電池之下達到最長時間的使用效率是很重要的議題。

目前，亦有許多學者，針對環保節能方面，發表多篇論文。近年來，由於環保意識高漲，且綠色能源議題需要在開源與節流的方式並進，因此，我們針對嵌入式裝置上作節能的分析，相信可以提供開發的廠商，或是廣大的使用者，一個較為適切可行的方式去使用行動手持裝置，提升電池電力使用效能。

第三章　文獻探討

我們對於常用的幾種數位影像與數位音訊常見的編碼，做一有系統且完整的了解與分析研究。

處理數位影像常見的 Codecs

1. MP3：

MPEG-1 Audio Layer 3，即 MP3，是當今流行的一種數字音訊編碼和有損壓縮格式，它是在 1991 年由位於德國埃爾朗根的研究組織 Fraunhofer-Gesellschaft 的一組工程師發明和標準化的。它可以大幅度地降低音訊的數據量，且對於大多數人的聽覺感受來說，其音質與最初未壓縮音頻相比沒有明顯的下降。在 MP3 中使用了許多技術其中包括心理聲學以確定音頻的哪一部分可以丟棄。MP3 音頻可以按照不同的位元率進行壓縮，提供了在數據大小和聲音質量之間進行權衡的一個範圍。

2. WMA：

WMA(Windows Media Audio)是微軟公司開發的一種數字音頻壓縮格式。一些使用 Windows Media Audio 編碼格式編碼其所有內容的純音訊 ASF 文件也使用 WMA 作為擴展名。WMA 格式最初為微軟公司私有，但是隨著蘋果公司的 iTunes 對它的支持，這個格式正在成為 MP3 格式的競爭對手。另外，一般情況下相同音質的 WMA 和 MP3 音訊檔案，WMA 體積較小。

3. OGG：

OGG 是一個完全開放的多媒體系統計劃的名稱，也是 OGG Vorbis 文件的擴展名。OGG Vorbis 是一種類似於 Mp3 的有損音頻壓縮格式，但是它自由且開放原始碼。Vorbis 為此種音頻壓縮格式的名稱。OGG Vorbis 格式非常先進，雖然 Vorbis 也是有損壓縮，但是由於其使用了更加先進的聲學模型，同樣 Bit rate (比特率)下的 OGG 文件比 Mp3 文件聽起來更好一些。

處理數位音訊常見的 Codecs

1. MPEG-4：

MPEG-4 是一套用於音頻、視頻信息的壓縮編碼標準，由國際標準化組織 IEC 活動圖

像專家組（即 MPEG）制定，第一版在 1998 年 10 月通過，第二版在 1999 年 12 月通過。MPEG-4 格式的主要用途在於網上（串流媒體）及光碟分發，語音傳送（視像電話），以及電視廣播。

MPEG-4 包含了 MPEG-1 及 MPEG-2 的絕大部份功能及其他格式的長處，並加入及擴充對虛擬現實模型語言(VRML for Virtual Reality Modeling Language)的支援，物件導向的合成檔案（包括音效，視訊及 VRML 物件），以及數位權限管理及其他互動功能。

2. H.263：

H.263 是由 ITU-T 在 1995/1996 年制定的視頻會議用的低碼率視頻編碼標準，屬於視頻編解碼器。它是 ITU-T 視頻編碼專家組(VCEG)的視訊編碼標準 H.26x 家族成員之一。H.263 最初設計為基於 H.324 的系統進行視訊資料傳輸(即基於公共交換電話網路 PSTN，和其它基於電路交換的網路，進行視訊會議和視訊電話用)。後來發現 H.263 也可以成功的應用在 H.323（基於 RTP/IP 網路的視訊會議系統），H.320（基於 ISDN 的視訊會議系統），RTSP（串流媒體傳輸系統）和 SIP（基於網際網路的視訊會議系統）。在 H.263 之後，ITU-T(在與 MPEG 的合作下)的下一代視頻編解碼器是 H.264，或者叫 AVC 以及 MPEG-4 第 10 部分。

3. WMV：

WMV 是在網際網路上最流的視訊編解碼器之一，與其它編解碼器彼此競爭，例如 Real Video、DivX、Xvid 與 H.264 等。WMV 可以使用 MPlayer 或者 Windows Media Player 等播放器播放。若用於 Linux 等不同平臺上,則使用 Ffmpeg 來實現 WMV 編解碼的第三方播放器。WMV 通常使用 Advanced Streaming Format（ASF）封裝，也可以使用 AVI 或 Matroska 格式封裝。AVI 封裝的檔案可以是.avi，ASF 封裝的話則是.wmv 或者.asf，MKV 封裝的話則是.mkv。當使用 VirtualDub 編碼器編碼和 WMV9 VCM 編解碼實現的時候，WMV 可以儲存在 AVI 檔案中。Mac 的微軟公司媒體播放器不支持所有的 WMV 編碼的檔案格式，因為它只支持 ASF 檔案格式封裝，Flip4Mac 和 QuickTime 或者用於 MacOSX 的 Mplayer 則可以播放更多格式的檔案。當使用 ASF 檔案格式封裝的時候，WMV 能夠支援以用於保護知識產權的數位權利管理工具。

第四章　研究方法

系統架構

我們希望能在相同的環境下建構出兩組實驗環境，分別針對音訊與影像的播放進行實驗分析。我們利用具有開發性的嵌入式平台來建構系統架構，如此一來可以將我們的實驗結果，導入到一般嵌入式產品的實際優化、分析上。

我們將原始的數位影像及音訊利用數種編碼來進行編碼，編碼後的多媒體檔案分別存入嵌入式系統中利用播放軟體進行播放。播放時，利用電力資料擷取裝置來擷取因播放多媒體檔案所多消耗的電力。為求公平，我們可採取數首音樂分別執行多次的實驗，擷取時亦可針對單首音樂擷取數千次的電力訊號做平均，這樣可以取得較為真實的電力消耗情形。最後，利用電腦軟體分析整體電力消耗情形，這樣可以看出在何種條件下，撥放影音數位訊號消耗最多電量。

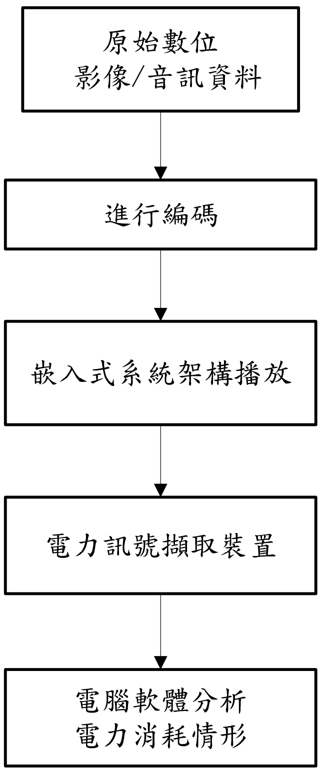

圖 一 系統架構圖

整個系統的概略架構如圖一中表示，將原始數位影像或音訊利用 codec 來做編碼，編碼完存放至嵌入式系統中播放同時利用電力訊擷取裝置將訊號讀入後轉換，再傳送給電

腦軟體去做統計分析。我們就電腦軟體統計電力消耗的情形趨勢，判斷在何種編碼與參數下能達到最低的電力消耗。

硬體架構

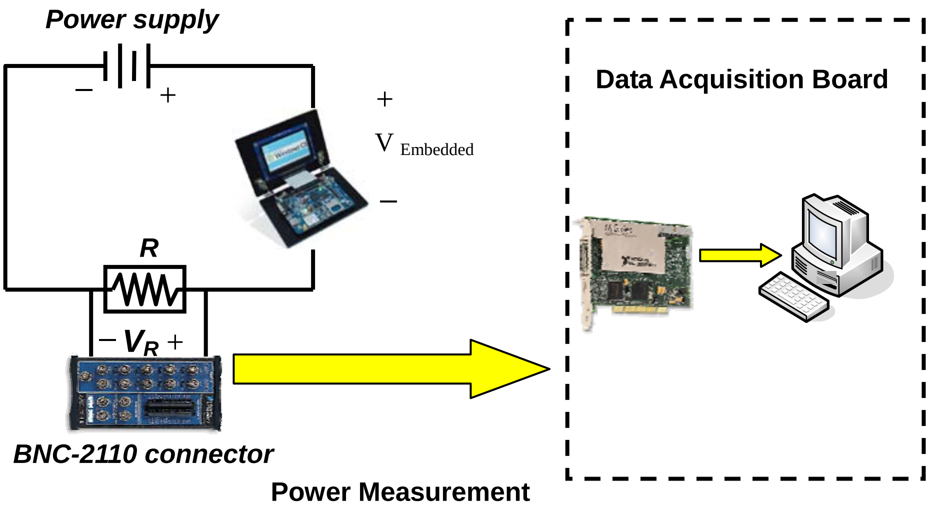

圖 二 系統架構圖

圖二為系統架構圖。我們將嵌入式系統接上外部電源，再串接一個電阻。由電阻上的電位差，可得流經嵌入式裝置的電流，再由電力訊號轉換器將這些訊號轉換成擷取裝置可讀的訊號。最後將擷取裝置所擷取到的訊號傳至電腦中的分析軟體加以記錄與分析。

第五章 結果與討論

We measure energy consumption of various audio tracks encoded by AC3, MP2, MP3, MPC, OGG, and WMA playing back on the embedded system. Based on the experimental results, we have the following observations:

(1) Effects on energy consumption due to music genres:

We choose four music genres: R&B, rap, rock, and instrumental. Averagely, audio tracks of various music genres consume similar amount of electricity. It is a good result since it would be impossible to ask mobile device users to listen to specific music genre all the time.

(2) Effects on energy consumption due to codecs:

We choose six popular codecs: AC3, MP2, MP3, MPC, OGG, WMA. The OGG files consume the most energy and the MP2 files consume the least. So, the MP2 file format is recommended to encode audio tracks to replay on mobile devices for best energy efficiency.

(3) Effects on energy consumption due to headers:

In our experiments, MP2 files are encoded with different headers: MP2-1 with AVI header, MP2-2 with MP2 header, and MP2-3 with MPG header. The experimental results show that header types have little effect on energy consumption.

(4) Effects on energy consumption due to bit rates:

Higher bit rates results in more energy consumption. But, the growth rate of energy consumption when the bit rate is doubled is low. It is advisable to encode audio tracks in high enough bit rates to have satisfactory sound quality.

(5) Effects on energy consumption due to sample rates:

Higher sample rates result in much more energy consumption than do higher bit rates. The growth rate of energy consumption when the sample rate is doubled is relatively high. It is not advisable to encode audio tracks with sample rates higher than 44,100 Hz to play back on embedded systems.

In order to have audio tracks of higher fidelity, we can encode audio tracks with higher bit rates or sample rates. From observations (4) and (5), an energy-efficient policy is to increase the bit rate but keep or lower the sample rate. So, we suggest the users of embedded systems to encode audio tracks with higher bit rates and the same or lower sample rates. This strategy normally results in better sound quality and higher energy efficiency on embedded systems.

第六章 計畫成果自評

本研究計畫針對不同類型的多媒體音訊與視訊，藉由不同的編碼選擇做編碼後，分析其在嵌入式裝置播放時，電力的效能表現。由實測的電力分析，對嵌入式裝置使用者，如何最佳化使用嵌入式裝置來播放多媒體影音，提供建議。

實驗結果得知使用者可以藉由不同的編碼選擇，得到適合的音訊與視訊，並以節能的方式播放，以延長嵌入式裝置上電池有限的電力時間，進而達成節能減碳的目標。

透過一年來計畫的執行，總共對下列三篇期刊論文，以及五篇會議論文的發表有所資助。感謝國科會經費的幫助，方有如此良好的成果。我們亦會更加多方研究思考，以提出更具有發展性的計畫。

三篇期刊論文：

Chu-Hsing Lin, Jung-Chun Liu, Chun-Wei Liao, “Energy analysis of multimedia video decoding on mobile handheld devices,” Computer Standards & Interfaces 32(1-2): 10-17 (2010) (SCI)

Chu-Hsing Lin, Jung-Chun Liu, and Chien-Ting Kuo, “Analysis of Priority Queue-Based Scheme to Alleviate Malicious Flows from Distributed DoS Attacks,” International Journal of Future Generation Communication and Networking, (IJFGCN Vol.3 No.2 June 2010) (EI)

Jung-Chun Liu, Chao-Tung Yang, Chu-Hsing Lin, Tsu-Fen Han, Wei-Cheng Hsu, and Ching-Ru Chen, “Design and Implementation of a Cloud Computing Portal for G-BLAST,” Journal of Computers, Vol. 21, No. 1 pp.17-24

五篇會議論文

Wei-Cheng Hsu, Chu-Hsing Lin , and Jung-Chun Liu, “An Embedded Firewall System and Its Security,” National Symposium on Telecommunications, 2009 (NST 2009), Kaohsiung, Taiwan, December 11-12, 2009.

Chu-Hsing Lin, Jung-Chun Liu, Chien-Ting Kuo, and Chi Lo, “Analysis of Priority Queue-Based Scheme to Alleviate Malicious Flows from Distributed DoS Attacks,” The 2009 International Conference on Future Generation Communication and Networking (FGCN2009), Jeju Island, Korea, December 10-12, 2009.LNCS/CCIS 56, pp. 301-307. (Springer-Verlag LNCS/CCIS, EI)

Chu-Hsing Lin, Chen-Yu Lee, Jung-Chun Liu and Hao-Tian Zuo, “Investigations of Factors Affecting the Genetic Algorithm for Shortest Driving Time,” The International Conference of Soft Computing and Pattern Recognition (SoCPaR 2009), Malacca, Malaysia, December 4-7, 2009. (EI)

Chu-Hsing Lin, and Chen-Yu Lee, “Modified Autonomous Key Management Scheme with Reduced Communication/Computation Costs in MANET,” The 4th International Workshop on Intelligent, Mobile and Internet Services in Ubiquitous Computing (IMIS 2010, Poland, February 15-18, 2010. (EI)

Chu-Hsing Lin, Jung-Chung Liu, Wei-Cheng Hsu, Hsing-Weng Wang, Wei-Chih Lin, and Jian-Wei Li, “Tampering Detection and Recovery Using Dual Watermarks and Cyclic Redundancy Checks,” The 2nd International Conference on Advanced Communication and Networking (ACN2010), Miyazaki, Japan, June 23-25, 2010. (EI)

參考文獻

[1]. W. Ashmawi, R. Guerin, S. Wolf, and M. Pinson, “On the impact of policing and rate guarantees in DiffServ networks: A video streaming application perspective,” Proceedings of the 2001 conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, California, United States, Aug. 2001, pp. 83-95.

[2]. K. Brandenburg and G. Stoll, “ISO-MPEG-1 Audio: A Generic Standard for coding of High-Quality Digital Audio,” J. Audio Eng. Soc., vol. 42, pp.780-792, Oct. 1994.

[3]. K. Brandenburg, G. Stoll: ISO-MPEG-1 Audio: A Generic Standard for Coding of High Quality Digital Audio “Collected Papers on Digital Audio Bit-Rate Reduction (Gilchrist and Grewin), AES, 1996.

[4]. G. Cote, B. Erol, M. Gallant, F. Kossentini, “H.263+: Video Coding at Low Bit Rates,” IEEE Trans. on Circuits and Systems for Video Technology, Nov. 1998, pp. 849-866.

[5]. Edler, B.; Purnhagen, H., “Parametric audio coding,” Signal Processing Proceedings, 2000. WCCC-ICSP 2000. 5th International Conference onVolume 1, 21-25 Aug. 2000 pp.21 – 24.

[6]. M. L. Higa, D. M. Tawy, S. M. Lord, “An introduction to LabVIEW exercise for an electronics class,” The 32nd ASEE/IEEE Frontiers in Education Conference, Boston, MA, Volume 1, 6-9 Nov. 2002 pp.T1D-13 - T1D-16 vol.1.

[7]. S.-T. Hsiang and J. W. Woods, “Embedded video coding using invertible motion compensated 3-D subband/wavelet filter bank,” Signal Processing: Image Communications 16, pp. 705–724, May 2001.

[8]. Holt, A.; Huang, C.-Y.; Monk, J., “Performance analysis of mobile agents,” Communications, IET Volume 1, Issue 3, June 2007 pp.532 – 538.

[9]. Shih-Way Huang, Tsung-Han Tsai, Liang-Gee Chen, “A low complexity design of psycho-acoustic model for MPEG-2/4 advanced audio coding, ” IEEE Transactions on

Consumer Electronics, Vol 50,pp. 1209 – 1217, Nov. 2004.

[10]. Ramkumar Jayaseelan Tulika Mitra Xianfeng Li, "Estimating the Worst-Case Energy Consumption of Embedded Software," In Proc. of IEEE RTAS 2006, The 12th Real-Time and Embedded Technology and Applications Symposium, April 2006, San Jose, California, USA

[11]. R. Karri and P. Mishra, "Minimizing Energy Consumption of Secure Wireless Session with QoS Constraints," Proc. Int'l Conf. Comm., pp. 2053-2057, May 2002.

[12]. A. Kejariwal, S. Gupta, A. Nicolau, N. Dutt, R. Gupta, "Energy efficient watermarking on mobile devices using proxy-based partitioning," IEEE Trans. on Very Large Scale Integration (VLSI) Systems, June 2006, pp. 625-636.

[13]. K. Lahiri, A. Raghunathan, S. Dey, and D. Panigrahi, "Battery driven system design: a new frontier in low power design," In Proc. ASPDAC/VLSI Design 2002, Bangalore, India, January 2002, pp. 261-267.

[14]. Lambert, P., De Neve, W., De Neve, P., Moerman, I., Demeester, P., Van de Walle, R., "Rate-distortion performance of H.264/AVC compared to state-of-the-art video codecs," Circuits and Systems for Video Technology, IEEE Transactions on Volume 16, Issue 1, Jan. 2006 pp.134 – 140.

[15]. Chu-Hsing Lin, Jung-Chun Liu, Chun-Wei Liao, "Energy Analysis of Multimedia Video Decoding on Mobile Handheld Devices," 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE07), Seoul, Korea, April 26-28, 2007, pp.120 – 125.

[16]. Chu-Hsing Lin, Jung-Chun Liu, Chun-Wei Liao, "Energy Consumption Analysis of Audio Applications on Mobile Handheld Devices," TENCON 2007 – IEEE Region 10 Conference, Taipei, October 31, 2007, pp.124-125.

[17]. Robert N. Mayo, Parthasarathy Ranganathan "Energy Consumption in Mobile Devices: Why Future Systems Need Requirements-Aware Energy Scale-Down," HP Labs technical reports, Available on http://www.hpl.hp.com/techreports/2003/HPL-2003-167.pdf

[18]. N. R. Potlapally, S. R., A. Raghunathan, and N. K. Jha, "Analyzing the energy

consumption of security protocols," In Proceedings of the 2003 International Symposium on Low Power Electronics and Design, Seoul, Korea, 2003, pp. 30–35.

[19]. N. R. Potlapally, S. R., A. Raghunathan, and N. K. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols," IEEE Transactions on Mobile Computing, Issue 2, Volume 5, Feb. 2006, pp.128 – 143.

[20]. Schierl, T.; Stockhammer, T.; Wiegand, T. "Mobile Video Transmission Using Scalable Video Coding," Circuits and Systems for Video Technology, IEEE Transactions on Volume 17, Issue 9, Sept. 2007 pp.1204 – 1217.

[21]. T. K. Tan, A. Raghunathan, and N. K. Jha., "A simulation framework for energy-consumption analysis of OS-driven embedded applications," IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems, Sept. 2003, pp. 1284-1294.

[22]. US Department of Commerce, The Emerging Digital Economy II, http://www.esa.doc.gov/508/esa/TheEmergingDigitalEconomyII.htm, 1999.

[23]. S. Vernon, "Design and Implementation of AC-3 Decoders," IEEE Transactions on Consumer Electronics, Vol. 41, No. 3. Aug. 1995, pp.754-759.

[24]. T. Wiegand, G. Sullivan, and A. Luthra, "Draft ITU-T Recommendation and Final Draft International Standard of Joint Video Specification (ITU-T Rec. H.264 — ISO/IEC 14496-10 AVC)," JVTdocument JVT-G050r1, Geneva, Switzerland, Joint Video Team of ISO/IEC JTC1/SC29/WG11 and ITU-T SG16/Q.6, May 2003.

[25]. T. Wiegand, G. J. Sullivan, G. Bjøntegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," IEEE Trans. Circuits Syst. Video Technol. 13, pp. 560–576, July 2003.

[26]. T. Wiegand, H. Schwarz, A. Joch, F. Kossentini, and G. J. Sullivan, "Rate-constrained coder control and comparison of video coding standards," IEEE Trans. Circuits Syst. Video Technol. 13, pp. 688–703, July 2003.

[27]. Zhao, Xiaoli; Tao, Pin; Yang, Shiqiang "The Analysis of Offloading H.264 Video Encoder on Mobile Devices for Energy Saving" Systems, Man and Cybernetics, 2006.

ICSMC '06. IEEE International Conference on Volume 5, 8-11 Oct. 2006 pp.4315 – 4320.

[28]. “Applications and Requirements for Scalable Video Coding,” MPEG-document ISO/IECJTC1/SC29/WG11 N5540, Moving Picture Experts Group (MPEG), Mar. 2003. Available on http://www.chiariglione.org/mpeg/working_documents.

[29]. DivXNetworks, Inc. Available on http://www.divx.com/divx/

[30]. International Electrotechnical Commission, IEC. Available on http://www.iec.ch/

[31]. International Telecommunication Union, ITU. http://www.itu.int/

[32]. MPEG Industry Forum. http://www4if.org/.m Overview of the MPEG-4 Standard. Available on http://www.chiariglione.org/mpeg/standards/mpeg-4/mpeg-4.htm

[33]. Overview of the MPEG-4 Standard. Available on http://www.chiariglione.org/mpeg/standards/mpeg-4/mpeg-4.htm

[34]. Windows Media Audio Codecs web site. Available on http://www.microsoft.com/windows/windowsmedia/forpros/codecs/audio.aspx

[35]. XIPH. Ogg Vorbis Web Site. [Online]. Availableon http://www.xiph.org/vorbis/.

[36]. XviD Software Package [Online]. Available on http://www.xvid.org/

[37] M. L. Higa, D. M. Tawy, S. M. Lord, “An introduction to LabVIEW exercise for an electronics class” The 32nd ASEE/IEEE Frontiers in Education Conference, Boston, MA, Volume 1, 6-9 Nov. 2002 pp.T1D-13 - T1D-16 vol.1

[38] K.-M. Ho, W.-F. Poon, and K.-T. Lo, “Performance Study of Large-Scale Video Streaming Services in Highly Heterogeneous Environment” IEEE Trans. on Broadcasting, vol. 53, no. 4, Dec. 2007

[39] K.M. Ho, W.F. Poon and K.T. Lo, “Investigating the Performance of Hierarchical Video-on-Demand System in Heterogeneous Environment” The 2nd international conference on ubiquitous information Management and Communication, Jan. 2008

[40] HD-DVD Promotion Group. [Online]. Available: http://www.hddvdprg.com/

[41] Blu-ray Disc Association. [Online]. Available: http://www.blu-raydisc.com/

[42] Applications and Requirements for Scalable Video Coding, MPEG-document ISO/IEC JTC1/SC29/WG11 N5540, Mar. 2003.

行政院國家科學委員補助國內專家學者出席國際學術會議報告

<table>
<tr><td>報 告 人
姓 名</td><td>林祝興</td><td>服務機關
及職稱</td><td>東海大學資訊工程學系
教授</td></tr>
<tr><td>時間

會議地點</td><td>99年2月15日～2月18日
波蘭克拉科夫
Andrzej Frycz Modrzewski
Cracow College</td><td>本會核定
補助文號</td><td>NSC98-2221-E-029-021</td></tr>
<tr><td>會 議 名 稱</td><td colspan="3">(中文) 第四屆國際智能、行動與網際網路服務無處不在計算會議
(英文) The 4th International Workshop on Intelligent, Mobile and Internet Services in Ubiquitous Computing (IMIS 2010, in conjunction with CISIS 2010)</td></tr>
<tr><td>發表論文題目</td><td colspan="3">(英文) Modified Autonomous Key Management Scheme with Reduced Communication/Computation Costs in MANET</td></tr>
<tr><td colspan="4">報告內容：

一、參加會議過程

二、與會心得

三、考察參觀活動

四、建議

五、攜回資料名稱及內容

六、其他</td></tr>
</table>

第四屆國際智能、行動與網際網路服務無處不在計算會議

林祝興

東海大學資訊工程學系

一、參加會議過程

2010 年 2 月 11 日搭乘飛機從台灣桃園國際機場出發，途中在奧地利維也納國際機場進行轉機，最後到達波蘭克拉科國際機場，總共經過大約十七小時的飛行及兩小時的轉機時間。到達後，搭乘大會安排的巴士前往本次與會的地點「克拉科學院 (Andrzej Frycz Modrzewski Cracow College)」。

IMIS 2010 今年是第四次舉辦了，其會議內容探討的範圍相當廣泛，主辦的波蘭克拉科學院 (Andrzej Frycz Modrzewski Cracow College) 表現的也可圈可點。本人很榮幸在大會的第二天擔任 Security and Privacy in Mobile Ubiquitous Computing (W-IMIS-2010-S6) 的會議主持人。

在本次的大會中共安排了四場演講，從每天早上九點到十點半，使本人獲益良多。此外，大會將接受的論文分成十二個 Session（一天三場），每個 Session 分成九個房間同時舉行，每個房間安排大約 3 到 4 篇論文報告。聆聽其他人的研究成果，使我有種茅塞頓開的感覺，讓我的研究視野更加廣闊。

二、與會心得

在這次的 IMIS2010 研討會中，本人所發表的學術論文，所屬的議題為 Security and Privacy in Mobile Ubiquitous Computing (W-IMIS-2010-S5)，而論文的題目為 Modified Autonomous Key Management Scheme with Reduced Communication/Computation Costs in MANET。報告中主持人和與會者提出的問題讓本人思考更加深邃，挖掘出不少之前未注意到的地方，會後的討論也讓本人跟各國的學者與研究人員有更進一步的交流。

三、考察參觀活動

波蘭共和國（波蘭文：Rzeczpospolita Polska），簡稱波蘭，是北面濱臨波羅的海的中歐國家，西面與德國接壤，南部與捷克和斯洛伐克為鄰，烏克蘭和白俄羅斯在東，東北部和立陶宛及俄羅斯外飛地接壤。波蘭重要的地理位置以及地形導致歷史上連年的戰火紛爭，幾個世紀以來波蘭的版圖也一再更改。波蘭是歐洲聯盟，北約，聯合國，經濟合作與發展組織和世貿組織的成員。

波蘭絕大部分地區位於東歐平原，平均海拔 173 米。波蘭一詞源於斯拉夫語 Polanie，意思是居住在平原上的人。歷史上波蘭也因此無險可守，多次被列強瓜分。僅南部地勢有起伏，有喀爾巴阡山脈和蘇台德山脈等，最高點海拔 2,499 米。主要河流有維斯瓦河（Wisła）和奧得河。波蘭境內還有冰蝕作用形成的 9,300 多個湖泊，大部分集中在北部，最大湖泊為希尼亞爾德維湖。波蘭屬海洋性向大陸性氣候過渡的溫帶大陸性濕潤氣候，闊葉林發育，冬天寒冷、多雲、多降雨，夏天潮濕、多雷陣雨。

克拉科夫（波蘭語：Kraków；全稱克拉科夫皇家首都，波蘭語：Królewskie Stołeczne Miasto

Kraków）是小波蘭省的首府，波蘭的舊都。位於維斯杜拉河畔，克拉科夫—琴斯托霍瓦高地鄰近大城市。教宗若望保祿二世在 1963 年至 1978 年擔任當地的大主教。當地的機場在 1995 年以其命名。1978 年被列入世界文化遺產名錄。

克拉科夫老城 (Stare Miasto) 是波蘭城市克拉科夫市中心的歷史區域。這是波蘭最經典的老城，因為許多世紀以來，克拉科夫都是波蘭的京城，直到 1596 年，齊格蒙特三世才將他的宮廷遷往華沙。1978 年，克拉科夫歷史中心被聯合國教科文組織列為世界遺產。中世紀的克拉科夫周圍環繞著 3 公里長的城牆，有 46 個塔樓，7 個主要入口，修建花費了 2 個世紀的時間。

位於老城中心的中央集市廣場，是歐洲最大的中世紀城市廣場。在其附近，有許多歷史地標，例如聖母聖殿 (Kościół Mariacki)、聖沃伊切赫教堂 (St. Wojciech)、聖巴巴拉教堂。廣場周圍是聯排住宅 (kamienice) 和貴族府邸，文藝復興風格的紡織會館，克拉科夫國立美術館，以及市政廳鐘樓 (Wieża ratuszowa)。

波蘭國王的加冕遊行路線皇家之路縱貫整個克拉科夫老城。皇家之路開始於原來北側城牆以外的中世紀郊區 Kleparz，聖弗洛里亞諾教堂，經過建於 1499 年的哥德式的中世紀外堡 (Barbakan)，穿過弗洛里亞門進入老城。然後沿著弗洛里亞街，穿過中央集市廣場，再經過 Grodzka 街到達瓦維爾山，這是過去波蘭王室駐地，俯瞰著維斯瓦河。在 19 世紀，大部分城牆被拆除，護城河被填平，改為環城綠帶，稱為普朗蒂公園。

四、建議

The 4th International Workshop on Intelligent, Mobile and Internet Services in Ubiquitous Computing (IMIS 2010) 國際研討會，是具有前瞻性的國際會議，其中討論了許多 Ubiquitous Computing 的技術和相關應用趨勢，展現出各位學者不同的創新觀念與建議，透過與各學著的學習與討論，讓與會的人員都深感會益良多。希望未來我國能不斷地爭取類似此種國際研討會的主辦權，相信這將對我國的學術活動與國際地位有正面的意義與幫助，並且可以提升我國在軟體技術分面的競爭力。

五、攜回資料名稱及內容

- CISIS 2010 The Fourth International Conference on Complex, Intelligent and Software Intensive Systems 會議行程一本
- CISIS 2010 The Fourth International Conference on Complex, Intelligent and Software Intensive Systems 論文集光碟一片

六、其他

本人參加這次在波蘭克拉科舉辦的 The 4th International Workshop on Intelligent, Mobile and Internet Services in Ubiquitous Computing (IMIS 2010) 國際研討會感覺獲益良多，除了聽取許多外國學者的研究成果之外，在與國外學者的交流中也大大提升了英語的聽、說能力。此外，也順道參觀了古色古香的克拉科夫老城 (Stare Miasto) 並享用當地的特色美食，為此嚴肅的學術研討會增添了一絲輕鬆的氣息。最後本人特別感謝行政院國家科學委員會的補助經費，使本人有機會到克拉科夫參與此次盛會。未來，希望國家能讓更多的人有機會能參與類似的研討會，進而提升校內學者的學術涵養與實務能力。

Dear participant,

We are delighted to welcome you to Krakow and are looking forward to exciting and productive conference talks. This note contains essential information you should be aware of.

Oral presentations

If you have been selected to give an oral presentation, we kindly ask you meet with the session chair 15 minutes before the beginning of your session in your assigned lecture hall. Technical assistance will be available in the lecture hall.

Please also be aware that we have instructed the chair persons to stick to the time schedule so please assist them by being on time.

Announcements

Important information (e.g. program changes) is announced on the boards at the registration desk. We kindly ask you to have a look at these boards every time you walk by the registration desk. Further, the most up-to-date version of the program can be found at the conferences' web pages.

Internet access

On each floor, Internet Hotspots are available. The SSID is KA_Hot_Spot and they require no password. Please be aware that this connection uses no encryption. Thus, if you have to transmit confidential information, use adequate techniques (e.g. VPN).

If the capacity of the Hotspots are not sufficient, there are two PC rooms located on the 1st upper floor of the building A. The rooms are labeled as "Internet Rooms".

Food / Refreshments

Throughout the conference days, refreshments will be served during the coffee breaks in the 1st lower floor of building A. Lunch will be served at the University Mensa (building C). Please follow the signs or ask the conference staff at the Registration Desk. You can find the vouchers for each day within the envelope.

Social Events

Please join us for the Welcome Reception on the first evening starting on Monday 15th at 18:30 in the University Mensa (building C). At the Welcome Reception drinks, hot and cold dishes will be served. You can find the voucher within the envelope. On Tuesday, February 16th, you are invited to attend our Conference dinner. The conference dinner will take place at Tomaszowice Manor. The Tomaszowice Manor is an historical 19th century Manor and Park complex located at the north gateway to Kraków. A bus transfer to the conference dinner location will be provided. Busses will depart at 18.30 from the conference venue. You can find the voucher within the envelope.

Abstract leaflet

A leaflet containing all papers' abstracts is available at the conference web pages:

- http://www.ares-conference.eu/abstracts/Abstracts-Ares.pdf
- http://www.ares-conference.eu/abstracts/Abstracts-Cisis.pdf

Username: abstracts2010 Password: ares2010cisis

Assistance

If you require any assistance, please contact the conference staff at the reception desk. We will be happy to assist you.

We wish you inspiring and pleasant conference days and are looking forward to your contribution.

PROGRAM GUIDE

ARES 2010
The Fifth International Conference on Availability, Reliability and Security

CISIS 2010
The Fourth International Conference on Complex, Intelligent and Software Intensive Systems

February 15th – 18th 2010

Krakow, Poland

Overview

Monday 15th 2010

		CISIS Conference & Workshops						ARES Conference & Workshop		
		ROOM 1	ROOM 2	ROOM 3	ROOM 4	ROOM 5	ROOM 6	ROOM 7	ROOM 8	ROOM 9
Slot	Time	15.FEB.10								
Registration	8:00-18:00	REGISTRATION								
Session 1	09:00-10:30	Opening Keynote								
Coffee Break	*10:30-11:00*	*Coffee Break*								
Session 2	11:00-12:30	CISIS-S1	CISIS-S2	W-IIHCI-S1	W-SENSE-COCOSS-S1	W-MuCoCos-S1	W-IMIS-S1	WSDF-1	ARES-F1	FARES-S1
Lunch	*12:30-14:00*	*LUNCH*								
Session 3	14:00-15:30	CISIS-S3	CISIS-S4	W-IIHCI-S2	W-SENSE-COCOSS-S2	W-MuCoCos-S2	W-IMIS-S2	WSDF-2	ARES-F2	FARES-S2
Coffee Break	*15:30-16:00*	*Coffee Break*								
Session 4	16:00-18:00	CISIS-S5	CISIS-S6			W-MuCoCos-S3	W-IMIS-S3	WSDF-3	ARES-F3	FARES-S3
Social Event	*Evening*	*Welcome Party*								

Tuesday 16th 2010

		CISIS Conference & Workshops						ARES Conference & Workshop			
		ROOM 1	ROOM 2	ROOM 3	ROOM 4	ROOM 5	ROOM 6	ROOM 7	ROOM 8	ROOM 9	ROOM 10
Slot	Time	16.FEB.10									
Registration	8:00-18:00	REGISTRATION									
Session 1	09:00-10:30	Keynote									
Coffee Break	*10:30-11:00*	*Coffee Break*									
Session 2	11:00-12:30	CISIS-S7	CISIS-S8	W-OnAv-S1	W-VENOA-S1	W-IIBM-S1	W-IMIS-S4	WSDF-4	ARES-F4	FARES-S4	SECSE-1
Lunch	*12:30-14:00*	*LUNCH*									
Session 3	14:00-15:30	CISIS-S9	CISIS-S10	W-OnAv-S2	W-VENOA-S2	W-IIBM-S2	W-IMIS-S5			FARES-S5	SECSE-2
Coffee Break	*15:30-16:00*	*Coffee Break*									
Session 4	16:00-18:00	CISIS-S11	CISIS-S12	W-OnAv-S3	W-VENOA-S3	W-3PGIC-S1	W-IMIS-S6		ARES-F6	FARES-S6	SECSE-3
Social Event	*Evening*	*Conference Dinner*									

W-VENOA-2010-S2: Multimedia and Web

Session Chair: **Hiroaki Nishino, Oita University, Japan**

1. A Study of Haptic Interaction for Image Edition Tools
   Tsuneo Kagawa, Tatsuya Shimamoto, Hiroaki Nishino, and Kouichi Utsumiya
2. A Legwork Mechanism to Assist a Suggesting Module in Finding Worthy Webpages in Search Results
   Keizo Sato, Akira Nakanishi, Makoto Nakashima, and Tetsuro Ito
3. E-Government Websites Evaluation Using Correspondence Analysis
   Dahlan Nariman

W-IIBM-2010-S2: IIBM-2

Session Chair: **Oliver Ray, University of Bristol, UK**

1. MicroRNA Target Prediction and Exploration through Candidate Binding Sites Generation
   Paula Helena Reyes-Herrera, Andrea Acquaviva, Elisa Ficarra, and Enrico Macii
2. A Comprehensive System for Identifying Internal Repeat Substructures of Proteins
   Hua-Ying Kao, Tsang-Huang Shih, Tun-Wen Pai, Ming-Da Lu, and Hui-Huang Hsu
3. Gene Ontology Rewritten for Computing Gene Functional Similarity
   Alessia Visconti, Francesca Cordero, Marco Botta, and Raffaele A. Calogero
4. An Automated Tool for Scoring Biomedical Terms Correlation Based on Semantic Analysis
   F. Abate, Elisa Ficarra, Andrea Acquaviva, and Enrico Macii

W-IMIS-2010-S5:IMIS-SS1a:
Security and Privacy in Mobile Ubiquitous Computing

Session Chair: **Jinn-Ke Jan, Chung Hsing University, Taiwan**

1. Improvement of an Efficient ID-Based RSA Multisignature
   Fuw-Yi Yang, Jeng-Hung Lo, and Cai-Ming Liao
2. Modified Autonomous Key Management Scheme with Reduced Communication/Computation Costs in MANET
   Chu-Hsing Lin and Chen-Yu Lee
3. A New Noise Mingling Approach to Protect the Authentication Password
   Kangbin Yim

W-3PGIC-2010-S1: Middleware, Services and Programming Models

Session Chair: **Sabri Pllana, Vienna University, Austria**

1. Shared Data Grid Programming Improvements Using Specialized Objects
   Dacian Tudor, Georgiana Macariu, Wolfgang Schreiner, and Vladimir Cretu
2. A Web Service Discovery Method Based on Tag
   Zhaoyun Ding, Deng Lei, Jia Yan, Zhou Bin, and An Lun
3. Grid and P2P Middleware for Scientific Computing Systems
   Fatos Xhafa, Sabri Pllana, and Leonard Barolli
4. Next Generation Applications Mobility Management with SOA - A Scenario-Based Analysis
   Natalia Kryvinska, Christine Strauss, and Lukas Auer

W-IMIS-2010-S6: IMIS-SS1b:
Security and Privacy in Mobile Ubiquitous Computing

Session Chair: **Chu-Hsing Lin, Tunghai University, Taiwan**

1. Authenticated Group Key Agreement Protocol for Unbalanced Wireless Mobile Networks
   Chung-Fu Lu, Tzong-Chen Wu, and Tzay-Farn Shih
2. Using Mobile Device to Design a Secure Transaction
   Chin-Ling Chen, Jinn-Ke Jan, and Chih-Feng Chien
3. An Extensible Framework for Efficient Secure SMS
   Alfredo De Santis, Aniello Castiglione, Giuseppe Cattaneo, Maurizio Cembalo, FabioPetagna, and Umberto Ferraro Petrillo


14-02-10 11:38


ARES&CISIS
CONFERENCE
15-02-10 12:04


KRAKOWSKA AKADEMIA
im. Andrzeja Frycza Modrzewskiego
16-02-10 12:50


KRAKOWSKA AKADEMIA
im. Andrzeja Frycza Modrzewskiego
16-02-10 14:06


KRAKOWSKA AKADEMIA
im. Andrzeja Frycza Modrzewskiego
16-02-10 14:07


16-02-10 19:55

2010 International Conference on Complex, Intelligent and Software Intensive Systems

Modified Autonomous Key Management Scheme with Reduced Communication/Computation Costs in MANET

Chu-Hsing Lin[1] and Chen-Yu Lee[2]

[1] Department of Computer Science, Tunghai University, 181, Section 3, Taichung Port Road, Taichung 40704, TAIWAN
[2] Department of Computer Science, National Chiao Tung University, 1001 Ta-Hsueh Road, HsinChu, 30050, TAIWAN

The growing applications of Mobile Ad hoc Network (MANET) has made the security issue increasingly more important. B. Zhu et al. proposes a key management scheme using Shamir's secret sharing scheme to construct an Autonomous Key Management (AKM) hierarchy structure. However, Shamir's secret sharing in AKM to control key hierarchy needs larger message transmission costs. In this paper, we modify the secret sharing scheme and apply it to AKM for reducing communication and computation cost.

***Index Terms*—Mobile Ad hoc Network, Key Management, Autonomous Key Management**

I. Introduction

KEY MANAGEMENT within the Mobile Ad hoc Network (MANET) security issue is the only thing that cannot be ignored. Since 1999, increasingly more researchers have dedicated themselves to this field. Some schemes are suitable under limited nodes and are inefficient, insecure, or unreliable when the nodes increase [2-8]. The nodes furthermore join the MANET and leave later normally. Thus, the key management scheme in MANET needs to be dynamic. B. Zhu et al. proposes a key management scheme [1] using secret sharing scheme [9-14] to construct an AKM hierarchy structure. The scheme needs no central party to control the key structure, and each node cooperates to create virtual nodes in building the key hierarchy.

A supposed message of 2048 bits in size would make computing or calculating AKM communication cost difficult. Thus, this research work modifies the secret sharing scheme. The next section briefly introduces Shamir's secret sharing scheme and the AKM key management. Section 3 describes modified AKM which reduces share size with the same security properties. Section 4 discusses the performance improvement compared with the original AKM and it indicates the improved performance of communication and computation cost reduced to 1/t of the original AKM.

II. Related Work

Shamir's Secret Sharing Scheme

Let t, n be positive integers, $t \le n$. Shamir proposed a (t, n)-threshold scheme in 1979 [9]. His scheme is a method of sharing a key K among a set of n participants, in such a way that any t participants can compute the value of key K, but no group of t-1 participants can do so.

1) The Shamir (t, n)-threshold scheme in Z_p

D (the dealer) chooses n distinct, nonzero elements of Z_p, denoted x_i, $1 \le i \le n$, where $p > n$ is a large prime. D gives the values x_i to P_i, and each value x_i is public.

2) Share Distribution

(1) Suppose D wants to share a key $K \in Z_p$. D secretly chooses (independently at random) t-1 elements of Z_p, $a_1, \ldots, a_{t-1}$.

(2) For $1 \le i \le n$, D computes $y_i = a(x_i)$, where

$$a(x) = K + \sum_{j=1}^{t-1} a_j x^j \bmod p$$

Thus

$$y_i = a(x_i) = K + \sum_{j=1}^{t-1} a_j (x_i^j) \bmod p$$

(3) For $1 \le i \le n$, D gives the share y_i to P_i.

3) Proactive Security

It is hard to compromise the secret key K under (t, n)-threshold scheme unless the adversary collects at least t shares. In practice, each share exists in a machine, thus the risk of the secret key being compromised depends on the security of machine. For a security concern, it is necessary to update each share for a period of time. A proactive threshold scheme allows users to refresh shares without disclosing the secret key.

(a) Let

$$y_i = a(x_i) = K + \sum_{j=1}^{t-1} a_j (x_i^j) \bmod p$$

be the original share of key K for P_i.

(b) The dealer D computes

$$y'_i = a(x'_i) = \sum_{j=1}^{t-1} a_j (x'^j_i) \bmod p$$

(c) For $1 \le i \le n$, D gives the share y'_i to P_i.

(d) For $1 \le i \le n$, P_i computes $(y_i + y'_i)$ as new share.

Autonomous Key Management (AKM)

Autonomous key management (AKM) is proposed for the Mobile Ad hoc Network (MANET) with a large number of nodes [1], based on a hierarchical structure to provide flexibility and adaptivity. Every leaf node in the logical tree structure is a real ad hoc device and the others are virtual nodes. The root node holds the global secret key, and AKM distributes key shares to its children recursively from the root down to the leaves using Shamir's secret sharing scheme.

Every node has to store its own public key pair and its

978-0-7695-3967-6/10 $26.00 © 2010 IEEE
DOI 10.1109/CISIS.2010.70

parent node secret share except the AKM root node. The secret share each virtual branch node holds is as the secret key, and the public key can be generated using any asymmetric cryptographic scheme, such as RSA. Additionally, every real node has its PKI key pair before joining AKM.

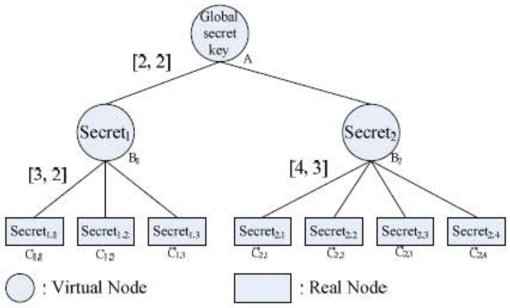

Fig. 1 Example of AKM

A tree with node A as its root is called region A. AKM includes six node-based /region-based operations from node joining, region partitioning, to node leaving. AKM runs dynamically with continuous node joining/leaves. The detail will be described in Section 4.

III. MODIFIED AKM

This section modifies the secret sharing of AKM. AKM runs dynamically in six node-based/region-based operations. The six operations are update, join, leave, merge, partition, and expansion.

We define the rules below the following,

(a) All leaves in the hierarchy of AKM are Real nodes. Each real node i has its own secret key SK_i, and $PK_i = g^{SK_i} \bmod p$.

(b) The non-leaf nodes are Virtual nodes, and their secret keys are generated directly/indirectly from real nodes through some region-based operations.

(c) A tree with node A as root is called $Region_A$. For example, region A has virtual nodes B_1, B_2, and real nodes $C_{1,1}$, $C_{1,2}$, $C_{1,3}$, $C_{2,1}$, $C_{2,2}$, $C_{2,3}$, and $C_{2,4}$. The number of the nodes that know the secret of the region is Overall region size (**ORS**). Finally, we compute the Regional trust coefficient (**RTC**) --- the ratio of the threshold to ORS evaluating how secure the region is. The AKM sets a Global trust coefficient (**GTC**) as a lower bound of all the RTC.

1) Function Update

Function update prevents any intruders from compromising the secret, and the AKM updates keys periodically. First, the region with (n, t)-threshold has to select t nodes and each node is indicated as node $i \in \{1, \ldots, t\}$.

Each node i generates update share $S_{i,j}$ $(1 \le j \le n)$ of key 0. It selects random numbers x_j $(1 \le j \le n)$ and r_d $(1 \le d \le i\text{-}1)$ to compute coefficients $a_d = (r_d \mid 0)$ $(1 \le d \le t\text{-}1)$. $S_{i,j} = a(x_j) = \sum_{r=0}^{t-1} a_r (x_j)^r \pmod p$, for $1 \le j \le n$. Node i then distributes $S_{i,j}$ to node $j \in \{1, \cdots, n\}$. When node j receives the update shares distributed from other t nodes in the region, it computes a new share

$$S'_j = S_j + \sum_{i=1}^{t} S_{i,j} \pmod p$$

The previous section mentions that AKM with six-region-based functions can manage its secret sharing hierarchical structure. The operations cover all possible region changes from node joining to leaving.

2) Function Join

Function Join is used when a node i wants to join into a (t, n)-threshold region. It sends a request to node $j \in \{1, \cdots, t\}$ in the region. Receiving the request, node j checks its certificate revoking list (CRL) first. If node j accepts the request, it computes a partial share S'_j of node i:

$$S'_j = S_j l_j(i) + \Delta_j \pmod q$$

,where

$$l_j(i) = \prod_{r=1, r \ne j}^{t} \frac{ID_i - ID_r}{ID_j - ID_r} \pmod q,$$

$$\Delta_j = \sum_{r=1, r \ne j}^{t} \sigma(j-r) \cdot S_{j,r}$$

, that $S_{j,r}$ is a number which pairs of nodes $(j, r) \in \{1 \le j \le t, 1 \le r \le t\}$, and $\sigma(x) = \begin{cases} 1 & , x > 0 \\ -1 & , x < 0 \\ 0 & , \text{otherwise} \end{cases}$

After receiving all partial shares, node i generates its secret share S_i:

$$S_i = \sum_{j=1}^{t} S'_j = \sum_{j=1}^{t} S_j l_j(ID_i) + \sum_{j=1}^{t} \Delta_j \pmod q$$

3) Function Leave

Function Leave is used when a node leaves a region. Any node j removes node i from its CRL when receiving Leave request from node i or detecting the node leaves.

4) Function Merge

Function Merge is used when the number of nodes in a region is under the threshold. We simply divide the region into many parts and they join to the other region respectively.

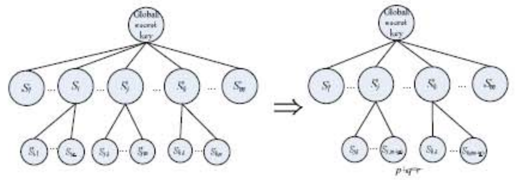

Fig. 2 Function Merge - merge S_i into S_j and S_k.

5) Function Partition

Function Partition is used when RTC of a region is under the GTC. Figure 3 shows that AKM partitions share S_i into S_i and $S_{(m+1)}$. It first selects t regions from S_1 to S_m and chooses t nodes $\{S_{j,1} \ldots S_{j,t}\}$ from each S_i region. Second, it creates a new node $S_{(m+1)}$, and joins into AKM. Furthermore, it partitions $2n$ nodes from S_i into two nodes, S_i and $S_{(m+1)}$.

We know that

$$S_i = \sum_{j=1}^{t} s_j l_j(ID_{S_i}) \pmod q$$

,where

$$l_j(ID_{S_i}) = \prod_{r=1, r \neq j}^{t} \frac{ID_{S_i} - ID_{S_r}}{ID_{S_j} - ID_{S_r}} \pmod q$$

by Lagrange interpolation. And

$$S_j = \sum_{v=1}^{t} S_{j,v} l_{j,v}(0) \pmod q$$

,where

$$l_{jv}(0) = \prod_{r=1, r \neq j}^{t} \frac{ID_{S_{j,r}}}{ID_{S_{j,r}} - ID_{S_{j,v}}} \pmod q$$

Thus

$$S_i = \sum_{j=1}^{t} \sum_{v=1}^{t} S_{j,v} l_{j,v}(0) l_j(ID_{S_i}) \pmod q$$

We also can get

$$S_{m+1} = \sum_{j=1}^{t} \sum_{v=1}^{t} S_{j,v} l_{j,v}(0) l_j(ID_{S_{m+1}}) \pmod q$$

,where

$$l_j(ID_{S_{m+1}}) = \prod_{r=1, r \neq j}^{t} \frac{ID_{S_{m+1}} - ID_{S_r}}{ID_{S_j} - ID_{S_r}} \pmod q$$

To generate each share $S_{(m+1),j}$ $(1 \leq j \leq n)$ of region $S_{(m+1)}$, $S_{(m+1),v}{}'$, where

$$S_{(m+1),v}{}' = S_{(m+1),v} l_{(m+1),v}(0) R_{(m+1)} \pmod q,$$

$$R_{(m+1)} = l_{(m+1)}(ID_{S_{m+1}}) - l_j(ID_{S_i})$$

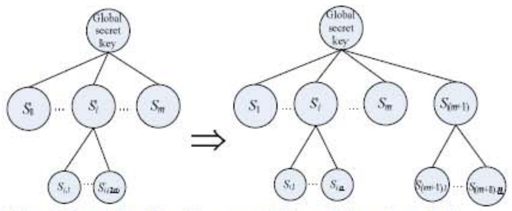

Fig. 3 Function Partition - partition S_i into S_j and $S_{(m+1)}$.

6) *Function Expansion*

Function Expansion is used when RTC of a region is under the GTC. But when the RTC is equal to GTC in all AKM regions, it has to perform expansion operation to extend the hierarchy. As in Figure 4, AKM extends region S_i from one level to two levels. It selects t nodes in region S_i, and executes function join to create a new node $S_{i,(n+1)}$. It then moves $S_{i,1}$, …, $S_{i,m}$ to be $S_{i,(n+1)}$'s children, $S_{i,(n+1),1}$, ⋯, $S_{i,(n+1),m}$ with shares $S_{i,(n+1),j}$, $1 \leq j \leq m$, that

$$S_{i,(n+1),j} = a(ID_{i,(n+1),j}) = \sum_{r=1}^{t} a_r x^r \pmod q$$

where $a_r = r_r \mid s_r$ $(1 \leq r \leq t)$, $S_{i,(n+1)} = s_t s_{t-1} \ldots s_1$, and all r_rs are the same used in region S_i. Region $S_{i,(n+1)}$ continues (n, t)-threshold as in region S_i.

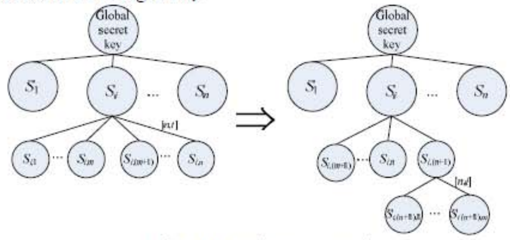

Fig. 4 Function Expansion.

The six-region-based operations form YeHLL's secret sharing scheme on MANET of AKM handle key management. The scheme does need TA (trusted authority) to start up, neither any central authorities to compute and distribute shares.

IV. Performance Analysis

This section discusses the performance improvement in two parts: communication cost and computation cost. Modified AKM inherits the AKM structure, and transmissions between each node are (update) shares. Thus the single message discussion needs to be transmitted showing significant improvement.

The length of secret key k, protected by the secret sharing scheme, must be long enough, such as 2048 bits or more for some security issues. In Shamir's secret sharing scheme, k is the constant in $a(x)$ equation. The length of all the shares $a(x_i) = \sum_{j=1}^{t-1} a_j x^j + k$, $1 \leq i \leq n$, is bounded by $|k|$. For example, if $|k|$=2048 bits long, the length of each share is at least 2048 bits. However, modified secret sharing scheme reduces share length to 1/t without security loss. The secret key is divided in each coefficient $a_j = r_k \mid k_j$, and $k = k_1 k_2 \ldots k_t$ with the length $|a(x_i)|$ as $1/t$ of $|k|$ on appropriate prime number p. Therefore, the modified MANET communication cost can be reduced to $1/t$.

Table. 1 Message length comparison

	Message (share) length size
AKM	$\lvert y_i \rvert = \lvert k \rvert \leq \lvert p \rvert$
Modified AKM	$\lvert y_i \rvert = \frac{\lvert k \rvert}{t} \leq \lvert k \rvert \leq \lvert p \rvert$

Computation cost on the MANET environment is a very important issue. Certain mobile ad-hoc devices have restricted power, and cannot support jobs requiring heavy computation cost. Our improvement also influences computation cost. Finding that the critical mathematical operation is module multiplication (/division) in all operations is easy, depending on operand length. Almost all operands in modified AKM reduce, resulting from each modified AKM share as $1/t$ faster than AKM. Furthermore, the computation cost of all operations can be reduced to $1/t$.

Table. 2 Operand length comparison

	operand length size
AKM	$\|y_i\| = \|k\| \leq \|p\|$
Modified AKM	$\|y_i\| = \dfrac{\|k\|}{t} \leq \|k\| \leq \|p\|$

V. Conclusion

This paper proposes the modified AKM to reduce the communication cost/computation cost to $1/t$ of the original cost without security loss. From the comparison, the modified AKM is more practical because it can handle huge numbers of dynamic nodes in MANET and provide sufficient security requirements. In further study, we will also attempt to simplify the computation complexity of some AKM operations for the workability of ad hoc devices.

References

[1] B. Zhu, F. Bao, R. H. Deng, M. S. Kankanhalli, G. Wang, "Efficient and robust key management for large mobile ad hoc networks," *Computer networks*, 48, pp. 657-682, 2005.

[2] A. Khalili, J. Katz, W. Arbaugh, "Toward secure key distribution in truly ad hoc networks," *Proc. of the IEEE Workshop on Security and Assurance in Ad Hoc Networks, in Conjunction with the 2003 International Symposium on Applications and the Internet*, 2003.

[3] B. Lehane, L. Doyle, D. OMahony, "Shared RSA key generation in a mobile ad hoc network," *Proc. of the IEEE Military Communications Conference (MILCOM 2003)*, 2003.

[4] H. Luo, J. Kong, P. Zerfos, S. Lu, L. Zhang, "Self-securing ad hoc wireless networks," *Proc. of the Seventh IEEE Symposium on Computers and Communications (ISCC02)*, 2002.

[5] H. Luo, J. Kong, P. Zerfos, S. Lu, L. Zhang, "URSA: ubiquitous and robust access control for mobile ad hoc networks," *IEEE/ACM Transactions on Networking*, Vol. 12, No, 6, pp. 1049–1063, 2004.

[6] J. Kong, P. Zerfos, H. Luo, S. Lu, L. Zhang, "Providing robust and ubiquitous security support for mobile ad hoc networks," *Proc. of the IEEE 9th International Conference on Network Protocols (ICNP01)*, 2001.

[7] L. Zhou, Z. J. Haas, "Securing ad hoc networks," *Special Issue of IEEE Network on Network Security*, Vol. 13, No. 6, pp. 24–30, 1999.

[8] S. C ˇ apkuny, L. Buttya´n, J.-P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," Technical Report 2002/34, EPFL/IC, 2002.

[9] Adi. Shamir, "How to share a secret," *Communications of the ACM*, Vol. 22, No. 11, pp.612–613, 1979.

[10] Y. Desmedt, "Threshold cryptography," *European Transactions on Telecommunications*, Vol.5, No. 4, pp. 449–457, 1944.

[11] Y. Desmedt, Y. Frankel, "Threshold cryptosystems," *Proc. of the Advances in Cryptology-CRYPTO89, LNCS 0435*, pp. 307–315, 1990.

[12] R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, "Secure distributed key generation for discrete-log based cryptosystem," *Proc. Of Eurocrypt 99*, pp. 295–310, 1999.

[13] Woei-Jiunn Tsaur and Haw-Tyng Pai, "Dynamic Key Management Schemes for Secure Group Communication Based on Hierarchical Clustering in Mobile Ad Hoc Networks," *Proc. of ISPA 2007 Workshops, LNCS* 4743, pp. 475–484, 2007.

[14] Mawloud Omar, Yacine Challal, Abdelmadjid Bouabdallah, "Reliable and fully distributed trust model for mobile ad hoc networks, " Computers & Security, Vol. 28, pp. 199-214, 2009.

無研發成果推廣資料

98 年度專題研究計畫研究成果彙整表

計畫主持人：劉榮春			計畫編號：98-2221-E-029-028-				
計畫名稱：嵌入式系統平台多媒體影音播放的電力效能分析							
成果項目			量化			單位	備註（質化說明：如數個計畫共同成果、成果列為該期刊之封面故事...等）
			實際已達成數（被接受或已發表）	預期總達成數(含實際已達成數)	本計畫實際貢獻百分比		
國內	論文著作	期刊論文	3	3	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	5	5	100%		
		專書	0	0	100%		
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（本國籍）	碩士生	4	0	100%	人次	
		博士生	1	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		
國外	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	0	0	100%		
		專書	0	0	100%	章/本	
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（外國籍）	碩士生	0	0	100%	人次	
		博士生	0	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		

其他成果 (無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。)	無

	成果項目	量化	名稱或內容性質簡述
科教處計畫加填項目	測驗工具(含質性與量性)	0	
	課程/模組	0	
	電腦及網路系統或工具	0	
	教材	0	
	舉辦之活動/競賽	0	
	研討會/工作坊	0	
	電子報、網站	0	
	計畫成果推廣之參與（閱聽）人數	0	

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估 ■達成目標 □未達成目標（請說明，以 100 字為限） □實驗失敗 □因故實驗中斷 □其他原因 說明：
2. 研究成果在學術期刊發表或申請專利等情形： 論文：■已發表 □未發表之文稿 □撰寫中 □無 專利：□已獲得 □申請中 ■無 技轉：□已技轉 □洽談中 ■無 其他：（以 100 字為限）
3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）（以 500 字為限） 因為消費性電子在日常生活無所不在與不知不覺地被使用，對全球能源造成相當大的壓力，也對全球資源與環境造成非常大的衝擊。本計畫探討在嵌入式系統平台上播放多媒體影音的電力效能。音頻與視訊藉著各種編碼器壓縮以利傳輸與儲存。因為各總編碼器具有不同的特點，壓縮後的音頻視訊在播放時耗電量亦不同，本計劃對常用的編碼器與編碼參數研究分析並做了電力效能的比較，對建置嵌入式系統電子裝置的使用者與廠商，提出參考建議，以達成節能與延長電池壽命等目的。