Calhoun: The NPS Institutional Archive

Center for Homeland Defense and Security (CHDS) Homeland Security Affairs (Journal)

2013-04

Homeland Security Affairs Journal, Supplement - 2013: IEEE 2012 Conference on Technology for Homeland Security: Best Papers

Monterey, California. Naval Postgraduate School

Homeland Security Affairs Journal, Supplement - 2013: IEEE 2012 Conference on Technology for Homeland Security: Best Papers

http://www.nps.edu/library

Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

Homeland Security Affairs

The Journal of the Naval Postgraduate School Center for Homeland Defense and Security

Supplement No. 6: April 2013

IEEE 2012 Conference on Technology for Homeland Security - Best Papers -

As the field of homeland defense and security expands and matures, the contributions from various disciplines become ever more important. Particularly exciting are technical advances that have real-world application to homeland security practices. For this reason, Homeland Security Affairs is pleased to partner, for the third year, with the IEEE in presenting the best papers from the Conference on Technologies for Homeland Security.

The 2012 HST Conference drew attendees from federal agencies, universities, national laboratories, federally funded research and development centers, small businesses, and industry. Peer-reviewed technical papers were organized along four tracks highlighting emerging technologies in the areas of (1) cyber security; (2) attack and disaster preparation, recovery, and response; (3) land and maritime border security; and (4) biometric and forensics. One paper from each of these tracks was selected as the "best paper"; a fifth paper was awarded as the "best paper" from the conference as a whole.

The practical application of the technological innovations presented in these papers adds to the overall strength of homeland security efforts. As always, we welcome your comments and opinions at www.hsaj.org.

Notes From The Editor

Homeland Security Affairs is proud to publish the best papers from the IEEE 2012 Conference on Technology for Homeland Security.

The award for best conference paper overall went to **"A Compressed Sensing Approach for Detection of Explosive Threats at Standoff Distances using a Passive Array of Scatterers,"** by Jose Angel Martinez-Lorenzo and others. Addressing an important real-world problem, the research described in this paper applies millimeter wave radar imaging to find threats concealed under clothing at standoff distances up to fifty meters. Using a passive array of scatters in the target zone, compressive sensing can be used to linearize an otherwise difficult nonlinear problem. The result is an imaging algorithm used to achieve a resolution of 7.5 mm at 60 GHz which can accurately reconstruct the reflectivity values of both weak dielectric scatterers, such as explosives, including Tri-Nitro-Toluene (TNT), and strong scatters, like metallic pipes. The authors present a clever approach with good theoretical explanation, reasonable CONOPS and numerical validation.

The conference also awarded papers in four specific tracks: Cyber Security; Attack and Disaster Preparation, Recovery, and Response; Land and Maritime Border Security; and Biometrics and Forensics.

In the Cyber Security track, the award for best paper went to **"Return-Oriented Vulnerabilities in ARM Executables,"** by Zi-Shun Huang and Ian G. Harris. This paper presents a virus-scan approach to detect code sequences that can result in stack-smashing attacks on ARM devices. The work extends previous work on an important topic in special purpose static analysis techniques.

Lance Fiondella and others received the award for best paper in the Attack and Disaster Preparation, Recovery, and Response track for **"Security and Performance Analysis of Passenger Screening for Mass-transit."** This paper addresses an important modern problem: that of deciding when and how much security is appropriate at mass transit terminals (i.e., the metro, rail, and bus stations). The authors recognize a fundamental tradeoff between security and terminal productivity (from delays, costs), and apply it to a specific terminal to demonstrate its analytic-effectiveness. They then describe how this method can drive policy decisions as well as research investments.

In the Land and Maritime Border Security Track, the award for best paper went to **"Intelligent Radiation Sensor System (IRSS) Advanced Technology Demonstrator (ATD),"** by Daniel Cooper and others. The paper describes spectroscopic radiation detectors designed to improve the detection, localization, and identification of potential radiological threats, presenting a significant multi-year end-to-end field technology demonstration of short-range radiological sensor network. The system is primarily targeted to situations where it is not feasible to direct traffic through portal radiation detection systems, e.g. large events, search team objectives, etc. The capability to intelligently network individual portable detectors and fuse their data using advanced algorithms and COTS hardware has been shown within this program to significantly increase the effectiveness of an assortment of portable radiation detectors in a variety of naturally occurring backgrounds.

"A Video-based Hyper-focal Imaging Method for Iris Recognition in the Visible Spectrum," by Sriram Tankasala and others was recognized as the best paper in the Biometrics and Forensics track. The authors create a visible-wavelength iris imaging system and test it on 46 volunteers imaged under highly controlled conditions at a 45-minute interval. Using a freely available comparison package, ROCs for left and right irises are developed for both the hyperfocal and single frame images showing the performance improvement for the hyperfocal method.

We would like to thank the IEEE for the opportunity to publish this important research in *Homeland Security Affairs*.

A compressed sensing approach for detection of explosive threats at standoff distances using a Passive Array of Scatters

Jose Angel Martinez-Lorenzo, Yolanda Rodriguez-Vaqueiro and Carey M. Rappaport
ALERT Center of Excellence for Department of Homeland Security,
Gordon CenSSIS, Northeastern University Boston (MA), USA
{ jmartine ; rappapor }@ece.neu.edu

Oscar Rubinos Lopez, Antonio Garcia Pino
Dept. of Signal Theory and Communications, University of Vigo, Vigo, Spain
{ oscar ; agpino }@com.uvigo.es

***Abstract*—This work presents a new radar system concept, working at millimeter wave frequencies, capable of detecting explosive related threats at standoff distances. The system consists of a two dimensional aperture of randomly distributed transmitting/receiving antenna elements, and a Passive Array of Scatters (PAS) positioned in the vicinity of the target. In addition, a novel norm one minimization imaging algorithm has been implemented that is capable of producing super-resolution images. This paper also includes a numerical example in which 7.5 mm resolution is achieved at the standoff range of 40 m for a working frequency of 60 GHz.**

***Index Terms*—radar, compressive sensing, millimeter wave imaging.**

I. Introduction

DURING the last decade, new systems based on Millimeter-Wave-Radar technology have been deployed on airport checkpoints all around the world [1]. Millimeter wave systems are preferred to X-ray systems [2]-[4], for this particular application, because the former do not use ionizing radiation. These systems have been proved to be successful on finding explosives concealed underclothing; the success of this technology is mainly due to the short range between the sensing components of the system and the person under test. A new important challenge arises when the same technology is desired for threat detection at standoff distances [5]-[8], which include ranges running between ten to fifty meters.

In this work, a novel configuration based on an array of randomly distributed transmitting/receiving antennas, located on a two dimensional aperture, is used to scan a person at standoff distances. In order to improve the resolution of the radar system, a Passive Array of Scatters (PAS) is also placed near the target region. Under this configuration, the non-linear imaging problem can be linearized if the field produced by the two dimensional array and the PAS is accurately known across the imaging region. As a result, the imaging problem can be written into a matrix form. The sensing matrix, with coefficients representing the propagation from the target to the sensor establishes the linear relationship between the reflectivity value of a pixel on the target and the field measured on the array of receivers. For the particular case in which the number of pixels in the image is much larger than the number of sensors, the sensing matrix may become singular and difficult to invert.

A new approach, based on compressive sensing [9]-[16], can be used to invert the matrix if two conditions are satisfied: 1) the image can be represented by a sparse representation of customized basis functions; and 2) the sensing matrix complies with the mathematical Restricted Isometric Property (RIP) condition. If both conditions are satisfied, the image can be reconstructed by solving a convex problem.

This paper shows how this imaging algorithm has been used to achieve a resolution of 1.5 wavelengths, or 7.5 mm at 60 GHz. The proposed algorithm can accurately reconstruct the reflectivity values of both weak dielectric scatterers, such as explosives, including Tri-Nitro-Toluene (TNT), and strong scatters, like metallic pipes, concealed under clothing.

II. System Configuration

A. System Concept of operation

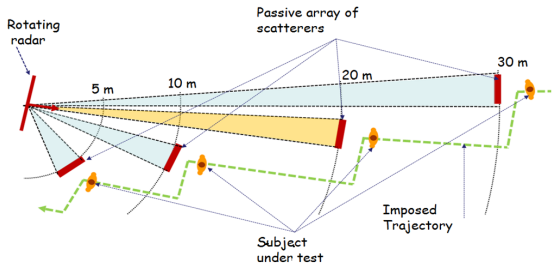
The proposed system configuration is shown schematically in Fig. 1. It is composed of an inexpensive, high-resolution radar system that can distinguish foreign

objects hidden on individuals at a distance, and that can still fit in or on a van. Additionally, a PAS is placed between the radar and the person under test in order to be able to achieve a super-resolution radar system. The concept of using multiple PAS over an imposed trajectory (see Fig.1 (b)) for person movement in places like airport terminals or bus stations provides the system with the option of re-configurability so that it might be applicable to indoor scenarios at multiple ranges.

B. System parameters

Fig. 2 represents a top view of the configuration and parameters of the system. The blue dots, on the left, represent the positions of the transmitting and receiving antennas. The radar is located on a square aperture of width L_1, and the total number of transmitting/receiving antennas is n_a. The orange dots, at the center of the image, represent the positions of the elements composing the PAS. The PAS is also located on a square aperture of width L_2, and the total number of elements on the PAS is n_d. The person under test is represented by the red silhouette on the right; and the reconstruction is performed by the imaging algorithm on a two dimensional plane, represented by a red line in Fig. 2, located in front of the person under test with n_p pixels. The distance between the radar and the person under test is Z_0, and the distance between the PAS and the person under test is Z_2. The resolution of the radar system, which is equal to the pixel size of the reconstructed image, is indicated by the parameter l.

(a)



(b)

Fig. 1. (a) General sketch of our van-based, high resolution radar system for standoff detection of potential suicide bombers. (b) Top view of the multiple-range concept of operation.

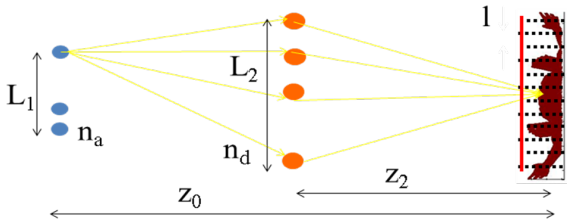


Fig. 2. Top view of the radar configuration. The blue circles on the left represent an thinned array of transmitter/receiver antennas; the orange dots on the center represent the passive array of scatters, which randomly redirect the energy of the radar towards the target; the person under test (target) is represented by the red silhouette on the right, and the two dimensional plane over which the reconstruction is implemented is represented by the red line in front of the person under test.

III. Mathematical formulation for the imaging problem

A. Sensing matrix

In this particular work, the sensing matrix, used by the imaging algorithm, is computed by using the phase term associated with an electromagnetic wave traveling as follows: 1) from each one of the transmitting antennas to each one of the scatters in the PAS; 2) from each one of the scatters on the PAS to each pixel on reconstruction plane; 3) from each pixel on the reconstruction plane to each one of the scatters on the PAS; and 4) from each one of the scatters on the PAS to each receiving antenna. This approximation is based on the following assumptions: 1) the amplitude attenuation associated with the electromagnetic wave propagation is considered to be constant, since it's impact on the quality of the reconstructed image is negligible; 2) the mutual coupling among pixels in the reconstructed image is not taken into account; 3) the amplitude and phase of the induced currents on the reconstruction plane is proportional to the incident field produced by radar illumination the latter approximation is equivalent to traditional Physical Optics method.

The system works on a multiple mono-static configuration, in which each element of the array transmits and receives on different slots of time without interacting with the radiation of other elements in the array.

Under this configuration, the sensing matrix A establishes a linear relationship between the unknown complex reflectivity vector $x \in C^{n_p}$ and the measured complex field data $y \in C^{n_d}$. This relationship can be expressed in a matrix form as follows:

$$A \cdot x + n = y \tag{1}$$

where $n \in C^{n_d}$ represents the noise collected by each receiving antenna. The matrix A can be rewritten as

the product of two matrices: 1) E_b, which is a diagonal matrix accounting for the background incident field produced by a single transmitting/receiving antenna and PAS on the reconstruction plane; and 2) P, which is a full matrix accounting for the propagation from each point on the reconstruction plane to each transmitting/receiving antenna after passing though the PAS. After applying some algebraic operations, the coefficients a_{ij} of the sensing matrix A can be expressed as follows:

$$a_{ij} = \sum_{p=1}^{n_d} \left(e^{-j2k|r_i - r''_p|} e^{-j2k|r''_p - r'_j|} \right) \qquad (2)$$

where k is the free space wave number; r_i is a vector indicating the position of the i-th transmitting/receiving antenna; r'_j is a vector indicating the position of the j-th pixel in the reconstruction plane; and r''_p is a vector indicating the position of p-th scatter in the PAS.

B. Imaging algorithm using compressive sensing approach

The proposed radar system is designed in accordance with the compressive sensing theory [9]-[16]. In order to apply such principles for standoff detection of explosive related-threats, certain mathematical conditions must be satisfied by the sensing matrix A and the reconstructed reflectivity image x. These conditions can be summarized as follows [13]: 1) the sensing matrix must satisfy the Restricted-Isometry-Property condition, which is related to the independency of the columns of the matrix; and 2) the unknown reflectivity vector must accept a sparse representation as a solution, which related to the number of non-zero entries on the solution vector. The parameters of the systems can be modified until these two conditions are satisfied; the optimized parameters include the following: aperture length of the radar, aperture length of the PAS, resolution in the reconstruction plane, number of antennas on the radar aperture, number of scatters in the PAS, working frequency, separation between the radar and the PAS, separation between the PAS and the target. In this work, this optimization is done manually, but it is expected that in further research contributions such optimization process should be automatized.

If the two aforementioned conditions are satisfied, then the reconstruction of the unknown vector can be performed with a small number of measurements (transmitting/receiving antennas) by solving the following convex problem [15]:

$$\min \|x\|_1 \qquad s.t. \quad Ax = y \qquad (3)$$

where $\|x\|_1$ represents the norm-one of the vector x. In the particular case where x is not sparse, the problem can still be solved if one can find a discretized functional W, in which a sparse representation x_p of the unknown vector x can be found through the following relationship: $x_p = Wx$. Therefore, the "Compressive Sensing" problem can be now solved by the following problem:

$$\min \|Wx\|_1 \qquad s.t. \quad Ax = y \qquad (4)$$

A Total Variation (TV) functional W is used in this particular work [15]. The TV functional W computes and adds the two directional gradients of the image x for each pixel; thus achieving a sparse representation x_p of the original image x.

IV. Numerical examples

A. Radar configuration

The imaging principles described in the previous section are evaluated on two different scenarios (see Table I): configuration #1, in which the distance between the radar and person under test is ten meters; and configuration #2, in which the distance between the radar and person under test is forty meters. Table I also summarizes all the parameters used for the numerical simulations. It is important to realize that in order to increase the range by a factor of four, from ten to forty meters, the length of the radar aperture must also be increased by a factor of four, and the number of antennas in such aperture must also be increased by a 60% factor, from five to eight hundred. The size and the number of scatters of the PAS is the same for both configurations, leading to the same system resolution of 7.5 millimeters. For the simulations in this work, a uniform white noise of 25 dB of signal to noise ratio is considered; and the working frequency of the system is 60 GHz.

PARAMETER	CONFIG. #1	CONFIG. #2
Z_0	2000λ = 10 m	8000λ = 40 m
Z_2	250λ = 1.25 m	250λ = 1.25 m
L_1	80λ = .4 m	320λ = 1.6 m
L_2	250λ = 1.25 m	250λ = 1.25 m
n_a	500	800
n_d	1000	1000
l	7.5 mm	7.5 mm

TABLE I
PARAMETERS FOR THE NUMERICAL EXAMPLES.

B. Target specifications

In order to test the feasibility of the system, a projection into a two dimensional plane of the three dimensional geometry, –a person with attached explosives– is

used as ground truth for the imaging algorithm. This two dimensional simplification of the three dimensional problem allows for a fast reconstruction using only one frequency for the radar configuration, and its extension to the three dimensional problem can be easily implemented in the future.

Fig. 3 (a) shows the two dimensional projection of a person under test; and Fig. 3 (b) shows the same person with two different types of explosive stimulants: two vertical metallic pipes of high reflectivity, and one square made of TNT of low dielectric reflectivity. The colorbar in the image indicate the absolute value of the reflectivity divided by the average reflectivity on the whole image.

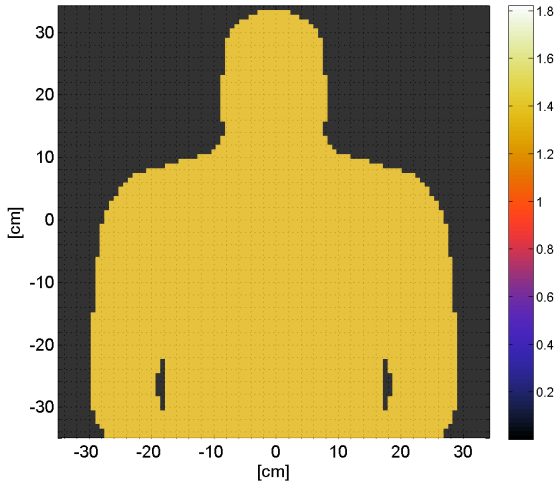


Fig. 3. Projection of the person under test used as ground truth by the imaging algorithm: (a) no-threat case, (b) threat case composed of two metallic pipes with high reflectivity and TNT square of low dielectric reflectivity.

C. Reconstruction results

Fig. 4 (a) and (b) show the reconstructed image when traditional Fourier-based SAR techniques [1] are used for the case of a person without and with explosive stimulants located at ten meters from the radar system (Configuration #1). This algorithm did not use the PAS; and, therefore, the resolution of the system is limited to that of the radar aperture. The quality of the reconstruction is quite deficient, and it is very difficult to discern the threat from the no-treat cases. Only an amplitude-based algorithm could be used to distinguish between the cases. The threat case, containing metallic pipes, shows some pixels with higher intensity level than those of the no-threat case.

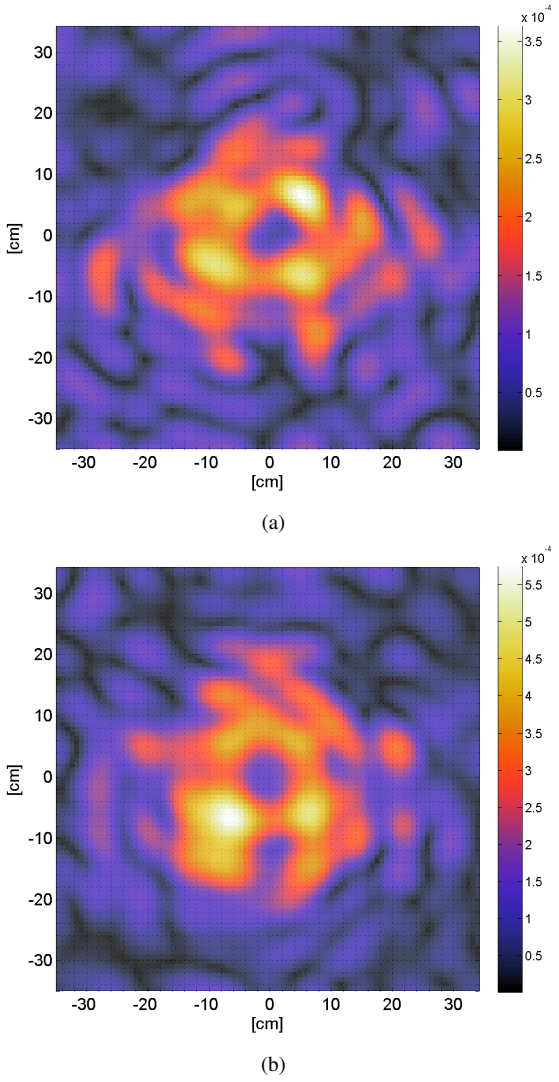


Fig. 4. Reconstruction using traditional Fourier-based SAR algorithms for configuration #1: (a) no-threat case, and (b) threat case.

When the PAS is introduced and the norm-one minimization is used for the imaging algorithm, the quality

of the reconstructed images, for both threat and no-threat cases, is substantially improved when compared to those produced by traditional SAR imaging algorithms [17][18] as it can be seen on Fig. 5 (a)-(b).

Fig. 5 (c) shows the reconstructed image for configuration #2, in which the radar and the target are separated 40 meters, when the PAS and the norm-one minimization on the imaging algorithm are used. Standoff detection at 40 meters requires that the length of the square radar aperture be increased from 0.4 meters to 1.6 meters, and the number of transmitting/receiving antennas is also increased from 500 to 800. This upgraded version of the system is capable of producing a resolution of 7.5 millimeters at 40 meters range.

V. Conclusions

This paper describes a new millimeter wave imaging system, which is able to produce super resolution images at standoff distances. Unlike traditional imaging systems in which the radar system directly illuminates the target under test, this system illuminates a passive array of scatters that redirects the energy of the radar towards the person under test. The PAS can be seen as a magnification lens that is located in front of the target, producing a super-resolution image. The imaging algorithm used for this system is based on compressive sensing theory. This imaging algorithm is different than traditional SAR algorithms because instead of just performing a Fourier transform of the measured data, it solves a norm-one minimization problem. Another important feature of this system is that it can be configured to work at multiple ranges if a specified trajectory is imposed on the person under test, making this system well suited for deployment for indoor spaces such as airport terminals or bus stations.

The performance of the system in terms of quality of the reconstructed image was tested for two target range configurations 10 and 40 m. In both cases, the system produced a resolution of 7.5 mm. The same PAS was used for both configurations, but it was necessary to increase the size of the radar aperture for the farther case to achieve the required 7.5 mm resolution.

Acknowledgment

This material is based upon work supported by the Science and Technology Directorate, U.S. Department of Homeland Security, Award No. “008-ST-061-ED0001” By the“Ministerio de Economa y Competitividad” Government of Spain under the project CSD2008-00068 (TERASENSE) and TEC2011-28683-C02-02 (TeraRADAR). The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of DHS.

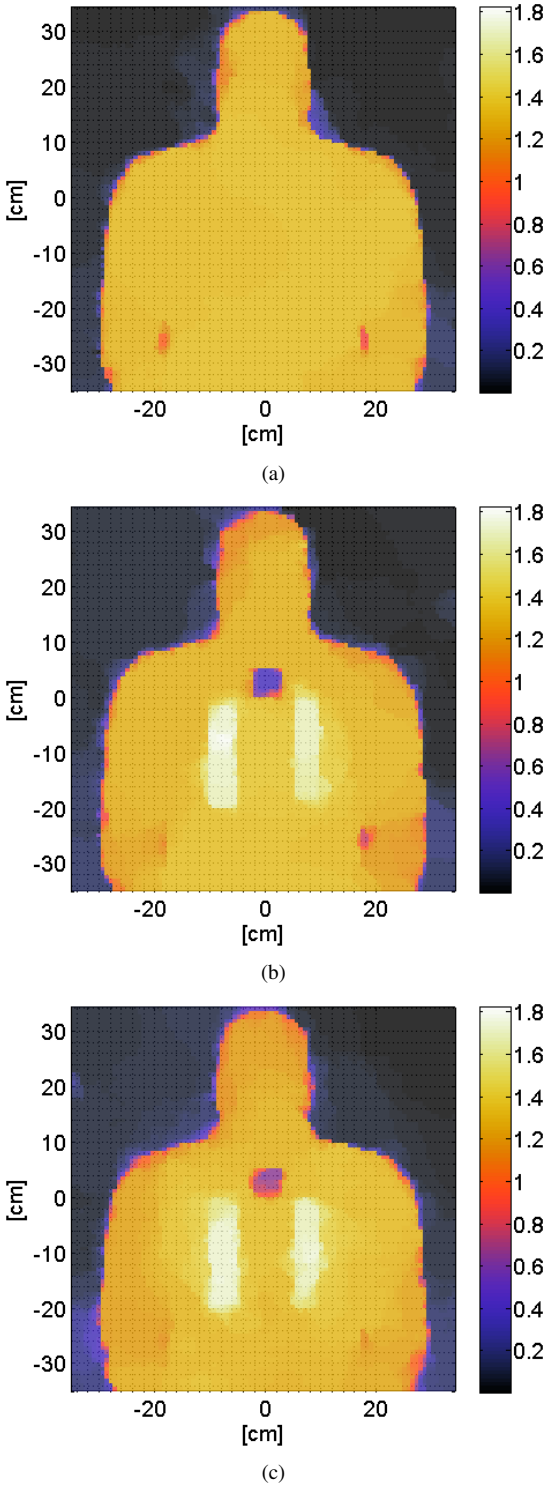


Fig. 5. Reconstruction using compressive sensing and the passive array of scatters: (a) no-threat case in configuration #1, (b) threat case in configuration #1, and (c) threat case in configuration #2.

REFERENCES

[1] D. M. Sheen, D. L. McMakin, T. E. Hall, *"Three-Dimensional Millimeter-Wave Imaging for Concealed Weapon Detection", IEEE Transactions on Microwave Theory and Techniques*, Vol. 49, No. 9, pp. 1581-1592, September 2001.

[2] US patent 5181234, Steven W. Smith, *"X-ray Backscatter Detection System"*, Issued 1993-01-19.

[3] R. F. Eilbert, Shi Shuanghe, *"Improved imaging for X-ray inspection systems", IEEE Aerospace and Electronic Systems Magazine*, Vol. 20, Issue 3, pp. 23-28, 2005.

[4] TSA X-ray Screening Technology Safety Reports: http://www.tsa.gov/research/reading/xray_screening_technology_safety_reports_march_2011.shtm

[5] J. A. Martinez-Lorenzo, F. Quivira and C. M. Rappaport, *"SAR imaging of suicide bombers wearing concealed explosive threats", Progress In Electromagnetics Research*, 125, pp. 255272, 2012.

[6] J. Fernandes, C. M. Rappaport, J. A. Martnez-Lorenzo, M. Hagelen, *"Experimental results for standoff detection of concealed body-worn explosives using millimeter-wave radar and limited view ISAR processing", 2009 IEEE Conference on Technologies for Homeland Security (HST09)*. Waltham, MA, May 11-12, 2009. pp. 456-460.

[7] A. Angell, C. Rappaport,*"Computational Modeling Analysis of Radar Scattering by Metallic Body-Worn Explosive Devices Covered with Wrinkled Clothing", 2007 IEEE/MTT-S International Microwave Symposium*. Honolulu, HI, June 3-8, 2007. pp. 1943-1946.

[8] K. B. Cooper, R. J. Dengler, N. Llombart, B. Thomas, G. Chattopadhyay, P. H. Siegel, *"THz Imaging Radar for Standoff Personnel Screening", IEEE Trans. Terahertz Science and Tech.*, Vol.1, pp.169-182, Sept. 2011.

[9] E. Candes, J. Romberg, and T. Tao, *"Robust Uncertainly Principles: Exact Signal Reconstruction from Highly Incomplete Frequency Information", IEEE Transactions on Information Theory*, 52, 2, February 2006, pp. 489-502.

[10] E. Candes, J. Romberg, and T. Tao, *"Signal Recovery from Incomplete and Inaccurate Measurements", Communications on Pure and Applied Mathematics*, 59, 2006, pp. 1207-1223.

[11] D. L. Donoho, *"Compressed Sensing", IEEE Transactions on Information Theory*, 52, 4, April 2006, pp. 1289-1306.

[12] R.G. Baraniuk, *"Compressive Sensing", IEEE Signal Processing Magazine*, 24(4), pp.118-121, July 2007.

[13] A. C. Fannjiang, T. Strohmer, and P. Yan, *"Compressed Remote Sensing of Sparse Objects", SIAM J. Imaging Sciences*, Vol. 3, No. 3, 2010, pp. 595-618.

[14] M.D.Migliore, D.Pinchera, *"Compressed Sensing in Electromagnetics: Theory, Applications and Perspectives", Proc. of the EuCAP*, Rome (Italy), 2011.

[15] S. Becker, J. Bobin, E. J. Candes, *"NESTA: A Fast accurate first-order method for sparse recovery" Siam J. on Imaging Sciencies*, Vol. 4, pp. 1-39.

[16] http://www-stat.stanford.edu/ candes/nesta/

[17] Y. Alvarez, J. A. Martinez, F. Las-Heras, C. M. Rappaport, *"An inverse Fast Multipole Method for geometry reconstruction using scattered field information". IEEE Transactions on Antennas and Propagation*, Vol. 60, No. 7, pp. 3351-3360, July 2012.

[18] Y. Alvarez, J. A. Martinez-Lorenzo, F. Las-Heras and C. M. Rappaport. *"An inverse fast multipole method for imaging applications", IEEE Antennas and Wireless Propagation Letters*, 10:12591262, 2011.

ABOUT THE AUTHORS

Jose Angel Martinez-Lorenzo *- jmartine@ece.neu.edu*

Yolanda Rodriguez-Vaqueiro

Carey Rappaport *- rappapor@ece.neu.edu*

ALERT Center of Excellence for Department of Homeland Security,

Gordon CenSSIS, Northeastern University Boston (MA), USA

Oscar Rubinos Lopez *- oscar@com.uvigo.es*

Antonio Garcia Pino *- agpino@com.uvigo.es*

Dept. of Signal Theory and Communications, University of Vigo, Vigo, Spain

---

© 2013 IEEE and published here with permission. *Homeland Security Affairs* is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of this article is expressly prohibited without the written consent of the copyright holder, the Institute of Electrical and Electronics Engineers (IEEE). *Homeland Security Affairs* is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).

http://www.hsaj.org

Return-Oriented Vulnerabilities in ARM Executables

Zi-Shun Huang
Center for Embedded Computer Systems
University of California Irvine
zishunh@uci.edu

Ian G. Harris
Center for Embedded Computer Systems
University of California Irvine
harris@ics.uci.edu

Abstract

Return-oriented programming is a method of computer exploit technique which is growing in popularity among attackers because it enables the remote execution of arbitrary code without the need for code injection. Return-to-LibC (Ret2LibC) is the most common return-oriented attack in use today, allowing an attacker to leverage control of the stack to execute common library functions which are already present on the target system, such as LibC. ARM-based processors, commonly used in embedded systems, are not directly vulnerable to Ret2LibC attacks because function arguments in the ARM are passed through registers rather than the stack. In 2011 Itzhak Avraham presented a new Return-to-Zero-Protection (Ret2ZP) attack against ARM processors which enables the same control as a Ret2LibC attack.

Our research contribution is to provide a formal definition of the Ret2ZP attack and to define an algorithm to detect vulnerabilities to Ret2ZP in ARM executables. Our algorithm for detecting vulnerabilities can be used to screen executables for vulnerabilities before they are deployed.

1 Introduction

Within the past 15 to 20 years embedded systems have seen increasingly widespread adoption. The complexity of many embedded devices is effectively invisible to users, operating inside components used everyday including automobiles, televisions, and video game consoles. The research firm IDC reports the market for embedded computer systems already generates more than US 1 trillion in revenue annually and will double in size over the next four years [20]. IDC also predicts that much of this growth will be propelled by more sophisticated, cloud-connected embedded system which will have a high degree of network connectivity. The embedded nature of these systems successfully conceals complexity, allowing users to forget about security vulnerabilities that they are exposed to. The media has improved public awareness of cyberattacks against servers operating at institutions such as banks, credit card agencies, and nuclear material enrichment facilities. However, people are not sufficiently aware of the vulnerabilities inside embedded devices which they use much more frequently. Embedded systems are increasingly network-enabled, typically connected to the internet through a TCP/IP stack. Network connectivity makes these systems vulnerable to many of the same cyberattacks as desktop, laptop, and server machines.

Malware is a collection of instructions that executes on a machine and make the system to perform somemalicious operation [4]. There are several recent examples of malware which targets embedded devices. For example, millions of printers were found to contain a security weakness that could allow attackers to take control of the systems, steal data and issue commands that could cause the devices to overheat and catch fire [10]. Even in industrial systems such as programmable logic controller (PLC) and supervisory control and data acquisition (SCADA) have the risk to be attacked. The Stuxnet worm, discovered in June 2010, initially spreads via Microsoft Windows, and targets Siemens industrial software and equipment [13]. Embedded systems are often required to meet strict timing, cost, and power requirements. As a result, traditional defense mechanisms are not suitable for embedded systems. Security vulnerabilities often depend on very specific aspects of the behavior the underlying processor, so embedded systems vulnerabilities may be significantly different from those of general-purpose platforms.

Return-oriented programming [24] describes a growing class of exploits which code segments already present on a system to execute a range of malicious behaviors. The most common type of return-oriented

attack is Return-to-LibC (Ret2LibC) [8] where an attacker exploits a buffer overflow to redirect control flow to a library function already present in the system. To perform a Ret2LibC attack, the attacker must overwrite a return address on the stack with the address of a library function. Additionally, the attacker must place the arguments of the library function on the stack in order to control the execution of the library function. Ret2LibC is commonly applied against Intel x86 architectures, but the ARM architectures [17] used in embedded systems are not directly vulnerable to this attack because function parameters are passed through registers instead. ARM-based processors are the most commonly used microprocessors in embedded systems due in part to their low power consumption compared to Intel x86.

At the BlackHat Convention in 2011, Itzhak Avraham [6] first presented the Return-to-Zero-Protection (Ret2ZP) attack which effectively allows a Ret2LibC attack to be applied to ARM-based processors. This is an important development because reveals a significant vulnerability in ARM-based processors which is likely to be exploited to create malware targeted at embedded systems.

The contribution of this paper is an approach and a tool to analyze the software on an ARM-based system and determine whether or not it is vulnerable to a Ret2ZP attack. The feasibility of a Ret2ZP attack depends on the existence of special code sequences on the embedded system platform. We define the nature of the code sequences which expose a system to a Ret2ZP attack. Our tool automatically scans an existing ARM executable and identifies all vulnerable code sequences. Once identified, vulnerable code sequences can be patched to remove the vulnerability.

2 Related Work

Return-to-LibC (Ret2LibC) [11] is a method of exploiting based on buffer overflow to defeat a system that has a non-executable stack. The difference between Ret2LibC and traditional buffer overflow code inject attack is that the return address is overwritten to point to a shared library such as C library. In addition, the required arguments to the shared library function are also placed on the stack. This allows attackers to call existing library functions without injecting malicious code into a program. Dynamic shared libraries must be executable, so non-executable memory regions provide no protection against this attack. Ret2LibC is a special case of a return-oriented programming attack [24] which has the potential to enable arbitrary code execution.

To prevent Ret2LibC attacks, many mechanisms have conceived. One protection technique focuses on monitoring control flow and memory activities to detect violations [23]. These approaches may use hardware support [14, 5, 19, 25] such as a shadow stack. These methods require a new architecture [15, 7], and may affect the original pipeline performance [16, 3]. This techniques need to check all instructions, memory, or stack. If it does not check all instruction, the risk of attack is possible. Checking all instruction comes with a significant reduction in performance [21, 12, 9]. Protected free-branch instructions technique can be implemented by using code rewriting techniques to remove all unaligned instructions that can be used to link the gadgets. However, because of code rewriting, its main disadvantage is code size increase [22].

Ret2LibC attack requires passing arguments to libc functions from the stack. By ARM calling convention [17], passing parameters occurs through registers rather than the stack. A stack buffer overflow gives the attacker direct control of the stack, but not the registers. As a result, Ret2LibC attacks does not work againstARM-based processors. In [6], Avraham developed the Return-to-Zero-Protection (Ret2ZP) attack against ARM-based processors which allows an attacker to control registers from the stack. By allowing control of registers, Ret2ZP enables the Ret2LibC attack to be applied to ARM-based processors.

3 Return to Zero Protection (Ret2ZP)

A Ret2ZP attack exploits a stack buffer overflow to redirect control flow to a function present on the system, and to control the arguments to that function. Redirecting control flow can be performed directly by overwriting a return address on the stack with the address of the desired function. However, controlling the function arguments is more difficult because functions executing on the ARM architecture accept arguments through argument registers r0 - r3, rather than the stack. To control the arguments to a function, the contents of one or more of these registers must be assigned before control flow is redirected to the desired function.

To control the values of the argument registers and to redirect control flow to the desired function, the Ret2ZP attack depends on the existence of a **vulnerable code sequence (VCS)**, already present on the system, which copies data from the stack to the

argument registers, and then from the stack to the program counter (PC) register. The Ret2ZP attack first places the library function arguments and the library function address onto the stack. Then control flow is redirected to the VCS which moves the arguments from the stack to the argument registers, and moves the library function address from the stack to the PC, redirecting control flow to the library function.

Figures 1a, b, and c show the contents of the stack at different points during the execution of a Ret2ZP attack. Figure 1a shows the contents of the original stack, before the attack has been executed. Two stack frames are shown, where stack frame 0 is the current stack frame at the top of the stack. The stack frames have been simplified for the purposes of this presentation, so only the contents important to the Ret2ZP attack are shown. Each stack frame contains a space labeled *locals* for local variables for the corresponding function, and a space labeled *ret_addr* which contains the return address for code execution after the corresponding function is complete. The current stack frame contains a buffer labeled *buff* which we assume is vulnerable to buffer overflow by the attack.

Figure 1b shows the contents of the stack after the buffer overflow. The stack grows down in memory addresses, so the memory addresses increase down in the stack pictures of Figure 1. When the buffer overflows, the stack below the buffer is altered, as can be seen in Figure 1b. The buffer overflow places three different blocks of data onto the stack. The address of the VCS, *&VCS*, is written over the old return address so that the the VCS will be executed when the current function completes. The arguments to be passed to the desired library function, *args*, and the address of the desired library function, *&libfn* are placed on the stack.

Figure 1c shows the contents of the stack after the current function completes its execution and returns. Since the old return address was overwritten with *&VCS*, the VCS is now executing. The *locals* region for stack frame 0 was popped off of the stack when the previous function completed its execution, so the top of the stack contains the arguments for the desired library function and the address of the library function, as shown in Figure 1c. At this point, it is the job of the VCS to move the arguments from the stack to the argument registers, and move *&libfn* to the PC.

3.1 Vulnerable Code Sequence (VCS)

The Ret2ZP attack depends on the existence of an appropriate VCS in the system. A VCS, is a consecutive sequence of instructions which are resident in the memory of the victim machine. It would be possible for a vulnerable code sequence to be composed of multiple discontinuous code sequences which are connected by intervening jump instructions but we ignore this possibility for the sake of simplicity, and because it is unlikely to occur in practice. Any valid VCS must satisfy the following set of constraints that our tool checks for.

1. The final instruction in the sequence must copy data from the stack to the PC register. The execution of this final instruction which transfers control to the desired library function.

2. The sequence must contain no instruction which writes data to the PC register, other than the final instruction. This constraint ensures that the instruction sequence is continuous.

3. The sequence must move data from the stack into some subset of the argument registers.

4. The sequence must not write data to the stack. This is required because any data written to the stack might overwrite the library function arguments or the library function address which are already on the stack.

Figure 2 shows an example of a VCS. The first line of code loads argument registers r0 and r1 from the stack which is addressed by the stack pointer, SP. The final line of code executes a function return by popping the top of the stack and placing the popped value in the program counter, PC. Notice that the stack contents can be read using a load-type of instruction such as ldm, or a pop instruction which also updates the stack pointer.

4 VCS Detection

We have implemented a tool which identifies the presence of vulnerable code sequences in an executable. Detection of these sequences will allow the software to be patched, removing the vulnerability before the software is deployed. In order to analyze the executable, our tool uses the Radare toolkit [1] to disassemble the executable and generate assembly code which we can process. Once the executable is disassembled, our tool performs a single-pass scan of each instruction to identify any VCS.

An important aspect of a VCS is that it must move data from the stack into the argument registers. To

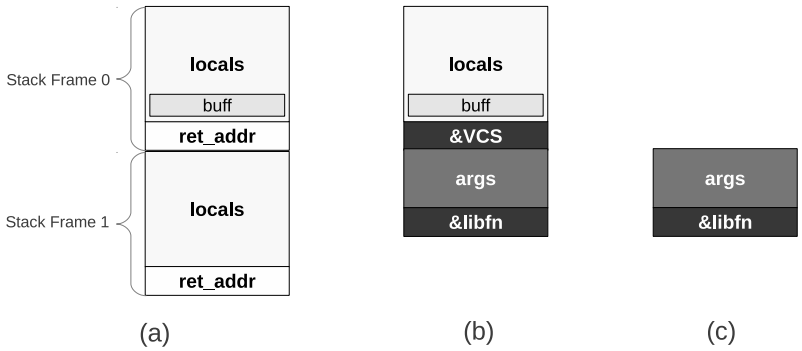


Figure 1: Stack contents during Ret2ZP attack, (a) before buffer overflow, (b) after buffer overflow, (c)start of VCS execution

```
ldm sp, {r0, r1}
add sp, sp, #8
pop {pc}
```

Figure 2: Vulnerable code sequence example

assist our discussion of this topic, we refer to a register as being *stack-controllable* at a point during program execution if the current value of the register was copied directly from the stack. A register becomes stack-controllable when an instruction loads stack contents into the register, and it is no longer controllable after the registers value is modified in any way, other than loading it from the stack.

The executable is scanned linearly from beginning to end, and at each line a set of stack-controllable argument registers R is maintained. A VCS is detected if an instruction is encountered which loads the PC from the stack, and $R \neq \emptyset$. Additional constraints are that the VCS should contain no branches to any address not taken from the stack, and that no instruction within the VCS should write to the stack. To enforce these constraints we set $R = \emptyset$ whenever either a non-stack branch or a write to the stack are encountered.

Figure 3 contains the pseudocode describing our VCS detection algorithm. In the pseudocode we use the following definitions:

- A is the set of argument registers.
- PC refers to the program counter register.
- R is the current set of stack-controllable argument registers.
- I is the ordered sequence of instructions in the executable.

1. $R = \emptyset$
2. foreach $i \in I$
3. foreach $r \in A$
4. if $i \in L_r$ then $R = R \cup r$
5. if $i \in M_r$ then $R = R - r$
6. if $(i \in W)$ OR $(i \in B)$ then $R = \emptyset$
7. if $i \in L_{PC}$ AND $R \neq \emptyset$ then
8. print VCS Detected
9. $R = \emptyset$

Figure 3: VCS Detection Pseudocode

- L_r is the set of instructions in the executable which load register r from the stack.
- M_r is the set of instructions in the executable which modify register r without loading register r from the stack.
- W is the set of instructions in the executable which write data to the stack.
- B is the set of instructions in the executable which branch to an address not taken from the stack.

The algorithm in Figure 3 initializes the set of stack-controllable registers on line 1, and enters a loop starting on line 2 which iteratively processes each instruction of the executable. The set of stack-controllable registers is updated on lines 3 - 5 where an argument register is added to the set if it is loaded from the stack, and deleted from the set if it is modified. A check for non-stack branch instructions and stack writing instructions is performed on line 6. The end of a VCS is detected at line 7 as an instruction which moves the stack contents to the PC while

File Name	C	exec.	# VCS
aes_expanded_key	508	28878	1
aes_set_key	481	27449	1
Bitband	515	25151	0
boot_demo1	491	32923	0
boot_demo2	510	34313	0
boot_demo_eth	529	67360	0
enet_io	1234	66532	0
enet_lwip	741	66627	0
enet_ptpd	1095	66621	1
enet_uip	690	62218	0
hello	539	36919	0
gpio_jtag	543	62218	0
Graphics	719	24014	0
interrupts	616	29175	0
mpu_fault	563	31472	0
Pwmgen	470	24623	1
qs_ek-lm3s6965	5178	66726	0
sd_card	731	62332	0
timers	497	26462	0
uart_echo	515	30110	0
Watchdog	476	25338	0

Table 1: VCS Detection Results

$R \neq \emptyset$. If a VCS is detected then success is announced (line 8) and the stack-controllable set is reset to start scanning for a new VCS in the remainder of the executable (line 9).

5 Experimental Results

We used our vulnerability analysis tool to detect vulnerable code segments in a set of same ARM executables. As our benchmark set of ARM executables we used the example programs provided for use with the EK-LM3S6965 Evaluation Board from Texas Instruments [2]. The board uses an ARM-based TI Stellaris LM3S6965 microprocessor. The sample programs are provided in C which we compiled for the LM3S6965 processor using the GCC compiler [18].

Table 1 shows the results of our analysis of all of the sample ARM-executables. Each row contains the results for a different program and the first column contains the name of the program. The second and third columns show the size of the original C programs and the size of the compiled executable. The final column labeled **# VCS** shows the number of vulnerable code segments found in each executable. The table shows that almost 20% of these executables contained a vulnerability to the Ret2ZP attack. The total CPU time required to detect VCS in all examples is 0.117 seconds.

```
ldmibeq sp!, {r0, r1, r2, r4, r5, r6,
              r7, fp, sp, pc}
```

Figure 4: VCS example in Pwmgen

The vulnerable code sequences detected in these examples were all comprised of a single line of code which loaded the argument registers as well as the PC. An example is shown in Figure 4 which was found in the Pwmgen sample program.

6 Conclusions

We have developed a tool which is used to detect Ret2ZP vulnerabilities in ARM executables. The popularity of return-oriented programming attacks underscores the need for the tool that we have developed. Our experimental results show that almost 20% of the programs that we evaluated actually contained vulnerabilities. Since the frequency of vulnerabilities can be expected to increase with program size, the detection of vulnerabilities becomes even more important for larger systems.

References

[1] **radare**, reverse engineering toolkit. http://radare.org.

[2] Texas Instruments EK3S6965 Evaluation Kit. http://www.ti.com/tool/eki-lm3s6965.

[3] M. Abadi, M. Budiu, U. Erlingsson, and Jay Ligatti. Control-flow integrity principles, implementations, and applications. *ACM Transactions on Information and System Security (TISSEC)*, 13(1):4, 2009.

[4] Aleph One. Smashing The Stack For Fun And Profit, 1995. http://insecure.org/stf/smashstack.html.

[5] Divya Arora, Srivaths Ravi, Anand Raghunathan, and N.K. Jha. Secure embedded processing through hardware-assisted run-time monitoring. In *Proceedings of the conference on Design, Automation and Test in Europe-Volume 1*, pages 178–183. IEEE Computer Society, 2005.

[6] Itzhak(Zuk) Avraham. Non-Executable Stack ARM Exploitation Research Pa-

per. In *BlackHat Security Convention*, 2011. https://media.blackhat.com/bh-dc-11/Avraham/BlackHat_DC_2011_Avraham_ARM Exploitation-wp.2.0.pdf.

[7] Mihai Budiu, U. Erlingsson, and M. Abadi. Architectural support for software-based protection. In *Proceedings of the 1st workshop on Architectural and system support for improving software dependability*, pages 42–51. ACM, 2006.

[8] cOntext. Bypassing Non-Executable Stack During Exploitation Using Return-to-LibC. http://infosecwriters.com/text_resources/pdf/return-tolibc.pdf.

[9] M.L. Corliss, E.C. Lewis, and A. Roth. Using DISE to protect return addresses from attack. *ACM SIGARCH Computer Architecture News*, 33(1):65–72, 2005.

[10] Ang Cui and Sal Stolfo. Print Me If You Dare Firmware Update Attack and the Rise of Printer Malware, 2011. http://ids.cs.columbia.edu/sites/default/files/CuiPrintMeIfYouDare.pdf.

[11] Solar Designer. Getting around non-executable stack (and fix), 1997. http://seclists.org/bugtraq/1997/Aug/63.

[12] Ú. Erlingsson, M. Abadi, Michael Vrable, M. Budiu, and G.C. Necula. XFI: Software guards for system address spaces. In *Proceedings of the 7th symposium on Operating systems design and implementation*, pages 75–88. USENIX Association, 2006.

[13] Nicolas Falliere. Stuxnet Introduces the First Known Rootkit for Industrial Control Systems, 2010. http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices.

[14] Aurélien Francillon, Daniele Perito, Claude Castelluccia, and Inria Rhône-alpes. Defending Embedded Systems Against Control Flow Attacks Categories and Subject Descriptors. In *Proceedings of the first ACM workshop on Secure execution of untrusted code*, pages 19–26, 2009.

[15] Saugata Ghose, Latoya Gilgeous, Polina Dudnik, Aneesh Aggarwal, and Corey Waxman. Architectural support for low overhead detection of memory violations. In *Design, Automation & Test in Europe Conference & Exhibition, 2009. DATE'09.*, pages 652–657. IEEE, 2009.

[16] Koji Inoue. Energy-security tradeoff in a secure cache architecture against buffer overflow attacks. *ACM SIGARCH Computer Architecture News*, 33(1):81–89, 2005.

[17] ARM Ltd. Procedure Call Standard for the ARM Architecture, 2009. http://infocenter.arm.com/help/topic/com.arm.doc.ihi0042d/IHI0042D_aapcs.pdf.

[18] GCC the GNU compiler collection. gcc.gnu.org.

[19] Milena Milenković, A. Milenković, and E. Jovanov. Hardware support for code integrity in embedded processors. In *Proceedings of the 2005 International Conference on Compilers, Architectures and Synthesis for Embedded Systems*, pages 55–65. ACM, 2005.

[20] Mario Morales and Michael J Palma. Intelligent systems : The next big opportunity, 2010. www.idc.com.

[21] G. Novark, E.D. Berger, and B.G. Zorn. Exterminator: automatically correcting memory errors with high probability. *Communications of the ACM - Surviving the data deluge*, 42(6):1–11, 2008.

[22] Kaan Onarlioglu, Leyla Bilge, Andrea Lanzi, Davide Balzarotti, and Engin Kirda. G-free: defeating return-oriented programming through gadget-less binaries. In *Proceedings of the 26th Annual Computer Security Applications Conference*, ACSAC '10, pages 49–58, 2010.

[23] R.G. Ragel, S. Parameswaran, and S.M. Kia. Micro embedded monitoring for security in application specific instruction-set processors. In *Proceedings of the 2005 International Conference on Compilers, Architectures and Synthesis for Embedded Systems*, pages 304–314, 2005.

[24] Hovav Shacham. The geometry of innocent flesh on the bone: Return-into-libc without function calls (on the x86). In *Proceedings of the 14th ACM Conference on Computer Communications and Security*, pages 552–561, 2007.

[25] T. Zhang, X. Zhuang, S. Pande, and Wenke Lee. Anomalous path detection with hardware support. In *Proceedings of the 2005 International Conference on Compilers, Architectures and Synthesis for Embedded Systems*, pages 43–54, 2005.

ABOUT THE AUTHORS

Zi-Shun Huang - *zishunh@uci.edu*

Ian G. Harris - *harris@ics.uci.edu*

Center for Embedded Computer Systems

University of California Irvine

© 2013 IEEE and published here with permission. *Homeland Security Affairs* is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of this article is expressly prohibited without the written consent of the copyright holder, the Institute of Electrical and Electronics Engineers (IEEE). *Homeland Security Affairs* is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).

http://www.hsaj.org

Security and Performance Analysis of a Passenger Screening Checkpoint for Mass-transit Systems

Lance Fiondella and Swapna S. Gokhale
Department of Computer Science and Engineering
University of Connecticut
Storrs, CT 06269, U.S.A
{lfiondella,ssg}@engr.uconn.edu

Nicholas Lownes and Michael Accorsi
Department of Civil and Environmental Engineering
University of Connecticut
Storrs, CT 06269, U.S.A
nlownes@engr.uconn.edu

***Abstract*—During the past decade, the international community has witnessed several attacks on forms of mass transportation such as train stations and subways. The Department of Homeland Security requested that we develop methods to assess the security of mass transit in order to mitigate the vulnerability of the nation's public transportation systems. We present a methodology to quantify the impact of imposing screening on mass transit, which considers both security and delays incurred on the traveling public. We demonstrate the approach through a case study, the Fairfield Metro Station in Fairfield, Connecticut. Our results indicate that rigorous aviation-style screening will slow the flow of passengers drastically. We also show how to use the approach to identify where faster screening technologies can improve passenger throughput while ensuring security. The approach can thus be used to identify areas where investments in technology improvement would most effectively enhance security and convenience.**

Keywords-mass-transit; passenger screening; security; performance;

I. INTRODUCTION

Screening is critical to ensure the security of every mode of transit in the nation's transportation infrastructure. Both aviation and port security employ screening to minimize the chance that airplanes and boats carry illegal or dangerous items and individuals. Domestic mass transit systems such as railroads and subways, however, cannot impose rigorous security procedures because the time incurred in screening will produce a noticeable drag on the smooth flow of large volumes of passengers. The inconvenience and high cost of screening rail and subway passengers is undesirable, however, in the past decade, these modes of transportation have been the targets of several terrorist attacks throughout the world [1]. Moreover, it is public knowledge that terrorist organizations such as Al-Qaeda plan to perpetrate such attacks. Mass-transit may also be an attractive terrorist target because of the widespread attention and public fear such acts inspire. Therefore, although the screening delays inconvenience passengers and harm profitability, protecting people and assets remains a significant concern. This suggests that advances in the speed of screening technologies are necessary before such comprehensive screening can be implemented for mass-transit systems.

Prevalent research focuses on the engineering of security technologies rather than exploring their performance. For example, Burgoon *et al.* [2] automate techniques to detect deceptive behavior in individuals at border crossings. Tambe [3] has applied game theoretic techniques to security problems, including screening of cars entering Los Angeles International Airport, scheduling Federal Air Marshals on flights with potentially dangerous passengers, and randomized Coast Guard patrols to detect terrorism and drug trafficking. Most of these works focus on how existing screening technologies can be used effectively to improve security. However, there is very little research [4] on whether these technologies balance security and performance when employed at checkpoints. Therefore, such screening can be reasonably employed only when the volume of passengers is low, such as at airports. They do not scale to mass transit systems, which usually experience extremely high volumes of traffic. Therefore, to enhance the security of mass transit systems through passenger screening, methods which assess both the security and performance of a checkpoint are needed to determine if specific design and technologies exhibit desired levels of threat detection while maintaining acceptable passenger throughput.

This paper presents a methodology to quantify the security and performance of a screening checkpoint in terms of the security and performance metrics of its constituent technologies and their organizational layout. We demonstrate our approach using the case study of the Fairfield Metro Station, which is the first railroad station to be built in Connecticut in over 90 years. The methodology allows us to quantify the probability that a threat will be detected as it passes through the checkpoint, along with the degradation in passenger throughput caused by screening. Our results indicate that imposing rigorous aviation-style screening will slow the flow of passengers drastically. Therefore, unless screening technologies can be made faster they will be too cumbersome for mass-transit. Our approach can thus systematically identify checkpoint designs and technology improvements that can balance the security and performance concerns, to enable their use in securing the mass transit infrastructure.

The paper is organized as follows: Section 2 outlines the challenges in quantifying security and performance with an example. Section 3 proposes the modeling approaches. Section 4 demonstrates these approaches. Section 5 summarizes lessons learned and offers suggestions for enhancements. Conclusions and future research are offered in Section 6.

II. Problem Formulation

This section describes the challenges in assessing performance and security of screening checkpoints for mass transit systems using the layout of the security turnstiles in the lobby of Fairfield Metro Center (FMC), as shown in Fig. 1 Passengers arrive at the station at rate $\lambda(t)$. This arrival process is a function of time because travelers rely on mass transit systems for their daily commute. Hence, higher volumes may be expected during the rush hour, with lighter traffic at other times. Next, the passengers walk down a hallway to insert their ticket into one of three turnstiles for scanning, where a computer records the time and outputs the voided ticket before opening a gate to allow them to pass. The passengers then proceed to the platform of their departing train.

To enhance passenger throughput, these turnstiles are placed side-by-side to create multiple parallel lanes. A passenger typically selects the turnstile with the shortest line. When passenger volume is high, however, the lines at all turnstiles are approximately equal. Therefore, we set the probability of selecting a particular turnstile equal ($x_1 = x_2 = x_3 = 1/3$). The process of inserting a ticket and passing through the turnstile requires approximately three seconds.

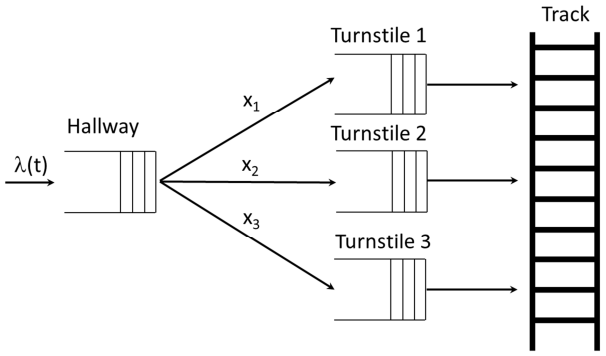


Figure 1. Fairfield Metro Center turnstile configuration.

To understand the impact of introducing airport screening into mass-transit, Fig. 2 shows the primary components and key decision points in a simple checkpoint. These components could replace the turnstiles within FMC without requiring major modifications to the interior of the building.

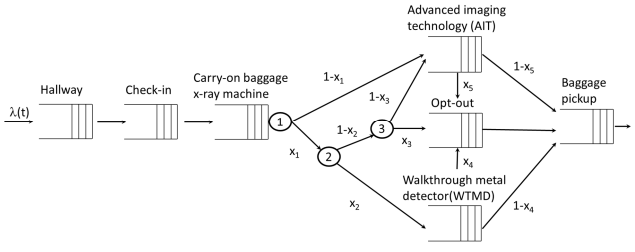


Figure 2. Passenger screening checkpoint.

In this layout, passengers arriving at the screening checkpoint must first check-in by providing their ticket and identification to a security officer. Next, they must divest themselves of their carry-on baggage and other personal items to be placed on a conveyor belt for x-ray screening. After this step, there are several decision points. First, a passenger may choose to undergo scanning by an Advanced Imaging Technology (AIT) machine or the older but more popular Walkthrough Metal Detector (WTMD). We assume that the probability of WTMD screening, denoted x_1, is greater than that of AIT screening ($1 - x_1 = \bar{x}_1$) because AIT exposes passengers to radiation and passengers believe that it generates revealing images. The second branch occurs because an attending officer has the authority to ask a passenger to undergo AIT scanning ($\bar{x}_2$), even if the passenger prefers WTMD. This leads to the third decision point because passengers have the right to *opt-out* of AIT and request alternative screening procedures (x_3), involving a pat down inspection. Some passengers passing through WTMD forget to remove metal items and may also be asked to undergo a pat down (x_4). AIT may also fail to ascertain the absence of concealed items, in which case a pat down will be requested (x_5). Once passengers clear the screening stations, they proceed to retrieve their carry-on baggage, shoes, and other personal items. Subsequently, they will exit the screening checkpoint and continue to the platform from which their train will depart.

The types of technologies in Fig. 2 include several implicit security policies employed at mass-transit checkpoints. They also reflect existing policies. For example, passengers' identities are verified manually at check in. Such manual screening may be acceptable for high-speed rail, but will be extremely labor-intensive for subways. x-ray screening of carry-on baggage assumes that passengers will be required to submit their luggage for inspection. Finally, although WTMD and opt-out show limited effectiveness for detecting concealed threats, these alternative forms of screening continue to be retained because these forms may be necessary to respect the passengers' privacy by offering them these choices.

WTMD and opt out cannot be eliminated; in fact, a large fraction of passengers may prefer these slower forms, leading to underutilization of AIT and long lines for WTMD, requiring passengers to arrive for their trip earlier. Moreover, these alternative screening methods are laborious; suggesting that passenger preference for them will influence performance. It will also have a negative impact on security, because they have a lower probability of detecting concealed non-metal items. Thus, these technologies hinder the implementation of screening in mass-transit. Inclusion of AIT assumes that future mass-transit screening will consist primarily of this modern technology and that older less effective ones such as WTMD, opt-out, and unattended turnstiles will be phased out.

In summary, the goal of modeling mass-transit screening is to assess the impact of passenger preference and the detection probabilities of the screening technologies on the security and performance of the screening checkpoint. A method to quantify tradeoffs between the security and performance will identify improvements that can reduce the waiting time while simultaneously ensuring the protection of people and assets.

III. Modeling Approach

This section describes our approach to quantitatively assess the impact of imposing screening on mass transit. Security and

performance of a checkpoint are analyzed as a function of the organization of the screening technologies and flow of passengers through the machines and checkpoint.

A. *Security Analysis*

Security is defined as the probability that a screening technology or a checkpoint successfully detects a threat. We refer to our approach as architecture-based analysis because it expresses the checkpoint security in terms of the security of the screening stations comprising the checkpoint and the probabilistic flow of passengers through these stations. Let n denote the number of screening stations in the checkpoint. We represent the layout of these screening stations in terms of the one-step transition probability matrix of an absorbing DTMC [5] $\mathbf{P}_{n\times n}$, where $p_{i,j}$ denotes the probability that a passenger moves to station j after passing through station i. Without loss of generality, we assume that screening begins at station 1 and completes after station n. Thus, station 1 is designated as the initial state, and station n is the final or the absorbing state of the DTMC. The entry $p_{n,n}$ of $\mathbf{P}$ is set to 1.0.

We augment the DTMC with two absorbing states D and F, where D corresponds to successful threat detection and the failure state F is reached if a threat escapes the checkpoint undetected. From each station i, a transition (i,D) with probability s_i is added, which is the likelihood that the station detects the threat. The original transition probability $p_{i,j}$ between stations i and j is revised to $\bar{s}_i p_{i,j}$, where $\bar{s}_i = (1 - s_i)$. This indicates that a passenger moves to station j only if station i does not detect a threat. Finally, a transition is added from station n to state D with probability $p_{n,D} = s_n$ and to state F with probability $p_{n,F} = \bar{s}_n$. Thus, the checkpoint fails if a threat is undetected at all stations the passenger visits. The process of composing the layout of the checkpoint with stations' detection probabilities assumes that the transitions among the stations are independent and that the detection of a threat at any station implies that the checkpoint is successful. We refer to the resulting model as the 'composite model' because it offers an integrated representation of the layout of the checkpoint and the detection capabilities of the stations.

Once the composite model is built, the following sequence of operations can be performed to obtain an expression, S, for the security of the checkpoint.

- Set $\mathbf{P}_{n,n}$=0.
- Define diagonal matrix $\mathbf{M}_{n\times n}$ with $m_{i,i} = \bar{s}_i$.
- Let $\mathbf{Q}_{n\times n}$=$\mathbf{M}\cdot\mathbf{P}$.
- Compute $\mathbf{V}_{n\times n}$=$(\mathbf{I}-\mathbf{Q})^{-1}$.
- Set $\bar{S} = v_{1,n} s_n$.
- Then $S = 1 - \bar{S}$.

The matrix $\mathbf{V}_{n\times n}$ contains visit statistics, where $v_{i,j}$ represents the mean number of times a passenger visits station j given that they enter the checkpoint at station i. Because an absorbing state can only be visited zero or one time during the screening of a passenger, it is a Bernoulli random variable with average probability of success given by $v_{i,n} \leq 1.0$. Thus, $v_{1,n}$ represents the probability of reaching the baggage pickup station starting from the check-in station with no threat detected. Therefore, $v_{1,n}$ multiplied by $\bar{s}_n$, the probability station n fails to detect a threat, represents the probability the checkpoint fails to detect a threat $\bar{S}$. Thus, checkpoint security is simply $S = 1 - \bar{S}$.

B. *Performance Analysis*

Traditional performance models [5] quantify the number of passengers screened per unit time. In this paper, we quantify performance as the percentage of passengers that can clear a security checkpoint before their train departs. Performance is commonly assessed using queuing theory, which is efficient and effective for such analysis. However, it requires restrictive assumptions that are often violated in practice. For example, the passenger arrival process needs to follow the well-known exponential distribution which implies a constant arrival rate. Passenger arrivals at mass transit, however, may not follow the exponential distribution. Passenger arrivals will exhibit temporal variations, often peaking during the rush hour, and waning at other times. Analytical queuing models cannot flexibly characterize such variations, and hence, cannot produce accurate estimates of screening performance.

We develop a simulation model to consider time-varying trends in passenger arrivals. In this approach, passengers can arrive at a checkpoint consisting of n screening stations according to an arbitrary stochastic process $\lambda(t)$. Similar to the security model, the one-step transition probability matrix $\mathbf{P}$ of the DTMC controls the flow of passengers among stations, which is determined by the checkpoint layout and the decision probabilities $\mathbf{X}$. The vector $\boldsymbol{\mu}$, with element μ_i represents an arbitrary service time distribution describing the wait time of a passenger at station i. We denote m as the total number of passengers that will arrive at a checkpoint for a particular train. Fig. 2 shows the steps of the simulation procedure:

- Step 1 simulates the vector of arrival times $\mathbf{T}^a$ according to the arrival process [6].
- Step 2 enqueues all m passengers at station one within the checkpoint.
- Step 3 checks the completion time of the passenger at the front of each queue $1 \leq i \leq n$ to determine the passenger that moves next.
- Step 4 removes this next passenger k from the front of queue i.
- Step 5 determines the station j to which passenger k moves after finishing at station i according to the transition probability matrix $\mathbf{P}$.
- Step 6 tests if the destination station j is an absorbing station.
- Step 7 simulates t_k^j, the time at which passenger k will depart station j as follows. If there are no other passengers at station j, the completion time of the passenger is simply the time at which they completed service at station i, t_k^i, plus the randomly generated time sampled from μ_j for the time spent waiting at station j. However, if other passengers are at station j the completion time of passenger k is the randomly

generated time sampled from μ_j plus the completion time of the passenger at the end of queue *j*.

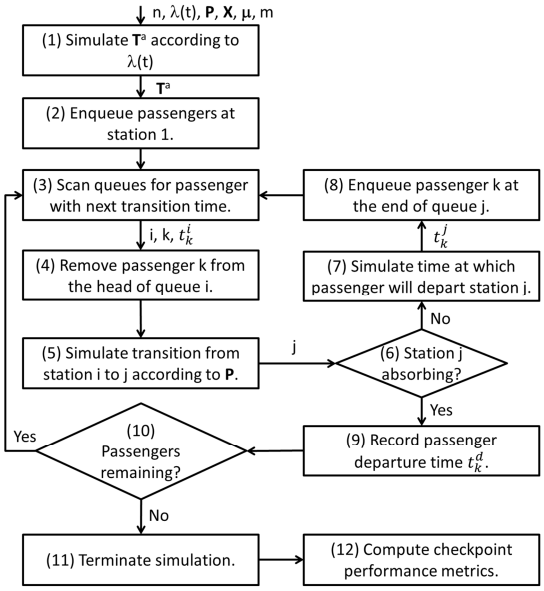


Figure 3. Checkpoint simulation procedure.

- Step 8 enqueues passenger *k* at the end of queue *j* and returns to Step 3 to determine the next passenger to move.
- Step 9 records t_k^d, the time passenger *k* departs the checkpoint after having completed screening.
- Step 10 checks to see if all *m* passengers have departed the checkpoint and returns to Step 3 if passengers remain. If no passengers remain, Steps 11 and 12 terminate the simulation and compute performance metrics of the checkpoint, which are described below.

By tracking the vector of passenger arrival times $\mathbf{T}_a = \langle t_1^a, \ldots, t_m^a \rangle$, the times at which passengers depart their present screening station t_k^i, and the vector of times at which the passengers depart the screening checkpoint $\mathbf{T}_d = \langle t_1^d, \ldots, t_m^d \rangle$, it is possible to calculate the number of passengers at each station at time *t* and the number of passengers in the checkpoint at time *t*. We can also determine the time spent in the queue by computing the difference $t_k^d - t_k^a$ for each passenger and then plot completion times as a function of the arrival times. We compute the fraction of passengers that miss their train because they fail to pass through the checkpoint in a timely manner.

IV. Illustrations

This section demonstrates the security and performance assessment techniques through a series of examples. For both attributes, we initially demonstrate how to quantify the metric, followed by an illustration of how the sensitivity of the metric to various parameters of the layout and constituent technologies can be analyzed.

A. *Security Analysis*

This example quantifies the security of the station layout shown in Fig. 1, using the transition matrix **P** in Table I, where element *(i,j)* denotes the probability that a passenger moves to station j, upon the completion of screening at station *i*.

TABLE I. Transition Probabilities Among Stations

i\j	c	x	a	o	w	P
(c) Check-in	0	1.	0	0	0	0
(x) x-ray	0	0	$\bar{x}_1 + x_1\bar{x}_2\bar{x}_3$	$x_1\bar{x}_2x_3$	x_1x_2	0
(a) AIT	0	0	0	x_5	0	$\bar{x}_5$
(o) Opt-out	0	0	0	0	0	1.
(w) WTMD	0	0	0	x_4	0	$\bar{x}_4$
(p) Pickup	0	0	0	0	0	0

Here x_i correspond to the decision points described in Section II. The sequence of matrix operations from Section 2 produces the following expression for checkpoint security.

$$S = 1 - \big((x_1x_3 + x_1x_2x_3)\bar{s}_c\bar{s}_x\bar{s}_o + (\bar{x}_1 + x_1\bar{x}_2\bar{x}_3)(1 - x_5 + x_5\bar{r}_4)\bar{s}_c\bar{s}_x\bar{s}_a + x_1x_2(1 - x_4 + x_4\bar{s}_4)\bar{s}_c\bar{s}_x\bar{s}_w\big)\bar{s}_p. \quad (1)$$

Equation (1) expresses checkpoint security in terms of the decision points and detection probabilities of the stations. Thus, it is possible to evaluate checkpoint security for different types of threats and decision probabilities. For example, when a passenger conceals an object under clothing, the check-in, carry-on baggage x-ray machine, and baggage pickup stations have no chance of detecting this threat. Hence, s_c, s_x, and s_p are set to *0*. AIT will be the most effective at detecting this hidden threat, followed by manual screening at the opt-out station, while the WTMD will exhibit the lowest probability of detection. Thus, the securities of these three stations are set to s_a=*0.9999*, s_o=*0.99*, and s_w=*0.9* to reflect their relative effectiveness. We set the probabilities of the five decision parameters to nominal values shown in Table II.

TABLE II. Decision Parameters

(i) Decision	Probability (x_i)
(1) Passenger selects WTMD	0.90
(2) Officer allows WTMD	0.85
(3) Passenger opts-out of AIT	0.30
(4) WTMD passenger undergoes pat down	0.10
(5) AIT passenger undergoes pat down	0.05

Table II indicates that most passengers prefer and are allowed to undergo WTMD screening. Approximately *30%* of passengers selected for AIT screening opt out. Furthermore, one in ten passengers screened by WTMD will also be screened manually, but only one in twenty passengers going

through AIT require manual screening. These values are chosen solely for the sake of illustration. In practice, detection and transition probabilities may be determined from measurements made in transportation security laboratories and operational environments. For these parameters, Equation (1) computes that the threat detection probability is *0.9306*. This illustrates that even though the AIT machine can detect threats with a higher probability, passenger preference for WTMD can significantly lower checkpoint security.

Realistically, the detection probabilities of certain technologies cannot be improved beyond a certain threshold. For example, WTMD may have inherently low detection probability for most concealed, non-metal threats. Thus, Equation (1) suggests that an alternative method to improve security is to boost the probability that passengers select modern screening technologies. We thus analyze the sensitivity of checkpoint security to decision parameters using Equation (1). These parameters include the probability that a: (i) passenger selects WTMD (x_1); (ii) security officer allows a passenger to undergo WTMD screening (x_2), and (iii) passenger selected for AIT screening opts-out (x_3). These probabilities were varied individually in the range (0,1), while holding all the other parameters at their values in Table II.

Fig. 4 illustrates that a significant improvement in checkpoint security could be obtained by eliminating the possibility passengers choose WTMD ($x_1 = 0$), which increases detection probability to *0.9999* (4 nines). A strategy that selects every passenger wishing to undergo WTMD for AIT screening increases detection probability to *0.9972* (2 nines) [7] while eliminating passenger opt out shows the smallest improvement of 0.*9311*. This analysis quantitatively confirms that passenger preference for WTMD over AIT lowers checkpoint security significantly. Therefore, passenger aversion to AIT must be decreased, which may be achieved using two possible strategies. The first approach is to mitigate health and privacy concerns through public education. A second method is to select more passengers for AIT screening (decreasing x_2), to create a learning effect through passenger familiarity.

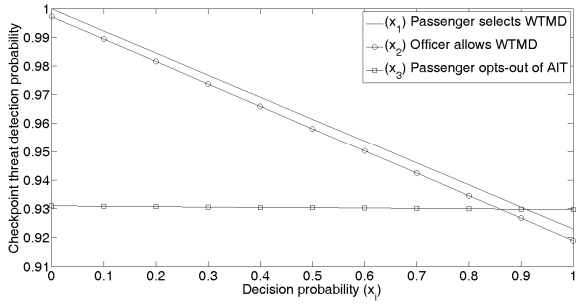


Figure 4. Sensitivity of security to decision parameters.

B. *Performance Analysis*

This example compares the performance of the current turnstile configuration in Fig. 1 with the rigorous passenger screening checkpoint in Fig. 2 using the simulation model. We consider *m=100* passengers arriving for an 8:00am train according to a normal distribution with mean $\mu = -20$ and standard deviation $\sigma = 6$. The mean indicates that the passengers arrive on an average *20* minutes prior to the departure of the train, while the standard deviation accommodates passengers arriving more conservatively, *30* minutes or more in advance of the departure time. It also accounts for late and seasoned passengers who arrive just minutes before departure. According to these parameters, approximately *99%* of the passengers will arrive sometime in the interval $\mu \pm 3\sigma = (7{:}22am, 7{:}58am)$. Although we use the normal distribution for illustration, it can be determined empirically based on the data collected by the turnstiles while stamping tickets.

We assume that *80* passengers ($\mu_h = 80$) can walk down the hallway leading to the turnstiles per minute, passengers get in line at one of the three turnstiles with equal probability ($x_i = 1/3,\ i = \{1, 2, 3\}$), and the time required for the computer to read and stamp the ticket follows an exponential distribution with an average time of *3* seconds, or twenty passengers per minute ($\mu_t = 20$). The decision parameters of the passenger screening checkpoint are set to the values in Table II, while Table III provides the service rates of the passengers per minute for each station in the security checkpoint.

TABLE III. CHECKPOINT STATION RATE PARAMETERS

(i) Station	Rate (μ_i)	(i) Station	Rate (μ_i)
(h) Hallway	80.0	(o) Opt-out	3.0
(c) Check-in	6.0	(w) WTMD	4.0
(x) x-ray	4.0	(p) Pickup	5.0
(a) AIT	7.5		

Fig. 5 shows the results of a single experiment. The first passenger arrives approximately 35 minutes early, while the last passenger arrives just five minutes before the train departs. We fed the same sequence of arrival times to the simulation models of both the turnstile and screening checkpoint. The completion times under the turnstile model indicate that passengers quickly pass through and continue on to the train. A small slowdown can be seen slightly after 7:40am. The arrival distribution reaches its maximum at that time causing many passengers to arrive about twenty minutes before departure waiting at the turnstiles. However, the maximum wait time never exceeds 1 minute and no passengers miss the train. Under the screening checkpoint model, however, the last passenger clears the checkpoint over an hour after the train departure and only *40* of the *100* passengers can clear the checkpoint to board the train.

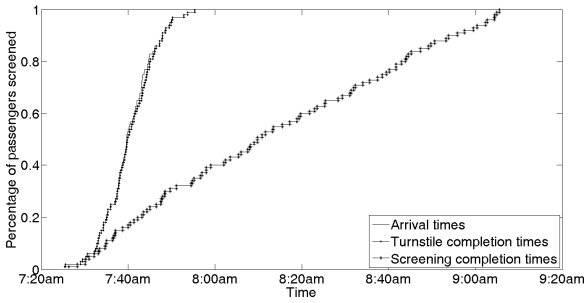


Figure 5. Comparison of turnstile and screening completion times.

The difference between the arrival and wait time grows because the time needed for passengers to clear the checkpoint is greater than their arrival rate. This is consistent with a well-known tenet from queuing theory [5], which states that the queue will be bounded only if arrival rate at the checkpoint is greater than its service rate. This property is not satisfied because the time-varying arrival process peaks at 20 minutes prior to the train's departure.

Fig. 6 shows the length of the line at the check-in station as a function of time, revealing that this check-in desk is the bottleneck. The arrival rate at *7:30am* is not sufficiently high for the queue to grow unbounded. However, the queue begins to grow in the interval between *7:30am* and *7:35am* because passengers begin to arrive faster than they can be checked in. The increase in the queue length accelerates in the time interval *(7:35am,7:45am)* since the normal distribution characterizing passenger arrivals peaks at *7:40am*. As the rate of arrival decreases in the interval *(7:45am, 7:50am)*, the queue length levels off. However a delay with one passenger at *7:50am* causes the queue to grow yet again. After *7:55am*, all passengers have arrived and the queue empties at an approximately constant rate.

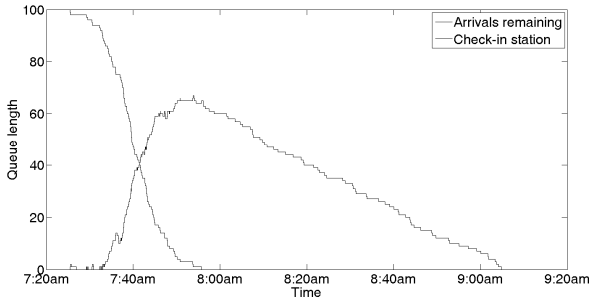


Figure 6. Passenger check-in queue length.

The bottleneck created by the check-in desk suggests that manual verification of passengers' identities is infeasible. Moreover, as noted earlier, introducing additional check-in stations is not feasible because of its cost. Thus, in order to avoid eliminating identity verification, faster technologies such as biometrics can be used. An experiment which removed the check-in station from Fig. 1 and allowed passengers to proceed directly to the baggage station shifted the bottleneck to the baggage station, suggesting that baggage scanning also needs to be expedited.

The results of the above experiment revealed that imposing rigorous aviation security screening on mass-transit could create serious delays. Next, we demonstrate how the approach could be used to quantitatively compare the impact of improvements in individual stations. Usually, a single simulation experiment does not provide metrics with sufficient accuracy, so it is customary to compute the average metrics over several runs. We thus repeated the simulation with the station parameters in Table III 10,000 times, which indicated that on an average 34 passengers (approximately one third) can be cleared before the train departure. Having established this baseline, we next doubled the completion rate of each station in Table III one at a time and estimated the average number of passengers that would be cleared before departure. Table IV reports the results of this analysis for each station in the checkpoint and ranks the improvements according to the increase in the number of passengers that make their train.

TABLE IV. SENSITIVITY OF STATION PERFORMANCE

Station	Increase	Rank	Station	Increase	Rank
Check-in	2.298	1	Opt-out	0.067	6
x-ray	0.377	2	WTMD	0.290	3
AIT	0.170	5	Pickup	0.226	4

This analysis quantitatively confirms that accelerating check-in would produce the greatest improvement in passenger throughput followed by the x-ray machine, WTMD, and pickup stations respectively. Examining Fig. 2, all passengers must pass the check-in, x-ray, and pickup stations, potentially creating bottlenecks. Intuitively, Table III might suggest that the x-ray machine is the biggest bottleneck because it can service only four passengers per minute. The simulation results, however, indicate that the check-in desk creates the greatest slowdown because it is the first one in the network of stations. This causes the long line in Fig. 6 suggesting that the earlier stations are more critical to checkpoint performance. Improvements in WTMD rank higher than AIT because a larger percentage of the passengers will prefer and ultimately undergo WTMD inspection. AIT ranks higher than opt out for similar reasons. Substituting the probabilities from Table II into the transition matrix in Table I indicates that on an average 76 of the 100 passengers go through the WTMD, while the AIT station and opt-out stations are visited by 19 and 5 passengers respectively. Thus, the criticality rankings given in Table IV are influenced by the service rates of the stations given in Table III and the average number of passengers visiting a station. The approach can therefore quantify the impact of each station on the performance of the checkpoint despite these complex factors influencing a station's importance.

V. POLICY RECOMMENDATIONS

This section offers policy recommendations based on our observations and lessons to improve security and balance performance for mass-transit screening. Specifically:

- Introducing aviation-style screening checkpoints into mass-transit could dramatically slow passengers causing several passengers to miss their train.
- Including alternative technologies like WTMD and opt out can significantly lower security.
- Increasing passenger acceptance of AIT will offer the highest improvement in security.
- Technologies to verify passengers' identity and screen baggage must be accelerated.

These lessons suggest that, to make mass transit screening effective and efficient, older screening methods such as WTMD and opt out must be phased out by increasing acceptance of AIT. Improved education to mitigate health and privacy concerns and selecting a larger number of passengers for AIT screening to increase their familiarity may accelerate this acceptance.

VI. Conclusions and Future Research

This paper presents techniques to quantify the security and performance of passenger screening checkpoints and applied them to assess the impact of imposing screening on mass-transit. The results reveal that the performance of screening technologies must be improved and passenger aversion to newer and faster technologies must be addressed to ensure the feasibility of screening for mass-transit. Our future research will enrich the security and performance assessment techniques by developing sophisticated modeling capabilities. For example, the model may be enhanced to incorporate batch or grouped arrivals of passengers, such as a family traveling together. To enhance the scalability of the approach and improve the accuracy of the metrics, more efficient data structures will be explored. We will use these enhanced simulation techniques as the basis of an optimization framework to identify investments in technology improvement offering the greatest improvements in security and performance.

Acknowledgment

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2008-ST-061-TS002. The authors would like to thank Steve Curtain for sharing information on the Fairfield Metro Center and hosting a site visit.

Disclaimer

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

References

[1] List of terrorist incidents involving railway systems. In *Wikipedia*. Retrieved June 8, 2012, from Http://en.wikipedia.org/wiki/List of terrorist incidents involving railway systems.

[2] J. Burgoon, D. Twitchell, M. Jensen, T. Meservy, M. Adkins, J. Kruse, A. Deokar, G. Tsechpenakis, S. Lu, D. Metaxas, J. Nunamaker, and R. Younger, "Detecting concealment of intent in transportation screening: A proof of concept," *IEEE Transactions on Intelligent Transportation Systems*, vol. 10, no. 1, pp. 103-112, 2009.

[3] M. Tambe, Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned. Cambridge, UK: Cambridge University Press, 2011.

[4] K. Severin, C. Spinner, M. Calvo, D. Doran, and L. Fiondella, "Reliability and performance assessment of an aviation security screening checkpoint. In *Proc. of International Conference on Reliability and Quality in Design (ISSAT 2012)*, Boston, MA, July 2012.

[5] K. Trivedi, Probability and Statistics with Reliability, Queuing and Computer Science Applications. New York, NY: John Wiley & Sons, Inc., 2002.

[6] L. Leemis and S. Park, Discrete Event Simulation. Upper Saddle River, NJ: Prentice-Hall, 2006.

[7] A. Shapiro, "An ultra reliability project for NASA," In *Proc. of IEEE Aerospace Conference*, Big Sky, MT, March 2005.

ABOUT THE AUTHORS

Lance Fiondella *- lfiondella@engr.uconn.edu*

Swapna Gokhale *- ssg@engr.uconn.edu*

Department of Computer Science and Engineering

University of Connecticut

Storrs, CT 06269, U.S.A

Nicholas Lownes *- nlownes@engr.uconn.edu*

Michael Accorsi

Department of Civil and Environmental Engineering

University of Connecticut

Storrs, CT 06269, U.S.A

© 2013 IEEE and published here with permission. *Homeland Security Affairs* is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of this article is expressly prohibited without the written consent of the copyright holder, the Institute of Electrical and Electronics Engineers (IEEE). *Homeland Security Affairs* is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).

http://www.hsaj.org

Intelligent Radiation Sensor System (IRSS) Advanced Technology Demonstrator (ATD)

Daniel A. Cooper, Robert J. Ledoux, Krzysztof Kamieniecki, Stephen E. Korbly, Jeffrey Thompson, James Batcheler, Shirazul Chowdhury, Neil Roza, James Costales, Vijaya Aiyawar

Passport Systems, Inc.
N. Billerica, MA, USA
cooper@passportsystems.com

***Abstract*—In response to the Domestic Nuclear Detection Office's (DNDO) BAA 09-102 Passport Systems, Inc. of Billerica, MA has developed and tested a prototype system of networked portable spectroscopic radiation detectors designed to improve the detection, localization, and identification of potential radiological threats. A system of this nature is primarily targeted to situations where it is not feasible to direct traffic through portal radiation detection systems, e.g. large events, search team objectives, etc. The capability to intelligently network individual portable detectors and fuse their data using advanced algorithms and COTS hardware has been shown within this program to significantly increase the effectiveness of an assortment of portable radiation detectors in a variety of NORM (naturally occurring radioactive material) backgrounds. An overview of current work will be provided in two parts: 1) A review of the system design, including trade space analysis, of both the hardware and algorithmic components; and 2) Presentation of data and results to date focusing on the improvement afforded by the networked data fusion**

Keywords-component; Networks, Nuclear Physics, Intelligent Systems, Decision Support Systems, Radiation Detectors, System Analysis & Design, Gamma-Ray Spectroscopy, Distributed Tracking, Distributed Algorithms, Signal Detection, Maximum Likelihood Estimation, Scintillation Detectors

I. INTRODUCTION

The use of human portable radiation detectors (HRPLs) has become more common in recent years among first responders, customs agents, and HAZMAT teams, in addition to their traditional use by radiological search teams, to aid in their mission to ensure public safety. Such a trend is expected to continue considering the ongoing and increasing specter of the use of radiological materials for terrorist threats.

Interest in the use of these devices can be further illustrated by the fact that the Domestic Nuclear Detection Office (DNDO) has devoted considerable resources for research by various companies to develop man-portable Intelligent Personal Radiation Locators (IPRLs) capable of detecting, measuring, locating, and identifying radiological threats. As capable and useful as each of these devices either is, or is expected to be, their effective range is still limited by their small form-factor and the basic physics governing the detection of radiation. One method by which the performance of man-portable radiation detectors can be enhanced in an operational setting is through the networking and fusion of data from several devices in a localized region-of-interest. With multiple devices all sharing data, a team of operators can leverage that integrated collection of devices to increase overall system sensitivity (through total increased detector volume) and also to enable new capabilities which emerge from the distributed nature of the detector network (e.g. source localization).

By networking radiation detectors, not only would their joint, integrated performance be expected to surpass that of the individual detectors for sensitivity and coverage, but the networked system would effectively become a new tool to solve challenges not addressed by current technology. Portal radiation monitors, despite some limitations, have become useful equipment at locations where traffic can be funneled through a small area – such as major ports and border crossings. However, in situations where such restrictions are not possible, such as at major events or within urban cores, a networked system of small, unobtrusive radiation detectors utilized by a team of operators could provide for the detection, localization and identification of potential radiological threats in those less controlled environments.

With such reasons in mind DNDO issued BAA 09-102 Advanced Technology Demonstration (ATD) for Intelligent Radiation Sensor System (IRSS) for the purpose of demonstrating the feasibility of a cost-effective system of networked radiation detectors designed from COTS and OEM components and using advanced data fusion algorithms to make optimal use of the data from those networked detectors. This program was focused on algorithm development, system integration, and prototyping to prove out the advanced technologies required to improve detection, localization, and identification of radiological sources using intelligently networked sensors.

The IRSS program was a 2.5 year four-phase effort culminating in the ATD. This paper summarizes the design, development, integration, and testing efforts of Passport Systems, Inc. during the execution of the IRSS ATD program.

II. System Overview

The proposed IRSS system overview is shown in Figure 1. The major components pictured are the detection device (DD), the base control unit (BCU), and the reach-back node. For the purposes of the ATD the reach-back node capability to alert a central authority via a reach back network was not critical to demonstrating the effectiveness of the mesh network and was not tested. The remaining system components are described below.

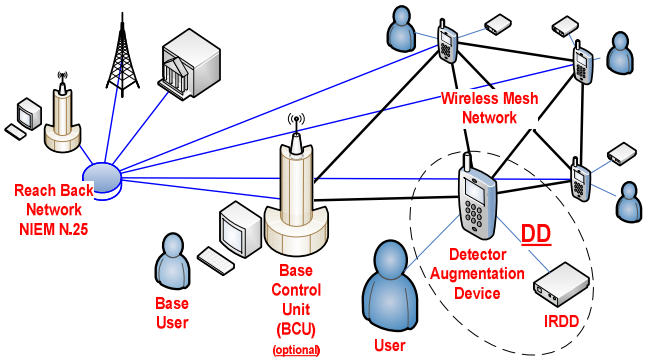


Figure 1: IRSS System Overview

A. Detection Device (DD)

The detection device (DD) is a key system element of IRSS and, as highlighted in Figure 1, is comprised of two parts: 1) the detector augmentation device (DAD) and 2) the individual radiation detection device (IRDD). The two devices are loosely coupled to maintain flexibility and upgradability. The DDs themselves will automatically set up and maintain a wireless *ad hoc* mesh network, capable of automatic reconfiguration when necessary and providing data throughout the system, including to the optional BCU.

The IRSS program was not a hardware development effort; however, it was determined early in the program that a true off-the-shelf radiation detector was not available that met the program requirements – including full spectroscopic capability, full interoperability with external devices (i.e. the DAD), and cost restrictions. Therefore, a portable prototype device had to be designed and built to support the program requirements. The IRDD consists of COTS and OEM components – including signal processing electronics, HV supply, battery, photo-multiplier tube, and scintillator crystal – that were integrated into a modular, portable system. This modular design philosophy allows for plug-and-play of various sensors with unique characteristics (e.g. sensitivity and spectroscopic resolution) depending on operator need and component availability. Indeed, during the course of the program it was determined that evaluation criteria could best be met through the availability of two detector sizes. These are shown in Figure 2. The active detection elements are both NaI(Tl) crystals, but two different sizes were utilized: 2"×2" and 1"×2" [dia. × length]. The modular design facilitated this mid-program decision with no schedule or design impact. The design modularity, including the decision to use standard interfaces (e.g. USB) also facilitated the easy integration of external components – such as the differential GPS antenna visible in Figure 2 – when determined necessary during initial program testing.

Figure 2: IRSS DDs. The 2"×2" device is on the left and the 1"×2" device is on the right

B. Base Control Unit (BCU)

The BCU was designed as an optional component of the final system. For the purposes of the ATD it provided the important capability for data storage and performance characterization as well as post-event evaluation. The BCU was implemented using a Toughbook™ ruggedized laptop. For all intents and purposes the BCU was simply another node in the network – albeit one configured in this instance without an attached detector. The BCU ran the same data collection and analysis software developed for the DDs. The only difference was that an enhanced GUI interface was designed for the BCU to allow for improved monitoring and control during system testing activities.

As part of an operational system a BCU provides a means for a local command authority to improve situational awareness, direct search teams, and enable the use of more complex algorithms in situations where the portable units are inadequate. However, the BCU is not required for the network to function properly. The IRSS system was designed this way to ensure network robustness and avoid any single points of failure in the system.

C. Detector Augmentation Device (DAD)

In many ways the DAD was the focus of design work performed for this program. The DAD was implemented by leveraging existing Android smartphone technology, and it provides all the functionality to interface with the IRDD and the operational user through an appropriate, configurable GUI. The DAD also provides a platform for all the communications and computation.

The DAD is responsible for establishing and maintaining a robust *ad hoc* network. This is accomplished using the native WiFi (IEEE 802.11b) capability on the smartphone and open-source mesh network applications. Data is transferred around the network to all connected nodes – through multiple hops if

This program in funded by the U.S. Department of Homeland Security Domestic Nuclear Detection Office (DNDO) under contract HSHQDC-09-C-00123.

necessary – so that all current data is available to every node at each processing interval.

The DAD is also the primary computation engine and hosts all of the advanced algorithms responsible for integrating shared data, estimating background and radiological source levels, and making decisions concerning the detection, localization, and identification of those sources. All the data fusion and processing is done on every DAD separately using all the available data from the connected nodes. This architecture has the advantage of ensuring that there is no single point-of-failure for the system. Every detector calculates the best solution based on all the available information, whether it is data from only that detector or includes data from other near-by detectors. The significant computations required by the advanced algorithms, described below, were all carried out on the smartphone processor.

III. IRSS Algorithms

The primary focus of the IRSS program was to demonstrate that networked systems are capable of improved performance compared to individual detectors and to quantify that performance advantage in a quasi-operational setting. The development and testing of advanced data fusion algorithms which improve detection, localization, and identification of radiological sources using a networked system was the central program goal, despite the effort that went into the development of appropriate prototype detection units.

The advanced algorithms fall into two separate development categories: background estimation and source estimation, each of which is described below.

A. Background Estimation

Background estimation is considered important for two reasons. First, for the vast majority of time any given detector is measuring only NORM (naturally occurring radioactive material) background so it is important to understand and characterize it well to avoid false positive readings – particularly as NORM can vary significantly over short spatial intervals. Second, if the background is measured with high certainty within an area then the system as a whole will be more sensitive to deviations, e.g. radioisotope source signatures, from that estimated background.

The IRSS background estimation is a hybrid algorithm that provides a continuous estimate of the NORM radiation levels. The first part of the algorithm maintains a background map of measurements averaged across the full network of detectors. Using this map, an estimate of the local background is calculated along with a confidence based on the total measurement time for all detectors and distance of those measurements from the current location. An example of this networked background mapping is shown in Figure 3, where three detectors mapped out the background radiation levels of a park in downtown Boston, MA. The data, represented by an arbitrary, normalized count rate scale on the right, show that even over this small area the measured radiation levels vary by more than a factor of two. In order to account for this background variation in the absence of background estimation, detection thresholds would have to be set near the highest levels to avoid false alarms and thereby miss detection of potentially small signals. Such background estimations not only help real-time system performance but can also be saved for future reference and comparison.

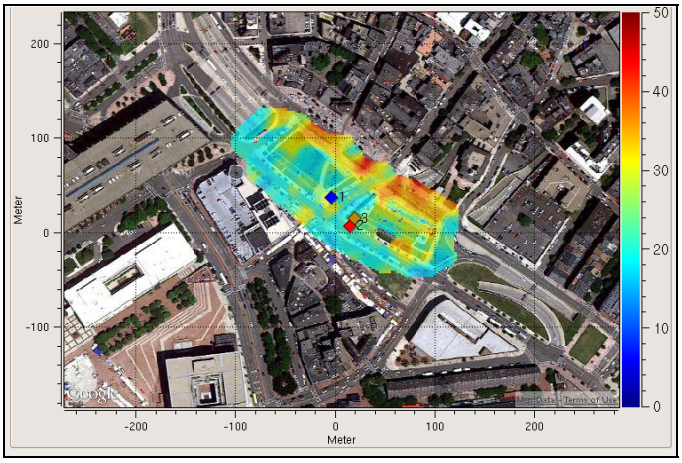


Figure 3: NORM background measurements using three networked detectors on the Rose Kennedy Greenway Park in Boston, MA

When no background data exists, either from neighboring detectors or from previous measurements, the system must still estimate the local background. This is done by comparing the estimated background spectrum to a linear superposition of basis functions determined through analysis of data collected in a number of background environments. The contributions of the spectral components are constrained by count rates in sections of the spectrum (ranging from 60-3000 keV) that are not expected to contain source signals. An example of background from various materials is shown in Figure 4 where the top six curves show both measurements and the scaled-component fit for a number of different background environments with nearly a factor of ten variation in overall radiation levels.

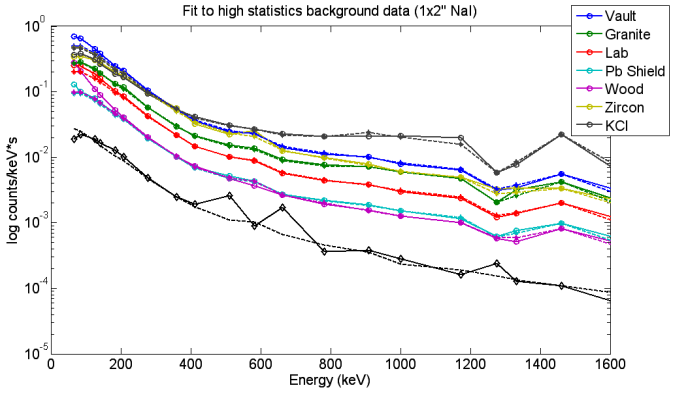


Figure 4: Scaled-component background measurement (solid lines) and fit (dotted lines) results. The top six curves represent various backgrounds. The bottom curve includes both ^{137}Cs and ^{22}Na sources

The fit for the background cases in Figure 4 (dotted lines) is quite good. The bottom curve illustrates the fit for a measurement including ^{137}Cs (662 keV) and ^{22}Na (511 and 1275 keV) photopeaks. Again the fit to the expected background levels is good and the deviation from that estimate at the expected source energies is clear.

B. Source Estimation

The goal of the source estimation algorithms developed for the IRSS program is to provide detection, localization and

identification of radiological sources. Detection and localization of sources are achieved via a sampled Bayesian inference method while the identification functionality is implemented separately using a peak-finding and peak-matching technique.

In order to perform source detection and localization, the full probability density function (PDF) for the source is approximated using the number of counts in each detector in the network and accounting for Poisson statistics and the $1/r^2$ relation between count rate and source-to-detector distance. Visualization of this PDF is achieved through uniform sampling of the log-likelihood map. Figure 5 shows an simulation of such a log-likelihood map where the log-likelihood function has a maximum near the actual position of the simulated source. Figure 6 illustrates the evolution of the PDF over time as increased statistics are gathered from all the detectors and the solution becomes more constrained. Detection is a result of comparing source hypotheses against null hypotheses – the likelihood ratio of the two (referred to as "fidelity") needs to exceed a pre-determined threshold defined by required sensitivity and false alarm rates. Source localization occurs naturally by identifying the spatial location of the peak likelihood. For the IRSS program potential source motion (both direction and magnitude) are included in the hypothesis space so source tracking is also a natural result of the Bayesian estimation.

During integration testing the application of the Bayesian inference algorithms showed a significant improvement over the individual detectors. Figure 7 illustrates laboratory results from a four detector network of 1"×2" detectors at various radial distances (D) evenly distributed around an 8.9 μCi ^{137}Cs source. The source was exposed after 60 seconds and in the nearest three cases the network detected the source at least two times faster than any individual detector. As the detectors moved farther away (D = 233 cm) the network still outperformed the individual detectors but the required detection threshold was not crossed during the time displayed in Figure 7.

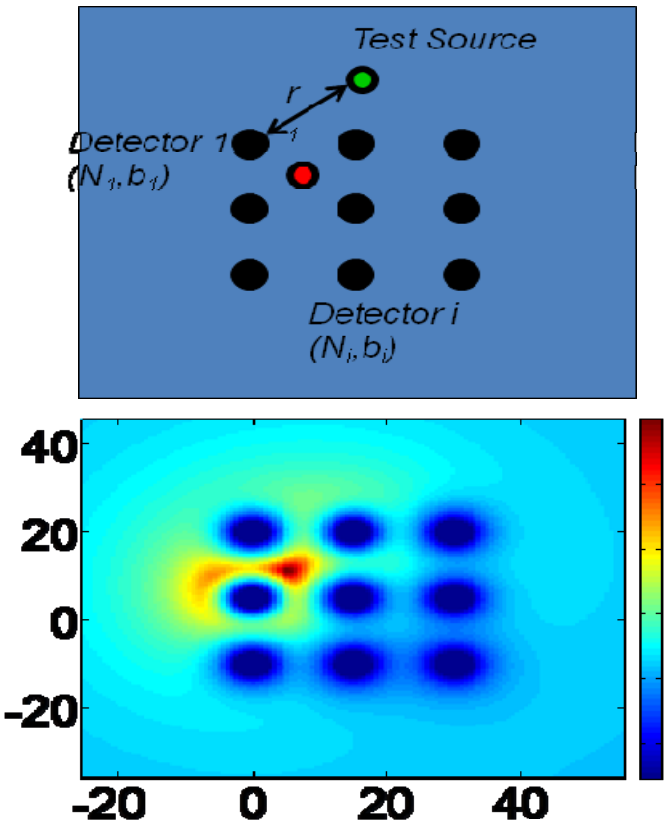


Figure 5: Log-likelihood map for sample scenario of one stationary radioactive source and nine regularly spaced detectors. Actual source location at the red circle in the top plot

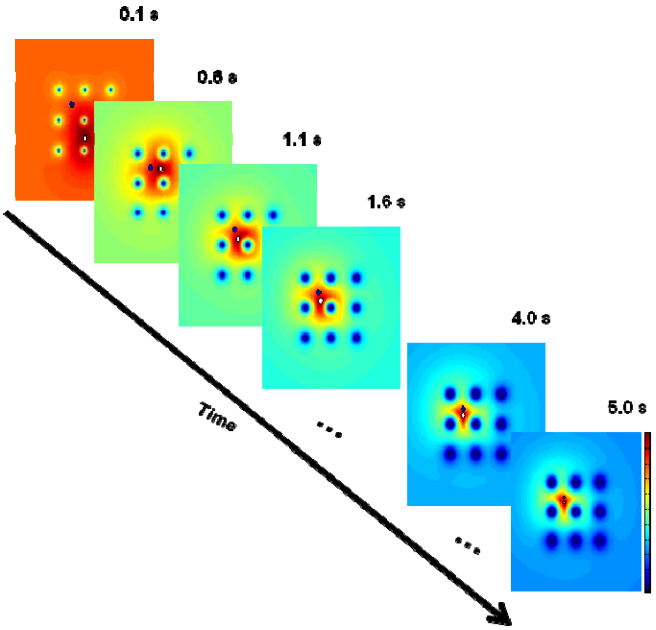


Figure 6: Time evolution of the log-likelihood map as statistics are gathered and confidence and localization improve

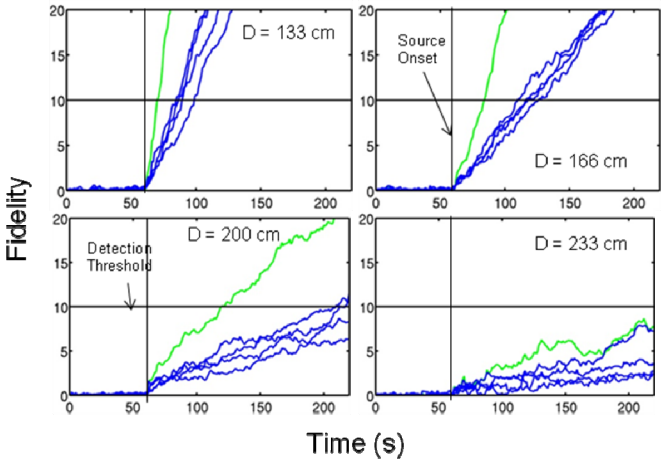


Figure 7: Network detection results for a 4 detector network at various radial distances from a central ^{137}Cs source. Source was exposed at 60 seconds. Network results are in green. Individual DD results are in blue

These same data fusion algorithms have also been shown to enable detection of weak signals while maintaining a low system false alarm rate. Typically, the overall false alarm rate for a set of N independent detectors would be N times the individual rate. However, by fusing and processing all of the available data at each node the system false alarm rate can be kept low while maintaining sensitivity to weak signals. Figure 8 illustrates simulation results for a weak source moving at walking speeds (1.6 m/s) through a network of nine detectors with an inter-detector spacing of 21 m.

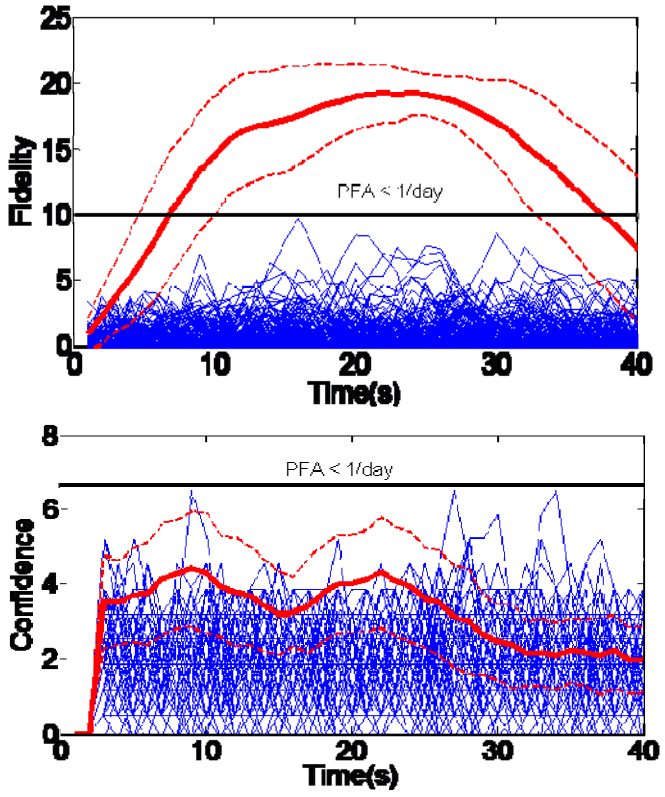


Figure 8: Detection confidence for networked and non-networked detectors for a very weak moving source. The red line is the average detection metric with the source present. The blue lines are source absent trials. The dashed red lines indicate ± 1 standard deviation

The top and bottom plots in figure show the performance of the networked and individual detectors, respectively. For both sets of trials the detection threshold was set to result in a false alarm rate < 1/day for the set of nine detectors using trials where the source is absent (blue lines). The top plot shows that the networked detectors effectively integrate the weak signal counts across multiple detectors by applying the possibility of a moving source and thereby demonstrate a higher probability of detection. In contrast, the bottom plot shows that when the individual detectors are taken separately a very low probability of breaking the detection threshold occurs before the source has moved through the detector grid.

The source tracking capability is illustrated in Figure 9. Data was collected using a grid of 15 2"×2" detectors (shown as green circles) with an inter-detector spacing of 14 m. A ~500μCi ^{57}Co source is moved through the center of the detector grid. Figure 9 overlays the sampled hypotheses (blue dots) on the full PDF to illustrate that the sampling does a good job of tracking the full solution. The red circle is the average position of all the hypotheses and is shown to track the source with reasonable accuracy. It should be noted that each of the detectors is non-directional and provides no position estimation for a detected source. It is only through fusion of distributed measurements from spatially dispersed detectors that the capability for source localization and tracking emerges.

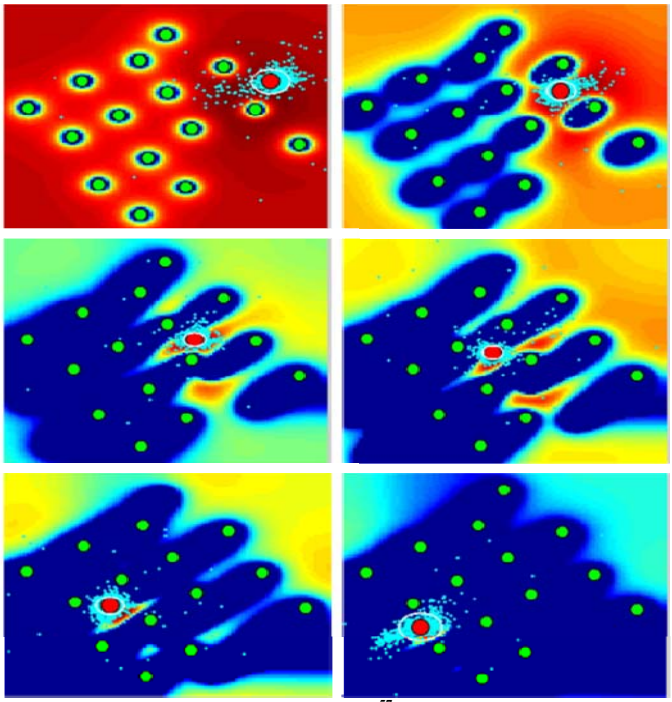


Figure 9: Live tracking experiment of a ^{57}Co source. Green circles are detectors. Blue dots are source position hypotheses. The red circle is the estimated source position and the white ellipse represents the positional uncertainty. The colored background is the full PDF.

C. Identification

Spectroscopic data from the detectors is preprocessed into separate energy bins each of which are processed through the Bayesian inference engine independently to improve computational efficiency and allow for real-time processing on the smartphone platform. These bins have been centered at the photopeak energies of expected radioisotopes, and their widths have been set by the detector resolution, to increase SNR for those potential signals. One benefit of implementing the signal

processing in this way is that the detection process itself results in a coarse identification. Detection in a given pre-defined energy bin implies the existence of that particular isotope. This is only a coarse identification capability because there may be several isotopes that emit gamma rays at energies that are too close to be resolved by the IRSS detectors utilized herein. In other words, the sources share an energy bin so there is some potential for ambiguity in the bin-based identification. To resolve this ambiguity a high-statistics identification algorithm was also implemented.

The high-statistics identification begins collecting data once detection has occurred and collects sufficient counts to develop unambiguous photopeaks in the gamma-ray spectrum. The background is subtracted via an erosion method [1] and the signal confidence is calculated on a per channel basis. Confidence is compared to a predetermined, energy-dependent threshold and high confidence peaks are compared to a standard isotope library.

This technique has several advantages over standard template matching, or deconvolution, techniques in that it is easier to add to the list of possible isotopes for identification. It is sufficient to simply know the expected photopeak energy(s) rather than having to measure the full response function for each isotope-detector pair. This was an important resource consideration for development of the prototype IRSS system. Additionally, peak-matching techniques do not require corrections for distortion in the low-energy Compton region, as does template matching, due to energy-dependent shielding effects.

The network implementation of the high-statistics identification algorithm was done at the decision-level as opposed to the data level as in the detection/localization algorithm. That is, the individual detector signal confidences were combined to get an overall system confidence. This avoids the problem of diluting accumulated spectra with data from detectors that don't see a source and thereby reducing overall SNR. However, it also means that the identification function is dominated by the detector closest to the source

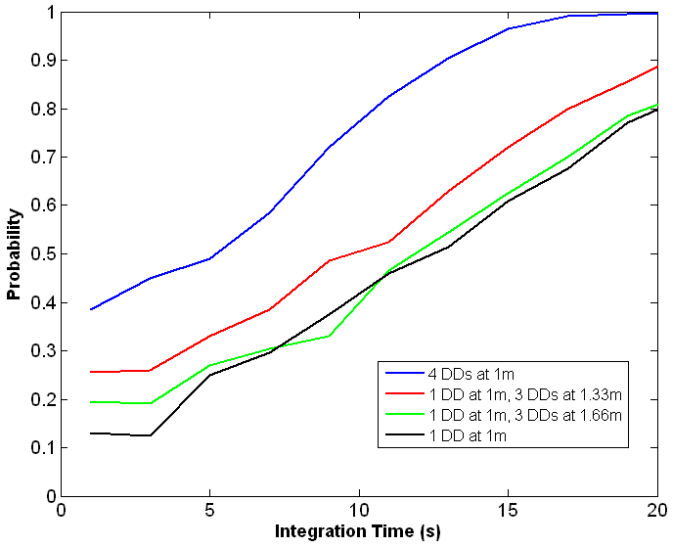


Figure 10: Probability of correct identification vs. integration time for networked and individual detectors

Figure 10 shows the probability of identifying an 8.9 μCi ^{137}Cs source as a function of integration time for measurements made by four networked 1"×2" detectors. When the detectors are equidistant from the source there is a performance increase compared to that of an individual detector, but that advantage quickly drops as three of the detectors are moved further from the source.

IV. Program Status & Conclusions

Passport Systems, Inc. has completed the IRSS ATD program as of June 1, 2012. Forty-four prototype detectors (22 each of the types shown in Figure 2) capable of sharing data through an *ad hoc* wireless network were designed, built, tested, and delivered to DNDO for the ATD, as were two BCUs. Advanced algorithms were designed and implemented to fuse and exploit the networked data, demonstrating increased performance in detection, localization, and identification of potential radioactive isotopic sources. The program has demonstrated the utility and feasibility of a robust system of man-portable networked radiation sensors using COTS/OEM components. Both government and Passport analyses of data collected at SRNL (Savannah River National Laboratory) during Phase IV characterization and evaluation activities are on-going.

Acknowledgment

This work supported by The US Department of Homeland Security Domestic Nuclear Detection Office, under competitively awarded contract HSHQDC-09-C-00123.

This support does not constitute an express or implied endorsement on the part of the Government. All claims and representations contained herein are those of the author alone.

References

[1] East LV, Phillips RL, Strong AR. "A Fresh Approach To NaI Scintillation Detector Spectrum Analysis". 1982. Nucl. Inst. and Meth. 193:147-155

ABOUT THE AUTHORS

Daniel Cooper - *cooper@passportsystems.com*

Robert Ledoux

Krzysztof Kamieniecki

Stephen Korbly

Jeffrey Thompson

James Batcheler

Shirazul Chowdhury

Neil Roza

James Costales

Vijaya Aiyawar

Passport Systems, Inc.

N. Billerica, MA, USA

© 2013 IEEE and published here with permission. *Homeland Security Affairs* is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of this article is expressly prohibited without the written consent of the copyright holder, the Institute of Electrical and Electronics Engineers (IEEE). *Homeland Security Affairs* is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).

http://www.hsaj.org

A video-based hyper-focal imaging method for iris recognition in the visible spectrum

Sriram P. Tankasala, Vikas Gottemukkula,
Sashi Kanth Saripalle, Venkata Goutam Nalamati,
Reza Derakhshani
Dept. of Computer Science and Electrical Engineering,
University of Missouri - Kansas City

Raghunandan Pasula, Arun Ross
Lane Department of Computer Science and
Electrical Engineering,
West Virginia University

***Abstract*—We design and implement a hyper-focal imaging system for acquiring iris images in the visible spectrum. The proposed system uses a DSLR Canon T2i camera and an Okii controller to capture videos of the ocular region at multiple focal lengths. The ensuing frames are fused in order to yield a single image with higher fidelity. Further, the proposed setup extends the imaging depth-of-field (DOF), thereby preempting the need for employing expensive cameras for increased DOF. Experiments convey the benefits of utilizing a hyper-focal system over a traditional fixed-focus system for performing iris recognition in the visible spectrum.**

I. INTRODUCTION

The texture of the iris is typically imaged in the near infrared (NIR) spectrum. This is because the texture of dark-colored irides is more easily discernible in the NIR spectrum rather than the visible (RGB) spectrum. However, recent work has explored the possibility of conducting iris recognition in the visible spectrum using RGB images [3], [7], [12], [13], [15]. Iris recognition using RGB images is challenging for darker irides due to the effect of melanin. Darker irides have a higher concentration of melanin that absorbs most of the visible light and the images appear dark due to the low power of the reflected light. The effect of melanin decreases significantly in the NIR spectrum thereby revealing textural patterns even for darker irides [4]. Iridal information in visible spectrum can be improved by using a controlled lighting setup to illuminate the structure of the iris and producing sufficient reflected light towards the imaging camera. However, due to the required higher intensity illumination for visible light iris captures, especially for darker eyes, the placement of such illuminators should be carefully studied in order to avoid user discomfort.

Quality of an acquired iris image is a very important metric that directly affects the performance of an iris recognition system. Image focus plays a predominant role in estimating image quality [2], [6]. Better focused images can be only acquired at the time of image acquisition and cannot be easily compensated for once the process is complete[1]. A higher focus value is preferred for better quality images. Camera's depth of field (DOF) is defined as physical depth of the volume being imaged that appears in-focus on the capture image. Another important factor in iris image quality is shutter speed, as faster shorter exposures result in less motion blur. Yet the corresponding reduced exposure times require larger camera apertures that, in turn, reduce DOF and cause the image to be partially out of focus. To make things worse, during RGB iris acquisition, the illumination level has to be high in order to better expose texture of darker irides, which in turn requires either longer exposure times (leading to motion blur) or larger apertures which lead to shallower DOFs, or both. Meanwhile, simply increasing the intensity of illuminator may result in subject discomfort and is not practical. The aforementioned opposing requirements create further challenges for visible light iris recognition.

In this paper, we propose an imaging method using a combination of focus bracketing with lateral white LED lighting as solution to overcome the aforementioned RGB iris exposure and depth of field problems. A traditional approach to increase the DOF is to increase the f-number of the lense. However, as mentioned earlier, increasing the f-number decreases the optics aperture and requires longer exposure time or higher illumination intensity. To better expose irides, especially those with heavy pigmentation, we initially allow for larger apertures. As a result, a single frame of the ocular area will be only partially in-focus. Next, multiple captures of the same ocular area are takes in rapid succession but each at a slightly different focal plane (focus bracketing technique), and the stack of images is then fused to improve overall focus. Focus bracketing, also known as hyper-focal imaging, is a technique to obtain a single sharp, high DOF image from a series of images captured at varying focal distances. In this paper, we demonstrate the benefits of this technique for RGB ocular biometrics.

Earlier work on overcoming the focus problem include [11], [14], [16] that use wavefront coding to achieve extended DOF at a fixed focus. In [10], the authors use specular reflection of the IR-LED illuminator to rapidly assess the focus of a sequence of frames acquired at varying focal lengths and select the best focused frames for iris recognition. In [5], the authors use auto-focus feature based on lens design and self-alignment to position the iris in the camera's depth of field. The system in [4] maximizes the spectral power in the middle and upper frequencies of the 2D Fourier spectrum of the acquired images in order to select the best frame for iris recognition.

In this paper we introduce a novel iris imaging platform designed to record RGB iris details in a video format by

[1]Exceptions include Lytro camera (https://www.lytro.com/camera#) and Throwable panoramic ball camera (http://jonaspfeil.de/ballcamera)

employing hyper-focal imaging and lateral white LED lighting resulting in a sharp, well exposed, and high DOF image of the eye. This overcomes the problems associated with capturing dark irides in visible light. A comparative study between single-focus and hyper-focal images is performed to demonstrate the positive effects of hyper-focal imaging in the context of visible spectrum iris biometrics.

II. Data Acquisition

A. Platform Design

We designed a hyper-focal video recording platform using focus bracketing with 30 FPS 1080p HD video. A novel technique was developed to adjust the focus of the camera lens automatically in real time by programming an Okii FC1 Arduino-based follow focus controller (Okii Systems LLC, Apex, NC) to communicate with the Canon T2i dSLR's internal motorized focus mechanism through the camera's USB port. The Okii controlled Canon T2i is mounted on a tripod setup while the subject uses a chin rest to face the lens and its attached lighting element (Figure 1). A single focus stack acquisition takes around 0.5 seconds at full HD frame rate of 30 fps. Average distance from the camera to the subject is 1.5 ft. The camera is operated at F number F5.6, an exposure time of 1/125 sec, and ISO of 800.

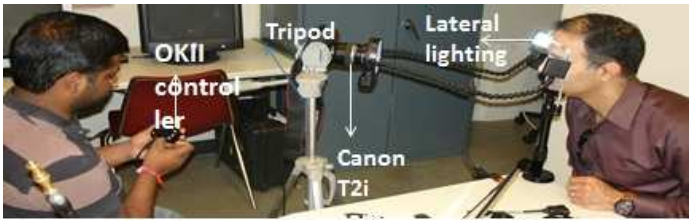


Fig. 1. The image acquisition setup that was adopted in this work. The images are acquired in a cooperative environment. Future work will include relaxing some of the acquisition constraints in order to obtain images from less cooperative subjects.

B. Optics and illumination devices

A modified Digi-Slave Flex Ring 6400 is used for illumination. This macro light is equipped with 64 oversized white LEDs, 32 LEDs in the ring (center light with 11 cm outer diameter and 7 cm inner diameter) and two flexible arms (modified to extend 50 cm long to the side of each eye) with 16 white LEDs on each pad (Figure 2). The light is used as in continuous mode to avoid photic startle. A polarizing filter film is applied to each side light pad for subject comfort. In this experiment we used only side lights for illumination and the center ring was turned off. Camera lens consisted of an EFS 50 mm, f/2.8 macro lens and an OKII micro controller.

C. Okii micro controller

Okii micro controller is a programmable Aurdino-based USB follow-focus host device connected to the camera. It is powered by Atmel Atmega328P that runs at 8MHz. The programmed device works on the principle that, when two focal points are saved, the speed of movement of the lens between these two focal points is determined by the number of steps required to move between these two focal points. The controller may be operated in small, medium and large focus step modes that correspond to the rate of motorized focus change introduced in the camera lens. Medium setting was used in this acquisition protocol. A button on the OKII controller is programmed to move the lens from a focal plane around subject's tip of the nose, which is defined as point A, to the vicinity of the ear, which is defined as point B.

Fig. 2. Lateral LED illumination setup

III. Data collection protocol

Data was collected from 46 volunteers based on IRB protocol 11-57e. Image stacks were collected over two sessions for each subject with a time gap of 45 minutes between sessions. Analysis was performed based on video recordings captured in session-1 and session-2. The data is acquired in a dark environment to avoid external artifacts. Lateral LED lighting pads were used to illuminate the iris as shown in Figure 1. It is hypothesized that this lighting configuration and location provides good textural information since the 3D iris structure casts more shadows at such incident angles compared to frontal illumination thus accentuating the iridial textures. Furthermore, the indirect lighting angle alleviates subject discomfort despite the proximity of the pads to the iris. Subjects were asked to place their head on the chin rest while data collection was in progress. *Note that this study was conducted under controlled conditions using cooperative users in order to first establish the benefits of hyper-focal imaging. Future work will explore the use of a less controlled acquisition environment.* Each recording included movements of focal point from tip of the nose (point A) to end of the ear (point B) labeled as round 1, and back (from B to A) labeled as round 2. The total recording time is one second (0.5 sec for each round). The acquired video at the rate of 30 fps provides sufficient number of frames for hyper-focal processing in one complete pass. In each session, subjects were asked to look straight at the camera during the recordings. A sequence of frames was extracted from the captured 1-second clip [2]. From the extracted frames, we used only 8 frames per direction i.e. 8 in the forward direction from A to B) and 8 in the reverse direction (from B to A). In our study we used two

[2]http://www.dvdvideosoft.com/products/dvd/free-video-to-jpg-converter.htm

fused samples, one pertaining to the forward direction and one pertaining to the reverse direction. The analysis is performed using two fused samples from session-1 and two fused samples from session-2 for each subject.

IV. Image Fusion Using Helicon Focus

A sequence (focus stack) of 8 frames obtained at varying focal planes is fused to result in a sharp, high DOF hyper-focal image. The 8 consecutive frames are manually selected from the acquired video based on the prototype shown in Figure 3.

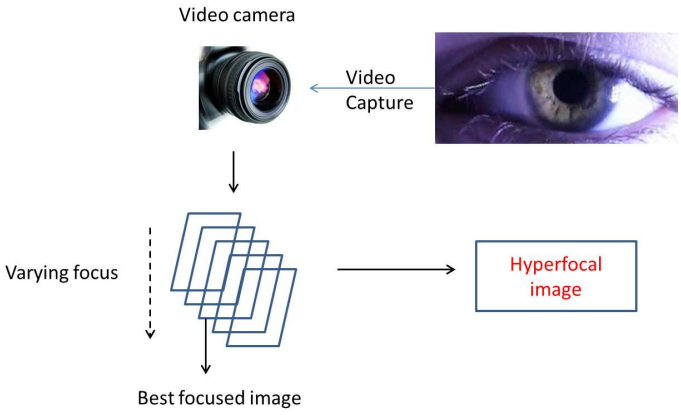


Fig. 3. Fusion prototype using the hyper-focal acquisition system

The Helicon focus software (Helicon Soft Ltd., Kharkov, Ukraine) [1] uses information from the sequence of images in the focus stack and produces a single hyper-focal image by fusing the sharper areas from each frame while adjusting for subtle movement and scaling aberrations across focal planes. Helicon focus software provides two options for focus stack fusion. Method A computes fusion weights for each pixel based on their contrast information, and all the corresponding pixel weights are averaged across the sequence of frames. Method B uses the sharpest pixels information and produces a depth map for stack fusion. This method has an advantage of overcoming halo effects across contrast edges. The focus measure at each point is determined by the distribution of pixels at a certain distance R from the point under consideration. Smoothing is another fusion parameter determining how smoothly the focus areas across stack captures are combined in the final hyper-focal image. This software registers the input images before applying the above mentioned methods. In our study we used Method B with a radius of R=45 pixels and a default smoothing value of 4. The exact method of registration and matching are proprietary.

Figure 4(b)(d)(f) shows examples of hyper-focal fusion using the Helicon focus software.

V. Iris Segmentation and Matching

Ocular regions for left and right eyes were manually cropped from every acquired face image. The original face image had dimensions of 1088×1920 pixels and iris region in the cropped ocular images had an average of 82 pixels across its diameter. The final dataset has 184 iris images for each eye corresponding to 4 fused samples per subject for 46 subjects. These 4 fused samples are obtained over two sessions with 2 fused samples per session: one fused sample is generated from frames in the forward direction (round 1) and the other fused sample is generated from frames in the reverse direction (round 2).

The red channel image is used for iris matching as this is assumed to reveal maximum textural information due to its proximity to the NIR spectrum. The iris images are segmented by approximating the limbic boundary and pupillary boundary as circles and searching for the largest gradient values in circular Hough space. The upper and lower eye lids are approximated with straight lines. More details of the segmentation process can be found in [9].

Improperly segmented irides are visually determined and are manually rectified. This is to avoid issues related to incorrect segmentation that can affect the subsequent matching results. Pupillary boundary for darker irides is virtually indistinguishable from the surrounding iris region in RGB and poses a major problem for automatic segmentation. Segmented iris images are unwrapped to a pseudo-polar rectangular grid using Daugman's rubber sheet model [4]. The gray scale rectangular normalized image is converted to an IrisCode [4] using Masek's encoding method [9] that uses log-Gabor filters in the Fourier domain and further quantization to convert the filter response to a binary code known as IrisCode. Normalized Hamming distance is used to measure the dissimilarity between two IrisCodes. Thus, a lower match score indicates a better match. Several match scores are generated by computing the Hamming distance between one IrisCode and horizontally shifted versions of the other and the least score is selected as the final match score. This accounts for rotational inconsistencies between the two iris images.

Figure 5 shows the result of segmentation and normalization on a sample iris image.

VI. Focus Measure

A focus metric is used to compare the quality of the acquired sequence of frames with their corresponding hyper-focal fused image. We used a simple wavelet based focus metric [8] in this study. It is noted that focus index of an image is highly correlated with sum of its wavelet coefficients, where a higher sum indicates better focus. Wavelet coefficients are generated based on equation below, where I(X, Y) is the input image and ψ is the basis function:

$$W_{\psi}^{i}(j,m,n) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} I(x,y)\psi_{j,m,n}(x,y)$$

,

$$i = \{H, V, D\}$$

$$I_f = Mean\left(\sum W_{\psi}^{i}(j,m,n)\right), i = \{H, V, D\}$$

Wavelet decomposition of image in the horizontal (H), Vertical (V) and diagonal (D) directions is performed using

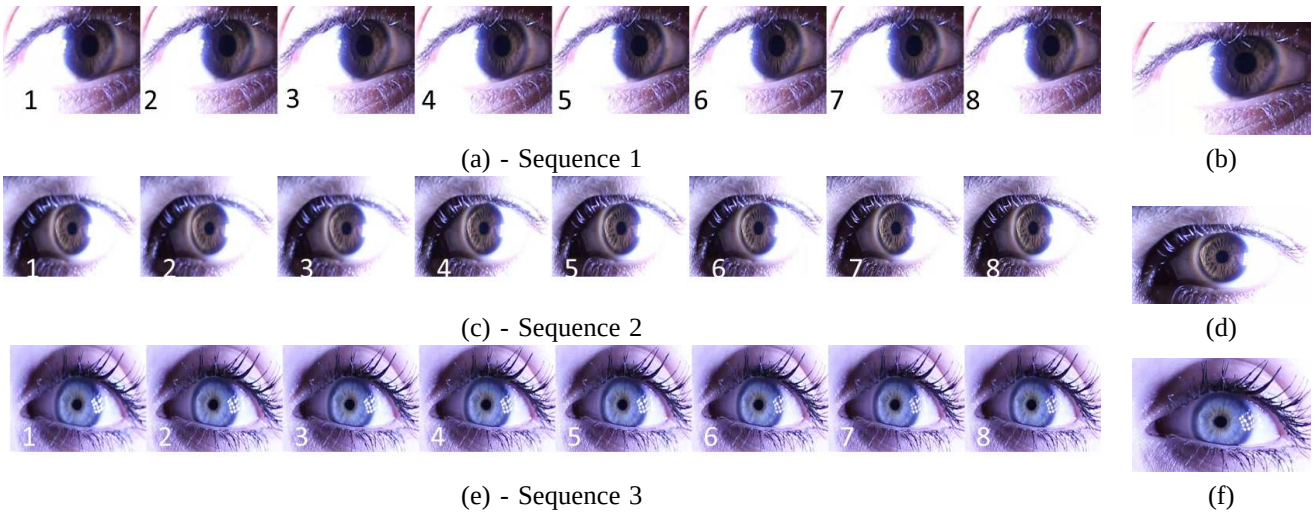


Fig. 4. Examples for individual frame sequences and corresponding hyper-focal fused images. Here, (a), (c) and (e) represent 3 sets of input frames. (b), (d) and (f) are the corresponding fused frame.

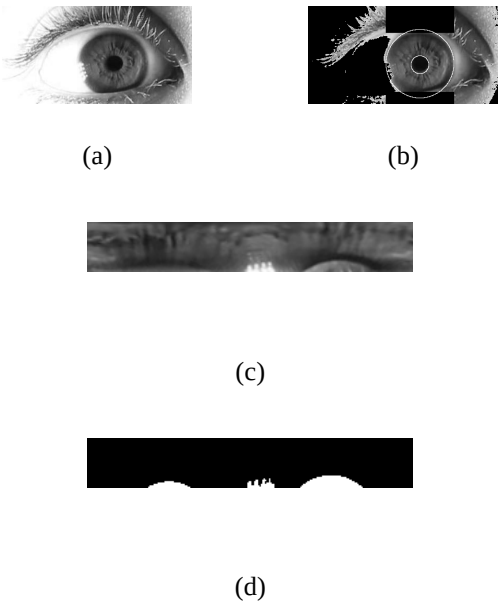


Fig. 5. (a) Original image (b) Segmentation output (c) Normalized image and (d) corresponding mask image

Daubechies mother wavelet of order one. I_f is the mean of the wavelet coefficients in all the directions resulting in our focus metric. Figure 6 shows the focus values for individual frames in the video sequence shown in Figure 4 (focus stack) and the corresponding value for fused hyper-focal image. It is evident that hyper-focal fusion yields a higher focus measure for fused image compared to the input frames.

VII. Experiments

We compared the performance of single focus and hyper-focal images independently on the left and right eyes. In this analysis we chose the middle frame (4th frame) from the 8-frame sequence and generated iris match scores on the dataset. Choosing the fused hyper-focal image for matching resulted in a decreased EER compared to matching using only the middle frame. Figure 7 shows the plotted ROC curves and Table I shows the corresponding EER values for middle frame and fused hyper-focal image matching.

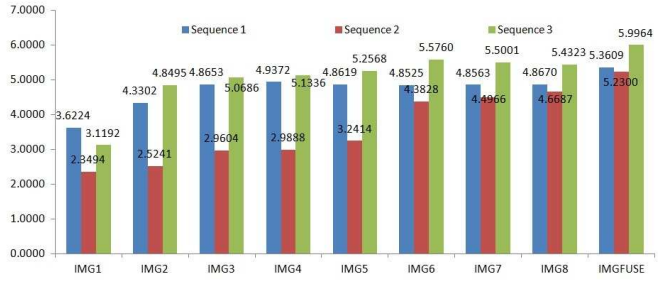


Fig. 6. Focus measure for individual frames against the fused hyper-focal image

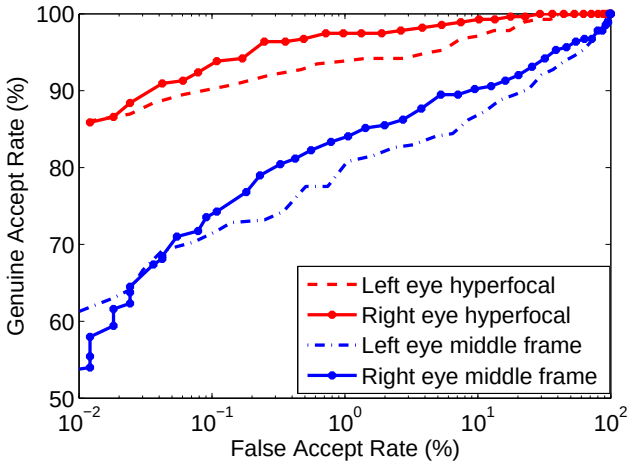


Fig. 7. ROC curves for left and right eye of Hyper-focal images and middle frame from the stack of variable focus images

TABLE I
ROC ANALYSIS FOR HYPER-FOCAL IMAGES AND MIDDLE FRAMES FROM SEQUENCE OF 8 FRAMES USED FOR HYPER-FOCAL FUSION

	Hyper-focal images	Fixed focus images
	EER	EER
Left Eye	0.04997	0.1245
Right Eye	0.021588	0.096347

To illustrate the effect of focus of the captured image on the iris match scores, box plots are shown in Figure 8.

For each subject, 8 frames are available in the first sequence each of Session-1 and Session-2. Genuine match scores are generated by matching all the 8 frames from first sequence of Session-1 against all the 8 frames from the first sequence of Session-2. Figure 8 shows the box plots of these genuine scores along with the match score (red dot) for matching the best focused frames in both the sessions and corresponding match score (green dot) for fused hyper-focal images. It is clearly evident as shown in Figure 8, that the genuine match score for the fused hyper-focal image is much lower than that of the middle frame, there by suggesting a better match.

Wilcoxon signed rank test [17] is used to demonstrate the statistical significance of the improvement in genuine match score when using hyper-focal image compared to single focus images (middle frame). Table II shows the z-values and the corresponding p-values for different scenarios. S1(S2) stands for Session-1(Session-2) and R1(R2) stands for the first(second) sequence.

TABLE II
STATISTICAL SIGNIFICANCE TABLE FOR HYPER-FOCAL IMAGE VS. BEST FOCUSED IMAGE (WILCOXON TEST RESULTS)

	S1R1 vs S2R1	S1R1 vs S2R2	S1R2 vs S2R1	S1R2 vs S2R2
z-statistic	4.4166	3.2694	4.4603	4.6351
p-value	$<$0.0001	0.0005	$<$0.0001	$<$0.0001

Values in Table II reject the null hypothesis that the genuine match score of hyper-focal image is greater than genuine match score for middle frame of the 8 selected frames. Another scenario is considered where hyper-focal match score is compared against the minimum possible match score for a fixed focus frame. Assuming the basic assumptions for t-test to be true, Table III shows the significance of hyper-focal images in iris recognition.

TABLE III
STATISTICAL SIGNIFICANCE TABLE FOR HYPER-FOCAL IMAGE VS. BEST MATCH SCORE USING A SINGLE FIXED FOCUS IMAGE

	S1R1 vs S2R1	S1R1 vs S2R2	S1R2 vs S2R1	S1R2 vs S2R2
t-statistic	2.3714	2.4330	2.7123	2.3448
p-value	0.0110	0.0095	0.0047	0.0117

Table III shows that genuine score for fused hyper-focal image is lower(better) than the best possible genuine score for fixed focus image scenario with a high statistical significance.

VIII. DISCUSSION

A sequence of 8 images captured in a fraction of a second was used for fusion in our study. However, this number depends on the native frame rate of the camera, 3D depth of an eye, and also speeds of the motorized lens moving mechanism. Higher native speed of the camera would ultimately reduce the chances of observing motion blur and occlusions in image acquisition. We used 1080p HD video recordings with 30 fps instead of the regular burst mode full frame image captures and used the lens' internal focus motors for smoother lens movements. This obviates the use of moving rails and external motor-operated lens moving mechanisms. These traditional mechanisms when operated at higher speeds might induce vibration resulting in motion artifacts. Another instrumental factor in our design is the use of side lighting making RGB iris captures a possibility. Our statistical analysis and ROC analysis clearly show that hyper-focal imaging performs better than regular imaging. However, hyper-focal imaging technique in conjunction with existing commercial technologies would help in improving iris recognition rates.

IX. CONCLUSION AND FUTURE WORK

In this paper we introduced a novel image acquisition platform using hyper-focal imaging technique and side lighting to acquire high quality images of iris in the visible spectrum with greater DOF. Statistical analysis confirm, with high confidence, that hyper-focal imaging systems produce better results compared to fixed focus systems. In future we would like to implement this technique to see the effect of imaging for on iris-on-the-move systems. Using these high-resolution RGB iris images a study on pigmentation and ethnicity assessment using iris color information will be performed in the future.

X. ACKNOWLEDGMENTS

Research was sponsored by the Leonard Wood Institute in cooperation with the U.S. Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-07-2-0062. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Leonard Wood Institute, the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation heron. Authors thank Bret Lesan, CMfgE, Senior Research and Design Engineer, UMKC for help with mechanical design of the acquisition system and Plamen Doynov for assisting with preparation of the initial draft.

REFERENCES

[1] "Helicon Soft ". Helicon soft ltd,. http://www.heliconsoft.com/.
[2] K.W. Bowyer, K. Hollingsworth, and P.J. Flynn. Image understanding for iris biometrics: A survey. *Computer Vision and Image Understanding*, 110(2):281–307, 2008.

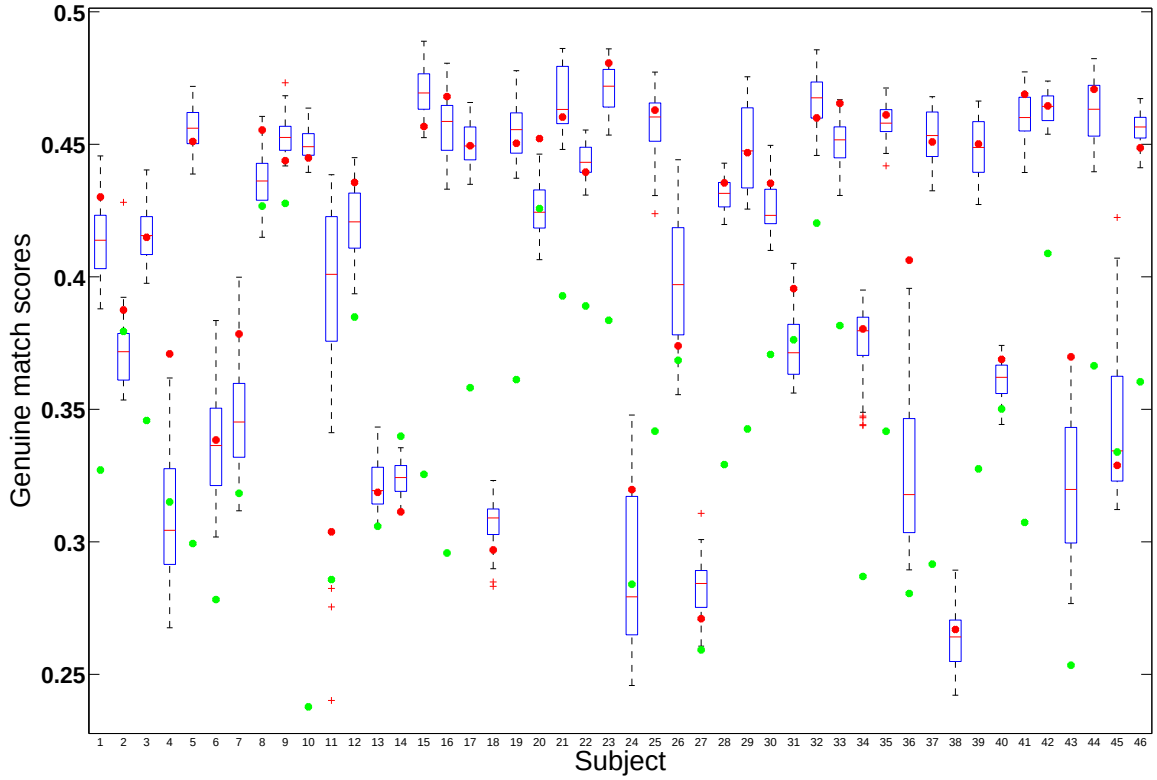


Fig. 8. Box plots of genuine match scores for all the 46 subjects for session 1 against session 2

[3] C. Boyce, A. Ross, M. Monaco, L. Hornak, and X. Li. Multispectral iris analysis: A preliminary study. In *Computer Vision and Pattern Recognition Workshop*, pages 51–51. IEEE, 2006.

[4] J. Daugman. How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology,*, 14(1):21–30, 2004.

[5] Y. He, J. Cui, T. Tan, and Y. Wang. Key techniques and methods for imaging iris in focus. In *18th International Conference on Pattern Recognition*, volume 4, pages 557–561. IEEE, 2006.

[6] N.D. Kalka, J. Zuo, N.A. Schmid, and B. Cukic. Estimating and fusing quality factors for iris biometric images. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans,*, 40(3):509–524, 2010.

[7] E. Krichen, M.A. Mellakh, S. Garcia-Salicetti, and B. Dorizzi. Iris identification using wavelet packets. In *Proceedings of the 17th International Conference on Pattern Recognition*, volume 4, pages 335–338. IEEE, 2004.

[8] J.H. Lee, K.S. Kim, B.D. Nam, J.C. Lee, Y.M. Kwon, and H.G. Kim. Implementation of a passive automatic focusing algorithm for digital still camera. *IEEE Transactions on Consumer Electronics,*, 41(3):449–454, 1995.

[9] Peter Kovesi Libor Masek. Matlab source code for a biometric identification system based on iris patterns, 2003.

[10] K.R. Park and J. Kim. A real-time focusing algorithm for iris recognition camera. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews,*, 35(3):441–444, 2005.

[11] R. Plemmons, M. Horvath, E. Leonhardt, VP Pauca, S. Prasad, S. Robinson, H. Setty, T. Torgersen, J. van der Gracht, E. Dowski, et al. Computational imaging systems for iris recognition. In *Proc. SPIE*, volume 5559, pages 346–357, 2004.

[12] H. Proença and L. Alexandre. Ubiris: A noisy iris image database. *ICIAP*, pages 970–977, 2005.

[13] P. Radu, K. Sirlantzis, WGJ Howells, S. Hoque, and F. Deravi. Information fusion for unconstrained iris recognition. *International Journal of Hybrid Information Technology*, 4(4):1–12, 2011.

[14] Paulo E.X. Silveira Ramkumar Narayanswamy. Iris recognition at a distance with expanded imaging volume. *Biometric Technology for Human Identification - II*, 5779:41–50, 2005.

[15] A. Ross. Iris recognition: The path forward. *Computer*, 43(2):30–35, 2010.

[16] K.N. Smith, V.P. Pauca, A. Ross, T. Torgersen, and M.C. King. Extended evaluation of simulated wavefront coding technology in iris recognition. In *International Conference on Biometrics: Theory, Applications, and Systems*, pages 1–7. IEEE, 2007.

[17] F. Wilcoxon. Individual comparisons by ranking methods. *Biometrics Bulletin*, 1(6):80–83, 1945.

ABOUT THE AUTHORS

Sriram Tankasala

Vikas Gottemukkula

Sashi Kanth Saripalle

Venkata Goutam Nalamati

Reza Derakhshani

Dept. of Computer Science and Electrical Engineering,

University of Missouri - Kansas City

Raghunandan Pasula

Arun Ross

Lane Department of Computer Science and

Electrical Engineering,

West Virginia University

© 2013 IEEE and published here with permission. *Homeland Security Affairs* is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of this article is expressly prohibited without the written consent of the copyright holder, the Institute of Electrical and Electronics Engineers (IEEE). *Homeland Security Affairs* is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).

http://www.hsaj.org