Naval Postgraduate School Cyber Academic Group Compilation of Abstracts

Monterey, California. Naval Postgraduate School

Naval Postgraduate School
Cyber Academic Group

Compilation of Abstracts

Unrestricted Theses and Dissertations by September 2017 Graduates

2017-09

Naval Postgraduate School
Monterey, California • www.nps.edu

This compilation of abstracts highlights the breadth of cyber-related student research at the Naval Postgraduate School (NPS) in Summer Quarter 2017 and reinforces the importance of cyber as an integral aspect of today's Naval enterprise. The abstracts provided represent publicly releasable theses and dissertations completed by September 2017 graduates. They are the product of the NPS Cyber Academic Group (CAG), which is a national resource for the interdisciplinary study and design of secure and resilient cyber systems and the conduct of cyber operations.

Cyberspace is now a primary warfare area. By establishing the U.S. Tenth Fleet/Fleet Cyber Command and the position of Deputy Chief of Naval Operations for Information Dominance (N2N6), the U.S. Navy created an enterprise able to address the opportunities and challenges for cyber systems and operations within its vision for the information warfare community. Reflecting a growing cognizance of the importance of cyber operations, other elements of the U.S. military and U.S. government, such as the Department of Homeland Security, have created similar or complementary organizations.

Optimizing military and U.S. government cyber assets for future operations will require leaders who both understand how to defend our networks from penetration and employ cyber capabilities to ensure an advantage in future operations. This objective cannot be reached without a cadre of officers able to address a broad range of cyber operations: computer network attack, defense, and exploitation; cyber analysis, operations, planning, and engineering; and cyber intelligence operations and analysis.

The CAG is an interdisciplinary association of two dozen faculty members, including those holding named chairs, representing eight distinct academic disciplines. Established by NPS on 23 September 2011, the CAG has responsibility for oversight and management of the Cyber Systems and Operations curriculum. Graduate-level instruction and research support in interdisciplinary programs is delivered by members of this academic group and by faculty primarily from the following academic departments: Computer Science, Electrical and Computer Engineering, and Information Sciences.

For more information, please contact the following individuals or visit our website at: http://my.nps.edu/web/cag/.

Dr. Clark Robertson, Chair, Cyber Academic Group
crobertson@nps.edu

CDR Zachary Staples, Director, Center for Cyber Warfare
zhstaple@nps.edu

LEVERAGING THE NPS FEMTO SATELLITE FOR ALTERNATIVE SATELLITE COMMUNICATION NETWORKS
Faisal S. Alshaya–Major, Royal Saudi Armed Forces
Master of Science in Systems Technology (Command, Control, and Communications)
Advisor: Steven J. Iatrou, Department of Information Sciences
Advisor: Peter Ateshian, Department of Electrical and Computer Engineering

Femto satellites may provide solutions for the U.S. military in different areas. Specifically, these satellites may offer an effective and affordable alternative approach when the military faces a denial of access to primary space assets. Their low cost allows for the rapid simultaneous deployment of multiple Femto satellites, which contributes to rapid recovery from a denial situation. This thesis focuses on the communication application of Femto satellites by investigating the ability of the first and next generations of Naval Postgraduate School Femto Satellites (NPSFS) to provide a low data throughput. We modeled the first generation of NPSFS as a space-based network using System Tool Kit with QualNet (STK/QualNet) software. For the next generation of NPSFS, we conducted an experiment using Intel Arduino 101 to control the Iridium 9602 Modem, also known as the RockBlock MK2, to test the possibility of sending a text file from one terminal to another. The results confirmed the power limitation associated with Femto satellites, which reduces their suitability for implementation as a viable space network. Nevertheless, the results showed that providing a low data throughput is feasible. Finally, we suggest ways to improve the next-generation NPSFS. Full Text

Keywords: space, Femto satellite, NPSFS, network, communication, Arduino, RockBlock, Iridium Modem

DRFM CORDIC PROCESSOR AND SEA CLUTTER MODELING FOR ENHANCING STRUCTURED FALSE TARGET SYNTHESIS
Pak Siang Ang–Military Expert 5, Republic of Singapore Air Force
Master of Science in Electrical Engineering
Advisor: Phillip E. Pace, Department of Electrical and Computer Engineering
Co-Advisor: Douglas J. Fouts, Department of Electrical and Computer Engineering

In this thesis, we investigate two critical components of a digital-image synthesizer electronic warfare architecture that can be used to infuse false targets into high-range resolution profiling radars. The first investigation encompasses the design of an in-phase and quadrature (I/Q) converter based on a CORDIC (Coordinate Rotation Digital Computer) algorithm. Mathematical modeling is used to examine the accuracy of converting a digitized radar signal I/Q sample into a corresponding five-bit binary phase angle. Results obtained from MATLAB show that 18 CORDIC iterations are required to achieve accuracy at 5.625˚. The resulting design was implemented using the Verilog hardware description language. The second investigation concerns generating sea clutter to impose on the false target. The mean-power return of the sea clutter is calculated using the average power of the radar-cross section derived from the Naval Research Laboratory sea clutter model. The modulation coefficients for the sea clutter were generated using the fluctuating power returns and Doppler spectra generated using a random KA distribution. The coefficients for several sea states were generated using MATLAB. Results show that the correct sea clutter model can effectively add realism to the false target image. Full Text

Keywords: inverse synthetic aperture radar, sea clutter modeling, CORDIC, Coordinate Rotation Digital Computer, Digital Image Synthesizer, DRFM, digital radio frequency memory, electronic attack

ASSESSMENT OF AN ONBOARD EO SENSOR TO ENABLE DETECT-AND-SENSE CAPABILITY FOR UAVs OPERATING IN A CLUTTERED ENVIRONMENT
Wee Kiong Ang–Captain, Singapore Army
Master of Science in Systems Engineering
Advisor: Oleg Yakimenko, Department of Systems Engineering
Co-Advisor: Dong Hye Ye, Purdue University

In an increasingly complex environment crowded with obstacles, particularly manned and unmanned traffic, technological advancements can autonomously provide alerts to the presence of incoming threats. In other words, advancements such as computer vision (CV) capability enhance overall situation awareness. This thesis explores the development and integration of CV capability onboard a functional unmanned aerial vehicle (UAV) to detect and track multiple proximate moving targets autonomously. A systems engineering approach is applied to define, analyze, and synthesize systematically a proposed system architecture for the real-time autonomous detection and tracking capability via visual sensors onboard the UAV. Both the hardware and software architecture design are discussed at length. Then, a series of tests that were conducted progressively to assess and evaluate the overall system architecture are described. Multiple UAVs and unmanned ground vehicles represented the contested operational environment. The developed CV algorithm proved successful at detecting and tracking multiple moving targets in real-time operation, thus laying the foundation for future research and implementation of the developed techniques in the automatic vision-based collision-avoidance guidance architecture. Full Text

Keywords: unmanned aerial system, electro-optics sensor, computer vision, optical flow, situation awareness

DEVELOPMENT OF INFORMATION ASSURANCE PROTOCOL FOR LOW BANDWIDTH NANOSATELLITE COMMUNICATIONS
Cervando A. Banuelos II–Civilian, National Science Foundation CyberCorps
Master of Science in Computer Science
Advisor: Marcus S. Stefanou, Department of Computer Science
Co-Advisor: Jim Horning, Space Systems Academic Group

Nanosatellites provide a light, efficient, and cost-effective way for research institutions to carry out experiments in low Earth orbit. These satellites frequently use the ultra-high and very high frequency bands to transfer their data to the ground stations, and oftentimes will use internet protocol and Transmission Control Protocol as a standard for communication to ensure the arrival and integrity of the data transmitted. Due to bandwidth limitations and signal noise, these connection-based protocols end up accruing a large data bandwidth cost in headers and retransmissions. Furthermore, due to connection unreliability, encryption and integrity checks present a challenge. The aim of this thesis is to develop a

software-based low-bandwidth reliable network protocol that can support a cryptographic system for encrypted communications using commercial off-the-shelf components. This protocol reduces the data overhead, retains the retransmission functionality and integrates support for a cryptographic system. This thesis develops the encryption mechanism, assesses its resilience to error propagation, and develops the protocol to work over a simulated network. The result of the study is a proof of concept that the protocol design is feasible, applicable, and could be used as a communication standard in future projects. Full Text

Keywords: commercial off-the-shelf technology, nanosatellites, CubeSat, encrypted communications

EXPERIMENTAL VALIDATION OF MODEL UPDATING AND DAMAGE DETECTION VIA EIGENVALUE SENSITIVITY METHODS WITH ARTIFICIAL BOUNDARY CONDITIONS
Matthew D. Bouwense–Lieutenant, United States Navy
Master of Science in Mechanical Engineering
Advisor: Joshua H. Gordis, Department of Mechanical and Aerospace Engineering
Second Reader: Young W. Kwon, Department of Mechanical and Aerospace Engineering

The use of finite element modeling (FEM) in design has expanded as computers have become more capable. Despite these advancements, the construction of physical prototypes remains an essential aspect of design and testing. FEM limitations include the inability to accurately account for joints, damping, and geometric complexities. Due to the reality gap between a FEM and the prototype, there may be design deficiencies that cannot be identified until the prototype is tested. Using eigenvalue sensitivities, enhanced by artificial boundary conditions (ABC), the gap between simulation and reality can be closed via FEM updating. With an updated FEM, the same eigenvalue sensitivities can be utilized to detect damage in structural systems in use. Damage that produces differences in natural frequencies between the structure and its FEM can be related to the loss in flexural rigidity, as it is usually assumed that mass modeling is correct. This indicator allows adjustment of a FEM to match a prototype or to detect damage in a potentially compromised structure via comparison to an updated FEM. Based on simulation, a combination of multiple pin and spring ABCs is optimal for producing an ideal sensitivity matrix, and thus, ideal damage detection capability. However, in the experimental realm, the synthesis transformation used to apply ABCs to the measured frequency response functions can distort the frequency response function peaks, leading to error. A compromise of a single pin ABC permits both effective model updating and damage detection. Full Text

Keywords: finite element model, eigenvalue sensitivity, artificial boundary condition, frequency response function, natural frequency, model update, damage detection

SYMMETRIC LINK KEY MANAGEMENT FOR SECURE NEIGHBOR DISCOVERY IN A DECENTRALIZED WIRELESS SENSOR NETWORK
Kelvin T. Chew–Captain, United States Marine Corps
Master of Science in Electrical Engineering
Advisor: Preetha Thulasiraman, Department of Electrical and Computer Engineering
Second Reader: Murali Tummala, Department of Electrical and Computer Engineering

Wireless sensor networks provide a low-signature communications system that can be used for a wide variety of military applications. These networks are vulnerable to intrusion, however, and must balance security with performance and longevity. The neighbor discovery process is vital for nodes to maintain network connectivity but introduces security vulnerabilities; therefore, a lightweight security protocol is necessary to prevent unauthorized nodes from accessing network data and resources. In this thesis, we focus on the management of encryption keys in a resource-limited, peer-to-peer, decentralized network. Existing protocols for securing the neighbor discovery process use public key encryption, which is too computationally expensive for low-powered, resource-constrained IEEE 802.15.4-enabled devices. We therefore develop a key management scheme that modifies the Neighbor Discovery Protocol (NDP) and Secure Neighbor Discovery (SEND) protocol and implements the Diffie-Hellman key exchange algorithm for symmetric key management. We simulate our scheme in MATLAB to demonstrate its effectiveness in securing the neighbor discovery protocol while providing energy efficiency, key security, and error resistance. Full Text

Keywords: wireless sensor network, 6LOWPAN, key management, neighbor discovery, symmetric cryptography, identity-based cryptography, Diffie-Hellman key exchange, cyber

THE THRESHOLD SHORTEST PATH INTERDICTION PROBLEM FOR CRITICAL INFRASTRUCTURE RESILIENCE ANALYSIS
Charles R. Clark–Lieutenant Commander, United States Navy
Master of Science in Operations Research
Advisor: W. Matthew Carlyle, Department of Operations Research
Second Reader: David L. Alderson, Department of Operations Research

We formulate and solve the threshold shortest path interdiction problem, which we define as follows: Find a finite set of arcs to attack within a network such that the resulting shortest path from a given source node to a given destination is longer than a specified threshold. Ultimately, we are concerned with determining the number of such attacks and using it as a measure of resilience or lack thereof, in an instance of the shortest-path interdiction problem. We develop and implement algorithms to reduce the required computational effort to solve this counting problem exactly. We illustrate via test cases the impact of different interdiction combinations with regards to the threshold value. Whether these interdictions are random occurrences or intentional, this analysis provides decision makers a tool with which to more completely characterize the resilience of a system of interest. Full Text

Keywords: network interdiction, attacker-defender, defender-attacker-defender, infrastructure resilience,

shortest path interdiction

SYSTEMATIC ASSESSMENT OF THE IMPACT OF USER ROLES ON NETWORK FLOW PATTERNS
Jeffrey S. Dean–Civilian, United States Air Force
Doctor of Philosophy in Computer Science
Advisor: Neil Rowe, Department of Computer Science

Defining normal computer user behavior is critical to detecting potentially malicious activity. To facilitate this, some anomaly-detection systems group the profiles of users expected to behave similarly, setting thresholds of normal behavior for each group. One way to group users is to use organizational role labels, as people with similar roles in an organization often share common tasks and activities. Another way is to group users based on observed behavioral similarities. We tested the premise that users sharing roles behave similarly on networks, applying two machine-learning classifiers (nearest-centroid and a support vector machine) to differentiate between groups based on flow-data feature vectors. We conducted tests using 1.2 billion network-flow records from a large building at the Naval Postgraduate School over five weeks. Tests showed similar results when they were conducted with and without removal of automated flows. Tests showed that users in role groups do not exhibit significantly similar network behaviors. We also clustered feature-vector data to group users by patterns of network behavior and showed that defining user groups this way provides a better way to bound normal user behavior. Full Text

Keywords: netflow, user behavior, machine learning, organizational role

ANALYSIS OF TRAFFIC SIGNALS ON A SOFTWARE-DEFINED NETWORK FOR DETECTION AND CLASSIFICATION OF A MAN-IN-THE-MIDDLE ATTACK
Julian N. D'Orsaneo–Captain, United States Marine Corps
Master of Science in Electrical Engineering
Advisor: Murali Tummala, Department of Electrical and Computer Engineering
Co-Advisor: John C. McEachen, Department of Electrical and Computer Engineering
Second Reader: Bryan Martin, Department of Electrical and Computer Engineering

Software-defined networking (SDN) has the potential to revolutionize the management capabilities of a highly distributed military communications environment. Yet military adoption of SDN is contingent on a thorough analysis of security implications. In this thesis, we investigate a man-in-the-middle (MITM) attack that exploits the centralized topological view critical to SDN operations. In particular, we present a new scheme for detection and classification of the attack at the network layer. We apply wavelet analysis to detect anomalous conditions introduced by the MITM attack at traffic signals collected at network switch ports. Furthermore, we identify unique characteristics of reported anomalies in the collected traffic signals to build a classification framework. Other cyber events, such as a distributed denial-of-service attack and network congestion, are presented to the detection scheme to validate its general applicability. Overall, we successfully demonstrate the capability to detect and classify the MITM attack in addition to other cyber events at the network layer, thereby contributing to the security of SDN. Full Text

Keywords: software-defined networking, network monitoring, wavelet analysis, anomaly detection, man-in-the-middle attack, anomaly classification

POWER ANALYSIS OF AN ENTERPRISE WIRELESS COMMUNICATION ARCHITECTURE
Howen Q. Fernando–Civilian, Department of the Navy
Master of Science in Systems Engineering Management
Advisor: Ronald Giachetti, Department of Systems Engineering
Second Reader: Anthony Pollman, Department of Systems Engineering

Technological advancements in Software Defined Radios (SDR), high-speed serial buses, and high-performance computing systems have brought us a power reduction breakthrough in military wireless communications. This thesis develops and analyzes a model to demonstrate that an enterprise computing architecture for Software Defined Radios results in significant power savings between 11% and 13% under ordinary operational loads. The thesis presents easy-to-understand mathematical power consumption models and simulations of general military communications systems in an Expeditionary Command, Control, Communications, and Computers (C4) scenario. The comparison of regular versus enterprise SDR architectures exposes the power savings realized in the Enterprise Wireless Communications (EWC) architecture. Full Text

Keywords: command and control, C2, Internet of Things, IoT, model based systems engineering, MBSE, marine air-ground task force, MAGTF, command control and communications, C3, command control communications and computers, C4, size weight and power, SWaP, software defined radio, SDR, software communication architecture, SCA, electronic warfare, EW, dynamic spectrum allocation, DSA

TESTING THE FORENSIC INTERESTINGNESS OF IMAGE FILES BASED ON SIZE AND TYPE
Raymond M. Goldberg–Second Lieutenant, United States Army
Master of Science in Cyber Systems and Operations
Advisor: Neil Rowe, Department of Computer Science
Second Reader: George Dinolt, Department of Computer Science

In this thesis, we investigate the relationship between the size and type of a file and its forensic usefulness. We investigate GIF, MP3, MP4, PNG, and JPEG files found in a large collection called the Real Drive Corpus, and the files' classification as software-based, entertainment-based, or personal. Results of these experiments were compared to prior work to find interesting files. Results show that the previous experiments were effective at marking interesting files as interesting, but there were still a lot of uninteresting files that were marked as interesting. Also, the results do not show a correlation between the interestingness of a file, its type, and its size. Full Text

Keywords: Real Drive Corpus, scanning, white listing, known files database

LOW-COST GROUND SENSOR NETWORK FOR INTRUSION DETECTION
Dingyao Hoon–Major, Army, Singapore Armed Forces
Yueng Hao Kenneth Foo–Project Manager, Defence Science and Technology Agency, Singapore
Master of Science in Computer Science
Advisor: John H. Gibson, Department of Computer Science
Co-Advisor: Gurminder Singh, Department of Computer Science

Perimeter surveillance of forward operating locations, such as Forward Arming and Refueling Points (FARPs), is crucial to ensure the survivability of personnel and materiel. FARPs are frequently located well outside the protective cover of the main forward operating bases. Therefore, they must provide their own organic perimeter defenses. Such defenses are manpower intensive. Our research investigates how cheap, remote, unattended sensors using commercial off-the-shelf (COTS) components can help reduce the manpower requirement for this task and yet not compromise the security of the operating location. We found Internet of Things (IoT) platforms such as Raspberry Pi, paired with passive infra-red sensors and cameras, to be useful in this application. We built a prototype sensor system, tested it in a simulated field environment, and evaluated its performance. We conclude that COTS IoT platforms have much potential to support surveillance of FARPs and other forward operating locations. Full Text

Keywords: wireless, low-cost, network, IoT, PIR, image recognition, air base ground defense system, OpenCV, sensor, Raspberry Pi

THE INSIDER THREAT TO CYBERSECURITY: HOW GROUP PROCESS AND IGNORANCE AFFECT ANALYST ACCURACY AND PROMPTITUDE
Ryan F. Kelly–Captain, United States Army Reserve
Doctor of Philosophy in Information Sciences
Advisor: Dan Boger, Department of Information Sciences

The recent increase in high-profile insider cyber exploits indicates that current insider threat analysis (ITA) is insufficient to handle the growing insider threat problem. Well-established academic literature agrees that information overload is a problem ITA must overcome because ITA remains a human-intensive task. Two conceptual strategies to overcome information overload include reducing information and distributing information among additional people to accommodate the load. This dissertation applies attribution theory and process loss theory to test two ITA factors: ignorance and teamwork. A laboratory experiment with a convenience sample of 48 ITA-trained, top secret–cleared participants supported the research. Participants performed ITA with National Insider Threat Task Force training scenarios and applied the adjudicative guidelines for access to classified information. Teamwork conditions resulted in slightly higher accuracy at a significant cost of time, indicating that ITA analysts are best organized in different structures per informational and temporal constraints. However, ignorance level had little effect on ITA analyst accuracy. ITA analysts were substantially more accurate at implication scenarios but slightly better than chance at exoneration scenarios. Lower decision confidence associated with exoneration scenarios indicated that ITA analysts are more likely to guess when presented with an exoneration scenario. Further research involving larger independent samples and temporal constraints is

necessary to verify these findings. Full Text

Keywords: insider threat to cybersecurity, cybersecurity philosophy, attribution theory, process loss theory

PROOF OF CONCEPT IN DISRUPTED TACTICAL NETWORKING
Thomas D. Kline–Major, United States Marine Corps
Master of Science in Information Technology Management
Advisor: Alex Bordetsky, Department of Information Sciences
Second Reader: Steve Mullins, Department of Information Sciences

Current systems used to control unmanned assets and maintain command and control networks typically rely upon persistent signals. However, the Department of Defense (DoD) predicts that adversaries will be able to detect, geolocate, and target through electromagnetic (EM) spectrum operations in the future operating environment. Unable to rely upon constant interconnection, the DoD must begin to reconsider the nature and behavior of its networks. In 2011, Bordetsky and Netzer proposed networks that do not exist as a potential solution. They envision multi-domain networks whose links connect only long enough to transmit critical information securely. The links quickly disconnect, leaving no trace electromagnetically. The DoD lacks sufficient research that evaluates the merits of short-living network solutions. Without adequate research, the future DoD may either unnecessarily expose its forces to adversaries through the networks or impair decision-making by choosing not to communicate because of the risk of detection. In this study, we design projectile-based mesh networking prototypes as one potential type of short-living network node and use the projectiles to observe some of the merits and challenges of moving from persistent signal networks to cluster-based networks created only during disruption. Full Text

Keywords: mesh networking, projectile-based, bursty tactical networks

APPLICABILITY OF DEEP-LEARNING TECHNOLOGY FOR RELATIVE OBJECT-BASED NAVIGATION
Wee Leong Lai–Civilian, ST Electronics (Info-Comm Systems) Pte. Ltd.
Master of Science in Systems Engineering
Advisor: Oleg A. Yakimenko, Department of Systems Engineering
Second Reader: Fotis A. Papoulias, Department of Systems Engineering

In a GPS-denied environment, one of the possible selections for navigating an unmanned ground vehicle (UGV) is through real-time visual odometry. To navigate in such an environment, the UGV needs to be able to detect, identify, and relate the static and dynamic objects such as trucks, motorbikes, and pedestrians in the on-board camera field of view. Therefore, object recognition becomes crucial in navigating UGVs. However, object recognition is known to be one of the challenges in the field of computer vision. Current analytic video software inadequately utilizes heuristics like size, shape, and direction to determine whether a detected object is a human, a vehicle, or an animal. This thesis explores

another approach, the deep-learning technique, which makes use of neural networks based on vast collections of training data images. This thesis follows a systems engineering approach in analyzing the need and suggesting a solution. It shows how to create and train the aforementioned networks using just three objects: a chair, a table, and a car. A Pioneer UGV equipped with the corresponding sensors is then used to test the developed algorithms. The preliminary analysis conducted in this thesis shows good potential for using the deep-learning technique on future UGVs. Full Text

Keywords: unmanned ground vehicle, navigation, computer vision, deep learning, object recognition

CORRELATION IMMUNITY, AVALANCHE FEATURES, AND OTHER CRYPTOGRAPHIC PROPERTIES OF GENERALIZED BOOLEAN FUNCTIONS
Thor Martinsen–Commander, United States Navy
Doctor of Philosophy in Applied Mathematics
Advisor: Pantelimon Stănică, Department of Applied Mathematics

This dissertation investigates correlation immunity, avalanche features, and the bent cryptographic properties for generalized Boolean functions defined on Vn with values in Zq. We extend the concept of correlation immunity from the Boolean case to the generalized setting, and provide multiple construction methods for order 1 and higher correlation immune generalized Boolean functions. We establish necessary and sufficient conditions for generalized Boolean functions. Additionally, we discuss correlation immune and rotation symmetric generalized Boolean functions, introducing a construction method along the way. Using a graph-theoretic and probabilistic frame of reference, we subsequently establish several, increasingly stringent, strict avalanche criteria along with a construction method for generalized Boolean functions. We introduce the notion of a uniform avalanche criterion and demonstrate that generalized Boolean functions that satisfy this criterion are also order 1 correlation immune and always have Boolean function components that are both order 1 correlation immune and satisfy the strict avalanche criterion. We subsequently investigate linear structures, directional derivatives and define a unit vector gradient for generalized Boolean function. We introduce the Walsh-Hadamard transform of a generalized Boolean function along with the notion of generalized bent Boolean functions. We provide a construction of generalized bent Boolean functions with outputs in Z8 and establish necessary conditions for generalized bent Boolean functions. Full Text

Keywords: cryptography, coding theory, Boolean functions, generalized Boolean functions, correlation immunity, strict avalanche criterion, bent functions, cyber, information warfare, information security, communications security

DECEPTION USING AN SSH HONEYPOT
Ryan J. McCaughey–Second Lieutenant, United States Army
Master of Science in Cyber Systems and Operations
Advisor: Neil Rowe, Department of Computer Science
Second Reader: Alan Shaffer, Department of Information Sciences

The number of devices vulnerable to unauthorized cyber access has been increasing at an alarming rate. A honeypot can deceive attackers trying to gain unauthorized access to a system; studying their interactions with vulnerable networks helps better understand their tactics. We connected an SSH honeypot responding to secure-shell commands to the Naval Postgraduate School network, bypassing the firewall. During four phases of testing, we altered the login credential database and observed the effects on attackers using the honeypot. We used different deception techniques during each phase to encourage more interaction with the honeypot. Results showed that different attackers performed different activities on the honeypot. These activities differed in total login attempts, file downloads, and commands used to interact with the honeypot. Attackers also performed TCP/IP requests from our honeypot to direct traffic to other locations. The results from this experiment confirm that testing newer and updated tools, such as honeypots, can be extremely beneficial to the security community by helping to prevent attackers from quickly identifying a network environment. Full Text

Keywords: honeypot, deception, SSH

PARALLEL PROCESSING WITH TREECLUST
I. Taylor McKechnie–Captain, United States Marine Corps
Master of Science in Operations Research
Advisor: Samuel E. Buttrey, Department of Operations Research
Second Reader: Lyn R. Whitaker, Department of Operations Research

Clustering data is one of the most common statistical and machine learning techniques for analyzing big data. Clustering can be particularly difficult when the data sets include categorical, missing, or noise variables. The tree clustering algorithm developed by Samuel Buttrey and Lyn Whitaker, as described in the December 2015 issue of The R Journal, seems to provide a solution to these problems, but it requires a large set of overhead computations. This issue is intensified when working with high-dimensional data because the extent of treeClust's overhead computations are based on the dimensions of the data. High performance computing (HPC) and parallel processing present a solution to this overhead computation burden, but treeClust's existing parallel processing method does not work on the Naval Postgraduate School's HPC, the Hamming Supercomputer (HSC). Furthermore, correctly determining what HPC resources to use can be a difficult task. In this thesis, we present a new HSC-specific method for parallel processing data using the treeClust R package developed by Buttrey and Whitaker. Based on the results of our experiments, our method approximates the optimal resource HPC request, so that users realize the best run time when using treeClust on the HSC. Full Text

Keywords: tree clusters, parallel processing, high performance computing, big data sets, batch scripting,

information systems technology

RECRUITING THE CYBER LEADER: AN EVALUATION OF THE HUMAN RESOURCE MODEL USED FOR RECRUITING THE ARMY'S "CYBER OPERATIONS OFFICER"
Wallace C. Nicholson–Major, United States Army
Sean A. Gibbs–Major, United States Army
Master of Science in Information Technology Management
Advisor: Steve Mullins, Department of information Sciences
Advisor: Alejandro Hernandez Department of Systems Engineering
Second Reader: William Hatch, Graduate School of Business and Public Policy

For the first time since the creation of the Special Forces branch in 1987, the Army authorized the creation of a new branch, the Cyber branch. With this, the Army joined the ranks of other organizations in this rapidly expanding arena. The Army found itself in a situation where it needed to quickly fill the positions required of this new branch. To accomplish this goal, the Army developed a recruitment strategy based on the Army human resource management model. The purpose of our research is to evaluate the effectiveness of that model to recruit Cyber Operations Officers and to examine the effects of its continued use. To perform this evaluation, we conduct an operational assessment that included identifying and assessing measures of performance (MOPs) and measures of effectiveness (MOEs) based on data collected from: Army institutions; a survey of the Cyber Branch population; and the Person-Event Data Environment database. Our research also examined recruitment strategies and practices in other selected organizations to identify practical recommendations for improvements to current Army practices. The results of this research suggest that while the Army was generally successful in accomplishing the identified tasks of its recruitment strategy, there were inconsistencies in its application. Additionally, through analysis of the survey data we were able to identify attributes that had the most impact on achieving desired effects. Finally, we found that the Army did not recruit in accordance with best practices for the cyber workforce and that it did not use available tools to measure aptitude in its recruitment and the selection process. We identify some practical implications and provide recommendations for further research in this fast-paced operational environment. Full Text

Keywords: cyber, cyber operations, Cyber Operations Officer, human resource management, recruitment

INVESTIGATING THE DETECTION OF MULTI-HOMED DEVICES INDEPENDENT OF OPERATING SYSTEMS
Javan A. Rhinehart–Lieutenant Commander, United States Navy
Master of Science in Electrical Engineering
Advisor: Murali Tummala, Department of Electrical and Computer Engineering
Advisor: John C. McEachen, Department of Electrical and Computer Engineering
Second Reader: Bryan J. Martin, Department of Electrical and Computer Engineering

Networks protected by firewalls and physical separation schemes are threatened by multi-homed devices. The purpose of this study is to detect multi-homed devices on a computer network. More

specifically, the goal is to evaluate passive detection of multi-homed devices running various operating systems while communicating on a network. TCP timestamp data was used to estimate clock skews using linear regression and linear optimization methods. Analysis revealed that detection depends on the consistency of the estimated clock skew. Through vertical testing, it was also shown that clock skew consistency depends on the installed operating system. The linear programming and linear regression methods agree with one another when clock skews are consistent, indicating that linear regression is sufficient to identify multi-homed hosts in networks with low network delay. Further analysis showed inconsistencies of clock skew estimation on newer versions of OS X and freeBSD 12.0; the clock skews from these operating systems prevented multi-homed fingerprinting using the proposed detection scheme. Full Text

Keywords: software-defined network, multi-homed host, network monitoring, fingerprinting, clock skew

DEVELOPMENT OF A VISION-BASED SITUATIONAL AWARENESS CAPABILITY FOR UNMANNED SURFACE VESSELS

Ying Jie Benjemin Toh–Civilian, Singapore Technologies Electronics Limited
Master of Science in Systems Engineering
Advisor: Oleg A. Yakimenko, Department of Systems Engineering
Second Reader: Fotis A. Papoulias, Department of Systems Engineering

The current generations of unmanned surface vessels (USVs) are reliant on the human operator for collision avoidance. This reliance poses a constraint on the operational envelope of the USV, as it requires a high bandwidth and low latency communication link between the USV and control station. This thesis adopts a systems engineering approach in identifying the capability gap and the factors that drive the need for a USV with autonomous capability. An algorithm employing edge detection and morphological structuring methods is developed in this thesis to explore the feasibility of using a computer vision–based technique to provide a situational awareness capability, which is required to achieve autonomous navigation. The algorithm was tested with both color video imagery and infrared video imagery, and the results obtained from processing the images demonstrated the viability of using this information to provide situational awareness to the USV. It is recommended that further work be done to improve the robustness of the algorithm. Full Text

Keywords: unmanned systems, situational awareness

PERFORMANCE ANALYSIS OF WIRELESS NETWORKS FOR INDUSTRIAL AUTOMATION-PROCESS AUTOMATION (WIA-PA)

Brandon Wyatt–Lieutenant, United States Navy
Master of Science in Electrical Engineering
Advisor: Preetha Thulasiraman, Department of Electrical and Computer Engineering
Second Reader: John McEachen, Department of Electrical and Computer Engineering

The Wireless Networks for Industrial Automation-Process Automation (WIA-PA) standard is not well known in North America and is a relatively new industrial control system standard when compared to WirelessHart and ISA100.11A. An evaluation of the WIA-PA standard needs to be conducted by the Department of Defense and its affiliates to determine whether its operation is on par with WirelessHart and ISA100.11A. The objective of this thesis is to provide a performance analysis of the WIA-PA standard. Utilizing MATLAB, we implemented a custom-built WIA-PA system model and measured the end-to-end delay, and received packet error rate and timeslot utilization. We expect WIA-PA to perform as well as WirelessHart and ISA100.11A in multiple network scenarios. We also found that, due to the limitations of MATLAB, further analysis of the standard should be conducted on a network simulator such that network traffic can be properly emulated and the standard's vulnerabilities can be further assessed. Full Text

Keywords: cyber, ICS, IEEE 802.15.4, Slotted CSMA/CA, WIA-PA, WSN