

2024 IEEE International Conference on Cyber Security and Resilience (CSR 2024)

**London, United Kingdom
2-4 September 2024**

Pages 1-465



**IEEE Catalog Number: CFP24Y52-POD
ISBN: 979-8-3503-7537-4**

**Copyright © 2024 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP24Y52-POD
ISBN (Print-On-Demand):	979-8-3503-7537-4
ISBN (Online):	970-8-3503-7536-7

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com



Table of Contents

Table of contents	iii
Message from the chairs	xvii
Conference sponsors	xix
Program committees	xxi
Authors' index	xxxii

Cyber security

A hybrid ensemble learning-based intrusion detection system for the Internet of things	1
<i>M. Alani, A. Awad, and E. Barka</i>	
Verifying the robustness of machine learning based intrusion detection against adversarial perturbation	9
<i>E. Nowroozi, R. Taheri, M. Hajizadeh, and T. Bauschert</i>	
ReBotDetector: A detection model with LSTM feature extractor for session-replay web bot attacks	16
<i>S. Sadeghpour and N. Vlajic</i>	
Explainable federated learning for botnet detection in IoT networks	22
<i>R. Kalakoti, H. Bahsi, and S. Nomm</i>	
Navigating (in)security of AI-generated code	30
<i>S. Ambati, N. Ridley, E. Branca, and N. Stakhanova</i>	
When rewards deceive: Counteracting reward poisoning on online deep reinforcement learning	38
<i>M. Bouhaddi and K. Adi</i>	



Are IDS violating segmentation in industrial networks?.....	45
<i>G. Gaggero, R. Caviglia, P. Girdinio, and M. Marchese</i>	
New approach to shorten feature set via TF-IDF for machine learning-based webshell detection.....	50
<i>V. Phan, J. Jerabek, D. Le, and T. Gotthans</i>	
Can deep learning detect fake news better when adding context features?.....	56
<i>R. Ladouceur, A. Hassan, F. Jaafar, and M. Mejri</i>	
A trust management delegation protocol for fog computing applications	62
<i>P. Fongta and S. Terzis</i>	
AI-based attacker models for enhancing multi-stage cyberattack simulations in smart grids using co-simulation environments.....	68
<i>O. Sen, C. Pohl, I. Hacker, M. Stroot, and A. Ulbig</i>	
A version-based algorithm for quality enhancement of automatically generated vulnerability inventories	76
<i>S. Bonomi, M. Cuoci, and S. Lenti</i>	
Enabling cyber threat intelligence sharing for resource constrained IoT	82
<i>A. Karlsson, R. Hoglund, H. Wang, A. Iacovazzi, and S. Raza</i>	
Novel approach to Tor user de-anonymization: Client-side generated watermark	90
<i>N. Vljajic and D. Brown</i>	
Deep graph learning for DDoS detection and multi-class classification IDS	96
<i>B. Saunders, R. E. de Grande, G. Carvalho, and I. Woungang</i>	
Use of visibility graphs for the early detection of DoS attacks	101
<i>J. Lopes, P. Pinto, A. Partida, and A. Pinto</i>	
A2HD: Adaptive adversarial training for hyperdimensional computing-based intrusion detection against adversarial attacks.....	107
<i>O. Gungor, T. Rosing, and B. Aksanli</i>	
Emerging trends in 5G malicious traffic analysis: Enhancing incremental learning intrusion detection strategies	114
<i>Z. Wang, K. Fok, and V. Thing</i>	
Multi-blockchain model for IoT devices forensic investigations on Spidernet.....	120
<i>S. Harding and M. Adda</i>	



A forensic framework for screen capture validation in legal contexts	127
<i>C. Greco, M. Ianni, G. Seminara, A. Guzzo, and G. Fortino</i>	
A systematic review of cybersecurity audit frameworks for the Internet of things.....	133
<i>D. Hanson and J. Straub</i>	
A survey of digital forensic tools for android and iOS smart phones	139
<i>S. Ntshangase, N. Nelufule, D. Mulihase, M. Mtshali, C. Mokoena, and P. Moloi</i>	
Active learning-based mobile malware detection utilizing auto-labeling and data drift detection.....	146
<i>Z. Deng, A. Hubert, S. Ben yahia, and H. Bahsi</i>	
Rigorous evaluation of machine learning-based intrusion detection against adversarial attacks	152
<i>O. Gungor, E. Li, Z. Shang, Y. Guo, J. Chen, J. Davis, and T. Rosing</i>	
A hybrid anomaly detection approach for obfuscated malware	159
<i>G. Shu fuhnwi, M. Revelle, and C. Izurieta</i>	
Ransomware detection: Ensemble machine learning models using disjoint data	166
<i>C. Michael Ribeiro da Silva, P. Lima de Castro, and C. De Azevedo Castro Cesar</i>	
Automatic discovery of cyberattacks.....	172
<i>G. Hutzler, H. Klaudel, W. Klaudel, F. Pommereau, and A. Rataj</i>	
Leveraging threat modelling for effective penetration testing in 5G systems.....	180
<i>L. Chianese, D. Granata, P. Palmiero, and M. Rak</i>	
The danger within: Insider threat modeling using business process models.....	186
<i>J. Von der Assen, J. Hochuli, and T. Grubl</i>	
Data siphoning in ICSs: Attack tree and role of cryptoperiods	193
<i>N. Vljajic, G. Cianfarani, and R. Noce</i>	
Harnessing TI feeds for exploitation detection.....	200
<i>K. Patel, Z. Shafiq, M. Nogueira, D. Menasche, E. Lovat, T. Kashif, A. Woiwood, and M. Martins</i>	
Attack-specific feature construction to detect malicious TCP flows.....	208
<i>V. Vedula, R. Boppana, and P. Lama</i>	



Empirical analysis and practical assessment of ransomware attacks to data in motion	216
<i>R. Reinosa Simon, C. Valero, J. Martinez Cadenas, E. Heymann, I. Lacalle, B. Miller, and C. Palau</i>	
Investigating the health state of X.509 digital certificates	222
<i>S. Orlando, A. Barengi, G. Pelosi</i>	
ROT: Retention and operation limitation using TEE	228
<i>S. Paul and D. Knox</i>	
Energy-efficient hardening of the SEDIMENT methodology for scalable IoT network security.....	235
<i>D. Shur, G. Di Crescenzo, T. Chen, Z. Patni, Y. Lin, S. Alexander, B. Flin, and R. Levonas</i>	
Detecting covert channels in cloud access control policies using large language models	241
<i>H. Karmarkar, V. Joshi, and R. Venkatesh</i>	
An end-to-end framework for cybersecurity taxonomy and ontology generation and updating	247
<i>A. Kougioumtzidou, A. Papoutsis, D. Kavallieros, T. Mavropoulos, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris</i>	
Application of robotic exploration principles to the challenge of cybersecurity penetration testing.....	255
<i>J. Straub</i>	
Leveraging reinforcement learning in red teaming for advanced ransomware attack simulations.....	262
<i>C. Wang, C. Redino, R. Clark, A. Rahman, S. Aguinaga, S. Murli, D. Nandakumar, R. Rao, L. Huang, D. Radke, and E. Bowen</i>	
Autonomous cyberattack with security-augmented generative artificial intelligence.....	270
<i>J. Gregory and Q. Liao</i>	
A looping process for cyberattack mitigation.....	276
<i>D. Brighenti, F. Pizzato, R. Sisto, and F. Valenza</i>	
Structural generalization in autonomous cyber incident response with message-passing neural networks and reinforcement learning	282
<i>J. Nyberg and P. Johnson</i>	



Ineffectiveness of digital transformations for detecting adversarial attacks against quantized and approximate CNNs	290
<i>S. Della Torca, S. Barone, and V. Casola</i>	
CyberMetric: A benchmark dataset based on retrieval-augmented generation for evaluating LLMs in cybersecurity knowledge	296
<i>N. Tihanyi, M. Amine Ferrag, R. Jain, T. Bisztray, and M. Debbah</i>	
A time-series and density-based filter for DNS log reduction and analysis.....	303
<i>T. Perkins and B. Lachine</i>	
A security analysis of a deterministic key generation scheme	309
<i>D. Song, Y. Yan, G. Shao, F. Zhu, and M. Song</i>	
Detecting cryptographic functions for string obfuscation	315
<i>P. Mondon and R. De Lemos</i>	
Dynamic security provisioning for cloud-native networks: An intent-based approach	321
<i>F. Settanni, A. Zamponi, and C. Basile</i>	
Enhancing ATM security management in the post-quantum era with quantum key distribution.....	329
<i>F. Ahmad, A. Kanta, S. Shiaeles, A. Naeem, Z. Khalid, and K. Mahboob</i>	
Peer-to-peer meets onion: The Veilid framework	335
<i>S. Glatzer, S. Shiaeles, R. Khusainov, and R. Taheri</i>	
Understanding and mitigating the challenges of securing Jupyter notebooks online.....	341
<i>A. Ramsingh and P. Verma</i>	
Identifying Android banking malware through measurement of user interface complexity.....	348
<i>S. McElroy</i>	
Forensic analysis of android notifications' history.....	354
<i>E. Dragonas and C. Lambrinoudakis</i>	
Building a secure cross-device communication channel for smart devices based on app accounts	360
<i>L. Pan, R. Qiu, C. Zhang, and M. Yang</i>	
A privacy-preserving and secure scheme for online payment in the realm of mobile commerce.....	367
<i>M. Momeni, A. Jabbari, and C. Fung</i>	



IPv6 connection shuffling for moving target defense (MTD) in SDN.....	373
<i>N. Mayone, P. Kunz, B. Yigit, W. Soussi, B. Stiller, and G. Gur</i>	
Evaluating few-shot learning generative honeypots in a live deployment.....	379
<i>J. Ragsdale and R. Boppa</i>	
A modular generative honeypot shell.....	387
<i>S. Johnson, R. Hassing, J. Pijpker, and R. Loves</i>	
Can a llama be a watchdog? Exploring llama 3 and code llama for static application security testing.....	395
<i>C. Curto, D. Giordano, D. Indelicato, and V. Patatu</i>	
Video-based abnormal human behaviour detection for video forensics	401
<i>I. Ziani, G. Bendiab, M. Bouzenada, and S. Shiaeles</i>	
On impact of video motion on image encryption/decryption. Comparative results.....	407
<i>M. Oussalah and A. Voitenko</i>	
Static detection of missing validations in solidity smart contracts.....	413
<i>S. Munir, W. Taha, and M. Baig</i>	
SEAGuard: A blockchain-based security framework for IoT maritime transportation systems.....	421
<i>P. Leonis, K. Ntouro, A. Mazilu, S. Brotsis, and N. Kolokotronis</i>	
Renyi differential privacy analysis of Skellam under federated learning in Internet of health things.....	427
<i>M. Amjath and S. Henna</i>	
Software security testing lifecycle for automotive products	432
<i>A. Pandey and K. Singh</i>	

Cyber resilience

Asset-centric threat modeling for AI-based systems.....	437
<i>J. Von der Assen, J. Sharif, and C. Feng</i>	
Third-party cloud risk management.....	445
<i>B. Pinto</i>	



Zero to trust? Bringing application-level intelligence at scale to detection engineering	452
<i>F. Gey, C. Hebert, and H. Mack</i>	
Towards live detection of ransomware attacks.....	458
<i>K. Thummapudi, R. Boppana, and P. Lama</i>	
DefenceRank – Ranking based attack graph analysis and defence prioritization	466
<i>R. Patil, M. Kallman, and V. Fodor</i>	
On the ISO compliance of model-based risk assessment for autonomous cyber-physical production systems	474
<i>M. Zahid, A. Bucaioni, and F. Flammini</i>	
The need for cyber-resilience in complex systems.....	480
<i>S. Acur and T. Hendriks</i>	
A lightweight firmware resilience engine for IoT devices leveraging minimal processor features.....	486
<i>U. Budak, F. De Santis, and G. Sigl</i>	
Advancing security in 5G core networks through unsupervised federated time series modeling	492
<i>S. Sheikhi and P. Kostakos</i>	
Using a sensor-health-aware resilient fusion for localization in the presence of GPS spoofing attacks	498
<i>S. Moosavi, I. Moore, and S. Gopalswamy</i>	
Identifying novelty in network traffic.....	506
<i>J. Sylvester and R. De Lemos</i>	
Safety analysis for cyber-physical systems under cyber attacks using digital twin	512
<i>R. Wang, S. Venugopalan, and S. Adepu</i>	
Situational awareness scoring system in cyber range platforms	520
<i>A. Damianou, M. Mazi, G. Rizos, A. Voulgaridis, and K. Votis</i>	
Cybersecurity as a backbone for sustainability	526
<i>G. Sargsyan</i>	
Assessment of the impact of cyber-attacks and security breaches in diagnostic systems on the healthcare sector	531
<i>K. Srivastava, K. Faist, B. Lickert, K. Neville, N. McCarthy, M. Fehling-Kaschek, and A. Stolz</i>	



A SDR-based framework for cybersecurity assessment of vehicle-to-everything (V2X) systems.....	537
<i>M. Sohail, F. Patrone, G. Portomauro, and M. Marchese</i>	
The affordability of cybersecurity costs in developing countries: A systematic review	545
<i>C. Uwaoma and A. Enkhtaivan</i>	
The effect of privacy concerns, interaction, trust, age, and gender on self-disclosure behaviours on social networking sites	551
<i>A. Coca, F. Li, S. Shiaeles, D. Wu, and F. Liu</i>	
Strengthening the digital ecosystem: Effects of the cyber resilience act (CRA) on open-source software	557
<i>M. Kikelj and I. Sabic</i>	
Designing trustworthy decentralized cross-chain marketplaces: A 6G network of networks perspective	562
<i>L. Jagadeesan, S. Liu, and L. Velazquez</i>	
Strengthening cybersecurity certifications through robust chain of custody practices	570
<i>J. Cosic, A. Jukan, and M. Baca</i>	
Investigating cyber risks in a surgical process for healthcare cyber resilience	575
<i>M. Pourmadadkar, M. Lezzi, and A. Aghazadeh Ardebili</i>	

Cyber physical systems security

Anomaly detection in operational technology systems using non-intrusive load monitoring based on supervised learning	581
<i>A. Schroeder, P. McClure, and P. Thulasiraman</i>	
Building a use case-driven adversarial threat matrix: A comprehensive approach.....	587
<i>P. Kiriakidis, E. Kafali, G. Rizos, A. Voulgaridis, T. Semertzidis, S. Gazut, P. Daras, and K. Votis</i>	
Unraveling the threat landscape of CPS: Modbus TCP vulnerabilities in the era of I4.0	593
<i>G. Lazaridis, A. Drosou, P. Chatzimisios, and D. Tzouvaras</i>	
Vehicular network security against RF jamming: An LSTM detection system.....	599
<i>M. Murshed, A. Jubaida, R. E. de Grande, and G. Silva de Carvalho</i>	



From data to defense: Real-time detection of botnets in IoT using LSTM networks	605
<i>S. Sadeghpour, F. Zareen, and W. Johnson</i>	
Toward a unified security framework for digital twin architectures	612
<i>S. Abdullahi and S. Lazarova-Molnar</i>	
Secure AI/ML-based control in intent-based management system	618
<i>L. Karaçay, A. Baktir, R. Fuladi, E. Dehghan Biyar, Ö. Faruk Tuna, and I. Arikan</i>	
DIONYSUS: Leveraging digital-twin deception networks for the cybersecurity of physical protection systems	624
<i>C. De la Vergne de Cerval, W. Stout, E. Perret, J. Sarrazin, O. Fichot, V. Urias, and S. Maldonado Rosado</i>	
Enhancing cyber-physical security: Integrating virtual fences within digital twins.....	630
<i>A. Aghazadeh Ardebili, A. Longo, and A. Ficarella</i>	
Lightweight testbed for IEC61162-450-related cyber security research	638
<i>G. Visky, S. Katsikas, and M. Olaf</i>	
Hybrid cybersecurity research and education environment for maritime sector	644
<i>G. Visky, A. Siganov, U. Muan, R. Vaarandi, H. Bahsi, and L. Tsiopoulos</i>	
Cybersecurity for safety: Risk assessment of autonomous cyber-physical systems	652
<i>S. Perone, L. Faramondi, S. Guarino, R. Setola, M. Nobili, F. Flammini, and F. Corradini</i>	

CSR WS privacy-preserving data processing and analysis (2P-DPA)

DSCS: Towards an extensible secure decentralised distributed computation protocol	658
<i>A. Dalton, D. Thomas, and P. Cheung</i>	
A novel approach for securing federated learning: Detection and defense against model poisoning attacks	664
<i>G. Cristiano, S. D'Antonio, and F. Uccello</i>	
Secure and transparent data sharing among connected devices: Integrating data spaces and provenance	670
<i>R. Nardone, A. Petruolo, and F. Uccello</i>	



Enhancing healthcare data confidentiality through decentralized TEE attestation	676
<i>S. D'Antonio, J. Giglio, G. Mazzeo, F. Uccello, and T. Mannarino</i>	
Simplifying differential privacy for non-experts: the ENCRYPT project approach	682
<i>S. Erotokritou, I. Giannoulakis, E. Kafetzakis, and K. Kaltakis</i>	
ZADIG: A novel extended detection and response system	688
<i>S. Perone, L. Faramondi, S. Guarino, R. Setola, M. Nobili, E. Del Prete, G. Patruno, L. Piccirillo, and A. Laurenda</i>	
Towards GPU accelerated FHE computations	694
<i>O. Papadakis, M. Papadimitriou, A. Stratikopoulos, M. Xekalaki, J. Fumero, N. Foutris, and C. Kotselidis</i>	
Towards a generic framework for knowledge graph construction: The healthcare domain	700
<i>C. Karalka, G. Meditskos, M. Papoutsoglou, and N. Bassiliades</i>	

CSR WS security, privacy and resilience of critical assets in critical infrastructure (SPARC)

Active honeyfiles for ransomware encryption mitigation	706
<i>I. Stamelos, G. Hatzivasilis, and S. Ioannidis</i>	
Adversarial attacks in intrusion detection systems: Triggering false alarms in connected and autonomous vehicles	714
<i>F. Aloraini and A. Javed</i>	
Towards developing an asset-criticality identification framework in smart grids	720
<i>Y. Alrowaili, N. Saxena, and P. Burnap</i>	
Foundations for modelling conscientious attacking in electromagnetic cyberspace	726
<i>N. Davies, H. Dogan, D. Ki-Aries, N. Jiang, and C. Williams</i>	
The impact of GPS interference in the middle east	732
<i>V. Ieropoulos</i>	



CSR WS synthetic data generation for a cyber-physical world (SDGCP)

Synthetic data for identifying inclusive language (Case study: Job descriptions in Italian) 737
T. Romano', F. Mohammadi, and P. Ceravolo

Active learning methodology in large language models fine-tuning 743
P. Ceravolo, F. Mohammadi, and M. Tamborini

CSR WS cyber resilience and economics (CRE)

Cyber resilience in OT: Characteristics and security challenges 750
M. Cotiga, J. Pedersen, and E. Dushku

Framework for quantitative evaluation of resilience solutions: An approach to determine the value of resilience for a particular site 757
M. Weimar

PentestAI: An LLM-powered multi-agent framework for penetration testing automation leveraging MITRE ATTACK 763
S. G. Bianou and R. G. Batogna

Taxonomy of cyber risk mitigation cost benefit analysis methods for energy infrastructure 771
Y. Kam, K. Tam, K. Jones, and R. Rawlinson-Smith

CSR WS electrical power and energy systems security, privacy and resilience (EPES-SPR)

AI-driven anomaly and intrusion detection in energy systems: Current trends and future direction 777
G. Andronikidis, C. Eleftheriadis, Z. Batzos, K. Kyranou, P. Radoglou-Grammatikis, N. Maropoulos, G. Sargsyan, and P. Sarigiannidis

AI4COLLAB: An AI-based threat information sharing platform 783
C. Dalamagkas, D. Asimopoulos, P. Radoglou-Grammatikis, N. Maropoulos, T. Lagkas, V. Argyriou, G. Sargsyan, and P. Sarigiannidis



SDN-based reconfiguration of distributed and cooperative microgrid control systems for mitigating synchronization attacks	789
---	-----

A. Kpoze, A. Lahmadi, I. Chrisment, and J. Degila

CSR WS dependability and resilience in digital cultural heritage ecosystems (DR-DCHE)

Towards a reputational-based trustworthy archaeological information system	795
--	-----

E. Bellini, M. Bottoni, and E. Farinetti

Transitioning SSH European research infrastructures to critical infrastructure through resilience	801
---	-----

E. Bellini and E. Innocenti

CSR WS autonomic computing for secure industrial control systems and industrial-IoT (ACSICS)

SoK: Autonomic computing based methods for ICS/SCADA and IIoT security	807
--	-----

C. Rouff and A. Tekeoglu

Autonomic passive IT-OT device classification in ICS/SCADA networks	813
---	-----

B. Rubin, A. Tekeoglu, and C. Rouff

CSR WS information and operational technology security (IOSEC)

Developing a robust communication infrastructure for a distributed smart grid IDS	819
---	-----

V. Menzel, J. Speckamp, and A. Remke

SecureExecutor: An automated way to leverage SCONE to enhance application security	827
--	-----

C. Spyridakis, A. Aktypi, T. Kyriakakis, and S. Ioannidis

Composite inspection and certification (CIC) system for cybersecurity assessment of ICT products, services, and processes	833
---	-----

S. Papastergiou, S. Islam, and E. M. Kalogeraki



A deep learning framework for safety monitoring of a railway section.....	839
<i>F. Chriki, E. Simo, F. Aguilo, I. Garcia-Mila, and X. Masip</i>	
Quantifying the odds in real world attack scenarios.....	845
<i>P. Tavolato, S. Eresheim, R. Luh, S. Gmeiner, and S. Schrittwieser</i>	
OntoHunt – A semantic reasoning approach to cyber threat hunting with indicators of behaviour	853
<i>R. Chetwyn, M. Eian, and A. Josang</i>	
Uncovering hidden threats: Automated, machine learning-based discovery and extraction of cyber threat intelligence from online sources.....	860
<i>R. Ellinitakis, K. Fysarakis, P. Bountakas, and G. Spanoudakis</i>	
DID:RING: Ring signatures using decentralised identifiers for privacy-aware identity proof.....	866
<i>D. Kasimatis, S. Grierson, W. Buchanan, C. Eckl, P. Papadopoulos, N. Pitropakis, C. Chrysoulas, C. Thomson, and B. Ghaleb</i>	

CSR WS cyber forensics and advanced threat investigations in emerging technologies (CFATI)

Challenges of digital investigations in nowadays communication networks	872
<i>D. Spiekermann and J. Keller</i>	
Forensic communication analysis: Challenges and opportunities	878
<i>J. Xi, L. Jaeckel, M. Spranger, M. Siegel, and D. Labudde</i>	

CSR WS hardware cybersecurity systems (HACS)

Static power consumption as a new side-channel analysis threat to elliptic curve cryptography implementations	884
<i>I. Kabin, Z. Dyka, A. Sigourou, and P. Langendoerfer</i>	
Communication architecture under siege: An in-depth analysis of fault attack vulnerabilities and countermeasures.....	890
<i>H. Zhao, V. Lapotre, and G. Gogniat</i>	



On-line anomaly detection and qualification of random bit streams.....	897
<i>C. Caratozzolo, V. Rossi, K. Witek, A. Trombetta, and M. Caccia</i>	
Stealth attacks on PCBs: An experimental plausibility analysis	905
<i>I. Kabin, J. Schaeffner, A. Sigourou, D. Petryk, Z. Dyka, D. Klein, S. Freud, and P. Langendoerfer</i>	
FPGA-based cloud security for 5G networks.....	913
<i>M. Papadopoulos, K. Lampropoulos, and P. Kitsos</i>	
Minimizing area footprint of UAV communication security using FPGAs.....	919
<i>E. Konstantopoulou, G. Athanasiou, and N. Sklavos</i>	