

Contents

Part I Bio-inspiring Systems in Cyber Security

1	A Bio-inspired Comprehensive Distributed Correlation Approach for Intrusion Detection Alerts and Events	3
	Ayman M. Bahaa-Eldin	
1.1	Introduction	4
1.1.1	IDS Correlation Problem Definition	4
1.1.2	Article Organization	4
1.2	Related Work	5
1.2.1	Distributed and Bio Inspired Intrusion Detection	5
1.2.2	Distributed Correlation	5
1.2.3	Agents in IDS and Correlation	5
1.2.4	Comprehensive Approach Model for IDS Alert Correlation	5
1.2.5	Distributed Agent Correlation Model	6
1.2.6	IDSs Correlation Agents	7
1.2.7	INFOSEC Tools Agents	8
1.2.8	System and Application Log Agents	8
1.2.9	DACM Central Agent	9
1.2.10	Response Agent	10
1.2.11	Learning Agent	10
1.2.12	The Knowledge Base and Security Policy	10
1.2.13	DACM Components	11
1.2.14	Implementation Scope and Performance Enhancement	12
1.3	DACM Design and Algorithms	12
1.3.1	IDS Alert Correlation	12
1.3.2	Modified CAM Time	13
1.3.3	DACM Individual Agents	15
1.3.4	Implementation Environment	27
1.4	DACM Results and Analysis	27
1.4.1	CRIAS Data Set	27
1.4.2	IDS Alerts Correlation Results	28
1.4.3	DACM Components Results	31

1.4.4	DACM Central Agent Results	32
1.4.5	DACM Evaluation and Assessment	33
1.5	Conclusions and Future Work	35
	References	36
2	Bio-inspired Evolutionary Sensory System for Cyber-Physical System Security	39
	Mohamed Azab and Mohamed Eltoweissy	
2.1	Introduction	40
2.2	Attack Scenario	42
2.3	CPS Attack Detection and Resolution Techniques	45
2.3.1	Malware Detection	45
2.3.2	Standalone and Distributed Monitoring and Evaluation Solutions	48
2.3.3	CPS Related Control Solutions	50
2.4	Evolutionary Sensory System (CyPhyMASC)	51
2.4.1	Overview of the Cell-Oriented Architecture	51
2.4.2	The Foundation	52
2.4.3	CyPhyMASC Security Provisioning Methodology	53
2.4.4	Evolutionary Sensing and Effecting Framework	56
2.4.5	CyPhyMASC Brain Architecture	58
2.5	Example of CyPhyMASC Security Mission	65
2.5.1	Detection and Resolution Scenario	66
2.5.2	CyPhyMASC Addressing the BW Attacker Assumptions	67
2.6	Conclusion	68
	References	68
3	An Optimized Approach for Medical Image Watermarking	71
	Mona M. Soliman, Aboul Ella Hassanien and Hoda M. Onsi	
3.1	Introduction	72
3.2	Preliminaries	74
3.2.1	Swarm Intelligent Optimization	74
3.3	The Proposed Medical Watermarking Approach	80
3.3.1	Watermark Embedding Procedure	80
3.3.2	Watermark Extraction Procedure	83
3.4	Experimental Results and Analysis	84
3.4.1	Evaluation Analysis	85
3.4.2	Convergence Comparison	88
3.5	Conclusion and Future Works	89
	References	90

4	Bio-inspiring Techniques in Watermarking Medical Images:	
	A Review	93
	Mona M. Soliman, Aboul Ella Hassanien and Hoda M. Onsi	
4.1	Introduction	94
4.2	Bio-inspiring Computing	95
4.2.1	Artificial Neural Networks.	95
4.2.2	Evolutionary Algorithms	96
4.2.3	Genetics Algorithms	97
4.2.4	Swarm Intelligence	98
4.3	Medical Image Watermarking: Classification and Generic Model	99
4.3.1	Medical Watermarking Classification	100
4.3.2	Generic Medical Image Watermarking System.	101
4.4	BI in Medical Image Watermarking	102
4.4.1	Artificial Neural Networks in Medical Image Watermarking	102
4.4.2	Genetic Algorithms in Medical Image Watermarking	103
4.4.3	Swarms Intelligent in Medical Image Watermarking	104
4.4.4	Hybrid Bio-inspiring Systems in Medical Watermarking	107
4.5	Watermarking Assessment Measures.	108
4.5.1	Imperceptibility or Transparency	109
4.5.2	Robustness.	110
4.6	Conclusions and Future Directions	111
	References	112
5	Efficient Image Authentication and Tamper Localization	
	Algorithm Using Active Watermarking	115
	Sajjad Dadkhah, Azizah Abd Manaf and Somayeh Sadeghi	
5.1	Introduction	116
5.2	Related Work.	118
5.2.1	Digital Image Authentication Methods	118
5.3	The Proposed Algorithm	120
5.3.1	The Proposed Watermarking Scheme	121
5.3.2	The Proposed Tamper Detection Scheme	130
5.4	Experimental Results	133
5.4.1	Watermark Quality Experiments Result.	134
5.4.2	Tamper Detection Experiments Results	136
5.4.3	Deletion and Copy-Move Tampering Attacks.	136
5.4.4	Bit Tampering Experiments Results	142
5.5	Conclusion.	146
	References	146

Part II Mobile Ad Hoc Networks and Key Managements

6	TARA: Trusted Ant Colony Multi Agent Based Routing Algorithm for Mobile Ad-Hoc Networks	151
	Ayman M. Bahaa-Eldin	
6.1	Introduction	151
6.2	Background	153
6.2.1	Mobile Ad-Hoc Networks	153
6.2.2	Swarm Intelligence	161
6.3	Trusted Routing Protocols for MANETs	163
6.3.1	Examples of Trusted Routing Protocols.	163
6.4	Trusted Ant Colony Based Routing Algorithm for Mobile Ad-Hoc Networks.	169
6.4.1	Routing Table Data Structure.	171
6.4.2	Node Trust Evaluation	171
6.4.3	Route Discovery.	172
6.4.4	Route Selection and Route Failure Handling	175
6.4.5	Route Maintenance.	175
6.4.6	TARA Complexity Analysis	176
6.5	Performance Evaluation of TARA	177
6.5.1	Simulation Environment	177
6.5.2	Simulation Results and Analysis.	178
6.6	Conclusion.	181
	References	182
7	An Overview of Self-Protection and Self-Healing in Wireless Sensor Networks.	185
	Tarek Gaber and Aboul Ella Hassanien	
7.1	Introduction	185
7.2	Wireless Sensor Networks Architecture.	186
7.3	Autonomic Computing	187
7.3.1	Autonomic Computing Characteristic	188
7.3.2	Autonomic Computing Elements	189
7.4	Self-Protection	190
7.4.1	Self-Protection in WSN.	191
7.5	Self-Healing.	193
7.6	Self-Healing in WSNs.	195
7.6.1	Existing Solution of WSN with Self-Healing	195
7.7	BiSNET: Biologically-Inspired Architecture for Sensor NETworks.	198
7.7.1	Overview of BiSNET	198
7.7.2	Self-Healing in BiSNET	199
7.8	Conclusions	200
	References	201

8	Cybercrime Investigation Challenges: Middle East and North Africa	203
	Mohamed Sarrah, Nasser Alalwan, Ahmed Alzahrani and Mahdi Kordestani	
8.1	Introduction	204
8.2	Related Work.	205
8.3	Conceptualizing Cybercrime	205
8.4	State of Information Security in North Africa and Middle East	206
8.4.1	Information Technology Infrastructure	207
8.4.2	Growth of IT User	207
8.4.3	Lack of Regulations and Training of Law Enforcements	208
8.5	Internet Users and Population Statistics for Middle East	208
8.6	Internet Users and Population Statistics for North Africa.	210
8.7	Case Study	213
8.7.1	Stuxnet	213
8.7.2	W32.Disttrack	214
8.7.3	Duqu.	216
8.7.4	Flame	218
8.8	Discussion	219
8.9	Challenges	220
8.10	Conclusion.	221
	References	222
9	Multilayer Machine Learning-Based Intrusion Detection System	225
	Amira Sayed A. Aziz and Aboul Ella Hassanien	
9.1	Introduction	226
9.2	Background	227
9.2.1	Intrusion Detection Systems.	227
9.2.2	Genetic Algorithm	228
9.2.3	Principal Component Analysis	228
9.2.4	Artificial Immune System	230
9.2.5	Negative Selection Algorithm	230
9.3	The Proposed Multilayer Machine Learning-Based IDS	231
9.3.1	Layer I: Feature Selection Based Principal Components Analysis Layer.	232
9.3.2	Layer II: Anomaly Detection-Based Genetic Algorithm with Negative Selection Layer	233
9.3.3	Layer III: Detected Anomalies Classification Layer	234

9.4	Experimental Results and Discussion	235
9.4.1	Data Set	235
9.4.2	Results	236
9.5	Conclusion and Future Work	245
	References	246
10	An Improved Key Management Scheme with High Security in Wireless Sensor Networks	249
	D. Satish kumar, N. Nagarajan and Ahmad Taher Azar	
10.1	Introduction	250
10.2	Related Work.	251
10.3	INTK Scheme	253
10.3.1	Initial INTK Setup Process	255
10.3.2	INTK Structure Operation Algorithm	257
10.3.3	INTK Security Feature	258
10.4	Simulation Environment	259
10.5	Results and Discussion	260
10.6	Conclusion.	263
	References	263
11	Key Pre-distribution Techniques for WSN Security Services	265
	Mohamed Mostafa M. Fouad and Aboul Ella Hassanien	
11.1	Introduction	265
11.2	Security Services for the WSNs	266
11.2.1	Authentication	266
11.2.2	Data Confidentiality	267
11.2.3	Data Integrity.	267
11.2.4	Availability	268
11.2.5	Data Freshness	268
11.2.6	Self-Organization	268
11.2.7	Time Synchronization	269
11.2.8	Secure Localization	269
11.3	WSN's Threat Model	269
11.4	Security Attacks on Sensor Networks	270
11.5	Key Distribution Techniques for Distributed WSNs	272
11.6	Pairwise Key Distributed Schemes	273
11.6.1	Polynomial Based Key Pre-distribution Scheme	274
11.6.2	Probabilistic Key Pre-distribution (PRE)	275
11.6.3	Q-Composite Random Key Pre-distribution Scheme	276
11.6.4	Random Pairwise Keys Scheme	276

11.6.5	Polynomial Pool-Based Key Pre-distribution Scheme	276
11.6.6	Location Based Pairwise Key Scheme.	278
11.6.7	Time Based Pairwise Key Scheme	279
11.7	Conclusion and Future Works	280
	References	281

Part III Biometrics Technology and Applications

12	Fusion of Multiple Biometric Traits: Fingerprint, Palmprint and Iris	287
	N. L Manasa, A Govardhan and Ch Satyanarayana	
12.1	Introduction	288
12.1.1	Kinds of Information Fusion	293
12.2	Motivation and Challenges	294
12.2.1	Fusion of Multiple Representations of Single Biometric Trait.	294
12.2.2	Fusion of Multiple Biometric Traits	295
12.3	Contributions	297
12.4	Fusion of Multiple Representations of Individual Fingerprint, Palmprint and Iris	298
12.4.1	Global Feature Extraction	299
12.4.2	Local Feature Extraction	301
12.4.3	Feature Fusion	302
12.4.4	Feature Matching	304
12.5	Fusion of Multiple Biometric Traits: Fingerprint, Palmprint, Iris	304
12.5.1	Parallel Architecture Based Fusion	309
12.5.2	Hierarchical-Cascading Architecture Based Fusion	311
12.6	Description of Databases	315
12.7	Discussion and Future-Work	316
	References	318
13	Biometric Recognition Systems Using Multispectral Imaging	321
	Abdallah Meraoumia, Salim Chitroub and Ahmed Bouridane	
13.1	Introduction	322
13.2	Related Works	323
13.3	Multimodal Biometric System	324
13.3.1	Fusion at Image Level	324
13.3.2	Fusion at Matching Score Level.	325

13.4	Multispectral Palmprint Identification	325
13.4.1	Multispectral Palmprint Image	325
13.4.2	Multispectral Palmprint Database	326
13.4.3	Palmprint Preprocessing	326
13.4.4	Unimodal Identification System Test Results	327
13.4.5	Multimodal Identification System Test Results.	339
13.5	Reliability of Multispectral Imaging	342
13.6	Summary and Conclusions.	344
	References	345
14	Electrocardiogram (ECG): A New Burgeoning Utility for Biometric Recognition.	349
	Manal Tantawi, Kenneth Revett, Abdel-Badeeh Salem and M. Fahmy Tolba	
14.1	Introduction	350
14.2	Heart Fundamentals	352
14.2.1	Heart Anatomy.	352
14.2.2	Flow of Blood	352
14.2.3	The Electrical Activity of the Heart	352
14.3	Electrocardiogram.	353
14.3.1	ECG and Biometrics.	354
14.3.2	ECG Motivation.	354
14.3.3	ECG Challenges.	354
14.4	Existing ECG Based Biometric Systems	355
14.4.1	Fiducial Based Systems.	356
14.4.2	Non-Fiducial Based Systems	361
14.4.3	Combined Fiducial and Non-fiducial Based Systems.	367
14.4.4	Fiducial Versus Non-fiducial Based Systems	369
14.5	Methodology	371
14.5.1	Data Preparation.	371
14.5.2	Preprocessing.	371
14.5.3	Feature Extraction	372
14.5.4	Feature Reduction.	372
14.5.5	Classification	374
14.6	Results and Discussion	375
14.6.1	The Global Phase (Significance of the Structure Parts).	376
14.6.2	Local Phase (Significance of Coefficients).	378
14.6.3	Generalization	379
14.7	Conclusion and Future Work	379
	References	380

15	Image Pre-processing Techniques for Enhancing the Performance of Real-Time Face Recognition System Using PCA	383
	Behzad Nazarbakhsh and Azizah Abd Manaf	
15.1	Introduction	384
15.2	Literature Survey	387
15.2.1	Image Acquisition	387
15.2.2	Segmentation	387
15.2.3	Localization	390
15.2.4	Normalization	390
15.2.5	Feature Selection and Extraction	391
15.2.6	Classification	392
15.3	Methodology	394
15.3.1	Image Preprocessing Using for Detection	395
15.3.2	Color Conversion and Segmentation	396
15.3.3	Localization	396
15.3.4	Normalization	396
15.3.5	Face Recognition	396
15.3.6	Feature Extraction	397
15.3.7	Classification	397
15.4	Proposed Method	397
15.4.1	Color Conversion	397
15.4.2	Segmentation	399
15.4.3	Eyes and Mouth Identification and Localization	402
15.4.4	Average Half Face	407
15.4.5	Feature Extraction and Classification	412
15.5	Experimental Result	416
15.5.1	Understanding the Ratio of Training to Test Images Numbers Needed	416
15.5.2	Changing the Training and Test Image Combination	417
15.5.3	Calculating False Positive Rate and Sensibility	418
15.5.4	Performance Comparison of Proposed Method with the Similar Recognition Framework	418
15.6	Conclusion	419
	References	421
16	Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues	423
	Reham Amin, Tarek Gaber, Ghada ElTaweel and Aboul Ella Hassanien	
16.1	Introduction	423
16.2	Traditional Authentication Methods	425
16.2.1	Knowledge-Based Authentication	425
16.2.2	Object-Based Authentication	427

16.3	Biometric Authentication Techniques	428
16.3.1	Biometric Authentication and Its Types.	429
16.3.2	Components of a Typical Biometric System	429
16.3.3	How Biometric Authentication Works?	429
16.3.4	Performance Evaluation of Biometric Authentication	431
16.3.5	Physiological Biometrics	432
16.3.6	Behavioral Biometrics	435
16.4	Biometric Versus Traditional Authentication	440
16.5	Comparison Among Authentication Techniques	440
16.6	Explicit and Implicit Authentication	441
16.7	Open Issues	443
16.8	Conclusion.	443
	References	444

Part IV Cloud Security and Data Services

17	Cloud Services Discovery and Selection: Survey and New Semantic-Based System	449
	Yasmine M. Afify, Ibrahim F. Moawad, Nagwa L. Badr and M. F. Tolba	
17.1	Introduction	450
17.2	Related Work.	451
17.2.1	Cloud Service Discovery	451
17.2.2	Cloud Service Selection	453
17.2.3	Cloud Service Discovery and Selection.	455
17.2.4	Summary of Key Findings.	455
17.3	The Proposed System	456
17.3.1	System Architecture	456
17.3.2	Unified Ontology	456
17.3.3	Service Registration Sub-system.	459
17.3.4	Service Discovery Sub-system	460
17.3.5	Service Non-functional Selection Sub-system.	461
17.4	Hybrid Service Matchmaking Algorithm	464
17.5	Experimentation and Evaluation.	468
17.5.1	Experimental Setup.	468
17.5.2	Evaluation Metrics	469
17.5.3	Experimental Scenarios	469
17.5.4	Experimental Evaluation	470
17.5.5	Experiment 2	471
17.5.6	Experiment 3	472
17.6	Conclusion and Future Work	473
	References	474

18 Data and Application Security in Cloud	479
Rajesh P. Barnwal, Nirnay Ghosh and Soumya K. Ghosh	
18.1 Introduction	480
18.2 Cloud Computing	480
18.2.1 Security in Cloud Computing.	483
18.3 Data and Application Security	484
18.3.1 Secure Data Transmission	485
18.3.2 Secure Data Storage and Integrity Verification.	486
18.3.3 Prevention Against Attacks	488
18.3.4 Isolation of Customer-Specific Data and Application	490
18.4 Research Directions	492
18.5 Conclusion.	493
References	493
19 Security Issues on Cloud Data Services	497
Nour Zawawi, Mohamed Hamdy El-Eliemy, Rania El-Gohary and Mohamed F. Tolba	
19.1 Introduction	498
19.2 Security Issues	500
19.2.1 Traditional Security Challenges	501
19.3 Data Integrity.	503
19.4 Data Availability	506
19.5 Data Confidentiality	508
19.6 Security and Trust Cloud Data Service	510
19.6.1 EWRDN Service Model	510
19.6.2 EWRDN Utilization of Resources	513
19.7 Conclusion.	514
References	515
20 A Reputation Trust Management System for Ad-Hoc Mobile Clouds	519
Ahmed Hammam and Samah Senbel	
20.1 Introduction	520
20.2 Related Work.	521
20.3 PlanetCloud in Brief.	522
20.3.1 Client Agent	523
20.3.2 Cloud Agent	523
20.3.3 Resource Server.	523
20.4 Proposed Trust management System for Ad-Hoc Mobile Cloud TMC	523
20.4.1 TMC System Design.	523
20.4.2 Simulator.	526
20.4.3 Comparison Between TMC and Existing Trust Management Systems for MANET.	530

20.5	System Performance Test	530
20.5.1	Performance Test: One	531
20.5.2	Performance Test: Two	532
20.5.3	Performance Test: Three	534
20.6	Conclusion.	538
	References	538
21	Secured and Networked Emergency Notification Without GPS Enabled Devices	541
	Qurban A. Memon	
21.1	Introduction	541
21.2	Location Based Service Applications	544
21.3	System Concepts and Related Work	545
21.4	Location Methods and Technologies	548
21.5	Positioning Equations	550
21.6	Operational Considerations and Privacy	554
21.7	A Case Study Experiment	555
21.8	Standardization Efforts	560
21.9	Conclusions	561
	References	562
22	Towards Cloud Customers Self-Monitoring and Availability-Monitoring	565
	Sameh Hussein and Nashwa Abdelbaki	
22.1	Introduction	565
22.2	Monitoring and Controlling Cloud Computing	567
22.2.1	Monitoring and Controlling Cloud Layers	567
22.2.2	Cloud Customer/Provider Conflict of Interests	569
22.3	Cloud Layers Under Cloud Customer Control	569
22.4	Cloud Service Availability.	572
22.4.1	Cloud Availability Notable Comments	573
22.4.2	Surveying the Existing Cloud Availability Monitoring Tools	573
22.5	Our Developed Availability Monitoring Tool.	574
22.5.1	Flowchart of Our Tool Operation	576
22.5.2	Tool Examination in Test Environment	576
22.5.3	Tool Accumulative Function	582
22.6	Conclusions and Future Work	583
	References	584

Bio-inspiring Cyber Security and Cloud Services: Trends
and Innovations

Hassanien, A.E.; Kim, T.-H.; Kacprzyk, J.; Awad, A.I. (Eds.)
2014, XXII, 585 p. 235 illus., 17 illus. in color., Hardcover
ISBN: 978-3-662-43615-8