SNOWBALLING REPORT (UPDATED WITH THE WORKS FROM 2015)

State of the Art of Cyber-Physical Systems Security: an Automatic Control perspective

VERSION 1.0

YURIY ZACCHIA LUN [◦]

ALESSANDRO D'INNOCENZO [◇]

FRANCESCO SMARRA [◇]

IVANO MALAVOLTA [⋆]

MARIA DOMENICA DI BENEDETTO [◇]

[◦] **IMT School for Advanced Studies Lucca**
Piazza San Francesco, 19 - 55100 Lucca - Italy

[◇] **University of L'Aquila**
Via Giovanni Di Vincenzo 16/B - 67100 L'Aquila - Italy

[⋆] **Vrije Universiteit Amsterdam**
De Boelelaan 1105 - 1081 HV Amsterdam - Netherlands

State of the Art of Cyber-Physical Systems Security: an Automatic Control perspective

VERSION 1.0

ABSTRACT

In order to identify additional sources published in other journals or venues which may not have been considered during the automatic and manual searches, we applied (backward and forward) snowballing techniques on the primary studies selected by the automatic and manual searches. This report provides details of this activities.

KEYWORDS

Systematic mapping study, snowballing, cyber-physical systems, CPS, networked control systems, NCS, security, attacks, protection.

Contents

List of Tables

1 Snowballing

In order to identify additional sources published in other journals or venues which may not have been considered during the automatic and manual searches, we applied (backward and forward) snowballing on the primary studies selected by the automatic and manual searches. More specifically, we considered all the studies selected by the automatic and manual searches and we searched through Google Scholar all the papers referring them (i.e., forward snowballing [Woh14]); then, we scrutinized also the references of each selected study to identify important studies that might have been missed during the initial search (i.e., backward snowballing [Woh14]). This process was repeated interactively until we examined all the relevant works.

2 Selection procedure

In the same way as for the automatic and manual searches, after the snowballing activity we considered all the collected studies and filtered them according to a set of well-defined inclusion and exclusion criteria. This criteria are the following.

2.1 Inclusion criteria

(I1) Studies focussing on security of cyber-physical systems (CPS).

(I2) Studies proposing a method or technique for CPS security enforcing or breaching.

(I3) Studies providing some kind of validation of the proposed method or technique (e.g., via formal analysis, controlled experiment, exploitation in industry, example usage).

2.2 Exclusion criteria

(E1) Studies not subject to peer review [WRH+12] (e.g., journal papers, papers published as part of conference proceedings will be considered, whereas white papers will be discarded).

(E2) Studies written in any language other than English.

(E3) Studies focussing on security method or technique not specific to cyber-physical system (e.g studies focussing on either the physical or cyber part only of the system under consideration).

(E4) Studies published before 2006 (because the cyber-physical systems discipline has emerged in 2006).

(E5) Secondary or tertiarty studies (e.g., systematic literature reviews, surveys, etc.).

(E6) Studies in the form of tutorial papers, short papers, poster papers, editorials, because they do not provide enough information.

In this context, a study was selected as a primary study if it satisfied *all* inclusion criteria, and it was discarded if it met *any* exclusion criterion. In order to reduce the likelihood of bias, the selection criteria of this study have been decided during the review protocol definition.

With a view to handle studies selection in a cost effective way we used the adaptive reading depth [PFMM08], as the full-text reading of clearly excluded approaches is unnecessary. So, we considered *title*, *keywords* and *abstract* of each potentially relevant study and, if selection decision could not be made, other information (like *conclusion* or even *full-text*) have been exploited [ZBT11]. By following the approach proposed in [AP14], two researchers classified each potentially relevant study either as *relevant*, *uncertain*, or *irrelevant*; any study classified as *irrelevant* has been directly excluded, whereas all the other approaches have been discussed with the help of a third researcher.

2.3 Selection of the papers by backward snowballing

Using the *references* of each selected paper is referred to as backward snowballing [Woh14]. To all the relevant studies identified in this phase we have applied inclusion and exclusion criteria[1]. The results are reported in Tables 1 - 9.

2.4 Selection of the papers by forward snowballing

Using the *citations* of each selected paper is referred to as forward snowballing [Woh14]. We have performed the procedure in 2015, April 15 - 20. To all the relevant studies identified in this phase we have applied inclusion and exclusion criteria. The results are reported in Tables 10 - 20.

[1] with exception of the exclusion criteria [E4], considered too restrictive in this case

Table 1: Studies **6001 - 6029** retrieved by application of backward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
6001	[TAS+10]	✓	✓	✓							Can be considered together with 6002: [TDSJ11]
6002	[TDSJ11]	✓	✗								Follow up of 6001 with realistic experimentation
6003	[MS10]	✓	✓	✓							
6004	[XMS10]	✓	✓	✓							
6005	[LNR11]	✓	✓	✓							
6006	[STJ10]	✓	✓	✓							
6007	[BRW+10]	✓	✓	✓							Follow up of 6126, defender's point of view
6008	[PCB11]	✓	✓	✓							Surely related, but is the focus on security?
6009	[KP11]	✓	✓	✓							
6010	[KHLF10]	✓	✗								
6011	[CHK+12]	✓	✗								Sums up 6009 [KP11] & 6046 [TKPC11]
6012	[MPM10]	✗									
6013	[EVM+10a]	✓	✓	✓							Extended by 4146: [VEM+15]
6014	[FTD12]	✓	✓	✓							Extended by 0506: [FTD14]
6015	[Smi11]	✓	✓	✓							Extended by 0653: [Smi15]
6016	[SH11]	✗									
6017	[TLP09]	✗									
6018	[ALSB10]	✓	✓	✓							
6019	[BGA11a]	✓	✓	✓							
6020	[BB10]	✓	✓	✓							
6021	[GLB10]	✓	✓	✓							
6022	[MGCS10]	✓	✓	✓							
6023	[WGL+14]	✓	✓	✓							
6024	[KJTT11]	✓	✓	✓							Journal extension of 6025, 6044, 6045
6025	[KJTT10b]	✓	✓	✓							Extended by 6024: [KJTT11]
6026	[YMG06]	✗									
6027	[KFL+10]	✓	✗								
6028	[ESHS13]	✓	✓	✓							Is electricity market a CPS?
6029	[VWB13]	✓	✓	✓							

Table 2: Studies **6030 - 6054** retrieved by application of backward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
6030	[LGW+13]	✓	✓	✓							
6031	[CAS08]	✓	✗								
6032	[GSJS09]	✓	✗								
6033	[MS09]	✓	✓	✓							
6034	[TSDJ12]	✓	✗								Related to security indices in 6006: [STJ10]
6035	[TSSJ12]	✓	✓	✓							
6036	[DSA96]	✗									
6037	[DS10]	✓	✓	✓							Related to security indices in 6006: [STJ10]
6038	[ML11]	✓	✓	✓							Defines I-net-based load altering attacks
6039	[GBG+11]	✓	✓	✓							Extended to journal paper 6059: [GBG+13]
6040	[EP10]	✗									Fault diagnosis, no security
6041	[PBB11]	✓	✓	✓							Necessary and sufficient condition for the existence of vulnerabilities inherent to the power network interconnection structure
6042	[CAS+09]	✓	✗								
6043	[YYY+11]	✓	✓	✓							
6044	[KJTT10c]	✓	✓	✓							Extended by 6024 [KJTT11]
6045	[KJTT10a]	✓	✓	✓							Extended by 6024 [KJTT11]
6046	[TKPC11]	✓	✓	✓							Forward snowballing?
6047	[BM08]	✓	✗								
6048	[FN07]	✓	✗								
6049	[ZMRB11]	✓	✗								
6050	[EDEO06]	✓	✗								
6051	[SPH+10]	✓	✓	✓							
6052	[FTD11]	✓	✓	✓							Design of secure state estimation for me is a method for security enforcing. Isn't it?
6053	[HKMS12]	✓	✗								
6054	[BZ11]	✓	✓	✓							# and placement of security measurements

Table 3: Studies **6055 - 6078** retrieved by application of backward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
6055	[KT13a]	✓	✓	✓							Secure phasor measurement units (PMUs) placement: necessary and sufficient condition for detectability of state and topology attacks
6056	[ENZH11]	✓	✓	✓							I have some doubts about novelty/contribution...
6057	[RM12]	✓	✓	✓							FDIAs with incomplete knowledge: mathematical model, vulnerability measure
6058	[BZ14a]	✓	✓	✓							Optimal protection against FDIAs problem as a variant of a Steiner tree problem in a graph
6059	[GBG+13]	✓	✓	✓							Extension of 6039: [GBG+11]
6060	[KTT14a]	✓	✓	✓							
6061	[ILW06]	✓	✗								
6062	[ALSB13]	✓	✗								
6063	[SSJ14]	✓	✓	✓							
6064	[PLD11]	✗									Recursive networked predictive control (RNPC) method based on round-trip time delay
6065	[AW08]	✓	✗								
6066	[LRJ11]	✓	✗								
6067	[ME10a]	✓	✓	✗			✓				
6068	[BBB+92]	✓	✗								
6069	[SMR09]	✓	✗								
6070	[KFM+11]	✓	✗								
6071	[LTM09]	✓	✗							✓	
6072	[FM10]	✓	✗								
6073	[AM12]	✓	✗								
6074	[MPP13]	✓	✓	✓							
6075	[MKFM12]	✓	✗								
6076	[GSFW12]	✓	✗								
6077	[LP12]	✗									Privacy is out of scope...
6078	[LP14]	✗									Privacy is out of scope...

Table 4: Studies **6079 - 6103** retrieved by application of backward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
6079	[MMS13]	✗									Confidentiality enforcing at design time
6080	[PCBB10]	✗									Detection of corrupted components in large scale systems: consensus' problem
6081	[LKAH12]	✓	✓	✓							Not available, followed by 0519: [KLH13]
6082	[VSDS11]	✓	✗								Security metrics
6083	[JTT12b]	✓	✗								Beginning study of attacks on nonlinear power systems: Forward snowballing is a must here
6084	[BHK+10]	✓	✗								
6085	[BGN+09]	✓	✗								
6086	[Eri07]	✓	✗								
6087	[MFL+13]	✓	✗								Mathematical definitions of concepts within resilient control
6088	[RGM09]	✓	✗								
6089	[YLS+11]	✓	✗								
6090	[DWDG13]	✗									
6091	[FFK+11a]	✗									
6092	[ZWS+11]	✓	✓	✓			✓				
6093	[MYLR13]	✓	✗								
6094	[QLC13]	✓	✓	✓							Extension of 0618 [QLC12] with two algorithms for attack and defence
6095	[YLR11]	✓	✗								
6096	[WLJ+11]	✓	✗	✗							
6097	[HEN+13]	✓	✗								Follow up of 6133 [HLCH11] and 6056 [ENZH11]
6098	[SLL12]	✗									
6099	[XXD13]	✗									
6100	[XMS11]	✓	✓	✓							
6101	[MFJ+10]	✓	✗								
6102	[ZCW+14]	✓	✓	✓							
6103	[FM12a]	✓	✓	✓							

Table 5: Studies **6104 - 6132** retrieved by application of backward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
6104	[AFL11]	✓	✓	✗			✓				
6105	[THL11]	✗									
6106	[QWT+11]	✓	✗								
6107	[SSJ13]	✓	✓	✓							
6108	[ST13]	✓	✓	✓	✓						Published in **2016** as [ST16], **highly cited**
6109	[HJJ+14]	✓	✓	✓							
6110	[Ami11]	✓	✗								
6111	[CDF+07]	✓	✗				✓				
6112	[LLE13b]	✓	✓	✓							
6113	[HG12]	✓	✓	✓							
6114	[WR09]	✓	✗								
6115	[EVM+10b]	✓	✓	✓							Follows 6013: [EVM+10a]
6116	[ABF+08]	✓	✗								
6117	[ACS+06]	✓	✗								
6118	[Cle08]	✗									
6119	[dAKO02]	✗									
6120	[DSEB12]	✓	✗								
6121	[DTO+06]	✓	✗								
6122	[FWLS09]	✓	✗								
6123	[FKW08]	✓	✗								
6124	[GKR+08]	✓	✗								
6125	[KKW07]	✓	✗								
6126	[LNR09]	✓	✓	✓							Conference paper extended by 6005: [LNR11]
6127	[MB09]	✓	✗								
6128	[MBFB06]	✓	✗								
6129	[SSJ12b]	✓	✓	✓							
6130	[Tak07]	✓	✗								
6131	[TLM07]	✓	✗				✓				See also 0633 [TLM08]
6132	[SCL+07]	✓	✗				✓				

Table 6: Studies **6133 - 6161** retrieved by application of backward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
6133	[HLCH11]	✓	✓	✓							
6134	[NPYG09]	✓	✗								
6135	[CSK+10]	✓	✗								
6136	[BL04]	✓	✗								
6137	[BFP+13]	✗									
6138	[VD13b]	✓	✓	✓							
6139	[RNLV08]	✗									
6140	[Bau10]	✓	✗		✓				✓		
6141	[JTT12a]	✓	✓	✓							
6142	[CX12]	✓	✓	✓							
6143	[SSJ11]	✓	✓	✓							
6144	[MHR+12]	✓	✓	✓							
6145	[EHS12]	✓	✓	✓							
6146	[SZS+08]	✓	✗								
6147	[NG10]	✗									
6148	[SMTS13]	✗									
6149	[SM10]	✓	✗								
6150	[SKTP11]	✗									
6151	[STF05]	✓	✗								
6152	[PMDL10]	✗									
6153	[YLR12]	✓	✓	✓							
6154	[ME10b]	✓	✗								
6155	[LLQ10]	✓	✗								
6156	[CDHX11]	✓	✗				✓				Reliable strategies for 2 types of defensive tasks
6157	[KT13b]	✓	✓	✓							Conference paper extended by 0418: [KT13c]
6158	[CB05]	✓	✗				✓				
6159	[LWH05]	✓	✗								
6160	[SM11]	✓	✗								
6161	[DCEF11]	✗									

Table 7: Studies **6162 - 6188** retrieved by application of backward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
6162	[HJW07]	✗									
6163	[SWB04]	✗					✓				Identification of critical system components vulnerable to physical attacks
6164	[YEPA07]	✗					✓				Resource allocation in electric power network defence against physical attacks
6165	[DAA10]	✗					✓				Vulnerability analysis of the electric grid under terrorist threat
6166	[Arr10]	✗					✓				The same line as 6165: [DAA10]
6167	[AG05]	✗					✓				Problem of deliberate outages. See also 6166: [Arr10] and 6165: [DAA10]
6168	[MAG05]	✗					✓				The same line as 6165 - 6167
6169	[SWB09]	✗					✓				A solution to electric power grid interdiction problem
6170	[PTM+05]	✗			✓		✓				
6171	[CBD+09]	✗									
6172	[JSDA12]	✓	✗				✓				
6173	[BDS+14]	✓	✗								
6174	[KWG+12]	✓	✗				✓				
6175	[GLS+12]	✓	✗								
6176	[MC14b]	✓	✗						✓		
6177	[TLHC14]	✗									
6178	[LLE13a]	✓	✗				✓				
6179	[CP12]	✗	✗								It's a book on FDI of 4000 citations, that was first published in 1999
6180	[Fra90]							✓	✓		
6181	[FD97]							✓	✓		
6182	[HKKS10]								✓		
6183	[Ise84]							✓	✓		
6184	[IPL14b]	✓									Already analyzed tech rep [IPL14a]
6185	[KCR+10]	✓					✓				
6186	[Wil76]							✓	✓		
6187	[KOJ11]	✓							✓		
6188	[HKD11]	✓	✗				✓				

Table 8: Studies **6189 - 6217** retrieved by application of backward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
6189	[LN08]	✓	✗				✓				
6190	[Oni12]	✓	✗				✓				
6191	[YMS+14]	✓	✓	✓			✓				
6192	[RES+10]	✗							✓		
6193	[ZKSY14]	✓	✓	✓			✓				
6194	[ZHH12]	✓	✓	✓			✓				
6195	[FK15]	✓	✓	✓							It introduces a new type of attack
6196	[ZCSC16]	✓	✓	✓							It was published only in 2016...
6197	[LOCL10]	✗	✗				✓				
6198	[PBB12]	✓	✓	✓			✗				See the end of Section V.P at pg. 20 of our ArXiv article for additional details
6199	[GMRR10]	✓	✓	✓			✓				
6200	[XZ08]	✗									
6201	[CFM+14]	✓	✗								
6202	[PR+14]	✗									
6203	[LSHP12]	✓								✓	
6204	[BS12]	✗									
6205	[TML10]	✓							✓		
6206	[PLR07]	✗									
6207	[VPHC+06]	✗									
6208	[GS14]	✓					✓				
6209	[FS14]	✗									
6210	[FPV+08]	✓	✓	✓			✓				
6211	[FBB09]	✓	✓	✓			✓				
6212	[FDB14]	✓	✓	✓			✓				
6213	[BFDS08]	✓	✓	✓			✓				
6214	[MC14c]	✓	✓	✓			✓				
6215	[Lou15]	✓	✗						✓		This book provides a good survey of the state of the art on the general cyber-physical attacks (including IoT and embedded systems)
6216	[SS14]	✓	✗								It's a comparative study of Machine Learning algorithms for IDS
6217	[KLK14]	✓	✓	✓			✓				

Table 9: Studies **6218 - 6245** retrieved by application of backward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
6218	[ZJB10]	✓	✓	✓							
6219	[MK09]	✓	✓	✓							
6220	[FGMS11]	✓	✗								
6221	[HWT+15]	✓	✗				✓				
6222	[MYK+13]	✓	✓	✓			✓				
6223	[BPG15b]	✓	✓	✓							It is the same is ref. 7282, [BPG15a]
6224	[CKBR06]	✗							✓		
6225	[LLQ11]	✓	✗								
6226	[LCH+14]	✓	✓	✓			✓				It is a conference version of [LCH+15], that is a work on consensus
6227	[LFC15]	✓	✓	✓			✓				It is a work on consensus
6228	[GDJ12]	✓	✓	✓			✗				Basically, it is a work on consensus
6229	[AE12]	✓	✓	✗							
6230	[HTP+13]	✗									
6231	[KBC+13]	✗									
6232	[AEV+12]	✓								✓	
6233	[VSDS12]	✓	✓	✓			✓				
6234	[ZJCH14]	✓	✓	✓			✓				It is essentially a consensus problem
6235	[WLN07]	✗									
6236	[KTD14]	✓	✓	✓							
6237	[SJ10]	✗									
6238	[BBH+14]	✗									It studies the geographically correlated failures in power grids
6239	[HKJ08]	✓	✓	✓			✓				
6240	[FVP+07a]	✗									FDI for multi-agent systems
6241	[PBB07]	✓	✓	✓			✓				Consensus
6242	[FEG08]	✓	✓	✓			✓				Consensus
6243	[NAB08]	✓	✗				✓				
6244	[FVP+07b]	✓	✓	✓			✗				In a multi-agent setting it studies a problem based on eventbased cooperation rules
6245	[WLJ+10]	✓	✓	✓			✓				

Table 10: Studies **7001 - 7027** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7001	[FHKB14]	✓	✓	✓							Practical limitations of sliding-mode switching attacks in single-machine infinite-bus systems *
7002	[FHAK14]	✓	✓	✓							Parametric game-theoretic controller to stabilize power systems during & after a switching attack
7003	[KCS14]	✓	✓	✓							
7004	[LZZ+15]	✓	✗								
7005	[CKM15]	✓	✓	✓	✓						Published in **2017** as [CKM17], and already it has **several citations**
7006	[LSM13]	✓	✓	✓							
7007	[CJM15]	✓	✓	✓							
7008	[AMT15]	✓	✓	✓							
7009	[GT13]	✓	✗						✓		Useless, but satisfying selection criteria
7010	[Yu13]	✓	✗							✓	
7011	[CSCZ15]	✓	✓	✓							
7012	[ZCSC15]	✓	✓	✓	✓						Technical report at the basis of 7011: [CSCZ15]
7013	[YS14]	✗									
7014	[YS15]	✗									
7015	[YSL15]	✓	✓	✓							
7016	[SPN+15]	✓	✓	✓							
7017	[IPL14a]	✗			✓						
7018	[WSBL14]	✗									
7019	[MZPP14]	✓	✓	✓							
7020	[ST14]	✓	✓	✓							
7021	[MM15]	✓	✓	✓							Generalises the results of 7022: [MS15]
7022	[MS15]	✓	✓	✓							Journal version of 7023: [MS13]
7023	[MS13]	✓	✓	✓							Extended by 7022 [MS15] and 7021 [MM15]
7024	[WMS14]	✓	✓	✓							
7025	[BCQ13]	✓	✓	✓							
7026	[HWMD15]	✓	✓	✓	✓						Not published yet
7027	[BYH+15]	✓	✗								

Table 11: Studies **7028 - 7055** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7028	[BGA15]	✓	✓	✓							Journal version of 3276: [BGA11b]
7029	[HAH13]	✓	✗								
7030	[DT15]	✓	✓	✓							
7031	[AMA14]	✓	✗								LTC transformer operation analysis under FDIA
7032	[HTC+14]	✓	✓	✓							Journal version of 6133: [HLCH11]
7033	[TSST14]	✓	✓	✓							
7034	[DBV14a]	✓	✓	✓							
7035	[XGS+15]	✓	✗								
7036	[LBLL15]	✓	✓	✓							
7037	[RAK14b]	✓	✓	✓							
7038	[CI15a]	✓	✓	✓							
7039	[RAK14a]	✓	✗								Impact analysis, linked to 7037: [RAK14b]
7040	[CMBK13]	✓	✗								
7041	[DFN15]	✓	✗								
7042	[GSS+14]	✓	✗								
7043	[BG14]	✓	✓	✓							
7044	[FEK14]	✓	✓	✓	✓		✓				Monitoring of mission profile at mission execution and software code operation levels
7045	[SJ15]	✓	✓	✓							
7046	[ZM]	✓	✓	✓	✓						Follows the 0555: [ZM11]; not published yet
7047	[DMBH12]	✓	✓	✓							
7048	[HB14]	✗									Power grid system monitoring: change detection
7049	[AM14]	✓	✗						✓		
7050	[MZ14]	✗									
7051	[CWH15]	✓	✓	✓			✓				
7052	[WBP+14]	✓	✓	✓							
7053	[WBP+13]	✓	✓	✓			✓				No cyber part. It is related to 7052: [WBP+14]
7054	[BDSL15]	✓	✓	✓							
7055	[BWP+14]	✓	✓	✓							

Table 12: Studies **7056 - 7082** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7056	[CIH15]	✓	✓	✓							New entry related to 2015. ArXiv version was considered
7057	[RVLD13]	✓	✓	✗							
7058	[CWVW14]	✓	✗								
7059	[JKB14]	✓	✓	✓							
7060	[RVD14]	✓	✓	✓							Similar to 7056: [RVLD13]
7061	[GM13]	✓	✗								Forward snowballing –¿ subsequent journal?
7062	[LVRD14]	✓	✓	✓							
7063	[CHPB15]	✓	✗								
7064	[KLH14]	✓	✓	✓							
7065	[HH11]	✓	✗								
7066	[BS11]	✓	✓	✓							
7067	[XR12]	✓	✓	✓							
7068	[Bis11]	✓	✗								
7069	[DR13]	✗									
7070	[ZXLW13]	✓	✗				✓				
7071	[FNU13]	✓	✓	✓			✓				Fault detection and isolation approach
7072	[GLMR14]	✓	✗								
7073	[NNC15]	✓	✓	✓							
7074	[AMP15]	✓	✓	✓							
7075	[ZYT+15]	✗									
7076	[PB14]	✗									
7077	[HZR12]	✓	✗								
7078	[DS12]	✓	✗						✓		
7079	[SB14]	✓	✗								
7080	[VF13]	✓	✓	✗							
7081	[LVD14]	✓	✗				✓				
7082	[SBPV14]	✓	✓	✓							

Table 13: Studies **7083 - 7112** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7083	[CUC+11]	✓	✗								
7084	[TBYK13]	✓	✓	✓							
7085	[NPA+12]	✓	✗								
7086	[GS13]	✓	✗								
7087	[BMC13]	✓	✓	✗			✓				
7088	[KMP+14]	✓	✓	✓			✓				
7089	[PKM+14]	✓	✗				✓				
7090	[MCH12]	✓	✗								
7091	[CPW13]	✓	✗								
7092	[CA14a]	✓	✗								
7093	[LSS+13]	✓	✗								
7094	[WXZ+14]	✓	✓	✓			✓				
7095	[CA14b]	✓	✗				✓				
7096	[GGI+15]	✓	✗								
7097	[PSC+14]	✓	✗								
7099	[YGG+15]	✓	✓	✓							Not 100% sure...
7100	[KPH+15]	✓	✗				✓		✓		
7101	[SHC+14]	✓	✗				✓		✓		
7102	[FM12b]	✓	✓	✓	✓						See also 6103: [FM12a]
7103	[FM13]	✓	✓	✓							See also 7102: [FM12b] and 6103: [FM12a]
7104	[ZGDL13]	✓	✓	✓			✓				
7105	[CM12]	✓	✗								
7106	[SYA14]	✓	✓	✓							
7107	[DT14b]	✓	✓	✓							Conference version of 7030: [DT15]
7108	[KH13]	✓	✓	✓							
7109	[DT14a]	✓	✓	✓							See also 7030: [DT15] and 7107: [DT14b]
7110	[VFLG14]	✓	✗								
7111	[DWD14]	✓	✓	✓							
7112	[YGA15]	✓	✗								

Table 14: Studies **7113 - 7138** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7113	[HK13]	✓	✗								
7114	[RB15b]	✓	✓	✓							
7115	[BA13]	✓	✗								
7116	[AR14b]	✓	✗								
7117	[LL14]	✓	✓	✓							
7118	[RP14]	✓	✗								
7119	[MC14a]	✗									Iterative Observer Scheme identifying arbitrarily attacked or faulty sensors in smart grids: FDI
7120	[LED+14]	✓	✓	✓							
7121	[Ran14]	✗									
7122	[GSXY15a]	✓	✗						✓		Important! To download!
7123	[ENZH13]	✓	✓	✓							
7124	[LEH13]	✓	✓	✓							
7125	[BZ14b]	✓	✓	✓							
7126	[NBSS13]	✓	✗								
7127	[KSWC14]	✓	✗								
7128	[RAB14]	✓	✓	✓							
7129	[LW14]	✓	✓	✓							
7130	[VD14]	✓	✓	✓							Journal version of 7131: [VD13a]
7131	[VD13a]	✓	✓	✓							Conference paper, ground for 7130: [VD14]
7132	[Kos13]	✓	✓	✓						✓	
7133	[Kos14]	✓	✓	✓							
7134	[YOTI14]	✓	✓	✓							
7135	[Yu12]	✓	✗							✓	
7136	[WL13]	✓	✗				✓		✓		Cyber security in the Smart Grid communications: pure cyber solutions
7137	[CX13]	✓	✓	✓							
7138	[ESHS12]	✓	✓	✓							Conference paper as a base for 6028: [ESHS13]

Table 15: Studies **7139 - 7164** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7139	[WPS+14]	✓	✗								
7140	[RAR13]	✓	✗								Interesting as an implementation result...
7141	[KPP14]	✗									
7142	[LN14]	✓	✓	✓			✓				
7143	[BW14]	✓	✗								
7144	[LN15b]	✓	✓	✗	✓						arXiv
7145	[YC15]	✓	✓	✓							Seems very promising...
7146	[MVW13]	✓	✓	✓			✓				
7147	[MVW15]	✗									
7148	[PMA15a]	✗									
7149	[WR14a]	✓	✓	✓							
7150	[WR14b]	✓	✓	✓							Following of 7149: [WR14a]
7151	[OEV+13]	✓	✓	✓							
7152	[LKS14]	✓	✓	✓							
7153	[ZGL+13]	✗									
7154	[SLL14]	✗									
7155	[SMT+14]	✓	✗				✓				
7156	[SG14]	✓	✓	✓			✓				
7157	[GSE15]	✓	✓	✓						✓	
7158	[GZLD12]	✗									
7159	[Taj14]	✓	✓	✗							Joint detection-estimation framework for (structured or random) bad data detection and system state recovery
7160	[EPP14]	✓	✓	✗							
7161	[LYRS14]	✓	✓	✗							
7162	[NI14]	✓	✓	✓			✓				Is there a cyber part? The validation is good enough?
7163	[AR14a]	✗									
7164	[TDS+14]	✓	✓	✗							

Table 16: Studies **7165 - 7193** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7165	[IYF+14]	✓	✓	✓			✓				
7166	[BZ13a]	✓	✓	✓							
7167	[GCQ14]	✓	✓	✓	✓						Not published yet
7168	[AZSE12]	✗									
7169	[AZSE14]	✗									The extended version of 7169: [AZSE12]
7170	[RM13a]	✓	✗								
7171	[LYW15a]	✓	✓	✓							
7172	[LAPD12]	✓	✗								
7173	[LAP12]	✓	✗								See also 7173: [LAPD12]
7174	[AYA+14]	✓	✓	✓							
7175	[FFB+13]	✓	✗								
7176	[GA13]	✓	✗								
7177	[MCHL14]	✓	✗								
7178	[GA14]	✓	✗								
7179	[ATKF13]	✓	✗								
7180	[SJ13]	✓	✓	✓							Extended to 7045: [SJ15]
7181	[GB13]	✓	✗							✓	Agenda of our future research...
7182	[GBP14]	✓	✓	✓							Related to 6059: [GBG+13], less technical
7183	[DDS13b]	✓	✓	✗							
7184	[DDS13a]	✓	✓	✓							
7185	[CMM+14]	✓	✗								
7186	[YQST12]	✗									
7187	[LXL+12]	✓	✗				✓		✓		
7188	[LLWW10]	✗									
7189	[CCC12]	✓	✗				✓				
7190	[MMA11]	✗									
7191	[SLP11]	✗									
7192	[HBEH12]	✗									
7193	[GBH+12]	✓	✓	✓							Follows 6039: [GBG+11]

Table 17: Studies **7194 - 7222** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7194	[ZGLP11]	✓	✓	✓	✓		✓				Related to 7104: [ZGDL13]
7195	[LSK+13]	✓	✓	✓			✓				
7196	[OEY+12]	✓	✓	✓							
7197	[SPK13]	✓	✗				✓				
7198	[RM13b]	✓	✓	✓			✓				
7199	[MP13]	✓	✗				✓				
7200	[BGY12]	✓	✓	✓			✓				See also 7099: [YGG+15]
7201	[WMO13]	✓	✓	✓							
7202	[WLM+13]	✓	✗								
7203	[OEYV+12]	✓	✗								
7204	[DBV14d]	✓	✓	✓							
7205	[TLQ12]	✓	✗								
7206	[PNZL13]	✗	✗								
7207	[MG13]	✓	✗								
7208	[YGLV13]	✓	✗								
7209	[AR14d]	✓	✗								
7210	[TWQ12]	✓	✓	✓							
7211	[NH12]	✓	✓	✓			✓			✓	
7212	[AHG14]	✓	✗				✓				
7213	[SNG14]	✓	✗								
7214	[KTT13]	✓	✓	✓							
7215	[MM12]	✓	✗								
7216	[SNP+14]	✓	✓	✓	✓						arXiv - related to 7016: [SPN+15]
7217	[AR14c]	✓	✗								
7218	[ZLL+13]	✓	✗								
7219	[DBV14b]	✓	✓	✓							Linked to 7034: [DBV14a]
7220	[OEY+15]	✓	✗								
7221	[NL15]	✓	✓	✓			✓				
7222	[TVDH14]	✗									

Table 18: Studies **7223 - 7251** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7223	[GM14]	✓	✗								
7224	[ZC12]	✓	✗				✓		✓		
7225	[BBFP15]	✓	✗								
7226	[GZT+12]	✓	✓	✓			✓				See also 7104: [ZGDL13]
7227	[CYM+15]	✓	✓	✗			✓				
7228	[SLZX14]	✓	✓	✗			✓				
7229	[SYZ15]	✓	✓	✓							
7230	[LK14]	✓	✓	✓							
7231	[KS15]	✓	✗								Application of bat and firefly algorithms for state estimation with fake data measurements
7232	[RA13]	✓	✗								Presents AMISecChecker
7233	[ZRZ+13]	✓	✗								
7234	[YGZ+12]	✓	✗							✓	
7235	[SAD+14]	✓	✗								
7236	[HPK+14]	✓	✓	✓							
7237	[PS14]	✓	✓	✗							
7238	[DBV14c]	✓	✓	✓	✓						arXiv
7239	[HBA+14]	✓	✓	✓			✓				
7240	[MLSH15]	✓	✓	✓							
7241	[GBR13]	✓	✗								
7242	[LCCY13]	✓	✓	✓			✓				
7243	[DGPH14]	✓	✗								
7244	[VHSM14]	✓	✓	✓			✓				
7245	[RMS14]	✗									
7246	[LH11]	✓	✓	✓							
7247	[BZD+14]	✓	✗				✓		✓		
7248	[TEL13]	✓	✗								
7249	[ZYSH13]	✓	✓	✓			✓				
7250	[LYY13]	✗									
7251	[BS13]	✗									

Table 19: Studies **7252 - 7279** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7252	[Bis12]	✗									Security?
7253	[PK12]	✗									
7254	[MBS12]	✗									
7255	[ZYT+14]	✓	✓	✓			✓				Sequential attacks: only link removal, no dynamics
7256	[FZT+14]	✓	✗								
7257	[GLMM13]	✓	✗								
7258	[GHB+12]	✓	✗				✓				
7259	[JAL13]	✗									
7260	[FFK+11b]	✓	✓	✓			✓				
7261	[LLZ+14]	✓	✓	✓			✓				
7262	[DGS15]	✓	✓	✓							
7263	[AG12]	✓	✗								
7264	[KS14]	✓	✗								
7265	[WKJ12]	✗									Fault detection & isolation pb. in power nets
7266	[CMK+11]	✓	✗								
7267	[ZS10]	✓	✗				✓		✓		
7268	[XRWD11]	✓	✗								
7269	[SSJ12a]	✓	✓	✓							
7270	[BZ13b]	✓	✓	✓							
7271	[BHWC13]	✓	✗						✓		
7272	[DSV+09]	✗									
7273	[SLV+07]	✗									
7274	[LTJ11]	✓	✗								
7275	[ZLW+10]	✓	✗								
7276	[WZLZ11]	✓	✗								
7277	[KTT14b]	✓	✓	✓							
7278	[LWW+12]	✗							✓		
7279	[CIMR13]	✓	✗	✗							

Table 20: Studies **7280 - 7306** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7280	[DNWH13]	✗							✓		
7281	[MSK+15]	✓	✓	✓							
7282	[BPG15a]	✓	✓	✓							Finalist for the Best Student-Paper Award at IEEE ACC 2015
7283	[JKTT14]	✓	✓	✓							Journal extension of 6141: [JTT12a]
7284	[MHS14]	✗									
7285	[DSDB15]	✓	✓	✓							Best Application Paper Award winner.
7286	[XWR14]	✓	✓	✓							Journal version of [XR12]
7287	**[HPK+15b]**	✓	✓	✓							
7288	[FIRT15]	✗									
7289	[SMY+15]	✓	✓	✓							It considers the PHY model of the sensor, and exploits the PHY dynamics (challenge to actuator)
7290	[SLCL15]	✗									
7291	[WS15]	✓	✓	✓							Mathematical proof is a validation method here
7292	[TPSJ15]	✓	✓	✓							
7293	[SC15]	✓	✗	✗					✓		A useful survey
7294	[TKYK15]	✓	✓	✓							It is related to [TBYK13]
7295	[LSE15]	✓	✓	✓							
7296	[LDZ+15]	✗									
7297	[PMA15b]	✓	✗				✓				
7298	[YHY+15]	✓					✓				
7299	[GH15]	✓	✗	✗					✓		A survey to consider
7300	[SNP+15]	✓	✗	✗							To be considered together with [SPN+15]
7301	[UKWI15]		✗								
7302	[KYH15]	✓	✗								See also [LKAH12], [KH13] and [KLH14]
7303	[DBV15c]	✓	✓	✓							
7304	[DBV15d]	✓	✓	✓							See also the related [DBV15c]
7305	[NM15a]	✓	✓	✓							Necessary and sufficient condition for the existence of a resilient estimator
7306	[PSC15]	✓	✓	✓							BDD via on line equivalent impedance for detecting malicious manipulation in PMUs

Table 21: Studies **7307 - 7329** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7307	[ZYLY15]	✓	✓	✓			✓				The impacts of these false data injection attacks on the effectiveness of the dynamic microgrid partition process based on Connected Graph Constrained Knapsack Problem
7308	[DZC15]	✓	✗	✓							The economic impact of the data integrity attack to distributed DC-OPF algorithms
7309	[KCG15]	✗									The studies focused on the reaching consensus in the presence of malicious agents is out of scope, see the survey for additional details.
7310	[CHT15]	✓			✓						
7311	[LALH15]	✓					✓				
7312	[WHY15a]	✓	✗	✓							
7313	[GXSL+15]	✗									Encodes the analysis problems as logical decision problems, to be solved via SMT solvers
7314	[IL15]	✗					✓				
7315	[WHY15b]	✓	✓	✓							
7316	[CI15b]	✓	✗								
7317	[LLL15]	✓	✗								It assesses the risk of transmission lines being overloaded due to false data injection attacks
7318	[ENZ+18]	✓	✓	✓							See also [ESHS13], [EHS12], [ESHS12]. It was available from 2015, but was published in 2018
7319	[AKWM15]	✗					✓				
7320	[MLF+15]	✓	✗								It introduces a 13.8-kV microgrid security test bed. It is built on a real power facility
7321	[SNB+15]	✓	✓	✓	✓						
7322	[AHT+15]	✓	✓	✓							
7323	[NC15]	✓	✓	✓							
7324	[YYL+15]	✓	✓	✓							
7325	[SLSY15]	✓	✓	✓							
7326	[HWT+15]	✓	✗				✓				
7327	[ZZC15]	✓	✓	✓			✓				
7328	[LSSH15]	✓	✗	✗					✓		
7329	[Adh15]				✓						PhD Thesis

Table 22: Studies **7330 - 7355** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7330	[SS15a]	✓	✓	✓							Multiple data injection attackers are considered
7331	[FFFS15]	✓	✗								It studies impacts of error in measurements on system security indices
7332	[LQDS15]	✓	✓	✓							
7333	[Bha15]				✓						
7334	[KMT15]	✓	✓	✓			✓				
7335	[GGB15]	✓	✓	✓							
7336	[EPPK15]				✓						
7337	[DBV15b]	✓	✓	✓							
7338	[LYW15b]	✓	✓	✓							See also [LYW15a]
7339	[AMS15]	✓	✗				✓				
7340	[HMX15]	✓	✓	✓	✗						
7341	[GAY15]	✓		✗							
7342	[XW15]	✓	✓	✓							
7343	[D+15]				✓						
7344	[Lia15]				✓						
7345	[Sar15]				✓						
7346	[Rav15]				✓						
7347	[HWC15]	✓	✗								It analyzes the likelihood of cyber data attacks to power systems
7348	[FHFFS15]	✓	✗								It studies the impact of cyber attacks on the system security indices
7349	[Ton15]				✗						
7350	[MZG+15]	✗									
7351	[BFW15]	✓	✗				✓				All the references are not compiled!
7352	[Wan15]				✓						
7353	[TSST15]	✓	✗	✓							The problem of constructing data integrity attacks against real-time electrical market is formulated as a simulation-based global optimization problem
7354	[LTRC+15]	✗									
7355	[XWYL15]	✓	✗				✓				Coordinated attacks formulated as bilevel optimization problems

Table 23: Studies **7356 - 7380** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7356	[XN15]	✓	✓	✗							It presents 2 heuristic approaches with a tradeoff between the computational cost and the quality of state estimation; however, it omits both the proofs and details of the systems and considered attacks
7357	[AVS15]				✓	✓					Just awful! Predatory journal publication
7358	[TKSJ15]	✓	✗						✓		A good survey of cyber security solutions for control and monitoring systems
7359	[Liu15]				✓						
7360	[Dri15]	✓			✓						
7361	[Rot15]				✓						
7362	[DB15]	✓	✗				✓				
7363	[Bis15]				✓						
7364	[MFK+15]	✓	✗				✓				
7365	[Bai15]				✓						
7366	[Sak15]				✓						
7367	[Zha15d]				✓						
7368	[Che15]				✓						
7369	[Nab15]				✓						
7370	[HBB15]	✓	✗								It formulates and solves an optimization problem to select which nodes to protect, to minimize the MSE degradation due to uncoordinated and state-uninformed attacks on DC power flow model
7371	[CLZ+15]	✗									
7372	[FDTB15]	✗									
7373	[ZS15]				✗						
7374	[Zha15a]				✗						
7375	[LVDH15b]	✓	✓	✓							Follow up of [RVD14], [LVRD14], and [LVP+15]
7376	[Rah15]				✗						
7377	[MSM15]	✓	✗								It discusses the detection of FDI attacks using aberration index and normalised residues
7378	[FA15]	✗									
7379	[CGS+15]	✓	✗	✗			✓				
7380	[JCX15]	✓					✓				

Table 24: Studies **7383 - 7411** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7381	[Sri15]				✗						
7382	[Xu15]				✗						
7383	[Ye15]				✓						
7384	[WAKM15]	✗									
7385	[Cha15]				✓						
7386	[BH15]	✗	✗	✗							
7387	[BH15]	✗	✗	✗							
7388	[Kho15]	✓			✗						It proposes an approach based on matroid theory to construct sparsest attacks
7389	[SSL+15]	✗									
7390	[TLG15]	✗									
7391	[GSXY15b]	✓	✗						✓		A small survey of FDIA in smart grid
7392	[KLM15b]	✗									
7393	[KLM15a]	✗									
7394	[KSJ15]	✓	✗								
7395	[YA15]	✗									Anti-spoofing in PMU receiver, not on CPS itself
7396	[HK15]	✗									
7397	[BGBZ15]	✗									
7398	[BJ15]	✓	✗								
7399	[SS15b]	✗									
7400	[FPH15]	✓	✗								
7401	[Man15]				✓						
7402	[GHPK15]	✓	✗								
7403	[ZWJ15]	✗									
7404	[Gha15]				✗						
7405	[ZM15b]	✗									
7406	[NJ15a]	✓	✗								An optimal strategy via Q-learning for the cyber defence. It's a journal version of [NJ15b]
7407	[LZ15]	✗									
7408	[AHZM15]	✓	✗								
7409	[PFG15]	✗									
7410	[HPK+15a]	✓	✗								
7411	[BD15]	✗									

Table 25: Studies **7412 - 7438** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7412	[BA15]	✗									
7413	[TQGA15]	✓	✗								
7414	[LPK+15]				✓						
7415	[KTD15]	✓	✓	✓							
7416	[Tah15]				✓						
7417	[ABPT+15]	✗									
7418	[TSJ15]	✓	✓	✗							Stealthy attacks via a dissipative systems approach, no validation
7419	[APMR15]	✓	✓	✓			✓				Dynamic load altering detection solely based on load signal
7420	[BCF+15]	✗									
7421	[TO15a]	✗									
7422	[Nud15]				✓						
7423	[CBZ+15]				✓						
7424	[TO15b]	✗									
7425	[TO15c]	✗									
7426	[MLX15]	✗	✗								
7427	[LSC+15b]	✗	✗								
7428	[SLL15]	✓	✗								
7429	[RH15]	✗									
7430	[E+15]	✓	✗						✓		A small survey for a conference
7431	[TAN+15]	✗									
7432	[GR15]	✓	✗	✓							It proposes a new expression to quantify the trustiness of the measurements in smart grid. See also [LLD11]
7433	[NS15]	✓	✗				✓				It applies a deep (supervised) learning technique for detection of simple integrity attacks
7434	[RL15c]	✗									
7435	[RL15b]	✗									
7436	[LMD+15]	✗									
7437	[RP15]	✗									
7438	[MMY15]	✓	✗								The authors developed a smart grid simulation test-bed and designed evaluation scenarios

Table 26: Studies **7439 - 7468** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7439	[RL15a]	✗									
7440	[MSSFM15]	✗									
7441	[LN15a]	✗									
7442	[LMO+15]	✓					✓				
7443	[MLK+15]	✓	✓	✓							
7444	[LM15]	✗									
7445	[SRK+15]	✗									
7446	[GLW+15]	✓					✓				
7447	[LVP+15]	✓	✓	✓							
7448	[SEC15]	✗									
7449	[ABE15]	✗					✓				
7450	[CWSS15]	✗									
7451	[KM15]	✓	✗	✗							It is an application paper. It formulates an attack strategy by reverse engineering the firmware of an existing commercial protection relay.
7452	[KKG15]	✓					✓				
7453	[BLL+15]	✗									
7454	[LWLL15]	✗									
7455	[YQL15]	✗							✓		
7456	[NAH15]	✓	✗				✓				
7457	[DC15]	✗									
7458	[KA15]	✓	✗						✓		A small survey for a conference
7459	[PLSH15]	✗									
7460	[DSK15]	✗									
7461	[LMB+15]				✓						
7462	[CABvM15]	✗									
7463	[YLVY15]	✗									
7464	[ASM15]	✗									
7465	[WWX+15]	✗	✗								
7466	[CRGH15]	✗									
7467	[ZYY15]						✓				
7468	[VLG15]	✓	✗								Four-wheel-drive robotic vehicle's case study

Table 27: Studies **7469 - 7498** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7469	[BHY+15]	✓	✗		✓						Highly cited arXiv paper on experimental analysis of cyber security threats against teleoperated surgical robots
7470	[KL15]	✓	✗		✓						White paper, DEFCON 23
7471	[CAS15b]	✓	✗				✓				
7472	[FFWZ15]	✗	✗								
7473	[Har15]				✓						
7474	[PPM+15]	✗									
7475	[ZNA15]	✗									
7476	[ZZLN15]	✓	✗								It studies the LQG control performance under jamming attack
7477	[SWW+15]	✗									
7478	[Gun15]				✓						
7479	[ZYBV15]	✓	✗								
7480	[WSH15]	✗	✗								
7481	[Jon15]				✓						
7482	[ADC15]	✗									
7483	[ZHX+15]	✓					✓				
7484	[KGH15]	✓					✓				
7485	[GGH15]	✓	✗								
7486	[NM15b]	✓	✗	✗							It analyses the threats exploited by Stuxnet.
7487	[SMF+15]	✗									
7488	[CZS15]	✓	✗								NISTIR 8089, to mention
7489	[SLM15]	✓	✗								
7490	[HCPB15]	✓	✗								
7491	[Pei15]	✗									
7492	[SLK+15]	✓	✗								
7493	[Chi15]				✓		✓				
7494	[Lyn15]				✓						
7495	[Zha15b]				✓						
7496	[TSME15]	✗									
7497	[Zha15c]	✓	✗				✓				
7498	[CBB+16]	✓	✗						✓		

Table 28: Studies **7499 - 7530** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7499	[CZZL15]	✗	✓	✓							
7500	[LHX+15]	✗									
7501	[YZF15]	✗									It has some ties to security issues, but those are not the main focus of this work
7502	[ZM15a]	✗									
7503	[VLGB15]	✓	✓	✓			✓				Decision Trees
7504	[FHK15b]	✓	✗								The following 6 papers are all equal
7505	[FHK15d]	✓	✗								These papers are all equal
7506	[HFK15b]	✓	✗								These papers are all equal
7507	[FHK15a]	✓	✗								These papers are all equal
7508	[FHK15c]	✓	✗								These papers are all equal
7509	[HFK15a]	✓	✗								These papers are all equal
7510	[CLSC15]	✗									
7511	[Rat15]				✓						
7512	[YT15]	✗									
7513	[RSG15]	✗									
7514	[MA15]	✗									
7515	[HZ15]	✗									
7516	[AY15]	✗			✓						
7517	[GQ15]	✗									
7518	[GQS15]	✗									
7519	[ZAS15]	✗									
7520	[TR15]	✗									
7521	[TSDR15]	✗									
7522	[RD15]	✗									
7523	[SGK15]	✗							✓		
7524	[MB15]	✗									
7525	[Moo15]				✓						
7526	[YZQS15]	✓	✗								
7527	[ZLD+15]	✓	✗								
7528	[PR15]	✗									
7529	[Foo15]				✓						
7530	[LWW+15]	✗							✓		

Table 29: Studies **7531 - 7544** retrieved by application of forward snowballing technique

ID	Study	(I1)	(I2)	(I3)	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	Notes
7531	[ZH15]	✗									
7532	[MRP+15]	✗									
7533	[DMWW15]	✗									
7534	[Par15]	✗									
7535	[Cas15a]	✗									
7536	[HJK+15]	✗									
7537	[JAK+15b]	✗									
7538	[JAK+15a]	✗									
7539	[TGW15]	✗								✓	
7540	[Nuz15]				✓						
7541	[RB15a]	✓							✓		
7542	[KMM+15]	✓	✗				✓				
7543	[DBV15a]	✓			✓						
7544	[LVDH15a]	✓	✓	✓							

References

[ABE15] Nawal Ait Aali, Amine Baina, and Loubna Echabbi. Trust integration in collaborative access control model for critical infrastructures. In *Intelligent Systems: Theories and Applications (SITA), 2015 10th International Conference on*, pages 1–6. IEEE, 2015.

[ABF+08] S.J. Almond, S. Baird, B.F. Flynn, D.J. Hawkins, and A.J. Mackrell. Integrated protection and control communications outwith the substation: Cyber security challenges. In *Developments in Power System Protection, 2008. DPSP 2008. IET 9th International Conference on*, pages 698–701, March 2008.

[ABPT+15] Bilal Al Baalbaki, Jesus Pacheco, Cihan Tunc, Salim Hariri, and Youssif Al-Nashif. Anomaly behavior analysis system for zigbee in smart buildings. In *Computer Systems and Applications (AICCSA), 2015 IEEE/ACS 12th International Conference of*, pages 1–4. IEEE, 2015.

[ACS+06] M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee. Security challenges in next generation cyber physical systems. In *Proceedings of Beyond SCADA: Networked Embedded Control for Cyber Physical Systems Meeting (HCSS-NEC4CPS)*, November 2006.

[ADC15] Ahmad W Al-Dabbagh and Tongwen Chen. Modelling and control of wireless networked control systems: A fixed structure approach. In *Control Applications (CCA), 2015 IEEE Conference on*, pages 1051–1056. IEEE, 2015.

[Adh15] Uttam Adhikari. *Event and intrusion detection systems for cyber-physical power systems*. Mississippi State University, 2015.

[AE12] Waseem Abbas and Magnus Egerstedt. Securing multiagent systems against a sequence of intruder attacks. In *American Control Conference (ACC), 2012*, pages 4161–4166. IEEE, 2012.

[AEV+12] Göran Andersson, Peyman Mohajerin Esfahani, Maria Vrakopoulou, Kostas Margellos, John Lygeros, André Teixeira, György Dán, Henrik Sandberg, and Karl H Johansson. Cyber-security of scada systems. In *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*, pages 1–2. IEEE, 2012.

[AFL11] C. Alcaraz, C. Fernandez-Gago, and J. Lopez. An early warning system based on reputation for energy control systems. *Smart Grid, IEEE Transactions on*, 2(4):827–834, December 2011.

[AG05] J.M. Arroyo and F.D. Galiana. On the solution of the bilevel programming formulation of the terrorist threat problem. *Power Systems, IEEE Transactions on*, 20(2):789–797, May 2005.

[AG12] S.M. Amin and A.M. Giacomoni. Smart grid, safe grid. *Power and Energy Magazine, IEEE*, 10(1):33–40, January 2012.

[AHG14] A. Ashok, A. Hahn, and M. Govindarasu. Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment. *Journal of Advanced Research*, 5(4):481–489, 2014.

[AHT+15] Khaled F Alotaibi, Milad Moghassem Hamidi, Morteza Talebi, Jinsheng Xu, and Abdollah Homaifar. Using spy node to identify cyber-attack in power systems as a novel approach. In *Electro/Information Technology (EIT), 2015 IEEE International Conference on*, pages 581–586. IEEE, 2015.

[AHZM15] Muhammad Daniel Hafiz Abdullah, Zurina Mohd Hanapi, Zuriati Ahmad Zukarnain, and Mohamad Afendee Mohamed. Attacks, vulnerabilities and security requirements in smart metering networks. *KSII Transactions on Internet & Information Systems*, 9(4), 2015.

[AKWM15] Pacome L. Ambassa, Anne V.D.M. Kayem, Stephen D. Wolthusen, and Christoph Meinel. Secure and reliable power consumption monitoring in untrustworthy microgrids. In *International Conference on Future Network Systems and Security*, pages 166–180. Springer, 2015.

[ALSB10] S. Amin, X. Litrico, S.S. Sastry, and A.M. Bayen. Stealthy deception attacks on water SCADA systems. In *Proceedings of the 13th ACM International Conference on Hybrid Systems: Computation and Control*, HSCC '10, pages 161–170, New York, NY, USA, 2010. ACM.

[ALSB13] S. Amin, X. Litrico, S.S. Sastry, and A.M. Bayen. Cyber security of water scada systems – part ii: Attack detection using enhanced hydrodynamic models. *Control Systems Technology, IEEE Transactions on*, 21(5):1679–1693, September 2013.

[AM12] A. Ashok and G. Manimaran. Cyber attacks on power system state estimation through topology errors. In *Power and Energy Society General Meeting, 2012 IEEE*, pages 1–8, July 2012.

[AM14] A. Anwar and A.N. Mahmood. Vulnerabilities of smart grid state estimation against false data injection attack. In J. Hossain and A. Mahmud, editors, *Renewable Energy Integration*, Green Energy and Technology, pages 411–428. Springer Singapore, 2014.

[AMA14] A. Anwar, A.N. Mahmood, and M. Ahmed. False data injection attack targeting the LTC transformers to disrupt smart grid operation. In *10th International Conference on Security and Privacy in Communication Networks, SecureComm 2014*, Springer Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer International Publishing, September 2014.

[Ami11] M. Amin. Guaranteeing the security of an increasingly stressed grid. *IEEE Smart Grid Newsletter*, February 2011.

[AMP15] S. Amini, H. Mohsenian-Rad, and F. Pasqualetti. Dynamic load altering attacks in smart grid. In *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, February 2015.

[AMS15] Adnan Anwar, Abdun Naser Mahmood, and Zubair Shah. A data-driven approach to distinguish cyber-attacks from physical faults in a smart grid. In *Proceedings of the 24th ACM International on Conference on Information and Knowledge Management*, pages 1811–1814. ACM, 2015.

[AMT15] A. Anwar, A.N. Mahmood, and Z. Tari. Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid. *Information Systems*, 53(0):201–212, October 2015.

[AP14] N.B. Ali and K. Petersen. Evaluating strategies for study selection in systematic literature studies. In *Empirical Software Engineering and Measurement, 8th ACM/IEEE International Symposium on*, ESEM '14, pages 45:1–45:4. ACM, 2014.

[APMR15] Sajjad Amini, Fabio Pasqualetti, and Hamed Mohsenian-Rad. Detecting dynamic load altering attacks: A data-driven time-frequency analysis. In *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, pages 503–508. IEEE, 2015.

[AR14a] J. Abad Torres and S. Roy. Stabilization and destabilization of network processes by sparse remote feedback: Graph-theoretic approach. In *American Control Conference (ACC), 2014*, pages 3984–3989. IEEE, June 2014.

[AR14b] G. Anusha and R. Ramesh. Awful data injection attack and defense in electricity business sector using game theory. *International Journal of Emerging Engineering Research and Technology*, 2(8):62–68, November 2014.

[AR14c] A. Arvani and V.S. Rao. Cyber security of smart grid systems using intrusion detection methods. In *The International Conference on Computer Security and Digital Investigation (ComSec2014)*, pages 21–28. The Society of Digital Information and Wireless Communication, 2014.

[AR14d] A. Arvani and V.S. Rao. Detection and protection against intrusions on smart grid systems. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 3(1):38–48, 2014.

[Arr10] J.M. Arroyo. Bilevel programming applied to power system vulnerability analysis under multiple contingencies. *IET generation, transmission & distribution*, 4(2):178–190, 2010.

[ASM15] Araz Ashouri, Paul Stadler, and François Maréchal. Day-ahead promised load as alternative to real-time pricing. In *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, pages 551–556. IEEE, 2015.

[ATKF13] A. Almalawi, Z. Tari, I. Khalil, and A. Fahad. SCADAVT-A framework for SCADA security testbed based on virtualization technology. In *Local Computer Networks (LCN), 2013 IEEE 38th Conference on*, pages 639–646, October 2013.

[AVS15] Amatus Salam Ayesha, Drg Veeranjaneyulu, and Khadarbi Shaik. On false information infusion assaults on force framework state: Estimation& countermeasures. *International Journal of Advanced Technology and Innovative Research*, 2015.

[AW08] M. Abrams and J. Weiss. Malicious control system cyber security attack case study – maroochy water services, australia. *McLean, VA: The MITRE Corporation*, 2008.

[AY15] Gürdal Arslan and Serdar Yüksel. Decentralized Q-learning for stochastic teams and games. *arXiv preprint arXiv:1506.07924*, 2015.

[AYA+14] M.Q. Ali, R. Yousefian, E. Al-Shaer, S. Kamalasadan, and Q. Zhu. Two-tier data-driven intrusion detection for automatic generation control in smart grid. In *Communications and Network Security (CNS), 2014 IEEE Conference on*, pages 292–300, October 2014.

[AZSE12] Y. Abdallah, Z. Zheng, N.B. Shroff, and H. El Gamal. On the efficiency-vs-security tradeoff in the smart grid. In *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*, pages 1954–1959, December 2012.

[AZSE14] Y. Abdallah, Z. Zheng, N.B. Shroff, and H. El Gamal. The impact of stealthy attacks on smart grid performance: Tradeoffs and implications. *arXiv preprint arXiv:1502.06004*, 2014.

[BA13] Z.A. Baig and A.-R. Amoudi. An analysis of smart grid attacks and countermeasures. *Journal of Communications*, 8(8):473–479, August 2013.

[BA15] Justin M Bradley and Ella M Atkins. Optimization and control of cyber-physical vehicle systems. *Sensors*, 15(9):23020–23049, 2015.

[Bai15] Cheng-Zong Bai. *On the application of relative entropy in sequential detection and cyber-physical security*. University of Notre Dame, 2015.

[Bau10] T. Baumeister. Literature review on smart grid cyber security. Technical report, University of Hawaii at Manoa, 2010.

[BB10] S. Bhattacharya and T. Başar. Game-theoretic analysis of an aerial jamming attack on a UAV communication network. In *American Control Conference (ACC), 2010*, pages 818–823, June 2010.

[BBB+92] N. Balu, T. Bertram, A. Bose, V. Brandwajn, G. Cauley, D. Curtice, A. Fouad, L. Fink, M.G. Lauby, B.F. Wollenberg, and J.N. Wrubel. On-line power system security analysis. *Proceedings of the IEEE*, 80(2):262–282, February 1992.

[BBFP15] A. Barenghi, L. Breveglieri, M. Fugini, and G. Pelosi. Computer security anchors in smart grids: The smart metering scenario and challenges. In *Trusted Computing for Embedded Systems*, pages 47–59. Springer, 2015.

[BBH+14] Andrey Bernstein, Daniel Bienstock, David Hay, Meric Uzunoglu, and Gil Zussman. Power grid vulnerability to geographically correlated failuresanalysis and control implications. In *INFOCOM, 2014 Proceedings IEEE*, pages 2634–2642. IEEE, 2014.

[BCF+15] Giorgio Battistelli, Luigi Chisci, Nicola Forti, Giuseppe Pelosi, and Stefano Selleri. Point source estimation via finite element multiple-model Kalman filtering. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages 4984–4989. IEEE, 2015.

[BCQ13] C. Barreto, Á.A. Cárdenas, and N. Quijano. Controllability of dynamical systems: Threat models and reactive security. In S.K. Das, C. Nita-Rotaru, and M. Kantarcioglu, editors, *Decision and Game Theory for Security*, volume 8252 of *Lecture Notes in Computer Science*, pages 45–64. Springer International Publishing, 2013.

[BD15] Saverio Bolognani and Florian Dörfler. Fast power system analysis via implicit linearization of the power flow manifold. In *Communication, Control, and Computing (Allerton), 2015 53rd Annual Allerton Conference on*, pages 402–409. IEEE, 2015.

[BDS+14] Z. Birnbaum, A. Dolgikh, V. Skormin, E. O'Brien, and D. Muller. Unmanned aerial vehicle security using recursive parameter estimation. In *Unmanned Aircraft Systems (ICUAS), 2014 International Conference on*, pages 692–702, May 2014.

[BDSL15] N. Bezzo, Y. Du, O. Sokolsky, and I. Lee. A Markovian approach for attack resilient control of mobile robotic systems. In *2nd International Workshop on Robotic Sensor Networks, CPSWEEK 2015*, April 2015.

[BFDS08] Antonio Bicchi, Adriano Fagiolini, Gianluca Dini, and Ida Maria Savino. Tolerating, malicious monitors in detecting misbehaving robots. In *Safety, Security and Rescue Robotics, 2008. SSRR 2008. IEEE International Workshop on*, pages 109–114. IEEE, 2008.

[BFP+13] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi. Communication security for smart grid distribution networks. *Communications Magazine, IEEE*, 51(1):42–49, January 2013.

[BFW15] Alessio Baiocco, Chiara Foglietta, and Stephen D Wolthusen. Delay and jitter attacks on hierarchical state estimation. In *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, pages 485–490. IEEE, 2015.

[BG14] C.-Z. Bai and V. Gupta. On Kalman filtering in the presence of a compromised sensor: Fundamental performance bounds. In *American Control Conference (ACC), 2014*, pages 3029–3034, June 2014.

[BGA11a] G.K. Befekadu, V. Gupta, and P.J. Antsaklis. Risk-sensitive control under a class of Denial-of-Service attack models. In *American Control Conference (ACC), 2011*, pages 643–648, June 2011.

[BGA11b] G.K. Befekadu, V. Gupta, and P.J. Antsaklis. Risk-sensitive control under a Markov modulated Denial-of-Service attack model. In *2011 50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC)*, pages 5714–5719, 345 E 47Th St, New York, NY 10017 USA, 2011. IEEE.

[BGA15] G.K. Befekadu, V. Gupta, and P.J. Antsaklis. Risk-sensitive control under Markov modulated Denial-of-Service (DoS) attack strategies. *Automatic Control, IEEE Transactions on*, PP(99):1–1, 2015.

[BGBZ15] F Benhamida, A Graa, L Benameur, and I Ziane. A mathematical model of power system state estimation for power flow solution. *World Academy of Science, Engineering and Technology, International Journal of Mathematical and Computational Sciences*, 2(10), 2015.

[BGN+09] E. Bompard, C. Gao, R. Napoli, A. Russo, M. Masera, and A. Stefanini. Risk assessment of malicious attacks against power systems. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, 39(5):1074–1085, September 2009.

[BGY12] S. Bhattarai, L. Ge, and W. Yu. A novel architecture against false data injection attacks in smart grid. In *Communications (ICC), 2012 IEEE International Conference on*, pages 907–911, June 2012.

[BH15] Elisa Bertino and Nathan W Hartman. Cybersecurity for product lifecycle management a research roadmap. In *Intelligence and Security Informatics (ISI), 2015 IEEE International Conference on*, pages 114–119. IEEE, 2015.

[Bha15] Jahshan Ahmed Bhatti. *Sensor deception detection and radio-frequency emitter localization*. PhD thesis, The University of Texas at Austin, 2015.

[BHK+10] M. Brunner, H. Hofinger, C. Krauß, C. Roblee, P. Schoo, and S. Todt. Infiltrating critical infrastructures with next-generation attacks. *Fraunhofer Institute for Secure Information Technology (SIT), Munich*, 2010.

[BHWC13] E. Bompard, T. Huang, Y. Wu, and M. Cremenescu. Classification and trend analysis of threats origins to the security of power systems. *International Journal of Electrical Power & Energy Systems*, 50:50–64, 2013.

[BHY+15] Tamara Bonaci, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno, and Howard Jay Chizeck. To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots. *arXiv preprint arXiv:1504.04339*, 2015.

[Bis11] A.N. Bishop. A robust reachability review for control system security. In *Australian Control Conference (AUCC), 2011*, pages 381–385, November 2011.

[Bis12] A.N. Bishop. False-data attacks in stochastic estimation problems with only partial prior model information. In *Control, Automation and Information Sciences (ICCAIS), 2012 International Conference on*, pages 1–6, November 2012.

[Bis15] Nancy Bissinger. *Cyberintrusion Detection in Critical Infrastructure*. PhD thesis, Auburn University, 2015.

[BJ15] Ying Bi and Abbas Jamalipour. A time correlated attacker-defender model for smart grid communication networks. In *Communications (ICC), 2015 IEEE International Conference on*, pages 815–819. IEEE, 2015.

[BL04] E. Byres and J. Lowe. The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress*, volume 116, pages 213–218, 2004.

[BLL+15] Feifei Bai, Yong Liu, Yilu Liu, Kai Sun, Navin Bhatt, Alberto Del Rosso, Evangelos Farantatos, and Xiaoru Wang. Measurement-based correlation approach for power system dynamic response estimation. *IET Generation, Transmission & Distribution*, 9(12):1474–1484, 2015.

[BM08] W. Boyer and M. McQueen. Ideal based cyber security technical metrics for control systems. In J. Lopez and B.M. Hämmerli, editors, *Critical Information Infrastructures Security*, volume 5141 of *Lecture Notes in Computer Science*, pages 246–260. Springer Berlin Heidelberg, 2008.

[BMC13] M. Burmester, E. Magkos, and V. Chrissikopoulos. T-ABAC: An attribute-based access control model for real-time availability in highly dynamic systems. In *Computers and Communications (ISCC), 2013 IEEE Symposium on*, pages 143–148, July 2013.

[BPG15a] C.-Z. Bai, F. Pasqualetti, and V. Gupta. Security in stochastic control systems: Fundamental limitations and performance bounds. In *American Control conference (ACC), 2015*, July 2015.

[BPG15b] Cheng-Zong Bai, Fabio Pasqualetti, and Vijay Gupta. Security in stochastic control systems: Fundamental limitations and performance bounds. In *American Control Conference (ACC), 2015*, pages 195–200. IEEE, 2015.

[BRW+10] R.B. Bobba, K.M. Rogers, Q. Wang, Hi. Khurana, K. Nahrstedt, and T.J. Overbye. Detecting false data injection attacks on DC state estimation. In *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010*, April 2010.

[BS11] A.N. Bishop and A.V. Savkin. On false-data attacks in robust multi-sensor-based estimation. In *Control and Automation (ICCA), 2011 9th IEEE International Conference on*, pages 10–17, December 2011.

[BS12] Hendrik Baumann and Werner Sandmann. Markovian modeling and security measure analysis for networks under flooding DoS attacks. In *Parallel, Distributed and Network-Based Processing (PDP), 2012 20th Euromicro International Conference on*, pages 298–302. IEEE, 2012.

[BS13] A.N. Bishop and A.V. Savkin. Set-valued state estimation and attack detection for uncertain descriptor systems. *Signal Processing Letters, IEEE*, 20(11):1102–1105, November 2013.

[BW14] A. Baiocco and S.D. Wolthusen. Stability of power network state estimation under attack. In *Innovative Smart Grid Technologies - Asia (ISGT Asia), 2014 IEEE*, pages 441–446, May 2014.

[BWP+14] N. Bezzo, J. Weimer, M. Pajic, O. Sokolsky, G.J. Pappas, and I. Lee. Attack resilient state estimation for autonomous robotic systems. In *Intelligent Robots and Systems (IROS 2014), 2014 IEEE/RSJ International Conference on*, pages 3692–3698, September 2014.

[BYH+15] T. Bonaci, J. Yan, J. Herron, T. Kohno, and H.J. Chizeck. Experimental analysis of Denial-of-Service attacks on teleoperated robotic systems. In *6th International Conference on Cyber-Physical Systems (ICCPS)*. ACM/IEEE, April 2015.

[BZ11] S. Bi and Y.J. Zhang. Defending mechanisms against false-data injection attacks in the power system state estimation. In *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, pages 1162–1167, December 2011.

[BZ13a] S. Bi and Y.J. Zhang. False-data injection attack to control real-time price in electricity market. In *Global Communications Conference (GLOBECOM), 2013 IEEE*, pages 772–777, December 2013.

[BZ13b] S. Bi and Y.J. Zhang. Mitigating false-data injection attacks on dc state estimation using covert topological information. In *Global Communications Conference (GLOBECOM), 2013 IEEE*, pages 766–771, December 2013.

[BZ14a] S. Bi and Y.J. Zhang. Graphical methods for defense against false-data injection attacks on power system state estimation. *Smart Grid, IEEE Transactions on*, 5(3):1216–1227, May 2014.

[BZ14b] S. Bi and Y.J. Zhang. Using covert topological information for defense against malicious attacks on dc state estimation. *Selected Areas in Communications, IEEE Journal on*, 32(7):1471–1485, July 2014.

[BZD+14] C. Beasley, X. Zhong, J. Deng, R. Brooks, and G. Kumar Venayagamoorthy. A survey of electric power synchrophasor network cyber security. In *Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2014 IEEE PES*, pages 1–5, October 2014.

[CA14a] Q. Chen and S. Abdelwahed. A model-based approach to self-protection in SCADA systems. In *9th International Workshop on Feedback Computing (Feedback Computing 14)*. USENIX Association, 2014.

[CA14b] Q. Chen and S. Abdelwahed. Towards realizing self-protecting SCADA systems. In *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, CISR '14, pages 105–108, New York, NY, USA, 2014. ACM.

[CABvM15] Guido Cavraro, Reza Arghandeh, Grazia Barchi, and Alexandra von Meier. Distribution network topology detection with time-series measurements. In *Innovative Smart Grid Technologies Conference (ISGT), 2015 IEEE Power & Energy Society*, pages 1–5. IEEE, 2015.

[CAS08] Á.A. Cárdenas, S. Amin, and S.S. Sastry. Research challenges for the security of control systems. In *Proceedings of the 3rd Conference on Hot Topics in Security*, HOTSEC'08, pages 6:1–6:6, Berkeley, CA, USA, 2008. USENIX Association.

[CAS+09] Á.A. Cárdenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S.S. Sastry. Challenges for securing cyber physical systems. In *Proceedings of the Workshop on Future Directions in Cyber-Physical Systems Security*. National Science Foundation, July 2009.

[Cas15a] Christos G Cassandras. Event-driven control and optimization in hybrid systems. *Event-Based Control and Signal Processing*, pages 21–36, 2015.

[CAS15b] Qian Chen, Robert K Abercrombie, and Frederick T Sheldon. Risk assessment for industrial control systems quantifying availability using mean failure cost (mfc). *Journal of Artificial Intelligence and Soft Computing Research*, 5(3):205–220, 2015.

[CB05] A. Creery and E.J. Byres. Industrial cybersecurity for power system and SCADA networks. In *Petroleum and Chemical Industry Conference, 2005. Industry Applications Society 52nd Annual*, pages 303–309, September 2005.

[CBB+16] Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart. A review of cyber security risk assessment methods for SCADA systems. *Computers & security*, 56:1–27, 2016.

[CBD+09] M. Cheminod, I.C. Bertolotti, L. Durante, P. Maggi, D. Pozza, R. Sisto, and A. Valenzano. Detecting chains of vulnerabilities in industrial networks. *Industrial Informatics, IEEE Transactions on*, 5(2):181–193, May 2009.

[CBZ+15] Ankush Chakrabarty, Gregery T Buzzard, Stanisław H Zak, Fanglai Zhu, and Ann E Rundell. Simultaneous unknown input and sensor noise reconstruction for nonlinear systems with boundary layer sliding mode observers. *arXiv preprint arXiv:1507.03924*, 2015.

[CCC12] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen. Smart attacks in smart grid communication networks. *Communications Magazine, IEEE*, 50(8):24–29, August 2012.

[CDF+07] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes. Using model-based intrusion detection for SCADA networks. In *Proceedings of the SCADA security scientific symposium*, volume 46, pages 1–12, 2007.

[CDHX11] G. Chen, Z.Y. Dong, D.J. Hill, and Y.S. Xue. Exploring reliable strategies for defending power systems against targeted attacks. *Power Systems, IEEE Transactions on*, 26(3):1000–1009, August 2011.

[CFM+14] E. Ciancamerla, B. Fresilli, M. Minichino, T. Patriarca, and Serguei Iassinovski. An electrical grid and its scada under cyber attacks: Modelling versus a hybrid test bed. In *Security Technology (ICCST), 2014 International Carnahan Conference on*, pages 1–6. IEEE, 2014.

[CGS+15] Vanea Chiprianov, Laurent Gallon, Khouloud Salameh, Manuel Munier, and Jamal El Hachem. Towards security software engineering the smart grid as a system of systems. In *System of Systems Engineering Conference (SoSE), 2015 10th*, pages 77–82. IEEE, 2015.

[Cha15] Gu Chaojun. *Modelling and analysis of cyber-security and reliability of energy delivery for resilient smart grid systems*. PhD thesis, National University of Singapore, 2015.

[Che15] Xuhui Chen. *Secure cloud computing for solving large-scale linear systems of equations*. PhD thesis, Mississippi State University, 2015.

[Chi15] Nayana Teja Chiluvuri. *A trusted autonomic architecture to safeguard cyber-physical control leaf nodes and protect process integrity*. PhD thesis, Virginia Tech, 2015.

[CHK+12] S. Cui, Z. Han, S. Kar, T.T. Kim, H.V. Poor, and A. Tajer. Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions. *Signal Processing Magazine, IEEE*, 29(5):106–115, September 2012.

[CHPB15] N.T. Chiluvuri, O.A. Harshe, C.D. Patterson, and C.T. Baumann. Using heterogeneous computing to implement a trust isolated architecture for cyber-physical control systems. In *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, CPSS '15, pages 25–35, New York, NY, USA, 2015. ACM.

[CHT15] Young Hwan Chang, Qie Hu, and Claire J. Tomlin. Secure estimation based kalman filter for cyber-physical systems against adversarial attacks. *arXiv preprint arXiv:1512.03853*, 2015.

[CI15a] Y. Chakhchoukh and H. Ishii. Coordinated cyber-attacks on the measurement function in hybrid state estimation. *Power Systems, IEEE Transactions on*, 30(5):2487–2497, September 2015.

[CI15b] Yacine Chakhchoukh and Hideaki Ishii. Cyber attacks scenarios on the measurement function of power state estimation. In *American Control Conference (ACC), 2015*, pages 3676–3681. IEEE, 2015.

[CIH15] Ahmet Cetinkaya, Hideaki Ishii, and Tomohisa Hayakawa. Event-triggered output feedback control resilient against jamming attacks and random packet losses. *IFAC-PapersOnLine*, 48(22):270–275, 2015. 5th IFAC Workshop on Distributed Estimation and Control in Networked Systems (NecSys).

[CIMR13] C. Carryl, M. Ilyas, I. Mahgoub, and M. Rathod. The PEV security challenges to the smart grid: Analysis of threats and mitigation strategies. In *Connected Vehicles and Expo (ICCVE), 2013 International Conference on*, pages 300–305, December 2013.

[CJM15] G. Chaojun, P. Jirutitijaroen, and M. Motani. Detecting false data injection attacks in AC state estimation. *Smart Grid, IEEE Transactions on*, 6(5):2476–2483, September 2015.

[CKBR06] Glenn Carl, George Kesidis, Richard R. Brooks, and Suresh Rai. Denial-of-service attack-detection techniques. *IEEE Internet computing*, 10(1):82–89, 2006.

[CKM15] Y. Chen, S. Kar, and J.M.F. Moura. Dynamic attack detection in cyber-physical systems with side initial state information. *arXiv preprint arXiv:1503.07125*, 2015.

[CKM17] Yuan Chen, Soummya Kar, and José MF Moura. Dynamic attack detection in cyber-physical systems with side initial state information. *IEEE Transactions on Automatic Control*, 62(9):4618–4624, 2017.

[Cle08] F.M. Cleveland. Cyber security issues for advanced metering infrasttructure (ami). In *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, pages 1–5, July 2008.

[CLSC15] Xianghui Cao, Lu Liu, Wenlong Shen, and Yu Cheng. Distributed scheduling and delay-aware routing in multi-hop mr-mc wireless networks. *networks*, 5:7, 2015.

[CLZ+15] Nina Chaichi, Joao Lavoie, Soheil Zarrin, Rafaa Khalifa, and Felix Sie. A comprehensive assessment of cloud computing for smart grid applications: A multi-perspectives framework. In *Management of Engineering and Technology (PICMET), 2015 Portland International Conference on*, pages 2541–2547. IEEE, 2015.

[CM12] Á.A. Cárdenas and R. Moreno. Cyber-physical systems security for the smart grid. In *NISTIR 7916 Proceedings of the Cybersecurity in Cyber-Physical Systems Workshop*, 2012.

[CMBK13] B. Chen, S. Mashayekh, K.L. Butler-Purry, and D. Kundur. Impact of cyber attacks on transient stability of smart grids with voltage support devices. In *Power and Energy Society General Meeting (PES), 2013 IEEE*, pages 1–5, July 2013.

[CMK+11] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*. San Francisco, 2011.

[CMM+14] H. Cam, P. Mouallem, Yilin Mo, B. Sinopoli, and B. Nkrumah. Modeling impact of attacks, recovery, and attackability conditions for situational awareness. In *Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2014 IEEE International Inter-Disciplinary Conference on*, pages 181–187, 2014.

[CP12] Jie Chen and Ron J. Patton. *Robust model-based fault diagnosis for dynamic systems*, volume 3. Springer Science & Business Media, 2012.

[CPW13] D. Chen, Y. Peng, and H. Wang. Development of a testbed for process control system cybersecurity research. In *3rd International Conference on Electric and Electronics*. Atlantis Press, 2013.

[CRGH15] Yousu Chen, Mark Rice, Kurt Glaesemann, and Zhenyu Huang. Sub-second state estimation implementation and its evaluation with real data. In *Power & Energy Society General Meeting, 2015 IEEE*, pages 1–5. IEEE, 2015.

[CSCZ15] J. Chen, L. Shi, P. Cheng, and H. Zhang. Optimal Denial-of-Service attack scheduling with energy constraint. *Automatic Control, IEEE Transactions on*, 60(11):3023–3028, November 2015.

[CSK+10] R. Chabukswar, B. Sinopoli, G. Karsai, A. Giani, H. Neema, and A. Davis. Simulation of network attacks on SCADA systems. In *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010*, April 2010.

[CUC+11] R. Chow, E. Uzun, Á.A. Cárdenas, Z. Song, and S. Lee. Enhancing cyber-physical security through data patterns. In *Proceedings of the Workshop on Foundations of Dependable and Secure Cyber-Physical Systems (FDSCPS), CPSWeek 2011*, pages 25–29, April 2011.

[CWH15] M.S. Chong, M. Wakaiki, and J.P. Hespanha. Observability of linear systems under adversarial attacks. In *American Control conference (ACC), 2015*, July 2015.

[CWSS15] Wentao Chen, Junzheng Wang, Ling Shi, and Dawei Shi. State estimation of finite-state hidden markov models subject to stochastically event-triggered measurements. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages 3712–3717. IEEE, 2015.

[CWVW14] V. Chetty, N. Woodbury, E. Vaziripour, and S. Warnick. Vulnerability analysis for distributed and coordinated destabilization attacks. In *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*, pages 511–516, December 2014.

[CX12] D.-H. Choi and L. Xie. Malicious ramp-induced temporal data attack in power market with look-ahead dispatch. In *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, pages 330–335, November 2012.

[CX13] D.-H. Choi and L. Xie. Ramp-induced data attacks on look-ahead dispatch in real-time power markets. *Smart Grid, IEEE Transactions on*, 4(3):1235–1243, September 2013.

[CYM+15] P.-Y. Chen, S. Yang, J.A. McCann, J. Lin, and X. Yang. Detection of false data injection attacks in smart-grid systems. *Communications Magazine, IEEE*, 53(2):206–213, February 2015.

[CZS15] Richard Candell, Timothy Zimmerman, and Keith Stouffer. An industrial control system cybersecurity performance testbed. *National Institute of Standards and Technology. NISTIR*, 8089, 2015.

[CZZL15] Long Cao, Hangsheng Zhao, Jianzhao Zhang, and Yongxiang Liu. Secure cooperative spectrum sensing based on energy efficiency under SSDF attack. In *Wireless Symposium (IWS), 2015 IEEE International*, pages 1–4. IEEE, 2015.

[D+15] Van Long Do et al. *Sequential detection and isolation of cyber-physical attacks on SCADA systems*. PhD thesis, Troyes, 2015.

[DAA10] A. Delgadillo, J.M. Arroyo, and N. Alguacil. Analysis of electric grid interdiction with line switching. *Power Systems, IEEE Transactions on*, 25(2):633–641, May 2010.

[dAKO02] D. Conte de Leon, J. Alves-Foss, A. Krings, and P. Oman. Modeling complex control systems to identify remotely accessible devices vulnerable to cyber attack. In *ACM Workshop on Scientific Aspects of Cyber Terrorism,(SACT)*. Citeseer, 2002.

[DB15] Sri Yogesh Dorbala and Robin Singh Bhadoria. Analysis for security attacks in cyber-physical systems. In *Cyber-Physical Systems: A Computational Perspective*, pages 395–414. CRC Press, 2015.

[DBV14a] D. Deka, R. Baldick, and S. Vishwanath. Attacking power grids with secure meters: The case for breakers and jammers. In *Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on*, pages 646–651, April 2014.

[DBV14b] D. Deka, R. Baldick, and S. Vishwanath. Data attack on strategic buses in the power grid: Design and protection. In *PES General Meeting — Conference Exposition, 2014 IEEE*, pages 1–5, July 2014.

[DBV14c] D. Deka, R. Baldick, and S. Vishwanath. Hidden attacks on power grid: Optimal attack strategies and mitigation. *arXiv preprint arXiv:1401.3274*, 2014.

[DBV14d] D. Deka, R. Baldick, and S. Vishwanath. Optimal hidden SCADA attacks on power grid: A graph theoretic approach. In *Computing, Networking and Communications (ICNC), 2014 International Conference on*, pages 36–40, February 2014.

[DBV15a] D Deka, R Baldick, and S Vishwanath. Data attacks on the power grid despite detection. *IEEE PES Innovative Smart Grid Technologies*, 2015.

[DBV15b] Deepjyoti Deka, Ross Baldick, and Sriram Vishwanath. Data attacks on power grids: Leveraging detection. In *Innovative Smart Grid Technologies Conference (ISGT), 2015 IEEE Power & Energy Society*, pages 1–5. IEEE, 2015.

[DBV15c] Deepjyoti Deka, Ross Baldick, and Sriram Vishwanath. One breaker is enough: hidden topology attacks on power grids. In *Power & Energy Society General Meeting, 2015 IEEE*, pages 1–5. IEEE, 2015.

[DBV15d] Deepjyoti Deka, Ross Baldick, and Sriram Vishwanath. Optimal data attacks on power grids: Leveraging detection & measurement jamming. In *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, pages 392–397. IEEE, 2015.

[DC15] Mangal Hemant Dhend and Rajan Hari Chile. Innovative scheme for smart grid distribution SCADA system. In *Future Energy Electronics Conference (IFEEC), 2015 IEEE 2nd International*, pages 1–6. IEEE, 2015.

[DCEF11] S. D'Antonio, L. Coppolino, I.A. Elia, and V. Formicola. Security issues of a phasor data concentrator for smart grid infrastructure. In *Proceedings of the 13th European Workshop on Dependable Computing*, EWDC '11, pages 3–8, New York, NY, USA, 2011. ACM.

[DDS13a] A. D'Innocenzo, M Di Benedetto, and E. Serra. Fault tolerant control of multi-hop control networks. *Automatic Control, IEEE Transactions on*, 58(6):1377–1389, June 2013.

[DDS13b] A. D'Innocenzo, M.D. Di Benedetto, and F. Smarra. Fault detection and isolation of malicious nodes in MIMO multi-hop control networks. In *Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on*, pages 5276–5281, December 2013.

[DFN15] V.L. Do, L. Fillatre, and I. Nikiforov. Two sub-optimal algorithms for detecting cyber/physical attacks on SCADA systems. In *Proceedings of the 10th International Conference on System Identification and Control Problems (SICPRO'15)*, pages 1144–1156, January 2015.

[DGPH14] Z. Dai, H. Gao, Y. Peng, and L. Huikang. A new information security risk assessment method in power production system based on rough sets and bayesian network. In *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on*, pages 532–536, August 2014.

[DGS15] S. Dadras, R.M. Gerdes, and R. Sharma. Vehicular platooning in an adversarial environment. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ASIA CCS '15, pages 167–178, New York, NY, USA, 2015. ACM.

[DMBH12] K.R. Davis, K.L. Morrow, R. Bobba, and E. Heine. Power flow cyber attacks and perturbation-based defense. In *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, pages 342–347, November 2012.

[DMWW15] Chaoyang Dong, Aojia Ma, Qing Wang, and Zhaolei Wang. Robust fault-tolerant tracking control for nonlinear networked control system: asynchronous switched polytopic approach. *Mathematical Problems in Engineering*, 2015, 2015.

[DNWH13] Q. Dong, D. Niyato, P. Wang, and Z. Han. Deferrable load scheduling optimization under power price information attacks in smart grid. In *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*, pages 4683–4688, April 2013.

[DR13] R. Dhal and S. Roy. Vulnerability of continuous-time network synchronization processes: A minimum energy perspective. In *Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on*, pages 823–828, December 2013.

[Dri15] Anis Drira. *Characterization of Optimal Cyber Attacks on Control Systems*. PhD thesis, University of Tennessee - Knoxville, 2015.

[DS10] G. Dán and H. Sandberg. Stealth attacks and protection schemes for state estimators in power systems. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 214–219, October 2010.

[DS12] Y. Deng and S. Shukla. Vulnerabilities and countermeasures – a survey on the cyber security issues in the transmission subsystem of a smart grid. *Journal of Cyber Security and Mobility*, 1(2):251–276, 2012.

[DSA96] C.L. De Marco, J.V. Sariashkar, and F. Alvarado. The potential for malicious control in a competitive power systems environment. In *Control Applications, 1996., Proceedings of the 1996 IEEE International Conference on*, pages 462–467, September 1996.

[DSDB15] A. D'Innocenzo, F. Smarra, and M.D. Di Benedetto. Further results on fault detection and isolation of malicious nodes in Multi-hop Control Networks. In *Control Conference (ECC), 2015 European*, pages 1–6, July 2015. PP.

[DSEB12] G. Dán, H. Sandberg, M. Ekstedt, and G. Björkman. Challenges in power system information security. *IEEE Security & Privacy*, 10(4):62–70, 2012.

[DSK15] Prachi Deshpande, SC Sharma, and P Sateesh Kumar. Security threats in cloud computing. In *Computing, Communication & Automation (ICCCA), 2015 International Conference on*, pages 632–636. IEEE, 2015.

[DSV+09] R. Diao, K. Sun, V. Vittal, R.J. O'Keefe, M.R. Richardson, N. Bhatt, D. Stradford, and S.K. Sarawgi. Decision tree-based online voltage security assessment using PMU measurements. *Power Systems, IEEE Transactions on*, 24(2):832–839, May 2009.

[DT14a] C. De Persis and P. Tesi. On resilient control of nonlinear systems under Denial-of-Service. In *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*, pages 5254–5259, December 2014.

[DT14b] C. De Persis and P. Tesi. Resilient control under Denial-of-Service. In *19th IFAC World Congress*, pages 134–139, 2014.

[DT15] C. De Persis and P. Tesi. Input-to-State stabilizing control under Denial-of-Service. *Automatic Control, IEEE Transactions on*, 60(11):2930–2944, November 2015.

[DTO+06] C.M. Davis, J.E. Tate, H. Okhravi, C. Grier, T.J. Overbye, and D. Nicol. SCADA cyber security testbed development. In *Power Symposium, 2006. NAPS 2006. 38th North American*, pages 483–488, September 2006.

[DWD14] D. Ding, Z. Wang, and H. Dong. Dynamic output feedback control for discrete-time stochastic nonlinear systems with adversaries. In *Control Conference (CCC), 2014 33rd Chinese*, pages 5428–5432, July 2014.

[DWDG13] S.S.S.R. Depuru, L. Wang, V. Devabhaktuni, and R.C. Green. High performance computing for detection of electricity theft. *International Journal of Electrical Power & Energy Systems*, 47(0):21–30, 2013.

[DZC15] Jie Duan, Wente Zeng, and Mo-Yuen Chow. Economic impact of data integrity attacks on distributed DC optimal power flow algorithm. In *North American Power Symposium (NAPS), 2015*, pages 1–7. IEEE, 2015.

[E+15] Mohamed Essaaidi et al. An overview of smart grid cyber-security state of the art study. In *Renewable and Sustainable Energy Conference (IRSEC), 2015 3rd International*, pages 1–7. IEEE, 2015.

[EDEO06] J. Eisenhauer, P. Donnelly, M. Ellis, and M. O'Brien. Roadmap to secure control systems in the energy sector. Technical report, Energ. Incorp., U.S. Dept. Energy and the U.S. Dept. Homeland Secur., January 2006.

[EHS12] M. Esmalifalak, Z. Han, and L. Song. Effect of stealthy bad data injection on network congestion in market based power system. In *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*, pages 2468–2472, April 2012.

[ENZ+18] M. Esmalifalak, H. Nguyen, R. Zheng, L. Xie, L. Song, and Z. Han. A stealthy attack against electricity market using independent component analysis. *IEEE Systems Journal*, 12(1):297–307, March 2018.

[ENZH11] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han. Stealth false data injection using independent component analysis in smart grid. In *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, pages 244–248, October 2011.

[ENZH13] M. Esmalifalak, N.T. Nguyen, R. Zheng, and Z. Han. Detecting stealthy false data injection using machine learning in smart grid. In *Global Communications Conference (GLOBECOM), 2013 IEEE*, pages 808–813, December 2013.

[EP10] D.G. Eliades and M.M. Polycarpou. A fault diagnosis and security framework for water systems. *Control Systems Technology, IEEE Transactions on*, 18(6):1254–1265, November 2010.

[EPP14] I. Esnaola, S.M. Perlaza, and H.V. Poor. Equilibria in data injection attacks. In *Signal and Information Processing (GlobalSIP), 2014 IEEE Global Conference on*, pages 779–783, December 2014.

[EPPK15] Iñaki Esnaola, Samir M Perlaza, H Vincent Poor, and Oliver Kosut. *Decentralized maximum distortion MMSE attacks in electricity grids*. PhD thesis, Inria-Research Centre Grenoble–Rhône-Alpes, 2015.

[Eri07] G.N. Ericsson. Toward a framework for managing information security for an electric power utility – cigrÉ experiences. *Power Delivery, IEEE Transactions on*, 22(3):1461–1469, July 2007.

[ESHS12] M. Esmalifalak, G. Shi, Z. Han, and L. Song. Attack against electricity market-attacker and defender gaming. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 3147–3152, December 2012.

[ESHS13] M. Esmalifalak, G. Shi, Z. Han, and L. Song. Bad data injection attack and defense in electricity market using game theory study. *Smart Grid, IEEE Transactions on*, 4(1):160–169, March 2013.

[EVM+10a] P.M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson. Cyber attack in a two-area power system: Impact identification using reachability. In *American Control Conference (ACC), 2010*, pages 962–967, June 2010.

[EVM+10b] P.M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson. A robust policy for automatic generation control cyber attack in two area power network. In *Decision and Control (CDC), 2010 49th IEEE Conference on*, pages 5973–5978, December 2010.

[FA15] Muhammad Omer Farooq and Muhammad Abid. Robust fault diagnosis of power grid network system. In *Electrical Engineering (RAEE), 2015 Symposium on Recent Advances in*, pages 1–6. IEEE, 2015.

[FBB09] Adriano Fagiolini, Francesco Babboni, and Antonio Bicchi. Dynamic distributed intrusion detection for secure multi-robot systems. In *Robotics and Automation, 2009. ICRA'09. IEEE International Conference on*, pages 2723–2728. IEEE, 2009.

[FD97] Paul M. Frank and Xianchun Ding. Survey of robust residual generation and evaluation methods in observer-based fault detection systems. *Journal of process control*, 7(6):403–424, 1997.

[FDB14] Adriano Fagiolini, Gianluca Dini, and Antonio Bicchi. Distributed intrusion detection for the security of industrial cooperative robotic systems. *IFAC Proceedings Volumes*, 47(3):7610–7615, 2014.

[FDTB15] Athanasios Fevgas, Konstantis Daloukas, Panagiota Tsompanopoulou, and Panayiotis Bozanis. A study of sparse matrix methods on new hardware: Advances and challenges. *International Journal of Monitoring and Surveillance Technologies Research (IJMSTR)*, 3(3):1–19, 2015.

[FEG08] Mauro Franceschelli, Magnus Egerstedt, and Alessandro Giua. Motion probes for fault detection and recovery in networked control systems. In *American Control Conference, 2008*, pages 4358–4363. IEEE, 2008.

[FEK14] R. Felix, J. Economou, and K. Knowles. UAS behaviour and consistency monitoring system for countering cyber security threats. Technical report, SAE Technical Paper, 2014.

[FFB+13] Y. Feng, C. Foglietta, A. Baiocco, S. Panzieri, and S.D. Wolthusen. Malicious false data injection in hierarchical electric power grid state estimation systems. In *Proceedings of the Fourth International Conference on Future Energy Systems*, e-Energy '13, pages 183–192, New York, NY, USA, 2013. ACM.

[FFFS15] Mohammad Farajollahi, Mahmud Fotuhi-Firuzabad, and Amir Safdarian. Impact of erroneous measurements on power system real-time security analysis. In *Electrical Engineering (ICEE), 2015 23rd Iranian Conference on*, pages 1630–1635. IEEE, 2015.

[FFK+11a] Z.M. Fadlullah, M.M. Fouda, N. Kato, X. Shen, and Y. Nozaki. An early warning system against malicious activities for smart grid communications. *Network, IEEE*, 25(5):50–55, September 2011.

[FFK+11b] M.M. Fouda, Z.M. Fadlullah, N. Kato, R. Lu, and X. Shen. A lightweight message authentication scheme for smart grid communications. *Smart Grid, IEEE Transactions on*, 2(4):675–685, December 2011.

[FFWZ15] Xiaohe Fan, Kefeng Fan, Yong Wang, and Ruikang Zhou. Overview of cyber-security of industrial control system. In *Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on*, pages 1–7. IEEE, 2015.

[FGMS11] Igor Nai Fovino, Luca Guidi, Marcelo Masera, and Alberto Stefanini. Cyber security assessment of a power plant. *Electric Power Systems Research*, 81(2):518–526, 2011.

[FHAK14] A.K. Farraj, E.M. Hammad, A. Al Daoud, and D. Kundur. A game-theoretic control approach to mitigate cyber switching attacks in smart grid systems. In *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, pages 958–963, November 2014.

[FHFFS15] M. Farajollahi, S.H. Hosseini, M. Fotuhi-Firuzabad, and A. Safdarian. Bad data injection as a threat for power system security. In *Smart Grid Conference (SGC), 2015*, pages 138–144. IEEE, 2015.

[FHK15a] Abdallah Farraj, Eman Hammad, and Deepa Kundur. On using distributed control schemes to mitigate switching attacks in smart grids. In *Electrical and Computer Engineering (CCECE), 2015 IEEE 28th Canadian Conference on*, pages 1578–1582. IEEE, 2015.

[FHK15b] Abdallah Farraj, Eman Hammad, and Deepa Kundur. On using distributed energy resources to reshape the dynamics of power systems during transients. In *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, pages 756–761. IEEE, 2015.

[FHK15c] Abdallah Farraj, Eman Hammad, and Deepa Kundur. Robustness analysis of feedback linearization distributed control schemes in smart grid systems. In *Power & Energy Society General Meeting, 2015 IEEE*, pages 1–5. IEEE, 2015.

[FHK15d] Abdallah Farraj, Eman Hammad, and Deepa Kundur. A systematic approach to delay-adaptive control design for smart grids. In *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, pages 768–773. IEEE, 2015.

[FHKB14] A.K. Farraj, E.M. Hammad, D. Kundur, and K.L. Butler-Purry. Practical limitations of sliding-mode switching attacks on smart grid systems. In *PES General Meeting — Conference Exposition, 2014 IEEE*, pages 1–5, July 2014.

[FIRT15] Paolo Frasca, Hideaki Ishii, Chiara Ravazzi, and Roberto Tempo. Distributed randomized algorithms for opinion formation, centrality computation and power systems estimation: A tutorial overview. *European journal of control*, 24:2–13, 2015.

[FK15] Abdallah K. Farraj and Deepa Kundur. On using energy storage systems in switching attacks that destabilize smart grid systems. In *Innovative Smart Grid Technologies Conference (ISGT), 2015 IEEE Power & Energy Society*, pages 1–5. IEEE, 2015.

[FKW08] T. Fleury, H. Khurana, and V. Welch. Towards a taxonomy of attacks against energy control systems. In M. Papa and S. Shenoi, editors, *Critical Infrastructure Protection II*, volume 290 of *The International Federation for Information Processing*, pages 71–85. Springer US, 2008.

[FM10] T. Flick and J. Morehouse. *Securing the smart grid: next generation power grid security*. Elsevier, 2010.

[FM12a] H.S. Foroush and S. Martinez. On event-triggered control of linear systems under periodic Denial-of-Service jamming attacks. In *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*, pages 2551–2556, December 2012.

[FM12b] H.S. Foroush and S. Martínez. On single-input controllable linear systems under periodic DoS jamming attacks. *arXiv preprint arXiv:1209.4101*, 2012.

[FM13] H.S. Foroush and S. Martínez. On multi-input controllable linear systems under unknown periodic DoS jamming attacks. In *SIAM Conf. on Control and its Applications*, pages 222–229. SIAM, 2013.

[FN07] M. Fabro and T. Nelson. Control systems cyber security: Defense-in-depth strategies. Technical Report INL/CON-07-12804, Idaho National Laboratory, Houston, TX, 2007. ISA Expo.

[FNU13] Y. Fujita, T. Namerikawa, and K. Uchida. Cyber attack detection and faults diagnosis in power networks by using state fault diagnosis matrix. In *Control Conference (ECC), 2013 European*, pages 398–403, July 2013.

[Foo15] Ming Qing Foo. *Secure electric power grid operation*. PhD thesis, Massachusetts Institute of Technology, 2015.

[FPH15] Shih-Wei Fang, Anthony Portante, and Mohammad Iftekhar Husain. Moving target defense mechanisms in cyber-physical systems. *Securing Cyber-Physical Systems*, page 63, 2015.

[FPV+08] Adriano Fagiolini, Marco Pellinacci, Gianni Valenti, Gianluca Dini, and Antonio Bicchi. Consensus-based distributed intrusion detection for multi-robot systems. In *Robotics and Automation, 2008. ICRA 2008. IEEE International Conference on*, pages 120–127. IEEE, 2008.

[Fra90] Paul M Frank. Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: A survey and some new results. *automatica*, 26(3):459–474, 1990.

[FS14] Roberto Filippini and Andrés Silva. A modeling framework for the resilience analysis of networked systems-of-systems based on functional dependencies. *Reliability Engineering & System Safety*, 125:82–91, 2014.

[FTD11] H. Fawzi, P. Tabuada, and S. Diggavi. Secure state-estimation for dynamical systems under active adversaries. In *Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on*, pages 337–344, September 2011.

[FTD12] H. Fawzi, P. Tabuada, and S. Diggavi. Security for control systems under sensor and actuator attacks. In *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*, pages 3412–3417, December 2012.

[FTD14] H. Fawzi, P. Tabuada, and S. Diggavi. Secure estimation and control for cyber-physical systems under adversarial attacks. *Automatic Control, IEEE Transactions on*, 59(6):1454–1467, June 2014.

[FVP+07a] Adriano Fagiolini, Gianni Valenti, Lucia Pallottino, Gianluca Dini, and Antonio Bicchi. Decentralized intrusion detection for secure cooperative multi-agent systems. In *Decision and Control, 2007 46th IEEE Conference on*, pages 1553–1558. IEEE, 2007.

[FVP+07b] Adriano Fagiolini, Gianni Valenti, Lucia Pallottino, Gianluca Dini, and Antonio Bicchi. Local monitor implementation for decentralized intrusion detection in secure multi-agent systems. In *Automation Science and Engineering, 2007. CASE 2007. IEEE International Conference on*, pages 454–459. IEEE, 2007.

[FWLS09] E.B. Fernandez, J. Wu, M.M. Larrondo-Petrie, and Y. Shao. On building secure SCADA systems using security patterns. In *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*, CSIIRW '09, pages 17:1–17:4, New York, NY, USA, 2009. ACM.

[FZT+14] Y. Fan, Z. Zhang, M. Trinkle, A.D. Dimitrovski, J.B. Song, and H. Li. A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids. *Smart Grid, IEEE Transactions on*, PP(99):1–1, 2014.

[GA13] M. Göl and A. Abur. Identifying vulnerabilities of state estimators against cyber-attacks. In *PowerTech (POWERTECH), 2013 IEEE Grenoble*, pages 1–4, June 2013.

[GA14] M. Göl and A. Abur. Effective measurement design for cyber security. In *Power Systems Computation Conference (PSCC), 2014*, pages 1–8, August 2014.

[GAY15] Zhitao Guan, Peixiu An, and Tingting Yang. Matrix partition-based detection scheme for false data injection in smart grid. *International Journal of Wireless and Mobile Computing*, 9(3):250–256, 2015.

[GB13] A. Giani and R. Bent. Addressing smart grid cyber security. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, CSIIRW '13, pages 44:1–44:4, New York, NY, USA, 2013. ACM.

[GBG+11] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla. Smart grid data integrity attacks: characterizations and countermeasures. In *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, pages 232–237, October 2011.

[GBG+13] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla. Smart grid data integrity attacks. *Smart Grid, IEEE Transactions on*, 4(3):1244–1253, September 2013.

[GBH+12] A. Giani, R. Bent, M. Hinrichs, M. McQueen, and K. Poolla. Metrics for assessment of smart grid data integrity attacks. In *Power and Energy Society General Meeting, 2012 IEEE*, pages 1–8, July 2012.

[GBP14] A. Giani, R. Bent, and F. Pan. Phasor measurement unit selection for unobservable electric power data integrity attack detection. *International Journal of Critical Infrastructure Protection*, 7(3):155–164, 2014.

[GBR13] H. Gawand, A. Bhattacharjee, and K. Roy. Confirmation of theoretical results regarding control theoretic cyber attacks on controllers. *Dynamics and Control of Process Systems*, 10(1):702–707, 2013.

[GCQ14] J. Giraldo, Á.A. Cárdenas, and N. Quijano. Attenuating the impact of integrity attacks on real-time pricing in smart grids. *arXiv preprint arXiv:1410.5111*, 2014.

[GDJ12] Meng Guo, Dimos V Dimarogonas, and Karl Henrik Johansson. Distributed real-time fault detection and isolation for cooperative multi-agent systems. In *American Control Conference (ACC), 2012*, pages 5270–5275. IEEE, 2012.

[GGB15] Manuel Garcia, Annarita Giani, and Ross Baldick. Smart grid data integrity attacks: Observable islands. In *Power & Energy Society General Meeting, 2015 IEEE*, pages 1–5. IEEE, 2015.

[GGH15] Béla Genge, Flavius Graur, and Piroska Haller. Experimental assessment of network design approaches for protecting industrial control systems. *International Journal of Critical Infrastructure Protection*, 11:24–38, 2015.

[GGI+15] D. Gollmann, P. Gurikov, A. Isakov, M. Krotofil, J. Larsen, and A. Winnicki. Cyber-physical systems security: Experimental analysis of a vinyl acetate monomer plant. In *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, CPSS '15, pages 1–12, New York, NY, USA, 2015. ACM.

[GH15] Sanjay Goel and Yuan Hong. Security challenges in smart grid implementation. In *Smart Grid Security*, pages 1–39. Springer, 2015.

[Gha15] Hamid Reza Ghasemi. *Architecture and Circuit Cross-Cutting Approaches for Power-Efficient Multi-Core Processors*. PhD thesis, The University of Wisconsin-Madison, 2015.

[GHB+12] D. Grochocki, J.H. Huh, R. Berthier, R. Bobba, W.H. Sanders, A.A. Cardenas, and J.G. Jetcheva. AMI threats, intrusion detection requirements and deployment recommendations. In *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, pages 395–400, November 2012.

[GHPK15] Sanjay Goel, Yuan Hong, Vagelis Papakonstantinou, and Dariusz Kloza. *Smart grid security*. Springer, 2015.

[GKR+08] A. Giani, G. Karsai, T. Roosta, A. Shah, B. Sinopoli, and J. Wiley. A testbed for secure and robust SCADA systems. *SIGBED Rev.*, 5(2):4:1–4:4, July 2008.

[GLB10] A. Gupta, C. Langbort, and T. Başar. Optimal control in the presence of an intelligent jammer with limited actions. In *Decision and Control (CDC), 2010 49th IEEE Conference on*, pages 1096–1101, December 2010.

[GLMM13] A. Giani, O. Linda, M. Manic, and M. McQueen. Known secure sensor measurements concept and its application for critical infrastructure systems. In *Optimization and Security Challenges in Smart Power Grids*, pages 181–201. Springer, 2013.

[GLMR14] H.E. Garcia, W.-C. Lin, S.M. Meerkov, and M.T. Ravichandran. Resilient monitoring systems: Architecture, design, and application to boiler/turbine plant. *Cybernetics, IEEE Transactions on*, 44(11):2010–2023, November 2014.

[GLS+12] J. Goppert, W. Liu, A. Shull, V. Sciandra, I. Hwang, and H. Aldridge. Numerical analysis of cyberattacks on unmanned aerial systems. In *Infotech@Aerospace 2012*. American Institute of Aeronautics and Astronautics, 2012.

[GLW+15] Longhua Guo, Jianhua Li, Jun Wu, Zhengmin Xia, and Shengjun Zheng. A security mechanism for demand response using rbac and pub/sub. In *Autonomous Decentralized Systems (ISADS), 2015 IEEE Twelfth International Symposium on*, pages 260–265. IEEE, 2015.

[GM13] B. Groza and M. Minea. Bridging Dolev-Yao adversaries and control systems with time-sensitive channels. In E. Luiijf and P. Hartel, editors, *Critical Information Infrastructures Security*, volume 8328 of *Lecture Notes in Computer Science*, pages 167–178. Springer International Publishing, 2013.

[GM14] W. Gao and T.H Morris. On cyber attacks and signature based intrusion detection for modbus based industrial control systems. *Journal of Digital Forensics, Security and Law*, 9(1):37–56, 2014.

[GMRR10] Wei Gao, Thomas Morris, Bradley Reaves, and Drew Richey. On SCADA control system command and response injection and intrusion detection. In *eCrime Researchers Summit (eCrime), 2010*, pages 1–9. IEEE, 2010.

[GQ15] Azwirman Gusrialdi and Zhihua Qu. Growing connected networks under privacy constraint: Achieving trade-off between performance and security. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages 312–317. IEEE, 2015.

[GQS15] Azwirman Gusrialdi, Zhihua Qu, and Marwan A Simaan. Game theoretical designs of resilient cooperative systems. In *Control Conference (ECC), 2015 European*, pages 1705–1711. IEEE, 2015.

[GR15] Malini Ghosal and Vittal Rao. Mitigation of adverse effect of false data injection in optimally controlled smart grid. In *ASME 2015 Power Conference collocated with the ASME 2015 9th International Conference on Energy Sustainability, the ASME 2015 13th International Conference on Fuel Cell Science, Engineering and Technology, and the ASME 2015 Nuclear Forum*, pages V001T11A010–V001T11A010. American Society of Mechanical Engineers, 2015.

[GS13] B. Genge and C. Siaterlis. Investigating the effect of network parameters on coordinated cyber attacks against a simulated power plant. In S. Bologna, B. Hämmerli, D. Gritzalis, and S. Wolthusen, editors, *Critical Information Infrastructure Security*, volume 6983 of *Lecture Notes in Computer Science*, pages 140–151. Springer Berlin Heidelberg, 2013.

[GS14] Béla Genge and Christos Siaterlis. Physical process resilience-aware network design for SCADA systems. *Computers & Electrical Engineering*, 40(1):142–157, 2014.

[GSE15] A. Gaber, K.G. Seddik, and A.Y. Elezabi. Joint estimation-detection of cyber attacks in smart grids: Bayesian and non-bayesian formulations. In *Wireless Communications and Networking Conference (WCNC), 2015 IEEE*, pages 1–6, March 2015. Poster.

[GSFW12] S. Giorgi, F. Saleheen, F. Ferrese, and C.-H. Won. Adaptive neural replication and resilient control despite malicious attacks. In *Resilient Control Systems (ISRCS), 2012 5th International Symposium on*, pages 112–117, August 2012.

[GSJS09] A. Giani, S. Sastry, K.H. Johansson, and H. Sandberg. The VIKING project: An initiative on resilient control of power networks. In *Resilient Control Systems, 2009. ISRCS '09. 2nd International Symposium on*, pages 31–35, August 2009.

[GSS+14] J. Goppert, A. Shull, N. Sathyamoorthy, W. Liu, I. Hwang, and H. Aldridge. Software / hardware-in-the-loop analysis of cyberattacks on unmanned aerial systems. *Journal of Aerospace Information Systems*, 11(5):337–343, 2014.

[GSXY15a] Z. Guan, N. Sun, Y. Xu, and T. Yang. A comprehensive survey of false data injection in smart grid. *Int. J. Wireless and Mobile Computing*, 8(1):27–33, January 2015.

[GSXY15b] Zhitao Guan, Nan Sun, Yue Xu, and Tingting Yang. A comprehensive survey of false data injection in smart grid. *International Journal of Wireless and Mobile Computing*, 8(1):27–33, 2015.

[GT13] P.T. Gunjal and S.G. Tamhankar. Review of attack detection scheme for cyber physical security system. *International Journal of Computer Science and Mobile Computing*, 2(12):401–405, December 2013.

[Gun15] Volkan Gunes. *Ensuring reliability and fault-tolerance for the cyber-physical system design*. PhD thesis, University of California, Irvine, 2015.

[GXSL+15] Sicun Gao, Le Xie, Armando Solar-Lezama, Dimitrios Serpanos, and Howard Shrobe. Automated vulnerability analysis of AC state estimation under constrained false data injection in electric power systems. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages 2613–2620. IEEE, 2015.

[GZLD12] S. Gong, Z. Zhang, H. Li, and A.D. Dimitrovski. Time stamp attack in smart grid: Physical mechanism and damage analysis. *arXiv preprint arXiv:1201.2578*, 2012.

[GZT+12] S. Gong, Z. Zhang, M. Trinkle, A.D. Dimitrovski, and H. Li. GPS spoofing based time stamp attack on real time wide area monitoring in smart grid. In *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, pages 300–305, November 2012.

[HAH13] T. Huynh, A. Alsadah, and F. Hu. Cyber-physical system controls. *Cyber-Physical Systems: Integrated Computing and Engineering Design*, pages 35–48, 2013.

[Har15] Omkar Anand Harshe. *Preemptive detection of cyber attacks on industrial control systems*. PhD thesis, Virginia Tech, 2015.

[HB14] Q. He and R.S. Blum. New hypothesis testing-based rapid change detection for power grid system monitoring. *International Journal of Parallel, Emergent and Distributed Systems*, 29(3):239–263, 2014.

[HBA+14] H. Hosseini, S.M.T. Bathaee, A. Abedini, M. Hosseina, and A. Fereidunain. Defending false data injection attack on smart grid network using neuro-fuzzy controller. *Journal of Intelligent and Fuzzy Systems*, 27(3):1457–1467, 2014.

[HBB15] Qian He, Duo Bai, and Rick S Blum. Optimum node selection for protection under power grid state estimation. In *Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference on*, pages 2864–2868. IEEE, 2015.

[HBEH12] D. Hadziosmanovic, D. Bolzoni, S. Etalle, and P. Hartel. Challenges and opportunities in securing industrial control systems. In *Complexity in Engineering (COMPENG), 2012*, pages 1–6, June 2012.

[HCPB15] O. A. Harshe, N. Teja Chiluvuri, C. D. Patterson, and W. T. Baumann. Design and implementation of a security framework for industrial control systems. In *2015 International Conference on Industrial Instrumentation and Control (ICIC)*, pages 127–132, May 2015.

[HEN+13] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li, and L. Song. Bad data injection in smart grid: attack and defense mechanisms. *Communications Magazine, IEEE*, 51(1):27–33, January 2013.

[HFK15a] Eman Hammad, Abdallah Farraj, and Deepa Kundur. On the effects of distributed control area design for the stabilization of cyber-enabled smart grids. In *Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2015 Workshop on*, pages 1–6. IEEE, 2015.

[HFK15b] Eman Hammad, Abdallah Farraj, and Deepa Kundur. Paradigms and performance of distributed cyber-enabled control schemes for the smart grid. In *Power & Energy Society General Meeting, 2015 IEEE*, pages 1–5. IEEE, 2015.

[HG12] G. Hug and J.A. Giampapa. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. *Smart Grid, IEEE Transactions on*, 3(3):1362–1370, September 2012.

[HH11] H. Hashimoto and T. Hayakawa. Distributed cyber attack detection for power network systems. In *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*, pages 5820–5824, December 2011.

[HJJ+14] J.M. Hendrickx, K.H. Johansson, R.M. Jungers, H. Sandberg, and K.C. Sou. Efficient computations of a security index for false data attacks in power networks. *Automatic Control, IEEE Transactions on*, 59(12):3194–3208, December 2014.

[HJK+15] Iman Haghighi, Austin Jones, Zhaodan Kong, Ezio Bartocci, Radu Gros, and Calin Belta. SpaTeL: a novel spatial-temporal logic and its applications to networked systems. In *Proceedings of the 18th International Conference on Hybrid Systems: Computation and Control*, pages 189–198. ACM, 2015.

[HJW07] A.J. Holmgren, E. Jenelius, and J. Westin. Evaluating strategies for defending electric power networks against antagonistic attacks. *Power Systems, IEEE Transactions on*, 22(1):76–84, February 2007.

[HK13] R. Hewett and P. Kijsanayothin. Securing system controllers in critical infrastructures. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, CSIIRW '13, pages 29:1–29:4, New York, NY, USA, 2013. ACM.

[HK15] Joseph Herkert and Timothy Kostyk. Societal implications of the smart grid: Challenges for engineering. In *Engineering Identities, Epistemologies and Values*, pages 287–306. Springer, 2015.

[HKD11] Tobias Hoppe, Stefan Kiltz, and Jana Dittmann. Security threats to automotive CAN networks practical examples and selected short-term countermeasures. *Reliability Engineering & System Safety*, 96(1):11–25, 2011.

[HKJ08] Fazirulhisyam Hashim, M Rubaiyat Kibria, and Abbas Jamalipour. Detection of dos and ddos attacks in ngmn using frequency domain analysis. In *Communications, 2008. APCC 2008. 14th Asia-Pacific Conference on*, pages 1–5. IEEE, 2008.

[HKKS10] Inseok Hwang, Sungwan Kim, Youdan Kim, and Chze Eng Seah. A survey of fault detection, isolation, and reconfiguration methods. *IEEE Transactions on control systems technology*, 18(3):636–653, 2010.

[HKMS12] J. Hull, H. Khurana, T. Markham, and K. Staggs. Staying in control: Cybersecurity and the modern electric grid. *Power and Energy Magazine, IEEE*, 10(1):41–48, January 2012.

[HLCH11] Y. Huang, H. Li, K.A. Campbell, and Z. Han. Defending false data injection attack on smart grid network using adaptive CUSUM test. In *Information Sciences and Systems (CISS), 2011 45th Annual Conference on*, pages 1–6, March 2011.

[HMX15] Duo Han, Yilin Mo, and Lihua Xie. Convex optimization based state estimation against sparse integrity attacks. *arXiv preprint arXiv:1511.07218*, 2015.

[HPK+14] J. Hao, R.J. Piechocki, D. Kaleshi, W.H. Chin, and Z. Fan. Optimal malicious attack construction and robust detection in smart grid cyber security analysis. In *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, pages 836–841, November 2014.

[HPK+15a] Jinping Hao, Robert J Piechocki, Dritan Kaleshi, Woon Hau Chin, and Zhong Fan. Multistage pmu placement scheduling for robust state estimation in power systems. In *Communication Workshop (ICCW), 2015 IEEE International Conference on*, pages 1952–1957. IEEE, 2015.

[HPK+15b] Jinping Hao, Robert J Piechocki, Dritan Kaleshi, Woon Hau Chin, and Zhong Fan. Sparse malicious false data injection attacks and defense mechanisms in smart grids. *IEEE Transactions on Industrial Informatics*, 11(5):1–12, 2015.

[HTC+14] Y. Huang, J. Tang, Y. Cheng, H. Li, K.A. Campbell, and Z. Han. Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis. *Systems Journal, IEEE*, PP(99):1–12, 2014.

[HTP+13] S Tmar-Ben Hamida, PH Thevenon, Jean-Benoît Pierrot, O Savry, and Claude Castelluccia. Detecting relay attacks in rfid systems using physical layer characteristics. In *Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP*, pages 1–8. IEEE, 2013.

[HWC15] Yingshuai Hao, Meng Wang, and Joe Chow. Likelihood of cyber data injection attacks to power systems. In *Signal and Information Processing (GlobalSIP), 2015 IEEE Global Conference on*, pages 657–661. IEEE, 2015.

[HWMD15] Z. Huang, Y. Wang, S. Mitra, and G. Dullerud. Controller synthesis for linear time-varying systems with adversaries. *arXiv preprint arXiv:1501.04925*, 2015.

[HWT+15] Zongshuai Hu, Yong Wang, Xiuxia Tian, Xiaoli Yang, Dejun Meng, and Rusen Fan. False data injection attacks identification for smart grids. In *Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), 2015 Third International Conference on*, pages 139–143. IEEE, 2015.

[HZ15] Yezekael Hayel and Quanyan Zhu. Attack-aware cyber insurance for risk sharing in computer networks. In *International Conference on Decision and Game Theory for Security*, pages 22–34. Springer, 2015.

[HZR12] F. He, J. Zhuang, and N.S.V. Rao. Game-theoretic analysis of attack and defense in cyber-physical network infrastructures. In G. Lim and J.W. Herrmann, editors, *Proceedings of the Industrial and Systems Engineering Research Conference*, 2012.

[IL15] Vittorio P Illiano and Emil C Lupu. Detecting malicious data injections in event detection wireless sensor networks. *IEEE Transactions on Network and Service Management*, 12(3):496–510, 2015.

[ILW06] V.M. Igure, S.A. Laughter, and R.D. Williams. Security issues in SCADA networks. *Computers & Security*, 25(7):498–506, 2006.

[IPL14a] R. Ivanov, M. Pajic, and I. Lee. Attack-resilient sensor fusion for safety-critical cyber-physical systems. Technical report, University of Pennsylvania, October 2014.

[IPL14b] Radoslav Ivanov, Miroslav Pajic, and Insup Lee. Attack-resilient sensor fusion. In *Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014*, pages 1–6. IEEE, 2014.

[Ise84] Rolf Isermann. Process fault detection based on modeling and estimation methods - a survey. *Automatica*, 20(4):387–404, 1984.

[IYF+14] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi. On detection of cyber attacks against voltage control in distribution power grids. In *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, pages 842–847, November 2014.

[JAK+15a] Austin Jones, Derya Aksaray, Zhaodan Kong, Mac Schwager, and Calin Belta. Enforcing temporal logic specifications via reinforcement learning. In *Proceedings of the 18th International Conference on Hybrid Systems: Computation and Control*, pages 279–280. ACM, 2015.

[JAK+15b] Austin Jones, Derya Aksaray, Zhaodan Kong, Mac Schwager, and Calin Belta. Robust satisfaction of temporal logic specifications via reinforcement learning. *arXiv preprint arXiv:1510.06460*, 2015.

[JAL13] P. Jokar, N. Arianpoo, and V.C.M. Leung. Intrusion detection in advanced metering infrastructure based on consumption pattern. In *Communications (ICC), 2013 IEEE International Conference on*, pages 4472–4476, June 2013.

[JCX15] Wang Jianqiao, Chen Cailian, and Guan Xinping. An overlapping distributed state estimation and detection method in smart grids. In *Wireless Communications & Signal Processing (WCSP), 2015 International Conference on*, pages 1–5. IEEE, 2015.

[JKB14] A. Jones, Z. Kong, and C. Belta. Anomaly detection in cyber-physical systems: A formal methods approach. In *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*, pages 848–853, December 2014.

[JKTT14] L. Jia, J. Kim, R.J. Thomas, and L. Tong. Impact of data quality on real-time locational marginal price. *Power Systems, IEEE Transactions on*, 29(2):627–636, March 2014.

[Jon15] Austin Jones. *Formal methods paradigms for estimation and machine learning in dynamical systems*. PhD thesis, Boston University, 2015.

[JSDA12] A.Y. Javaid, W. Sun, V.K. Devabhaktuni, and M. Alam. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, pages 585–590, November 2012.

[JTT12a] L. Jia, R.J. Thomas, and L. Tong. Impacts of malicious data on real-time price of electricity market operations. In *Proceedings of the 2012 45th Hawaii International Conference on System Sciences*, HICSS '12, pages 1907–1914, Washington, DC, USA, 2012. IEEE Computer Society.

[JTT12b] L. Jia, R.J. Thomas, and L. Tong. On the nonlinearity effects on malicious data attack on power system. In *Power and Energy Society General Meeting, 2012 IEEE*, pages 1–8, July 2012.

[KA15] Benahmed Khelifa and Smahi Abla. Security concerns in smart grids: Threats, vulnerabilities and countermeasures. In *Renewable and Sustainable Energy Conference (IRSEC), 2015 3rd International*, pages 1–6. IEEE, 2015.

[KBC+13] Denis Foo Kune, John Backes, Shane S Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. Ghost talk: Mitigating emi signal injection attacks against analog sensors. In *Security and Privacy (SP), 2013 IEEE Symposium on*, pages 145–159. IEEE, 2013.

[KCG15] Vaibhav Katewa, Aranya Chakrabortty, and Vijay Gupta. Protecting privacy of topology in consensus networks. In *American Control Conference (ACC), 2015*, pages 2476–2481. IEEE, 2015.

[KCR+10] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al. Experimental security analysis of a modern automobile. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 447–462. IEEE, 2010.

[KCS14] J.Y. Keller, K. Chabir, and D. Sauter. Input reconstruction for networked control systems subject to deception attacks and data losses on control signals. *International Journal of Systems Science*, pages 1–7, 2014.

[KFL+10] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K.L. Butler-Purry. Towards a framework for cyber attack impact analysis of the electric smart grid. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 244–249, October 2010.

[KFM+11] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. L. Butler-Purry. Towards modelling the impact of cyber attacks on a smart grid. *International Journal of Security and Networks*, 6(1):2–13, January 2011.

[KGH15] István Kiss, Béla Genge, and Piroska Haller. A clustering-based approach to detect cyber attacks in process control systems. In *Industrial Informatics (INDIN), 2015 IEEE 13th International Conference on*, pages 142–148. IEEE, 2015.

[KH13] C. Kwon and I. Hwang. Analytical analysis of cyber attacks on unmanned aerial systems. In *AIAA Guidance, Navigation, and Control (GNC) Conference*, February 2013.

[KHLF10] H. Khurana, M. Hadley, N. Lu, and D.A. Frincke. Smart-grid security issues. *Security Privacy, IEEE*, 8(1):81–85, January 2010.

[Kho15] Michael Khokhlov. A matroid theory approach to constructing the sparse attacks on power system state estimation. In *6th International Conference on Liberalization and Modernization of Power Systems*, page n/a. International Institute for Critical Infrastructures, 2015.

[KJTT10a] O. Kosut, L. Jia, R.J. Thomas, and L. Tong. Limiting false data attacks on power system state estimation. In *Information Sciences and Systems (CISS), 2010 44th Annual Conference on*, pages 1–6, March 2010.

[KJTT10b] O. Kosut, L. Jia, R.J. Thomas, and L. Tong. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 220–225, October 2010.

[KJTT10c] O. Kosut, L. Jia, R.J. Thomas, and L. Tong. On malicious data attacks on power system state estimation. In *Universities Power Engineering Conference (UPEC), 2010 45th International*, pages 1–6, August 2010.

[KJTT11] O. Kosut, L. Jia, R.J. Thomas, and L. Tong. Malicious data attacks on the smart grid. *Smart Grid, IEEE Transactions on*, 2(4):645–658, December 2011.

[KKG15] Irina Kolosok, Elena Korkina, and Liudmila Gurina. Vulnerability analysis of the state estimation problem under cyber attacks on WAMS. In *Intern. Conf. on Problems of Critical Infrastructures*, pages 67–75, 2015.

[KKW07] H. Khurana, M.M.H. Khan, and V. Welch. Leveraging computational grid technologies for building a secure and manageable power grid. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pages 115–115, January 2007.

[KL15] Marina Krotofil and Jason Larsen. Rocking the pocket book: Hacking chemical plants. In *DefCon Conference, DEFCON*, 2015.

[KLH13] C. Kwon, W. Liu, and I. Hwang. Security analysis for cyber-physical systems against stealthy deception attacks. In *American Control Conference (ACC), 2013*, pages 3344–3349, June 2013.

[KLH14] C. Kwon, W. Liu, and I. Hwang. Analysis and design of stealthy cyber attacks on unmanned aerial systems. *Journal of Aerospace Information Systems*, 11(8):525–539, 2014.

[KLK14] Gisung Kim, Seungmin Lee, and Sehun Kim. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 41(4):1690–1700, 2014.

[KLM15a] Igor Kaitovic, Slobodan Lukovic, and Miroslaw Malek. Proactive failure management in smart grids for improved resilience: A methodology for failure prediction and mitigation. In *Globecom Workshops (GC Wkshps), 2015 IEEE*, pages 1–6. IEEE, 2015.

[KLM15b] Igor Kaitovic, Slobodan Lukovic, and Miroslaw Malek. Unifying dependability of critical infrastructures: electric power system and ICT: concepts, figures of merit and taxonomy. In *Dependable Computing (PRDC), 2015 IEEE 21st Pacific Rim International Symposium on*, pages 50–59. IEEE, 2015.

[KM15] Charalambos Konstantinou and Michail Maniatakos. Impact of firmware modification attacks on power systems field devices. In *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, pages 283–288. IEEE, 2015.

[KMM+15] BooJoong Kang, Peter Maynard, Kieran McLaughlin, Sakir Sezer, Filip Andrén, Christian Seitl, Friederich Kupzog, and Thomas Strasser. Investigating cyber-physical attacks against iec 61850 photovoltaic inverter installations. In *Emerging Technologies & Factory Automation (ETFA), 2015 IEEE 20th Conference on*, pages 1–8. IEEE, 2015.

[KMP+14] G. Koutsandria, V. Muthukumar, M. Parvania, C. McParland, A. Scaglione, and S. Peisert. A hybrid network IDS for protective digital relays in the power transmission grid. In *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, pages 908–913, November 2014.

[KMT15] Michael G Kallitsis, George Michailidis, and Samir Tout. Correlative monitoring for detection of false data injection attacks in smart grids. In *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, pages 386–391. IEEE, 2015.

[KOJ11] Pierre Kleberger, Tomas Olovsson, and Erland Jonsson. Security aspects of the in-vehicle network in the connected car. In *Intelligent Vehicles Symposium (IV), 2011 IEEE*, pages 528–533. IEEE, 2011.

[Kos13] O. Kosut. Malicious data attacks against dynamic state estimation in the presence of random noise. In *Global Conference on Signal and Information Processing (GlobalSIP), 2013 IEEE*, pages 261–264, December 2013.

[Kos14] O. Kosut. Max-flow min-cut for power system security index computation. In *Sensor Array and Multichannel Signal Processing Workshop (SAM), 2014 IEEE 8th*, pages 61–64, June 2014.

[KP11] T.T. Kim and H.V. Poor. Strategic protection against data injection attacks on power grids. *Smart Grid, IEEE Transactions on*, 2(2):326–333, June 2011.

[KPH+15] W. Knowles, D. Prince, D. Hutchison, J.F.P. Disso, and K. Jones. A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, PP(99):1–1, 2015.

[KPP14] N. Komninos, E. Philippou, and A. Pitsillides. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *Communications Surveys Tutorials, IEEE*, 16(4):1933–1954, Fourthquarter 2014.

[KS14] P. Kaster and P.K. Sen. Power grid cyber security: Challenges and impacts. In *North American Power Symposium (NAPS), 2014*, pages 1–6, September 2014.

[KS15] R. Khorshidi and F. Shabaninia. A new method for detection of fake data in measurements at smart grids state estimation. *IET Science, Measurement & Technology*, 2015.

[KSJ15] Surender Kumar, MK Soni, and DK Jain. Cyber security threats in synchrophasor system in wide area monitoring system. *Indonesian Journal of Electrical Engineering and Computer Science*, 15(3):436–444, 2015.

[KSWC14] K. Kuntz, M. Smith, K. Wedeward, and M. Collins. Detecting, locating, & quantifying false data injections utilizing grid topology through optimized D-FACTS device placement. In *North American Power Symposium (NAPS), 2014*, pages 1–6, September 2014.

[KT13a] J. Kim and L. Tong. On phasor measurement unit placement against state and topology attacks. In *Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on*, pages 396–401, October 2013.

[KT13b] J. Kim and L. Tong. On topology attack of a smart grid. In *Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES*, pages 1–6, February 2013.

[KT13c] J. Kim and L. Tong. On topology attack of a smart grid: Undetectable attacks and countermeasures. *Selected Areas in Communications, IEEE Journal on*, 31(7):1294–1305, July 2013.

[KTD14] Efstathios Kontouras, Anthony Tzes, and Leonidas Dritsas. Adversary control strategies for discrete-time systems. In *Control Conference (ECC), 2014 European*, pages 2508–2513. IEEE, 2014.

[KTD15] Efstathios Kontouras, Anthony Tzes, and Leonidas Dritsas. Covert attack on a discrete-time system with limited use of the available disruption resources. In *Control Conference (ECC), 2015 European*, pages 812–817. IEEE, 2015.

[KTT13] J. Kim, L. Tong, and R.J. Thomas. Data framing attack on state estimation with unknown network parameters. In *Signals, Systems and Computers, 2013 Asilomar Conference on*, pages 1388–1392, November 2013.

[KTT14a] J. Kim, L. Tong, and R.J. Thomas. Data framing attack on state estimation. *Selected Areas in Communications, IEEE Journal on*, 32(7):1460–1470, July 2014.

[KTT14b] J. Kim, L. Tong, and R.J. Thomas. Dynamic attacks on power systems economic dispatch. In *The 48th Asilomar Conference on Signals, Systems, and Computers*, November 2014.

[KWG+12] A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge. Cyber attack vulnerabilities analysis for unmanned aerial vehicles. In *Infotech@Aerospace 2012*. American Institute of Aeronautics and Astronautics, 2012.

[KYH15] Cheolhyeon Kwon, Scott Yantek, and Inseok Hwang. Real-time safety assessment of unmanned aircraft systems against stealthy cyber attacks. *Journal of Aerospace Information Systems*, 13(1):27–45, 2015.

[LALH15] Rongxing Lu, Khalid Alharbi, Xiaodong Lin, and Cheng Huang. A novel privacy-preserving set aggregation scheme for smart grid communications. In *Global Communications Conference (GLOBECOM), 2015 IEEE*, pages 1–6. IEEE, 2015.

[LAP12] Y.W. Law, T. Alpcan, and M. Palaniswami. Security games for voltage control in smart grid. In *Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on*, pages 212–219, October 2012.

[LAPD12] Y.W. Law, T. Alpcan, M. Palaniswami, and S. Dey. Security games and risk minimization for automatic generation control in smart grid. In J. Grossklags and J. Walrand, editors, *Decision and Game Theory for Security*, volume 7638 of *Lecture Notes in Computer Science*, pages 281–295. Springer Berlin Heidelberg, 2012.

[LBLL15] X. Liu, Z. Bao, D. Lu, and Z. Li. Modeling of local false data injection attacks with reduced network information. *Smart Grid, IEEE Transactions on*, 6(4):1686–1696, July 2015.

[LCCY13] H. Liu, Y. Chen, M.C. Chuah, and J. Yang. Towards self-healing smart grid via intelligent local controller switching under jamming. In *Communications and Network Security (CNS), 2013 IEEE Conference on*, pages 127–135, October 2013.

[LCH+14] Hao Liu, Xianghui Cao, Jianping He, Peng Cheng, Jiming Chen, and Youxian Sun. Distributed identification of the most critical node for average consensus. *IFAC Proceedings Volumes*, 47(3):1843–1848, 2014.

[LCH+15] H. Liu, X. Cao, J. He, P. Cheng, C. Li, J. Chen, and Y. Sun. Distributed identification of the most critical node for average consensus. *IEEE Transactions on Signal Processing*, 63(16):4315–4328, Aug 2015.

[LDZ+15] Fengji Luo, Zhao Yang Dong, Junhua Zhao, Xin Zhang, Weicong Kong, and Yingying Chen. Enabling the big data analysis in the smart grid. In *Power & Energy Society General Meeting, 2015 IEEE*, pages 1–5. IEEE, 2015.

[LED+14] L. Liu, M. Esmalifalak, Q. Ding, V.A. Emesih, and Z. Han. Detecting false data injection attacks on power grid by sparse optimization. *Smart Grid, IEEE Transactions on*, 5(2):612–621, March 2014.

[LEH13] L. Liu, M. Esmalifalak, and Z. Han. Detection of false data injection in power grid exploiting low rank and sparsity. In *Communications (ICC), 2013 IEEE International Conference on*, pages 4461–4465, June 2013.

[LFC15] Yan Li, Hao Fang, and Jie Chen. Communication-based fault detection and isolation for multi-agent systems. In *Control Conference (ASCC), 2015 10th Asian*, pages 1–5. IEEE, 2015.

[LGW+13] T. Liu, Y. Gu, D. Wang, Y. Gui, and X. Guan. A novel method to detect bad data injection attack in smart grid. In *INFOCOM, 2013 Proceedings IEEE*, pages 3423–3428, April 2013.

[LH11] H. Li and Z. Han. Manipulating the electricity power market via jamming the price signaling in smart grid. In *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, pages 1168–1172, December 2011.

[LHX+15] Guoqi Li, Wuhua Hu, Gaoxi Xiao, Lei Deng, Pei Tang, Jing Pei, and Luping Shi. Minimum-cost control of complex networks. *New Journal of Physics*, 18(1):013012, 2015.

[Lia15] Jingwen Liang. *Consequences of false data injection on power system state estimation*. PhD thesis, Arizona State University, 2015.

[Liu15] Lanchao Liu. *Big Data Optimization for Modern Communication Networks*. PhD thesis, University of Houston, 2015.

[LK14] D. Lee and D. Kundur. Cyber attack detection in PMU measurements via the expectation-maximization algorithm. In *Signal and Information Processing (GlobalSIP), 2014 IEEE Global Conference on*, pages 223–227, December 2014.

[LKAH12] W. Liu, C. Kwon, I. Aljanabi, and I. Hwang. Cyber security analysis for state estimators in air traffic control systems. In *AIAA Conference on Guidance, Navigation, and Control*. American Institute of Aeronautics and Astronautics, 2012.

[LKS14] J. Liang, O. Kosut, and L. Sankar. Cyber attacks on AC state estimation: Unobservability and physical consequences. In *PES General Meeting — Conference Exposition, 2014 IEEE*, pages 1–5, July 2014.

[LL14] X. Liu and Z. Li. Local load redistribution attacks in power systems with incomplete network information. *Smart Grid, IEEE Transactions on*, 5(4):1665–1676, July 2014.

[LLD11] H. Li, L. Lai, and S.M. Djouadi. Combating false reports for secure networked control in smart grid via trustiness evaluation. In *Communications (ICC), 2011 IEEE International Conference on*, pages 1–5, June 2011.

[LLE13a] S. Liu, P.X. Liu, and A. El Saddik. A stochastic security game for Kalman filtering in networked control systems under Denial of Service (DoS) attacks. *Intelligent Control and Automation Science*, 3(1):106–111, 2013.

[LLE13b] S. Liu, X.P. Liu, and A. El Saddik. Denial-of-Service (DoS) attacks on load frequency control in smart grids. In *Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES*, pages 1–6, February 2013.

[LLL15] Xuan Liu, Xingdong Liu, and Zuyi Li. Cyber risk assessment of transmission lines in smart grids. *Energies*, 8(12):13796–13810, 2015.

[LLQ10] H. Li, L. Lai, and R.C. Qiu. Communication capacity requirement for reliable and secure state estimation in smart grid. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 191–196, October 2010.

[LLQ11] Husheng Li, Lifeng Lai, and R. C. Qiu. A denial-of-service jamming game for remote state monitoring in smart grid. In *2011 45th Annual Conference on Information Sciences and Systems*, pages 1–6, March 2011.

[LLWW10] Z. Lu, X. Lu, W. Wang, and C. Wang. Review and evaluation of security threats on the communication networks in the smart grid. In *Military Communications Conference, 2010 - MILCOM 2010*, pages 1830–1835, October 2010.

[LLZ+14] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen. An efficient merkle-tree-based authentication scheme for smart grid. *Systems Journal, IEEE*, 8(2):655–663, June 2014.

[LM15] Jônatas Boás Leite and José Roberto Sanches Mantovani. Development of a smart grid simulation environment, part i: project of the electrical devices simulator. *Journal of Control, Automation and Electrical Systems*, 26(1):80–95, 2015.

[LMB+15] Jordan Landford, Rich Meier, Richard Barella, Xinghui Zhao, Eduardo Cotilla-Sanchez, Robert B Bass, and Scott Wallace. Fast sequence component analysis for attack detection in synchrophasor networks. *arXiv preprint arXiv:1509.05086*, 2015.

[LMD+15] Long Liu, Jin Ma, Zhaoyang Dong, Guo Chen, and Kit Po Wong. Influence of enhanced interconnecting links on cascading failures in smart grid. In *Power & Energy Society General Meeting, 2015 IEEE*, pages 1–5. IEEE, 2015.

[LMO+15] Guo Longhua, Dong Mianxiong, Kaoru Ota, Wu Jun, and Li Jianhua. Event-oriented dynamic security service for demand response in smart grid employing mobile networks. *China Communications*, 12(12):63–75, 2015.

[LN08] Ulf E. Larson and Dennis K. Nilsson. Securing vehicles against cyber attacks. In *Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead*, page 30. ACM, 2008.

[LN14] J. Lu and R. Niu. False information injection attack on dynamic state estimation in multi-sensor systems. In *Information Fusion (FUSION), 2014 17th International Conference on*, pages 1–8, July 2014.

[LN15a] Huan Aaron Li and Nirmal-Kumar C Nair. Multi-agent systems and demand response: A systematic review. In *Power Engineering Conference (AUPEC), 2015 Australasian Universities*, pages 1–6. IEEE, 2015.

[LN15b] J. Lu and R. Niu. A state estimation and malicious attack game in multi-sensor dynamic systems. *arXiv preprint arXiv:1502.03531*, 2015.

[LNR09] Y. Liu, P. Ning, and M.K. Reiter. False data injection attacks against state estimation in electric power grids. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 21–32, New York, NY, USA, 2009. ACM.

[LNR11] Y. Liu, P. Ning, and M.K. Reiter. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.*, 14(1):13:1–13:33, May 2011.

[LOCL10] Shinyoung Lim, Tae Hwan Oh, Young B. Choi, and Tamil Lakshman. Security issues on wireless body area network for remote healthcare monitoring. In *Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010 IEEE International Conference on*, pages 327–332. IEEE, 2010.

[Lou15] George Loukas. *Cyber-physical attacks: A growing invisible threat*. Butterworth-Heinemann, 2015.

[LP12] J. Le Ny and G.J. Pappas. Differentially private Kalman filtering. In *Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on*, pages 1618–1625, October 2012.

[LP14] J. Le Ny and G.J. Pappas. Differentially private filtering. *Automatic Control, IEEE Transactions on*, 59(2):341–354, February 2014.

[LPK+15] Xiaofei Liu, Sergio Pequito, Soummya Kar, Bruno Sinopoli, and A Pedro Aguiar. Minimum sensor placement for robust observability of structured complex networks. *arXiv preprint arXiv:1507.07205*, 2015.

[LQDS15] Y. Li, D. E. Quevedo, S. Dey, and L. Shi. Fake-acknowledgment attack on ACK-based sensor power schedule for remote state estimation. In *2015 54th IEEE Conference on Decision and Control (CDC)*, pages 5795–5800, Dec 2015.

[LRJ11] C. Li, A. Raghunathan, and N.K. Jha. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on*, pages 150–156, June 2011.

[LSC+15a] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo. Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. *IEEE Transactions on Automatic Control*, 60(10):2831–2836, Oct 2015.

[LSC+15b] Xindong Liu, Mohammad Shahidehpour, Yijia Cao, Zuyi Li, and Wei Tian. Risk assessment in extreme events considering the reliability of protection systems. *IEEE Transactions on Smart Grid*, 6(2):1073–1081, 2015.

[LSE15] Chanhwa Lee, Hyungbo Shim, and Yongsoon Eun. Secure and robust state estimation under sensor attacks, measurement noises, and process disturbances: Observer-based combinatorial approach. In *Control Conference (ECC), 2015 European*, pages 1872–1877. IEEE, 2015.

[LSHP12] Chen-Ching Liu, Alexandru Stefanov, Junho Hong, and Patrick Panciatici. Intruders in the grid. *IEEE Power and Energy magazine*, 10(1):58–66, 2012.

[LSK+13] H. Lin, A. Slagell, Z. Kalbarczyk, P.W. Sauer, and R.K. Iyer. Semantic security analysis of scada networks to detect malicious control commands in power grids. In *Proceedings of the First ACM Workshop on Smart Energy Grid Security*, SEGS '13, pages 29–34, New York, NY, USA, 2013. ACM.

[LSM13] P. Loh, G. Sabaliauskaite, and A. Mathur. Detecting injection attacks in linear time invariant systems. In *Cybernetics and Intelligent Systems (CIS), IEEE Conference on*, pages 84–89, November 2013.

[LSS+13] B. Lamas, A. Soury, B. Saadallah, A. Lahmadi, and O. Festor. An experimental testbed and methodology for security analysis of SCADA systems. Technical Report RT-0443, INRIA Nancy, 2013.

[LSSH15] Carlos Lopez, Arman Sargolzaei, Hugo Santana, and Carlos Huerta. Smart grid cyber security: an overview of threats and countermeasures. *Journal of Energy and Power Engineering*, 9:632–647, 2015.

[LTJ11] M.B. Line, I.A. Tøndel, and M.G. Jaatun. Cyber security challenges in smart grids. In *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on*, pages 1–8, Decembe 2011.

[LTM09] C.-C. Liu, C.-W. Ten, and G. Manimaran. Cybersecurity of SCADA systems: Vulnerability assessment and mitigation. In *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*, pages 1–3, March 2009.

[LTRC+15] Germano Lambert-Torres, Ronaldo Rossi, Maurilio Pereira Coutinho, Carlos Henrique Valerio de Moraes, and Luiz Eduardo Borges da Silva. Some discussions about data in the new environment of power systems. In *Power & Energy Society General Meeting, 2015 IEEE*, pages 1–5. IEEE, 2015.

[LVD14] Y. Li, H. Voos, and M. Darouach. Robust H_∞ cyber-attacks estimation for control systems. In *Control Conference (CCC), 2014 33rd Chinese*, pages 3124–3129, July 2014.

[LVDH15a] Yumei Li, Holger Voos, Mohamed Darouach, and Changchun Hua. An algebraic detection approach for control systems under multiple stochastic cyber-attacks. *IEEE/CAA Journal of Automatica Sinica*, 2(3):258–266, 2015.

[LVDH15b] Yumei Li, Holger Voos, Mohamed Darouach, and Changchun Hua. An application of linear algebra theory in networked control systems: stochastic cyber-attacks detection approach. *IMA Journal of Mathematical Control and Information*, 33(4):1081–1102, 2015.

[LVP+15] Yumei Li, Holger Voos, Lin Pan, Mohamed Darouach, and Changchun Hua. Stochastic cyber-attacks estimation for nonlinear control systems based on robust H_∞ filtering technique. In *Control and Decision Conference (CCDC), 2015 27th Chinese*, pages 5590–5595. IEEE, 2015.

[LVRD14] Y. Li, H. Voos, A. Rosich, and M. Darouach. A stochastic cyber-attack detection scheme for stochastic control systems based on frequency-domain transformation technique. In M.H. Au, B. Carminati, and C.-C.J. Kuo, editors, *Network and System Security*, volume 8792 of *Lecture Notes in Computer Science*, pages 209–222. Springer International Publishing, 2014.

[LW14] Y. Li and Y. Wang. State summation for detecting false data attack on smart grid. *International Journal of Electrical Power & Energy Systems*, 57(0):156–163, 2014.

[LWH05] M. Long, C.-H.J. Wu, and J.Y. Hung. Denial of service attacks on network-based control systems: impact and mitigation. *Industrial Informatics, IEEE Transactions on*, 1(2):85–96, May 2005.

[LWLL15] Xiaoqin Li, Jing Wu, Chengnian Long, and Shaoyuan Li. A novel decomposition of power systems for PMU placement. In *Control Conference (CCC), 2015 34th Chinese*, pages 8975–8980. IEEE, 2015.

[LWW+12] Y. Li, R. Wang, P. Wang, D. Niyato, W. Saad, and Z. Han. Resilient PHEV charging policies under price information attacks. In *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, pages 389–394. IEEE, November 2012.

[LWW+15] Yuqiang Luo, Zidong Wang, Guoliang Wei, Bo Shen, Xiao He, Hongli Dong, and Jun Hu. Fuzzy-logic-based control, filtering, and fault detection for networked systems: a survey. *Mathematical Problems in Engineering*, 2015, 2015.

[LXL+12] J. Liu, Y. Xiao, S. Li, W. Liang, and C.L.P. Chen. Cyber security and privacy issues in smart grids. *Communications Surveys Tutorials, IEEE*, 14(4):981–997, Fourth 2012.

[Lyn15] Kevin G Lyn. *Classification of and resilience to cyber-attacks on cyber-physical systems*. PhD thesis, Georgia Institute of Technology, 2015.

[LYRS14] Y. Liu, L. Yan, J.-W. Ren, and D. Su. Research on efficient detection methods for false data injection in smart grid. In *Wireless Communication and Sensor Network (WCSN), 2014 International Conference on*, pages 188–192, December 2014.

[LYW15a] S. Li, Y. Yilmaz, and X. Wang. Quickest detection of false data injection attack in wide-area smart grids. *Smart Grid, IEEE Transactions on*, 6(6):2725–2735, November 2015.

[LYW15b] Shang Li, Yasin Yilmaz, and Xiaodong Wang. Sequential cyber-attack detection in the large-scale smart grid system. In *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, pages 127–132. IEEE, 2015.

[LYY13] J. Lin, W. Yu, and X. Yang. On false data injection attack against multistep electricity price in electricity market in smart grid. In *Global Communications Conference (GLOBECOM), 2013 IEEE*, pages 760–765, December 2013.

[LZ15] Zili Li and Li Zeng. A hybrid vertex outlier detection method based on distributed representation and local outlier factor. In *Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), 2015 IEEE 12th Intl Conf on*, pages 512–516. IEEE, 2015.

[LZZ+15] T. Lu, J. Zhao, L. Zhao, Y. Li, and X. Zhang. Towards a framework for assuring cyber physical system security. *SERSC International Journal of Security and Its Applications*, 9(3):25–40, 2015.

[MA15] Thulasi Mylvaganam and Alessandro Astolfi. Control of microgrids using a differential game theoretic framework. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages 5839–5844. IEEE, 2015.

[MAG05] A.L. Motto, J.M. Arroyo, and F.D. Galiana. A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat. *Power Systems, IEEE Transactions on*, 20(3):1357–1365, August 2005.

[Man15] Kebina Manandhar. *Enhanching Security in the Future Cyber Physical Systems*. PhD thesis, Georgia State University, 2015.

[MB09] M.A. McQueen and W.F. Boyer. Deception used for cyber defense of control systems. In *Proceedings of the 2nd conference on Human System Interactions, HSI*, volume 9, 2009.

[MB15] Jun Moon and Tamer Başar. Minimax control over unreliable communication channels. *Automatica*, 59:182–193, 2015.

[MBFB06] M.A. McQueen, W.F. Boyer, M.A. Flynn, and G.A. Beitel. Quantitative cyber risk reduction estimation methodology for a small SCADA control system. In *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on*, volume 9, pages 226–226, Jan 2006.

[MBS12] I. Matei, J.S. Baras, and V. Srinivasan. Trust-based multi-agent filtering for increased smart grid security. In *Control Automation (MED), 2012 20th Mediterranean Conference on*, pages 716–721, July 2012.

[MC14a] K. Manandhar and X. Cao. Attacks/faults detection and isolation in the smart grid using Kalman filter. In *Computer Communication and Networks (ICCCN), 2014 23rd International Conference on*, pages 1–6, August 2014.

[MC14b] R. Mitchell and I.-R. Chen. Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. *Systems, Man, and Cybernetics: Systems, IEEE Transactions on*, 44(5):593–604, May 2014.

[MC14c] Robert Mitchell and Ray Chen. Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 44(5):593–604, 2014.

[MCH12] K. Manandhar, X. Cao, and F. Hu. Attack detection in water supply systems using kalman filter estimator. In *Sarnoff Symposium (SARNOFF), 2012 35th IEEE*, pages 1–6, May 2012.

[MCHL14] K. Manandhar, X. Cao, F. Hu, and Y. Liu. Combating false data injection attacks in smart grid using Kalman filter. In *Computing, Networking and Communications (ICNC), 2014 International Conference on*, pages 16–20, February 2014.

[ME10a] A.R. Metke and R.L. Ekl. Security technology for smart grid networks. *Smart Grid, IEEE Transactions on*, 1(1):99–107, June 2010.

[ME10b] A.R. Metke and R.L. Ekl. Smart grid security technology. In *Innovative Smart Grid Technologies (ISGT), 2010*, pages 1–7, January 2010.

[MFJ+10] Z. Mohajerani, F. Farzan, M. Jafary, Y. Lu, D. Wei, N. Kalenchits, B. Boyer, M. Muller, and P. Skare. Cyber-related risk assessment and critical asset identification within the power grid. In *Transmission and Distribution Conference and Exposition, 2010 IEEE PES*, pages 1–4, April 2010.

[MFK+15] Kieran McLaughlin, Ivo Friedberg, BooJoong Kang, Peter Maynard, Sakir Sezer, and Gavin McWilliams. Secure communications in smart grid: Networking and protocols. In *Smart Grid Security*, pages 113–148. Elsevier, 2015.

[MFL+13] A.M. Melin, E.M. Ferragut, J.A. Laska, D.L. Fugate, and R. Kisner. A mathematical framework for the analysis of cyber-resilient control systems. In *Resilient Control Systems (ISRCS), 2013 6th International Symposium on*, pages 13–18, August 2013.

[MG13] T.H. Morris and W. Gao. Industrial control system cyber attacks. In *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research*, page 22, 2013.

[MGCS10] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli. False data injection attacks against state estimation in wireless sensor networks. In *Decision and Control (CDC), 2010 49th IEEE Conference on*, pages 5967–5972, December 2010.

[MHR+12] K.L. Morrow, E. Heine, K.M. Rogers, R.B. Bobba, and T.J. Overbye. Topology perturbation for detecting malicious data injection. In *System Science (HICSS), 2012 45th Hawaii International Conference on*, pages 2104–2113, January 2012.

[MHS14] Y. Mo, J.P. Hespanha, and B. Sinopoli. Resilient detection in the presence of integrity attacks. *Signal Processing, IEEE Transactions on*, 62(1):31–43, January 2014.

[MK09] Nader Meskin and Khashayar Khorasani. Actuator fault detection and isolation for a network of unmanned vehicles. *IEEE Transactions on Automatic Control*, 54(4):835–840, 2009.

[MKFM12] A. Melin, R. Kisner, D. Fugate, and T. McIntyre. Minimum state awareness for resilient control systems under cyber-attack. In *Future of Instrumentation International Workshop (FIIW), 2012*, pages 1–4, October 2012.

[ML11] A.-H. Mohsenian-Rad and A. Leon-Garcia. Distributed internet-based load altering attacks against smart power grids. *Smart Grid, IEEE Transactions on*, 2(4):667–674, December 2011.

[MLF+15] H Alan Mantooth, Yusi Liu, Chris Farnell, Fengli Zhang, Qinghua Li, and Jia Di. Securing DC and hybrid microgrids. In *DC Microgrids (ICDCM), 2015 IEEE First International Conference on*, pages 285–286c. IEEE, 2015.

[MLK+15] Subhankar Mishra, Xiang Li, Alan Kuhnle, My T Thai, and Jungtaek Seo. Rate alteration attacks in smart grid. In *Computer Communications (INFOCOM), 2015 IEEE Conference on*, pages 2353–2361. IEEE, 2015.

[MLSH15] J. Ma, Y. Liu, L. Song, and Z. Han. Multiact dynamic game strategy for jamming attack in electricity market. *Smart Grid, IEEE Transactions on*, PP(99):1–1, 2015.

[MLX15] H Mo, B Liu, and X Xiao. Importance measures for control systems with degrading components. In *Industrial Engineering and Engineering Management (IEEM), 2015 IEEE International Conference on*, pages 772–776. IEEE, 2015.

[MM12] P. McDaniel and S. McLaughlin. Structured security testing in the smart grid. In *Communications Control and Signal Processing (ISCCSP), 2012 5th International Symposium on*, pages 1–4, May 2012.

[MM15] Y. Mo and R.M. Murray. Multi-dimensional state estimation in adversarial environment. In *2015 IEEE 34th Chinese Control Conference (CCC)*, July 2015.

[MMA11] S. McLaughlin, P. McDaniel, and W. Aiello. Protecting consumer privacy from electric load monitoring. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, pages 87–98, New York, NY, USA, 2011. ACM.

[MMS13] W.A. Malik, N.C. Martins, and A. Swami. LQ control under security constraints. In D.C. Tarraf, editor, *Control of Cyber-Physical Systems*, volume 449 of *Lecture Notes in Control and Information Sciences*, pages 101–120. Springer International Publishing, 2013.

[MMY15] Sriharsha Mallapuram, Paul Moulema, and Wei Yu. On a simulation study for reliable and secured smart grid communications. In *Cyber Sensing 2015*, volume 9458, page 945808. International Society for Optics and Photonics, 2015.

[Moo15] Jun Moon. *Control and estimation with limited information: A game-theoretic approach*. PhD thesis, University of Illinois at Urbana-Champaign, 2015.

[MP13] T. Mehra and R.K. Pateriya. Cyber security considerations for advanced metering infrastructure in smart grid. *International Journal of Scientific & Engineering Research*, 4(8):939–944, August 2013.

[MPM10] S. McLaughlin, D. Podkuiko, and P. McDaniel. Energy theft in the advanced metering infrastructure. In E. Rome and R. Bloomfield, editors, *Critical Information Infrastructures Security*, volume 6027 of *Lecture Notes in Computer Science*, pages 176–187. Springer Berlin Heidelberg, 2010.

[MPP13] F. Miao, M. Pajic, and G.J. Pappas. Stochastic game approach for replay attack detection. In *Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on*, pages 1854–1859, December 2013.

[MRP+15] Patrizio Manganiello, Mattia Ricco, Giovanni Petrone, Eric Monmasson, and Giovanni Spagnuolo. Dual-Kalman-filter-based identification and real-time optimization of PV systems. *IEEE Transactions on Industrial Electronics*, 62(11):7266–7275, 2015.

[MS09] Y. Mo and B. Sinopoli. Secure control against replay attacks. In *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, pages 911–918, September 2009.

[MS10] Y. Mo and B. Sinopoli. False data injection attacks in control systems. In *Preprints of the 1st workshop on Secure Control Systems, CPSWEEK 2010*, April 2010.

[MS13] Y. Mo and B. Sinopoli. Robust estimation in the presence of integrity attacks. In *Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on*, pages 6085–6090, December 2013.

[MS15] Y. Mo and B. Sinopoli. Secure estimation in the presence of integrity attacks. *Automatic Control, IEEE Transactions on*, 60(4):1145–1151, April 2015.

[MSK+15] S. Mishra, Y. Shoukry, N. Karamchandani, S. Diggavi, and P. Tabuada. Secure state estimation: Optimal guarantees against sensor attacks in the presence of noise. In *2015 IEEE International Symposium on Information Theory (ISIT)*, June 2015.

[MSM15] Sindhuja Mangalwedekar, Sunil K Surve, and HA Mangalvedekar. False data injection attacks and detection scenarios in the power system. In *India Conference (INDICON), 2015 Annual IEEE*, pages 1–6. IEEE, 2015.

[MSSFM15] Angelos K Marnerides, Paul Smith, Alberto Schaeffer-Filho, and Andreas Mauthe. Power consumption profiling using energy time-frequency distributions in smart grids. *IEEE Communications Letters*, 19(1):46–49, 2015.

[MVW13] S. Mousavian, J. Valenzuela, and J. Wang. Real-time data reassurance in electrical power systems based on artificial neural networks. *Electric Power Systems Research*, 96:285–295, 2013.

[MVW15] S. Mousavian, J. Valenzuela, and J. Wang. A probabilistic risk mitigation model for cyber-attacks to PMU networks. *Power Systems, IEEE Transactions on*, 30(1):156–165, January 2015.

[MYK+13] T Morita, Shuichi Yogo, Masato Koike, Takashi Hamaguchi, S Jung, Ichiro Koshijima, and Yoshihiro Hashimoto. Detection of cyber-attacks with zone dividing and PCA. *Procedia Computer Science*, 22:727–736, 2013.

[MYLR13] C.Y.T. Ma, D.K.Y. Yau, X. Lou, and N.S.V. Rao. Markov game analysis for attack-defense of power networks under possible misinformation. *Power Systems, IEEE Transactions on*, 28(2):1676–1686, May 2013.

[MZ14] S. McLaughlin and S. Zonouz. Controller-aware false data injection against programmable logic controllers. In *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, pages 848–853, November 2014.

[MZG+15] Sabita Maharjan, Yan Zhang, Stein Gjessing, Oystein Ulleberg, and Frank Eliassen. Providing microgrid resilience during emergencies using distributed energy resources. In *Globecom Workshops (GC Wkshps), 2015 IEEE*, pages 1–6. IEEE, 2015.

[MZPP14] F. Miao, Q. Zhu, M. Pajic, and G.J. Pappas. Coding sensor outputs for injection attacks detection. In *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*, pages 5776–5781, December 2014.

[NAB08] Kien C Nguyen, Tansu Alpcan, and Tamer Başar. A decentralized Bayesian attack detection algorithm for network security. In *IFIP International Information Security Conference*, pages 413–428. Springer, 2008.

[Nab15] Seyedbehzad Nabavi. *Measurement-Based Methods for Model Reduction, Identification, and Distributed Optimization of Power Systems*. PhD thesis, North Carolina State University, 2015.

[NAH15] Ziaeddin Najafian, Vahe Aghazarian, and Alireza Hedayati. Signature-based method and stream data mining technique performance evaluation for security and intrusion detection in advanced metering infrastructures (ami). *International Journal of Computer and Electrical Engineering*, 7(2):128, 2015.

[NBSS13] W. Niemira, R.B. Bobba, P. Sauer, and W.H. Sanders. Malicious data detection in state estimation leveraging system losses & estimation of perturbed parameters. In *Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on*, pages 402–407, October 2013.

[NC15] Seyedbehzad Nabavi and Aranya Chakrabortty. An intrusion-resilient distributed optimization algorithm for modal estimation in power systems. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages 39–44. IEEE, 2015.

[NG10] T. Novak and A. Gerstinger. Safety- and security-critical services in building automation and control systems. *Industrial Electronics, IEEE Transactions on*, 57(11):3614–3621, November 2010.

[NH12] R. Niu and L. Huie. System state estimation in the presence of false information injection. In *Statistical Signal Processing Workshop (SSP), 2012 IEEE*, pages 385–388, August 2012.

[NI14] H. Nishino and H. Ishii. Distributed detection of cyber attacks and faults for power systems. In *Proceedings of the 19th IFAC World Congress*, August 2014.

[NJ15a] Haifeng Niu and S Jagannathan. Optimal defense and control of dynamic systems modeled as cyber-physical systems. *The Journal of Defense Modeling and Simulation*, 12(4):423–438, 2015.

[NJ15b] Haifeng Niu and Sarangapani Jagannathan. Optimal defense and control for cyber-physical systems. In *Computational Intelligence, 2015 IEEE Symposium Series on*, pages 634–639, December 2015.

[NL15] R. Niu and J. Lu. False information detection with minimum mean squared errors for Bayesian estimation. In *Information Sciences and Systems (CISS), 2015 49th Annual Conference on*, pages 1–6, March 2015.

[NM15a] Yorie Nakahira and Yilin Mo. Dynamic state estimation in the presence of compromised sensory data. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages 5808–5813. IEEE, 2015.

[NM15b] Arash Nourian and Stuart Madnick. A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet. *IEEE Transactions on Dependable and Secure Computing*, 2015.

[NNC15] T.R. Nudell, S. Nabavi, and A. Chakrabortty. A real-time attack localization algorithm for large power system networks using graph-theoretic techniques. *Smart Grid, IEEE Transactions on*, 6(5):2551–2559, Sept 2015.

[NPA+12] J. Nutaro, I. Patterson, G. Allgood, T. Kuruganti, and D. Fugate. A method for engineering secure control systems with application to critical infrastructures. In *Proceedings of the 2012 International Conference on Security & Management (SAM 2012)*, pages 145–149, 2012.

[NPYG09] M. Negrete-Pincetic, F. Yoshida, and G. Gross. Towards quantifying the impacts of cyber attacks in the competitive electricity market environment. In *PowerTech, 2009 IEEE Bucharest*, pages 1–8, June 2009.

[NS15] Stavros Ntalampiras and Yannis Soupionis. Detection of integrity attacks in cyper physical systems based on reservoir networks. *Entropy*, 20:2, 2015.

[Nud15] Thomas R. Nudell. *Graph-Theoretic Algorithms for Monitoring and Control of Large Networked Dynamic Systems*. PhD thesis, North Carolina State University, 2015.

[Nuz15] Pierluigi Nuzzo. *Compositional design of cyber-physical systems using contracts*. PhD thesis, EECS Department, University of California, Berkeley, 2015.

[OEV+13] M. Ozay, I. Esnaola, F.T.Y. Vural, S.R. Kulkarni, and H.V. Poor. Sparse attack construction and state estimation in the smart grid: Centralized and distributed models. *Selected Areas in Communications, IEEE Journal on*, 31(7):1306–1318, July 2013.

[OEY+12] M. Ozay, I. Esnaola, F.T. Yarman Vural, S.R. Kulkarni, and H.V. Poor. Distributed models for sparse attack construction and state vector estimation in the smart grid. In *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, pages 306–311, November 2012.

[OEY+15] M. Ozay, I. Esnaola, F.T. Yarman Vural, S.R. Kulkarni, and H.V. Poor. Machine learning methods for attack detection in the smart grid. *Neural Networks and Learning Systems, IEEE Transactions on*, PP(99):1–1, 2015.

[OEYV+12] M. Ozay, I. Esnaola, F.T. Yarman Vural, S.R. Kulkarni, and H.V. Poor. Smarter security in the smart grid. In *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, pages 312–317, November 2012.

[Oni12] Hiro Onishi. Paradigm change of vehicle cyber security. In *Cyber Conflict (CYCON), 2012 4th International Conference on*, pages 1–11. IEEE, 2012.

[Par15] Pangun Park. Optimized medium access probability for networked control systems. *Journal of the Korea Institute of Information and Communication Engineering*, 19(10):2457–2464, 2015.

[PB14] Kalana Pothuwila and Jordan M Berg. Qualitative behavioral analyzer for fault detection and cyber security of control networks. In *ASME 2014 Dynamic Systems and Control Conference*, pages V002T26A005–V002T26A005. American Society of Mechanical Engineers, 2014.

[PBB07] Fabio Pasqualetti, Antonio Bicchi, and Francesco Bullo. Distributed intrusion detection for secure consensus computations. In *Decision and Control, 2007 46th IEEE Conference on*, pages 5594–5599. IEEE, 2007.

[PBB11] F. Pasqualetti, A. Bicchi, and F. Bullo. A graph-theoretical characterization of power network vulnerabilities. In *American Control Conference (ACC), 2011*, pages 3918–3923, June 2011.

[PBB12] Fabio Pasqualetti, Antonio Bicchi, and Francesco Bullo. Consensus computation in unreliable networks: A system theoretic approach. *IEEE Transactions on Automatic Control*, 57(1):90–104, 2012.

[PCB11] F. Pasqualetti, R. Carli, and F. Bullo. A distributed method for state estimation and false data detection in power networks. In *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, pages 469–474, October 2011.

[PCBB10] F. Pasqualetti, R. Carli, A. Bicchi, and F. Bullo. Identifying cyber attacks via local model information. In *Decision and Control (CDC), 2010 49th IEEE Conference on*, pages 5961–5966, December 2010.

[Pei15] S Peisert. ASCR cybersecurity for scientific computing integrity. DOE Workshop report, 2015.

[PFG15] Héctor Poveda, Guillaume Ferré, and Eric Grivel. Way to design an orthogonal frequency-division multiple access-base station receiver disturbed by a narrowband interfering cognitive radio signal. *IET Communications*, 9(12):1547–1554, 2015.

[PFMM08] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson. Systematic mapping studies in software engineering. In *Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering*, EASE'08, pages 68–77, Swinton, UK, UK, 2008. British Computer Society.

[PK12] S. Parthasarathy and D. Kundur. Bloom filter based intrusion detection for smart grid SCADA. In *Electrical Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference on*, pages 1–6, April 2012.

[PKM+14] M. Parvania, G. Koutsandria, V. Muthukumary, S. Peisert, C. McParland, and A. Scaglione. Hybrid control network intrusion detection systems for automated power distribution systems. In *Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on*, pages 774–779, June 2014.

[PLD11] Z.-H. Pang, G.P. Liu, and Z. Dong. Secure networked control systems under denial of service attacks. In *18th IFAC World Congress*, 2011.

[PLR07] Tao Peng, Christopher Leckie, and Kotagiri Ramamohanarao. Information sharing for distributed intrusion detection systems. *Journal of Network and Computer Applications*, 30(3):877–899, 2007.

[PLSH15] Erte Pan, Husheng Li, Lingyang Song, and Zhu Han. Kernel-based non-parametric clustering for load profiling of big smart meter data. In *Wireless Communications and Networking Conference (WCNC), 2015 IEEE*, pages 2251–2255. IEEE, 2015.

[PMA15a] S. Pan, T. Morris, and U. Adhikari. Developing a hybrid intrusion detection system using data mining for power systems. *Smart Grid, IEEE Transactions on*, PP(99):1–1, 2015.

[PMA15b] Shengyi Pan, Thomas H Morris, and Uttam Adhikari. A specification-based intrusion detection framework for cyber-physical environment in electric power system. *IJ Network Security*, 17(2):174–188, 2015.

[PMDL10] A. Pinar, J. Meza, V. Donde, and B. Lesieutre. Optimization strategies for the vulnerability analysis of the electric power grid. *SIAM Journal on Optimization*, 20(4):1786–1810, 2010.

[PNZL13] Y. Park, D.M. Nicol, H. Zhu, and C.W. Lee. Prevention of malware propagation in AMI. In *Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on*, pages 474–479, October 2013.

[PPM+15] Neha Pande, Vipul Pagrut, Ragini Meshram, Faruk Kazi, Navdeep Singh, and Sushama Wagh. Real time distributed control of variable speed drive system in cyber physical framework. *IFAC-PapersOnLine*, 48(30):357–362, 2015.

[PR+14] Yudha Purwanto, Budi Rahardjo, et al. Traffic anomaly detection in ddos flooding attack. In *Telecommunication Systems Services and Applications (TSSA), 2014 8th International Conference on*, pages 1–6. IEEE, 2014.

[PR15] Stephane Paul and Laurent Rioux. Over 20 years of research in cybersecurity and safety engineering: a short bibliography. In *6th International Conference on Safety and Security Engineering (SAFE)*, 2015.

[PS14] S. Pal and B. Sikdar. A mechanism for detecting data manipulation attacks on PMU data. In *Communication Systems (ICCS), 2014 IEEE International Conference on*, pages 253–257, November 2014.

[PSC+14] N. Papakonstantinou, S. Sierla, K. Charitoudi, B. O'Halloran, T. Karhela, V. Vyatkin, and I. Turner. Security impact assessment of industrial automation systems using genetic algorithm and simulation. In *Emerging Technology and Factory Automation (ETFA), 2014 IEEE*, pages 1–8, September 2014.

[PSC15] Seemita Pal, Biplab Sikdar, and Joe H Chow. Detecting malicious manipulation of synchrophasor data. In *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, pages 145–150. IEEE, 2015.

[PTM+05] L.R. Phillips, B. Tejani, J. Margulies, J.L. Hills, B.T. Richardson, M.J. Baca, and L. Weiland. Analysis of operations and cyber security policies for a system of cooperating flexible alternating current transmission system (facts) devices. Technical Report SAND2005-7301, Sandia National Laboratories, Albuquerque, New Mexico 87185, December 2005.

[QLC12] Z. Qin, Q. Li, and M.-C. Chuah. Unidentifiable attacks in electric power systems. In *Cyber-Physical Systems (ICCPS), 2012 IEEE/ACM Third International Conference on*, pages 193–202, April 2012.

[QLC13] Z. Qin, Q. Li, and M.-C. Chuah. Defending against unidentifiable attacks in electric power grids. *Parallel and Distributed Systems, IEEE Transactions on*, 24(10):1961–1971, October 2013.

[QWT+11] H. Qi, X. Wang, L.M. Tolbert, F. Li, F.Z. Peng, P. Ning, and M. Amin. A resilient real-time system design for a secure and reconfigurable power grid. *Smart Grid, IEEE Transactions on*, 2(4):770–781, December 2011.

[RA13] M.A. Rahman and E. Al-Shaer. A declarative logic-based approach for threat analysis of advanced metering infrastructure. In *Automated Security Management*, pages 59–77. Springer, 2013.

[RAB14] M.A. Rahman, E. Al-Shaer, and R.B. Bobba. Moving target defense for hardening the security of the power system state estimation. In *Proceedings of the First ACM Workshop on Moving Target Defense*, MTD '14, pages 59–68, New York, NY, USA, 2014. ACM.

[Rah15] Mohammad Ashiqur Rahman. *Automated formal analytics for smart grid security and resiliency*. PhD thesis, The University of North Carolina at Charlotte, 2015.

[RAK14a] M.A. Rahman, E. Al-Shaer, and R. Kavasseri. Impact analysis of topology poisoning attacks on economic operation of the smart power grid. In *Distributed Computing Systems (ICDCS), 2014 IEEE 34th International Conference on*, pages 649–659, June 2014.

[RAK14b] M.A. Rahman, E. Al-Shaer, and R.G. Kavasseri. Security threat analytics and countermeasure synthesis for power system state estimation. In *Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on*, pages 156–167, June 2014.

[Ran14] R. Rangarajan. Quantifying the economic impacts of attacks on competitive energy markets. In *North American Power Symposium (NAPS), 2014*, pages 1–6, September 2014.

[RAR13] M.A. Rahman, E. Al-Shaer, and M.A. Rahman. A formal model for verifying stealthy attacks on state estimation in power grids. In *Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on*, pages 414–419, October 2013.

[Rat15] Lillian Jane Ratliff. *Incentivizing Effiiency in Societal-Scale Cyber-Physical Systems*. University of California, Berkeley, 2015.

[Rav15] Maruth T Ravichandran. *Resilient monitoring and control systems: design, analysis, and performance evaluation*. PhD thesis, University of Michigan, 2015.

[RB15a] Danda B Rawat and Chandra Bajracharya. Cyber security for smart grid systems: Status, challenges and perspectives. In *SoutheastCon 2015*, pages 1–6. IEEE, 2015.

[RB15b] D.B. Rawat and C. Bajracharya. Detection of false data injection attacks in smart grid communication systems. *Signal Processing Letters, IEEE*, 22(10):1652–1656, October 2015.

[RD15] Sandip Roy and Rahul Dhal. Situational awareness for dynamical network processes using incidental measurements. *IEEE Journal of Selected Topics in Signal Processing*, 9(2):304–316, 2015.

[RES+10] Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya, and Qishi Wu. A survey of game theory as applied to network security. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, pages 1–10. IEEE, 2010.

[RGM09] C.G. Rieger, D.I. Gertman, and M.A. McQueen. Resilient control systems: Next generation design research. In *Human System Interactions, 2009. HSI '09. 2nd Conference on*, pages 632–636, May 2009.

[RH15] Tsotsope Daniel Ramotsoela and Gerhard P Hancke. Data aggregation using homomorphic encryption in wireless sensor networks. In *Information Security for South Africa (ISSA), 2015*, pages 1–8. IEEE, 2015.

[RL15a] Md Masud Rana and Li Li. Distributed generation monitoring of smart grid using accuracy dependent kalman filter with communication systems. In *Information Technology-New Generations (ITNG), 2015 12th International Conference on*, pages 496–500. IEEE, 2015.

[RL15b] Md Masud Rana and Li Li. Kalman filter based microgrid state estimation using the internet of things communication network. In *Information Technology-New Generations (ITNG), 2015 12th International Conference on*, pages 501–505. IEEE, 2015.

[RL15c] Md Masud Rana and Li Li. An overview of distributed microgrid state estimation and control for smart grids. *Sensors*, 15(2):4302–4325, 2015.

[RM12] M.A. Rahman and H. Mohsenian-Rad. False data injection attacks with incomplete information against smart power grids. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 3153–3158, December 2012.

[RM13a] M.A. Rahman and H. Mohsenian-Rad. False data injection attacks against nonlinear state estimation in smart power grids. In *Power and Energy Society General Meeting (PES), 2013 IEEE*, pages 1–5, July 2013.

[RM13b] T. Roth and B.M. McMillin. Breaking nondeducible attacks on the smart grid. In B.M. Hämmerli, N. Kalstad Svendsen, and J. Lopez, editors, *Critical Information Infrastructures Security*, volume 7722 of *Lecture Notes in Computer Science*, pages 80–91. Springer Berlin Heidelberg, 2013.

[RMS14] X. Ren, Y. Mo, and L. Shi. Optimal DoS attacks on Bayesian quickest change detection. In *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*, pages 3765–3770, December 2014.

[RNLV08] T. Roosta, D.K. Nilsson, U. Lindqvist, and A. Valdes. An intrusion detection system for wireless process control systems. In *Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008. 5th IEEE International Conference on*, pages 866–872, September 2008.

[Rot15] Thomas Patrick Roth. *Distributed state verification in the smart grid using physical attestation*. PhD thesis, Missouri University of Science and Technology, 2015.

[RP14] S. Ruj and A. Pal. Analyzing cascading failures in smart grids under random and targeted attacks. In *Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on*, pages 226–233, May 2014.

[RP15] Anup P Ranekar and AR Bhagat Patil. Survey of DoS defense mechanisms. In *Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on*, pages 1–5. IEEE, 2015.

[RSG15] Ivan Ruchkin, Bradley Schmerl, and David Garlan. Analytic dependency loops in architectural models of cyber-physical systems. In *International Workshop on Model-based Architecting of Cyber-Physical and Embedded Systems*, 2015.

[RVD14] A. Rosich, H. Voos, and M. Darouach. Cyber-attack detection based on controlled invariant sets. In *Control Conference (ECC), 2014 European*, pages 2176–2181, June 2014.

[RVLD13] A. Rosich, H. Voos, Y. Li, and M. Darouach. A model predictive approach for cyber-attack detection and mitigation in control systems. In *Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on*, pages 6621–6626, December 2013.

[SAD+14] H. Suleiman, I. Alqassem, A. Diabat, E. Arnautovic, and D. Svetinovic. Integrated smart grid systems security threat model. *Information Systems*, PP(99):1–1, 2014.

[Sak15] Yasser Shoukry Sakr. *Security and Privacy in Cyber-Physical Systems: Physical Attacks and Countermeasures*. PhD thesis, University of California, Los Angeles, 2015.

[Sar15] Arman Sargolzaei. *Time-Delay Switch Attack on Networked Control Systems, Effects and Countermeasures*. PhD thesis, Florida International University, 2015.

[SB14] Y. Soupionis and T. Benoist. Cyber attacks in power grid ICT systems leading to financial disturbance. In *Critical Information Infrastructures Security, 9th International Conference on (CRITIS 2014)*, October 2014.

[SBPV14] B.M. Sanandaji, E. Bitar, K. Poolla, and T.L. Vincent. An abrupt change detection heuristic with applications to cyber data attacks on power systems. In *American Control Conference (ACC), 2014*, pages 5056–5061, June 2014.

[SC15] Neetesh Saxena and Bong Jun Choi. State of the art authentication, access control, and secure integration in smart grid. *Energies*, 8(10):11883–11915, 2015.

[SCL+07] S. Sheng, W.L. Chan, K.K. Li, X. Duan, and X. Zeng. Context information-based cyber security defense of protection system. *Power Delivery, IEEE Transactions on*, 22(3):1477–1481, July 2007.

[SEC15] Dawei Shi, Robert J Elliott, and Tongwen Chen. Event-based state estimation of a discrete-state hidden Markov model through a reliable communication channel. In *Control Conference (CCC), 2015 34th Chinese*, pages 4673–4678. IEEE, 2015.

[SG14] S. Sridhar and M. Govindarasu. Model-based attack detection and mitigation for automatic generation control. *Smart Grid, IEEE Transactions on*, 5(2):580–591, March 2014.

[SGK15] Samina Subhani, M Gibescu, and WL Kling. Autonomous control of distributed energy resources via wireless machine-to-machine communication; a survey of big data challenges. In *Environment and Electrical Engineering (EEEIC), 2015 IEEE 15th International Conference on*, pages 1437–1442. IEEE, 2015.

[SH11] S. Sundaram and C.N. Hadjicostis. Distributed function calculation via linear iterative strategies in the presence of malicious agents. *Automatic Control, IEEE Transactions on*, 56(7):1495–1508, July 2011.

[SHC+14] S. Sierla, M. Hurkala, K. Charitoudi, C.-W. Yang, and V. Vyatkin. Security risk analysis for smart grid automation. In *Industrial Electronics (ISIE), 2014 IEEE 23rd International Symposium on*, pages 1737–1744, June 2014.

[SJ10] Anjali Sardana and Ramesh Chandra Joshi. Dual-level attack detection and characterization for networks under ddos. In *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*, pages 9–16. IEEE, 2010.

[SJ13] H. Sedghi and E. Jonckheere. Statistical structure learning of smart grid for detection of false data injection. In *Power and Energy Society General Meeting (PES), 2013 IEEE*, pages 1–5, July 2013.

[SJ15] H. Sedghi and E. Jonckheere. Statistical structure learning to ensure data integrity in smart grid. *Smart Grid, IEEE Transactions on*, 6(4):1924–1933, July 2015.

[SKTP11] L. Sankar, S. Kar, R. Tandon, and H.V. Poor. Competitive privacy in the smart grid: An information-theoretic approach. In *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, pages 220–225, October 2011.

[SLCL15] Sergio Salinas, Changqing Luo, Xuhui Chen, and Pan Li. Efficient secure outsourcing of large-scale linear systems of equations. In *Computer Communications (INFOCOM), 2015 IEEE Conference on*, pages 1035–1043. IEEE, 2015.

[SLK+15] Aamir Shahzad, Malrey Lee, Hyung Doo Kim, Seon-mi Woo, and Naixue Xiong. New security development and trends to secure the SCADA sensors automated transmission during critical sessions. *Symmetry*, 7(4):1945–1980, 2015.

[SLL12] S. Salinas, M. Li, and P. Li. Privacy-preserving energy theft detection in smart grids. In *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012 9th Annual IEEE Communications Society Conference on*, pages 605–613, June 2012.

[SLL14] P. Shakarian, H. Lei, and R. Lindelauf. Power grid defense against malicious cascading failure. In *Proceedings of the 2014 International Conference on Autonomous Agents and Multi-agent Systems*, AAMAS '14, pages 813–820, Richland, SC, 2014. International Foundation for Autonomous Agents and Multiagent Systems.

[SLL15] Alexandru Stefanov, Chen-Ching Liu, and Kithsiri Liyanage. Ict modeling for cosimulation of integrated cyberpower systems. In *Securing Cyber-Physical Systems*, page 27. CRC Press, 2015.

[SLM15] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. Intrusion detection for airborne communication using PHY-Layer information. In Magnus Almgren, Vincenzo Gulisano, and Federico Maggi, editors, *Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 67–77. Springer International Publishing, 2015.

[SLP11] D. Seo, H. Lee, and A. Perrig. Secure and efficient capability-based power management in the smart grid. In *Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011 Ninth IEEE International Symposium on*, pages 119–126, May 2011.

[SLSY15] Ying Sun, Wen-Tai Li, Wentu Song, and Chau Yuen. False data injection attacks with local topology information against linear state estimation. In *Innovative Smart Grid Technologies-Asia (ISGT ASIA), 2015 IEEE*, pages 1–5. IEEE, 2015.

[SLV+07] K. Sun, S. Likhate, V. Vittal, V.S. Kolluri, and S. Mandal. An online dynamic security assessment scheme using phasor measurements and decision trees. *Power Systems, IEEE Transactions on*, 22(4):1935–1943, November 2007.

[SLZX14] M. Shange, J. Lin, X. Zhang, and C. Xu. A game-theory analysis of the rat-group attack in smart grids. In *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference on*, pages 1–6, April 2014.

[SM10] S. Sridhar and G. Manimaran. Data integrity attacks and their impacts on SCADA control system. In *Power and Energy Society General Meeting, 2010 IEEE*, pages 1–6, July 2010.

[SM11] S. Sridhar and G. Manimaran. Data integrity attack and its impacts on voltage control loop in power grid. In *Power and Energy Society General Meeting, 2011 IEEE*, pages 1–6, July 2011.

[SMF+15] Martin Strohmeier, Ivan Martinovic, Markus Fuchs, Matthias Schäfer, and Vincent Lenders. OpenSky: A swiss army knife for air traffic security research. In *Digital Avionics Systems Conference (DASC), 2015 IEEE/AIAA 34th*, pages 4A1–1. IEEE, 2015.

[Smi11] R.S. Smith. A decoupled feedback structure for covertly appropriating networked control systems. In *Proceedings of the 18th IFAC world congress*, pages 90–95, August–September 2011.

[Smi15] R.S. Smith. Covert misappropriation of networked control systems: Presenting a feedback structure. *Control Systems, IEEE*, 35(1):82–92, February 2015.

[SMR09] J. Stamp, A. McIntyre, and B. Ricardson. Reliability impacts from cyber attack on electric power systems. In *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*, pages 1–8, March 2009.

[SMT+14] T. Spyridopoulos, K. Maraslis, T. Tryfonas, G. Oikonomou, and S. Li. Managing cyber security risks in industrial control systems with game theory and viable system modelling. In *System of Systems Engineering (SOSE), 2014 9th International Conference on*, pages 266–271, June 2014.

[SMTS13] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava. Non-invasive spoofing attacks for anti-lock braking systems. In G. Bertoni and J.-S. Coron, editors, *Cryptographic Hardware and Embedded Systems - CHES 2013*, volume 8086 of *Lecture Notes in Computer Science*, pages 55–72. Springer Berlin Heidelberg, 2013.

[SMY+15] Yasser Shoukry, Paul Martin, Yair Yona, Suhas Diggavi, and Mani Srivastava. Pycra: Physical challenge-response authentication for active sensors under spoofing attacks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1004–1015. ACM, 2015.

[SNB+15] Yasser Shoukry, Pierluigi Nuzzo, Nicola Bezzo, Alberto L Sangiovanni-Vincentelli, Sanjit A Seshia, and Paulo Tabuada. A satisfiability modulo theory approach to secure state reconstruction in differentially flat systems under sensor attacks. *arXiv preprint arXiv:1509.03262*, 2015.

[SNG14] Y. Soupionis, S. Ntalampiras, and G. Giannopoulos. Faults and cyber attacks detection in critical infrastructures. In *9th International Conference on Critical Information Infrastructures Security, to appear*, pages 1–12, October 2014.

[SNP+14] Y. Shoukry, P. Nuzzo, A. Puggelli, A.L. Sangiovanni-Vincentelli, S.A. Seshia, and P. Tabuada. Secure state estimation under sensor attacks: A satisfiability modulo theory approach. *arXiv preprint arXiv:1412.4324*, 2014.

[SNP+15] Yasser Shoukry, Pierluigi Nuzzo, Alberto Puggelli, Alberto L Sangiovanni-Vincentelli, Sanjit A Seshia, Mani Srivastava, and Paulo Tabuada. Imhotep-SMT: A satisfiability modulo theory solver for secure state estimation. In *Proc. Int. Workshop Satisfiability Modulo Theories*, pages 3–13, 2015.

[SPH+10] S. Sundaram, M. Pajic, C.N. Hadjicostis, R. Mangharam, and G.J. Pappas. The wireless control network: Monitoring for malicious behavior. In *Decision and Control (CDC), 2010 49th IEEE Conference on*, pages 5979–5984, December 2010.

[SPK13] F. Schuster, A. Paul, and H. König. Towards learning normality for anomaly detection in industrial control networks. In G. Doyen, M. Waldburger, P. Čeleda, A. Sperotto, and B. Stiller, editors, *Emerging Management Mechanisms for the Future Internet*, volume 7943 of *Lecture Notes in Computer Science*, pages 61–72. Springer Berlin Heidelberg, 2013.

[SPN+15] Y. Shoukry, A. Puggelli, P. Nuzzo, A.L. Sangiovanni-Vincentelli, S.A. Seshia, and P. Tabuada. Sound and complete state estimation for linear dynamical systems under sensor attack using satisfiability modulo theory solving. In *American Control conference (ACC), 2015*, July 2015.

[Sri15] Siddharth Sridhar. *Cyber risk modeling and attack-resilient control for power grid*. PhD thesis, Iowa State University, 2015.

[SRK+15] Yuquan Shan, Jayaram Raghuram, George Kesidis, David J Miller, Anna Scaglione, Jeff Rowe, and Karl Levitt. Generation bidding game with potentially false attestation of flexible demand. *EURASIP Journal on Advances in Signal Processing*, 2015(1):29, 2015.

[SS14] K. Sravani and P. Srinivasu. Comparative study of machine learning algorithm for intrusion detection system. In *Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013*, pages 189–196. Springer, 2014.

[SS15a] Anibal Sanjab and Walid Saad. Smart grid data injection attacks: To defend or not? In *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, pages 380–385. IEEE, 2015.

[SS15b] Konark Sharma and Lalit Mohan Saini. Performance analysis of smart metering for smart grid: An overview. *Renewable and Sustainable Energy Reviews*, 49:720–735, 2015.

[SSJ11] K.C. Sou, H. Sandberg, and K.H. Johansson. Electric power network security analysis via minimum cut relaxation. In *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*, pages 4054–4059, December 2011.

[SSJ12a] K.C. Sou, H. Sandberg, and K.H. Johansson. Computing critical k-tuples in power networks. *Power Systems, IEEE Transactions on*, 27(3):1511–1520, August 2012.

[SSJ12b] K.C. Sou, H. Sandberg, and K.H. Johansson. Detection and identification of data attacks in power system. In *American Control Conference (ACC), 2012*, pages 3651–3656, June 2012.

[SSJ13] K.C. Sou, H. Sandberg, and K.H. Johansson. On the exact solution to a smart grid cyber-security analysis problem. *Smart Grid, IEEE Transactions on*, 4(2):856–865, June 2013.

[SSJ14] K.C. Sou, H. Sandberg, and K.H. Johansson. Data attack isolation in power networks using secure voltage magnitude measurements. *Smart Grid, IEEE Transactions on*, 5(1):14–28, January 2014.

[SSL+15] Zhiguo Shi, Ruixue Sun, Rongxing Lu, Le Chen, Jiming Chen, and Xuemin Sherman Shen. Diverse grouping-based aggregation protocol with error detection for smart grid communications. *IEEE Transactions on Smart Grid*, 6(6):2856–2868, 2015.

[ST13] Y. Shoukry and P. Tabuada. Event-triggered state observers for sparse sensor noise/attacks. *arXiv preprint arXiv:1309.3511*, 2013.

[ST14] Y. Shoukry and P. Tabuada. Event-triggered projected Luenberger observer for linear systems under sparse sensor attacks. In *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*, December 2014.

[ST16] Yasser Shoukry and Paulo Tabuada. Event-triggered state observers for sparse sensor noise/attacks. *IEEE Transactions on Automatic Control*, 61(8):2079–2091, 2016.

[STF05] M. Shahidehpour, W.F. Tinney, and Y. Fu. Impact of security on power systems operation. *Proceedings of the IEEE*, 93(11):2013–2025, November 2005.

[STJ10] H. Sandberg, A. Teixeira, and K.H. Johansson. On security indices for state estimators in power networks. In *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010*, April 2010.

[SWB04] J. Salmeron, K. Wood, and R. Baldick. Analysis of electric grid security under terrorist threat. *Power Systems, IEEE Transactions on*, 19(2):905–912, May 2004.

[SWB09] J. Salmeron, K. Wood, and R. Baldick. Worst-case interdiction analysis of large-scale electric power grids. *Power Systems, IEEE Transactions on*, 24(1):96–104, February 2009.

[SWW+15] Yunchuan Sun, Lei Wu, Shizhong Wu, Shoupeng Li, Tao Zhang, Li Zhang, Junfeng Xu, and Yongping Xiong. Security and privacy in the internet of vehicles. In *Identification, Information, and Knowledge in the Internet of Things (IIKI), 2015 International Conference on*, pages 116–121. IEEE, 2015.

[SYA14] A. Sargolzaei, K. Yen, and M. Abdelghani. Delayed inputs attack on load frequency control in smart grid. In *Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES*, pages 1–5, February 2014.

[SYZ15] S. Soltan, M. Yannakakis, and G. Zussman. Joint cyber and physical attacks on power grids: Graph theoretical approaches for information recovery. In *SIGMETRICS '15: Proceedings of the 2015 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*, June 2015.

[SZS+08] D. Salem-Natarajan, L. Zhao, W. Shao, N. Varghese, S. Ghosh, M. Subramanian, G. Lin, H.-D. Chiang, and H. Li. State estimator for CA ISO market and security applications - relevance and readiness. In *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, pages 1–8, July 2008.

[Tah15] Ahmad Fayez Taha. *Secure estimation, control and optimization of uncertain cyber-physical systems with applications to power networks*. PhD thesis, Purdue University, 2015.

[Taj14] A. Tajer. Energy grid state estimation under random and structured bad data. In *Sensor Array and Multichannel Signal Processing Workshop (SAM), 2014 IEEE 8th*, pages 65–68, June 2014.

[Tak07] M. Takano. Sustainable cyber security for tility facilities control system based on defense-in-depth concept. In *SICE, 2007 Annual Conference*, pages 2910–2913, September 2007.

[TAN+15] RCG Teive, FF Andrade, EAC Aranha Neto, LM Rosário, and JA De Bettio. Novel method for typical load curves characterization of industrial consumers towards the smart grids. In *Intelligent System Application to Power Systems (ISAP), 2015 18th International Conference on*, pages 1–7. IEEE, 2015.

[TAS+10] A. Teixeira, S. Amin, H. Sandberg, K.H. Johansson, and S.S. Sastry. Cyber security analysis of state estimators in electric power systems. In *Decision and Control (CDC), 2010 49th IEEE Conference on*, pages 5991–5998, December 2010.

[TBYK13] R. Tan, V. Badrinath Krishna, D.K.Y. Yau, and Z. Kalbarczyk. Impact of integrity attacks on real-time pricing in smart grids. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 439–450, New York, NY, USA, 2013. ACM.

[TDS+14] A. Teixeira, G. Dán, H. Sandberg, R. Berthier, R.B. Bobba, and A. Valdes. Security of smart distribution grids: Data integrity attacks on integrated volt/VAR control and countermeasures. In *American Control Conference (ACC), 2014*, pages 4372–4378, June 2014.

[TDSJ11] A. Teixeira, G. Dán, H. Sandberg, and K.H. Johansson. A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator. In *Proceedings of the 18th IFAC world congress*, pages 11271–11277, August–September 2011.

[TEL13] E.E. Tiniou, P.M. Esfahani, and J. Lygeros. Fault detection with discrete-time measurements: An application for the cyber security of power networks. In *Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on*, pages 194–199, December 2013.

[TGW15] Tasnuva Tithi, Ryan Gerdes, and Chris Winstead. Poster: Position verification in vehicular platoons using a euclidean distance matrix. In *Proc. Symp. Security and Privacy*, 2015.

[THL11] C.-W. Ten, J. Hong, and C.-C. Liu. Anomaly detection for cybersecurity of the substations. *Smart Grid, IEEE Transactions on*, 2(4):865–873, December 2011.

[TKPC11] A. Tajer, S. Kar, H.V. Poor, and S. Cui. Distributed joint cyber attack detection and state recovery in smart grids. In *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, pages 202–207, October 2011.

[TKSJ15] André Teixeira, Friederich Kupzog, Henrik Sandberg, and Karl H Johansson. Cybersecure and resilient architectures for industrial control systems. In *Smart Grid Security*, pages 149–183. Elsevier, 2015.

[TKYK15] Rui Tan, Varun Badrinath Krishna, David KY Yau, and Zbigniew Kalbarczyk. Integrity attacks on real-time pricing in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, 18(2):5, 2015.

[TLG15] Yakubu Tsado, David Lund, and Kelum AA Gamage. Resilient communication for smart grid ubiquitous sensor network: State of the art and prospects for next generation. *Computer Communications*, 71:34–49, 2015.

[TLHC14] Y. Tang, X. Luo, Q. Hui, and R.K.C. Chang. Modeling the vulnerability of feedback-control based internet services to low-rate DoS attacks. *Information Forensics and Security, IEEE Transactions on*, 9(3):339–353, 2014.

[TLM07] C.-W. Ten, C.-C. Liu, and G. Manimaran. Vulnerability assessment of cybersecurity for SCADA systems using attack trees. In *Power Engineering Society General Meeting, 2007. IEEE*, pages 1–8, June 2007.

[TLM08] C.-W. Ten, C.-C. Liu, and G. Manimaran. Vulnerability assessment of cybersecurity for SCADA systems. *Power Systems, IEEE Transactions on*, 23(4):1836–1846, November 2008.

[TLP09] P. Tague, M. Li, and R. Poovendran. Mitigation of control channel jamming under node capture attacks. *Mobile Computing, IEEE Transactions on*, 8(9):1221–1234, September 2009.

[TLQ12] M. Talebi, C. Li, and Z. Qu. Enhanced protection against false data injection by dynamically changing information structure of microgrids. In *Sensor Array and Multichannel Signal Processing Workshop (SAM), 2012 IEEE 7th*, pages 393–396, June 2012.

[TML10] Chee-Wooi Ten, Govindarasu Manimaran, and Chen-Ching Liu. Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 40(4):853–865, 2010.

[TO15a] Sebastian F. Tudor and Cristian Oara. H_∞ control problem for discrete-time algebraic dynamical systems. *SIAM Journal on Control and Optimization*, 53(5):3171–3194, 2015.

[TO15b] Sebastian F Tudor and Cristian Oară. h_∞ control problem for generalized discrete-time LTI systems. In *American Control Conference (ACC), 2015*, pages 4640–4645. IEEE, 2015.

[TO15c] Sebastian F Tudor and Cristian Oara. A mobius transformation for algebraic dynamical systems. In *Control Systems and Computer Science (CSCS), 2015 20th International Conference on*, pages 931–937. IEEE, 2015.

[Ton15] Yue Tong. *Data security and privacy in smart grid*. PhD thesis, University of Tennessee - Knoxville, 2015.

[TPSJ15] André Teixeira, Kaveh Paridari, Henrik Sandberg, and Karl H Johansson. Voltage control for interconnected microgrids under adversarial actions. In *Emerging Technologies & Factory Automation (ETFA), 2015 IEEE 20th Conference on*, pages 1–8. IEEE, 2015.

[TQGA15] Kutub Thakur, Meikang Qiu, Keke Gai, and Md Liakat Ali. An investigation on cyber security threats and security models. In *Cyber Security and Cloud Computing (CSCloud), 2015 IEEE 2nd International Conference on*, pages 307–311. IEEE, 2015.

[TR15] Jackeline Abad Torres and Sandip Roy. A two-layer transformation for characterizing the zeros of a network input-output dynamics. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages 902–907. IEEE, 2015.

[TSDJ12] A. Teixeira, H. Sandberg, G. Dán, and K.H. Johansson. Optimal power flow: Closing the loop over corrupted data. In *American Control Conference (ACC), 2012*, pages 3534–3540, June 2012.

[TSDR15] Jackeline Abad Torres, Dinuka Sahabandu, Rahul Dhal, and Sandip Roy. Local open-and closed-loop manipulation of multi-agent networks. In *Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems*, pages 21–30. ACM, 2015.

[TSJ15] André Teixeira, Henrik Sandberg, and Karl H Johansson. Strategic stealthy attacks: the output-to-output 2-gain. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages 2582–2587. IEEE, 2015.

[TSME15] B Thanudas, S Sreelal, BS Manoj, and Sumathy Eswaran. Agent-controller based security infrastructure for enterprise network. *Software Engineering and Technology*, 7(7):204–207, 2015.

[TSSJ12] A. Teixeira, I. Shames, H. Sandberg, and K.H. Johansson. Revealing stealthy attacks in control systems. In *Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on*, pages 1806–1813, October 2012.

[TSST14] S. Tan, Z. Song, W, M. Stewart, and L. Tong. LPAttack: Leverage point attacks against state estimation in smart grid. In *Global Communications Conference (GLOBECOM), 2014 IEEE*, pages 643–648, December 2014.

[TSST15] Song Tan, Wen-Zhan Song, Michael Stewart, and Lang Tong. Construct data integrity attacks against real-time electrical market in smart grid. In *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, pages 398–403. IEEE, 2015.

[TVDH14] N.M. Torrisi, O. Vuković, G. Dán, and S. Hagdahl. Peekaboo: A gray hole attack on encrypted SCADA communication using traffic analysis. In *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, pages 902–907, November 2014.

[TWQ12] M. Talebi, J. Wang, and Z. Qu. Secure power systems against malicious cyber-physical data attacks: Protection and identification. In *International Conference on Power Systems Engineering*, pages 112–119. World Academy of Science, Engineering and Technology, June 2012.

[UKWI15] Muhammad Sharif Uddin, Anthony Kuh, Yang Weng, and Marija Ilić. Online bad data detection using kernel density estimation. In *Power & Energy Society General Meeting, 2015 IEEE*, pages 1–5. IEEE, 2015.

[VD13a] O. Vuković and G. Dán. Detection and localization of targeted attacks on fully distributed power system state estimation. In *Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on*, pages 390–395, October 2013.

[VD13b] O. Vuković and G. Dán. On the security of distributed power system state estimation under targeted attacks. In *Proceedings of the 28th Annual ACM Symposium on Applied Computing*, SAC '13, pages 666–672, New York, NY, USA, 2013. ACM.

[VD14] O. Vuković and G. Dán. Security of fully distributed power system state estimation: Detection and mitigation of data integrity attacks. *Selected Areas in Communications, IEEE Journal on*, 32(7):1500–1508, July 2014.

[VEM+15] M. Vrakopoulou, P.M. Esfahani, K. Margellos, J. Lygeros, and G. Andersson. Cyber-attacks in the automatic generation control. In S.K. Khaitan, J.D. McCalley, and C.C. Liu, editors, *Cyber Physical Systems Approach to Smart Electric Power Grid*, Power Systems, pages 303–328. Springer Berlin Heidelberg, 2015.

[VF13] U. Vaidya and M. Fardad. On optimal sensor placement for mitigation of vulnerabilities to cyber attacks in large-scale networks. In *Control Conference (ECC), 2013 European*, pages 3548–3553, July 2013.

[VFLG14] T. Vuong, A. Filippoupolitis, G. Loukas, and D. Gan. Physical indicators of cyber attacks against a rescue robot. In *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference on*, pages 338–343, March 2014.

[VHSM14] K.G. Vamvoudakis, J.P. Hespanha, B. Sinopoli, and Y. Mo. Detection in adversarial environments. *Automatic Control, IEEE Transactions on*, 59(12):3209–3223, December 2014.

[VLG15] Tuan Phan Vuong, George Loukas, and Diane Gan. Performance evaluation of cyber-physical intrusion detection on a robotic vehicle. In *Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on*, pages 2106–2113. IEEE, 2015.

[VLGB15] Tuan Phan Vuong, George Loukas, Diane Gan, and Anatolij Bezemskij. Decision tree-based detection of denial of service and command injection attacks on robotic vehicles. In *Information Forensics and Security (WIFS), 2015 IEEE International Workshop on*, pages 1–6. IEEE, 2015.

[VPHC+06] Tran Van Phuong, Le Xuan Hung, Seong Jin Cho, Young-Koo Lee, and Sungyoung Lee. An anomaly detection algorithm for detecting attacks in wireless sensor networks. In *Proceedings of the 4th IEEE international conference on Intelligence and Security Informatics*, pages 735–736. Springer-Verlag, 2006.

[VSDS11] O. Vuković, K.C. Sou, G. Dán, and H. Sandberg. Network-layer protection schemes against stealth attacks on state estimators in power systems. In *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, pages 184–189, October 2011.

[VSDS12] Ognjen Vukovic, Kin Cheong Sou, Gyorgy Dan, and Henrik Sandberg. Network-aware mitigation of data integrity attacks on power system state estimation. *IEEE Journal on Selected Areas in Communications*, 30(6):1108–1118, 2012.

[VWB13] J. Valenzuela, J. Wang, and N. Bissinger. Real-time intrusion detection in power system operations. *Power Systems, IEEE Transactions on*, 28(2):1052–1062, May 2013.

[WAKM15] Talha Wahab, Muhammad Abid, Abdul Qayyum Khan, and Ghulam Mustafa. Robust fault detection of linearized power grid network system. In *Power Generation System and Renewable Energy Technologies (PGSRET), 2015*, pages 1–6. IEEE, 2015.

[Wan15] Yu Wang. *Algorithms for Optimal Energy Management in the Smart Grid*. PhD thesis, Auburn University, 2015.

[WBP+13] J. Weimer, N. Bezzo, M. Pajic, G.J. Pappas, O. Sokolsky, and I. Lee. Resilient parameter-invariant control with application to vehicle cruise control. In D.C. Tarraf, editor, *Control of Cyber-Physical Systems*, volume 449 of *Lecture Notes in Control and Information Sciences*, pages 197–216. Springer International Publishing, 2013.

[WBP+14] J. Weimer, N. Bezzo, M. Pajic, O. Sokolsky, and I. Lee. Attack-resilient minimum mean-squared error estimation. In *American Control Conference (ACC), 2014*, pages 1114–1119, June 2014.

[WGL+14] D. Wang, X. Guan, T. Liu, Y. Gu, C. Shen, and Z. Xu. Extended distributed state estimation: A detection method against tolerable false data injection attacks in smart grids. *Energies*, 7(3):1517–1538, 2014.

[WHY15a] Jingxuan Wang, Lucas C.K. Hui, and H.S.M. Yiu. System-state-free false data injection attack for nonlinear state estimation in smart grid. *International Journal of Smart Grid and Clean Energy*, 2015.

[WHY15b] Jingxuan Wang, Lucas CK Hui, and Siu-Ming Yiu. Data framing attacks against nonlinear state estimation in smart grid. In *Globecom Workshops (GC Wkshps), 2015 IEEE*, pages 1–6. IEEE, 2015.

[Wil76] Alan S. Willsky. A survey of design methods for failure detection in dynamic systems. *Automatica*, 12(6):601–611, 1976.

[WKJ12] J. Weimer, S. Kar, and K.H. Johansson. Distributed detection and isolation of topology attacks in power networks. In *Proceedings of the 1st International Conference on High Confidence Networked Systems*, HiCoNS '12, pages 65–72, New York, NY, USA, 2012. ACM.

[WL13] W. Wang and Z. Lu. Cyber security in the smart grid: Survey and challenges. *Computer Networks*, 57(5):1344–1371, 2013.

[WLJ+10] Dong Wei, Yan Lu, Mohsen Jafari, Paul Skare, and Kenneth Rohde. An integrated security system of protecting smart grid against cyber attacks. In *Innovative Smart Grid Technologies (ISGT), 2010*, pages 1–7. IEEE, 2010.

[WLJ+11] D. Wei, Y. Lu, M. Jafari, P.M. Skare, and K. Rohde. Protecting smart grid automation systems against cyberattacks. *Smart Grid, IEEE Transactions on*, 2(4):782–795, December 2011.

[WLM+13] X. Wang, Q. Liang, J. Mu, W. Wang, and B. Zhang. Physical layer security in wireless smart grid. *Security and Communication Networks*, pages n/a–n/a, 2013.

[WLN07] Cliff Wang, An Liu, and Peng Ning. Cluster-based minimum mean square estimation for secure and resilient localization in wireless sensor networks. In *Wireless Algorithms, Systems and Applications, 2007. WASA 2007. International Conference on*, pages 29–37. IEEE, 2007.

[WMO13] I. Watanabe, K. Masutomi, and I. Ono. Robust meter placement against false data injection attacks on power system state estimation. In M. Lee, A. Hirose, Z.-G. Hou, and R.M. Kil, editors, *Neural Information Processing*, volume 8226 of *Lecture Notes in Computer Science*, pages 569–576. Springer Berlin Heidelberg, 2013.

[WMS14] S. Weerakkody, Y. Mo, and B. Sinopoli. Detecting integrity attacks on control systems using robust physical watermarking. In *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*, pages 3757–3764, December 2014.

[Woh14] C. Wohlin. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, EASE '14, pages 38:1–38:10, New York, NY, USA, 2014. ACM.

[WPS+14] K. Wang, Y. Pan, W. Song, W. Wang, and L. Xie. Integrated learning environment for smart grid security. In *INFOCOMP 2014, The Fourth International Conference on Advanced Communications and Computation*, pages 126–131, 2014.

[WR09] J.-W. Wang and L.-L. Rong. Cascade-based attack vulnerability on the US power grid. *Safety Science*, 47(10):1332–1336, 2009.

[WR14a] S. Wang and W. Ren. Stealthy attacks in power systems: Limitations on manipulating the estimation deviations caused by switching network topologies. In *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*, pages 217–222, December 2014.

[WR14b] S. Wang and W. Ren. Stealthy false data injection attacks against state estimation in power systems: Switching network topologies. In *American Control Conference (ACC), 2014*, pages 1572–1577, June 2014.

[WRH+12] C. Wohlin, P. Runeson, M. Höst, M.C. Ohlsson, B. Regnell, and A. Wesslén. *Experimentation in Software Engineering*. Computer Science. Springer, 2012.

[WS15] Sean Weerakkody and Bruno Sinopoli. Detecting integrity attacks on control systems using a moving target approach. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages 5820–5826. IEEE, 2015.

[WSBL14] J. Weimer, O. Sokolsky, N. Bezzo, and I. Lee. Towards assurance cases for resilient control systems. In *Cyber-Physical Systems, Networks, and Applications (CPSNA), 2014 IEEE International Conference on*, pages 1–6, August 2014.

[WSH15] Mark Woodard, Sahra Sedigh Sarvestani, and Ali R Hurson. A survey of research on data corruption in cyber–physical critical infrastructure systems. In *Advances in Computers*, volume 98, pages 59–87. Elsevier, 2015.

[WWX+15] Weichao Wang, Chuang Wang, Le Xie, Wen-zhan Song, and Yi Pan. Security education for smart grid: Materials, experiments, and evaluation. In *19th Colloquium for Information Systems Security education*, 2015.

[WXZ+14] Y. Wang, Z. Xu, J. Zhang, L. Xu, H. Wang, and G. Gu. Srid: State relation based intrusion detection for false data injection attacks in scada. In *Computer Security - ESORICS 2014*, pages 401–418. Springer, 2014.

[WZLZ11] Y. Wang, B. Zhang, W.M. Lin, and T. Zhang. Smart grid information security - a research on standards. In *Advanced Power System Automation and Protection (APAP), 2011 International Conference on*, volume 2, pages 1188–1194, October 2011.

[XGS+15] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen. Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems. *Smart Grid, IEEE Transactions on*, PP(99):1–1, 2015.

[XMS10] L. Xie, Y. Mo, and B. Sinopoli. False data injection attacks in electricity markets. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 226–231, October 2010.

[XMS11] L. Xie, Y. Mo, and B. Sinopoli. Integrity data attacks in power market operations. *Smart Grid, IEEE Transactions on*, 2(4):659–666, December 2011.

[XN15] Kaiqi Xiong and Peng Ning. Cost-efficient and attack-resilient approaches for state estimation in power grids. In *Proceedings of the 30th Annual ACM Symposium on Applied Computing*, pages 2192–2197. ACM, 2015.

[XR12] M. Xue and S. Roy. Characterization of security levels for the dynamics of autonomous vehicle networks. In *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*, pages 3916–3921, December 2012.

[XRWD11] M. Xue, S. Roy, Y. Wan, and S.K. Das. Security and vulnerability of cyber-physical infrastructure networks: a control-theoretic perspective. In S.K. Das, K. Kant, and N. Zhang, editors, *Handbook on Securing Cyber-Physical Critical Infrastructure*, chapter 1. Morgan Kaufmann Publishers, November 2011.

[Xu15] Guobin Xu. *Towards a framework of enabling efficient and secured energy based cyber-physical system (CPS)*. PhD thesis, Towson University, 2015.

[XW15] Yingmeng Xiang and Lingfeng Wang. A game-theoretic approach to optimal defense strategy against load redistribution attack. In *Power & Energy Society General Meeting, 2015 IEEE*, pages 1–5. IEEE, 2015.

[XWR14] M. Xue, W. Wang, and S. Roy. Security concepts for the dynamics of autonomous vehicle networks. *Automatica*, 50(3):852–857, 2014.

[XWYL15] Yingmeng Xiang, Lingfeng Wang, David Yu, and Nian Liu. Coordinated attacks against power grids: Load redistribution attack coordinating with generator and line attacks. In *Power & Energy Society General Meeting, 2015 IEEE*, pages 1–5. IEEE, 2015.

[XXD13] Z. Xiao, Y. Xiao, and D.H. Du. Exploring malicious meter inspection in neighborhood area smart grids. *Smart Grid, IEEE Transactions on*, 4(1):214–226, March 2013.

[XZ08] Liang Xie and Sencun Zhu. Message dropping attacks in overlay networks: Attack detection and attacker identification. *ACM Transactions on Information and System Security (TISSEC)*, 11(3):15, 2008.

[YA15] Mohammad Yasinzadeh and Mahdi Akhbari. A novel PMU anti-spoofing algorithm based on smart grid infrastructures. In *Smart Grid Conference (SGC 2015)*. IEEE, 2015.

[YC15] Z.-H. Yu and W.-L. Chin. Blind false data injection attack using PCA approximation method in smart grid. *Smart Grid, IEEE Transactions on*, 6(3):1219–1226, May 2015.

[Ye15] Feng Ye. *Smart grid communication infrastructures-Big data and network security*. PhD thesis, The University of Nebraska-Lincoln, 2015.

[YEPA07] Y. Yao, T. Edmunds, D. Papageorgiou, and R. Alvarez. Trilevel optimization in power network defense. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 37(4):712–718, July 2007.

[YGA15] E. Yağdereli, C. Gemci, and A.Z. Aktaş. A study on cyber-security of autonomous and unmanned vehicles. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, pages 1–13, 2015.

[YGG+15] W. Yu, D. Griffith, L. Ge, S. Bhattarai, and N. Golmie. An integrated detection system against false data injection attacks in the smart grid. *Security and Communication Networks*, 8(2):91–109, 2015.

[YGLV13] J. Yan, M. Govindarasu, C.-C. Liu, and U. Vaidya. A PMU-based risk assessment framework for power control systems. In *Power and Energy Society General Meeting (PES), 2013 IEEE*, pages 1–5, July 2013.

[YGZ+12] Y. Yang, X. Guan, Y. Zhou, J. Wu, and T. Liu. Impact of information security on PMU-based distributed state estimation. In *Innovative Smart Grid Technologies - Asia (ISGT Asia), 2012 IEEE*, pages 1–4, May 2012.

[YHY+15] Xinyu Yang, Xiaofei He, Wei Yu, Jie Lin, Rui Li, Qingyu Yang, and Houbing Song. Towards a low-cost remote memory attestation for the smart grid. *Sensors*, 15(8):20799–20824, 2015.

[YLR11] Y. Yuan, Z. Li, and K. Ren. Modeling load redistribution attacks in power systems. *Smart Grid, IEEE Transactions on*, 2(2):382–390, June 2011.

[YLR12] Y. Yuan, Z. Li, and K. Ren. Quantitative analysis of load redistribution attacks in power systems. *Parallel and Distributed Systems, IEEE Transactions on*, 23(9):1731–1738, September 2012.

[YLS+11] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H.F. Wang. Impact of cyber-security issues on smart grid. In *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on*, pages 1–7, December 2011.

[YLVY15] Zheng Yan, Jun Liu, Athanasios V Vasilakos, and Laurence T Yang. Trustworthy data fusion and mining in Internet of Things. *Future Generation Computer Systems*, 49(C):45–46, 2015.

[YMG06] J. Yu, A. Mao, and Z. Guo. Vulnerability assessment of cyber security in power industry. In *Power Systems Conference and Exposition, 2006. PSCE '06. 2006 IEEE PES*, pages 2200–2205, October 2006.

[YMS+14] Yi Yang, Keiran McLaughlin, Sakir Sezer, Tim Littler, Eul Gyu Im, Bernardi Pranggono, and H.F. Wang. Multiattribute SCADA-specific intrusion detection system for power networks. *IEEE Transactions on Power Delivery*, 29(3):1092–1102, 2014.

[YOTI14] Y. Yamaguchi, A. Ogawa, A. Takeda, and S. Iwata. Cyber security analysis of power networks by hypergraph cut algorithms. In *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, pages 824–829, November 2014.

[YQL15] Shanhe Yi, Zhengrui Qin, and Qun Li. Security and privacy issues of fog computing: A survey. In *International Conference on Wireless Algorithms, Systems, and Applications*, pages 685–695. Springer, 2015.

[YQST12] Y. Yan, Y. Qian, H. Sharif, and D. Tipper. A survey on cyber security for smart grid communications. *Communications Surveys Tutorials, IEEE*, 14(4):998–1010, Fourth 2012.

[YS14] Y. Yuan and F. Sun. Secure the control system against DoS attacks: A JDL data fusion method. In *Multisensor Fusion and Information Integration for Intelligent Systems (MFI), 2014 International Conference on*, pages 1–6, September 2014.

[YS15] Y. Yuan and F. Sun. Data fusion-based resilient control system under DoS attacks: A game theoretic approach. *International Journal of Control, Automation and Systems*, pages 1–8, 2015.

[YSL15] Y. Yuan, F. Sun, and H. Liu. Resilient control of cyber-physical systems against intelligent attacker: a hierarchal stackelberg game approach. *International Journal of Systems Science*, PP(99):1–11, 2015.

[YT15] Zhang Yuan and Zhou Tong. A reinvestigation on the controllability and observability of networked dynamic systems. In *Control Conference (CCC), 2015 34th Chinese*, pages 6740–6746. IEEE, 2015.

[Yu12] W. Yu. False data injection attacks in smart grid: Challenges and solutions. In T. Brewer, editor, *Proceeding of the Cyber Security in Cyber-Physical System Workshop*. NIST, April 2012. NISTIR 7916.

[Yu13] W. Yu. Towards secured and efficient energy-based cyber-physical systems. In *NSF National Workshop on Energy Cyber-Physical systems*, pages 1–3, December 2013.

[YYL+15] Junjie Yang, Rong Yu, Yi Liu, Shengli Xie, and Yan Zhang. A two-stage attacking scheme for low-sparsity unobservable attacks in smart grid. In *Communications (ICC), 2015 IEEE International Conference on*, pages 7210–7215. IEEE, 2015.

[YYY+11] Q. Yang, J. Yang, W. Yu, N. Zhang, and W. Zhao. On a hierarchical false data injection attack on power system state estimation. In *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, pages 1–5, December 2011.

[YZF15] Sze Zheng Yong, Minghui Zhu, and Emilio Frazzoli. Simultaneous input and state estimation of linear discrete-time stochastic systems with input aggregate information. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages 461–467. IEEE, 2015.

[YZQS15] Chaoqun Yang, Heng Zhang, Fengzhong Qu, and Zhiguo Shi. Performance of target tracking in radar network system under deception attack. In *International Conference on Wireless Algorithms, Systems, and Applications*, pages 664–673. Springer, 2015.

[ZAS15] Haotian Zhang, Raid Ayoub, and Shreyas Sundaram. State estimation for linear systems with unknown inputs: Unknown input norm-observers and BIBOBS stability. In *American Control Conference (ACC), 2015*, pages 4186–4191. IEEE, 2015.

[ZBT11] H. Zhang, M. A. Babar, and P. Tell. Identifying relevant studies in software engineering. *Information and Software Technology*, 53(6):625–637, 2011.

[ZC12] L. Zhou and S. Chen. A survey of research on smart grid security. In *Network Computing and Information Security*, pages 395–405. Springer, 2012.

[ZCSC15] H. Zhang, P. Cheng, L. Shi, and J. Chen. Optimal Denial-of-Service attack scheduling in cyber-physical systems. Technical report, Zhejiang University, January 2015.

[ZCSC16] Heng Zhang, Peng Cheng, Ling Shi, and Jiming Chen. Optimal DoS attack scheduling in wireless networked control system. *IEEE Transactions on Control Systems Technology*, 24(3):843–852, 2016.

[ZCW+14] H. Zhang, P. Cheng, J. Wu, L. Shi, and J. Chen. Online deception attack against remote state estimation. In *Proceedings of World Congress of the International Federation of Automatic Control (IFAC)*, 2014.

[ZGDL13] Z. Zhang, S. Gong, A.D. Dimitrovski, and H. Li. Time synchronization attack in smart grid: Impact and analysis. *Smart Grid, IEEE Transactions on*, 4(1):87–98, March 2013.

[ZGL+13] Y. Zhang, S. Gjessing, H. Liu, H. Ning, L. Yang, and M. Guizani. Securing vehicle-to-grid communications in the smart grid. *Wireless Communications, IEEE*, 20(6):66–73, December 2013.

[ZGLP11] Z. Zhang, S. Gong, H. Li, and C. Pei. Time stamp attack on wide area monitoring system in smart grid. *arXiv preprint arXiv:1102.1408*, 2011.

[ZH15] Yixuan Zhang and Jingsha He. A proactive access control model based on stochastic game. In *Computer Science and Network Technology (ICCSNT), 2015 4th International Conference on*, volume 1, pages 1008–1011. IEEE, 2015.

[Zha15a] Jiazi Zhang. *Topology Attacks on Power System Operation and Consequences Analysis*. PhD thesis, Arizona State University, 2015.

[Zha15b] Yichi Zhang. *Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment*. PhD thesis, University of Toledo, 2015.

[Zha15c] Hua Zhao. The simulation experiment and research on an improved cumulative sum anomaly detection method. In *Applied Mechanics and Materials*, volume 743, pages 219–225. Trans Tech Publ, 2015.

[Zha15d] Yao Zhao. *Data Inference in Cloud Computing and Smart Grids: A Grassmann Manifold Approach*. PhD thesis, University of Calgary, 2015.

[ZHH12] Saman Zonouz, Amir Houmansadr, and Parisa Haghani. Elimet: Security metric elicitation in power grid critical infrastructures by observing system administrators' responsive behavior. In *Dependable Systems and Networks (DSN), 2012 42nd Annual IEEE/IFIP International Conference on*, pages 1–12. IEEE, 2012.

[ZHX+15] Chunjie Zhou, Shuang Huang, Naixue Xiong, Shuang-Hua Yang, Huiyun Li, Yuanqing Qin, and Xuan Li. Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 45(10):1345–1360, 2015.

[ZJB10] Shanshan Zheng, Tao Jiang, and John S. Baras. Robust state estimation under false data injection in distributed sensor networks. In *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pages 1–5. IEEE, 2010.

[ZJCH14] Jianhua Zhang, Prateek Jaipuria, Aranya Chakrabortty, and Alefiya Hussain. A distributed optimization algorithm for attack-resilient wide-area monitoring of power systems: Theoretical and experimental methods. In *International Conference on Decision and Game Theory for Security*, pages 350–359. Springer, 2014.

[ZKSY14] Saman A. Zonouz, Himanshu Khurana, William H Sanders, and Timothy M. Yardley. Rre: A game-theoretic intrusion response and recovery engine. *IEEE Transactions on Parallel and Distributed Systems*, 25(2):395–406, 2014.

[ZLD+15] Bowen Zheng, Wenchao Li, Peng Deng, Léonard Gérard, Qi Zhu, and Natarajan Shankar. Design and verification for transportation system security. In *Proceedings of the 52nd annual design automation conference*, page 96. ACM, 2015.

[ZLL+13] Y. Zhao, T. Liu, Y. Liu, Y. Sun, and Y. Gu. Event-oriented cyber-physical fusion method for attack detection in smart grid. In *IEEE Innovative Smart Grid Technologies Asia*, November 2013.

[ZLW+10] T. Zhang, W. Lin, Y. Wang, S. Deng, C. Shi, and L. Chen. The design of information security protection framework to support smart grid. In *Power System Technology (POWERCON), 2010 International Conference on*, pages 1–5, October 2010.

[ZM] M. Zhu and S. Martínez. On resilient networked control systems against replay attacks. Draft.

[ZM11] M. Zhu and S. Martínez. Stackelberg-game analysis of correlated attacks in cyber-physical systems. In *American Control Conference (ACC), 2011*, pages 4063–4068, June 2011.

[ZM15a] Minghui Zhu and Sonia Martínez. *Distributed optimization-based control of multi-agent networks in complex environments*. Springer, 2015.

[ZM15b] Minghui Zhu and Sonia Martínez. Distributed resilient formation control. In *Distributed Optimization-Based Control of Multi-Agent Networks in Complex Environments*, pages 91–118. Springer, 2015.

[ZMRB11] Q. Zhu, M. McQueen, C. Rieger, and T. Başar. Management of control system information security: control system patch management. In *Proceedings of the Workshop on the Foundations of Dependable and Secure Cyber-Physical Systems (FDSCPS-11)*, pages 51–54, April 2011.

[ZNA15] Mohsen Zamanim, Brett Ninness, and Juan C. Agüero. On identification of networked systems with time-invariant topology. *IFAC-PapersOnLine*, 48(28):1184–1189, 2015. 17th IFAC Symposium on System Identification SYSID 2015.

[ZRZ+13] C. Zhang, Z. Ren, A. Zhang, Y. Zhang, and Y. Geng. Malicious data injection attack against power system state estimation based on orthogonal matching pursuit. In *Control Conference (ASCC), 2013 9th Asian*, pages 1–6, June 2013.

[ZS10] B. Zhu and S. Sastry. SCADA-specific intrusion detection/prevention systems: a survey and taxonomy. In *Preprints of the 1st workshop on Secure Control Systems, CPSWEEK 2010*, April 2010.

[ZS15] Jiazi Zhang and Lalitha Sankar. Implication of unobservable state-and-topology cyber-physical attacks. *arXiv preprint arXiv:1509.00520*, 2015.

[ZWJ15] Yudong Zhang, Shuihua Wang, and Genlin Ji. A comprehensive survey on particle swarm optimization algorithm and its applications. *Mathematical Problems in Engineering*, 2015, 2015.

[ZWS+11] Y. Zhang, L. Wang, W. Sun, R.C. Green, and M. Alam. Distributed intrusion detection system in a multi-layer network architecture of smart grids. *Smart Grid, IEEE Transactions on*, 2(4):796–808, December 2011.

[ZXLW13] L. Zhang, L. Xie, W. Li, and Z. Wang. Security solutions for networked control systems based on DES algorithm and improved grey prediction model. *International Journal of Computer Network and Information Security (IJCNIS)*, 6(1):78, 2013.

[ZYBV15] Xingsi Zhong, Lu Yu, Richard Brooks, and Ganesh Kumar Venayagamoorthy. Cyber security in smart DC microgrid operations. In *DC Microgrids (ICDCM), 2015 IEEE First International Conference on*, pages 86–91. IEEE, 2015.

[ZYLY15] X. Zhang, X. Yang, J. Lin, and W. Yu. On false data injection attacks against the dynamic microgrid partition in the smart grid. In *2015 IEEE International Conference on Communications (ICC)*, pages 7222–'7227, June 2015.

[ZYSH13] Y. Zhu, J. Yan, Y. Sun, and H. He. Risk-aware vulnerability analysis of electric grids from attacker's perspective. In *Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES*, pages 1–6, February 2013.

[ZYT+14] Y. Zhu, J. Yan, Y. Tang, Y.L. Sun, and H. He. Resilience analysis of power grids under the sequential attack. *Information Forensics and Security, IEEE Transactions on*, 9(12):2340–2354, December 2014.

[ZYT+15] Y. Zhu, J. Yan, Y. Tang, Y.L. Sun, and H. He. Joint substation-transmission line vulnerability assessment against the smart grid. *Information Forensics and Security, IEEE Transactions on*, 10(5):1010–1024, May 2015.

[ZYY15] Zhesheng Zhang, Wei Yuan, and Fanyu You. Power allocation of jamming attackers against pev charging stations: A game theoretical approach. In *Soft Computing and Pattern Recognition (SoCPaR), 2015 7th International Conference of*, pages 111–116. IEEE, 2015.

[ZZC15] Wente Zeng, Yuan Zhang, and Mo-yuen Chow. A resilient distributed energy management algorithm for economic dispatch in the presence of misbehaving generation units. In *Resilience Week (RWS), 2015*, pages 1–5. IEEE, 2015.

[ZZLN15] Lifu Zhang, Heng Zhang, Cunhua Li, and Buxi Ni. Optimal jamming attack scheduling in networked sensing and control systems. *International Journal of Distributed Sensor Networks*, 11(10):206954, 2015.