PHYSICAL LAYER SECURITY FOR SMART GRID COMMUNICATIONS

SAPTARSHI GHOSH

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI
MARCH 2021

PHYSICAL LAYER SECURITY FOR SMART GRID COMMUNICATIONS

by

SAPTARSHI GHOSH

DEPARTMENT OF ELECTRICAL ENGINEERING

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

INDIAN INSTITUTE OF TECHNOLOGY DELHI
MARCH 2021

Certificate

This is to certify that the thesis entitled **"Physical Layer Security for Smart Grid Communications"** being submitted by **Mr. Saptarshi Ghosh** to the Department of Electrical Engineering, Indian Institute of Technology Delhi, for the award of the degree of **Doctor of Philosophy** is the record of the bona-fide research work carried out by him under my supervision. In my opinion, the thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted either in part or in full to any other university or institute for the award of any degree or diploma.

Date:
New Delhi

(Prof. Manav Bhatnagar)
Professor
Department of Electrical Engineering
Indian Institute of Technology Delhi

Date:
New Delhi

(Prof. Bijaya K. Panigrahi)
Professor
Department of Electrical Engineering
Indian Institute of Technology Delhi

Acknowledgements

I would first like to thank my supervisor **Prof. Manav Bhatnagar** and co-supervisor **Prof. Bijaya K. Panigrahi** for their expert guidance, constant support, and immense encouragement throughout my Ph.D. program. Their invaluable suggestions and insightful discussions made me enjoy my research. Also, their enormous enthusiasm, honest dedication, and the quest for knowledge are truly inspirational. My sincere appreciation also extends to Prof. Ranjan Bose, Prof. Brejesh Lal, Dr. Ashu Verma, and Dr. Arpan Chattopadhyay for their beneficial feedback and suggestions during my work.

I acknowledge my friends for helping me in various phases of my research work through numerous discussions and valuable inputs. I also thank my colleagues for sharing my joys and sorrows and the amazing time I spent with them. Without their help, I would have faced many difficulties in continuing my Ph.D. program.

I feel obligated for having supportive supervisors and friends. I feel blessed for their unconditional care and concern.

Saptarshi Ghosh

Abstract

Monitoring a physical process and estimating its state variables is an important function needed for the proper working of a smart grid. As such, performing the aforementioned function reliably and securely is of utmost importance. State estimation in a smart grid can be properly operated with wireless sensor networks (WSN) that provide low-cost and robust monitoring solutions. However, the broadcast nature of any wireless medium makes the WSNs prone to cyber-attacks. Jamming is one such attack that severely deteriorates the communication network's performance so that the measurements do not reach the destination. By congesting the communication network, jamming introduces a delay in the network. In this work, we model the delay experienced by time-critical operations in a smart grid network due to jamming and investigate its mitigation technique. False data injection (FDI) attacks are launched by an adversary to modify the measurements of a physical system that could manipulate the state variables' estimated values which can mislead the system operator and jeopardize the physical process. In this dissertation, we have investigated the issue of detecting FDI attacks on state estimation in WSN enabled smart grid, where inactive sensor nodes (SNs) of the network is compromised by the adversary to launch the attack over wireless channels. Both jamming and FDI attacks require the attacker to possess knowledge about some parameters of the physical process. In this regard, WSNs are also vulnerable to eavesdropping and signal interception that can disclose internal parameters of the physical process. Among other physical layer security techniques, allocating optimal power to transmit data over wireless channels is an important technique to secure wireless networks against cyber-attacks. Another major challenge in using WSNs for monitoring tasks and securing it against cyber attacks is the limited

capacity of the batteries powering the SNs. In this regard, wireless powered sensor networks (WPSNs) where the individual SNs follows harvest-then- transmit approach is being explored, extending the lifetime of the SNs used in monitoring critical functions. The threats from a sensor node, capable of harvesting energy from RF signal, are investigated in this thesis by studying its effects on the operation of a wireless network. Further, the SNs are operated by third parties and have the onboard processing power. Therefore, distributed resource allocation techniques are best-suited for WSNs. In this regard, game theory is used extensively as a tool for distributed resource allocation where there exists competition among the various nodes of the network. In this dissertation, the problem of physical layer security for WPSNs for smart grid communication is addressed by proposing various game-theory based distributed resource allocation. For complex games, the solution is obtained with Q-learning based algorithms. Different from existing learning techniques, we have proposed Q-learning methods that converge in environments with multiple decision-makers.

सार

एक भौतिक प्रक्रिया की निगरानी करना और उसके स्थिति चर का आकलन करना स्मार्ट ग्रिड के समुचित कार्य के लिए महत्वपूर्ण है। जैसे, उपर्युक्त कार्य को मज़बूती से और सुरक्षित रूप से करना अत्यंत महत्वपूर्ण है। वायरलेस सेंसर नेटवर्क (डब्लूएसएन) द्वारा एक स्मार्ट ग्रिड की स्थिति का आकलन मजबूत और कम लागत वाले तरीके से किया जा सकता है। हालांकि, की प्रसारण प्रकृति कोई भी वायरलेस माध्यम डब्लूएसएन को साइबर हमलों का शिकार बनाता है। जैमिंग एक ऐसा हमला है जो संचार नेटवर्क के प्रदर्शन को बुरी तरह से खराब कर देता है ताकि माप गंतव्य तक न पहुंच सके। संचार नेटवर्क को भीड़ कर, नेटवर्क में देरी का परिचय देता है। इस काम में, हम स्मार्ट ग्रिड नेटवर्क में समय-महत्वपूर्ण संचालन द्वारा अनुभव की गई देरी को जाम करने और इसकी शमन तकनीक की जांच करने के लिए तैयार करते हैं। गलत डेटा इंजेक्शन (एफडीआई) हमलों को एक भौतिक प्रणाली के माप को संशोधित करने के लिए शुरू किया जाता है जो स्थिति के अनुमानित मूल्यों में हेरफेर कर सकता है जो सिस्टम ऑपरेटर को भ्रमित कर सकता है और भौतिक प्रक्रिया को खतरे में डाल सकता है। इस शोध प्रबंध में, हमने डब्ल्यूएसएन सक्षम स्मार्ट ग्रिड में स्थिति के आकलन पर एफडीआई के हमलों का पता लगाने के मुद्दे की जांच की है, जहां नेटवर्क के निष्क्रिय सेंसर नोड्स (एसएन) वायरलेस चैनलों पर हमले शुरू करने के लिए विरोधी द्वारा समझौता किया जाता है। जैमिंग और एफडीआई दोनों हमलों में हमलावर को भौतिक प्रक्रिया के कुछ मापदंडों के बारे में जानकारी रखने की आवश्यकता होती है। इस संबंध में, डब्ल्यूएसएन भी ईव्सड्रॉपिंग और सिग्नल अवरोधन के लिए कमजोर हैं जो भौतिक प्रक्रिया के आंतरिक मापदंडों का खुलासा कर सकते हैं। अन्य तकनीक के बीच भौतिक परत सुरक्षा, वायरलेस चैनलों पर डेटा संचारित करने के लिए इष्टतम शक्ति आवंटित करना साइबर हमलों के खिलाफ वायरलेस नेटवर्क को सुरक्षित करने के लिए महत्वपूर्ण तकनीक है। एसएन को शक्ति देने वाली बैटरियों की सीमित क्षमता , कार्यों की निगरानी और साइबर हमलों के खिलाफ डब्ल्यूएसएन का उपयोग करना एक और बड़ी चुनौती है । इस संबंध में, वायरलेस संचालित सेंसर नेटवर्क (डब्ल्यूपीएसएन) जहां व्यक्तिगत एसएन महत्वपूर्ण निगरानी के लिए अपने जीवनकाल का विस्तार करते हैं आसपास के आरएफ संकेतों से ऊर्जा निकालकर कार्य करता है। एक वायरलेस नेटवर्क के संचालन पर इसके प्रभावों का अध्ययन करके, आरएफ सिग्नल से ऊर्जा लेने में सक्षम सेंसर नोड से होने वाले खतरों की जांच की जाती है। इसके

अलावा, एसएन तीसरे पक्ष द्वारा संचालित होते हैं और एसएन में होते हैं प्रसंस्करण शक्ति। इसलिए, वितरित संसाधन आवंटन तकनीक सबसे उपयुक्त हैं डब्ल्यूपीएसएन के लिए। इस संबंध में, गेम थ्योरी वितरित संसाधन आवंटन के लिए एक उपकरण के रूप में बड़े पैमाने पर उपयोग किया जाता है जहां प्रतिस्पर्धा मौजूद है नेटवर्क के विभिन्न नोड्स में। इस शोध प्रबंध में, स्मार्ट ग्रिड संचार के लिए डब्ल्यूपीएसएन में भौतिक परत सुरक्षा की समस्या को विभिन्न गेम-थ्योरी आधारित संसाधन आवंटन का प्रस्ताव करके संबोधित किया गया है। जटिल खेलों के लिए, क्यू-लर्निंग आधारित एल्गोरिदम के साथ समाधान प्राप्त किया जाता है। मौजूदा शिक्षण तकनीकों से अलग, हमने क्यू-लर्निंग विधियों का प्रस्ताव किया है जो कई निर्णय निर्माताओं के वातावरण में परिवर्तित होती हैं।

Table of Contents

List of Figures

List of Tables

Abbreviations

AWGN	Additive White Gaussian Noise
BG	Bayesian Game
BNE	Bayesian Nash Equilibrium
CPS	Cyber-Physical System
CRN	Cognitive Radio Network
CSI	Channel State Information
CSMA-CA	Carrier Sense Multiple Access Collision Avoidance
EH	Energy Harvest
FDI	False Data Injection
GOOSE	Generic Object Oriented Substation Event
HES	Hybrid Energy Source
IED	Intelligent Electronic Device
KKT	Karush-Kuhn-Tucker
LP	Linear Programming
MD	Measurement Device
MRC	Maximal Ratio Combining
NCG	Non-cooperative game
NE	Nash Equilibrium
ODE	Ordinary Differential Equation
PB	Power Beacon
PoA	Price of Anarchy
POMDP	Partially Observable Markov Decision Process
PR	Primary Receiver

PT	Primary Transmitter
QoS	Quality of Service
QSI	Queue State Information
RF	Radio Frequency
RSE	Robust Stackelberg Equilibrium
SE	Stackelberg Equilibrium
SN	Sensor Node
SNR	Signal-to-Noise Ratio
SR	Secondary Receiver
SSG	Stochastic Stackelberg Game
ST	Secondary Transmitter
SWIPT	Simultaneous Wireless Information and Power Transfer
WLAN	Wireless Local Area Network
WPSN	Wireless Powered Sensor Network
WPT	Wireless Power Transfer
WSN	Wireless Sensor Network

Notations

D_{m_k}	Average number of time slots k^{th} IED has to wait for m_k re-transmissions
ϕ_n^k	Average
β_n	Average
p_n^k	Transmit power allocated by k^{th} IED to the n^{th} channel
h_t^I	Action history of player I at time t
h_t^J	Action history of player J at time t
σ	Strategies of players I
τ	Strategies of players J
γ_{m_l}	Bayesian Game
δ_{m_c}	Bayesian Nash Equilibrium
$p(t_c, \boldsymbol{u})$	Mixed strategy of central controller
$q(t_a, \boldsymbol{v})$	Mixed strategy of Attacker
η	Efficiency with which energy can be harvested from the received signal
ρ	Power splitting ratio
$\tilde{n}_{i,m}$	Number of time slots of duration τ allocated to MD_i in time-frame m
$e_{i,m}$, $d_{i,m}$	State of energy and data buffer of MD_j in time-frame m
e_i^{max}, d_i^{max}	Maximum size of the energy and data buffer at MD_i
$\tilde{r}_{i,m}$	Incentive offered by MD_i in time-frame m to cooperative jammers
ϑ	Incentive per unit successfully transmitted bits