ENHANCED SECRECY TECHNIQUES IN THE PRESENCE OF A HYBRID ATTACKER FOR A RESOURCE-CONSTRAINED ENVIRONMENT

BHAWNA AHUJA

BHARTI SCHOOL OF TELECOMMUNICATION
TECHNOLOGY AND MANAGEMENT
INDIAN INSTITUTE OF TECHNOLOGY DELHI

July 2021

ENHANCED SECRECY TECHNIQUES IN THE PRESENCE OF A HYBRID ATTACKER FOR A RESOURCE-CONSTRAINED ENVIRONMENT

by

BHAWNA AHUJA

BHARTI SCHOOL OF TELECOMMUNICATION TECHNOLOGY AND MANAGEMENT

Submitted

in fulfillment of the requirements of the degree of

Doctor of Philosophy

to the

INDIAN INSTITUTE OF TECHNOLOGY DELHI

July 2021

Certificate

This is to certify that the thesis entitled **"Enhanced Secrecy Techniques in the Presence of A Hybrid Attacker for A Resource-constrained Environment"** being submitted by **Ms. Bhawna Ahuja** to the Bharti School of Telecommunication Technology and Management, Indian Institute of Technology Delhi, for the award of the degree of **Doctor of Philosophy** is the record of bonafide 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.

Dr. Ranjan Bose
Professor
Department of Electrical Engineering
and
Bharti School of Telecommunication
Technology & Management
Indian Institute of Technology Delhi

Date:
Place: New Delhi

Acknowledgements

I am deeply indebted to my supervisor Prof. Ranjan Bose for giving me the illuminous guidance, continued support and wise counsel throughout my research without which, it could not have been possible to bring this thesis into its present form. Apart from the academic advice, his constant encouragement and belief in my capability have been responsible in completing my research work within reasonable time-frame.

I am grateful to Prof. Brajesh Lall, Prof. Shankar Prakriya, Prof. Kolin Paul and Prof. Vinay Ribeiro for providing constructive feedback to enhance the quality of research work. It is an immense pleasure to express my sincere thanks and appreciation to Dr. Deepak Mishra for providing persistent support and timely suggestions towards my research work. It has been a greatly enriching experience for me to work with him.

My deep sense of appreciation is due to my mother-in-law and father-in-law for their moral support, love and affection, silent sacrifices and incessant encouragement which enabled me to keep going throughout. I extend my unending thanks and utmost appreciation to my parents for the constant emotional and moral support they have provided me and without whom I would not have reached so far.

I am extremely beholden to my husband Mr. Janender Ahuja who has stood as a pillar of strength for me with unending faith and empathy. I am not able to find words to express my feelings for my little angel Arshpreet who was really deprived of her mother's attention and care for a considerable period but whose love never wavered.

Finally, I am indebted and grateful to the almighty for helping me in this endeavor.

Bhawna Ahuja

Abstract

Broadcast and superposition nature of the wireless channel makes the wireless networks vulnerable to passive attacks such as eavesdropping and active attacks such as jamming. In the former attack, the legitimate transmission is tapped by the attacker to compromise the confidentiality and security, while in the latter type, the legitimate reception is impaired through generating the deliberate interference in the network, thus causing a denial of service. Therefore, secure communication transfer becomes quite challenging, especially in the resource-constrained networks like the Internet of Things (IoT). Due to low implementation complexity, physical layer security has attracted considerable attention to address the security vulnerability against passive eavesdropping attack. In this thesis, we address the security concern raised by a potential advanced adversary referred as a hybrid attacker that possesses capabilities to perform eavesdropping as well as jamming in a resource-constrained and stochastic environment. In the first part of the thesis, in pursuance to understand the behavior of a potential green hybrid attacker, a novel framework is proposed for optimizing its efficacy while considering the underlying energy consumption. We maximize the attacker energy efficiency (AEE) in secure IoT by proposing a non-trivial mode-switching based solution methodology for jointly global-optimal attacking mode, eavesdropping rate, and jamming power. Via analytical studies, the proposed architecture is demonstrated to provide about 45% improvement in AEE over relevant benchmarks.

In real-world implementations, the precise location of nodes is unknown, and hence the inter-node distance is a random parameter. Since secrecy capacity is a function of legitimate link distance, as well as, the attacker link distance, it is imperative to do accurate characterization of security performance to assess the impact of random

inter-node separations when all the link distances are unknown. To address this issue, we develop a comprehensive quality-of-service (QoS)-aware physical layer security framework using inter-node distance-based probabilistic distribution functions in the second part of this thesis. The proposed model takes into account the practical limits arising out of underlying QoS requirements, which include the maximum distance between legitimate users driven by transmit power and receiver sensitivity. In this regard, a novel concept of eavesdropping zone is also introduced. Via an analytical framework, the secrecy outage performance is characterized for both eavesdropping and jamming attacks. From the results, the threshold on the maximum distance between legitimate users and deployment range are obtained to achieve the desired QoS. The impact of the optimal eavesdropping range and the jamming power are also examined, and the conditions are investigated where eavesdropping outperforms jamming.

The third part of this thesis focuses on a more sophisticated hybrid attacker that is capable of performing eavesdropping and jamming simultaneously using full-duplex (FD) communication. Our first goal is to evaluate the secrecy performance in the presence of such a potential attacker by considering the unavailability of incomplete channel state information for all the ungoverned links including eavesdropping, jamming and self-interference links. The proposed analysis considers imperfect self-interference at the attacker's end in its modeling. The closed-form expressions have been obtained for intercept probability under generalized as well as special cases. The results obtained facilitate in investigating the impact of fading and residual self-interference under FD attack. We then propose an optimization framework aiming to enhance secrecy performance in the presence of FD hybrid attacker in an IoT network consisting of multiple users. Via linear programming and graph-theoretic tools, fair subcarrier allocation is obtained for the objective of minimizing maximum intercept probability among the given set of users. The performance of proposed schemes is evaluated in terms of optimal intercept probability and complexity. The adaptability of the proposed algorithms in practical scenarios is simulated over narrow-band (NB)-IoT protocol specifications. Performance studies demonstrate that the proposed algorithms offer significantly high secrecy performance against FD attacker while keeping the complexity low.

The proposed solutions contribute to secrecy enhancement of the resource-constrained wireless networks, as well as, offer hybrid attacker analysis for secrecy performance.

Deeper insights and understanding of secrecy-aware system design is presented through extensive analytical formulations. The analytical formulations validated through numerical results thereon offer good reference to the design considerations for emerging application areas including IoT, device-to-device networks and wireless sensor networks.

सार

वायरलेस चैनल का प्रसारण और सुपरपोजिशन प्रकृति वायरलेस नेटवर्क को निष्क्रिय हमलों जैसे कि चोरी छुपे सुनना या ईव्सड्रॉपिंग और सक्रिय हमलों जैसे जैमिंग के प्रति संवेदनशील बनाती है। पूर्व हमले में, वैध संचरण को हमलावर द्वारा गोपनीयता और सुरक्षा से समझौता करने के लिए टैप किया जाता है, जबकि बाद के प्रकार में, नेटवर्क में जानबूझकर हस्तक्षेप उत्पन्न करने के माध्यम से वैध रिसेप्शन खराब हो जाता है, इस प्रकार सेवा से इनकार कर दिया जाता है। इसलिए, सुरक्षित संचार हस्तांतरण काफी चुनौतीपूर्ण हो जाता है, विशेष रूप से इंटरनेट ऑफ थिंग्स (आईओटी) जैसे संसाधन-विवश नेटवर्क में। कार्यान्वयन की कम जटिलता के कारण, ईव्सड्रॉपिंग हमले के खिलाफ सुरक्षा भेद्यता को संबोधित करने के लिए भौतिक परत सुरक्षा ने काफी ध्यान आकर्षित किया है। इस थीसिस में, हम एक संभावित उन्नत विरोधी द्वारा उठाए गए सुरक्षा चिंता को संबोधित करते हैं जिसे हाइब्रिड हमलावर के रूप में संदर्भित किया जाता है, जिसमें संसाधन-विवश और स्टोकेस्टिक वातावरण में छिपकर बातें सुनने के साथ-साथ जैमिंग करने की क्षमता होती है । थीसिस के पहले भाग में, एक संभावित ग्रीन हाइब्रिड हमलावर के व्यवहार को समझने के लिए, अंतर्निहित ऊर्जा खपत पर विचार करते हुए इसकी प्रभावकारिता को अनुकूलित करने के लिए एक नया ढांचा प्रस्तावित किया गया है। हम संयुक्त रूप से वैश्विक-इष्टतम आक्रमण मोड, छिपकर बातें सुनने की दर, और जैमिंग करने की शक्ति के लिए एक गैर-तुच्छ मोड-स्विचिंग आधारित समाधान पद्धति का प्रस्ताव करके सुरक्षित आईओटी में हमलावर ऊर्जा दक्षता (एईई) को अधिकतम करते हैं। विश्लेषणात्मक अध्ययनों के माध्यम से, प्रस्तावित वास्तुकला को प्रासंगिक बेंचमार्क पर एईई में लगभग 45% सुधार प्रदान करने के लिए प्रदर्शित किया गया है।

वास्तविक दुनिया के कार्यान्वयन में, नोड्स का सटीक स्थान आमतौर पर अज्ञात होता है, और इसलिए अंतर-नोड दूरी एक यादृच्छिक पैरामीटर है। चूंकि गोपनीयता क्षमता, वैध लिंक दूरी के साथ-साथ हमलावर लिंक दूरी का एक कार्य है, इसलिए सभी लिंक दूरी अज्ञात होने पर यादृच्छिक इंटर-नोड अलगाव के प्रभाव का आकलन करने के लिए सुरक्षा प्रदर्शन का सटीक लक्षण वर्णन करना अनिवार्य है। इस समस्या को हल करने के लिए, हम इस थीसिस के दूसरे भाग में अंतर-नोड दूरी-आधारित संभाव्य वितरण कार्यों का उपयोग करके

एक व्यापक गुणवत्ता-सेवा (क्यूओएस)-जागरूक भौतिक परत सुरक्षा ढांचा विकसित करते हैं। प्रस्तावित मॉडल अंतर्निहित क्यूओएस आवश्यकताओं से उत्पन्न होने वाली व्यावहारिक सीमाओं को ध्यान में रखता है, जिसमें ट्रांसमिट पावर और रिसीवर संवेदनशीलता द्वारा संचालित वैध उपयोगकर्ताओं के बीच अधिकतम दूरी शामिल है। इस संबंध में, ईव्सड्रॉपिंग ज़ोन की एक नई अवधारणा भी पेश की गई है। एक विश्लेषणात्मक ढांचे के माध्यम से, गोपनीयता आउटेज प्रदर्शन को ईव्सड्रॉपिंग और जैमिंग हमलों दोनों के लिए विशेषता है। परिणामों से, वांछित गोपनीयता प्रदर्शन प्राप्त करने के लिए वैध उपयोगकर्ताओं और परिनियोजन सीमा के बीच अधिकतम दूरी पर सीमा प्राप्त की जाती है। इष्टतम ईव्सड्रॉपिंग रेंज और जैमिंग पावर के प्रभाव की भी जांच की जाती है और उन स्थितियों की जांच की जाती है जहां ईव्सड्रॉपिंग जैमिंग से बेहतर प्रदर्शन करता है।

इस थीसिस का तीसरा भाग एक अधिक परिष्कृत हाइब्रिड हमलावर पर केंद्रित है जो पूर्ण-द्वैध (एफडी) संचार का उपयोग करके एक साथ छिपकर बात करने और जाम करने में सक्षम है। हमारा पहला लक्ष्य ऐसे संभावित हमलावर की उपस्थिति में गोपनीयता के प्रदर्शन का मूल्यांकन करना है, जिसमें सभी अनियंत्रित लिंक के लिए अधूरी चैनल स्थिति की जानकारी की अनुपलब्धता पर विचार करना, जिसमें छिपकर बातें करना, जाम करना और आत्म-हस्तक्षेप शामिल हैं। प्रस्तावित विश्लेषण अपने मॉडलिंग में हमलावर के अंत में अपूर्ण आत्म-हस्तक्षेप पर विचार करता है। क्लोज्ड-फॉर्म एक्सप्रेशन सामान्यीकृत के साथ-साथ विशेष मामलों के तहत इंटरसेप्ट प्रायिकता के लिए प्राप्त किए गए हैं। प्राप्त परिणाम एफडी हमले के तहत लुप्त होती और अवशिष्ट आत्म-हस्तक्षेप के प्रभाव की जांच में सुविधा प्रदान करते हैं। इसके बाद हम कई उपयोगकर्ताओं वाले आईओटी नेटवर्क में एफडी हाइब्रिड हमलावर की उपस्थिति में गोपनीयता के प्रदर्शन को बढ़ाने के उद्देश्य से एक अनुकूलन ढांचे का प्रस्ताव करते हैं। रैखिक प्रोग्रामिंग और ग्राफ-सैद्धांतिक उपकरणों के माध्यम से, उपयोगकर्ताओं के दिए गए सेट के बीच अधिकतम अवरोध संभावना को कम करने के उद्देश्य से उचित उपवाहक आवंटन प्राप्त किया जाता है। प्रस्तावित योजनाओं के प्रदर्शन का मूल्यांकन इष्टतम अवरोधन संभाव्यता और जटिलता के संदर्भ में किया जाता है। व्यावहारिक परिदृश्यों में प्रस्तावित एल्गोरिदम की अनुकूलन क्षमता संकीर्ण-बैंड आईओटी प्रोटोकॉल विनिर्देशों पर सिम्युलेटेड है। प्रदर्शन अध्ययनों से पता चलता है कि प्रस्तावित एल्गोरिदम जटिलता को कम रखते हुए एफडी हमलावर के खिलाफ काफी उच्च गोपनीयता प्रदर्शन प्रदान करते हैं।

प्रस्तावित समाधान संसाधन-विवश वायरलेस नेटवर्क की गोपनीयता बढ़ाने में योगदान करते हैं, साथ ही गोपनीयता प्रदर्शन के लिए हाइब्रिड हमलावर विश्लेषण प्रदान करते हैं। व्यापक विश्लेषणात्मक फॉर्मूलेशन के माध्यम से गोपनीयता-जागरूक प्रणाली डिजाइन की गहरी अंतर्दृष्टि और समझ प्रस्तुत की जाती है। संख्यात्मक परिणामों के माध्यम से मान्य विश्लेषणात्मक फॉर्मूलेशन आईओटी, डिवाइस-टू-डिवाइस नेटवर्क और वायरलेस सेंसर नेटवर्क सहित उभरते अनुप्रयोग क्षेत्रों के लिए डिजाइन विचारों के लिए अच्छा संदर्भ प्रदान करते हैं।

Table of Contents

List of Figures

List of Algorithms

List of Abbreviations

AEE	Attacker energy efficiency
AWGN	Additive white Guassian noise
BER	Bit error rate
CDF	Cumulative distribution function
CSI	channel state information
CUE	Cellular user equipment
D2D	Device-to-device network
DMC	Discrete memoryless channel
DoS	Denial-of-Service
DUE	Device-to-device users equipment
EE	Energy efficiency
EIRP	Effective isotropically radiated power
FCC	Federal communications commission
FD	Full-duplex
GS	Golden section
HD	Half-duplex
ILP	Integer linear program

ISM	Industrial, scientific and medical
IoT	Internet of things
LBAP	Linear bottlencek assignment problem
MIMO	Multiple-input multiple-output
MISO	Multiple input single ouput
NB	Narrow band
OFDMA	Orthogonal frequency division multiple access
PDF	Probability distribution function
PLS	Physical layer security
PPP	Poisson Point Process
PT	Prospect Theory
QoS	Quality of Service
ROA	Relaxation and Ordering based Allocation
SC	Secrecy capacity
SI	Self-interference
SIR	Signal-to-interference ratio
SINR	Signal-to-interference-noise ratio
SNR	Signal-to-noise ratio
SOP	Secrecy outage probability
SRD	Short Range Device
TAPM	Threshold adaptive perfect matching
UHF	Ultra high frequency