VENUS CyberSecurity Corp.
Ottawa, ON K1E3W3
(613) 216-9474
ibrahimee@ieee.org
alhaol.com

Ibrahim AbuAlhaol

Research Statement

Background

My **Ph.D. research (2005-2008)** started at the center for wireless communications at the University of Mississippi, United States. I contributed to the development of the project titled "Adaptive Resource Allocations to Enhance the Reliability of Communication Link for Unmanned Airborne Vehicles (UAVs)". I proposed four protocols to maximize the UAV mission range and the transmission rate, and to minimize the power consumption in the down-link communication. The proposed protocols are: Channel State Detection Protocol (CSDP), Best Hopping Sequence Selection Protocol (BHSSP), Adaptive Power Control Protocol (APCP), and Communication Loss Recovery Protocol (CLRP). In another project related to my **Ph.D. research**, a cooperative relay-based resource allocation technique was proposed for MIMO-OFDM system. In this technique, sub-channels allocation, M-QAM modulation order, and power distribution among different sub-channels in the relay-based MIMO-OFDM system were jointly optimized according to the channel state information (CSI) of the relay and the direct link. The optimized cooperative relay-based system enabled exploiting diversities in the frequency, space, and time to maximize system power efficiency.

During my work as an **Assistant Professor (2009-2014)** at Khalifa University, I was the principle investigator in a research proposal titled "**Vehicular ad-hoc networks (VANETs) for intelligent transportation systems (ITSs): Enhancing the safety and the traffic management in United Arab Emirates**". The research consisted of three sub-projects: the design of efficient cooperative schemes, the development of channel estimation/tracking algorithms, and the design of a cooperative OFDM scheme. In a second research grant, I worked on a project titled "**Cross-Layer Design for Secure Land Transport Systems**". The long-term goal of this research project is to develop both fundamental theories and practical designs of efficient, secure and safe vehicular networks. To achieve the goal, existing technologies for various layers (i.e., all major layers of the Open System Interface (OSI) stack of protocols) were examined.

In my role as **Cyber-Security researcher (2014-2015)** at Carleton University, I worked on introducing adds-on algorithms on top of AES encryption and RSA key exchange standards to enhance communication privacy. Millions of users depend on on-line services (e.g., email, chatting, and VOIP) to communicate and to accomplish daily activities. Such on-line communications are highly dependent on the service providers' capabilities. The communication security of users is extremely important and highly considered by service providers to sustain their credibility and attain customers' loyalty and trust. Even if service providers succeeded in reducing external

attacks by adopting advanced and complicated security mechanisms, such mechanisms do not address insider attacks and therefore is not guaranteeing privacy. A better solution that achieves security and privacy, and help in reducing risks of outsider and insider access to communication data is by utilizing end-to-end encryption tools. In this research project, an innovative proposal was presented to provide users privacy and improve security in a fast and easy to implement algorithms through the use of RAND, FLIP and SHIFT/MAP algorithms. The proposed solution was recommended to the development team at XAHIVE.com (industry partner) for integration and testing.

Current Research

In my current work as a **Cyber-Security research engineer (2015-present)** at VENUS CyberSecurity Corporation, I collaborates with engineers and managers in industry, government, and academia, with extensive experience in cyber-security. In my current work, I am conducting research on physical layer security of device-to-device (D2D) communication. D2D enables the efficient use of wireless system resources (i.e., power and spectrum) and promotes users' privacy but increases the possibility of cyber attacks due to the limitations of current D2D wireless security infrastructure. D2D communication has attracted researchers in recent years but with little attention to the security aspect of D2D communication. Physical layer security solutions proposed, thus far, are difficult to implement using wireless devices currently available and lack the capability to evaluate using security measures. In my research, the answers to three important questions are investigated. Can we evaluate D2D security threats using quantitative measures? Can we employ cross-layer wireless system designs to reduce the threat of attack and the losses after attack? Can we design flexible systems with multiple security levels that trade-off agility and security based on user requirements, circumstances, and reliable security measures?

Many stakeholders will benefit from this research findings. Canadian entrepreneurs, made aware of the security risks in D2D communication today, will design new differentiated products and services with secure D2D wireless links for the global market. The Government of Canada and the Government of Ontario will secure critical government infrastructure against new threats associated with emerging technologies, including the Internet of Things (IoT) and smart cities. Managers of Canadian companies in the Information and Communications Technology (ICT) sector will be able to better assess the security implications of new D2D wireless technologies, providing an advantage to their firms.

In another multiphase project titled: "**Improving cybersecurity by operationalizing collective intelligence with artificial intelligence**". The main objective is to integrate collective intelligence and artificial intelligence to automate the research process that start with initiating Cybersecurity problem, followed by collection of evidences to support the problem, validating the evidences, collecting solutions, validating the solutions, and finally synthesize the outcomes in a compelling taxonomy. Each step in the process involves prototyping and experiments to validate that it results in the intended outcomes.

Future Research

Previous work contributes to the cyber physical D2D security by introducing the concept of continuous authenticity and proposing a security scoring (***SeS***) for measuring security. Using *SeS*, attacks are detected at the physical layer without requiring intensive computations at higher layers of the software stack. In addition, implementing security at the physical layer will complement the security of upper layers of the protocol stack and improve the overall system security. The security risk evaluation in **Fig. 1** emphasizes that when the attacker has enough capability with simple ineffective security in a system such as D2D, the attack risk is High (top right quadrant). Using security scoring measure (i.e., *SeS*, we can improve the system effectiveness and therefore the risk is Medium as shown in the top left quadrant in **Fig. 1**. Utilizing this score to trigger the multi-level multi-layer design as proposed in **Fig. 2** will degrade the capability of the attacker and minimize the risk, which result in very low attack risk (bottom left quadrant in **Fig. 1**). The use of security measure in multi-level multi-layer response system will result in improving security effectiveness and in reducing attacker capabilities.

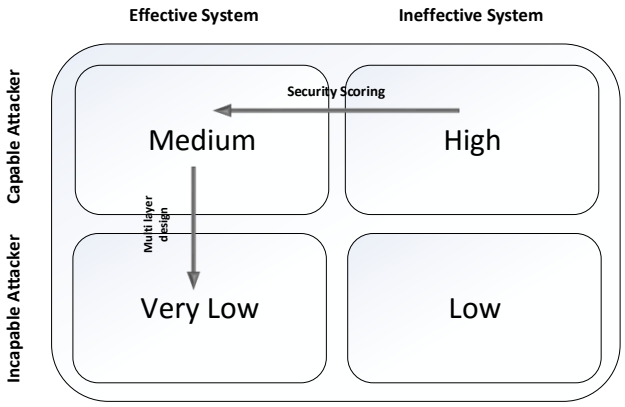

Fig.1: Security Risk can be reduced using security measure and multi level system design

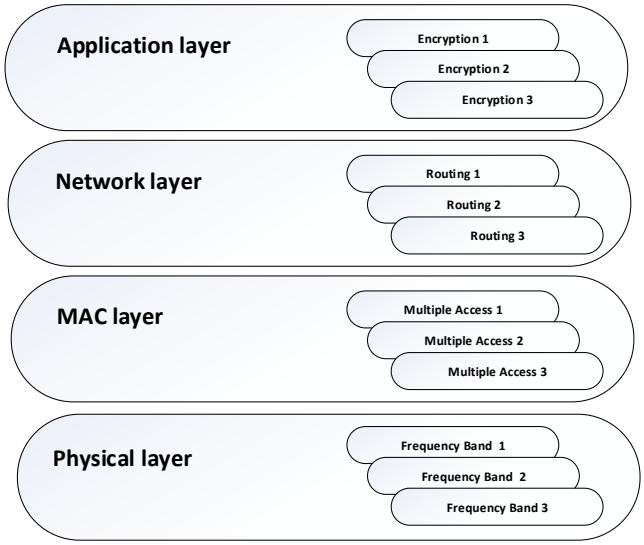

Fig.2: Agile multi-level multi-layer response

Future extensions include *(i)* designing legitimacy pattern that enhances privacy as well as improving security, *(ii)* coordination mechanisms to implement the agile multi-level multi-layer defensive response proposed in **Fig. 2** enabled by security scoring, and *(iii)* enfolding insights from other domains of inquiry (e.g., the social and behavioral sciences) to design improved legitimacy patterns to further improve security

I am confident in my ability to undertake high-quality research in cyber physical systems, to publish the results of my intended work, and to continue the trajectory of my current research. Future research directions will include cross-layer design of authentication patterns that enhance privacy while improving security and enfolding knowledge from social and behavioral sciences to design stronger authentication patterns that thwart attackers. I want to emphasize that I am very motivated to collaborate with faculties in your department to attract external funds and graduate students.