Secure Device Discovery in Big Data Communications Networks: Opportunities and Challenges

Shahab Tayeb*, Adrian Ruiz, Shahram Latifi
Department of Electrical and Computer Engineering, University of Nevada, Las Vegas, NV, USA.

* Corresponding author. Email: Shahab.Tayeb@unlv.edu
Manuscript submitted May 12, 2018; accepted July 23, 2018.
doi: 10.17706/ijeeee.2019.9.2.108-115

Abstract: This manuscript reviews the device to device (D2D) discovery in a dynamically changing topology. The discovery protocols covered focus on the first and second layers of the TCP/IP reference model, with a focus on time-sensitive protocols. These protocols can be categorized as wake-up scheduling, contact-probing intervals, and slotted channel structure. Such techniques allow nodes to stay idle or asleep often in a network, but also receive and transmit information when needed. Since device discovery is usually time and energy consuming, many of the mentioned protocols attempt to lower both costs. The goal of this manuscript is to provide information on time-based D2D discovery protocols. Given the prevalence of transient sensors in the Internet of Things, efficient dynamic device discovery remains a paramount issue for large-scale deployment of IoT. A key issue in a hierarchical topology is to perspicaciously and efficiently identify and utilize the nearest available resource. We conclude that the existing discovery mechanisms do not consider the introduced overhead and are designed without consideration of the real-time computation requirements.

Key words: Big data networks, device discovery, internet of things.

1. Introduction

Internet of Things (IoT) networks mark the next frontier of a new digital revolution. IoT allows companies to increase productivity, city services to converge, vehicles to become autonomous, and homes to become smarter. There has been much research on the design, evaluation, testing, and verification of CPS and its associated IoT. Nonetheless, research on the development of security models and frameworks for IoT networks is very limited. A key challenge is that security solutions for IoT should not hinder the openness of the network, nor should they introduce additional latency or overhead to communications across the network. These requirements are achieved by incorporating security into the design of IoT infrastructures. This project is focused on two main principles: “adaptive security architecture” and “IoT-based CPS or ICPS” both of which are listed on Gartner’s 2017 top 10 strategic technology trends.

ICPS are increasingly gaining momentum and there have been global efforts to standardize the different aspects of IoT and its real-life applications. ICPS not only has the support of providers and business-end giants such as IBM, HP, Intel, Microsoft, and Cisco, it is also fed by innovative services of the so-called pillars of today’s consumer-oriented Internet, namely: Apple, Google, and Amazon. IoT networks utilize traditional networking protocols operating at physical and data link layers as well as some newer protocols and standards that are mainly designed for IoT applications. 802.15 wireless personal area network (WPAN) standards are used for short-range communications, typically between 1 m and 100 m, such as 802.15.1

(Bluetooth compatible) and 802.15.4 (ZigBee compatible). Several short-range wireless protocols also support communications such as near-field communication (NFC) with a proximity of centimeters rather than meters. Standards such as IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) offer low-power IoT objects with smaller encapsulation by compressing the header. Due to the diversity of protocols and technologies surrounding the ICPS and because of the heterogeneity of devices connected to IoT, dynamically discovering devices is an important and challenging task.

The IoT is composed of many layers of technologies, each with its own set of challenges. Smart devices are now capable of gathering and curating sensed data which makes them more susceptible to being targeted by a variety of attack types from single target impersonation, rogue nodes, and privileged access to batched ones such as botnets and DDoS. This study aims to advance insight to IoT and identify the challenges with device discovery while attempting to develop methodologies to guard against cyber-attacks that can penetrate such techniques through a wide range of heterogeneous devices. New generations of devices bring along a newer and more sophisticated generation of discovery requirements and security needs. This concern is addressed by preventing the problem from happening through integrating security in design. ICPS lack a secure design for implementation and are prone to attacks, because they are complex. ICPS utilize a wide array of protocol and technology concepts such as Application Programming Interfaces (APIs), sensor-equipped edge devices, and messaging protocols. Figure 1 illustrates an array of possible ICPS vertical markets.

2. Device Discovery

2.1. Common Device Discovery Techniques

Long-Term Evolution Advanced (LTE) is a standard for high-speed wireless communication for mobile devices, and increases the capacity and speed [1]. With LTE, applications include connecting cars to a network, emergency services, forecasts, and more. However, for these applications to work, the devices in the network need to know where the location of each other. And since these are mobile devices, the devices cannot consume too much energy, or the battery would not last long. D2D discovery protocols allow for communication between devices while not consuming too much energy.

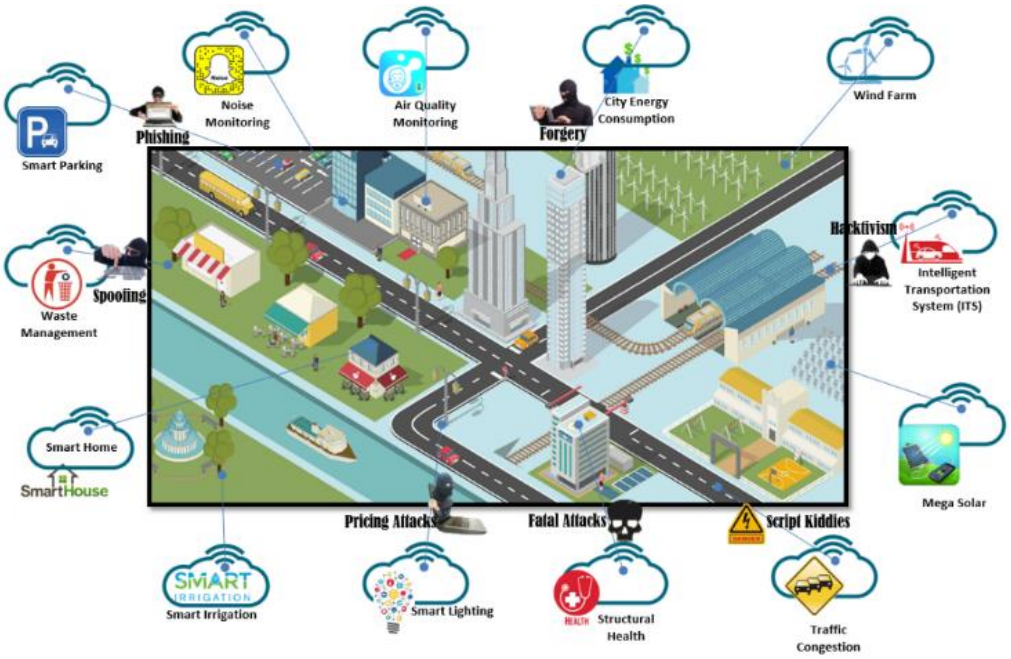

Fig. 1. ICPS vertical networks.

Bluetooth (IEEE 802.3) is a short range wireless communication technology which uses an inquiry procedure to attempt to discover different devices [2]-[5]. The process is like a wake-up and sleep schedule as devices send out scanning signals and response signals. A device sends out an inquiry signal on half of one the Bluetooth channels and then switches to half of another channel. The devices are also unsynchronized, so the devices are free running. The devices then listen for a response signal from one of the response channels, half on one and half on another. A device wanting to be discovered periodically uses the scan procedure in order find the inquiry signal, and when it does, it sends out the response signal. Because the devices are asynchronous, it is unlikely that two devices listen on the same channels. However, if a collision occurs, then the devices wait a random time and try again.

Wi-fi discovery is like Bluetooth discovery. It uses search and listen states. In the search state, the device transmits a request message on the Wi-fi channels, and using contention based transmission scheme with collision avoidance (CSMA/CA), waits for a response. CSMA/CA is a network multiple access method to avoid collisions by transmitting only when the channel is empty. A device in the listen state picks a channel to listen for the request messages. Once found, the devices use the same channel for the discovery process. If two or more searching devices are on the same channel, a listening device will still send the response; however, it will be transmitted on the CSMA/CA to avoiding multiple listeners responding at the same time.

2.2. Network-Assisted Discovery

In a network-assisted discovery, a device initiates the request with a target device, and the network triggers the D2D communication [6], [7]. The network informs the target and the source of each other's information. As shown in Xenakis's study [8], network-assisted D2D discovery is used to develop a framework that estimates the probability of two tagged devices in a proximity. Xenakis's study calculates the optimal number of base stations in an area which is used to calculate the probability of two devices. The probability is calculated for different device positions.

The main advantage of such techniques is high discovery efficiency. However, the main disadvantage is the relatively higher overhead and sensitivity to collision.

2.3. Packet-Based Discovery

When the source device wants to detect the presence of a neighbor, it sends out an encoded packet to the neighbor. The packet is full of all discovery information, and usually a confirmation is sent back. Since the packet contains the D2D information, any information regarding the discovery is available without additional signaling. However, packets could be large, and it is sensitive to collisions. As shown in Lee's study [9], it is possible to reduce the number of packets sent by piggybacking the MAC address packets with the neighbor solicitation packets. The main advantage of such techniques is exchange of complete D2D information. However, they are prone to collision.

2.4. Scheduling Discovery

A common discovery protocol is a wake-up and sleep schedule where nodes spend time asleep. While idle, nodes cannot receive or transmit information. Only when a node wakes up can it either action. A schedule tells a node when it is time to wake up and go to sleep. This can include having a simple duty cycle where nodes periodically sleep and wake up. However, a simple duty cycle has a problem involving energy and nodes discovered. To keep energy consumption down, the duty cycle must remain low. As shown in Guo's study [10], when duty cycle is very low, transmission rate also decreases. When a node attempts to transmit information, all other nodes are asleep. However, having a higher duty cycle leads to transmission rates, but also higher energy consumption. To balance the trade-offs, adaptive wake-up schedule. Adaptive wake-up schedule such as the one proposed by Zhang [11] attempt to optimize the tradeoff by using probability to

determine wake up times. In Zhang's proposal, if a transmission did not happen in the predicted time, the node would select a new transmission time. Because of this, less energy was consumed, and transmission still happened.

The main advantage of such techniques is that lower duty cycles consume less energy. However, the main disadvantage is the higher probability of false negative, i.e. high probability of missing devices.

2.5. Contact Probing

Another common solution is a contact-probing protocol which is like a wake-up schedule. A contact-probing protocol has a duty cycle, but the duty could change and vary based on the protocol. While Zhang's study could change the wake-up time of a node, the node's new wake-up time would have the same duty cycle. Different contact-probing protocols could change the duty cycle differently. In Wang's study [12], the team gathered transmission information by giving phones to volunteers, and measured the data gathered from their contact logs. The data the team gathered was used to make a framework for the protocol, STAR. STAR estimates the traffic that a phone would get and change the duty cycle based on the time of day. While traffic and duty cycle would be high at certain points of the day, it would lower in other points of the day. This lead to the transmission rate to stay high while the energy consumption would be lower. STAR recognizes that people have a similar schedule, the duty cycle would rarely change. It would also change the duty cycle if the person's schedule changed. Similar to STAR, eDiscovery [13] changes the duty cycle based on the number of peers. There's a threshold; if the number of discovered peers is greater than the threshold, then the duty cycle increases and vice versa.

2.6. Slotted-Channel Structures

A slotted structure uses slots in time for discovery and traffic while keeping the sleep and wake up schedule. This is usually to allow for the nodes to beacon their information. It could also be used to synchronize the devices, which prevents collision. In Baccelli's study [14], they proposed a slotted structure, FlashLinQ, as a method of discovery. It globally synchronizes all devices and makes the devices follow a slotted channel structure. A discovery slot is divided into mini slots, and an 8-second interval is one discovery period. A device looking for the discovery signal of a device which is transmitted during a mini discovery slot. It uses hopping to map to the PHY layer while using a greedy algorithm to get the MAC address. In Doukha's study [15], a slotted structure is used to divide time into divided time slots for a vehicular ad hoc network. It does so to make all the nodes to globally synchronized. This allows the vehicles to beacon their messages synchronized.

2.7. Resource Allocation

Discovery signals can be time or frequency multiplexed. Time multiplexing is not preferred in this case since in spreads the signal in frequency that reduces the transmission range. Because of this, frequency multiplexing is preferred since it leads to a longer range. The physical resources are grouped into physical resource blocks (RBs) in LTE. The discovery signal could occupy multiple RBs in the designated discovery subframes.

In Kaleem's study [16], the proposed solution used type- 2 discovery for user equipment (UE), in which the operator, UE, has full control of its resources. This was proposed to help with public safety applications in a LTE network. With this in type of discovery used, a framed structure was proposed where discovery happens in a ten-second frequency block followed by a resource block (RB). During the resource block, the UEs use a multi-channel slotted algorithm to combine the benefits of random resource allocation and sensing- based resource allocation.

Like Kaleem's study, Choi's [17] proposed solution also used RBs in order to discover UEs. However,

Choi's solution allows for adaptively allocates RBs to prevent underutilization of radio resources. The proposed solution also adds a new channel, D2D-PRACH, in order for UEs to send preambles to nearby UEs via a modified random-access procedure. The proposed scheme includes three phases, a D2D-PRACH phase, an Rx-UE phase, and a Tx-UE reporting phase. When each UEs start, they decide whether to transmit or receive randomly. When transmitting, a preamble is sent down the D2D-PRACH channel, and move on to the Tx-UE phase. When receiving UEs either receive a message or don't. UEs that do not receive a message restart again while UEs that do move on to the Rx-UE phase. During the Rx-UE phase, the UEs report their received preambles and send a reporting messages. During the Tx-UE phase, if an UE receives a confirmation message, then a report is made else the UE restarts

3. Secure Neighbor Discovery

While many of the mentioned D2D discovery protocols can detect nearby devices, many of them are unsecured. If an attacker wanted to affect the network, it could lead to leaked information of the network, or it could lead to degradation of the network. Data sent between devices are sensitive, and for some applications, could affect people in a negative way. This needs to be a fundamental function in networks deployed in a hostile environment [18]-[23].

In cloud computing, to protect sensitive from the public cloud, Xue [24], proposed a modified version of the k-Nearest Neighbors (kNN) algorithm that secures information sent between servers. The proposed framework uses different databases with each having different functions. One database encrypts data sets and makes a lookup table while the others decrypt and place the information into the lookup table. These techniques typically secure the data in lookup tables but are prone to slower retrievals.

In to break the circular dependency in mobile ad hoc networks (MANET)s, Zhang [25] proposed a protocol for a DSSS- based MANET in which devices generate a pool of secret spread-codes. Each device is preloaded with a random spread-codes, which is used for D2D discovery. Two devices discover each other if they share the same uncompromised spread-code or if there is uncompromised data path between devices. Devices remove compromised code from their sets in order stop spreading. With this method, if an attacker wanted to initiate an attack on the network, the damage would be minimized because the attacker would have limited spread codes. The unaffected devices would remain secret to the attacker. The main advantage of such techniques is that they reduce the effects of DoS attacks. However, they could potentially lead to nodes becoming undiscovered if the nodes have neighbors with no connecting path or a common spread code.

The applications of a vehicular ad hoc network (VANET) include road safety through awareness of real-time traffic and road conditions. To reduce the latency of the information, Forgue [26] proposed a neighbor discovery protocol that would allow vehicles that discovered an abnormality to message nearby vehicles. In order to keep the information sent between vehicles between secure, Forgue's solution uses messages sent between vehicles in order to determine if a vehicle is an attacker. If the position sent from one vehicle does not match the true position of neighbor's information, then it is considered an attack. The main advantage of such techniques is the possibility of countering attacks common in VANETS including Sybil and colluding attacks. However, the main disadvantage is that if messages are in a queue to be sent, it could cause overhead.

Neighbor Discovery Protocol is one of the protocols in IPv6; however, it is vulnerable to attacks since it assumes that all nodes on trust each other [27]. NDP uses a packet based method for discovery, but this makes NDP vulnerable to attacks. Secure Neighbor Discovery (SEND) then became proposed as a way of securing NDP. SEND uses cryptographically generated address (CGA) in order prevent address stealing by authenticating IPv6 addresses. It does so by hashing the addresses to create unique IDs. SEND uses other

features such as timestamps and sender signature to authenticate the information. The main advantage of such techniques is that they make NDP more secure. However, they are susceptible to certain attacks and typically put a heavy load on the device and network resources.

Wireless sensor networks (WSNs) are viable for many applications, but they could be easily compromised. To increase the security of WSN, Sun [28] proposed introducing a system of monitoring modules that are integrated with intrusion detection modules. This allows nodes around to verify if an event is happening or not. Nodes verify an event using a Kalman filter to detect if the event is happening or code was injected into the network. The Kalman filter monitors the information gathered from the nodes and calculates a normal range of future actions for the nodes. An extension is added to the filter to stop repeat attacks with small deviations. To deal with a lossy environment, a system dynamic model is proposed to mitigate packet losses.

4. Conclusion

This study overview and categorizes the existing device discovery techniques that have the potential to be applied to large-scale deployment, making them useful for IoT implementations. We also review the security of various device discovery techniques and the advantages and disadvantages of using the predominant discovery techniques. This research paves the path for researchers in the field of device discovery and their security by giving novel insights into existing discovery frameworks.

Acknowledgment

This material is based upon work supported in part by the National Science Foundation under Grant No. IIA-1301726 and in part by UNLV Graduate College Rebel Research and Mentorship Program (RAMP).

References

[1] Gozalvez, J. (2014, Sept.). Long-term evolution direct: A device-to-device discovery platform [mobile radio]. *IEEE Vehicular Technology Magazine*, *9(3)*, 10-17.

[2] Yang, K. W., *et al*. (2014, October). Device discovery for multihop cellular networks with its application in LTE. *IEEE Wireless Communications*, *21(5)*, 24-34.

[3] Mach, P., *et al*. (2015). In-band device-to-device communication in OFDMA cellular networks: A survey and challenges. *IEEE Communications Surveys & Tutorials*, *17(4)*, 1885-1922.

[4] Misra, G., *et al*. (2016). Device to device millimeter wave communication in 5G wireless cellular networks (A next generation promising wireless cellular technology). *Proceedings of 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)* (pp. 89-93).

[5] Mustafa, H. A. U., *et al*. (2016). Separation framework: An enabler for cooperative and D2D communication for future 5G networks. *IEEE Communications Surveys & Tutorials*, *18(1)*, 419-445.

[6] Zou, K. J., *et al*. (2014, June). Proximity discovery for device-to-device communications over a cellular network. *IEEE Communications Magazine*, *52(6)*, 98-107.

[7] Asadi, A., *et al*. (2014). A survey on device-to-device communication in cellular networks. *IEEE Communications Surveys & Tutorials*, *16(4)*, 1801-1819.

[8] Xenakis, D., *et al*. (2015). On the performance of network-assisted device-to-device discovery. *Proceedings of 2015 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-7).

[9] Lee, J. H. (2009, December). Cross-layered IPv6 neighbor discovery scheme over WLAN mesh networks. *IEEE Communications Letters*, *13(12)*, 992-994.

[10] Guo, S., *et al*. (2014, Nov.). Opportunistic flooding in low-duty-cycle wireless sensor networks with unreliable links. *IEEE Transactions on Computers*, *63(11)*, 2787-2802.

[11] Zhang, B., *et al*. (2016, July). Network science approach for device discovery in mobile device-to-device communications. *IEEE Transactions on Vehicular Technology*, *65(7)*, 5665-5679.

[12] Wang, W., *et al*. (2009, Oct.). Opportunistic energy-efficient contact probing in delay-tolerant applications. *IEEE/ACM Transactions on Networking*, *17(5)*, 1592-1605.

[13] Han, B., *et al*. (2015, April). On the energy efficiency of device discovery in mobile opportunistic networks: A systematic approach. *IEEE Transactions on Mobile Computing*, *14(4)*, 786-799.

[14] Baccelli, F., *et al*. On the design of device-to-device autonomous discovery. *Proceedings of 2012 Fourth International Conference on Communication Systems and Networks (COMSNETS 2012)* (pp. 1-9).

[15] Doukha, Z., & Moussaoui, S. (2016, Feb.). An SDMA-based mechanism for accurate and efficient neighborhood-discovery link-layer service. *IEEE Transactions on Vehicular Technology*, *65(2)*, 603-613.

[16] Kaleem, Z., *et al*. (2016). Public safety users' priority-based energy and time-efficient device discovery scheme with contention resolution for ProSe in third generation partnership project long-term evolution-advanced systems. *IET Communications*, *10(15)*, 1873-1883.

[17] Choi, K. W., & Han, Z. (2015, Jan.). Device-to-device discovery for proximity-based service in LTE-advanced system. *IEEE Journal on Selected Areas in Communications*, *33(1)*, 55-66.

[18] Wang, M., &Yan, Z. (2015). Security in D2D communications: A review. *2015 IEEE Trustcom/BigDataSE/ISPA*, 1199-1204.

[19] Wang, W., *et al*. (2017). Interference exploitation for enhanced security in D2D spectrum sharing networks. *Proceedings of 2017 IEEE International Conference on Communications (ICC)* (pp. 1-6).

[20] Zhang, A., & Lin, X. (2017, July-August). Security-aware and privacy-preserving D2D communications in 5G. *IEEE Network*, *31(4)*, 70-77.

[21] Haus, M., *et al*. (2017). Security and privacy in device-to-device (D2D) communication: A review. *IEEE Communications Surveys & Tutorials*, *19(2)*, 1054-1079.

[22] Wang, W., *et al*. (2017, Feb.). Enhanced physical layer security in D2D spectrum sharing networks. *IEEE Wireless Communications Letters*, *6(1)*, 106-109.

[23] Zhang, H., *et al*. (2014). Radio resource allocation for physical-layer security in D2D underlay communications. *Proceedings of 2014 IEEE International Conference on Communications (ICC)* (pp. 2319-2324).

[24] Xue, W., *et al*. Secure k nearest neighbors query for high-dimensional vectors in outsourced environments. *IEEE Transactions on Big Data*, *PP(99)*, 1-1.

[25] Zhang, R., *et al*. (2015, Oct.). Jamming-resilient secure neighbor discovery in mobile ad hoc networks. *IEEE Transactions on Wireless Communications*, *14(10)*, 5588-5601.

[26] Fogue, M., *et al*. (2015, June). Securing warning message dissemination in VANETs using cooperative neighbor position verification. *IEEE Transactions on Vehicular Technology*, *64(6)*, 2538-2550.

[27] AlSa'deh, A., & Meinel, C. (2012, July-Aug.). Secure neighbor discovery: Review, challenges, perspectives, and recommendations. *IEEE Security & Privacy*, *10(4)*, 26-34.

[28] Sun, B., *et al*. (2013, March). Anomaly detection based secure in-network aggregation for wireless sensor networks. *IEEE Systems Journal*, *7(1)*, 13-25.

Shahab Tayeb (Ph.D. '18 expected, M.S. with Distinction '12, B.S. Maxima Cum Laude '10) is a doctoral candidate at the College of Engineering, University of Nevada-Las Vegas, where he has been awarded numerous national and international scholarships. Prior to joining the Ph.D. program, he was the managing director at Cisco Networking Academy where he taught various entry, associate, professional, and expert-level courses. He has authored/co-authored 20+ refereed research papers over the past three years and his

research findings have been highlighted by the National Science Foundation. His research interests span the areas of Cybersecurity, Internet of Things, and Cyber-Physical Systems utilizing Big Data Analytics, Deep Learning, and Game Theory.

Adrian Ruiz (Ph.D. '18 expected, M.S. with distinction '12, B.S. maxima cum laude '10) was born in Las Vegas, Nevada. He is currently an undergraduate student at the University of Nevada Las Vegas pursuing a B.S degree in computer engineering. He started his research as part of the UNLV Graduate College Rebel Research and Mentorship Program (RAMP) and his research interests include IoT and device discovery.

Shahram Latifi an IEEE Fellow, received the master of science degree in electrical engineering from Fanni, Teheran University, Iran in 1980. He received the master of science and the Ph.D. degrees both in electrical and computer engineering from Louisiana State University, Baton Rouge, in 1986 and 1989, respectively. He is currently a professor of electrical engineering at the University of Nevada, Las Vegas. Dr. Latifi is the co-director of the Center for Information Technology and Algorithms (CITA) at UNLV. He has designed and taught undergraduate and graduate courses in the broad spectrum of computer science and engineering in the past three decades. He has given seminars on cyber-related topics all over the world. He has authored over 250 technical articles in the areas of networking, cybersecurity, image processing, biosurveillance, biometrics, document analysis, fault tolerant computing, parallel processing, and data compression. His research has been funded by NSF, NASA, DOE, DoD, Boeing, Lockheed and Cray Inc. Dr. Latifi was an Associate Editor of the IEEE Transactions on Computers (1999–2006), an IEEE Distinguished Speaker (1997–2000), and Co-founder and General Chair of the IEEE Int'l Conf. on Information Technology (2004–2015). Dr. Latifi is the recipient of several research awards, the most recent being the Silver State Research Award (2014). He is also a Registered Professional Engineer in the State of Nevada.