Jagannath University Research Journal (JURJ)
Volume No.-III, Issue No.–I, April, 2022, ISSN: 2582-6263

Analysis of Entropy Password Space in various Graphical PasswordsTechniques

Aakanksha Chopra[a], Prof. Dr. Vivek Kumar Sharma[b],Dr. Megha Gupta[c]
[a]Research Scholar, Department of Computer Science, Jagannath University, Jaipur, India.
aakankshachopra.spm@gmail.com
[b] Dean, Department of Engineering and Technology, Jagannath University, Jaipur, India.
vivek.sharma@jagannathuniversity.org
[c]Assistant Professor, Department of Computer Science, MSCW, University of Delhi, New Delhi, India.
meghabis@gmail.com

Abstract: User behaviour, their selection pattern, and the appropriate time they give in password creation are highly influential in information security. For passwords to be easily recalled, amenity and security should be assured. Existing schemes do not evaluate the list of leaked or exposed passwords; thus, they result in vulnerability towards attacks like a dictionary, shoulder surfing, andmany more. Graphical passwords additionally face a problem called unmanaged password space. The password space of the image depends on the type of image selected or uploaded as a password. Thus, understanding the behaviour of users keeping passwords is essential and the need of the hour, as the space needs to be understood, managed and correlated. This paperextends our previous work, where we proposed a technique Character Set and Direction technique(CSD) and developed an android application on it. This paper understands various Graphical Password schemes as per their configured password space. It compares them based on password space, several re-tries during login, ease to remember, recall and use. The paper also calculated the entropy password space and the number of re-tries by users for password login time usingthe proposed Character Set and Direction technique.

Keywords:Entropy passwords, Entropy bits, Graphical password security, login time, generation time, password space.

I. INTRODUCTION

Fora long time, text passwords have been omnipresent and have proved to be the easiest authentication technique for unlocking devices. However, despite this feature, they have not gained high scores in the security of passwords. The perfect alternative to this technique is the graphical password techniques present in four different categories. These categories are recognition, recall, pure recall, and hybrid. In addition, smartphones are now touchscreen phones, so that graphical passwords can provide more usability and security.

Graphical passwords have many advantages over traditional password schemes and are secured from many password attacks. However, the limitation of thegraphical password is understanding of password space. The password mapping process is relatively slow as it stores images, pictures, and icons as passwords and later processes them. Another issue or concern raised by researchers like(Kaka et al., 2021) Is that users must consider behaviouralattitude for password creation and hence increases memorability. Password creation depends upon human-to-human behaviour, although the user tries to select pertinent image areas that raise password predictability.

Humans' cognitive and visual behaviour plays a vital role in password memorability and generating strong or full-strength passwords. (Pietron & Han, 2020) investigated 36 Chinese students based on cognitive and visual behaviour. Their study concentrated on two sets of images: daily life experiences and socio-cultural context. No significant difference was found in the memory time of both groups.

As the quality of the image increases, the password space also increases. Therefore, image data management is a big concern for depicting the password space. As a result,the larger the data size,the slower the authentication process.

Looking into the current technique scenario, we proposed a novel technique as Character Set and Direction (CSD), a combination of character images and a direction. The user selects a 6-digit char-direction password containing 5- character images from a 4X4 grid and then 1 direction from four directions: left, right, top, and Bottom. This 4X4 grid is shown after the random selection of alphabets. During the authentication phase, a user

makes an indirect selection to avoid the security breaches like a shoulder surfing attack. CSD technique is implemented and tested on an android mobile application, with over 80 users in the first stage of testing and 67 in the second stage. Results turned out to be very supportive regarding security, memorability and usability.

This paper extends our previous work, where we proposed a technique Character Set and Direction technique(CSD) and developed an android application on it. Furthermore, this paper understands various Graphical Password schemes as per their configured password space. It compares them based on password space, several re-tries during login, ease to remember, recall and use.

II. LITERATURE REVIEW

Picture Gesture Authentication, commonly known as PGA, is a recall-based graphical password technique widely used with Windows 8 and 10. Users draw three gestures on a selected image rather than text passwords. Several researchers had time to time proved that many human and technological factors are responsible for password strength. These factors are- age, gender, device type for login, design space, grid size,etc. However, two dimensions, namely- background image and gesture drawing, are essential factors for tough passwords. It was also found from investigations done by the University of Cyprus that if image content is related to an individual's cultural thought,passwords created are more memorable(Pietron & Han, 2020).

(Khan & Chefranov, 2020) suggested two schemes Clicked on Object to Draw a Pattern (CODP) technique and the Click on Objects to Select Secrets (COSS) technique. Thistechnique is inspired by CaRP, Pass-Go, and BDAS schemes under graphical passwords. They proposed the extension of the CaRP scheme by using Alphanumeric, visual, click symbols (CS-AV) with Pass-Go. Even though graphical passwords have always been superior to other methods, they also facethe concern ofinsufficient password space.

(Juneja, 2020)represented a desktop and mobile application model in which the patterns were available onthe server-side in the XML schema format. The major drawback of this technique is that it performs a selection of passwords based on heterogeneous pictures, which may result in low performance and becomes a time-consuming process.

A simple image drawing tool was proposed for smartphones by(Fong & Poet, 2020). However, there is no central image database storage. Hence it will generate problems for the user during the login time from different devices. Moreover, the image path is not encoded and stored in the database, and this technique does not provide any security from brute force or dictionary attacks. Lastly, there should be restrictions on the number of failed attempts with an immediate intimation on registered email-id.

Many techniques have been proposed for GP, including password creation with eye gaze. This technique is based on the selection of non-familiar images by the user to estimate the strength by scrutinizing the password through eye gaze. The major drawback of this technique was eye-tracking study was not appropriate as users selection was influenced. Secondly, no proper testing results proved cracking passwords(Constantinides et al., 2020).

(Vaddeti et al., 2020) proposed a technique that claimsprevention against attacks like brute-force, educated guessing, sniffing, hidden camera, shoulder surfing, and phishing. This recognition-based scheme is built on a 5X5 grid butis unsuitable for mobile devices as no hardware or software is made for this system.

(Albakri et al., 2022)presented security threats in the Android system by reverse-engineering tools. Various vulnerabilities in Google's Android system were studied, althoughdesigningan effective vulnerability detection tool for mobileapplications needs to be arrayed.

(Jitendra et al., 2020)analysed the key loggerresistant text-based graphical passwords using colours. So the user has to remember graphical sequences. However, no such experiment was conducted to confirm resistance against mentioned attacks.

(Prati et al., 2022)proposed a deep learning model containinga random password list of 133,447 words in seven dictionaries. Further, a three-piece evaluation model in a lightweight file was constructed to assess, predict, and anticipate thesecurity firmness of a device password. The possibilityof leakage was tested, and prediction accuracy of 95.74% was verified for this model.A significant flaw was that the range used to compare leaked and non- leaked passwords are limited to prove this model's accuracy.

(Moradi et al., 2022)used a fingerprinting biometric contact technique. The scanned fingerprint is passed on to the authentication

system using the cellphone's camera. The proposed scheme managed to shrink the information volume by 15.9% and give high security at the same time. Furthermore, the classification resultsshowedan Equal Error Rate of 3.12%.

(Raptis & Katsini, 2021)proposed the GamePass technique, a gamified mechanism with an enormous password space. Here, the user draws on background images to interact broadly for avoiding predictable graphical passwords.However, the proposed scheme lacks behind in many aspects, such as further investigation is required with memorability, security and usability; the scheme needs to be compared with existing methods for proper performance evaluation; two-step authentications can be further added; lastly, the methods claim that password selection is based on behavioural patterns but not such study has been done to show the results.

(Andriotis et al., 2022)developed a Bu-Dash schemewith a user interface that alters each dynamic user screen swipe on laptops or mobiles. The authors claimthe technique to be robust against shoulder surfing and dictionary attacks, but user inclination was found with few shapes during the experiment.

(Suárez-Plasencia et al., 2022)detected the set of weak passwords by selecting five random imageswhose points contain patterns of the DIAG or LINE type. Then, they tried examining weak passwords and allowed attackers to conduct attacks on these passwords for practically fetching weak passwords.

(Tarish, 2022)recommended a Wi-Fi-based IoT network security solution, further implemented and tested in the GNS3 simulator.Aiming to avoid brute force attacks and dictionary attacks in Wi-Fi-based IoT applications, an SRPP, Secure Remote Password Protocol, is used.

(Abdalkareem et al., 2021) proposed a GP-MB graphical password scheme,developed on mouse motionand a click-based location for limited people from variant groups. A few essential key factors added to this scheme are the number of clicks for the location, fix point, and atmost three particulararеas are added to escalate the password complexity.

(Kausar et al., 2022)described an innovative, hybrid, and much more robust user authentication approach, GRA-PIN (GRAphical and PIN-based), a combination of graphical and PIN-basedtechniques. In this technique, random passwords are generated by performing basic arithmetic operations for each login attempt. This technique was tested via experimenting on three attacks; results were as high as 94% on SoftwareUsability Scale (SUS).

(Simon, 2022)examined protective behaviour and the primary behavioural intentionswhile coping with three messages. During the study, people who cautioned aboutsteady passwords createdtough passwords. It was also found that an immense effort is required to educate people to transcribe behavioural intention into action and thus keep memorable passwords.

(Mathis et al., 2021)mentioned that the prototype systems need to be evaluated based on privacy, usability, and security. But the primary challenge is designing such prototype structures suitable for these three crucial factors. Therefore, the author questioned twelve research and academia volunteers who evaluated privacy and securityprototypes.

III. PASSWORD ENTROPY

Any password is considered safe if and only if it has a higher entropy value. Entropy is an assessment done to check how predictable a password can be. Password entropy is considered a character set of all uppercase, lowercase numbers, symbols and the password length. It is measured in terms of bits. Entropy is calculated as – for example; a password is already familiar, then such password has Entropy as 0. If someone cracks the password in single-trial, then such password has Entropy as 1.

The graphical password strength is calculated as $\log_2 (C^n)$ entropy bits.

We calculated the Theoretical Password Space of the proposed CSD technique as 25.93 bits, where C is considered 16 characters in a grid with 4 direction set (16+4). The Entropy per character can be calculated as:

$M = \log_2 (C^n) = \log_2 (20^6) = 25.93$ bits

But if we consider C as 30, where 26 characters in a grid with 4 direction set (26+4), then the Entropy per character can be calculated as:
$M = \log_2 (C^n) = \log_2 (30^6) = 29.442$ bits

Overall Entropy of Character Set and Direction is:

C= 26(total character set) +16(char. in one grid) * 5(total no. of grids) + 4(total directions)
C= 110

Therefore, M = $\log_2 (C^n) = \log_2 (110^6)$ = 40.686 entropy bits

Henceforth, The estimated entropy bits= 40.686 bits, where n =6 (5 character + 1 direction)

Furthermore, to overcome the Graphical password space problem, each grid cell has an image alphabet or character with a 150x150 pixel size per grid. This is used as part of the password and for 5 character grid cell.
112500 +150 (for one direction grid)= 112650 pixel bits in total

Also, if user selects 5 character from 5 different grids (one character each grid) + 1(one direction out of four) then CSD scheme reached to:

5(total grid sheets)* 150 * 150= 112500 pixel

n=112650+6= 112656

then,

C=30 (total set of character and direction) + [(80+4) *(150 * 150)]
= 30+ 1890000= 1890030

Therefore,

M = $\log_2 (C^n) = \log_2 (1890030^{112656})$
=(112656 * 20.85)
=2348877.6
= **2.34×10^6 bits**

IV. COMPARISON OF CSD AND VARIOUS GRAPHICAL SCHEMES

After calculating entropy bits, it is proved that Character Set and Direction provide an ampleEffective Password Space (EPS).

4.1 Based on bit space- Table 1 showcases passwords space in bits of various graphical password techniques.Comparing all the entropy bit values, it can be concluded that CSD passwords are difficult to guess and super safe from brute force and dictionary attacks.The remaining details of bit space are taken from already existing literature.

Another correlation required is in terms of password generation. With users becoming impatient, it is highly recommended to understand the maximum, minimum and average time taken by participants during the experimentation phase. Here in Table 2, three methods are compared whose values of entropy bits were comparatively close, namely, CODP, COSS (with and without cue). In previous work onthe CSD technique, we constructed experiments on 80 participants at Level-I and 65 in level- II.

4.2 On the basis of password generation time- The CODP and COSS[3] used 40 participants' data for table 2. So, to compare equally, we also compared CSD data with 40 participants only. And the results show that the proposed scheme takes a more significant time for password creation. This happened because the participants were new to the system and took a lot of time to initially understand and be familiar with the mobile application in the testing phase.

4.3. On basis of the number of attempts to log in, memorability is essential for any password proposal. We have compared four different login attempts for 40 participants. CSD had proved to be high on memorability related to other schemes, see Table 3.

4.4. On basis of Login time- CSD took a minimum average login time of 22 seconds and a maximum average login time of 48 seconds. This time was calculated best average time out of three login attempts.

Table 1- Graphical password comparison on basis of bit T space

Schemes	*Entropy bits*
DAS (Jermyn et al., 1999)	57.7
BDAS (Dunphy & Yan, 2007)	76
Passpoint (Chiasson et al., 2007)	43
Pass-Go (Tao & Adams, 2008)	58
QBP(Togookhuu & Zhang, 2017)	<=271
CT(Zhu et al., 2014)	40
CA(Zhu et al., 2014)	42
CODP(Khan & Chefranov, 2020)	58.6
COSS (Khan & Chefranov, 2020)	$2.4X\ 10^4$
Proposed CSD	$2.34X\ 10^6$

Table 2- Comparison of password generation time by user (CSD, CODP, COSS)

Techniques	Minimum time (in seconds)	Maximum time (in seconds)	Average Time (in seconds)
CODP	18.20	34.26	27.45
COSS (without cued)	21.40	39.37	31.33
COSS (cued-based)	20.23	41.53	29.38
CSD	32	87	57.5

Table 3- Comparison of the number of re-attempts by the user. Description of number of times a user clicked on Forget password or reset the password at login time during testing phase (CSD, CODP, COSS)

Techniques	Percentageof users successfully login in 1^{st},2^{nd},3^{rd}, 4^{th} attempts			
	1^{st} attempt (%)	2^{nd} attempt (%)	3^{rd} attempt (%)	4^{th} attempt (%)
CODP (Khan & Chefranov, 2020)	43	34	21	2
COSS(without cued) (Khan & Chefranov, 2020)	37	35	22	6
COSS(cued) (Khan & Chefranov, 2020)	36	37	18	9
CSD(calculated based on number of attempts user	65	25	10	0

Table 4- Best login time out of three attempts by the user during the Level- II phase

Techniques	Minimum password login time (in seconds)	Maximum password login time (in seconds)
CSD	22	48

V. CONCLUSION

This paper correlated various graphical password techniquesbased on password space, login time, average login time, and several re-tries done by the user during password generation. The password scheme must have high password space to overcome the problems faced by the graphical password technique in terms of security, like-dictionary attack, brute force, and shoulder surfing attacks. The proposed methodprovided an increased range of entropy password space in bits as: $2.34X\ 10^6$.

Another aspect required for graphical passwordsis usability-the average login time calculated for the proposed CSD scheme was 57.5 seconds. The average was calculated from the best of three user logins.

Lastly, another factor required for a password scheme is memorability;more users recall a password without any mistake or click on a reset password. The results showcased that 65% (out of 40) of CSD users remembered their password in the first attempt or did not click on forget the password. Also,no user wasn't able to recall the password even on the fourth attempt. Hence, the CSD technique is much more secure, usable, and memorable than other techniques.

Further, a comparison based on ease of use was also made. The responses were collected from users after the survey questionnaire. Users had earlier used many graphical password techniques. Therefore, a high score was achieved in terms of ease of use. These values will be assessed in future, and more users will be involved in further research.

REFERENCES

[1]. Abdalkareem, Z. A., Akif, O. Z., Abdulatif, F. A., Amiza, A., & Ehkan, P. (2021). Graphical password based mouse behavior technique. Journal of Physics: Conference Series, 1755(1). https://doi.org/10.1088/1742-6596/1755/1/012021

[2]. Albakri, A., Fatima, H., Mohammed, M., Ahmed, A., Ali, A., Ali, A., & Elzein, N. M. (2022). Survey on Reverse-Engineering Tools for Android Mobile Devices. Mathematical Problems in Engineering, 2022. https://doi.org/10.1155/2022/4908134

[3]. Andriotis, P., Kirby, M., & Takasu, A. (2022). Bu-Dash: A Universal and Dynamic Graphical Password Scheme. https://www.playstation.com/en-gb/legal/copyright-and-trademark-notice/

[4]. Chiasson, S., Van Oorschot, P. C., & Biddle, R. (2007). Graphical Password Authentication Using Cued Click

Points. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 4734 LNCS, 359–374. https://doi.org/10.1007/978-3-540-74835-9_24

[5]. Constantinides, A., Belk, M., Fidas, C., & Pitsillides, A. (2020). An eye gaze-driven metric for estimating the strength of graphical passwords based on image hotspots. International Conference on Intelligent User Interfaces, Proceedings IUI, 33–37. https://doi.org/10.1145/3377325.3377537

[6]. Dunphy, P., & Yan, J. (2007). Do background images improve "draw a secret" graphical passwords? CCS '07: Proceedings of the 14th ACM Conference on Computer and Communications Security, 36–47. https://doi.org/10.1145/1315245.1315252

[7]. Fong, J., & Poet, R. (2020). Creating Graphical Passwords on a Mobile Phone: Graphical Passwords on a Mobile. In IEEE (Ed.), ACM International Conference Proceeding Series. Association for Computing Machinery. https://doi.org/10.1145/3433174.3433608

[8]. Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999). The Design and Analysis of Graphical Passwords. ACM Digital Library, 8(august).

[9]. Jitendra, N., Sai Vinay, N., Sri Ram, P., Naga Sidhardha, P., Deepthi, D., Tech Student, B., & Professor, A. (2020). TEXT-BASED SHOULDER SURFING AND KEY LOGGER RESISTANT GRAPHICAL PASSWORD. 11. www.jespublication.com

[10]. Juneja, K. (2020). An XML transformed method to improve effectiveness of graphical password authentication. Journal of King Saud University - Computer and Information Sciences, 32(1), 11–23. https://doi.org/10.1016/J.JKSUCI.2017.07.002

[11]. Kaka, J. G., Ishaq, O. O., & Ojeniyi, J. O. (2021). Recognition-based graphical password algorithms: A survey. Proceedings of the 2020 IEEE 2nd International Conference on Cyberspace, CYBER NIGERIA 2020, 44–51. https://doi.org/10.1109/CYBERNIGERIA51635.2021.9428801

[12]. Kausar, N., Din, I. U., Khan, M. A., Almogren, A., & Kim, B. S. (2022). GRA-PIN: A Graphical and PIN-Based Hybrid Authentication Approach for Smart Devices. Sensors 2022, Vol. 22, Page 1349, 22(4), 1349. https://doi.org/10.3390/S22041349

[13]. Khan, A., & Chefranov, A. G. (2020). A Captcha-Based Graphical Password with Strong Password Space and Usability Study. 2nd International Conference on Electrical, Communication and Computer Engineering, ICECCE 2020, August. https://doi.org/10.1109/ICECCE49384.2020.9179265

[14]. Mathis, F., Vaniea, K., & Khamis, M. (2021). Prototyping Usable Privacy and Security Systems: Insights from Experts. Https://Doi.Org/10.1080/10447318.2021.1949134, 38(5), 468–490. https://doi.org/10.1080/10447318.2021.1949134

[15]. Moradi, M., Moradkhani, M., & Tavakoli, M. B. (2022). A Real-Time Biometric Encryption Scheme Based on Fuzzy Logic for IoT. Journal of Sensors, 2022, 1–15. https://doi.org/10.1155/2022/4336822

[16]. Pietron, A. M., & Han, T. (2020). A Case Study of Graphical Passwords in a Chinese University. UMAP 2020 Adjunct - Adjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization, 175–180. https://doi.org/10.1145/3386392.3399558

[17]. Prati, A., Iglesias, C. A., Javier García Villalba, L., Cicirello, V. A., Hyeon Hong, K., & Mun Lee, B. (2022). A Deep Learning-Based Password Security Evaluation Model. Applied Sciences 2022, Vol. 12, Page 2404, 12(5), 2404. https://doi.org/10.3390/APP12052404

[18]. Raptis, G. E., & Katsini, C. (2021). Beter, funner, stronger: A gameful approach to nudge people into making less predictable graphical password choices. Conference on Human Factors in Computing Systems - Proceedings. https://doi.org/10.1145/3411764.3445658

[19]. Simon, J. (2022). Protect Your Password so it can Protect You: Improving Password Strength Through Coping Messages.

[20]. Suárez-Plasencia, L., Herrera-Macías, J. A., Legón-Pérez, C. M., Sosa-Gómez, G., & Rojas, O. (2022). Detection of DIAG and LINE Patterns in PassPoints Graphical Passwords Based on the Maximum Angles of Their Delaunay Triangles. Sensors 2022, Vol. 22, Page 1987, 22(5), 1987. https://doi.org/10.3390/S22051987

[21]. Tao, H., & Adams, C. (2008). Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. International Journal of Network Security, 7(2), 273–292.

[22]. Tarish, H. A. (2022). Enhanced IoT Wi-Fi protocol standard's security using secure remote password.

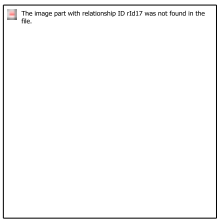
Periodicals of Engineering and Natural Sciences (PEN), 10(1), 632–644. https://doi.org/10.21533/PEN.V10I1.2728

[23]. Togookhuu, B., & Zhang, J. (2017). New Graphic Password Scheme Containing Questions-Background-Pattern and Implementation. Procedia Computer Science, 107, 148–156. https://doi.org/10.1016/J.PROCS.2017.03.071

[24]. Vaddeti, A., Vidiyala, D., Puritipati, V., Ponnuru, R. B., Shin, J. S., & Alavalapati, G. R. (2020). Graphical passwords: Behind the attainment of goals. Security and Privacy, 3(6), e125. https://doi.org/10.1002/SPY2.125

[25]. Zhu, B. B., Yan, J., Bao, G., Yang, M., & Xu, N. (2014). Captcha as graphical passwords - A new security primitive based on hard AI problems. IEEE Transactions on Information Forensics and Security, 9(6), 891–904. https://doi.org/10.1109/TIFS.2014.2312547

AUTHOR'S BIOGRAPHIES



First Author: Aakanksha Chopra is a keen programmer and has been working as an Assistant Professor (IT) with JIMS (GGSIPU) New Delhi for more than 9 years. She did her Master in Computers Applications (MCA) from GGSIPU Dwarka. She did her graduation with B.Sc (Hons.) Computer Sciences from Delhi University. Her research areas are programming, network security, cyber-attacks and cyber security. She has published several research papers in National and International Journals on Network Security and Cryptography. She has edited various magazines for postgraduate students. She has also chaired various International Conferences.

Second Author: Prof. Dr. Vivek Kumar Sharma has over 24 years of academic experience. Presently, he is the Dean, Research and Professorin Jagannath University, Jaipur, India in the department of Engineering and Technology, Jagannath University, Jaipur, India. He had completed his PhD. in 2006 from the University of Rajasthan, Jaipur, India.Dr. Sharma has designed and conducted various Faculty Development Programmes, workshops and National and International Conferences as convener. Dr. Sharma has several publications to his credit and has presented 43 research papers at National and International conferences organized by various central and state Universities and Government Affiliated Engineering Colleges. He is currently guiding 5 PhD Scholars, and nine students have been awarded a doctoral degree under his supervision. He is a reviewer in various international reputed journals. He has co-author 10 books. His area of interest includes soft computing, Fuzzy logic, Network optimization and fluid Dynamics.

Third Author: Dr. Megha Gupta is a PhD holder in Computer Engineering. She did her doctorate from NSIT, University of Delhi. She is presently working as an Assistant Professor in the Department of Computer Science, MSCW (University of Delhi). She completed her Masters's from Banasthali Vidyapith, Banasthali. She was the University rank holder in graduation and post-graduation courses and had more than 12 years of experience in teaching, research and the corporate world. She worked in telecom domain mobile automation testing during her corporate tenure and received client recognition awards. Her breadth of teaching experience includes NSIT (DU), JIMS (GGSIPU) and Miranda House (DU). She has presented various research papers at International Conferences and published research work in SCI, SCIE, and Scopus indexed international journals. Her areas of expertise include networks based on radio, cognitive, sensor, and opportunistic.