REFERENCES

[1] M. Tsikerdekis, “Identity deception prevention using common contribution network data,” *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1,pp. 188–199, Jan. 2017.

[2] T. Anwar and M. Abulaish, “Ranking radically influential Web forum users,” *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6,pp. 1289–1298, Jun. 2015.

[3] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, “Design and analysis of social botnet,” *Comput. Netw.*, vol. 57, no. 2, pp. 556–578,2013.

[4] D. Fletcher, “A brief history of spam,” *TIME*, Nov. 2, 2009.[Online]. Available:http://www.time.com/time/business/article/0,8599,1933796,00.html

[5] Y. Boshmaf, M. Ripeanu, K. Beznosov, and E. Santos-Neto, “Thwarting fake OSN accounts by predicting their victims,” in *Proc. AISec*, Denver,CO, USA, 2015, pp. 81–89.

[6] A. A. Amleshwaram, N. Reddy, S. Yadav, G. Gu, andC. Yang, “CATS: Characterizing automation of Twitter spammers,” in *Proc. COMSNETS*, Bengaluru, India, Jan. 2013, pp. 1–10.

[7] K. Lee, J. C. Lee, and S. Webb, “Uncovering social spammers: Socialhoneypots + machine learning,” in *Proc. SIGIR*, Geneva, Switzerland,Jul. 2010, pp. 435–442.

[8] G. Stringhini, C. Kruegel, and G. Vigna, “Detecting spammers on socialnetworks,” in *Proc. ACSAC*, Austin, TX, USA, 2010, pp. 1–9.

[9] H. Yu, M. Kaminsky, P. B. Gibbons, and A. D. Flaxman, “SybilGuard:Defending against sybil attacks via social networks,” *IEEE/ACM Trans.Netw.*, vol. 16, no. 3, pp. 576–589, Jun. 2008.

[10] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, “Detectingand characterizing social spam campaigns,” in *Proc. IMC*, Melbourne,VIC, Australia, 2001, pp. 35–47.

[11] W. Wei, F. Xu, C. C. Tan, and Q. Li “Sybildefender: Defend against sybil attacks in large social networks,” in *Proc. INFOCOM*, Orlando, FL, USA, Mar. 2012, pp. 1951–1959.

[12] C. Yang, R. C. Harkreader, and G. Gu, “Die free or live hard? Empirical evaluation and new design for fighting evolving Twitter spammers,” in *Proc. RAID*, Menlo Park, CA, USA, 2011, pp. 318–337.

[13] S. Lee and J. Kim, “WarningBird: A near real-time detection system forsuspicious URLs in Twitter stream,” *IEEE Trans. Depend. Sec. Comput.*,vol. 10, no. 3, pp. 183–195, May 2013.

[14] M. Sahami, S. Dumais, D. Heckerman, and E. Horvitz, “A Bayesianapproach to filtering junk e-mail,” in *Proc. Workshop Learn. Text Categorization*, Madison, WI, USA, 1998, pp. 98–105.

[15] C. Schäfer, “Detection of compromised email accounts used by a spam botnet with country counting and theoretical geographical travelling speed extracted from metadata,” in *Proc. ISSREW*, Naples, Italy,Nov. 2014, pp. 329–334.

[16] C. Schäfer, “Detection of compromised email accounts used for spamming in correlation with origin-destination delivery notification extracted from metadata,” in *Proc. ISDFS*, Tirgu Mures, Romania, Apr. 2017,pp. 1–6.

[17] A. H. Wang, “Detecting spam bots in online social networking sites:A machine learning approach,” in *Proc. DBSec*, Rome, Italy, 2010,pp. 335–342.

[18] F. Ahmed and M. Abulaish, “A generic statistical approach for spam detection in online social networks,” *Comput. Commun.*, vol. 36,nos. 10–11, pp. 1120–1129, 2013.

[19] C. Yang, R. Harkreader, and G. Gu, “Empirical evaluation and new design for fighting evolving Twitter spammers,” *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 8, pp. 1280–1293, Aug. 2013.

[20] Y. Zhu, X. Wang, E. Zhong, N. N. Liu, H. Li, and Q. Yang, “Discovering spammers in social networks,” in *Proc. AAAI*, Toronto, ON, Canada,2012, pp. 52–58.

[21] E. Tan, L. Guo, S. Chen, X. Zhang, and Y. Zhao, “Spammer behavioranalysis and detection in user generated content on social networks,”in *Proc. ICDCS*, Macau, China, Jun. 2012, pp. 305–314.

[22] S. Y. Bhat and M. Abulaish, “Community-based features for identifying spammers in online social networks,” in *Proc. Int. Conf. Adv.Social Netw. Anal. Mining*, Niagara Falls, ON, Canada, Aug. 2013,pp. 100–107.

[23] L. M. Aiello, M. Deplano, R. Schifanella, and G. Ruffo, “People are strange when you’re a stranger: Impact and influence of bots on socialnetworks,” in *Proc. AAAI*, Dublin, Ireland, 2012, pp. 10–17.

[24] S. Cresci, R. D. Pietro, M. Petrocchi, A. Spognardi, and M. Tesconi, “The paradigm-shift of social spambots: Evidence, theories, and toolsfor the arms race,” in *Proc. WWW*, Perth, WA, Australia, 2017,pp.