

- communications,” in *Proc. IFIP SCNC Workshop*, Shanghai, China, Apr. 2011.
- [2] “Introduction to NISTIR 7628 guidelines for smart grid cyber security,” National Institute of Standards and Technology (NIST), 2010 [Online]. Available: http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf
- [3] H. Nicanfar and V. C. M. Leung, “Smart grid multilayer consensus password-authenticated key exchange protocol,” in *Proc. IEEE SFCS Workshop*, Ottawa, ON, Canada, Jun. 2012.
- [4] Q. Li and G. Cao, “Multicast authentication in the smart grid with onetime signature,” *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 686–696, Dec. 2011.
- [5] A. P. Muniyandi, R. Ramasamy, and Indrani, “Password based remote authentication scheme using ECC for smart card,” in *Proc. ICCCS*, Orisa, India, Feb. 2011.
- [6] P. Jokar, H. Nicanfar, and V. C. M. Leung, “Specification-based intrusion detection for home area networks in smart grids,” in *Proc. IEEE SmartGridComm*, Brussels, Belgium, Oct. 2011.
- [7] X. Ding, C. Ma, and Q. Cheng, “Password authenticated key exchange protocol with stronger security,” in *Proc. ETCS Workshop*, Wuhan, Hubei, China, Mar. 2009.
- [8] H. Boumerzoug, B. A. Bensaber, and I. Biskri, “A keys management method based on an AVL tree and ECC cryptography for wireless sensor networks,” in *Proc. Q2SWinet*, Miami Beach, FL, Oct.–Nov. 2011.
- [9] E. J. Yooni and K. Y. Yoo, “A new elliptic curve Diffie-Hellman two party key agreement protocol,” in *Proc. ICSSSM Conf.*, Tokyo, Japan, Jun. 2010.
- [10] S. Wang, Z. Cao, M. A. Strangio, and L. Wang, “Cryptanalysis and improvement of an elliptic curve Diffie-Hellman key agreement protocol,” *IEEE Commun. Lett.*, vol. 12, no. 2, pp. 149–151, Feb. 2008.
- [11] A. H. Koblitz, N. Koblitzb, and A. Menezes, “Elliptic curve cryptography: The serpentine course of a paradigm shift,” *Elsevier J. Number Theory*, vol. 131, no. 5, pp. 781–814, May 2011.
- [12] S. M. Bellovin and M. Merritt, “Encrypted key exchange: Password-based protocols secure against dictionary attacks,” in *Proc. IEEE Comput. Soc. Symp. Res. Security Privacy*, Oakland, CA, May 1992.