References

[1] Schmidt, R., et al., *Body Area Network BAN–a key infrastructure element for patient-centered medical applications.* Biomedizinische Technik/Biomedical Engineering, 2002. **47**(s1a): p. 365-368.

[2] Yazdandoost, K.Y. and R. Kohno, *Body implanted medical device communications.* IEICE transactions on communications, 2009. **92**(2): p. 410-417.

[3] Strydis, C., G. Gaydadjiev, and S. Vassiliadis, *Implantable microelectronic devices: A comprehensive review.* Computer Engineering, Delft University of Technology," CE-TR-2006-01, 2006.

[4] Ellouze, N., et al. *Securing implantable cardiac medical devices: use of radio frequency energy harvesting*. in *Proceedings of the 3rd international workshop on Trustworthy embedded devices*. 2013. ACM.

[5] Pope, A., et al., *Innovation and Invention in Medical Devices:: Workshop Summary*. 2001: National Academies Press.

[6] Maisel, W.H., et al., *Pacemaker and ICD generator malfunctions: analysis of Food and Drug Administration annual reports.* Jama, 2006. **295**(16): p. 1901-1906.

[7] Flick, B.B. and R. Orglmeister, *A portable microsystem-based telemetric pressure and temperature measurement unit.* Biomedical Engineering, IEEE Transactions on, 2000. **47**(1): p. 12-16.

[8] Shults, M.C., et al., *A telemetry-instrumentation system for monitoring multiple subcutaneously implanted glucose sensors.* Biomedical Engineering, IEEE Transactions on, 1994. **41**(10): p. 937-942.

[9] Valdastri, P., et al., *An implantable telemetry platform system for in vivo monitoring of physiological parameters.* Information Technology in Biomedicine, IEEE Transactions on, 2004. **8**(3): p. 271-278.

[10] Min, M., et al., *An implantable analyzer of bio-impedance dynamics: mixed signal approach [telemetric monitors]*. Instrumentation and Measurement, IEEE Transactions on, 2002. **51**(4): p. 674-678.

[11] Smith, B., et al., *An externally powered, multichannel, implantable stimulator-telemeter for control of paralyzed muscle.* Biomedical Engineering, IEEE Transactions on, 1998. **45**(4): p. 463-475.

[12] Sawan, M., et al. *A wireless implantable electrical stimulator based on two FPGAs*. in *Electronics, Circuits, and Systems, 1996. ICECS'96., Proceedings of the Third IEEE International Conference on*. 1996. IEEE.

[13] Schwarz, M., et al., *Single chip CMOS imagers and flexible microelectronic stimulators for a retina implant system.* Sensors and Actuators A: Physical, 2000. **83**(1): p. 40-46.

[14] Halperin, D., et al. *Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses*. in *Security and Privacy, 2008. SP 2008. IEEE Symposium on*. 2008. IEEE.

[15] Bigger Jr, J.T., *Prophylactic use of implanted cardiac defibrillators in patients at high risk for ventricular arrhythmias after coronary-artery bypass graft surgery.* New England Journal of Medicine, 1997. **337**(22): p. 1569-1575.

[16] Halperin, D., et al., *Security and privacy for implantable medical devices.* Pervasive Computing, IEEE, 2008. **7**(1): p. 30-39.

[17] Carrara, S., et al., *Fully integrated biochip platforms for advanced healthcare.* Sensors, 2012. **12**(8): p. 11013-11060.

[18] Commission, F.C., *MICS Medical Implant Communication Services.* FCC 47CFR95: p. 601-95.673.

[19] Astrin, A.W., L. Huan-Bang, and R. Kohno, *Standardization for body area networks.* IEICE transactions on communications, 2009. **92**(2): p. 366-372.

[20] Bradley, P.D., *Implantable ultralow-power radio chip facilitates in-body communications.* RF DESIGN, 2007. **30**(6): p. 20.

[21] Maisel, W.H., *Safety issues involving medical devices: implications of recent implantable cardioverter-defibrillator malfunctions.* JAMA, 2005. **294**(8): p. 955-958.

[22] Holmes, C.F. and B.B. Owens, *Batteries for implantable biomedical applications.* Wiley Encyclopedia of Biomedical Engineering, 2006.

[23] Semiconductor, Z., *ZL70101 medical implantable RF transceiver data sheet*. 2007, May.

[24] Olivo, J., S. Carrara, and G. De Micheli, *Energy harvesting and remote powering for implantable biosensors.* IEEE Sensors Journal, 2011. **11**(EPFL-ARTICLE-152140): p. 1573-1586.

[25] Lee, I., et al., *High-confidence medical device software and systems.* Computer, 2006. **39**(4): p. 33-38.

[26] Fang, Q., et al., *Developing a wireless implantable body sensor network in MICS band.* Information Technology in Biomedicine, IEEE Transactions on, 2011. **15**(4): p. 567-576.

[27] Burleson, W., et al. *Design challenges for secure implantable medical devices*. in *Proceedings of the 49th Annual Design Automation Conference*. 2012. ACM.

[28] Li, C., A. Raghunathan, and N.K. Jha. *Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system*. in *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on*. 2011. IEEE.

[29] Rasmussen, K.B., et al. *Proximity-based access control for implantable medical devices*. in *Proceedings of the 16th ACM conference on Computer and communications security*. 2009. ACM.

[30] Recommendation, X., *800, Security Architecture for Open Systems Interconnection for CCITT Applications.* International Telecommunication Union (ITU), 1991.

[31] Gerrish, P., et al., *Challenges and constraints in designing implantable medical ICs.* Device and Materials Reliability, IEEE Transactions on, 2005. **5**(3): p. 435-444.

[32] Bruen, A.A., et al., *Applied cryptography: protocols, algorithms, and source code in C.* 1996.

[33] Carollo, K., *Can Your Insulin Pump Be Hacked.* ABC News: Medical Unit, 2012.

[34] Zhan, C., et al., *Cardiac device implantation in the United States from 1997 through 2004: a population-based analysis.* Journal of General Internal Medicine, 2008. **23**(1): p. 13-19.

[35] Myagmar, S., A.J. Lee, and W. Yurcik. *Threat modeling as a basis for security requirements*. in *Symposium on requirements engineering for information security (SREIS)*. 2005.

[36] Steven, J., *Threat Modeling-Perhaps It's Time.* Security & Privacy, IEEE, 2010. **8**(3): p. 83-86.

[37] Malasri, K. and L. Wang, *Securing wireless implantable devices for healthcare: Ideas and challenges.* Communications Magazine, IEEE, 2009. **47**(7): p. 74-80.

[38] Fu, K., *Inside risks Reducing risks of implantable medical devices.* Communications of the ACM, 2009. **52**(6): p. 25-27.

[39] Hansen, J.A. and N.M. Hansen. *A taxonomy of vulnerabilities in implantable medical devices*. in *Proceedings of the second annual workshop on Security and privacy in medical and home-care systems*. 2010. ACM.

[40] Paul, N., T. Kohno, and D.C. Klonoff, *A review of the security of insulin pump infusion systems.* Journal of diabetes science and technology, 2011. **5**(6): p. 1557-1562.

[41] Kermani, M.M., et al., *Emerging Frontiers in Embedded Security.* 2013: p. 203-208.

[42] Fu, K. and J. Blum, *Controlling for cybersecurity risks of medical device software.* Communications of the ACM, 2013. **56**(10): p. 35-37.

[43] Kune, D.F., et al. *Ghost talk: Mitigating EMI signal injection attacks against analog sensors*. in *Security and Privacy (SP), 2013 IEEE Symposium on*. 2013. IEEE.

[44] Fu, K. and J. Blum, *Controlling for Cybersecurity Risks of Medical Device Software*. Biomedical Instrumentation & Technology, 2014. **48**(s1): p. 38-41.

[45] Zhang, M., A. Raghunathan, and N.K. Jha. *Towards trustworthy medical devices and body area networks*. in *Proceedings of the 50th Annual Design Automation Conference*. 2013. ACM.

[46] Clark, S.S. and K. Fu, *Recent results in computer security for medical devices*, in *Wireless Mobile Communication and Healthcare*. 2012, Springer. p. 111-118.

[47] Rushanan, M., et al. *SoK: Security and privacy in implantable medical devices and body area networks*. in *Security and Privacy (SP), 2014 IEEE Symposium on*. 2014. IEEE.

[48] Hei, X., et al. *Defending resource depletion attacks on implantable medical devices*. in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*. 2010. IEEE.

[49] Food, U. and D. Administration, *Content of premarket submissions for management of cybersecurity in medical devices: draft guidance for industry and food and drug administration staff*. 2013.

[50] Shen, W., et al. *Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time*. in *Security and Privacy (SP), 2013 IEEE Symposium on*. 2013. IEEE.

[51] 51. Halevi, T. and N. Saxena. *On pairing constrained wireless devices based on secrecy of auxiliary channels: The case of acoustic eavesdropping*. in *Proceedings*

of the 17th ACM conference on Computer and communications security. 2010. ACM.

[52] Radcliffe, J. *Hacking medical devices for fun and insulin: Breaking the human SCADA system*. in *Black Hat Conference presentation slides*. 2011.

[53] Rostami, M., et al. *Balancing security and utility in medical devices?* in *Proceedings of the 50th Annual Design Automation Conference*. 2013. ACM.

[54] Pournaghshband, V., M. Sarrafzadeh, and P. Reiher, *Securing legacy mobile medical devices*, in *Wireless Mobile Communication and Healthcare*. 2013, Springer. p. 163-172.

[55] Shostack, A. *Experiences threat modeling at microsoft*. in *Modeling Security Workshop. Dept. of Computing, Lancaster University, UK*. 2008.

[56] Israel, C.W. and S.S. Barold, *Pacemaker systems as implantable cardiac rhythm monitors.* The American journal of cardiology, 2001. **88**(4): p. 442-445.

[57] Jebali, N., S. Beldi, and A. Gharsallah, *An RFID Antenna Implanted In The Human Arm For Medical Applications.* Skin, 2015. **41**: p. 0.874705.

[58] Kim, B., J. Yu, and H. Kim. *In-vivo NFC: remote monitoring of implanted medical devices with improved privacy*. in *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*. 2012. ACM.

[59] Freudenthal, E., et al. *Suitability of nfc for medical device communication and power delivery*. in *Engineering in Medicine and Biology Workshop, 2007 IEEE Dallas*. 2007. IEEE.

[60] Varshney, L.R., P. Grover, and A. Sahai. *Securing inductively-coupled communication*. in *Information Theory and Applications Workshop (ITA), 2012*. 2012. IEEE.

[61] Hancke, G. *Eavesdropping attacks on high-frequency RFID tokens*. in *4th Workshop on RFID Security (RFIDSec)*. 2008.

[62] Haselsteiner, E. and K. Breitfuß. *Security in near field communication (NFC)*. in *Workshop on RFID Security RFIDSec*. 2006.

[63] Cremers, C., et al. *Distance hijacking attacks on distance bounding protocols*. in *Security and Privacy (SP), 2012 IEEE Symposium on*. 2012. IEEE.

[64] Choi, S., et al. *Secure and resilient proximity-based access control*. in *Proceedings of the 2013 international workshop on Data management & analytics for healthcare*. 2013. ACM.

[65] Hosseini-Khayat, S. *A lightweight security protocol for ultra-low power ASIC implementation for wireless implantable medical devices*. in *Medical Information & Communication Technology (ISMICT), 2011 5th International Symposium on*. 2011. IEEE.

[66] Fan, X., et al. *FPGA implementations of the Hummingbird cryptographic algorithm*. in *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*. 2010. IEEE.

[67] Fan, X., et al. *Lightweight implementation of Hummingbird cryptographic algorithm on 4-bit microcontrollers*. in *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*. 2009. IEEE.

[68] Beck, C., et al. *Block cipher based security for severely resource-constrained implantable medical devices*. in *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*. 2011. ACM.

[69] Strydis, C., D. Zhu, and G.N. Gaydadjiev. *Profiling of symmetric-encryption algorithms for a novel biomedical-implant architecture*. in *Proceedings of the 5th conference on Computing frontiers*. 2008. ACM.

[70] Ohta, H. and M. Matsui, *A description of the misty1 encryption algorithm.* RFC2994, November, 2000.

[71] Malasri, K. and L. Wang, *Design and implementation of a securewireless mote-based medical sensor network.* Sensors, 2009. **9**(8): p. 6273-6297.

[72] Bergamasco, S., M. Bon, and P. Inchingolo. *Medical data protection with a new generation of hardware authentication tokens*. in *Mediterranean Conference on Medical and Biological Engineering and Computing*. 2001. Citeseer.

[73] Schechter, S., *Security that is Meant to be Skin Deep Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices.* 2010.

[74] Poon, C.C., Y.-T. Zhang, and S.-D. Bao, *A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health.* Communications Magazine, IEEE, 2006. **44**(4): p. 73-81.

[75] Cherukuri, S., K.K. Venkatasubramanian, and S.K. Gupta. *BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body*. in *Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on*. 2003. IEEE.

[76] Hu, C., et al. *OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks*. in *INFOCOM, 2013 Proceedings IEEE*. 2013. IEEE.

[77] Hei, X. and X. Du. *Biometric-based two-level secure access control for implantable medical devices during emergencies*. in *INFOCOM, 2011 Proceedings IEEE*. 2011. IEEE.

[78] Narasimhan, S., X. Wang, and S. Bhunia. *Implantable electronics: emerging design issues and an ultra light-weight security solution*. in *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE*. 2010. IEEE.

[79] Tsouri, G.R. *Securing wireless communication with implanted medical devices using reciprocal carrier-phase quantization*. in *World of Wireless, Mobile and Multimedia Networks & Workshops, 2009. WoWMoM 2009. IEEE International Symposium on a*. 2009. IEEE.

[80] Denning, T., K. Fu, and T. Kohno. *Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security*. in *HotSec*. 2008.

[81] Rostami, M., A. Juels, and F. Koushanfar. *Heart-to-heart (H2H): authentication for implanted medical devices*. in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 2013. ACM.

[82] Strydis, C., et al., *A system architecture, processor, and communication protocol for secure implants.* ACM Transactions on Architecture and Code Optimization (TACO), 2013. **10**(4): p. 57.

[83] Hu, F., et al., *Trustworthy data collection from implantable medical devices via high-speed security implementation based on IEEE 1363.* Information Technology in Biomedicine, IEEE Transactions on, 2010. **14**(6): p. 1397-1404.

[84] Gollakota, S., et al., *They can hear your heartbeats: non-invasive security for implantable medical devices.* ACM SIGCOMM Computer Communication Review, 2011. **41**(4): p. 2-13.

[85] Zheng, G., et al. *A Non-key based security scheme supporting emergency treatment of wireless implants*. in *Communications (ICC), 2014 IEEE International Conference on*. 2014. IEEE.

[86] Xu, F., et al. *IMDGuard: Securing implantable medical devices with the external wearable guardian*. in *INFOCOM, 2011 Proceedings IEEE*. 2011. IEEE.

[87] Hei, X., et al. *PIPAC: patient infusion pattern based access control scheme for wireless insulin pump system*. in *INFOCOM, 2013 Proceedings IEEE*. 2013. IEEE.

[88] Panescu, D., *Emerging Technologies [wireless communication systems for implantable medical devices]*. Engineering in Medicine and Biology Magazine, IEEE, 2008. **27**(2): p. 96-101.

[89] Fu, K., *Inside risksReducing risks of implantable medical devices.* Communications of the ACM, 2009. **52**(6): p. 25.

[90] St Denis, T., *Cryptography for developers*. 2006: Syngress.

[91] Bogdanov, A., et al., *PRESENT: An ultra-lightweight block cipher*. 2007: Springer.

[92] Bellare, M., P. Rogaway, and D. Wagner, *A conventional authenticated-encryption mode.* manuscript, April, 2003.

[93] Rogaway, P., M. Bellare, and J. Black, *OCB: A block-cipher mode of operation for efficient authenticated encryption.* ACM Transactions on Information and System Security (TISSEC), 2003. **6**(3): p. 365-403.

[94] Dworkin, M., *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004.* NIST Special Publication.

[95] Dworkin, M. *Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) for confidentiality and authentication*. in *Federal Information Processing Standard Publication FIPS*. 2006. Citeseer.

[96] Dworkin, M., *NIST Special Publication 800-38A," Recommendation for Block Cipher Modes of Operation: Methods and Techniques", 2001*.

[97] Martinovic, I., P. Pichota, and J.B. Schmitt. *Jamming for good: a fresh approach to authentic communication in WSNs*. in *Proceedings of the second ACM conference on Wireless network security*. 2009. ACM.

[98] Gupta, S.K., T. Mukherjee, and K. Venkatasubramanian. *Criticality aware access control model for pervasive applications*. in *Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM '06).* 2006. IEEE.

[99] Sandhu, R.S. and P. Samarati, *Access control: principle and practice.* Communications Magazine, IEEE, 1994. **32**(9): p. 40-48.

[100] Hu, J. and A.C. Weaver. *A dynamic, context-aware security infrastructure for distributed healthcare applications*. in *Proceedings of the first workshop on pervasive privacy security, privacy, and trust*. 2004. Citeseer.

[101] 101. Al-Muhtadi, J., et al. *Cerberus: a context-aware security scheme for smart spaces*. in *Pervasive Computing and Communications, 2003.(PerCom 2003). Proceedings of the First IEEE International Conference on*. 2003. IEEE.

[102] Sandhu, R.S., et al., *Role-based access control models.* Computer, 1996(2): p. 38-47.

[103] Alcaraz Calero, J.M., G. Martinez Perez, and A.F. Gomez Skarmeta, *Towards an authorisation model for distributed systems based on the Semantic Web.* Information Security, IET, 2010. **4**(4): p. 411-421.

[104] Ni, Q., et al., *Privacy-aware role-based access control.* ACM Transactions on Information and System Security (TISSEC), 2010. **13**(3): p. 24.

[105] Covington, M.J., et al. *Securing context-aware applications using environment roles*. in *Proceedings of the sixth ACM symposium on Access control models and technologies*. 2001. ACM.

[106] Xiong, J. and K. Jamieson. *SecureAngle: improving wireless security using angle-of-arrival information*. in *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*. 2010. ACM.

[107] Garcia-Morchon, O., et al., *Security Considerations in the IP-based Internet of Things.* 2013.

[108] Liu, H., et al., *Survey of wireless indoor positioning techniques and systems.* Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, 2007. **37**(6): p. 1067-1080.

[109] Lieckfeldt, D., *Efficient Localization of Users and Devices in Smart Environments*. 2010, Dissertation, University of Rostock.

[110] Luo, X., et al. *Encryption algorithms comparisons for wireless networked sensors*. in *Systems, Man and Cybernetics, 2004 IEEE International Conference on*. 2004. IEEE.

[111] Chang, C.-C., S. Muftic, and D.J. Nagel. *Measurement of energy costs of security in wireless sensor nodes*. in *Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on*. 2007. IEEE.

[112] Venugopalan, R., et al. *Encryption overhead in embedded systems and sensor network nodes: Modeling and analysis*. in *Proceedings of the 2003 international conference on Compilers, architecture and synthesis for embedded systems*. 2003. ACM.

[113] Großschädl, J., et al. *Energy evaluation of software implementations of block ciphers under memory constraints*. in *Proceedings of the conference on Design, automation and test in Europe*. 2007. EDA Consortium.

[114] Law, Y.W., J. Doumen, and P. Hartel, *Survey and benchmark of block ciphers for wireless sensor networks.* ACM Transactions on Sensor Networks (TOSN), 2006. **2**(1): p. 65-93.

[115] Needham, R.M. and D.J. Wheeler, *Correction to xtea*. 1998.

[116] Bellare, M., P. Rogaway, and D. Wagner, *A conventional authenticated-encryption mode.* manuscript, April, 2003.

[117] Rogaway, P., M. Bellare, and J. Black, *OCB: A block-cipher mode of operation for efficient authenticated encryption.* ACM Transactions on Information and System Security (TISSEC), 2003. **6**(3): p. 365-403.

[118] Dworkin, M.J., *Sp 800-38c. recommendation for block cipher modes of operation: the ccm mode for authentication and confidentiality.* 2004.

[119] McGrew, D.A. and J. Viega, *The security and performance of the Galois/Counter Mode (GCM) of operation (full version).* URL: http://csrc. nist. gov/CryptoToolkit/modes/proposedmodes/gcmgcm-ad. pdf, 2008.

[120] McGrew, D. and J. Viega, *The Galois/counter mode of operation (GCM).* Submission to NIST. http://csrc. nist. gov/CryptoToolkit/modes/proposedmodes/gcm/gcm-spec. pdf, 2004.

[121] Kohno, T., J. Viega, and D. Whiting, *The CWC-AES dual-use mode.* Submission to NIST Modes of Operation Process, 2003.

[122] Darji, M. and B.H. Trivedi, *Detection of active attacks on wireless IMDs using proxy device and localization information*, in *Security in Computing and Communications*. 2014, Springer. p. 353-362.

[123] Darji, M. and B. Trivedi, *Imd-ids a specification based intrusion detection system for wireless imds.* International Journal of Applied Information Systems, 2013. **5**(6): p. 19-23.

[124] Darji, M. and B.H. Trivedi, *Emergency Aware, Non-invasive, Personalized Access Control Framework for IMDs*, in *Recent Trends in Computer Networks and Distributed Systems Security*. 2014, Springer. p. 370-381.

[125] Eugster, P.T., et al., *The many faces of publish/subscribe.* ACM Computing Surveys (CSUR), 2003. **35**(2): p. 114-131.

[126] 126. Costa, P., G.P. Picco, and S. Rossetto. *Publish-subscribe on sensor networks: A semi-probabilistic approach*. in *Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on*. 2005. IEEE.

[127] Dworkin, M., *Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC*. 2007.

[128] 3-WAY, BLOWFISH, DES, GOST, IDEA, RC5 source code. www.cis.udel.edu/~mills/database/schneier/.

[129] SKIPJACK, LOKI91 source code. www.mirrors.wiretapped.net/security/

[130] Jariwala, Vivaksha, and D. C. Jinwala., *Evaluating Galois Counter mode in link layer security architecture for wireless sensor networks.* In *International Journal of Network Security & Its Applications* 2.4 (2010): 55-65.

[131] Jinwala, Devesh, Dhiren Patel, and Kankar Dasgupta., *FlexiSec: a configurable link layer security architecture for wireless sensor networks*, *arXiv preprint arXiv:1203.4697* (2012).

[132] Joan Daemen, Vincent Rijmen. *The Design of Rijndael AES - The Advanced Encryption Standard*. In *Springer Series on Information Security and Cryptography*, Springer-Verlag, 2002.

[133] Luk, Mark, et al. MiniSec: a secure sensor network communication architecture. In p*roceedings of the 6th international conference on Information processing in sensor networks*. ACM, 2007.

[134] IPSec: Requests For Comments. RFC 2401, RFC 2402, RFC 2406, RFC 2408. [Online]. Available:http://www.ietf.org/rfc/rfc240n.txt.

[135] Transport Layer Security. Requests For Comments:RFC 4346. [Online]. Available http://tools.ietf.org/html/rfc5246

[136] D. Wagner and B. Schneier. Analysis of the SSL 3.0 protocol. In *proceedings of the 2nd USENIX Workshop on Electronic Commerce (EC-96)*, pp. 29-40, USENIX Association, Berkeley, 1996.

[137] Kwak, Kyung Sup, Sana Ullah, and Niamat Ullah. An overview of IEEE 802.15. 6 standard. In *3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on*. IEEE, 2010.

[138] Moteiv Telos Motes. [Online]. Available :http://www.moteiv.com.

[139] T. Wollinger, M. Wang, J. Guajardo, and C. Paar. How well are high-end DSPs suited for the AES algorithms? In *proceedings of 3rd AES conference*, New York, pp. 94-105, 2000

[140] Devesh Jinwala, Dhiren Patel, K S Dasgupta. *Optimizing the Replay Protection at the Link Layer Security Framework in Wireless Sensor Networks. In* IAENG International Journal of Computer Science,International Association of Engineers Publication,Hong Kong. 2009

[141] David A. McGrew and John Viega. The Security and Performance of the Galois/Counter Mode (GCM) of Operation. In *proceedings of the INDOCRYPT*, LNCS Book Series, Vol. 9743, pp. 343- 355, Springer-Verlag, 2004.

[142] B. Bloom. "Space/time trade-offs in hash coding with allowable errors." *Communications of the ACM*, 13(7),pp. 422-426, July 1970.

[143] Paul Syverson. A Taxonomy of Replay Attacks. In *CSFW'94: Proceedings of the Seventh Computer Security Foundations Workshop*, pp. 187-191, IEEE Computer Society Press, 1994.

[144] T. Aura. Strategies against replay attacks. In *Proceedings of the 10th IEEE Computer SocietyFoundations Workshop*, pp. 59–68, IEEE Computer Society Press, MA, June 1997.

[145] Cryptographic Random Numbers Standard P1363: Appendix E, November, 1995

[146] Dworkin, Morris. Recommendation for block cipher modes of operation: methods and techniques. No. NIST-SP-800-38A. NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD COMPUTER SECURITY DIV, 2001.

[147] International Organization for Standardization. ISO/IEC 9798-2: Information Technology - Security techniques — Entity Authentication Mechanisms Part 2: Entity authentication using symmetric techniques. ISO/IEC, 1993

[148] Hankerson, Darrel, Alfred J. Menezes, and Scott Vanstone. *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[149] Lauter, Kristin. The advantages of elliptic curve cryptography for wireless security. In *IEEE Wireless communications*, 2004

[150] Eugster, P. T., Felber, P. A., Guerraoui, R., & Kermarrec. The many faces of publish/subscribe. *ACM Computing Surveys (CSUR)*,2005.

[151] Pallickara, S., Pierce, M., Gadgil, H., Fox, G., Yan, Y., & Huang, Y. A framework for secure end-to-end delivery of messages in publish/subscribe systems.

In *Proceedings of the 7th IEEE/ACM International Conference on Grid Computing* (pp. 215-222). IEEE Computer Society, 2006.

[152] Johnson, D., Menezes, A., & Vanstone. The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security*,*1*(1), 36-63, 2001.

[153] Picazo-Sanchez, P., Tapiador, J. E., Peris-Lopez, P., & Suarez-Tangil. Secure publish-subscribe protocols for heterogeneous medical wireless body area networks. *Sensors*, 2014

[154] Kaliski, B., & Staddon. *PKCS# 1: RSA cryptography specifications version 2.0*. RFC 2437, October 1998.

List of Publications

Patent Filed:

1. **An Improved System for Securing Implantable Medical Devices. Application Number: 92/MUM/2015**

Paper Presented or Published:

1 Darji, M. and B. Trivedi, *Secure leader election algorithm optimized for power saving using mobile agents for intrusion detection in MANET*, in *Recent Trends in Computer Networks and Distributed Systems Security*. 2012, Springer. p. 54-63.

2 Darji, M. and B. Trivedi, *Survey of intrusion detection and prevention system in MANETs based on data gathering techniques.* IJAIS, 2012. **1**: p. 38-43.

3 Darji, M. and B.H. Trivedi, *Detection of active attacks on wireless IMDs using proxy device and localization information*, in *Security in Computing and Communications*. 2014, Springer. p. 353-362.

4 Darji, M. and B. Trivedi, *Imd-ids a specification based intrusion detection system for wireless imds.* International Journal of Applied Information Systems, 2013. **5**(6): p. 19-23.

5 Darji, M. and B.H. Trivedi, *Emergency Aware, Non-invasive, Personalized Access Control Framework for IMDs*, in *Recent Trends in Computer Networks and Distributed Systems Security*. 2014, Springer. p. 370-381.