REFERENCES

Adekunle, a. a., & Woodhead, S. R. (2009). On Efficient Data Integrity and Data Origin Authentication for Wireless Sensor Networks Utilising Block Cipher Design Techniques. *2009 Third International Conference on Next Generation Mobile Applications, Services and Technologies*, 419–424. Ieee. Retrieved January 7, 2013, from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5337392

Aiash, M., Mapp, G., Phan, R. C.-W., Lasebae, A., & Loo, J. (2012). A Formally Verified Device Authentication Protocol Using Casper/FDR. *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 1293–1298. Ieee. Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6296128

Aschenbruck, N., Bauer, J., Bieling, J., Bothe, A., & Schwamborn, M. (2012). Selective and Secure Over-The-Air Programming for Wireless Sensor Networks. *2012 21st International Conference on Computer Communications and Networks (ICCCN)*, 1–6. Ieee. Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6289278

Brown, S., & Sreenan, C. J. (2006). Updating software in wireless sensor networks: A survey. *Dept. of Computer Science, National Univ. of Ireland, Maynooth, Tech. Rep*. Citeseer. Retrieved June 29, 2012, from http://www.mendeley.com/research/updating-software-in-wireless-sensor-networks-a-survey/

Bui, N., Ugus, O., Dissegna, M., Rossi, M., & Zorzi, M. (2010). An integrated system for secure code distribution in Wireless Sensor Networks. *2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 575–581. Ieee. Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5470503

Cao, Q., Abdelzaher, T., Stankovic, J., & He, T. (2008). The LiteOS Operating System: Towards Unix-Like Abstractions for Wireless Sensor Networks. *2008 International Conference on Information Processing in Sensor Networks (ipsn 2008)*, 233–244. Ieee. Retrieved April 16, 2012, from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4505477

Chien, T. V., Chan, H. N., Vu Chien, T., Nguyen Chan, H., & Nguyen Huu, T. (2011). A comparative study on operating system for Wireless Sensor Networks. *Advanced Computer Science and Information System (ICACSIS), 2011 International Conference on* (pp. 978–979). Retrieved June 29, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6140770

Christie, R. (1984). *Electricity, industry, and class in South Africa*. SUNY Press.

Chung-Wei Phan, R., Average, F. F., & Lee, S. (2002). Cryptanalysis of full Skipjack block cipher. *Electronics Letters*, *38*(2), 69–71. IET.

Crossbow. (n.d.). Mica2 Datasheet. Retrieved from http://bullseye.xbow.com:81/Products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf

Das, M. (2008). Dynamic program update in wireless sensor networks using orthogonality principle. *Communications Letters, IEEE*, *12*(6), 471–473. Retrieved June 29, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4542786

Deng, J., Han, R., Mishra, S., Dengcoloradoedu, J., & Hancoloradoedu, R. (2006). Secure code distribution in dynamically programmable wireless sensor networks. *Proceedings of the 5th international conference on Information processing in sensor networks* (pp. 292–300).

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *Information Theory, IEEE Transactions on*, *22*(6), 644–654. IEEE.

Dong, W., Chen, C., Liu, X., & Bu, J. (2010). Providing OS support for wireless sensor networks: Challenges and approaches. *Communications Surveys &*, *12*(4), 519–530. IEEE. Retrieved June 29, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5462978

Dunkels, A., Gronvall, B., & Voigt, T. (2004). Contiki - a Lightweight and Flexible Operating System for Tiny Networked Sensors. *Local Computer Networks, 2004. 29th Annual IEEE International Conference on* (pp. 455–462).

Dutta, P. K., Hui, J. W., Chu, D. C., & Culler, D. E. (2006). Securing the Deluge network programming system. *2006 5th International Conference on*

Information Processing in Sensor Networks, 326–333. ACM Press. Retrieved from http://portal.acm.org/citation.cfm?doid=1127777.1127826

Failures-Divergence Refinements – FDR2 user manual. (n.d.). . Retrieved January 13, 2013, from http://www.fsel.com/

Fan, X., & Gong, G. (2012). Accelerating signature-based broadcast authentication for wireless sensor networks. *Ad Hoc Networks*, *10*(4), 723–736. Elsevier B.V. Retrieved December 18, 2012, from http://linkinghub.elsevier.com /retrieve/pii/S157087051100148X

Galos, M., Mieyeville, F., Navarro, D., & O'Connor, I. (2011). Reprogramming hardware-software heterogeneous Wireless Sensor Networks. *Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on* (pp. 1–5). Retrieved June 29, 2012, from http:// ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6081547

Gay, D., Levis, P., Von Behren, R., Welsh, M., Brewer, E., & Culler, D. (2003). The nesC language: A holistic approach to networked embedded systems. *Acm Sigplan Notices* (Vol. 38, pp. 1–11).

Han, C. C., Kumar, R., Shea, R., Kohler, E., & Srivastava, M. (2005). A Dynamic Operating System for Sensor Nodes. *Proceedings of the 3rd international conference on Mobile systems, applications, and services*, 163–176.

Handschuh, H., Knudsen, L. R., & Robshaw, M. J. (2001). Analysis of SHA-1 in Encryption Mode, 70–83.

He, D., Member, S., Chen, C., Chan, S., & Bu, J. (2012). SDRP : A Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks, *59*(11), 4155–4163.

Housley, R., Yee, P., & Nace, W. (2000). *Encryption using KEA and SKIPJACK*.

Hu, W., Tan, H., Corke, P., Shih, W. C., & Jha, S. (2010). Toward trusted wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, *7*(1), 5. ACM. Retrieved June 29, 2012, from http://portal.acm.org /citation.cfm?doid=1806895.1806900

Hui, J. W., & Culler, D. (2004). The Dynamic Behavior of a Data Dissemination Protocol for Network Programming at Scale Categories and Subject Descriptors. *Proceedings of the 2nd international conference on Embedded networked sensor systems*, 81–94.

Hyun, S., Ning, P., Liu, A., & Du, W. (2008). Seluge: Secure and DoS-Resistant Code Dissemination in Wireless Sensor Networks. *2008 International Conference on Information Processing in Sensor Networks (ipsn 2008)*, 445–456. Ieee. Retrieved December 18, 2012, from http://ieeexplore.ieee.org /lpdocs/epic03/wrapper.htm?arnumber=4505494

Karlof, C., Sastry, N., & Wagner, D. (2004). TinySec: a link layer security architecture for wireless sensor networks. *Proceedings of the 2nd international conference on Embedded networked sensor systems* (pp. 162–175).

Kondratieva, V., & Seo, S. (2007). Optimized Hash Tree for Authentication in Sensor Networks. *IEEE Communications Letters*, *11*(2), 149–151. Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4115145

Kong, J. H., Ang, L.-M., Seng, K. P., & Ong, F. T. (2011). Low-complexity Two Instruction Set Computer architecture for sensor network using Skipjack encryption. *The International Conference on Information Networking 2011 (ICOIN2011)*, 472–477. Ieee. Retrieved from http://ieeexplore.ieee.org/ lpdocs/epic03/wrapper.htm?arnumber=5723161

Krawczyk, H., Canetti, R., & Bellare, M. (1997). HMAC: Keyed-Hashing for Message Authentication. Retrieved January 7, 2013, from http://tools.ietf.org/ html/rfc2104

Kulkarni, S. S. (2005). MNP: Multihop Network Reprogramming Service for Sensor Networks. *25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)*, 7–16. Ieee. Retrieved from http://ieeexplore.ieee.org/ lpdocs/epic03/wrapper.htm?arnumber=1437066

De la Parra, C. F. C., & Garcia-Macias, J. A. (2009). A protocol for secure and energy-aware reprogramming in WSN. *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing Connecting the World Wirelessly - IWCMC '09*, 292. New York, New York, USA: ACM Press. Retrieved from http://portal.acm.org/citation.cfm?doid= 1582379.1582443

Lanigan, P. E., Gandhi, R., & Narasimhan, P. (2006). Sluice: Secure Dissemination of Code Updates in Sensor Networks. *26th IEEE International Conference on Distributed Computing Systems (ICDCS'06)*, 53–53. Ieee. Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1648840

Law, Y., Zhang, Y., Jin, J., Palaniswami, M., & Havinga, P. (2011). Secure Rateless Deluge: Pollution-Resistant Reprogramming and Data Dissemination for Wireless Sensor Networks. *EURASIP Journal on Wireless Communications and Networking*, *2011*(1), 685219. Retrieved November 15, 2012, from http://jwcn.eurasipjournals.com/content/2011/1/685219

Li, B., Batten, L. M., & Doss, R. (2009). Lightweight Authentication for Recovery in Wireless Sensor Networks. *2009 Fifth International Conference on Mobile Ad-hoc and Sensor Networks*, 465–471. Ieee. Retrieved December 18, 2012, from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5401475

Liu, A., & Ning, P. (2008). TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. *Information Processing in Sensor Networks, 2008. IPSN'08. International Conference on* (pp. 245–256). Retrieved June 29, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4505478

Liu, W., Luo, R., & Yang, H. (2009). Cryptography Overhead Evaluation and Analysis for Wireless Sensor Networks. *2009 WRI International Conference on Communications and Mobile Computing*, 496–501. Ieee. Retrieved January 7, 2013, from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4797303

Lowe, G. (1997). Casper: a compiler for the analysis of security protocols. *Proceedings 10th Computer Security Foundations Workshop*, 18–30. IEEE Comput. Soc. Press. Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=596779

Maheshwari, R., Gao, J., & Das, S. R. (2007). Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information. *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, 107–115. Ieee. Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4215603

Michail, H. E., Kakarountas, a. P., Milidonis, a., & Goutis, C. E. (2004). Efficient implementation of the keyed-hash message authentication code (HMAC) using the SHA-1 hash function. *Proceedings of the 2004 11th IEEE International Conference on Electronics, Circuits and Systems, 2004. ICECS 2004.*, 567–570. Ieee. Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1399744

Michail, H., Kakarountas, a. P., Koufopavlou, O., & Goutis, C. E. (2005). A Low-Power and High-Throughput Implementation of the SHA-1 Hash Function. *2005 IEEE International Symposium on Circuits and Systems*, 4086–4089. Ieee. Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1465529

Munivel, E., & Ajit, G. M. (2010). Efficient Public Key Infrastructure Implementation in Wireless Sensor Networks. *2010 International Conference on Wireless Communication and Sensor Computing (ICWCSC)*, 1–6. Ieee. Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5415904

Ning, P., Liu, A., & Du, W. (2008). Mitigating DoS attacks against broadcast authentication in wireless sensor networks. *ACM Transactions on Sensor Networks*, *4*(1), 1–35. Retrieved from http://portal.acm.org/citation.cfm?doid=1325651.1325652

Park, K., Lee, J., Kwon, T., & Song, J. (2007). Supplementary Hash in Wireless Sensor Networks, 653–662.

Perrig, a., & Johnson, D. B. (2006). Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, *24*(2), 370–380. Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1589115

Phillips, L. A. (2005). *Aqueduct: Robust and efficient code propagation in heterogeneous wireless sensor networks*. University of Colorado. Retrieved June 29, 2012, from http://www-users.cs.umn.edu/~phillips/Aqueduct.pdf

Pura, M.-L., & Patriciu, V.-V. (2010). Security analysis of Robust User Authentication Protocol. *2010 8th International Conference on Communications*, 457–460. Ieee. Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5509078

Ramadass, S., Budiarto, R., & Ho, C. L. (2007). Unreliable Network Re-Authentication Protocol Based On Hybrid Key Using CSP Approach. *IJCSN International Journal Of Computer Science And Network Security*, *1*(11). Dr. Sang H. Lee.

Schneider, S. A., Goldsmith, M. H., Lowe, G., & Roscoe, A. W. (2010). The Modelling and Analysis of Security Protocols : the CSP Approach, (December).

Schroder-Preikschat, W., Kapitza, R., Kleinoder, J., Felser, M., Karmeier, K., Labella, T. H., & Dressler, F. (2007). Robust and efficient software

management in sensor networks. *Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on* (pp. 1–6). Retrieved June 29, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4268114

Shnayder, V, Hempstead, M., Chen, B., & Welsh, M. (2004). Powertossim: Efficient power simulation for tinyos applications.

Shnayder, Victor, Hempstead, M., Chen, B., Allen, G. W., & Welsh, M. (2004). Simulating the power consumption of large-scale sensor network applications. *Proceedings of the 2nd international conference on Embedded networked sensor systems - SenSys '04*, 188. New York, New York, USA: ACM Press. Retrieved from http://portal.acm.org/citation.cfm?doid=1031495.1031518

Sreenan, C. J., & Brown, S. (2006). A new model for updating software in wireless sensor networks. *Network, IEEE*, *20*(6), 42–47. IEEE.

Stathopoulos, T, Heidemann, J., & Estrin, D. (2003). *A remote code update mechanism for wireless sensor networks*.

Stathopoulos, Thanos, Heidemann, J., & Estrin, D. (2003). A Remote Code Update Mechanism for Wireless Sensor Networks. CALIFORNIA UNIV LOS ANGELES CENTER FOR EMBEDDED NETWORKED SENSING. Retrieved June 29, 2012, from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA482887

Su, M., Yang, X., Wei, L., & Yang, H. (2010). Key Management Scheme in WSN Based on Property of Circle. *2010 International Conference on Computational Intelligence and Software Engineering*, 1–4. Ieee. Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5676908

TinyOS. (n.d.). . Retrieved from http://www.tinyos.net

Ugus, O., Westhoff, D., & Bohli, J. M. (2009). A ROM-friendly secure code update mechanism for WSNs using a stateful-verifier τ-time signature scheme. *Proceedings of the second ACM conference on Wireless network security* (pp. 29–40). Retrieved June 29, 2012, from http://dl.acm.org/citation.cfm?id=1514279

Wander, A. S., Gura, N., Eberle, H., Gupta, V., & Shantz, S. C. (2005). Energy analysis of public-key cryptography for wireless sensor networks. *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on* (pp. 324–328).

Zeng, P., Cao, Z., Choo, K. K. R., & Wang, S. (2009). Security weakness in a dynamic program update protocol for wireless sensor networks. *Communications Letters, IEEE*, *13*(6), 426–428. IEEE. Retrieved June 29, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5090425

Zhou, L., & Haas, Z. J. (1999). Securing ad hoc networks. *Network, IEEE*, *13*(6), 24–30. IEEE.