Chapter 8

Acknowledgments

This work was supported in part by CYCIT TIC2003-09279-C02-01, by the I2CAT Foundation and by TEC2004-06437-C05-05/TCM.

I would like to thank all the people from the Nokia Research Center in Helsinki (where I worked for five years) that helped to make SAODV a reality. Special mention deserve my colleague N. Asokan and my bosses Jari Juopperi and Asko Vilavaara.

I would also like to thank Miquel Oliver (my tutor while I was taking the degree of Diploma of Advanced Studies) and my former colleagues at the Department of Technology at the Universitat Pompeu Fabra.

And, finally, thanks to Jorge García (my PhD thesis supervisor) and new colleagues at the Computer Architecture Department (DAC) of the Technical University of Catalonia (UPC).

Bibliography

[1] N. Asokan and P. Ginzboorg. Key agreement in ad-hoc networks. *Computer Communication Review*, 23(17):1627–1637, Nov. 2000.

[2] E. M. Belding-Royer. Report on the aodv interop. Tech Report 2002-18, UCSB, June 2002.

[3] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In *Proceedings of the 4th Annual International Conference on Mobile Computing and Networking*, pages 85–97, 1998.

[4] S. Cheshire and B. Aboba. Dynamic configuration of ipv4 link-local addresses. IETF INTERNET DRAFT, zeroconf working group, June 2001. draft-ietf-zeroconf-ipv4-linklocal-03.txt.

[5] S. Cheung. An efficient message authentication scheme for link state routing. In *13th Annual Computer Security Applications Conference*, pages 90–98, 1997.

[6] B. Dahill, B. N. Levine, E. Royer, and C. Shields. A secure routing protocol for ad hoc networks. Technical Report UM-CS-2001-037, University of Massachusetts, Departament of Computer Science, Aug. 2001.

[7] Douglas S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris. A high-throughput path metric for multi-hop wireless routing. In *Proceedings of the 9th annual international conference on Mobile computing and networking*, pages 134 – 146, September 2003.

[8] M. Guerrero Zapata. Secure Ad hoc On-Demand Distance Vector Routing. *ACM Mobile Computing and Communications Review (MC2R)*, 6(3):106–107, July 2002.

[9] M. Guerrero Zapata. Secure ad hoc on-demand distance vector (saodv) routing. first published in the IETF MANET Mailing List (October 8th 2001), Aug. 2002. INTERNET-DRAFT draft-guerrero-manet-saodv-00.txt.

[10] M. Guerrero Zapata. Key Management and Delayed Verification for Ad Hoc Networks. In *In Proceedings of HiPC Workshops 2004, Electronic proceedings, Trusted Internet Workshop, paper #8, 8 pages*, December 2004.

[11] M. Guerrero Zapata. Shortcut Detection and Route Repair in Ad-hoc Networks. In *In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'05)*, March 2005.

[12] M. Guerrero Zapata. Secure ad hoc on-demand distance vector (saodv) routing, Feb. 2006. INTERNET-DRAFT draft-guerrero-manet-saodv-05.txt.

[13] M. Guerrero Zapata. Secure dynamic manet on-demand (sdymo) routing protocol, Feb. 2006. INTERNET-DRAFT draft-guerrero-manet-sdymo-00.txt.

[14] M. Guerrero Zapata. Simple ad hoc key management (sakm), Feb. 2006. INTERNET-DRAFT draft-guerrero-manet-sakm-00.txt.

[15] M. Guerrero Zapata and N. Asokan. Securing Ad hoc Routing Protocols. In *Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002)*, pages 1–10, September 2002.

[16] C. Gui and P. Mohapatra. SHORT: self-healing and optimizing routing techniques for mobile ad hoc networks. In *Proceedings of the 4th ACM*

international symposium on Mobile ad hoc networking and computing, pages 279 – 290, June 2003.

[17] Z. J. Haas, M. R. Pearlman, and P. Samar. The interzone routing protocol (IERP) for ad hoc networks. INTERNET DRAFT, MANET working group, July 2002. draft-ietf-manet-zone-ierp-02.txt.

[18] R. Hauser, A. Przygienda, and G. Tsudik. Reducing the cost of security in link state routing. In *Symposium on Network and Distributed Systems Security (NDSS '97)*, pages 93–99, San Diego, California, Feb. 1997. Internet Society.

[19] R. Hinden and S. Deering. Ip version 6 addressing architecture. Internet Request for Comments RFC 2373, July 1998.

[20] Y. C. Hu, D. Johnson, and A. Perrig. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. In *4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), June 2002*, pages 3–13, June 2002.

[21] Y. C. Hu, A. Perrig, and D. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. Technical Report TR01-383, Rice University, Dec. 2001.

[22] IANA. Special-use ipv4 addresses. Internet Request for Comments RFC 3330, Sept. 2002.

[23] D. B. Johnson et al. The dynamic source routing protocol for mobile ad hoc networks (DSR). INTERNET DRAFT, MANET working group, Apr. 2003. draft-ietf-manet-dsr-09.txt.

[24] S. Kent, C. Lynn, J. Mikkelson, and K. Seo. Secure border gateway protocol (S-BGP) — real world performance and deployment issues, 2000.

[25] H. Krawczyk. Simple forward-secure signatures from any signature scheme. In *ACM Conference on Computer and Communications Security*, pages 108–115, 2000.

[26] R. Laboratories. Elliptic Curve Cryptography Standard. Public-Key Cryptography Standards (PKCS) 13, Jan. 1998.

[27] H. Lundgren, E. Nordstrm, and C. Tschudin. Coping with communication gray zones in IEEE 802.11b based ad hoc networks. In *Proceedings of the 5th ACM international workshop on Wireless mobile multimedia*, pages 49 – 55, September 2002.

[28] C. Madson and R. Glenn. The use of HMAC-MD5-96 within ESP and AH. Internet Request for Comments RFC 2403, Nov. 1998.

[29] C. Madson and R. Glenn. The use of HMAC-SHA-1-96 within ESP and AH. Internet Request for Comments RFC 2404, Nov. 1998.

[30] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, pages 255–265, 2000.

[31] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *The Handbook of Applied Cryptography.* CRC Press, 1996. ISBN 0-8493-8523-7.

[32] G. Montenegro and C. Castelluccia. Statistically unique and cryptographically verifiable (SUCV) identifiers and addresses. Network and Distributed System Security Symposium (NDSS '02), Feb. 2002.

[33] G. O'Shea and M. Roe. Child-proof authentication for mipv6 (CAM). ACM Computer Communication Review, Apr. 2001.

[34] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.

[35] C. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications*, pages 234–244, 1994.

[36] C. E. Perkins, E. M. Belding-Royer, and S. R. Das. Ad hoc on-demand distance vector (AODV) routing. Internet Request for Comments RFC 3561, Nov. 2003.

[37] R. Perlman. Fault-tolerant broadcast of routing information. In *Computer Networks, n. 7*, pages 395–405, 1983.

[38] A. Perrig, R. Canetti, D. Song, and D. Tygar. Efficient and secure source authentication for multicast. In *Network and Distributed System Security Symposium (NDSS'01)*, Feb. 2001.

[39] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar. SPINS: security protocols for sensor netowrks. In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, pages 189–199, 2001.

[40] S. Ramanathan and M. Steenstrup. A survey of routing techniques for mobile communications networks. *Mobile Networks and Applications*, 1(2):89–104, 1996.

[41] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. Address allocation for private internets. Internet Request for Comments RFC 1918, Feb. 1996.

[42] R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2), February 1978.

[43] E. M. Royer and C.-K. Toh. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications*, pages 46–55, Apr. 1999.

[44] B. R. Smith, S. Murthy, and J. J. Garcia-Luna-Aceves. Securing distance-vector routing protocols. In *Symposium on Network and Distributed Systems Security (NDSS '97)*, pages 85–92, San Diego, California, Feb. 1997. Internet Society.

[45] A. Srinivas and E. Modiano. Minimum energy disjoint path routing in wireless ad-hoc networks. In *Proceedings of the 9th annual international conference on Mobile computing and networking*, pages 122 – 133, September 2003.

[46] F. Stajano and R. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Proceedings of the 7th International Workshop on Security Protocols*, number 1796 in Lecture Notes in Computer Science, pages 172–194. Springer-Verlag, Berlin Germany, Apr. 1999.

[47] S. Thomson and T. Narten. Ipv6 stateless address autoconfiguration. IETF Request for Comments, Dec. 1998. `RFC 2462`.

[48] U. S. National Institute of Standards and Technology NIST, Computer Systems Laboratory. Digital Signature Standard (DSS). Federal Information Processing Standards Publication (FIPS PUB) 186, May 1994.

[49] J. Walter, J. Oleksy, and J. Kong. The role of ecdsa in wireless communications. Master Thesis. Computer Science Department. University of California, 2002.

[50] K. Zhang. Efficient protocols for signing routing messages. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS'98)*, July 2001.

[51] Q. Zhang and S. Kassam. Finite-state markov model for rayleigh fading channels. IEEE Transactions on Communications, vol. 47, no. 11, (1999) 1688–1692., Nov. 1999.

[52] L. Zhou and Z. J. Haas. Securing ad hoc networks. *IEEE Network Magazine*, 13(6):24–30, November/December 1999.