Chapter 2

Contributions

2.1 Publications

1. Manel Guerrero Zapata: "Secure Ad hoc On-Demand Distance Vector Routing". ACM Mobile Computing and Communications Review (MC2R), Vol 6. No. 3, pp. 106-107, July 2002. [8]

2. Manel 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. ISBN 1-58113-585-8. [15]

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

4. Manel Guerrero Zapata: "Shortcut Detection and Route Repair in Ad-hoc Networks". In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'05), pp. 237-242. ISBN 0-7695-2300-5. March 2005. [11]

5. Manel Guerrero Zapata: "Key Management and Delayed Verification for Ad Hoc Networks". In Journal of High Speed Networks Special Issue. Vol. 15, Num. 1, 2006. Pages 93-109. ISSN 0926-6801.

The first paper ("Secure Ad hoc On-Demand Distance Vector Routing" MC2R 2002) is a short paper that discusses different approaches that where proposed to provide security features to routing protocols in MANET networks (like symmetric cryptography, misbehaving detection schemes and the use of tamper resistant devices), argues that they are not appropriated for MANET networks and proposes SAODV as an alternative giving a short overview of how it works.

The second paper ("Securing Ad hoc Routing Protocols" WiSe 2002) explains in full detail how SAODV works. The main contribution of Asokan (the second author of the paper) among many others, is the use of hash chains to authenticate the hop count of the routing messages. The paper does not solve, however, the problem of key management. It just assumes that there is a key management scheme that allows any node to know the public key of the all the other nodes.

The third paper ("Key Management and Delayed Verification for Ad Hoc Networks" HiPC 2004) addresses the concerns raised by the research community (e.g., [34], [20], [21]) related to the use of SAODV: That SAODV's signatures might require a processing power that might be excessive for certain kinds of ad hoc scenarios and that not providing a key management scheme that explains how nodes get the public keys they need is not solving the whole problem. The paper solves both issues by modifying SAODV so that most of the signatures verifications do not need to be done and the verification of the other ones can be delayed (let us call it "delayed verification") and by providing a key management scheme that effectively ties the public keys to the IP addresses. Therefore, making SAODV a complete solution to secure AODV. The paper also presents simulation results that show that SAODV with delayed verification provide the same security with minimum impact in the network performance.

The fourth paper ("Shortcut Detection and Route Repair in Ad-hoc Networks" PERCOMW'05) proposes a way to enhance AODV in such a way that it uses the shortest routes most of the times. This approach let routes be discovered in the conventional way and periodically the protocol tries to discover shortcuts. In addition, it incorporates a much better route repair

method that the one specified by AODV.

Finally, the fifth paper is a revised and extended version of the third paper that has been published in a special issue of the Journal of High Speed Networks (JHSN).

2.2 Conferences

1. June 2002: Speaker: "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing". AODV Next Generation (AODVng) 2002 Workshop (Lausanne, Switzerland).

2. September 2002: Speaker. "Securing Ad hoc Routing Protocols". The 2002 ACM Workshop on Wireless Security (WiSe 2002), (Atlanta, Georgia, USA).

3. October 2002: Invited Speaker. "Securing Ad hoc Routing Protocols". Formal Methods Forum of the Helsinki University of Technology (Helsinki, Finland).

4. December 2002: Invited Speaker. "How to Design Wireless Security Mechanisms". 1st Workshop on Security in Ad-Hoc Networks (Ruhr University Bochum, Germany).

5. December 2004: Speaker. "Key Management and Delayed Verification for Ad Hoc Networks". 3rd International Trusted Internet Workshop (TIW 2004), (Bangalore, India).

6. March 2005: Speaker. "Shortcut Detection and Route Repair in Adhoc Networks". 1st International Workshop on Pervasive Wireless Networking (PWN05), (Kauai Island, Hawaii).

The first speech, (at the AODVng Workshop), was the first time I could present SAODV to the research community that were working with AODV. AODVng was organized by Charles Perkins and Elizabeth M. Belding-Royer (the two main authors of the AODV routing protocol). This workshop was organized to discuss future directions and enhancements for AODV.

The speeches number 2, 5 and 6 correspond respectively to the publications number 2, 3 and 4.

In the third speech, (at the Formal Methods Forum of the Helsinki University of Technology) I was invited to give a speech about SAODV. I also discussed whether the techniques used by SAODV would also be applicable to other similar routing protocols and about how a key management scheme could be used in conjunction with it.

Finally, in the fourth speech, (at the 1st Workshop on Security in Ad-Hoc Networks) I was invited to give a speech about the subject I would prefer (kind of like a keynote speech). In that occasion I chose to talk not about the security mechanism for wireless networks that I had designed (SAODV), but about how to design those mechanisms to be effective and to really achieve security.

2.3 Internet drafts

The solution proposed in the papers about SAODV is specified in the form of the saodv Internet-Draft. Delayed verification and key management are named SAKM (Simple Ad hoc Key Management) and specified in the form of the sakm Internet-Draft. The way SAODV secures AODV is applied to DYMO to designe a secure extension called SDYMO (Secure Dynamic MANET On-Demand Routing Protocol) that is specified in the form of the sdymo Internet-Draft.

- "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing"
  - Manel Guerrero Zapata: draft-guerrero-manet-saodv-00.txt. First published in the IETF MANET Mailing List (October 8th 2001). Submitted to the IETF on August 12th 2002. [9]
  - Manel Guerrero Zapata: draft-guerrero-manet-saodv-01.txt, August 2004.
  - Manel Guerrero Zapata: draft-guerrero-manet-saodv-02.txt, November 2004.

  - Manel Guerrero Zapata: draft-guerrero-manet-saodv-03.txt, March 2005.
  - Manel Guerrero Zapata: draft-guerrero-manet-saodv-04.txt, September 2005.
  - Manel Guerrero Zapata: draft-guerrero-manet-saodv-05.txt, February 2006. [12]

- "Simple Ad hoc Key Management (SAKM)"
  - Manel Guerrero Zapata: draft-guerrero-manet-sakm-00.txt, February 2006. [14]

- "Secure Dynamic MANET On-Demand (SDYMO) Routing Protocol"
  - Manel Guerrero Zapata: draft-guerrero-manet-sdymo-00.txt, February 2006. [13]

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). The IETF defines itself as "a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet". IETF is well known by everybody working with Internet protocols since it has standardized most of them (IP, TCP, UDP, STMP, and a long etcetera).

Internet-Drafts have a maximum life of six months. After that time, they must be updated, or they will be consider expired. A draft can be an individual submission or a working group submission. When a draft is considered to be mature by a working group it becomes an RFC (Request For Comments).

2.4 Other Contributions

- I've helped to correct and to improve the AODV protocol, thing that has been acknowledged by their authors in the AODV RFC [36].

- I implemented AODV and tested the implementation in the first AODV interoperability test [2].

2.5 Brief Future Research Plan

- Continue enhancing SAODV, SAKM and SDYMO through the publication of new drafts.

- Study how to adapt SAODV to sensor networks. Although sensor networks are basically MANET networks, they have very specific needs (like data aggregation, etcetera) and a very specific routing pattern (typically, from sensors to the sink). Data aggregation should be done in a secure way and it could take advantage of the specificity of its routing patterns in order to make routing more efficient.

- Study how to modify SAODV in such a way that tries to minimize battery consumption. Routing protocols for fixed networks assumed that the nodes had unlimited amount of electricity. But, for MANET networks battery consumption is probably the most scarce resource. Most MANET routing protocols are not battery consumption aware. Nevertheless, minimizing battery consumption should be one of the main aims of a MANET routing protocol.