Mobile Ad Hoc Network Security- A Cluster based Approach

G. S. R. Emil Selvan[1,*], S. Sivagurunathan[2], P. Subathra[3], and S.Dina Nidhya[3]

[1] Department of Information Technology
Thiagarajar College of Engineering
Madurai 625015, India
emil@tce.edu

[2] Department of Computer Applications
Thiagarajar College of Engineering
Madurai 625015, India
ssncse@tce.edu

[3] Department of Computer Science and Engineering
Thiagarajar College of Engineering
Madurai 625015, India
(pscse, dina)@tce.edu

Received 0 July 2009; Revised 20 August 2009; Accepted 8 September 2009

Abstract. Security has become a prime concern in providing communication between mobile nodes in a hostile environment. Unlike wired networks, the unique characteristics of Mobile Ad Hoc Networks (MANETs) pose a number of non-trivial challenges to security design. This paper presents a threshold security mechanism with a mobility based D-hop (MobDHop) clustering algorithm. A new metric has been introduced to measure the variation of distance between nodes over time in order to estimate the relative mobility of two nodes. Nodes that have similar moving pattern are grouped into a cluster. Unlike other clustering algorithms, the diameter of clusters is not restricted to two hops. Instead, the diameters of clusters are flexible and determined by the stability of clusters. The stability of clusters is estimated based on relative mobility of cluster members. A threshold cryptographic scheme is employed to protect routing information and data traffic. To ensure distributed trust in the clustered environment, the private key (k) is divided into n pieces in such a way that **k** is easily reconstruct able from any p number of pieces. Even complete knowledge of (p-1) pieces reveals absolutely no information about k.

Keywords: Mobility, clustering, threshold cryptography, mobile ad hoc networks

References

[1] 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),* San Antonio, TX, January 27-31, 2002.

[2] A.B. McDonald and T.F. Znati. "A Mobility-based Framework for Adaptive Clustering in Wireless Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, Vol. 17, No. 18, pp. 1466-1486, August 1999.

[3] S.J. Lee, W. Su, M. Gerla, "Ad Hoc Wireless Multicast with Mobility Prediction," *Proceedings of IEEE ICCCN'99, Boston, MA*, pp. 4-9, October 1999.

[4] C.R. Lin and M. Gerla. "Adaptive Clustering for Mobile Wireless Networks," *IEEE Journal on Selected Areas in Communications*, Vol. 15, No. 7, pp. 1265-1275, September 1997.

[5] C. Konstantopoulos, D. Gavalas, G. Pantziou, "Clustering in Mobile Ad Hoc Networks through Neighborhood Stability-based Mobility Prediction," *Computer Networks*, Vol. 52, No. 9, pp. 1797-1824, June 2008.

[6] Martha Steenstrup, Bolt Beranek, Newman, "Cluster-based Networks," Ad Hoc Networking, C.E. Perklins, *Addison*

* Corresponding Author

Wesley, pp.75-183, 2001.

[7] P. Basu, N. Khan, T. D. C. Little. "Mobility Based Metric for Clustering in Mobile Ad hoc Networks," *IEEE ICDCSW'01*, pp. 413-418, April 2001.

[8] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang. "Security in Mobile Ad-Hoc Networks- Challenges and Solutions," *IEEE Transactions on Wireless Communications*, Vol.11, No. 1, pp. 38-47, February 2004.

[9] X. Hong, M. Gerla, G. Pei, C. Chiang. "A Group Mobility Model for Ad Hoc Wireless Networks," *Proceeding of ACM-IEEE MSWiM, Seattle, WA*., pp. 53-60, August 1999.

[10] M. Jiang, J.li, Y.C.Tay, "Cluster based Routing Protocol (CBRP) Functional Specification," *IETF Internet Draft, MANET working group*, August 1999.

[11] E.M.Belding-Royer, "Multi-level Hierarchies for Scalable Ad-hoc Routing," *ACM Wireless Networks*, Vol. 9, No. 5, pp. 461-478, 2003.

[12] D.B. Johnson and D.A. Maltz. "Dynamic Source Routing in Ad-Hoc Wireless Networks," *Mobile Computing*, Vol. 353, pp. 153-181, 1996.

[13] Murphy and J.J. Garcia-Luna-Aceves. "An Efficient Routing Algorithm for Mobile Wireless Networks," *MONET,* Vol. 1, No. 2, pp. 183-197, October 1996.

[14] V.D. Park and M.S. Corson. "A Highly Adaptable Distributed Routing Algorithm for Mobile Wireless Networks," *IEEE INFOCOMM'97*, Kobe, Japan, pp.1045, 1997.

[15] J. Sharony. "A Mobile Radio Network Architecture with Dynamically Changing Topology using Virtual Subnets," *Proceedings of ICC/SUPERCOM'96*, Dallas, TX, pp. 807-812, June 1996.

[16] M. Gannaro, S.Jarecki, H. Karawczyk, T. Rabin "Robust Threshold DSS Signatures," *Advances in Cryptology-Eurococrypt'96*, pp. 354-371, 1996.

[17] C.Kaufman. DASS: "Distributed Authentication Security Service," *RFC 1507*, September 1993.

[18] J.J Tado and K. Alagappan, "SPX: Global Authentication using Public Key Certificates," *Proceedings of the 1991 IEEE Symposium on Security and Privacy*, Oakland, CA USA, pp. 232-244, May 1991.

[19] Y. Desmedt "Threshold Cryptography," *European Transactions on Telecommunications,* Vol. 5, No. 4, pp. 449-457, July-August 1994.

[20] Y. Desmedt and Y. Frankel . "Threshold Crypto System," *Advances in Cryptology-Crypto'89, 9th Annual International Cryptology Conference*, pp. 307-315, 1990.

[21] C.S. Suzuki and K. Nakada, "An Authentication Technique based on Distributed Security Management for the Global Mobility Network," *Symposium on Security and Privacy, IEEE Computer Society Press*, Vol. 15, No. 8, pp. 1608-1617, May 1991.

[22] A. Shamir, "How to Share a Secret," *Communications of the ACM*. Vol. 22, No. 11, pp.612-613. November 1979.
http://www.Comp.nus.edu.sg~tayyc/cbrp/draft-ietf-manet-cbrp-spec-01.txt.

[23] The Network Simulator - ns-2. (2006), http://www.isi.edu/nsnam/ns/