

Scopus

Document details

< Back to results | 1 of 1

[Export](#)
[Download](#)
[Print](#)
[E-mail](#)
[Save to PDF](#)
[Add to List](#)
[More... >](#)

[Full Text](#)
[View at Publisher](#)

Proceedings - 2014 International Symposium on Biometrics and Security Technologies, ISBAST 2014
 16 January 2015, Article number 7013110, Pages 137-143
 2014 4th International Symposium on Biometrics and Security Technologies, ISBAST 2014; Corus Hotel Kuala LumpurKuala Lumpur; Malaysia; 26 August 2014 through 27 August 2014; Category numberCFP1459D-ART; Code 110143

SECRET: A secure and efficient certificate revocation scheme for Mobile Ad hoc Networks (Conference Paper)

Mall, D.^a [✉](#), Konate, K.^a [✉](#), Pathan, A.-S.K.^b [✉](#) [👤](#)

^aDepartment of Mathematics and Computer Science, Université Cheikh Anta Diop de Dakar, Dakar, Senegal, Malaysia

^bDepartment of Computer Science, International Islamic University Malaysia, Kuala Lumpur, Malaysia

Abstract

[View references \(23\)](#)

The intent of this paper is to propose an enhanced certificate revocation scheme for Mobile Ad hoc Networks (MANETs). Our approach is built on mainly two previously proposed mechanisms. A combination of the schemes and optimization of certain steps with intelligent choices of parameters could significantly reduce the overhead associated with such mechanism. We prove the efficiency of our approach by performance analysis. Also, we present the security analysis that shows clear gains than the previously proposed schemes. © 2014 IEEE.

Author keywords

ad hoc certificate key mobile network revocation

Indexed keywords

Engineering controlled terms: Biometrics Networks (circuits) Telecommunication networks

ad hoc certificate
key mobile
revocation

Engineering main heading: Mobile ad hoc networks

Funding details

Funding number	Funding sponsor	Acronym
	Korea Institute of Construction Technology	KICT

ISBN: 978-147996444-4
Source Type: Conference Proceeding
Original language: English

DOI: 10.1109/ISBAST.2014.7013110
Document Type: Conference Paper
Sponsors:
Publisher: Institute of Electrical and Electronics Engineers Inc.

Metrics [View all metrics >](#)

1 Citation in Scopus
 75th Percentile
 1.21 Field-Weighted Citation Impact



PlumX Metrics [v](#)

Usage, Captures, Mentions, Social Media and Citations beyond Scopus.

Cited by 1 document

Revocation and update of trust in autonomous delay tolerant networks

Djamaludin, C.I. , Foo, E. , Camtepe, S. (2016) *Computers and Security*

[View details of this citation](#)

Inform me when this document is cited in Scopus:

[Set citation alert >](#)
[Set citation feed >](#)

Related documents

Key revocation for identity-based schemes in mobile ad hoc networks



Hoeper, K. , Gong, G. (2006) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*

Identity-based key management

Ramanuj, P. , Shah, J.S. (2016) *Advances in Intelligent Systems and Computing*

A survey of key revocation schemes in mobile ad HOC networks

References (23)

[View in search results format >](#) All [Export](#)  [Print](#)  [E-mail](#) [Save to PDF](#) [Create bibliography](#)

-
- 1 Zhou, L., Haas, Z.J.
Securing ad hoc networks

(1999) *IEEE Network*, 13 (6), pp. 24-30. Cited 1573 times.
doi: 10.1109/65.806983

[View at Publisher](#)
-
- 2 Luo, H., Zerfos, P., Kong, J., Lu, S., Zhang, L.
Self-securing ad hoc wireless networks

(2002) *Proceedings - IEEE Symposium on Computers and Communications*, art. no. 1021731, pp. 567-574. Cited 264 times.
ISBN: 0769516718; 978-076951671-4
doi: 10.1109/ISCC.2002.1021731

[View at Publisher](#)
-
- 3 Crépeau, C., Davis, C.R.
A certificate revocation scheme for wireless ad hoc networks

(2003) *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Security of Ad Hoc and Sensor Networks (in Association with 10th ACM Conference on Computer and Communications Security)*, pp. 54-61. Cited 37 times.
ISBN: 1581137834
-
- 4 Khan Pathan, A.-S., Hong, C.S.
Feasibility of PKC in resource-constrained wireless sensor networks

(2008) *Proceedings of 11th International Conference on Computer and Information Technology, ICCIT 2008*, art. no. 4803120, pp. 13-20. Cited 6 times.
ISBN: 978-142442136-7
doi: 10.1109/ICCITECHN.2008.4803120

[View at Publisher](#)
-
- 5 Mall, D., Konaté, K., Pathan, A.-S.K.
On the key revocation schemes in wireless sensor networks

(2013) *Proceedings - 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, GreenCom-iThings-CPSCoM 2013*, art. no. 6682080, pp. 290-297. Cited 4 times.
ISBN: 978-076955046-6
doi: 10.1109/GreenCom-iThings-CPSCoM.2013.66

[View at Publisher](#)
-
- 6 Deng, H., Mukherjee, A., Agrawal, D.P.
Threshold and identity-based key management and authentication for wireless ad hoc networks

(2004) *International Conference on Information Technology: Coding Computing, ITCC*, 1, pp. 107-111. Cited 110 times.
ISBN: 0769521088; 978-076952108-4
-

Fan, X. , Gong, G.
(2011) *Handbook of Security and Networks*

[View all related documents based on references](#)

[Find more related documents in Scopus based on:](#)

[Authors >](#) [Keywords >](#)

-
- 7 Hubaux, J.-P., Buttyán, L., Čapkun, S.
The quest for security in mobile ad hoc networks
(2001) Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and Computing: MobiHoc 2001, pp. 146-155. Cited 489 times.
ISBN: 1581134282
-
- 8 Khalili, A., Katz, J., Arbaugh, W.A.
Toward secure key distribution in truly ad-hoc networks
(2003) Proceedings - 2003 Symposium on Applications and the Internet Workshops, SAINT 2003, art. no. 1210183, pp. 342-346. Cited 195 times.
ISBN: 0769518737; 978-076951873-2
doi: 10.1109/SAINTW.2003.1210183

View at Publisher
-
- 9 Luo, H., Kong, J., Zerfos, P., Lu, S., Zhang, L.
URSA: Ubiquitous and robust access control for mobile ad hoc networks
(2004) IEEE/ACM Transactions on Networking, 12 (6), pp. 1049-1063. Cited 183 times.
doi: 10.1109/TNET.2004.838598

View at Publisher
-
- 10 Arboit, G., Crépeau, C., Davis, C.R., Maheswaran, M.
A localized certificate revocation scheme for mobile ad hoc networks
(2008) Ad Hoc Networks, 6 (1), pp. 17-31. Cited 40 times.
doi: 10.1016/j.adhoc.2006.07.003

View at Publisher
-
- 11 Fan, X., Gong, G.
Key revocation based on Dirichlet multinomial model for mobile ad hoc networks
(2008) Proceedings - Conference on Local Computer Networks, LCN, art. no. 4664309, pp. 958-965.
ISBN: 978-142442413-9
doi: 10.1109/LCN.2008.4664309

View at Publisher
-
- 12 Hoepfer, K., Gong, G.
Key revocation for identity-based schemes in mobile ad hoc networks
(2006) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 4104 LNCS, pp. 224-237. Cited 18 times.
<http://springerlink.com/content/0302-9743/copyright/2005/>
ISBN: 3540372466; 978-354037246-2

View at Publisher
-
- 13 Moore, T., Clulow, J., Nagaraja, S., Anderson, R.
New strategies for revocation in ad-hoc networks
(2007) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 4572 LNCS, pp. 232-246. Cited 29 times.
ISBN: 978-354073274-7

View at Publisher
-

-
- 14 Zhang, Y., Liu, W., Lou, W., Fang, Y.
Securing mobile ad hoc networks with certificateless public keys
(2006) *IEEE Transactions on Dependable and Secure Computing*, 3 (4), pp. 386-399. Cited 128 times.
doi: 10.1109/TDSC.2006.58
[View at Publisher](#)
-
- 15 Hoepfer, K.
(2007) *Authentication and Key Exchange in Mobile Ad Hoc Networks*. Cited 4 times.
Ph. D. thesis, Univ. of Waterloo, Waterloo, Canada
-
- 16 Hoepfer, K., Gong, G.
(2009) *Monitoring-based Key Revocation Schemes for Mobile Ad Hoc Networks: Design and Security Analysis*. Cited 2 times.
Technical Report 9 2009-15, Centre for Applied Cryptographic Research, March
-
- 17 Akbani, R., Korkmaz, T., Raju, G.V.S.
HEAP: Hop-by-hop efficient authentication protocol for mobile Ad-hoc networks
(2007) *Simulation Series*, pp. 157-165. Cited 3 times.
ISBN: 1565553128; 978-156555312-5
-
- 18 Perrig, A., Canetti, R., Song, D., Tygar, D.
The TESLA broadcast authentication protocol
(2002) *RSA Cryptobytes*, pp. 2-13. Cited 418 times.
-
- 19 Zhu, S., Xu, S., Setia, S., Jajodia, S.
LHAP: A lightweight hop-by-hop authentication protocol for ad-hoc networks
(2003) *Proceedings - 23rd International Conference on Distributed Computing Systems Workshops, ICDCSW 2003*, art. no. 1203642, pp. 749-755. Cited 63 times.
ISBN: 0769519210; 978-076951921-0
doi: 10.1109/ICDCSW.2003.1203642
[View at Publisher](#)
-
- 20 Lu, B., Pooch, U.W.
A lightweight authentication protocol for mobile Ad hoc networks
(2005) *International Conference on Information Technology: Coding and Computing, ITCC, 2*, pp. 546-551. Cited 15 times.
ISBN: 0769523153; 978-076952315-6
-
- 21 Hoepfer, K., Gong, G.
Identity-based key exchange protocols for ad hoc networks
(2005) *Canadian Workshop on Information Theory (CWIT'05)*. Cited 3 times.
-
- 22 Hortensius, L.
Dirichlet Distribution
Last accessed: 28 April, 2014
<http://www.tc.umn.edu/~horte005/docs/Dirichletdistribution.pdf>
-

- 23 Krawczyk, H., Bellare, M., Canetti, R.
 HMAC: Keyed-hashing for message authentication
 (1997) *Internet Request for Comments (RFC 2104)*. Cited 281 times.
 February

👤 Mall, D.; Department of Mathematics and Computer Science, Université Cheikh Anta Diop de Dakar, Dakar, Senegal, Malaysia
 © Copyright 2015 Elsevier B.V., All rights reserved.

< Back to results | 1 of 1

^ Top of page

About Scopus

- What is Scopus
- Content coverage
- Scopus blog
- Scopus API
- Privacy matters

Language

- 日本語に切り替える
- 切换到简体中文
- 切换到繁體中文
- Русский язык

Customer Service

- Help
- Contact us

ELSEVIER

[Terms and conditions](#) [Privacy policy](#)

Copyright © 2017 Elsevier B.V. All rights reserved. Scopus® is a registered trademark of Elsevier B.V.

Cookies are set by this site. To decline them or learn more, visit our [Cookies page](#).

 RELXGr