AUN/SEED-Net JICA

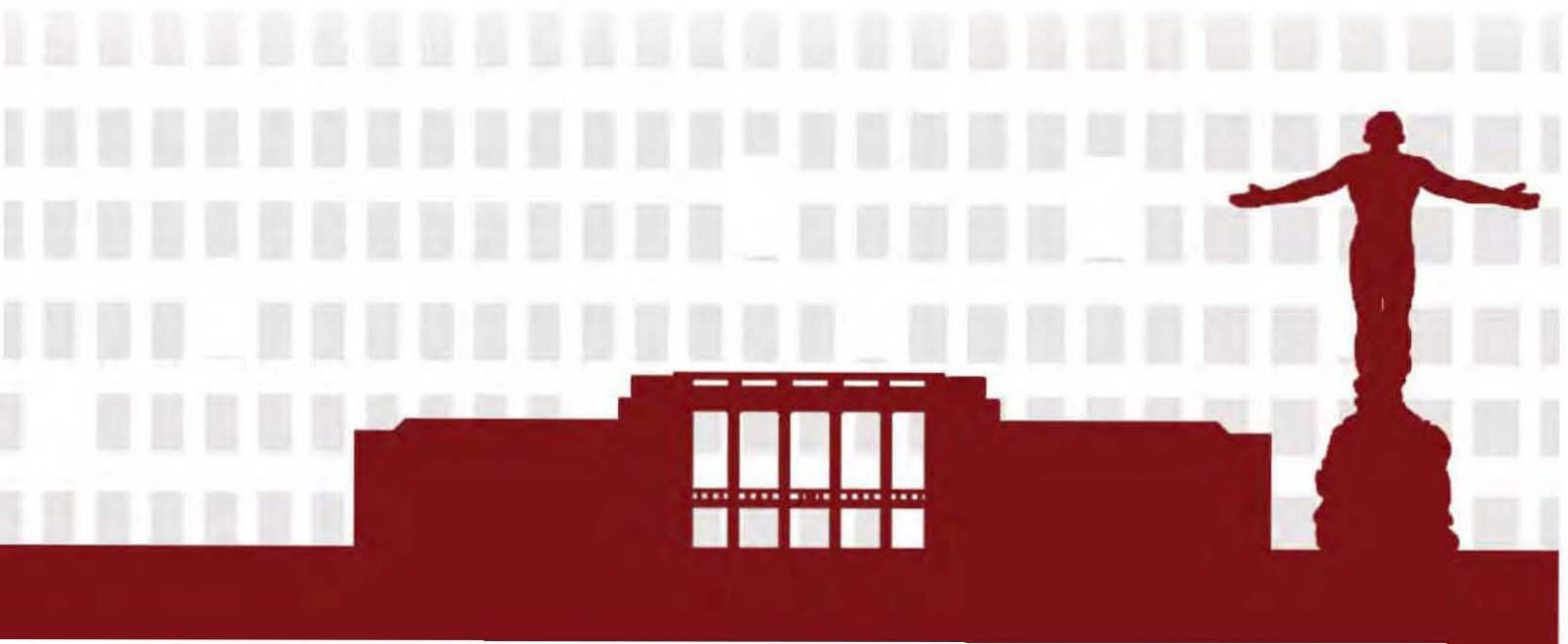
# 8th AUN/SEED-Net
## REGIONAL CONFERENCE ON ELECTRICAL AND ELECTRONICS ENGINEERING

Envision, Enable, and Empower
Smarter and Resilient Societies

*co-located with*

# 11th ERDT Conference
## on Semiconductor and Electronics, Information and Communications Technology and Energy

**16-17 November 2015**
**Metro Manila, Philippines**



**Proceedings of the 8th AUN/SEED-Net RCEEE 2015 and 11th ERDT Conference**
**on Semiconductor and Electronics, Information and Communications Technology, and Energy**

Editors:
Dr. Joel Joseph S. Marciano Jr.
Dr. Jhoanna Rhodette I. Pedrasa
Dr. Rhandley D. Cajote



ISBN: 978-616-406-075-3

Published by: ASEAN University Network / Southeast Asia Engineering Education Development Network (AUN/SEED-Net) JICA Project
Faculty of Engineering, Bldg. 2
Chulalongkorn University, Bangkok
Thailand 10330

Printed in the Philippines by: ERZALAN PRINTING PRESS
45 Cotabato Street, Luzviminda Village, Batasan Hills, Quezon City, Philippines

# 8th AUN/SEED-Net Regional Conference
## on Electrical and Electronics Engineering 2015

co-located with

# 11th ERDT Conference
## on Semiconductor and Electronics, Information and Communications Technology, and Energy

# Envision, Enable and Empower Smarter and Resilient Societies

Published by: ASEAN University Network / Southeast Asia Engineering Education Development Network (AUN/SEED-Net) in partnership with Engineering Research and Development for Technology (ERDT) and University of the Philippines Diliman.


ISBN: 978-616-406-075-3

# CXSENSE: A SCALABLE PASSWORD-BASED KEY MANAGEMENT SCHEME FOR MOBILE AD-HOC NETWORKS

**James Patrick A. Acang[1,2,*] and Susan P. Festin[1]**

[1]Department of Computer Science, University of the Philippines Diliman, PHILIPPINES.
[2]Department of Computer Science, Mariano Marcos State University, PHILIPPINES.
[*]E-mail: jamespatrickacang@gmail.com

## ABSTRACT

In a dynamic mobile ad-hoc network (MANET), nodes cooperatively participate to facilitate delivery of messages. Nodes establish links with other nodes, forming an arbitrary self-organized network where each node may route messages from the source to the destination. Since messages need to be passed from one node to the other before reaching the intended recipient, security becomes an important concern.

A key ingredient to try and secure messages in a MANET is an efficient key management scheme. Most of the existing schemes, however, have relied on trusted third parties, certificate authorities, and more powerful nodes to facilitate key management. Moreover, these components may make MANETs restrictive, unscalable, impractical to implement, and may require the network to have centralized administration. This can negatively impact on the self-organization aspects of a MANET.

We propose here a new key management scheme that follows the self-organization property of MANETs. This enables nodes to join and communicate freely without third party authorities to facilitate in the secured communication. We exploit here the characteristics of multicast communication to improve performance and to enhance scalability. We compared the performance of our scheme with two existing schemes via simulation. Our results show that our proposed scheme have performance gains over the existing schemes.

**Keywords**: Ad-hoc Network, Key management, MANET, Network security, Password-based, Scalable.

**Acknowledgment**

The authors would like to express appreciation for the support of the Engineering Research and Development for Technology (ERDT), the Science Education Institute of the Department of Science and Technology (DOST-SEI), and the Mariano Marcos State University (MMSU).

**References**

[1] S. Bellovin and M. Merritt. "Augmented Encrypted Key Exchange: A Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise". In: Conference on Computer and Communications Security. 1993, pp. 244–250.

[2] S.M. Bellovin and M. Merritt. "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks". In: Proc. IEEE Symp. Security and Privacy. 1992, pp. 72–84.

[3] BonnMotion. 2014. URL: http://sys.cs.uos.de/bonnmotion/doc/BonnMotion_Docu.pdf.

[4] D. Boneh, X. Boyen and H. Shacham. "Short Group Signatures". In: Advances in Cryptology–Crypto'04, Lecture Notes in Computer Science. Vol. 3152. 2004, 41–55.

[5] K. Sadasivam, V. Changrani and T. Yang. Scenario Based Performance Eveluation of Secure Routing in MANETs. 2014. URL: http://sce.uhcl.edu/sadasivamk/ MANETII05-draft.pdf.

[6] Y. Yeh, W. Ku, W. Chen and Y. Chen. "An Enhanced Simple Secure Remote Password Authentication Scheme without using Cryptography". In: Proc. 2012 1st IEEE International Conference on Communications in China (ICCC). 2012, pp. 231–235.

[7] S. Ehrampoosh and A. Mahani. “Secure Routing Protocol: Affection on MANETs Performance”. In: International Journal of Communications and Information Technology. Vol. 1. 2011, pp. 7–15.

[8] E. Igbesoko, T. Eze and M. Ghassemian. Performance Analysis of MANET Routing Protocols over Different Mobility Models. 2014. URL: http://www.ee.ucl.ac.uk/lcs/previous/LCS2010/lens2010.

[9] P. Felman. “A Practical Scheme for Non-Interactive Verifiable Secret Sharing”. In: Proceedings of the 28th Annual Symposium on the Foundations of Computer Science. 1987.

[10] S. Hwang and M. Chai. “A New Authenticated Key Agreement Protocol for Wireless Mobile Networks”. In: 5th International Conference on Information Assurance and Security (IAS ’09). Vol. 1. 2009, pp. 53–56.

[11] Introduction to R. 2014. URL: http://www.r-project.org/.

[12] T. Khdour and A. Aref. “A Hybrid Schema Zone- Based Key Management for MANETS”. In: Journal of Theoretical and Applied Information Technology. Vol. 35. 2012.

[13] E. Kushilevits and N. Nisan. Communication Complexity. 1997.

[14] F. Liu, S. Luo and C. Ren. “Cryptanalysis and Improvement of a Password-Based Key Exchange Protocol”. In: 2008 International Conference on Machine Learning and Cybernetics. Vol. 7. 2008, pp. 3668–3672.

[15] NS2. 2014. URL: http://www.isi.edu/nsnam/ns/.

[16] M. Saeed, A. Mackvandi, M. Naddafiun and H.R. Karimnejad. “An Enhanced Password Authenticated Key Exchange Protocol without Server Public Keys”. In: 2012 International Conference on ICT Convergence (ICTC). 2012, pp. 87–91.

[17] B. Aziz, E. Nourdine and E.-K. Mohamed. “A Recent Survey on Key Management Schemes in MANET”. In: 3rd International Conference on Information and Communication Technologies: From Theory to Applications. 2008, pp. 1–6.

[18] A. Menezes, P. Oorschot and S. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996.

[19] C. Paar and J. Pelz. Understanding Cryptography. 2010.