Lightweight Group Key Establishment for Reducing Memory Overhead

Siti Agustini*,**, Wirawan*, Gamantyo Hendrantoro*

*Department of Electrical Engineering, Institut Teknologi Sepuluh Nopember, Surabaya 60111, Indonesia

**Department of Informatics, Institut Teknologi Adhi Tama Surabaya, Surabaya 60117, Indonesia

7022211005@mhs.its.ac.id, wirawan@ee.its.ac.id, gamantyo@ee.its.ac.id

***Abstract*— Wireless Sensor Network (WSN) and Internet of Things (IoT) allow sensor devices to collect information about various critical sectors through wireless networks. However, when the WSNs are connected to a public network, the security of the WSN is vulnerable. Besides, WSN needs a key distribution scheme to secure data among other sensor devices. Furthermore, IoT devices have low computing, energy, and memory storage capabilities. Thus, designing a lightweight, efficient, and secure protocol communication for WSN is always a challenge due to the resource constraint of sensor devices. The existing schemes result in the number of keys stored by sensor devices depending on group size. When the group size increases, the number of the stored key by the sensor also increases. Other research proposes key establishment based on polynomial multiplicative and causes high computational capability. This paper proposed a key distribution scheme based on (p,q)-Lucas polynomial and XOR to achieve lightweight, memory overhead efficiency and security. The proposed method is evaluated in several parameters: memory overhead, communication overhead, energy consumption, computational complexity analysis, and security. The results indicate that our scheme outperforms the existing approaches regarding memory overhead, computation efficiency, and support security.**

***Keyword*— Group key establishment, WSN, Lucas polynomial, memory overhead, information security, key distribution.**

Siti Agustini was born in 1990. She received a bachelor's degree in telecommunication engineering from Electronic Engineering Polytechnic Institute of Surabaya (EEPIS), Surabaya, Indonesia, in 2012 and a master's degree in Department of Electrical Engineering from Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia in 2014. Currently, she is pursuing a Ph.D. degree with the Department of Electrical Engineering, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia. Her research interests include wireless communication, computer networks, wireless sensor networks, and cryptography, especially information security.

Wirawan was born in 1963. He received his bachelor's degree in 1987 from the Department of Electrical Engineering, Institute Teknologi Sepuluh Nopember, Surabaya. In 1996 and 2003, he received the DEA degree from Ecole Nationale Superieure d'Informatique (ESSI), Universite Nice Sophia Antipolis (UNSA), France, and the Ph.D. degree from Telecom ParisTech, Paris, France, (ENST), respectively. He is a lecturer in the Department of Electrical Engineering, Institut Teknologi Sepuluh Nopember, Surabaya. His research area involves wireless ad hoc networks, wireless communications, multimedia signal processing, underwater acoustics communication and networking, and sensor networks.

Gamantyo Hendrantoro (Senior Member, IEEE) was born in 1970. He received the B.Eng. degree in 1992 from Institut Teknologi Sepuluh Nopember (ITS), Surabaya, Indonesia, and the M.Eng. and Ph.D. degree from Carleton University, Ottawa, Canada in 1997 and 2001, all in the Department of Electrical Engineering. He is currently a Professor in the Department of Electrical Engineering, ITS. His research interests include wireless communications, channel modeling, wireless system for tropical areas, millimeter-wave propagation, signal processing, and radio propagation channel modeling.