

# Security Analysis of Hybrid Security Mechanisms for Heterogeneous Sensor Networks

Mangal Sain, Ki Hwan Kim, Hoon Jae Lee

*Department of Computer Engineering, Dongseo University, Busan, South Korea*

*mangalsain1@gmail.com, gend90@gmail.com, hjee@dongseo.ac.kr*

**Abstract**— An efficient hybrid security mechanism (called LIGER) for heterogeneous sensor networks (HSNs) was presented by Traynor et al. LIGER is composed of two subschemes: LION and TIGER. However, this paper presents the LIGER has some designs and security flaws, and cannot be advocated for the real-time critical applications. We have identified that LION and TIGER are vulnerable to the impersonation attacks, gateway-bypass attacks, denial-of-service attacks, and man-in-the-middle attacks. Moreover, both schemes do not care about the dynamic session key which is an indispensable security requirement for the real-time heterogeneous sensor networks.

**Keyword**— Authentication, session-key establishment, gateway bypass attack, man-in-the-middle attack



**Mangal Sain** received the M.Sc. degree in computer application from India in 2003 and the Ph.D. degree in computer science in 2011. Since 2012, he has been an Assistant Professor with the Department of Computer Engineering, Dongseo University, South Korea. His research interest includes wireless sensor network, cloud computing, Internet of Things, embedded systems, and middleware. He has authored over 30 international publications including journals and international conferences. He is a member of TIIS and a TPC member in several international conferences



**Ki Hwan Kim**

2013: BS at Dongseo University, Republic of Korea  
2015: MS at Dongseo University, Republic of Korea  
2015 ~ current: doctor's course Dongseo University, Republic of Korea  
Research Interests: Wireless Sensor Networks, Cryptography and Network Security, Side Channel Analysis



**Hoon-Jae Lee** received his BS, MS, and PhD. degrees in Electrical Engineering from Kyungpook National University, Daegu, South Korea, in 1985, 1987, and 1998, respectively. He is currently a professor in the Department of Information and Communication Engineering at Dongseo University. From 1987 to 1998, he was a research associate at the Agency for Defense Development (ADD). His current research interests include developing secure communication system, side-channel attack, and ubiquitous sensor network/radio frequency identification security.