Multivariate Symmetric Polynomial Based Group Key Management (MSPGKM) for Vehicular Ad hoc Networks

By
Dr. Dharma P. Agrawal
Ohio Board of Regents Distinguished Professor and
Director, Center for Distributed and Mobile Computing
Center for Distributed and Mobile Computing
University of Cincinnati, Cincinnati, OH 452221-0030
Tel: 513-556-4756 E-mail: dpa@cs.uc.edu web: www.cs.uc.edu/~dpa

Vehicular Ad hoc Networks (VANETs) are emerging as the first commercial implementation of mobile ad hoc networks. There has been a significant rise in the use of secure group communication as a result of the growth in the applications that require confidentiality and authorized access to multicast data. Numerous Group Key Management (GKM) schemes have been proposed to meet the security and QoS requirements. The highly dynamic nature of VANETs can cause significant overhead in the form of re-keying communication, if these existing GKMs are to be used. Hence, we identify the need for new solutions specific to VANETs and introduce a multivariable symmetric polynomial based GKM which eliminates the need for the re-distribution of keys upto a configurable number of membership changes, without compromising the forward or the backward secrecy. Furthermore, our scheme reduces the effect of mobility on the re-keying overhead by allowing vehicles to handoff between road side units (RSUs) within the group without re-keying.

Short Biography

Dharma P. Agrawal is the Ohio Board of Regents Distinguished Professor and the founding director for the Center for Distributed and Mobile Computing in the School of Computing Sciences and Informatics. He has been a faculty member at the ECE Dept., Carnegie Mellon University (on sabbatical leave), N.C. State University, Raleigh and the Wayne State University. His current research interests include resource allocation in wireless mesh networks, query processing and secured communication in sensor networks, environmental monitoring using sensor networks, and effective traffic handling in integrated wireless networks. His recent contribution in the form of a co-authored introductory text book on *Wireless and Mobile Computing* has been widely accepted throughout the world and third edition has just been published. The book has been has been reprinted both in China and India and translated in to Korean and Chinese languages. His co-authored book on *Ad hoc and Sensor Networks, 2nd edition,* has

been published in spring of 2011. A co-edited book entitled, *Encyclopedia on Ad Hoc and Ubiquitous Computing*, has been published by the World Scientific and co-authored books entitled *Wireless Sensor Networks: Deployment Alternatives and Analytical Modeling,* and *Innovative Approaches to Spectrum Selection, Sensing, On-Demand Medium Access in Heterogeneous Multihop Networks*, and *Sharing in Cognitive Radio Networks* have being published by Lambert Academic.

He is an editor for the *Journal of Parallel and Distributed Systems*, founding Editorial Board Member, I*nternational Journal on Distributed Sensor Networks*, *International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC), International Journal of Ad Hoc & Sensor Wireless Networks* and *the Journal of Information Assurance and Security (JIAS)*. He has served as an editor of the IEEE *Computer magazine*, and the *IEEE Transactions on Computers and* the *International Journal of High Speed Computing*. He has been the Program Chair and General Chair for numerous international conferences and meetings. He has received numerous certificates from the IEEE Computer Society. He was awarded a *Third Millennium Medal*, by the IEEE for his outstanding contributions. He has delivered keynote speech at 25 different international conferences. He has published over 592 papers, given 32 different tutorials and extensive training courses in various conferences in USA, and numerous institutions in Taiwan, Korea, Jordan, UAE, Malaysia, and India in the areas of Ad hoc and Sensor Networks and Mesh Networks, including security issues. He has graduated **62 PhDs and 52 MS students**. He has been named as an **ISI Highly Cited Researcher**, is a Fellow of the **IEEE,** the **ACM**, the **AAAS** and the **World Innovation Foundation,** and a recent recipient of **2008 IEEE CS Harry Goode Award**. In June 2011, he was selected as the **best Mentor for Doctoral Students** at the University of Cincinnati. Recently, he has been inducted as a **charter fellow of the National Academy of Inventers.** He has also been elected a **Fellow of the IACSIT** (International Association of Computer Science and Information Technology), 2013.