A
Dissertation
On

"AN ECC-TIMESTAMP BASED MUTUAL AUTHENTICATION AND KEY MANAGEMENT SCHEME FOR WSNs"

Submitted in partial fulfilment of the requirement of

Delhi Technological University, for the award of degree of

MASTER OF TECHNOLOGY
In
"Software Engineering"

Submitted By:
GAURAV INDRA
University Roll No. 07/SE/09
University Registration No. 01/MT/SE/FT

Under the Guidance of:
Dr. Daya Gupta
Professor, Head of Department
Department Of Computer Engineering
Delhi Technological University, Delhi

DEPARTMENT OF COMPUTER ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY

2009-2011

CERTIFICATE

DELHI TECHNOLOGICAL UNIVERSITY
(Govt. of National Capital Territory of Delhi)
BAWANA ROAD, DELHI – 110042

Date: _____

This is to certify that this thesis entitled **"An ECC-Timestamp based Mutual Authentication and Key Management Scheme for WSNs"** which is submitted by **Gaurav Indra, University Roll No. 07/SE/09** in the partial fulfilment of the requirement for the award of degree of **Master of Technology** in **Software Engineering** at **Delhi Technological University, Delhi** is a record of the candidate own work carried out by him under my supervision. The matter embodied in this thesis is original and has not been submitted for the award of any other degree.

Dr. Daya Gupta
Professor, Head of Department
Department of Computer Engineering
Delhi Technological University, Delhi

ACKNOWLEDGEMENT

I would like to take this opportunity to thank my project guide, **Dr. Daya Gupta, Professor, Head of Department, Department of Computer Engineering, Delhi Technological University,** for her support, guidance and patience during my studies at the Delhi Technological University. She gave me the freedom to explore the domain of Key Management in Wireless Sensor Networks. She invested her most valuable resource on my behalf: her time. She helped in pointing out places in several drafts of the thesis where clarity could be improved and claims made more precise.

I would also like to extend my deepest gratitude to my project guide and research advisor, **Mrs. Kakali Chatterjee**, **Research Scholar, Department of Computer Engineering, D.T.U,** for her patience and guidance throughout my research and also for sharing her knowledge and experience with me. Her continued support led me to the right way.

I would also like to thank all the faculty members and staff members of Department of Computer Engineering at Delhi Technological University for sharing their knowledge and experiences with me as well as for their support.

I would also like to thank honourable **Prof. P.B. Sharma, Vice Chancellor, Delhi Technological University,** for taking the initiative of starting the course of Master of Technology in Software Engineering at Delhi Technological University in the year 2009.

Finally, I am thankful to almighty God and my parents for having granted me the skills and opportunities that made this work possible.

Gaurav Indra
University Roll No. 07/SE/09
Master of Technology (Software Engineering)
Department of Computer Engineering
Delhi Technological University, Delhi

ABSTRACT

Public Key Cryptography has been playing an important and vital role in providing security in various domains including secure electronic transactions in distributed environment and secure communication between different nodes in a wireless ad-hoc network. The security in Wireless Sensor Networks is currently provided mostly through symmetric key cryptography. The proposed protocols in this domain are mainly based on the idea of keys before the deployment of the Wireless Sensor Network. However, due to the limitation on memory resources of wireless sensor nodes, these protocols are not able to achieve perfect security and also face a key management problem in large scale wireless sensor networks. On the other hand asymmetric key cryptography offers flexibility to node and clean interface for the security component in the sensor network.

This thesis proposes a novel Mutual Authentication and Key Management Scheme for a particular session between any two corresponding nodes of a Wireless Sensor Network based on Elliptic Curve Cryptography with a novel Timestamp Mechanism. Nevertheless the same Mutual Authentication and Key Management Scheme for a particular session in WSNs can be extended efficiently for a multi-session scenario in domain of WSNs or in the wired or wireless ad-hoc networks.