

**A
Dissertation
On**

“Wireless Sensor Network Security Mechanism”

**Submitted in Partial fulfillment of the requirement
For the award of Degree of**

**MASTER OF TECHNOLOGY
IN
Computer Science Engineering
Delhi Technological University, Delhi**

SUBMITTED BY

**Avant Panwar
University Roll No: 02K11/CSE/03**

UNDER THE GUIDANCE OF

**Mr. Manoj Kumar
Associate Professor
Delhi Technological University**



**DEPARTMENT OF COMPUTER ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
2011-2013**

CERTIFICATE

This is to certify that the work contained in this dissertation entitled “**Wireless Sensor Network Security Mechanism**” submitted in the partial fulfillment, for the award for the degree of M.Tech in Computer Science Engineering at **DELHI TECHNOLOGICAL UNIVERSITY** by **AVANT PANWAR, Roll No. 2K11/CSE/03** is carried out by him under my supervision. This matter embodied in this project work has not been submitted earlier for the award of any degree or diploma in any university/institution to the best of our knowledge and belief.

(Mr. Manoj Kumar)
Project Guide
Associate Professor
Department of Computer Engineering
Delhi Technological University

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to all the people who have supported and encouraged me during the course of this project without which, this work could not have been accomplished. First of all, I am very grateful to my project supervisor Mr Manoj Kumar for providing his guidance. I am deeply indebted to him for his support, advice and encouragement without which the project could not have been completed. Further I extend my thanks to all my friends and family for their continued support and encouragement throughout the research work.

I would like to thank my guide for his sparking ideas, inspiring discussions, his trust and belief, and his support throughout the process of the thesis. I gained a lot from his vast knowledge and skill in many areas and appreciate his assistance in writing this dissertation.

AVANT PANWAR

(University Roll No.: 02K11/CSE/03)

Abstract

The salient features of WSN like use of wireless radio communication, collaborative nature and deployment in the open environment exposes it to many security threats. Since WSN has tight limitations on the power consumption, transmission and computation the complex cryptographic algorithms can't be used to provide the security. Key management in WSN is the fundamental line of defense for a secure communication and thus it is very important. The use of single key for secure communication is not a good idea as if the node gets compromised all the key material will be extracted by the adversary which poses a great threat to the network. Moreover uses of traditional public key cryptography schemes are not suited to the WSN due to the tight constraints on the power, computation and transmission.

In this thesis we propose a new framework for enhanced Secure Key management for hierarchical WSN which enhances the security of the network. In our proposed work the base station computes all the keys required for both inter and intra cluster communications. Cluster is further isolated into small geographical areas on the basis of hop count from the cluster head. The sensor nodes in the network join the cluster on the basis of the distance (hop counts) from the cluster head which localizes the path key things and reduces the overhead.

Dissemination

1. Avant Panwar, Manoj Kumar and Sajendra Kumar “New Framework for Enhanced Secure Key Management in Hierarchical Wireless Sensor Network” in International Journal of Computer Applications (IJCA) July 2013 Edition. Accepted for Publication(Paper Reference ID: pxc3889730)

Table of Contents

Certificate	ii
Acknowledgement	iii
Abstract	iv
Dissemination	v
LIST OF FIGURE	viii
LIST OF TABLES	ix
1. INTRODUCTION.....	1
1.1. Wireless Sensor Network	1
1.2. Salient Features of Wireless Sensor Network.....	2
1.3. Application Of WSN.....	3
1.4. Security In WSN	5
1.5. Overview Of Thesis	7
2. Key Management and Security In WSN.....	9
2.1. Security In WSN.....	9
2.2. Security And Vulnerability Requirements in WSN.....	9
2.3. Security Requirements In WSN.....	11
2.4. Security Attacks In WSN.....	13
2.5. Security Mechanism.....	18
2.6. Key Management In WSN	21
2.7. Key Management Phases.....	22
2.8. Key Management Schemes	23

3. Key Distribution In Hierarchical WSN.....	25
3.1 Pair-wise Key Distribution.....	25
3.2 Group-Wise Key Distribution.....	27
3.3 Network Wise Key Distribution	28
4. Literature Review	32
5. Proposed Work	42
5.1. Framework For Enhanced Secure Key Management For Hierarchical WSN.....	43
5.1.1. Key Pre Distribution	44
5.1.2. Pair wise Key Establishment	45
5.1.3. Computing Path Key	48
5.1.4. Re-Key Process	50
6. Security Analysis And Experimental Results.....	52
6.1. Environmental Setup.....	52
6.2. Security Analysis	53
6.3. Experimental Setup	54
7. Conclusion And Future Scope.....	60

REFERENCES

APPENDIX

List Of Figures

Figure 1: Wireless Sensor Network Architecture	02
Figure 2: Overview of Sensor Applications	05
Figure 3: Hello Flooding Attack	15
Figure 4: Black Hole Attack on Cluster Network	16
Figure 5: Wormhole Attack	17
Figure 6: Sinkhole Attack	17
Figure 7: Sinkhole Attack with Wormhole Attack	18
Figure 8: Message from CH to BS	45
Figure 9: The Network Setup for TTL = 3	46
Figure 10: Message from BS to CH	46
Figure 11: Beacon Message from CH to SN	47
Figure 12: ACK Message from SN to CH	47
Figure 13: Message from BS to CH for Group Key	47
Figure 14: The different hope ranges from the CH	48
Figure 15: Re-election of the Cluster Head	51
Figure 16: MATLAB Network Creation	55
Figure 17: MATLAB Parameters for the experiment	56
Figure 18: MATLAB Network GUI	57
Figure 19: MATLAB Sensor Networks with Intrusion Nodes	58
Figure 20: MATLAB Graph for Experiment	59

List Of Tables

Table 1: Constraints of WSN and their Security Implications	07
Table 2: Overview of the Key Distribution Schemes	31