

SECURE DATA AGGREGATION SCHEME  
FOR SENSOR NETWORKS

A Dissertation

Submitted to the Faculty

of

Purdue University

by

Kavit Shah

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science in Electrical and Electronics Engineering

December 2014

Purdue University

Indianapolis, Indiana

This is the dedication.

## ACKNOWLEDGMENTS

This is the acknowledgments.

## PREFACE

This is the preface.

## TABLE OF CONTENTS

	Page
LIST OF TABLES . . . . .	vi
LIST OF FIGURES . . . . .	vii
SYMBOLS . . . . .	viii
ABBREVIATIONS . . . . .	ix
NOMENCLATURE . . . . .	x
GLOSSARY . . . . .	xi
ABSTRACT . . . . .	xii
1 Introduction . . . . .	1
2 Security/Data Aggregation Background . . . . .	2
3 Security/Networking/Cryptography tools . . . . .	3
4 In-network Data-Aggregation Overview . . . . .	4
5 Background on SIA . . . . .	5
6 A Protocol for Commitment Tree Generation . . . . .	6
LIST OF REFERENCES . . . . .	7

## LIST OF TABLES

Table

Page

## LIST OF FIGURES

Figure

Page

## SYMBOLS

$m$  mass

$v$  velocity



## ABBREVIATIONS

abbr	abbreviation
bcf	billion cubic feet
BMOC	big man on campus

## NOMENCLATURE

Alanine	2-Aminopropanoic acid
Valine	2-Amino-3-methylbutanoic acid

## GLOSSARY

chick    female, usually young

dude    male, usually young

## ABSTRACT

Shah, Kavit Master, Purdue University, December 2014. Secure data aggregation scheme for sensor networks. Major Professor: Dr. Brian King.

This is the abstract.

## 1. INTRODUCTION

## **2. SECURITY/DATA AGGREGATION BACKGROUND**

### **3. SECURITY/NETWORKING/CRYPTOGRAPHY TOOLS**

## **4. IN-NETWORK DATA-AGGREGATION OVERVIEW**



## 5. BACKGROUND ON SIA

## **6. A PROTOCOL FOR COMMITMENT TREE GENERATION**

## LIST OF REFERENCES

## LIST OF REFERENCES

- [1] B. Krishnamachari, D. Estrin, and S. Wicker, “The impact of data aggregation in wireless sensor networks,” in *Distributed Computing Systems Workshops, 2002. Proceedings. 22nd International Conference on.* IEEE, 2002, pp. 575–578.
- [2] D. Wagner, “Resilient aggregation in sensor networks,” in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks.* ACM, 2004, pp. 78–87.
- [3] H. Chan, A. Perrig, and D. Song, “Secure hierarchical in-network aggregation in sensor networks,” in *Proceedings of the 13th ACM conference on Computer and communications security.* ACM, 2006, pp. 278–287.