

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
1.1 Sensor Networks . . . . .	1
1.2 Internet Of Things . . . . .	1
1.3 Big Data . . . . .	1
1.4 Data Aggregation . . . . .	2
1.5 Cloud Computing . . . . .	2
1.6 Fog Computing . . . . .	2
2 security-in-data-aggregation . . . . .	3
3 security-networking-cryptography-tools . . . . .	4
4 data-aggregation-overview . . . . .	5
5 background . . . . .	6
6 contributions . . . . .	7
7 Summary . . . . .	8
8 Recommendations . . . . .	9
LIST OF REFERENCES . . . . .	10

## 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

Advancements in compute, storage, networks and sensors technologies have led to many new promising applications.

### 1.1 Sensor Networks

The sensor networks of the near future are envisioned to consist of hundreds to thousands of inexpensive wireless sensor nodes, each with some computational power and sensing capability, operating in an unattended mode. They are intended for a broad range of environmental sensing applications from vehicle tracking to habitat monitoring. Give an example and talk about energy, security constraints.

### 1.2 Internet Of Things

In the world of mass connectivity people need to get information all the time on an array of devices. Everything from your refrigerator to your thermostat is connected to wireless networks and joining the “internet of things”. Write about bandwidth constraints.

### 1.3 Big Data

All the large internet companies process massive amounts of data also know as “Big Data” in real time applications. These include batch-oriented jobs such as data mining, building search indices, log collection, log analysis, real time stream processing, web search and advertisement selection on big data. To achieve high scalability, these applications distributes large input data set over many servers. Each server process its share of the data, and generates local intermediate. The set of

intermediate results contained on all the servers is then aggregated to generate the final result. Often the intermediate data is large so it is divided across multiple servers which perform aggregation on a subset of the data to generate the final result. If there are  $N$  servers in the cluster, then using all  $N$  servers to perform the aggregation provides the highest parallelism. Talk about compute constraints. [?]

Airplanes are also a great example of “big data”. In a new Boeing Co.747, almost every part of the plane is connected to the Internet, recording and sometimes sending continuous streams of data about its status. According to General Electric Co. in a single flight one of its jet engines generates half a tera bytes of data. This shows that we have too much of data and we are just getting started.

#### **1.4 Data Aggregation**

Data aggregation is an important technique used in many system architectures. The key idea is to combine the data coming from different sources eliminating the data redundancy, minimizing the number of packet transmissions thus saving energy, bandwidth and memory usage. This technique allows us to focus more on data centric approaches for networking rather than address centric approaches. [1]

#### **1.5 Cloud Computing**

#### **1.6 Fog Computing**

## **2. SECURITY-IN-DATA-AGGREGATION**

Summary of the papers read on the following topic: Sensor networks Internet of things

Data aggregation Power consumption in sensor networks

Brief summary of all the papers read

Practical applications of your protocol

**3.****SECURITY-NETWORKING-CRYPTOGRAPHY-TOOLS**

Hash, Elliptic curve Networking



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

## 5. BACKGROUND

## 6. CONTRIBUTIONS

## 7. SUMMARY

This is the summary chapter.

## 8. RECOMMENDATIONS

Buy low. Sell high.

## 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.