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

LIST OF TABLES

LIST OF FIGURES

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

Cite papers read and also summarize

[1] [2]

3. SECURITY/NETWORKING/CRYPTOGRAPHY TOOLS

Networking - Algorithms of generating tree from a given graph. Optimal tree structure.

Hash

Elliptic curve

4. IN-NETWORK DATA AGGREGATION OVERVIEW

4.1 In-network data aggregation

Sensor networks are being used in scientific data collection, fire alarm systems, traffic monitoring, wildfire tracking, wildlife monitoring and many other applications. In sensor networks, thousands of sensor nodes interact with the physical environment and collectively monitors an area, generating a large amount of data to be transmitted and reason about. The sensor nodes in the network often have limited resources, such as computation power, memory, storage, communication capacity and most significantly, battery power. Also, data communication between nodes consumes a large portion of the total energy consumption. The in-network data aggregation reduces the energy consumption by eliminating redundant data being transmitted to the base station. For example, in-network data aggregation of the *SUM* function can be performed as follows. Each intermediate sensor node in the network forwards a single sensor reading containing the sum of all the sensor readings from all of its descendants, rather than forwarding each descendants sensor reading one at a time to the base station. It is shown that the energy savings achieved by in-network data-aggregation are significant [3]. The in-network data aggregation approach requires the sensor nodes to do more computations. But studies show that data transmission requires more energy than data computation. Hence, in-data aggregation is an efficient and widely used approach for saving bandwidth by doing less communications between sensor nodes and ultimately giving longer battery life to sensor nodes in the network.

We define following terms to help us define the goals of in-network data-aggregation approach.

Definition 4.1.1 ***Payload*** *is the part of the transmitted data which is the fundamental purpose of the transmission, to the exclusion of information sent with it such as metadata solely to facilitate the delivery.*

Definition 4.1.2 ***Information-rate*** *for a given node is the ratio of the* ***payloads****, number of* ***payloads*** *sent divided by the number of* ***payloads*** *received.*

The goal of the aggregation process is to achieve lowest possible ***information rate***. In the following section, we show that reducing ***information rate*** makes the intermediate (aggregator) sensor nodes more powerful. Also, it makes aggregated ***payload*** more fragile and vulnerable to various security attacks.

4.2 Security in In-network data aggregation

In-network data aggregation approach saves bandwidth by transmitting less ***payloads*** between sensor nodes but it gives more power to the intermediate aggregator sensor nodes. For example, a malicious intermediate sensor node who is doing aggregation over all of its descendants ***payloads***, needs to tamper with only one aggregated ***payload*** instead of tampering with all the ***payloads*** received from all of its descendants. It means a malicious intermediate sensor node needs to do less work to skew the final aggregated ***payload***. Also, an adversary controlling few sensor nodes in the network can cause the network to return unpredictable ***payloads***, making an entire sensor network unreliable. Notice that, the more descendants an intermediate sensor node has the more powerful it becomes. Despite the fact that in-network aggregation makes an intermediate sensor nodes more powerful, some aggregation approaches requires strong network topology assumptions or honest behaviors from the sensor nodes. For example, in-network aggregation schemes in [4, 5] assumes that all the sensor nodes in the network are honest. Secure Information Aggregation (SIA) of [6], provides security for the network topology with a single-aggregator model.

Secure hierarchical in-network aggregation (*SHIA*) in sensor networks [7] presents the first and provably secure sensor network data aggregation protocol for general networks and multiple adversaries. We discuss the details of the protocol in the next chapter. *SHIA* limits the adversary's ability to tamper with the aggregation result with the tightest bound possible but it does not help detecting an adversary in the network. Also, we claim that same upper bound can be achieved with compact label format defined in the next chapter.

5. BACKGROUND ON SIA

6. A PROTOCOL FOR COMMITMENT TREE GENERATION

LIST OF REFERENCES

LIST OF REFERENCES

[1] A. Wang, W. B. Heinzelman, A. Sinha, and A. P. Chandrakasan, "Energy-scalable protocols for battery-operated microsensor networks," *Journal of VLSI signal processing systems for signal, image and video technology*, vol. 29, no. 3, pp. 223–237, 2001.

[2] M. Ettus, "System capacity, latency, and power consumption in multihop-routed ss-cdma wireless networks," in *Radio and Wireless Conference, 1998. RAWCON 98. 1998 IEEE.* IEEE, 1998, pp. 55–58.

[3] S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "Tag: A tiny aggregation service for ad-hoc sensor networks," *ACM SIGOPS Operating Systems Review*, vol. 36, no. SI, pp. 131–146, 2002.

[4] Y. Yao and J. Gehrke, "The cougar approach to in-network query processing in sensor networks," *ACM Sigmod Record*, vol. 31, no. 3, pp. 9–18, 2002.

[5] S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "The design of an acquisitional query processor for sensor networks," in *Proceedings of the 2003 ACM SIGMOD international conference on Management of data.* ACM, 2003, pp. 491–502.

[6] B. Przydatek, D. Song, and A. Perrig, "Sia: Secure information aggregation in sensor networks," in *Proceedings of the 1st international conference on Embedded networked sensor systems.* ACM, 2003, pp. 255–265.

[7] 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.