https://doi.org/10.31449/inf.v48i1.5739 Informatica **48** (2024) 141–142 **141**

Enabling Decentralized Privacy Preserving Data Processing in Sensor Networks

Niki Hrovatin
Faculty of Mathematics, Natural Sciences and Information Technologies University of Primorska
E-mail: niki.hrovatin@famnit.upr.si

Thesis summary

Keywords: sensor networks, privacy, onion routing, distributed computing, multy-party computation

Received: February 15, 2024

The paper summarizes the findings of the Doctoral Thesis [1]. We propose a paradigm shift from traditional privacy-preserving joint computation, which relies on data obfuscation methods, to privacy preservation through anonymity. The main contribution of the thesis is a privacy-preserving protocol based on the Onion Routing concept that allows sensor network nodes to jointly compute an arbitrary function and keeps the participating nodes and their inputs private. We demonstrate the protocol's security and, through simulations, its effectiveness in large sensor networks.

Povzetek: Doktorska disertacija predlaga novo metodo ohranjanja zasebnosti preko anonimnosti, s poudarkom na protokolu za ohranjanje zasebnosti, osnovanem na konceptu Onion Routinga, ki omogoča skupno izračunavanje funkcij v omrežjih senzorjev, pri čemer ohranja zasebnost sodelujočih vozlišč in njihovih vhodov.

1 Introduction

In today's technological landscape, Sensor Networks are crucial for capturing geographically spread physical phenomena,serving a broad spectrum of applications from environmental monitoring to industrial automation. Despite their benefits, sensor networks also have several limitations such as susceptibility to faults, limited processing capacity, and vulnerabilities to security and privacy breaches [2].

These limitations are particularly prominent in the traditional centralized sensor network architecture, where nodes collect and transmit raw data to a remote system outside the sensor network for processing and analysis. As a result, there is a shift towards decentralized architectures, driven by the edge computing paradigm, performing data processing in the sensor network as close as possible to the data source [3]. Despite the benefits of edge computing and decentralization, existing distributed computing frameworks for sensor networks lack universality and face issues with security, privacy and efficiency. Specialized for tasks like data aggregation, query processing or machine learning, these frameworks struggle with adaptability.

This paper presents a summary of a Doctoral Thesis [1], introducing a novel communication protocol [4] that enables the joint computation of arbitrary functions on sensor network nodes and keeps the participating nodes and their inputs private.

2 The communication protocol

The communication protocol is based on the Onion Routing technique for anonymous communication over a computer network. We similarly employ messages structured into encryption layers, such that a layer can be decrypted only by the targeted node revealing an inner encryption layer addressed to another node in the network. Therefore, message decryption is carried out gradually by leading the layered message across network nodes following the precise order given at message construction.

Encryption layers are not enclosing only the inner layer, but also additional secret information revealed only to the node decrypting that layer. Path details and encryption keys are in this way conveyed to in-path nodes. Specifically, encryption key pairs, are delivered only to a subset of nodes in the message path. Unlike traditional onion routing, where encryption keys establish an anonymous communication channel, here, the keys grant access to the payload containing edge computing information. Please note that pairs of symmetric encryption keys include distinct keys; however, pairs are chained through layers of the layered object, as can be seen from Fig. 1.

The described protocol ensures privacy by establishing an anonymity set that conceals the nodes accessing the payload among all the nodes in the message path.

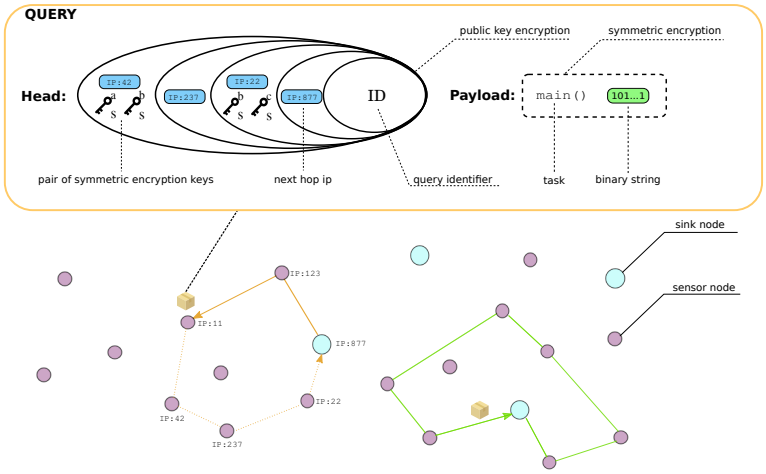

Figure 1: Illustration of messages defined by the privacy-preserving communication protocol.

3 Evaluation methodology and results

We provided privacy preservation analysis and formal proofs showing that the protocol is secure against the external and internal attacker models.

We realized a simulation of the protocol using the ns-3 simulator [1], testing it with networks of up to 400 nodes across two network topologies and testing several protocol parameters. Results show that the protocol is scalable and adequate for application in sensor networks.

The protocol was tested for machine learning training and inference. Results show that models trained using the protocol achieve comparable performance to machine learning models trained using traditional batch learning.

4 Discussion and further work

Our results demonstrate the protocol's effectiveness in preserving privacy, its high adaptability to various data processing tasks and the feasibility of application in large-scale sensor networks. Moving forward, we plan to transition our protocol from theory to practice by implementing it in real-world settings to collect and analyze air quality data directly on-site. Additionally, we plan to extend our protocol's application to the broader Internet of Things, in the form of a permission-less decentralized resource marketplace that incentivizes user participation and leverages blockchain for trust.

References

[1] N. Hrovatin, *Omogočanje decentralizirane obdelave podatkov z varovanjem zasebnosti v senzorskih omrežjih: doktorska disertacija*. PhD thesis, Univerza na Primorskem, Fakulteta za matematiko, naravoslovje in …, 2023.

[2] I. Tomić and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910–1923, 2017. `https://doi.org/10.1109/JIOT.2017.2749883`.

[3] A. Sorniotti, L. Gomez, K. Wrona, and L. Odorico, "Secure and trusted in-network data processing in wireless sensor networks: a survey," *Journal of Information Assurance and Security*, vol. 2, no. 3, pp. 189–199, 2007.

[4] N. Hrovatin, A. Tošić, M. Mrissa, and J. Vičič, "A general purpose data and query privacy preserving protocol for wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, 2023. `https://doi.org/10.1109/tifs.2023.3300524`.

[1] Network simulator ns-3: `https://www.nsnam.org/`