Semantically-driven Secure Task Execution over Wireless Sensor Networks

Niki Hrovatin[1,2][0000−0003−1082−0697], Aleksandar Tošić[1,2][0000−0001−5627−4420], and Michael Mrissa[1,2][0000−0002−2330−1004]

[1] Faculty of Mathematics, Natural Sciences and Information Technologies
University of Primorska,
6000 Koper, Slovenia
[2] InnoRenew CoE, Livade 6, 6310 Izola, Slovenia
niki.hrovatin@famnit.upr.si

Abstract. The growing adoption of low-cost sensors is raising valid concerns with regards to data, user, computation, and network privacy. In this paper we propose a semantically-driven secure task execution on wireless sensor networks. We rely on blockchain smart contracts and onion routed task execution driven by semantic descriptions to respectively provide role-based access control (RBAC) for query, and support local privacy-preserving task execution. We validate the feasibility of our approach in terms of query time, relative to size of the payload, and number of sensor in the network through NS3 simulations.

Keywords: Blockchain · Privacy · Semantic Web · WSN

1 Introduction

Nowadays, Wireless Sensor Networks (WSNs) nodes are powerful enough to support edge computing, thus allowing to execute data processing tasks on site, and to avoid cloud-related drawbacks (high latency, security, privacy. . .) [6]. However, edge computing raises security concerns (outside access to code), and semantic heterogeneity concerns (different nodes provide different functionalities and data) due to lack of explicit semantic description.

In this paper, we combine lightweight semantic reasoning with onion routing to enable semantic-driven decentralized execution of user tasks. Our solution uses semantic annotations to describe sensor capabilities and semantic reasoning to match them to tasks from user queries. We show how nodes contribute to distributed execution of semantically matched obfuscated tasks with onion routing. We remove any single point of failure, and decouple users from direct access to the WSN by using a permissioned blockchain network running a proof of authority consensus. We deploy a set of smart contracts implementing decentralized RBAC, which limits access to publicly exposed functions.

2 Related Work

Firstly, we identify related work on semantic annotation of sensors. The review in [8] references 30 ontologies from 2004 to 2018 to semantically describe sensors or measurements. Most ontologies have a general purpose, so they can be utilized in any application field, and a few of them are specialized to a specific field, such as weather forecast or manufacturing. The most widely adopted proposal nowadays is the W3C Semantic Sensor Network (SSN)[3]. In a similar fashion, the Sensor Web Enablement initiative from the Open Geospatial Consortium [1] provides data models and service interfaces to facilitate access to sensor data. In our work, we rely on the SSN ontology and combine it with well-known ontologies such as QUDT[4] to explicitly describe data concepts and context.

Secondly, our work relates to Onion Routing (OR) [7] as the most used systems for enabling anonymous communication over the Internet. Notable mentions are The Onion Router (TOR network) [5], Invisible Internet Project (I2P) [6], and Lokinet [7].The original technique described in [7] makes use of a particular message named the onion. The onion is used to establish a bi-directional communication channel for data interchange and guarantee anonymity since nodes involved in the onion relaying do not know the entire path of the onion.

The technique of encoding the message path information in the message itself is known as source routing [15], and it was proposed in several privacy-preserving schemes for WSNs. The source routing technique was applied in [2] to route a declarative query privately to one aggregator node of a WSN. The aggregator node is then executing the query sourcing data from its owned region. Moreover, due to the broadcasting nature of the wireless communication that could disclose the aggregator node, the described technique hides the identity of the aggregator node by issuing multiple bogus queries.

Even though OR is computationally demanding, many researchers are proposing its application to WSNs [5, 13]; however, these techniques use OR to establish an anonymous communication channel. In WSNs, this could lead to data origin deanonymization due to the open communication medium. The technique developed in [9] establishes an onion route that leads the message through a circular path and allows only specific nodes in the path to access the message content, thus preserving privacy both from internal and external threats. In this work, we propose an extension with semantic matching to provide distributed task execution and preserve privacy.

Thirdly, our work makes use of blockchain as a means to substitute the need for two or more interacting systems/parties to trust each other or a third party. In recent years, researchers experimented with replacing central trusted parties in many areas such as medical records [3], privacy preservation, telecommunication [11], wireless sensor networks [16]. Of particular relevance in this paper is

[3] https://www.w3.org/TR/vocab-ssn/

[4] http://www.qudt.org/

[5] https://www.torproject.org/

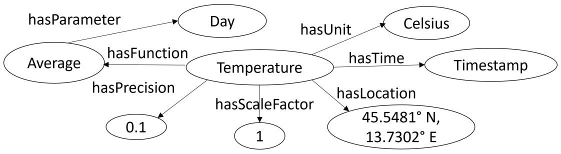
[6] https://geti2p.net/en/

[7] https://lokinet.org/

the application of blockchain for secure, and privacy preserving access control as described in [4] where the authors propose a RBAC system based on Ethereum smart contracts. The solution implements a challenge-response protocol to realize endorsement relationships between users and their roles. A later simplified implementation was provided by OpenZeppelin [8], which we followed in this paper. Commonly, solutions are implemented in permissioned environments such as private Ethereum [12] in order to avoid the cost of smart contract executions in permission-less environments.

3 Contribution

We propose a semantically-driven solution to execute tasks in a decentralized fashion. We rely on semantic matching to compare the data that nodes provide and the data required in a semantically described query. Typically, a data collection task consists in querying data that is relevant to the data mining process. Therefore, for each sensor, there is a need to describe the collected data (concept) and the conditions of its collection (context). Based on the semantic description of each sensor, it is then possible, using reasoning techniques such as subsumption, to align sensor data for the purpose of a query. For example, in a IAQ monitoring scenario, a query might need only the average of temperatures that are related to a window of 1 day before a certain date. The precision of the temperature value should also be accurate enough to participate in the collection. Then, the unit must also match the units of other values that collect similar data, especially in the case where a building is monitored using heterogeneous equipment (which is mostly the case in shared housing). Indeed, the location of the sensor is relevant for data interpretation. Fig. 1 gives a simplified overview (namespaces are not included) of a temperature concept and its context.



```
"concept":"temperature",
"context":{
    "location":45.5481° N, 13.7302° E,
    "timestamp":"May 11 2022",
    "unit":"celsius",
    "scalefactor":"1",
    "precision":"0.1",
    "function":"average",
    "parameters":{
        "unit":"day"
    }
}
```

Fig. 1: Graphical and JSON description of the temperature concept and context

Therefore, we propose to semantically describe the data concepts that each node can provide, together with its context. Being given a task on one side and a node description on the other, we are then able to apply semantic matching techniques to evaluate if the data matches any task from the query.

[8] https://docs.openzeppelin.com/contracts/2.x/access-control

To do so, we need to describe as a list of subtasks that can be executed with some order dependency. A task should be described as a couple `(concept, context)` where context is a set of descriptions about the conditions of the data to be collected. For example, a node could receive the task described in Fig. 1.

Through an onion route, each node on the network can look at the tasks and identify the parts it can realize. Data can be selected according to the semantic matching of the concepts described in the query with the concepts that describe the sensor and its data. Semantic matching offers the opportunity to not exactly match data, but to adapt to semantically equivalent or replaceable terms. In order to enable semantic matching, we rely on the work described in [14] where concepts are matched to describe functionalities of services. Considering that our solution follows the REST architectural style, our interfaces are generic. Therefore, instead of matching functionality, we use the semantic matching technique on data. That means that the concept described in the query must be equivalent to, or subsume, the one of the sensor description.

Concerning context, we match context similarly. Additional SWRL rules and builtin operators for comparison allow to describe more advanced matching[9]. For example, a data value that describes a precision of 0.01 matches a query that expects a precision of 0.1. Similarly, for the location, distance can be calculated so that the data from close sensors might be acceptable to fulfill the query.

3.1 Onion Routing for Secure Task Execution over WSN

The system described in this paper uses the alternative OR technique that was first proposed in [9]. The proposed scheme does not anonymize the sender and receiver, but it uses an onion message to create an anonymity set [10]. The anonymity set consists of nodes that perform an operation and nodes that only route the message. Therefore, the identity of nodes performing the operation remains hidden even to external actors eavesdropping on the wireless broadcasting. In [9], the anonymity set is established by delivering encryption keys in onion layers only to specific nodes in the onion path.

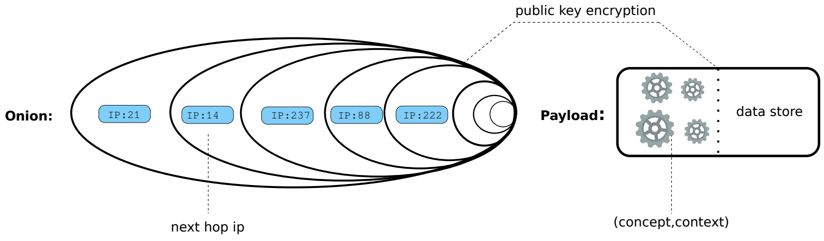


Fig. 2: Graphical representation of a message in the proposed system.

[9] https://www.w3.org/Submission/SWRL/#6.1

[10] https://datatracker.ietf.org/doc/html/draft-hansen-privacy-terminology-02

Here, we propose to establish the anonymity set via semantic matching and use the onion to provide privacy for task execution. Therefore, differently than in [9], each layer of the onion includes only path details. As can be seen from Fig. 2, the onion is accompanied by the payload, which consists of a set of tasks as described in Section 3 and a data store. The payload is protected using public-key cryptography applied on a hop-by-hop basis.

In the following, we resume the operations performed by a node of our system at message receipt. The message payload is deciphered using the node's private key. The node performs semantic matching completing the supported tasks and storing eventual results in the data store of the payload. The onion is deciphered using the node's private key, revealing the next-hop IP address and the inner onion layer. The next-hop IP address is used to determine the encryption key for payload encryption. The payload is encrypted, and the message consisting of the inner onion layer and the payload is forwarded to the node at the next-hop IP.

3.2 Query construction and execution

A set of Ethereum smart contracts were deployed on a private instance of the Ethereum network running a proof of authority PoA consensus mechanism. The solution features three modules, the RBAC module for protecting the query capabilities of the underlying WSN, the registry contract that stores a list of pairs `(public key, address)` of each sensor, and a union of all tasks the underlying WSN is supporting, and the query execution contract responsible executing queries, storing the onion messages and their corresponding results.

In its simplest form, the RBAC contract derives the public key from the calling wallet and maps it to a role. All exposed public functions are secured by the RBAC, which limits access to specific roles. An admin role is responsible for curating the list of users and their role assignments can be modified. The sensor role is given access to insert query results, and the query role is given to users who can query the WSN.

The registry contract exposes the register function limited to the admin role, which is responsible for adding a deployed sensor to the network by supplying the pair `(public key, address)`. The contract simply stores a map of all pairs `(public key, address)`, and the map of template pairs `(concept, context)` supported by the network. Respectively, the execution contract is responsible for storing the user created onion message, and the corresponding result.

To query the WSN, the user performs the following operation as shown in Figure 3: 1) Query the registry contract to obtain the list of pairs `(public key, address)` of all sensors, and available template pairs `(concept, context)`. 2) Shuffle the pairs `(public key, address)`, and select the query tasks. 3) Perform multi layer encryption using the pairs `(public key, address)` to create an onion and binds it with the selected tasks. The last layer of the onion includes the caller's public key for result submission. 4) Call the execution contract by submitting the onion message. 5) Monitor incoming blocks for the result sub-

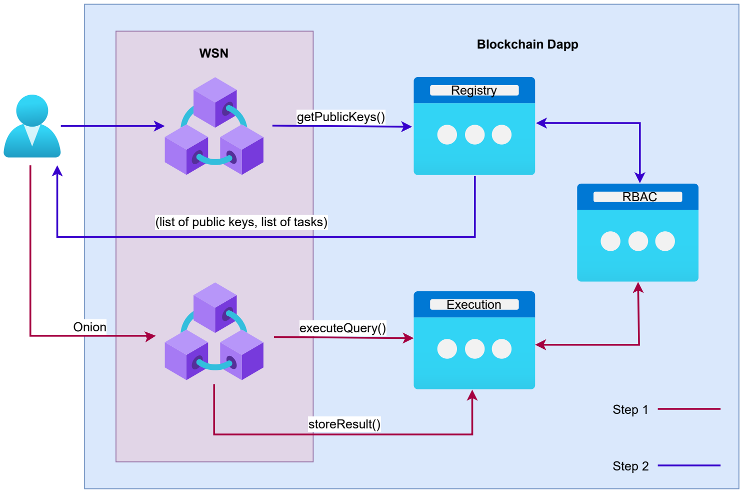


Fig. 3: Workflow diagram of user interactions with the smart contracts

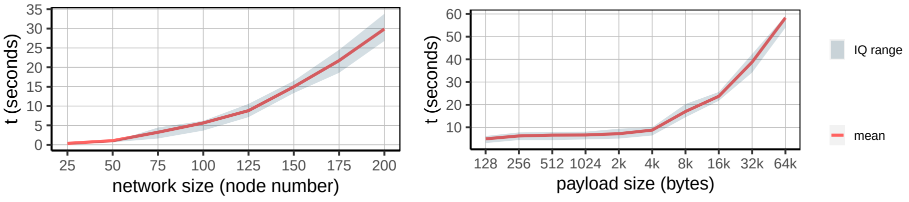
mitted by the last sensor in the path, encrypted with the caller's public key. 6) Decrypt the result using the corresponding private key.

4 Evaluation and Results

To evaluate the presented scheme for distributed task execution, we examine the propagation time of messages at varying onion and payload sizes. Our publicly released simulator [10] relies on the well-known network simulator NS3[11]. We ran two experiments: **a)** Examine the propagation time in networks of different sizes. **b)** Examine the propagation time at different payload sizes. The propagation time is metered starting from the message emanation by the origin node to the message's return to that same node. Each message is constructed to follow a randomized circuit-like path that leads the message through all the network nodes, with the last encryption layer of the onion containing the address of the origin node. Message size is kept fixed through padding.

We setup the simulator described in [9] to simulate the emission of messages in WSNs of various sizes. The WSN is constructed by deploying nodes following a grid structure. The distance between two neighbouring nodes is 60m, the wireless communication is based on the IEEE 802.11n standard at 2.4 GHz and a data rate of 13 Mbps. Messages are transmitted over the TCP protocol, multi-hop routing relies on the Optimized Link State Routing Protocol (OLSR)[12], and cryptography is handled with the Libsodium library[13].

[11] https://www.nsnam.org/
[12] https://www.ietf.org/rfc/rfc3626.txt
[13] https://doc.libsodium.org/



(a) (b)

Fig. 4: Mean and interquartile range of message propagation time for 20 messages. a) payload size set to 0 over different WSN sizes. b) different payload sizes and network size of 100 nodes.

In Fig. 4a we present the propagation time of messages in simulated networks of different sizes. For each network size, 20 onion messages were routed in the network. Each onion message was constructed to be routed through all the nodes in the network. Results confirm that the message propagation time increases faster than linearly at the increase of the network size.

Similarly, in Fig. 4b can be seen, that at payload size larger than $4k$ bytes, the message propagation time is significantly affected. However, it is possible to notice that the propagation time does not double at a fold increase in payload size. Therefore, the increase in payload size has a smaller effect on the message propagation time than increasing the network size.

5 Conclusion

In this work, we presented a scheme for the semantically-driven secure task execution over WSNs. The scheme allows authorized parties to obtain semantic descriptions of services provided by the WSN and construct a layered object for retrieving required results. The scheme employs semantic matching in onion routed messages to establish an anonymity set and avoid disclosing details about services provided by individual sensors to the service consumer or eventual malicious actors.

The scheme was evaluated using the simulation tool presented in [10], results show that applying the proposed technique introduces a substantial latency before obtaining the result. However, the introduced delay was smaller than 35s at a network size of 200 nodes; therefore, we consider such delay acceptable due to the added preservation of privacy.

Acknowledgments

The authors gratefully acknowledge the European Commission for funding the InnoRenew project (Grant Agreement #739574) under the Horizon2020 Widespread-Teaming program, the Republic of Slovenia (Investment funding of the Republic of Slovenia and the European Regional Development Fund) and the Slovenian Research Agency ARRS for funding the project J2-2504.

References

1. Botts, M., Percivall, G., Reed, C., Davidson, J.: Ogc® sensor web enablement: Overview and high level architecture. In: international conference on GeoSensor Networks. pp. 175–190. Springer (2006)
2. Carbunar, B., Yu, Y., Shi, W., Pearce, M., Vasudevan, V.: Query privacy in wireless sensor networks. ACM Transactions on Sensor Networks (TOSN) **6**(2), 1–34 (2010)
3. Chen, Y., Ding, S., Xu, Z., Zheng, H., Yang, S.: Blockchain-based medical records secure storage and medical service framework. Journal of medical systems **43**(1), 1–9 (2019)
4. Cruz, J.P., Kaji, Y., Yanai, N.: Rbac-sc: Role-based access control using smart contract. Ieee Access **6**, 12240–12251 (2018)
5. El Mougy, A., Sameh, S.: Preserving privacy in wireless sensor networks using onion routing. In: 2018 International Symposium on Networks, Computers and Communications (ISNCC). pp. 1–6. IEEE (2018)
6. Garcia Lopez, P., Montresor, A., Epema, D., Datta, A., Higashino, T., Iamnitchi, A., Barcellos, M., Felber, P., Riviere, E.: Edge-centric computing: Vision and challenges (2015)
7. Goldschlag, D.M., Reed, M.G., Syverson, P.F.: Hiding routing information. In: International workshop on information hiding. pp. 137–150. Springer (1996)
8. Honti, G.M., Abonyi, J., Natella, R.: A review of semantic sensor technologies in internet of things architectures. Complex. **2019** (jan 2019). https://doi.org/10.1155/2019/6473160, https://doi.org/10.1155/2019/6473160
9. Hrovatin, N., Tošić, A., Mrissa, M., Vičič, J.: A general purpose data and query privacy preserving protocol for wireless sensor networks. arXiv preprint arXiv:2111.14994 (2021)
10. Hrovatin, N., Tošić, A., Vičič, J.: Ppwsim: Privacy preserving wireless sensor network simulator. SoftwareX **18**, 101067 (2022)
11. Khalaf, O.I., Abdulsahib, G.M., Kasmaei, H.D., Ogudo, K.A.: A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications. International Journal of e-Collaboration (IJeC) **16**(1), 16–32 (2020)
12. Leal, F., Chis, A.E., González-Vélez, H.: Performance evaluation of private ethereum networks. SN Computer Science **1**(5), 1–17 (2020)
13. Palmieri, P.: Preserving context privacy in distributed hash table wireless sensor networks. In: International Conference on Information and Communications Security. pp. 436–444. Springer (2015)
14. Paolucci, M., Kawamura, T., Payne, T.R., Sycara, K.: Semantic matching of web services capabilities. In: Horrocks, I., Hendler, J. (eds.) The Semantic Web — ISWC 2002. pp. 333–347. Springer Berlin Heidelberg, Berlin, Heidelberg (2002)
15. Sunshine, C.A.: Source routing in computer networks. ACM SIGCOMM Computer Communication Review **7**(1), 29–33 (1977)
16. Tošić, A., Hrovatin, N., Vičič, J.: A wsn framework for privacy aware indoor location. Applied Sciences **12**(6), 3204 (2022)