Feedback-enabled anonymous deliveries

Rafał Leszczyna
Gdańsk University of Technology – Faculty of Management and Economics
Gdańsk, Poland *rafleszc@pg.edu.pl*

Abstract

Anonymity of the sender plays important role in modern delivery models such as discreet shipping or drop shipping. At the same time, existing anonymous delivery systems focus on the protection of recipients and employ elements that weaken their security. This paper introduces FEAdelivery – a system that takes advantage of unique delivery identifiers to protect senders' anonymity while retaining the option of each delivery being responded to. The solution was developed through empirical design research with prototyping and conceptual study.

Keywords: anonymous shipping, privacy, Industry 4.0, logistics, supply chain

1. Introduction

Assuring the anonymity of the sending party is indispensable for implementing delivery scenarios that have emerged with the development of e-commerce and Industry 4.0 and may be an enabler for realising new ones. For instance, in discreet shopping customers prefer to receive anonymised parcels where sender data are concealed so as not to reveal the nature of the ordered products. Another example is drop shipping where one of the major concerns is the 'reacting' process. Although the transportation is originally arranged by a retailer, eventually suppliers begin to take over and become competitors. FEAdelivery (*F*eedback-*E*nabled *A*nonymous *delivery*) is a system for providing anonymity during item deliveries that focuses on the anonymity of the sender e.g. a merchant or a supplier in e-commerce. It protects their anonymity without requiring user registration and storing any personal data. The sender's contact data are kept secret from the recipient, but responding to the original sender remains possible.

2. Related work

To assure the comprehensiveness of the analysis of the related work and to avoid any duplication of effort a systematic literature review process was implemented. The analysis comprised three parts: the *papers search*, the *patent search* and the *operational solutions search*. Table 1 demonstrates the findings of the analysis. It becomes evident that all the proposals focus on protecting the personal data of the recipient of a delivery. Scientific studies often embrace the entire ordering, paying and shipping process. They employ a trusted third party or the creation of a shipping route via several delivery points. In the former case, the trusted third party becomes a critical point, where the personal data of the recipient can be linked. In the latter, if the route is managed centrally, the managing central organisation may become a target of attacks.

3. FEAdelivery

FEAdelivery is a system that enables the anonymous shipping of items without registration and collecting personal data of participants. At the same time it allows for responding to the sender based on the unique identifiers of each delivery. No contact data of the sender are present. In this way, the recipient does not know the address of origin but may respond to the correspondence via the system, by providing the unique delivery identifier. The main objectives beyond this research are as follows. *O.1.* The system **should** enable a sender to send a physical item to

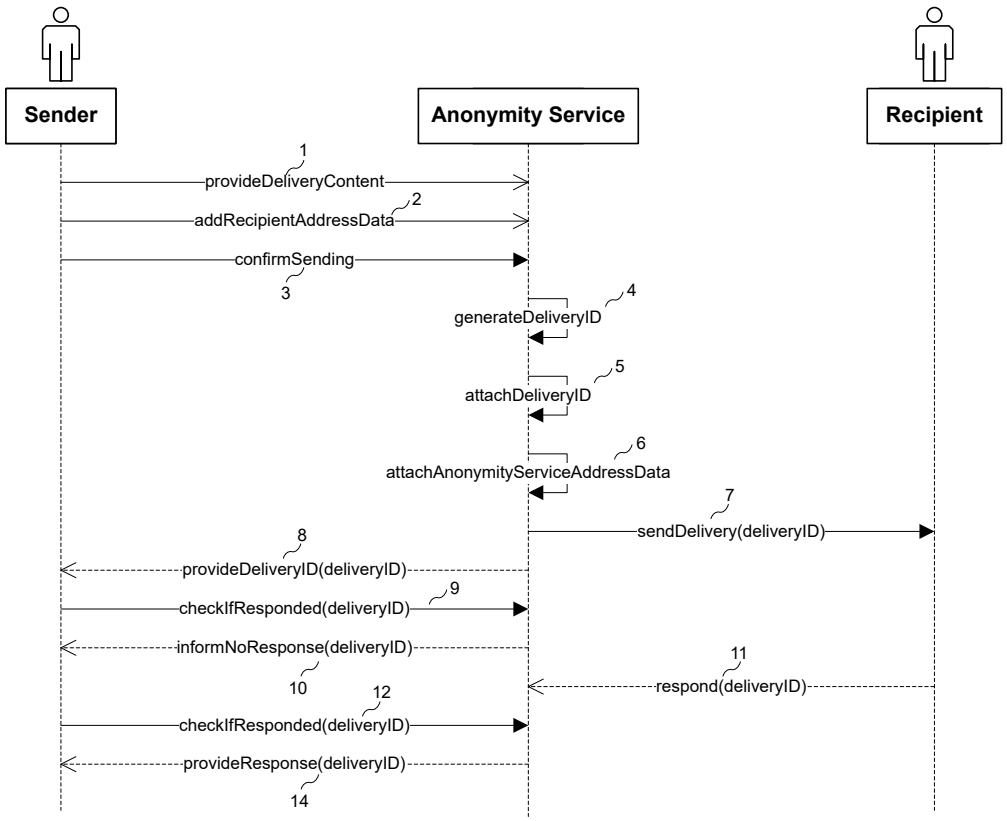

Fig. 1. Sequence diagram of sending an anonymous delivery and responding to it with FEAdelivery

a recipient. *O.2.* The sender's physical address **should** be unreadable to unauthorised parties. *O.3.* The recipient **should** be able to respond to the sender on the receipt of the delivery. *O.4.* Personal data of the sender and the recipient **should not** be stored in the system.*O.5.* The operation of the system **should** be straightforward and intuitive.

3.1. Threat model

FEAdelivery is intended to operate in any type of a delivery network capable of linking involved parties and delivering physical items from one to another. Examples include a postal network, a logistic network for mail or package delivery, or a combination of networks. The model of adversary embraces internal, external, single, k-listening, omnipresent, active, passive and hybrid adversaries as well as well as alliances between attackers. The following assumptions concerning the FEAparcel's operational environment's normal (non compromised) conditions are made. *A1:* Third parties are not informed about the presence of a parcel at a particular node or in a delivery link. *A2:* It is impossible to introduce into the network any entities aiming at observing and following parcels. *A3:* It is impossible to read the data and state of a node from outside. *A4:* All encryption mechanisms are correctly implemented and deployed, resulting in the computationally bound adversary being unable to subvert them.

3.2. FEAdelivery system and protocol

Briefly explained, a user willing to send an anonymous delivery with a possibility of response, prepares the delivery, provides it to the shipping company and notes the identifier generated by FEAdelivery. Then, when checking if the recipient responded to the delivery, she or he introduces the identifier into the system. Depending on the situation, a response is provided or

information that it has not arrived yet. The sequence diagram showing the interactions between the sender, the recipient and the FEAdelivery service involved in the anonymous sending of delivery and responding to it is presented in Figure 1.

4. Security analysis

The security of FEAdelivery is discussed concerning the system's main objectives and specifically O.2. In addition, traffic analysis and reading data content attacks are considered.

Internal adversary An internal adversary i.e. one capable of breaching a node in a delivery network will not be able to learn the physical address of the sender, because it is never provided to the FEAdelivery system and required for the delivery. The attacker will be able to read the delivery ID, but it will not help her or him in revealing the real address of the sender. Thus, the sender's address is *beyond suspicion*.

External, k-present, active and adaptive adversaries Also for an external adversary i.e. one able to compromise a communication link, the sender's physical address is *beyond suspicion*, because of its absence in the FEAdelivery system and the delivery scenario. Further analyses demonstrate that gaining by an attacker additional resources and becoming a K-present (succeeding in attacking k network nodes), adaptive (able to modify delivery processing and data in the network) or active (able to change their targets in any time) adversary does not give them any advantage.

Reading data content attacks Reading data content attacks in the context of parcel delivery refer to the attacks based on reading all information on a package, including the shipping label, as well as accessing the content of the package. By design, FEAdelivery protects the sender's address by not requiring it to be included in a package neither externally nor internally (the address *beyond suspicion*). At the same time, various scenarios can be envisaged where some information that can lead to the disclosure of the sender's address was associated with a parcel intentionally or unintentionally. For instance, the sender's address data might be present on the invoicing documentation included in the package or a package box with some old labelling could be reused. Protection against this type of attack can be achieved with package inspections performed primarily by the senders. This could be associated with appropriate awareness-raising campaigns informing about the danger. Also, the inspections could be performed by shipping companies. However, this would introduce a notable overhead to the parcels' processing.

Traffic analysis By design, FEAdelivery does not include measures to protect against traffic analysis attacks. As a result, it is susceptible to brute force, timing, reply, contextual and many other TA attacks that lead to the sender address becoming *exposed*. TA attacks specific to the physical form of communication include the use of tracking devices such as RFID tags or weight/size-based package tracing [1]. Traffic analysis requires substantial effort and resources from attackers. Performing it, constitutes an exceptional situation usually driven by very strong motivations. FEAdelivery aims at protecting the sender's address in common delivery scenarios when a sender does not wish her or his address can be simply read from a package. However, if protection against TA attacks is required, the FEAdelivery system could be extended with one of the solutions [1, 2, 3] presented in Section 2. It needs to noted that such an extension will introduce a substantial rise in complexity and resource consumption of the system.

5. Conclusions

In contrast to alternative systems that offer anonymity during item shipment, FEAdelivery focuses on protecting the anonymity of the sender. By employing temporarily unique identifiers it allows recipients to reply to each anonymous delivery. With these characteristics, FEAdelivery facilitates or enhances the implementation of modern logistic scenarios. The analysis security of characteristics of the proposal with respect to its main objectives and the threat model shows

the fulfilment of security requirements. In common delivery scenarios, the sender's physical address is made unreadable to unauthorised parties, while the recipient can respond to the sender on the receipt of the delivery. The potential future research directions on FEAdelivery include the development of a pilot system and its experimental evaluation. Based on the prototype, also assessing the user acceptance of the proposal will be possible.

References

[1] Aïmeur, E., Brassard, G., Onana, F.S.M.: Secure anonymous physical delivery (2006)

[2] AlTawy, R., ElSheikh, M., Youssef, A.M., Gong, G.: Lelantos: A blockchain-based anonymous physical delivery system. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST). pp. 15–1509 (2017)

[3] Androulaki, E., Bellovin, S.: Apod: Anonymous physical object delivery. In: Goldberg, I., Atallah, M.J. (eds.) Privacy Enhancing Technologies. pp. 202–215. Springer Berlin Heidelberg, Berlin, Heidelberg (2009)

[4] Chatterjee, K.: System And Method For Anonymous Mail Delivery Services (2008)

[5] Chen, J.L., Fang, B., Ruan, G.Y., You, Y.: Managing privacy of information during shipments (2018)

[6] Engstrom, G.E.: Method and apparatus for masking private mailing address information by manipulating delivery transactions (2007)

[7] Estes, J., Orbke, W.H., Penn, M.C., Pensabene, P.A., Ray, C.R.L., Rios, J.F., Robinson, J.M., Troxel, K.J.: System, method and article of manufacture for shipping a package privately to a customer (2010)

[8] NetServe ReMailing: Remailer.net - anonymous letter and package remailing service from any city/state – we remail letters & packages for you – fast, confidential and anonymous - packages, letters and more. `http://www.remailer.net/` (2025), accessed: April 2025

[9] PriParcel: Receive parcels anonymously – priparcel. `https://www.priparcel.eu/anonymity/` (2025), accessed: April 2025

[10] Private Box: Private box: Nzs #1 virtual po box & street address service. `https://www.privatebox.co.nz/` (2025), accessed: April 2025

[11] Ray, I., Geisterfer, M.: Towards a privacy preserving e-commerce protocol. In: Bauknecht, K., Bichler, M., Pröll, B. (eds.) E-Commerce and Web Technologies. pp. 154–163. Springer Berlin Heidelberg, Berlin, Heidelberg (2004)

[12] Stolfo, S.J., Smith, J.M., Chung, J.D.: Method and system for private shipping to anonymous users of a computer network (2001)

[13] Tsuei, H., Wells, S., Blagg, L.H., Barton, P.R., Barton, L.P.: Anonymous mailing and shipping transactions (2004)

[14] US Global Mail: Mail forwarding & virtual mailbox service. `https://www.usglobalmail.com/` (2025), accessed: April 2025

[15] Zhang, Q., Markantonakis, K., Mayes, K.: A practical fair-exchange e-payment protocol for anonymous purchase and physical delivery. In: IEEE International Conference on Computer Systems and Applications, 2006. pp. 851–858 (2006)

Table 1. Related works summary. Abbreviations: O - ordering, P - payment, S - sorting, D - delivering, TP - the need for trusted parties.

Ref.	Year	Approach	Advantages	Disadvantages	Stages covered	Data obfuscated	Architecture	TP
Scientific literature								
[11]	2004	Trusted Third Party mediation; Symmetric and asymmetric cryptography, nonces, identifiers and expiration times used to secure contents of communications	Entire ordering process covered; Payment data revealed only to bank, shipping address - only to shipping company	Relatively complex cryptographic infrastructure required; No direct protection from TA attacks	O, P, D	Customer's identity, payment data and physical address	Centralised	Yes
[1]	2006	Network of delivery points to be traversed by each delivery; Deposit Units, Mix-delivery Systems with multiple Delivery Agents and Retrieval Units; Networks and routes chosen by customers; Orders collected from pick-up points	High level of protection of customer's identity against TA	Complex infrastructure required including weight-unification, parcel shuffling and delaying; Time-consuming process	D	Customer's identity and physical address	Centrally managed mix-network	No
[3]	2009	Network of Delivery Companies with multiple mail stations to be traversed by each delivery; Delivery Companies and routes chosen by customers; Orders collected from pick-up points, PIN code required	High level of protection of customer's identity against TA	Complex infrastructure required	D	Customer's identity and physical address	Centrally managed mix-network	No
[2]	2017	Route of delivery companies composed dynamically by a customer with the aid of blockchain-based contracts to be traversed by each delivery	High level of protection of customer's identity against TA; Fair-Exchange assured	Complex infrastructure required	O, P, D	Customer's identity, payment data and physical address	Decentralised mix-network	No
[15]	2006	Symmetric and asymmetric cryptographic protocols used to secure payment and delivery data; Orders collected from Delivery Cabinets	Entire ordering process covered; Payment data revealed only to banks; Fair-Exchange assured	Relatively complex cryptographic infrastructure required; No protection from TA attacks	O, P, D	Customer's and merchant's account numbers; customer's physical address	Decentralised network of pick-up points	Yes
Patents								
[7]	2007-2010	Unique customer identifiers used to obfuscate the customer's address before a merchant	Shipping address revealed only to the shipping company	User registration required; No protection from TA attacks	D, P	Customer's identity and physical address	Centralised	Yes
[6]	2001	Substitute delivery addresses of pick-up points used to conceal the physical address of customer	Shipping address revealed only to shipping company	User registration required; No protection from TA attacks	D	Customer's physical address	Distributed	Yes
[5]	2017-2018	Encrypting different parts of customer's contact data	Only necessary contact data revealed to each party	Relatively complex cryptographic infrastructure required; No protection from TA attacks	O (partially), S, D	Customer's physical address, phone number, full name	Centralised	Yes
[12]	2001	Proxy identities and encryption utilised to conceal the customer's identity from merchants and shipping companies	Entire ordering process covered; Only necessary contact data revealed to each party; Customer's identity concealed from all parties	Complex identity management and cryptographic infrastructure required including secured servers and databases; No protection from TA attacks	O, P, D	Customer's identity and physical address	Centralised	Yes
[13]	2004	Aliases applied to secure customer's identity and payment data	Entire ordering process covered; Customer's personal data concealed from merchants	Complex infrastructure required including alias matching databases; No protection from TA attacks	O, P, D	Customer's identity and physical address	Centralised	Yes
[4]	2008	Anonymous identifiers utilised to conceal customer's physical address	Shipping address revealed only to shipping company	User registration required; No protection from TA attacks	D	Customer's physical address	Centralised	Yes
Operational services								
[10], [14]	2025	Alias physical addresses used to conceal customer's physical address; Deliveries forwarded to customer-indicated locations or collected by customers	Customer's physical address concealed from all parties; Additional services of package scanning and conversion into a digital form available; Limitation of unwanted correspondence	Complex infrastructure required; No direct protection from TA attacks	D	Customer's physical address	Centralised	Yes
[8, 9]	2025	Forwarding deliveries to customer-indicated locations	Customer's physical address concealed from all parties	Complex infrastructure required; No direct protection from TA attacks	D	Customer's physical address	Centralised	Yes