Discovering Suppliers' Customers by means of Statistical Disclosure Attacks

Simon D. Rihs
University of Berne

André Miede
University of Applied Sciences Saarbrücken

Abstract

This paper analyses the vulnerability of a Radio Frequency IDentification (RFID) equipped distribution centre (DC) of a supply chain against the Statistical Disclosure Attack (SDA). We built a simulation model to assess the success probabilities of the attack against differently configured distribution centres and attackers. The success probability of an SDA against a DC varies, depending on the organization of the DC, as well as on the number of customers and their structure. The success probability decreases if a supplier delivers multiple products to a customer in a single round, as well as if the fraction of observed deliveries by the attacker falls below a certain threshold.

1. Introduction

While the adaptation of Radio Frequency IDentification (RFID) systems in supply chains has fallen short of projected figures, there are more and more productive implementations of RFID systems.

The widespread adaptation of RFID has lead to a broad body of research regarding security aspects of RFID implementations. These aspects may not only cause problems for the privacy of individuals, but also facilitate industrial espionage.

For instance, RFID eavesdropping could be used to gather information that a company in the defence sector might want to keep secret, such as shipping information. A standard countermeasure against eavesdropping is the encryption of the communication or the data on the tags. But even with encryption there are possibilities to infer important information, using the statistical disclosure attack (SDA).

The SDA is an attack developed to identify the recipients of messages that were sent through an anonymizer such as a mix network. It requires knowledge of the statistical distribution of recipients and allows linking a recipient of a message to its sender retroactively.

The main goals of this paper are: 1) to analyse the intrinsic vulnerability of a DC to an SDA; 2) to explore the prerequisites for mounting the attack; and 3) to outline possible defences.

Our paper expands the existing literature and analyses whether an SDA is possible against a physical DC. Furthermore, we analyse the prerequisite conditions, in order to mount traffic analysis attacks against the DC of a supply chain. Finally, we explore the feasibility of traffic analysis attacks in a supply chain with a centralized DC, simulate success probabilities for the attack against differently organized DCs, and outline possible countermeasures [1,2].

While RFID has gained much attention recently, the underlying technology was already used in 1939, during the Second World War, to identify friendly airplanes [3]. In 1948, Stockman described the technology in his article, 'Communication by means of Reflected Power' [4].

An RFID system always has one or multiple tags, one or multiple readers, and one or multiple backend systems. In logistics operations of supply chains, most systems use passive tags, meaning that the tag does not have its own power source and gets its power from the reader.

A supply chain does not only look at a single supplier or the supply side of an organization, but also takes into account all the material, information and monetary flows of organizations participating in a supply chain [5]. In a supply chain, some functions can be delegated to a single organization, in order for the entire supply chain to benefit from specialization or economies of scale. For instance, a specialized company could handle transportation tasks.

In many cases, there is a distribution infrastructure from which deliveries are grouped and routed to the respective customer. Such a location could be centralized and referred to as DCs. By providing logistic services for one or multiple supply chains, the logistics provider can benefit from economies of scale.

RFID systems can contribute to the success of the members of the supply chain by making the information and material flow in a supply chain more efficient. For a literature review on the possibilities and impact of RFID use in Supply Chain Management; e.g. [6-8].

2. Related work

In this section we will briefly describe the related work regarding traffic analysis, as well as the disclosure of Web service customers.

2.1. Traffic analysis of anonymous communication systems and the statistical disclosure attack

Chaum first described Mix Networks in 1981 [9]. A mix provides unlinkability between the sender and receiver of a message, by using public key cryptography along multiple nodes in a network. Nodes of the mix each receive a batch of messages and strip them of the encryption of the previous node. Next, they reorder the messages randomly, encrypt them and relay them to the next member of the mix network. Thus it is ensured that a message cannot be linked to a sender, either by timing or by content analysis of the message.

A threshold mix is a specific implementation of a mix network that forwards messages in random order, after a certain number of messages (the threshold) have been gathered. This message-batching threshold is important to prevent simple timing attacks [10].

Attacks against anonymity systems can be separated either into attacks against a specific implementation of an anonymous communication system, or into generic disclosure attacks [11]. Owing to the broader applicability, this paper focuses on the latter.

The disclosure attack was designed against a generic random communication model, and is thus not dependent on flaws in specific implementations [12].

To carry out a successful disclosure attack, the attacker has to find mutually disjoint sets (set-packing-problem) in the recipients of the mix. This problem was transformed into solving the NP-complete binary constraints satisfaction problem, and thus requires exponentially more time for increasing numbers of analysed messages [12]. This makes the attack computationally expensive and unfeasible for most practical systems.

Danezis and Diaz developed the SDA, in 2003, as an improvement of the disclosure attack [13]. The following paragraphs give a short outline of the SDA.

While the disclosure attack provides results with certainty, it is computationally very complex, as one needs to solve an NP-complete problem. The SDA, on the other hand, is an approximate method as it only provides results within a chosen confidence interval (depending on the number of observation rounds).

The idea of the SDA is to estimate Alice's[1] contacts in each round when Alice is sending messages. This estimation is carried out by observing all the recipients of messages per round, and assuming that recipients of messages from Alice will appear in a set systematically more often than random messages. The estimates are correlated with all observations from previous rounds, and normalized.

An overview of the notation used in the equations is given in Table 1.

Table 1. Variables used

Variable	Explanation
$\boldsymbol{N}$	Number of participants in the mix
$\boldsymbol{b}$	Batch size (number of users per round)
$\boldsymbol{m}$	Number of Alice's recipients
$\boldsymbol{t}$	Round number
$\vec{\boldsymbol{v}}$	Probability distribution of Alice to choose a recipient. Vector with N elements of potential recipients in the system, where in the uniform distribution case the m recipients of Alice have a value of $\frac{1}{m}$ and others a value of 0, hence $\lvert\vec{v}\rvert = 1$
$\vec{\boldsymbol{u}}$	Uniform distribution over all recipients, where the N recipients have a value of $\frac{1}{N}$, hence $\lvert\vec{u}\rvert = 1$
$\overrightarrow{\boldsymbol{o_t}}$	Observed recipients of all messages in round t
$\overrightarrow{\boldsymbol{r_k}}$	Calculated likely recipient of Alice in round k
$\boldsymbol{l}$	Safety factor for the required time steps

[1]In accordance with computer security tradition, we use the names Alice (sender), Bob (receiver) and Eve (eavesdropper), when discussing specifics of protocols and attacks.

Owing to the law of large numbers, one can assume that the sum of the observed recipients per round is equal to the recipients of Alice plus the other recipients per batch:

$$\bar{O} = \frac{\sum_{i=1\ldots t} \vec{o_i}}{t} = \frac{\vec{v}+(b-1)\vec{u}}{b} \quad (1)$$

which can be solved for Alice's' recipients $\vec{v}$

$$\vec{v} = b\frac{\sum_{i=1\ldots t} \vec{o_i}}{t} - (b-1)\vec{u} \quad (2)$$

Therefore, the attacker only needs knowledge of the batch size b, the observations o_i and the model $\vec{u}$ of other senders to calculate the recipients of Alice $\vec{v}$.

With $\vec{v}$ known, the attacker can infer the communication partners of Alice in round k, by multiplying the vectors $\vec{v}$ and $\overrightarrow{o_k}$ and normalizing the result. As $\overrightarrow{r_k}$ is a probability vector, the normalization uses the L^1 norm.

$$\overrightarrow{r_k} = \frac{\vec{v}\cdot\overrightarrow{o_k}}{|\vec{v}\cdot\overrightarrow{o_k}|} \quad (3)$$

The most likely recipients of Alice at k are the elements with the highest probability in $\overrightarrow{r_k}$.

A necessary condition for executing this attack is a signal-to-noise ratio greater than one. The signal-to-noise requirement is satisfied if the total number of Alice's recipients per round is less than the number of all participants in the system, divided by the number of recipients per batch round minus one.

$$\frac{Alice'sSignal}{NoiseStrength} = \frac{\mu_{Alice}}{\mu_{Noise}} = \frac{\frac{1}{m}t}{\frac{b-1}{N}t} > 1 \Rightarrow m < \frac{N}{b-1} \quad (4)$$

Furthermore, it is important to know how many observations are necessary, in order to give results with adequate confidence.

In the case of a uniform distribution, the mean of Alice's Signal $\mu_{Alice} = \frac{1}{m}t$ has a variance of $\sigma^2_{Alice} = \frac{m-1}{m^2}t$, and thus a standard deviation of $\sigma_{Alice} = \sqrt{\frac{m-1}{m^2}}$. The noise has a mean of $\mu_{Noise} = \frac{1}{N}(b-1)t$, which leads to a variance of $\sigma^2_{Noise} = \frac{N-1}{N^2}(b-1)t$, and thus a standard deviation of $\sigma_{Noise} = \sqrt{\frac{N-1}{N^2}(b-1)}$. (5)

The number of required observations t should be large enough that the mean of the signal is larger than the sum of both standard deviations, multiplied by a safety factor l.

$$\mu_{Alice} - l\sigma_{Alice} > l\sigma_{Noise} \quad (6)$$

This leads to a minimum of required observations of t steps:

$$t > \left[ml\left(\sqrt{\frac{m-1}{m^2}} + \sqrt{\frac{N-1}{N^2}(b-1)}\right)\right]^2 \quad (7)$$

As we assume a uniform distribution, $l = 2$ gives a confidence of 95%, whereas $l = 3$ results in 99% confidence in identifying Alice's recipients. The values in confidence change if one assumes another distribution.

2.2. Disclosure of (Web) service users and the SDA

In [1] the use of SDA is described to infer the users of Web services. In an Internet of Services setting, an attacker monitors communications at the endpoints of communications. The standard SDA was adapted for the Internet of Services setting and evaluated with regard to the success probabilities of the attacker. While a uniform distribution and a low service complexity yielded promising results for the attacker, the success probabilities decreased for (more realistic) Zipfian distributions and more complex service compositions.

A main difference between the model in [1] and this paper is the customer structure and the implementation of the number of services in a service composition. In the Internet of Services settings, the service hub offers service compositions that consist of a number of individual services, each provided by a random supplier. The providers of the services are chosen at random for each service. In this paper, we analyse a physical DC for which a random provider of products is unlikely.

3. Simulation of attacking distribution centres

There are several real-world scenarios where the information gained about deliveries is potentially valuable.

In the military context, the knowledge of to whom ammunition or helicopter spare parts are delivered can lead to conclusions about the defensive capabilities in different locations. This information is typically classified and not obtainable by public sources. Furthermore, even without knowledge about contents, identifying the location where many deliveries are being sent can lead to valuable information about the location; e.g., of a command centre or a warehouse.

In business, gaining knowledge about the deliveries of a competitor to their customers could give a competitive advantage. This knowledge allows the attacker to infer information about sales volumes, and thus permit targeted campaigns.

Another possible scenario is law enforcement. When law enforcement officers investigate a source of counterfeited medication, they could gather information about the suspect's customers during the investigation, to strengthen their case or to facilitate recalls.

Requirements for secure RFID communication protocols in supply chains include access control, authenticity, supply chain visibility and unlinkability. While visibility and unlinkability seem to contradict each other, visibility should only be available to legitimate readers, whereas attacking readers should not be able to link two sightings of the same tag [14].

The underlying assumptions of the analysed DC are as follows.

A DC acts as an anonymizer, providing unlinkability. '*unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not'*. [15, pp. 13]. While providing unlinkability is not the main task of the DC, unlinkability is achieved from an observer's (attacker's) point of view, and is one of the requirements of a secure RFID system.

In the context of the modelled DC, this means that an incoming supply of goods cannot be linked (related) to an outgoing delivery of goods without knowledge (or compromising the security) of the inner workings of the DC. Thus, while comings and goings of deliveries are generally observable, it is not possible to link a supplier to a customer.

One can thus view a DC as a physical correspondent to an anonymity system that provides unlinkability, meaning that the goods sent in are sent out again to another link in the chain. While the flow of the goods is certainly observable, it is not linkable to a source or a target at the central point without compromising the backend. It is important to note that unlinkability only applies to third parties, as participants of the supply chain naturally have to know each other to conduct business.

Anonymity systems that provide unlinkability have been shown to be generally representable as a threshold mix [12]. Hence, the described DC could be modelled as an abstract threshold mix, and thus be vulnerable to an SDA, as the conditions for a successful SDA are a signal-to-noise ratio greater than one and a threshold mix to analyse.

Furthermore, we assume that, owing to security or efficiency concerns, the DC groups deliveries and sends them out in batches. Considering that delivery schedules also account for the load factor of trucks and, amongst others, try to maximize the utilization of trucks, this assumption is sound.

In the simulated scenario, there are multiple ways to access data: one could modify the RFID reader software, or add a rogue RFID reader to transmit the data for analysis. A fully passive attacker that is only eavesdropping on the communications of the legitimate readers is also possible. Owing to the power difference, the eavesdropping distance of the reader-to-tag communication is far greater than the tag-to-reader distance.

We assume that our attacker can eavesdrop electronically on the unloading and loading bays of the DC. While simple visual observation would also be possible, it has a higher detection probability and is more cumbersome and costly.

Eavesdropping takes place by intercepting the wireless communication between reader and tag, or by intercepting other communication (cf. Figure 1). Since a passive attack (no active injection of data of the eavesdropper in the communication) has a lower detection probability we assume a passive attacker.

3.1. Simulation model

The simulation model was implemented in the open source agent-based REPAST (Recursive Porous Agent Simulation Toolkit) modelling environment that supports multiple programming languages [16].

The model used in this paper was developed initially by Miede et al., and implemented in the programing language Java [1]. For the purpose of this research, the model was extended to allow more than one recipient per round. In this case, the attacker's calculation differs from the original SDA, to account for multiple recipients per round. We implemented the multiple recipient case according to [17]. Furthermore, the model was enhanced with additional validity checks, regarding the necessary conditions for a successful attack.

We assume the following process for the model and the simulation. Alice sends a tagged product to a DC. The DC retags the products (or encrypts the tags) and groups the deliveries; e.g. for a truck to be almost full before shipping. This leads to a delay before delivery. The eavesdropper Eve records the

products at the receiving and shipping bay (see Figure 1), and estimates the customers of Alice at round t by making the calculations outlined previously in Section 2.1.

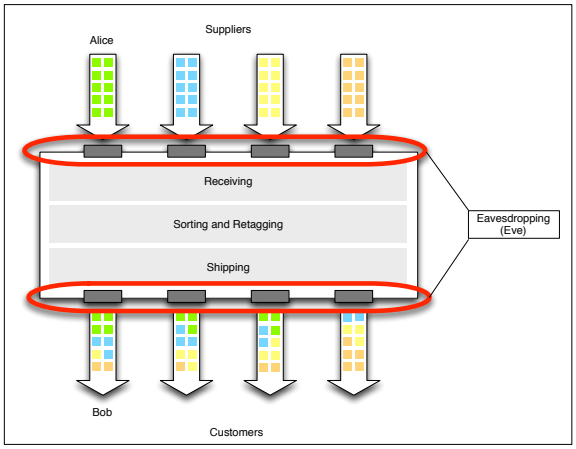

Figure 1. Attack Scenario, cf. [18].

While the described attack could also be possible without RFID, the tags serve as a facilitator to gain the desired information. The information could also be gathered by visual observation. However, the detection probability and the error rate of an visual observation is higher; cf. [19].

3.2. Results and interpretation

100 simulation runs were executed per scenario, to ensure an adequate reliability of the results.

A comparison between the best case for the attacker (worst case for Alice) and the average case reveals only small differences. Furthermore, the attacker cannot know at what point in time the best case exists, and simply stops the observations and calculations at a certain point in time, based on their desired confidence interval. Based on this, the values displayed always represent the average of the final values of each scenario.

The identification of Alice's customers out of all customers of the DC can be expressed as the retrieval of the relevant documents from a complete set of documents. As with any detection, there are true and false positives and negatives.

Identifying the Alice's supplier can be seen as the retrieval of the relevant document from a set of documents. Thus, the metrics used to analyse the success of the attack are derived from information retrieval, their suitability for this kind of attack scenarios was shown in [1] for the first time.

Precision measures the fraction of identified customers that are correctly identified. It is defined as the correctly identified customers (true positives) divided by the total number of identified customers. Therefore, if we only identify true customers of Alice as such, precision is 1 (no false positives). [20]

Recall is defined as the correctly identified customers (true positives) divided by total number of Alice's customers. Therefore, if we identify all of Alice's customers as such, recall is 1 (no false negatives).

As the SDA returns a ranking of the results in a probability vector, the quality of the rankings need to be taken into account as well. The mean average precision (MAP) is defined as the mean of the ranking quality of the true positives in the probability vector over the analysed simulation runs. MAP may decrease even if more true positives are identified, if these are ranked lower. [1]

Table 2. Simulation Variables

Variable	Explanation
N	Number of participants
b	Batch size, threshold after which the delivery is made
C	Total number of customers
aC	Total number of Alice customers
S	Spread of the attacker (percentage of rounds intercepted by Eve)
Ar	Number of customers per round (Alice recipients)

We conducted a sensitivity analysis on all variables of the simulation. Based on the sensitivity analysis and expected parameters in a real-world DC, we chose, N=2000, b=50 C=1000, aC=10 and S=100% as baseline.

As we can see in Figure 2, the impact of the batch size regarding the success of the attack is limited, with the batch size varying between 10 and 250.

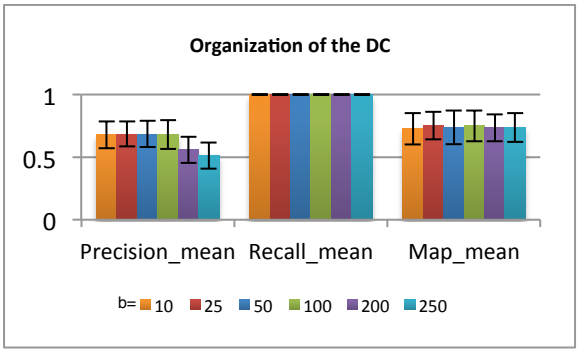

Figure 2. Changing the organization of the DC

While the precision tends to drop with increasing batch size, as long as the basic requirement of a sufficient signal-to-noise ratio is met, the attack is successful.

We observe in Figure 3 that while the precision when increasing the number of Alice's customers (Ar= 5, 10, 20, 20; aC = 10, 10, 100, 1000) per round remains constant or rises, the recall and the MAP drop.

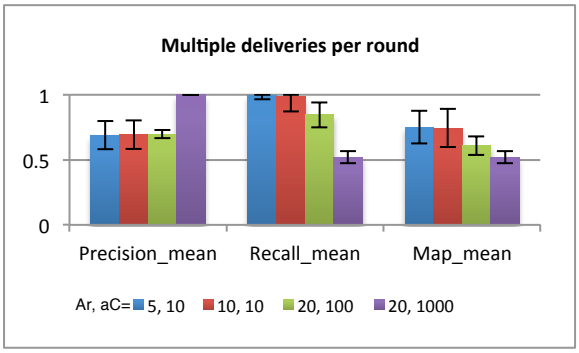

Figure 3. Varying the number of Alice's deliveries per round

A dropping recall means that the attacker identifies a smaller fraction of Alice's customers, whereas the drop in MAP signifies that the ranking of the correctly identified customers is getting worse.

Figure 4 shows a steady rise of precision and MAP with a growing number of customers (N = 100, 1000, 2000, 5000, 10000).

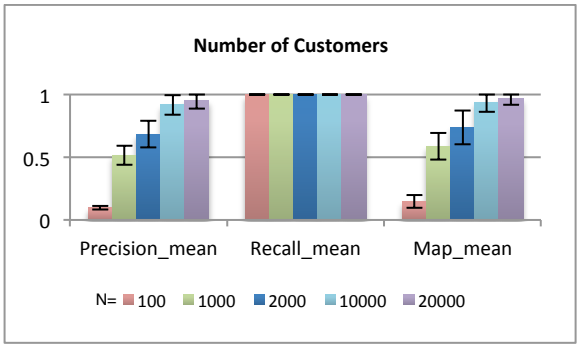

Figure 4. Varying the total number of customers

This is the expected result, as the number of customers is one of the determining factors to successfully conduct the attack. The sharp rise between 100 and 1000 is due to the fact that 100 total customers are not enough to satisfy the constraints of Equation 4.

In Figure 5, we see an obvious collapse of recall, precision and MAP, as soon as an attacker's spread (S= 100 %, 75%, 50%, 25%, 12,5%) drops lower than 25%. The attackers spread indicates the percentages of rounds that could be observed by the attacker.

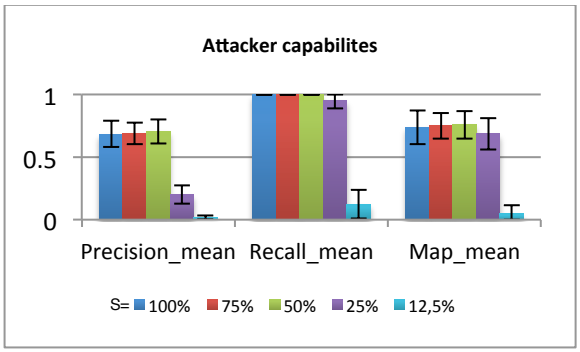

Figure 5. Varying the capabilities of the attacker

This can be explained by the conditions necessary to mount the attack. While the signal-to-noise ratio must remain larger than one, observations are only made for a fraction (with S ≤ 1) of each round, leading to the following result:

$$\left(\frac{\frac{1}{m}t}{\frac{b-1}{N}t}\right) * S > 1 \Rightarrow \frac{m}{S} < \frac{N}{b-1} \text{ with } S \leq 1 \qquad (8)$$

This can be transformed to

$$S > \frac{m}{\frac{N}{b-1}} \quad (9)$$

In the observed case, as soon as the spread is below 24.5% (with m = 10, N = 2000 and b = 50), the necessary conditions for the attack are no longer satisfied. Increasing the number of observations cannot compensate for the fundamental lack of information.

Note that if we assume that an attacker can only observe the rounds partially (S < 100%), for instance due to security measures at the DC, both conditions from equations 4 and 9 need to be met in order for the attack to be carried out successfully.

3.3. Limitations

An SDA against a DC is not necessary unless the RFID tags on the products are exchanged at the DC, or the tags use cryptography with no inherent information leakage. If this were not the case, a direct link between supplier and customer would be easily available by simply logging the information on the RFID tags arriving and leaving the DC. If the tags are neither replaced nor encrypted, an attack is trivial, since the attacker has a direct link between supply and customer, by means of the unique identifier on each item.

The assumption that a DC provides unlinkability is a rather strong one; this attack is only sensible if this holds true. If the DC does not provide unlinkability, the attack is unnecessary. However, if the attacker cannot observe the outgoing traffic, the attack is impossible.

The assumed security of the modelled DC is rather high. In a real-world setting there might be easier ways to gain this information.

We assumed a specific behaviour by Alice and, regarding customer structure a uniform distribution of customers might not be present in a real-world scenario. In future work different customer distributions such as a Zipfian distribution could be analysed.

We only simulated a single attack of the class of disclosure attacks; other attacks might be more successful and need fewer observations.

The simulation parameters, especially the number of participants and their distribution, the batch size, and the attacker spread, have a large influence on the results. A simulation run with parameters from an existing DC would strengthen the paper. However, as this work is exploratory, it provides some information regarding the vulnerability of DCs to disclosure attacks. An existing DC can analyze the relevant parameters in reality to determine if it is vulnerable against an SDA, and implement countermeasures if necessary.

Finally, in DCs with a little traffic and a low turnover, the required observations to reach a conclusion could take prohibitively long, and render the attack inapplicable.

4. Conclusions

We have shown that an SDA can yield the discovery of a link between the supplier and customer of a DC. Changing the batch size of the DC, while the signal-to-noise requirement of Equation (4) remains satisfied, has only a limited impact on the success probability of the SDA. A change in Alice's behaviour to allow for multiple deliveries in a round increases the uncertainty regarding the deliveries, and reduces the success of the attack. Finally, if the attacker can only observe a fraction of the rounds, the SDA may be unfeasible, even with an unlimited number of observations (cf. equations (8, 9)).

The assumptions regarding the DC for the simulation are a DC which groups its shipments and masks the link between sender and receiver of goods. Depending on the parameters of this DC, an SDA is possible (if there are sufficient deliveries and the signal to noise requirements are met), impossible (signal to noise ratio smaller than one) or impractical (e.g. few deliveries resulting in an very long observation period, or there is no eavesdropping possible).

The choice of conducting a simulation study as an approach to gain knowledge about the vulnerability of a DC against an SDA was motivated by the difficulty to gather the relevant data in reality. A simulation represents a reasonable approximation of reality in the key points of the desired analysis.

There are possible countermeasures to reduce the success probabilities of such an attack. One possible countermeasure is to introduce dummy traffic. By sending additional tags or empty boxes to dummy customers, the signal-to-noise ratio can be reduced to the point of making an SDA unfeasible.

Although increasing the batch size to values which violate the signal-to-noise requirement of Equation (4) seems promising on a theoretical level, it might not be possible to do so in a real-world scenario, as the batch size is most likely determined by logistical constraints.

In strengthening the physical security of the DC, opportunities for observations may be reduced, and the observations could fall below the threshold of Equation (9).

The time necessary to obtain the required number of observations depends mainly on the delivery frequency. If there is only one delivery per day, the required time for a successful attack can be measured in months. Nevertheless, in the right circumstances, an SDA is a possibility for an attacker to discover the customers of a supplier in a DC.

5. References

[1] A. Miede, G. Şimşek, S. Schulte, D.F. Abawi, J. Eckert, and R. Steinmetz, "Revealing Business Relationships: Eavesdropping Cross-Organizational Collaboration in the Internet of Services", In *Proceedings of The 10th International Conference Wirtschaftsinformatik*, Zürich, 2011, pp. 1083-1092.

[2] G. Danezis, "Statistical Disclosure Attacks", In *Proceedings of Security and Privacy in the Age of Uncertainty (SEC 2003)*, Springer, 2003, pp. 421-426.

[3] E. Kleefeld, "Efforts to Avoid 'Friendly Fire' Spawned Ancestor of Today's RFID", http://wistechnology.com/article.php?id=2348 (2013-09-09).

[4] H. Stockman, "Communication by Means of Reflected Power", In *Proceedings of the IRE 36 (10)*, 1948, pp. 1196-1204.

[5] Knolmayer, G., P. Mertens, and A. Zeier, *Supply Chain Management Based on SAP Systems*, Springer, Berlin, 2002.

[6] M. Tajima, "Strategic Value of RFID in Supply Chain Management", *Journal of Purchasing and Supply Management*, vol. 13 (4), 2007, pp. 261-273.

[7] A. Sarac, N. Absi, and S. Dauzère-Pérès, "A Literature Review on the Impact of RFID Technologies on Supply Chain Management", *International Journal of Production Economics,* 2010, pp. 77-95.

[8] K. Sari, "Exploring the Impacts of Radio Frequency Identification (RFID) Technology on Supply Chain Performance", *European Journal of Operational Research,* vol. 207 (1), 2010, pp. 174-183.

[9] D.L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM,* vol. 24 (2), 1981, pp. 84-90.

[10] A. Serjantov, R. Dingledine, and P. Syverson, "From a Trickle to a Flood: Active Attacks on Several Mix Types", In *Proceedings of Information Hiding,* Berlin, 2003, pp. 36-52.

[11] D. Kesdogan, D. Agrawal, V. Pham, and D. Rautenbach, "Fundamental Limits on the Anonymity Provided by the Mix Technique", In *Proceedings of IEEE Symposium on Security and Privacy,* Berkeley, 2006, pp. 99-113.

[12] D. Kesdogan, D. Agrawal, and S. Penz, "Limits of Anonymity in Open Environments", In *Proceedings Revised Papers from the 5th International Workshop on Information Hiding (IH 2002),* Berlin, 2002, pp. 53-69.

[13] G. Danezis, and C. Diaz, "A survey of anonymous communication channels", *Technical Report MSR-TR-2008-35,* Microsoft Research, January 2008.

[14] Y. Li, and X. Ding, "Protecting RFID Communications in Supply Chains", In *Proceedings of the 2nd ACM symposium on Information, computer and communications security ACM,* Singapore, 2007, pp. 234-241.

[15] A. Pfitzmann, and M. Hansen, "A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management" https://kantarainitiative.org/confluence/download/attachments/45059055/terminology+for+talking+about+privacy.pdf, (2011-10-17).

[16] "Repast Suite", http://repast.sourceforge.net/, (2013-09-09).

[17] N. Mathewson, and R. Dingledine, "Practical Traffic Analysis: Extending and Resisting Statistical Disclosure", In *Proceeding Privacy Enhancing Technologies,* Berlin, 2005, pp. 17-34.

[18] J.-P. Rodrigue, C. Comtois, and B. Slack, "Cross-Docking Distribution Centre", http://people.hofstra.edu/geotrans/eng/ch5en/conc5en/crossdocking.html, (2013-09-09).

[19] S. Rihs, "RFID Security Risks in Supply Chains: More than Privacy", *International Journal of Enterprise Network Management,* vol. 3 (4), 2009, pp. 347 - 357.

[20] Manning, C. D., P. Raghavan, and H. Schütze, *Introduction to information retrieval* (vol. 1). Cambridge, Cambridge University Press, 2008.

