Robust and Efficient Privacy Preservation in Industrial IoT via correlation completion and tracking

1st Aris S. Lalos
Industrial Systems Institute
Athena Research Center
26504 Platani - Patras, Greece
lalos@isi.gr

2nd Evangelos Vlachos
Institute for Digital Communications,
The University of Edinburgh
Edinburgh EH8 9YL, U.K
E.Vlachos@ed.ac.uk

3rd Kostas Berberidis
Computer Engineering & Informatics Department
University of Patras
26504 Patras, Greece
berberid@ceid.upatras.gr

4th Apostolos Fournaris & 5th Christos Koulamas
Industrial Systems Institute
Athena Research Center
26504 Platani- Patras, Greece
{fournaris,koulamas}@isi.gr

***Abstract*—The Industrial IoT (IIoT) is a key element of Industry 4.0, bringing together modern sensor technology, fog - cloud computing platforms, and artificial intelligence (AI) to create smart, self-optimizing industrial equipment and facilities. Though, the scale and sensitivity degree of information continuously increases, giving rise to serious privacy concerns. In this work we address the problem of efficiently and effectively tracking the structure of multivariate streams recorded in a network of IIoT devices. The time varying correlation data values are used to add noise which maximally preserves privacy, in the sense that it is very hard to be removed. To improve communication efficiency between connected IoT devices, we exploit low rank properties of the correlation matrices, and track the essential correlations from a small subset of correlation values estimated by a subset of network nodes. Extensive simulation studies, validate the correctness, efficiency, and effectiveness of our approach in terms of computational complexity, transmission energy efficiency and privacy preservation.**

I. Introduction

Industrial IoT has been introduced to describe the application of IoT in the industry, namely the utilization of disruptive elements such as sensors, actuators, control systems, machine-to-machine communication interfaces and enhanced security mechanisms to improve industrial systems and shape the futuristic Smart Factory concept [1], [2]. To mitigate privacy risks, several approaches have been proposed to learn from data which are owned by different parties who do not want to disclose their data. Though, these approaches, also known as (partially) homomorphic encryption schemes [3], [4], [5] suffer from limitations linked to their requirement which is the existence of a trusted third party. Moreover, several secure multi-party computation techniques presented in [6] are generally intractable when the number of parties is large and in the presence of transmission errors, while the utility of the published data in different mining applications decreases with increasing level of privacy [7].

Several privacy preserving approaches suggest adding random perturbation, where the noise is distributed along the principal components of the original data in order to achieve maximum privacy, given a fixed utility [8], [9], [10]. These approaches either work offline using stationary data streams [8] or they are capable of tracking correlations between time-evolving data streams, addressing challenges related to storage constraint or time evolving correlations. Despite the benefits offered by the online algorithms in evolving data streams, the communication overhead required for evaluating the principal components analysis (PCA) subspace locally, increases significantly with the number of nodes, which are not resilient over intrinsic (e.g. power depletion of a node, link failures/packet loss) as well as to extrinsic failures (e.g. malicious nodes).

To address the aforementioned limitations, we focus on the challenging problem of distributed reconstruction of the statistical correlation between the data that have been captured by the nodes in an IIoT platform, when several entries of the correlation matrix are missing due to the aforemention intrinsic and extrinsic failures. To that end, we propose a novel adaptive matrix completion approach, where at each step, a rank-one completion problem is solved iteratively. Specifically, the contributions of this work can be summarized as follows:

- We introduce a privacy-preserving method for the reconstruction of the PCA subspace from a subset of correlation values. This method ensures that the correlation matrices cannot reveal the measured data of a node to the others.
- We propose a low-complexity adaptive algorithm for the PCA subspace reconstruction at each node, which considers rank-one updates on the network-wide correlation matrix. For the case of large-scale networks, the proposed algorithm requires only linear complexity over the number of the nodes.

II. Preliminaries

A. Privacy Metrics

Data masking privacy-preserving techniques perturb data elements or attributes directly by additive noise, multiplicative noise or a combination of both. A straightforward approach for data masking is by using additive noise [11], i.e. $\mathbf{M}^* \triangleq$

978-1-7281-2927-3/19/$31.00 ©2019 IEEE

$\mathbf{M}+\mathbf{W}$, where $\mathbf{M}$ is the time-updated data matrix, while the entries of $\mathbf{W}$ are independent and identically distributed (i.i.d.) samples from a zero-mean unit-variance Gaussian distribution. When no correlations between the data are present, then i.i.d. perturbations are sufficient to effectively hide the data. However, real data typically exhibit such correlations. In these cases, it has been proved that this masking technique can be easily circumvented by using spectral filtering techniques. Specifically, we consider the *linear reconstruction* of the perturbed data $\mathbf{M}^*$ expressed as $\tilde{\mathbf{M}} = \mathbf{M}^*\mathbf{F}$, where the matrix $\mathbf{F} \in \mathbb{C}^{K\times K}$ applies a low-pass filter to the perturbed data matrix. To measure the privacy-preserving features of the investigated techniques we introduce related metrics. We use the term *discrepancy* $\mathcal{D}$ between two matrices $\mathbf{A}$ and $\mathbf{B}$ to denote the normalized squared Frobenius norm, i.e.,

$$\mathcal{D}(\mathbf{A},\mathbf{B}) \triangleq \frac{1}{K}\|\mathbf{A}-\mathbf{B}\|_F^2, \text{ where } \mathbf{A},\mathbf{B} \in \mathbb{C}^{K\times K}. \quad (1)$$

So, the privacy of a method can be measured based on the discrepancy between the original and the reconstructed data, i.e., $\mathcal{D}(\mathbf{M},\tilde{\mathbf{M}})$.

B. Data model and communication scheme

Let us consider a network with K sensor nodes where each node k measures $m_k^*(t) \in \mathbb{R}$ at time t. Consider that $m_k^*(t)$ is a discrete-time wide-sense stationary stochastic process with zero-mean. To ensure privacy of streaming data, each measurement is modified by adding noise

$$m_k(t) = m_k^*(t) + n_k(t), \quad (2)$$

where $n_k(t) \in \mathbb{R}$, correspond to zero mean noise samples. All noisy sensor measurements can be expressed into a vector form as $\mathbf{m}(t) = [m_1(t)\dots m_K(t)]^T \in \mathbb{R}^{K\times 1}$. The *correlation matrix* of the process $\mathbf{m}(t)$ is defined as $\mathbf{C} = \mathcal{E}\{\mathbf{M}(t)\} \in \mathbb{R}^{K\times K}$, where $\mathbf{M}(t) = \mathbf{m}(t)\mathbf{m}(t)^T$. Based on the mean ergodic theorem, we estimate the correlation matrix of the process $\mathbf{m}(t)$, as follows:

$$\mathbf{R}(t) = \mathbf{R}(t-1) + \mathbf{M}(t) = \frac{1}{t}\sum_{\tau=1}^{t}\mathbf{M}(\tau). \quad (3)$$

with $\lim_{t\to\infty}\mathbf{R}(t) = \mathbf{C}$. The low-rank property of the correlation matrix is expressed as $rank(\mathbf{C}) \ll K$.

Conventionally, to construct the entire correlation matrix, each node has to receive, at each time instant t, K measurements $\mathbf{m}(t)$ and evaluate $(K-1)^2/2+K$ multiplications. In this work we consider the realistic scenario where each node may have incomplete knowledge of the set of measurements, since many data packets may be lost during network transmissions or due to energy depletion of the nodes. Hence, our aim is that each node will obtain reconstruct the entire correlation matrix $\mathbf{R}(t)$ at each time instance as described in Algorithm 1, from a subset of obfuscated measurements received from other nodes, without having knowledge about the measurements of the entire network.

In the following, we describe the considered scheme for the estimation of the network-wide correlation matrix. This scheme consists of three steps, which are executed at each time instant t. In the first step, each node computes the correlation between its own measurements and the raw obfuscated measurements that could receive from its collaborating nodes. This procedure will fill some of the entries of the k-th row and column of the sought correlation matrix. In the second step, a sparse matrix will have been formed at each node. To obtain the missing entries, matrix completion techniques can be successfully employed, since in each time update the rank of the correlation updating term, $\mathbf{M}(t)$, is small compared to the size of the matrix. The completion steps of the network-wide correlation matrix are summarised in Algorithm 2.

Algorithm 1 Reconstruction scheme for the network-wide correlation matrix

1: **for** $t = 1, 2, \dots$ each node **do**
2: Based on the available obfuscated measurements (of its own and those received by the collaborating nodes), computes the corresponding correlation quantities.
3: Reconstruct the full correlation matrix from the known subset of the estimated correlations.
4: **end for**

Algorithm 2 Completion of Low-rank Correlation Matrix

1: **for** $k = 1, \dots, I_{max}$ **do**
2: $\mathbf{X}_k = \mathcal{D}_\tau(\mathbf{Y}_{k-1})$
3: $\mathbf{Y}_k = \mathbf{Y}_{k-1} + \delta_k\mathcal{P}_\Omega(\mathbf{C}-\mathbf{X}_k)$
4: **end for**

III. Completion of the network-wide correlation matrix

A. Reconstruction of the obfuscated correlation matrix

Matrix completion [12] refers to the procedure of recovering a low-rank matrix from a sampling of its entries, which formally, can be written as

$$\min_{\mathbf{X}} rank(\mathbf{X}) \text{ s. t. } \mathcal{P}_\Omega(\mathbf{X}) = \mathcal{P}_\Omega(\mathbf{C}) \quad (4)$$

where $\mathbf{C} \in \mathbb{R}^{K\times K}$ is the complete matrix, Ω is the set with the matrix indices of the non-zero entries, $\mathbf{X}$ is the optimization matrix variable and $rank(\mathbf{X})$ is the rank of the matrix $\mathbf{X}$. The $\mathcal{P}_\Omega(\mathbf{X})$ denotes the matrix where its (i,j)-th component is equal to $[X]_{ij}$ if $(i,j) \in \Omega$ and zero otherwise. The problem (4) is NP-hard and requires doubly exponential time in the dimension of K to be solved [13].

In [13], it was proposed that the matrix completion problem (4) can be approximately solved by the following convex optimization problem,

$$\min_{\mathbf{X}} \kappa\|\mathbf{X}\|_* + \frac{1}{2}\|\mathbf{X}\|_F^2 \text{ subject to } \mathcal{P}_\Omega(\mathbf{X}) = \mathcal{P}_\Omega(\mathbf{C}) \quad (5)$$

where $\kappa \geq 0$. The solution of the aforementioned problem can be obtainge by a two step iterative procedure that is summarized in Algorithm 1.

Algorithm 3 Completion of the rank-one correlation matrix

1: **for** $k = 1, \ldots, I_{max}$ **do**
2: $\quad \mathbf{u}_k \leftarrow \mathbf{u}_{k-1} + \alpha_k \mathbf{Y}_{k-1}\mathbf{u}_{k-1}$
3: $\quad \mathbf{u}_k \leftarrow \frac{\mathbf{u}_k}{\|\mathbf{u}_k\|}$
4: $\quad \mathbf{X}_k = \lambda_{max}\mathbf{u}_k\mathbf{u}_k^T$
5: $\quad \mathbf{Y}_k = \mathbf{Y}_{k-1} + \delta\mathcal{P}_\Omega(\mathbf{M} - \mathbf{X}_k)$
6: **end for**

B. Completion for rank-1 correlation matrix

To impose the rank-1 constraint, we replace step 1 of Algorithm 1 with the following one,

$$\mathbf{X}_k = \lambda_{max}\mathbf{u}_k\mathbf{u}_k^T \tag{6}$$

where $\mathbf{u}_k$ is the first column of $\mathbf{U}_k$ and $\lambda_{max} = \sigma_1^2$. Subsequently, $\mathbf{Y}_k$ is updated as follows,

$$\mathbf{Y}_k = \mathbf{Y}_{k-1} + \delta\mathcal{P}_\Omega(\mathbf{M} - \mathbf{X}_k) \tag{7}$$

where we have assumed that the parameter δ is independent of the iteration index, i.e. $\delta_k = \delta$. Note that, since $\mathbf{M}$ and $\mathbf{X}_k$ are symmetric matrices, matrix $\mathbf{Y}_k$ will also be symmetric, thus, the SVD operation collapses to eigenvalue decomposition (EVD). Eq. (6) requires only the maximum eigenvalue, hence, we could replace the SVT operator with the solution of the maximum eigenvalue problem, which is expressed as follows,

$$\mathbf{u}_k = arg\max_{\mathbf{u}} \frac{\mathbf{u}^T\mathbf{Y}_{k-1}\mathbf{u}}{\mathbf{u}^T\mathbf{u}}. \tag{8}$$

Therefore, at each iteration, the maximum eigenvector of the updated matrix $\mathbf{Y}_{k-1}$ must be computed. However, this operation has computational cost $\mathcal{O}(K^3)$, which is the same with the SVT algorithm. To overcome this problem, an adaptive technique for updating the maximum eigenvector $\mathbf{u}_k$ of the matrix $\mathbf{Y}_{k-1}$ may be employed. A suitable algorithm for this case is described by the following steps [14],

$$\mathbf{u}_k = \mathbf{u}_{k-1} + \alpha_k\mathbf{Y}_{k-1}\mathbf{u}_k \tag{9a}$$

$$\mathbf{u}_k = \frac{\mathbf{u}_k}{\|\mathbf{u}_k\|} \tag{9b}$$

where α_k is the step-size parameter of the algorithm.

IV. Privacy-preservation with Dynamic Correlation

In the previous section, we showed how we could update the estimation of the principal eigenvector of the constant correlation updating term from a small subset of correlation entries estimated by obfuscated measurements. In this section we focus on generating correlated additive noise that will be distributed along the principal component of the constant correlation matrix. The goal here is to add noise with the same covariance as the spatial correlation of the measurements in the network. All the obfuscated values that are generated in the nodes can be expressed into a vector form as $\mathbf{n}^*(t) = [n_1^*(t) \ldots n_K^*(t)]$. The correlated noise is estimated as $\mathbf{n}(t) = \mathbf{u}_{I_{max}} \circ \mathbf{n}^*(t)$, where $\mathbf{u}_{I_{max}} = [u_{1_{I_{max}}}, \ldots, u_{n_{I_{max}}}]$. Thus each node, after estimating the principal eigenvector of the rank-1 constant correlation matrix, using ALgorithm 3, estimates the noise for generating the obfuscated measurements $n_1(t) = u_{1_{I_{max}}} \times n_1^*(t)$. Then, tracking the principal components of the obfuscated streams $\mathbf{m}(t)$ can give a good estimate of the principal components of the original streams $\mathbf{m}^*(t)$. Formally, $cov(\mathbf{M}(t))cov(\mathbf{M}^*(t))$.

During reconstruction, a PCA based scheme is capable of removing all the noise orthogonal to the local principal components and inserts little additional error, since local PCA can usually track the data accurately. In other words, i.i.d. noise can be successfully removed, provided that the data streams are correlated. However, the perturbation from correlated distortions can-not be removed at all, since the the noise is distributed along the "instantaneous" correlation in the data streams. More specifically, a PCA based reconstruction scheme can be expressed in matrix form as $\hat{\mathbf{m}}^*(t) \approx \mathbf{U}_k(t)\mathbf{U}_k^T(t)\hat{\mathbf{m}}(t)$, where $\mathbf{U}_k(t)$ corresponds to a $K \times K$ matrix with the k principal eigenvectors of the autocorrelation matrix $\mathbf{R}(t)$.

V. Simulation Results

To evaluate the efficiency of the proposed approach in terms of several configuration parameters, in each MC realization, a new scenario of a network is created with K sensor nodes. A number of $L = |\Omega|$ edges are randomly generated, under the constraint that the constructed graph is connected. We assume that the communication links between the sensor nodes are noiseless. In order to verify the convergence of the proposed technique, we have adopted a simplified model for the measurements, where the stochastic vector $\mathbf{m}(t)$ has been generated according to $\mathbf{m}(t) = \mathbf{C}\mathbf{d}(t)$. The matrix $\mathbf{C} \in \mathbb{R}^{K\times K}$ is a fixed, matrix that represents the correlation structure among the sensors. Its entries have been drawn from a uniform distribution, i.e. $[C]_{i,j} \sim \mathcal{U}(0,1)$. The vector $\mathbf{d}(t)$ represents the underlying random process, and its entries are drawn from normal distribution, i.e. $[d(t)]_i \sim \mathcal{N}(0,1)$, for $i \in [1, \ldots, K]$.

Our goal is initially to evaluate privacy preservation of two different streaming scenarios where the obfuscated measurements are generated by adding : i) i.i.d. noise and ii) correlated additive noise. For the (ii) case, we evaluate the effect of both the number of missing entries in the correlation updating term and the executed iterations I_{max} in the privacy preservation. Privacy preservation is evaluated as the ratio between privacy and discrepancy (PD), e.g.,:

$$PD = \frac{||\mathbf{M_s}^* - \hat{\mathbf{M}}_\mathbf{s}||_2^2}{||\mathbf{M_s}^* - \mathbf{M_s}||_2^2}, \hat{\mathbf{M}}_\mathbf{s} = \mathbf{U}_k(t)\mathbf{U}_k^T(t)\mathbf{M_s} \tag{10}$$

where $\mathbf{M}_\mathbf{s}^* = [\mathbf{m}^*(1), \ldots, \mathbf{m}^*(t)], \mathbf{M_s} = [\mathbf{m}(1), \ldots, \mathbf{m}(t)]$ correspond to the matrix with the original and obfuscated measurements respectively, at all nodes and during the t time instances. The step size α_k in (9a) has been set to $\alpha_k = 1/k$. This value satisfies the necessary conditions for convergence, which are described in [14]. On the other hand, the step size δ in (7), has been set to a fixed value equal to one,

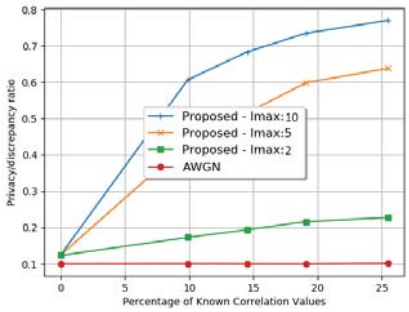

Fig. 1. The number of nodes is $K = 20$. discrepancy is 0.1.

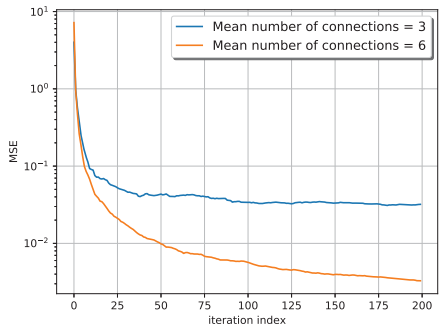

Fig. 2. The number of nodes is $K = 20$ and the discrepancy is 0.1.

i.e., it is independent of the iteration index. Note that, from Theorem 4.2 [13] the convergence for the completion problem is guaranteed provided that $0 < \delta < 2$.

1) Impact of I_{max} Iterations and missing entries in privacy preservation: In Figure 1 we provide the evolution of privacy-vs-discrepancy ratio with respect to the known correlation values that occur in various WSN network setups with $K = 20$ nodes. Each curve corresponds as the average of 100 realizations, executing the same number of I_{max} iterations for completing the missing entries. From the figure, it is obvious that the privacy perservation, is significantly increased with the number of iterations executed during the reconstruction of the rank-1 matrix. ore importantly by inspecting this figure, it is obvious that a small number of iterations (e.g., 5) affects significantly the privacy preservation metric as compared to the conventional AWGN case (e.g., 400% increase assuming 10% of known correlation values.)

2) Obfuscated vs Original Stream Covariance: To evaluate the effect of using the obfuscated measurements for the estimation of the Data correlation matrix, we make use of the normalized-mean-square-error (NMSE), between the time averaged data covariance matrix and the time averaged obfuscated data covariance matrix. Figure 2 presents this NMSE with respect to the time index assuming WSNs with 20 nodes, with different number of mean connections per node. The number of executed iterations is fixed to 20. By inspecting this figure it can be seen that the covariance estimation using obfuscated data is accurate even in sparse networks.

VI. Conclusion

In this paper, we have considered an IoT platform where the raw data measurements are obfuscated with additive and correlated noise to preserve privacy, and are constrained within a minimal subset of sensor nodes. The sample-based correlation matrix has been decomposed into a time-sequence of rank-one matrices. For each matrix, we have formulated a rank-one completion problem that is solved via a novel low-complexity technique. After a number of time instances, the proposed algorithm converges to the full rank correlation matrix which is used to encrypt the data. For a large-scale network, the complexity cost of the proposed privacy preserving algorithm (ideally suited for correlated data streams) can be linear over the number of the sensor nodes.

Acknowledgements

This work is supported by the project "I3T - Innovative Application of Industrial Internet of Things (IIoT) in Smart Environments" (MIS 5002434) implemented under the "Action for the Strategic Development on the Research and Technological Sector", funded by the Operational Programme "Competitiveness, Entrepreneurship and Innovation" (NSRF 2014-2020) and co-financed by Greece and the European Union (European Regional Development Fund).

References

[1] R. Schmidt, M. Möhring, R.-C. Härting, C. Reichstein, P. Neumaier, and P. Jozinović, "Industry 4.0-potentials for creating smart products: empirical research results," in *International Conference on Business Information Systems*. Springer, 2015, pp. 16–27.

[2] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[3] T. Graepel, K. Lauter, and M. Naehrig, "Ml confidential: Machine learning on encrypted data," in *International Conference on Information Security and Cryptology*. Springer, 2012, pp. 1–21.

[4] L. J. Aslett, P. M. Esperança, and C. C. Holmes, "Encrypted statistical machine learning: new privacy preserving methods," *arXiv preprint arXiv:1508.06845*, 2015.

[5] V. Nikolaenko, U. Weinsberg, S. Ioannidis, M. Joye, D. Boneh, and N. Taft, "Privacy-preserving ridge regression on hundreds of millions of records," in *2013 IEEE Symposium on Security and Privacy*. IEEE, 2013, pp. 334–348.

[6] Y. Lindell, "Secure multiparty computation for privacy preserving data mining," in *Encyclopedia of Data Warehousing and Mining*. IGI Global, 2005, pp. 1005–1009.

[7] D. Kifer and J. Gehrke, "Injecting utility into anonymized datasets," in *Proceedings of the 2006 ACM SIGMOD international conference on Management of data*. ACM, 2006, pp. 217–228.

[8] Z. Huang, W. Du, and B. Chen, "Deriving private information from randomized data," in *Proceedings of the 2005 ACM SIGMOD international conference on Management of data*. ACM, 2005, pp. 37–48.

[9] R. Mendes and J. P. Vilela, "Privacy-preserving data mining: methods, metrics, and applications," *IEEE Access*, vol. 5, pp. 10 562–10 582, 2017.

[10] Z. Xiao, X. Fu, and R. S. M. Goh, "Data privacy-preserving automation architecture for industrial data exchange in smart cities," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2780–2791, 2018.

[11] R. Agrawal and R. Srikant, "Privacy-preserving data mining," *SIGMOD Rec.*, vol. 29, no. 2, pp. 439–450, May 2000. [Online]. Available: http://doi.acm.org/10.1145/335191.335438

[12] E. Candès and B. Recht, "Exact matrix completion via convex optimization," *Foundations of Computational Mathematics*, vol. 9, no. 6, pp. 717–772, 2009.

[13] J.-F. Cai, E. J. Candès, and Z. Shen, "A singular value thresholding algorithm for matrix completion," *SIAM Journal on Optimization*, vol. 20, no. 4, pp. 1956–1982, 2010.

[14] E. Oja and J. Karhunen, "On stochastic approximation of the eigenvectors and eigenvalues of the expectation of a random matrix," *Journal of Mathematical Analysis and Applications*, vol. 106, pp. 69–84, 1985.