A survey on Distributed learning System

S Mugesh and G Sharmila

November 28, 2019

A survey on Distributed Learning System

ABSTRACT

S.Mugesh Bala M.E.,
Student,
Department of CSE,
Syed Ammal Engg College,
Ramanathapuram.

G.Sharmila M.E., (Ph.D).,
Assistant Professor,
Department of CSE,
Syed Ammal Engg College,
Ramanathapuram.

Machine learning has been widely used for scientific research and occupational purposes newly to extract valuable information. A most important experiment comes from the communication cost in the distributed computing environment. In specific, composed the iterative nature of many machine learning algorithms and the vastness of the models and the training data require a huge amount of communication amid different machines in the training process. To one side from the actual computational cost that is joint among multiple machines, distributed computing invites additional cost of communication overhead and machine synchronization. The conventional privacy-preserving distributed machine learning approaches emphasis on the simple distributed system architectures, which requires heavy computation loads or can only provide learning systems over the restricted scenarios. The proposed scheme not only reduces the overhead for the learning process but also be responsible for the comprehensive shield for each layer of the hierarchical distributed system.

Keywords : Machine learning, Distribute, Hierarchical

Introduction:

Machine learning has been extensively used for scientific research and occupational purposes recently to extract useful information. Coded Private ML keeps both the data and the model information-theoretically private, while allowing efficient parallelization of training across distributed workers. In Coded Private ML switches this challenge done polynomial approximations of the non-linear sigmoid function in the training phase. Coded Private ML achieves conjunction with comparable rate to conventional logistic regression.[1]. A differentially-private Stochastic Gradient Descent algorithm together with a mechanism to accurately track the privacy loss throughout training were designed, which could train deep neural networks with a modest privacy budget and a manageable model quality.[2] In Distributed Optimization algorithms, communication amid the computing nodes is based on either shared memory, as they can often handle much larger data sets. As many machine learning problems can be formulated as a global variable consensus problem, it opens new chances for these models to be learned more professionally in distributed computing environments.[4] For distributed computing, information conversation between machines is conducted over the communication network, which has limited bandwidth. Indeed, communiqué is one of the scarcest resources in a distributed computing system. Moreover, a machine may fail at any time, and a successively job can be preempted. These properties of distributed systems impose great challenges on developing efficient and reliable machine learning applications using distributed computing. When data parallelism is used, another measure of the performance of the optimization method is the communication cost, which includes the volume of communication required between the machines, and the amount of time that the machines stay idle due to communication latency or for the purpose of system synchronization.[5] Snap ML in both single-node and multi-node environments, quantifying the benefit of the hierarchical scheme and the data streaming functionality, and associating with other widely-used machine learning software frameworks.[6] By computing partial implication results locally and transmitting only gathered data up the hierarchy to the cloud we reduce the overall cost of data movement[7] the distributed networks implementing choices are highly recurrent in nature, which affects the kinds of computation that are performed. Third, these distributed and recurrent networks are prearranged into functional and temporal hierarchies.[8] Distributed computing jobs which need collecting and processing information from all processors. By limiting levels of the hierarchy to two, we will establish the analytically optimal hierarchical configurations for two popular interconnection networks: mesh and hypercube[9]. Homomorphic encryption, a limited amount of interface between the NN owner and the user is introduced, however, in contrast to previous works, the interaction is kept to a minimum, deprived of resorting to multiparty computation protocols[10]

Apart from the actual computational cost that is communal among multiple machines, distributed computing incurs additional cost of communication above and machine synchronization. Compared to repossessing the memory to retrieve information within a single machine,

The conventional privacy-preserving distributed machine learning approaches emphasis on the simple distributed system architectures, which requires heavy computation loads or can only provide learning systems over the restricted scenarios. The proposed scheme not only reduces the overhead for the learning process but also be responsible for the comprehensive shield for each layer of the hierarchical distributed system.

PRELIMINARIES

1. Alternating Direction Method of Multiplier

The alternating direction method of multipliers (ADMM) is a variant of the augmented Lagrangian scheme that uses partial updates for the dual variables. This method is often applied to solve problems such as

Min f(x)+g(x)

This is equivalent to the constrained problem

Minf(x)+g(y), x=y.

Though this change may seem trivial, the problem can now be attacked using methods of constrained optimization (in particular, the augmented Lagrangian method), and the objective function is separable in *x* and *y*. The twofold update requires solving a proximity function in *x* and *y* at the same time; the ADMM technique allows this problem to be solved approximately by first solving for *x* with *y* fixed, and then solving for *y* with *x* fixed. Rather than iterate until convergence (like the jaccobi method), the algorithm proceeds directly to updating the dual variable and then repeating the process. This is not equivalent to the exact minimization, but surprisingly, it can still be shown that this method converges to the right answer (under some assumptions). Because of this approximation, the algorithm is distinct from the pure augmented Lagrangian method.

2. Secure multi party computation protocol

Secure multi party computation (also known as secure computation, multi-party computation (MPC), or privacy-preserving computation) is a subfield of cryptography with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private. Unlike traditional cryptographic tasks, where cryptography assures security and integrity of communication or storage and the adversary is outside the system of participants (an eavesdropper on the sender and receiver), the cryptography in this model protects participants' privacy from each other.

. Basic properties that a multi-party computation protocol aims to ensure are:

- **Input privacy:** No information about the private data held by the parties can be inferred from the messages sent during the execution of the protocol. The only information that can be inferred about the private data is whatever could be inferred from seeing the output of the function alone.
- **Correctness**: Any proper subset of adversarial colluding parties willing to share information or deviate from the instructions during the protocol execution should not be able to force honest parties to output an incorrect result. This correctness goal comes in two flavours: either the honest parties are guaranteed to compute the correct output **.**

3.Homomorphic encryption:

Homomorphic encryption is a form of encryption that allow computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext. Homomorphic encryption can be used for privacy preserving outsourced storage and computation. This allows data to be encrypted and out-sourced to commercial cloud environments for processing, all while encrypted. In highly regulated industries, such as health care, homomorphic encryption can be used to enable new services by removing privacy barriers inhibiting data sharing. For example, predictive analytics in health care can be hard to apply due to medical data privacy concerns, but if the predictive analytics service provider can operate on encrypted data instead, these privacy concerns are diminished.

Conclusion

In the normal applications of distributed learning, we can smooth transform the simple architecture. Based on the analysis of hierarchical architecture, we introduce the privacy-preserving keys to altered data partition scenarios. The specific application clarifications of linear support vector machine are also provided for both upper and lower layers in the system. Additionally, we current a further upgrading in the learning efficiency by implementing the asynchronous learning strategy for different crowds of the system. The hierarchical systems to improve the efficiency, efficacy our approaches.

REFERENCE:

1. CodedPrivateML: A Fast and Privacy-Preserving Framework for Distributed Machine Learning-2019

2. SecureML: A System for Scalable Privacy-Preserving Machine Learning-2017
3. Asynchronous Distributed ADMM for Consensus Optimization-2014
4. Scaling Distributed Machine Learning with System and Algorithm Co-design
5. Celestine Dünner, Thomas Parnell, Dimitrios Sarigiannis, Nikolas Ioannou1 ”Snap ML: A Hierarchical Framework for Machin Learning” 32nd Conference on Neural Information Processing Systems (NeurIPS 2018), Montréal, Canada.Nov-2019
6. Anthony Thomas_, Yunhui Guo_, Arun “Hierarchical and Distributed Machine Learning Inference Beyond the Edge”
7. Laurence T. Hunt1 and Benjamin Y. Hayden” A distributed, hierarchical and recurrent framework for reward-based choice”
8. Dajin wang , Jiannong cao “On hierarchical configuration of distributed systems on mesh and hypercube”
9. Ji P, Jia Z, Wu C and Zhang Y (2008),”DAST: A QoS-Aware Routing Protocol for Wireless Sensor Networks”, in Proceedings for International Conference on Embedded Software System, pp. 259–264.

10. Hesamifard, E., Takabi, H., and Ghasemi, M. “CryptoDL: Deep neural networks over encrypted data”, arXiv:1711.05189, 2017

11. Gasc´on, A., Schoppmann, P., Balle, B., Raykova, M., Doerner,J., Zahur, S., and Evans, D.” Privacy-preserving distributed linear regression on high-dimensional data”, Proceedings on Privacy Enhancing Technologies, 2017(4):345–364, 2017.
12. Shokri, R. and Shmatikov, V, ” Privacy-preserving deep learning”, in Proceedings of the 2015 ACM SIGSAC Conference on Computer and Communications Security, pp. 1310–1321, 2015.