Metamorphic IOTA

Gewu Bu, Wassim Hana, Maria Potop-Butucaru

Metamorphic IOTA

Gewu Bu
Sorbonne University,
CNRS, LIP6
F-75005 Paris, France

Wassim Hana
Sorbonne University,
CNRS, LIP6
F-75005 Paris, France

Maria Potop-Butucaru
Sorbonne University,
CNRS, LIP6
F-75005 Paris, France

***Abstract*—IOTA opened recently a new line of research in distributed ledgers area by targeting algorithms that ensure a high throughput for the transactions generated in IoT systems. Transactions are continuously appended to an acyclic structure called tangle and each new transaction selects as parents two existing transactions (called tips) that it approves. G-IOTA, a very recent improvement of IOTA, targets to protect tips left behind offering hence a good confidence level. However, this improvement had a cost: the use of an additional tip selection mechanism which may be critical in IoT systems since it needs additional energy consumption. In this paper we propose a new metamorphic algorithm for tip selection that offers the best guaranties of both IOTA and G-IOTA. Our contribution is two fold. First, we propose a parameterized algorithm, E-IOTA, for tip selection which targets to reduce the number of random walks executed in previous versions (IOTA and G-IOTA) while maintaining the same security guaranties as IOTA and the same confidence level and fairness with respect to tips selection as G-IOTA. Then we propose a formal analysis of the security guaranties offered by E-IOTA against various attacks mentioned in the original IOTA proposal (e.g. large weight attack, parasite chain attack and splitting attack). Interestingly, to the best of our knowledge this is the first formal analysis of the security guaranties of IOTA and its derivatives.**

***Index Terms*—IoT, Distributed ledgers, Tangle, Energy aware**

I. Introduction

Bitcoin blockchain technology created a new design philosophy for executing and storing transactions in a decentralized and secure fashion [1]. A blockchain is a distributed ledger that mimics the functioning of a classical traditional ledger (i.e. transparency and falsification-proof of documentation) in an untrusted environment where the computation is distributed. The set of participants to the system are not known and it varies during the execution. Moreover, each participant follows his own rules to maximize its welfare. Blockchain systems maintain a continuously-growing list of ordered blocks that include one or more transactions that have been verified by the members of the system, called miners. Blocks are linked using cryptography and the order of blocks in the blockchain is the result of a form of agreement among the system participants. Participants strongly agree only on a prefix of the blockchain, the suffix of the blockchain may be different from one participant to another.

Bitcoin technology and similar proposals (e.g Ethereum) came with several drawbacks that prevent them from being used as standard for IoT industry. In the field of IoT the main attributes that are concerned are the speed, scalability, and energy costs; all of which Bitcoin suffers from as limitations. Hence the introduction of IOTA [2] designed specifically for the IoT industry. IOTA is a DAG (Directed Acyclic Graph) based distributed ledger, also known as the tangle, aimed to overcome limitations of Bitcoin when used in IoT environment while preserving equivalent security levels. IOTA uses tip selection algorithms for new transactions to approve two previous transactions. IOTA suffers from certain limitations in terms of security and fairness with respect to approved transactions. Therefore G-IOTA [3] was proposed as a new tips selection mechanism that combines a confidence fairness aware tips selection algorithm and a mutual supervision mechanism.

In this paper we introduce a new approach, E-IOTA, that aims at maximizing the fairness level in tip selection by approving left behind tips, and improving confidence within the main tangle. E-IOTA randomizes tip selection to reduce computational costs, as well as reduces left behind tips, and increases the security level of the tangle by avoiding a deterministic (predictable) tips selection algorithm (TSA). This makes the TSA and the tangle unpredictable for attackers. The algorithm creates a metamorphic main-chain that is as resistant to splitting attacks as IOTA and G-IOTA while reducing the costs of tip selection and hence preserving the energy of the nodes maintaining the tangle.

The organization of this paper is as follows. Section II introduces IOTA and G-IOTA and identifies their drawbacks. Section III proposes E-IOTA that is designed to overcome the drawbacks of both IOTA and G-IOTA tangles. Section IV focuses on the security analysis of E-IOTA. Section V discusses the process of evaluation and testing of E-IOTA and provides the performance analysis and the comparison between the IOTA, G-IOTA and E-IOTA tangles. Section VI concludes the paper and discusses future research directions.

II. Background on IOTA and G-IOTA

In this section we present the design details of the IOTA system. Furthermore we focus its drawbacks and describe the improvement G-IOTA and its drawbacks respectively.