Privacy Attacks on the IOTA Protocol

Pranav Nerurkar

VJTI Mumbai

September 2020

Outline

Background

- IOTA was proposed as a crypto-currency for the Internet-of-Things (IoT) industry in 2015 [**?** 1, 2].
- IOTA is bases on a Directed Acyclic graph data-structure named "Tangle".
- The main idea of the tangle is the following:
  - to issue a transaction, users must work to approve other un approved transactions (tip) by doing a Proof-of-work (hashcash) [3].
- Therefore, users who issue a transaction are contributing to the network's security.

Background

- IOTA crypto-currency was proposed in 2015 as globally scalable system for payments and transmitting message [4].
- It address the drawbacks of block centric crypto-currencies such as
  - lack of scalability
  - high latency
  - transaction fees
  - dependence on mining nodes for validating transactions.
- Due to these characteristics, it is suitable for broad spectrum of applications if challenges to its beta version "Coordicide" protocol (2020) are resolved [5, 6].

Literature survey

- Masked Authenticated Messaging (MAM) [3]
  - This protocol uses the Tangle network as one normally does, communicating by adding transactions, but with an extra layer of encryption
  - Messages are encrypted before adding the transactions on to the Tangle
  - In this case only the target party (or parties) can decode the encrypted message of the appended transaction

Literature survey

Authors performed experiments on DevNet of IOTA to investigate following questions:

- Is it possible to spam transactions that reference a single transaction without being kicked out of the network [7]
- Is it possible to outpace the cumulative weight of a normal transaction by artificially increasing the cumulative weight of a double-spending transaction? [7]
- Is IOTA centralized? [7]

Authors argue that on basis of experiments performed in 2019:

- IOTA is centralized
- It was also possible to spam the network with transactions quite easily and seemingly without any repercussions.
- In the parasite chain attack experiment it was indeed possible to outpace the cumulative weight of the normal transaction by artificially increasing the cumulative weight of a double-spending transaction using a parasite chain attack

Research gaps

- Attacker may create dummy users to flood network with transactions or approve conflicting transactions or prevent double spending transactions from becoming "orphaned"
- For a user to issue a valid transaction, the user must solve a cryptographic puzzle similar to those in the Bitcoin blockchain
- Assumption of IOTA that no entity can generate an abundance of transactions with "acceptable" weights in a short period of time

Research gaps

- No enforcement of a transaction approval strategy in Tangle. System allows users that want to issue a transaction, to choose two transactions at random and approve them.
  - A "lazy" user could always approve a fixed pair of very old transactions, not contributing to the approval of more recent transactions
  - A malicious entity can artificially inflate the number of tips by issuing many transactions that approve a fixed pair of transactions.
- Attacker can create double-spending transactions and using sufficient computational power the attacker could create a considerable amount of transactions that would directly and indirectly approve the double-spending ones

Research gaps

- To create a simple transaction from A to B, a requirement of 4.77 kBytes are needed
- Tangle storage is resource intensive compared with other Blockchain technologies
- After a period of 30 days, pruning is performed
- Post pruning to access data of old transactions, the only option is to request datacenters called permanodes
- There is no option to check if the requested data was manipulated or the request itself was manipulated

Research gaps

- Tip Selection Algorithm using Monte Carlo Markov Chain (MCMC) random walks in the DAG from old transactions toward new ones, to select two unconfirmed transactions [8].
- The random walk is weighted to favor transactions that are confirmed by more transactions.
- There is no analysis on how the assigned weight, based on the PoW of each transaction, affects the security of the protocol.
- This MCMC TSA is currently used by the IOTA cryptocurrency.

Research gaps

- If the TSA depends only on the PoW, then the weight of the honest transactions should exceed the hashing power of the adversary to prevent a double-spending attack [8].
- This means that honest nodes should constantly use their hashing power and issue new transactions, otherwise an adversary can attack the protocol even with a small fraction of the total hashing power.
- this means for any tip selection algorithm i.e., the protocol cannot be more secure by simply using a more complex TSA.

Aim and Objectives

- To verify the robustness of the Coordicide protocol against privacy attacks.
  - Develop new attacking scenarios that could use artificial intelligence
  - Analyze the cost and feasibility of the proposed attacks
  - Propose new security improvements to the protocol

[1] Serguei Popov, Olivia Saa, and Paulo Finardi. Equilibria in the tangle. *Computers & Industrial Engineering*, 136:160–172, 2019.

[2] Tomáš Janečko and Ivan Zelinka. Impact of security aspects at the iota protocol. In *International Conference on Intelligent Information Technologies for Industry*, pages 41–48. Springer, 2018.

[3] Paulo C Bartolomeu, Emanuel Vieira, and Joaquim Ferreira. Iota feasibility and perspectives for enabling vehicular applications. In *2018 IEEE Globecom Workshops (GC Wkshps)*, pages 1–7. IEEE, 2018.

[4] Daniel Ramos and Gabriel Zanko. Review of iota foundation as a moving force for massive blockchain adoption in different industry sectors.

[5] Serguei Popov and Q Lu. Iota: Feeless and free. *IEEE Blockchain Technical Briefs*, 2019.

[6] Serguei Popov, Hans Moog, Darcy Camargo, Angelo Capossele, Vassil Dimitrov, Alon Gal, Andrew Greve, Bartosz Kusmierz, Sebastian Mueller, Andreas Penzkofer, et al. The coordicide, 2020.

[7] D Cai. A parasite chain attack in iota. B.S. thesis, University of Twente, 2019.

[8] Quentin Bramas. The stability and the security of the tangle. 2018.

[9] Simon Bachmann. Analysis of the tangle in the iot domain.

Thank you

Appendix-1

- Distributed Ledger Technologies (DLT) such as Bitcoin, Ethereum have low transaction throughput
- Only option for increasing transaction throughput in such DLTs is to increase block size
- However, linear increase in block size causes linear increase in data stored in each node of the network
- A result of this is that nodes would exit the network due to limited storage capacity

Appendix-2

- Each node in Tangle calculates statistics of its neighbors
- A non-participative node can be dropped from the network
- This incentivizes all nodes to be participative even if they are not issuing transactions
- All nodes can issue and validate transactions in Tangle [9]

Appendix-3

- To create a new transaction on the network, a node will do three steps as follows [9]:
  - Choose two unconfirmed transactions (tips) using a random walk strategy
  - Check validity of these transactions
  - Perform a PoW to make the new transaction valid

Appendix-4

- Every transaction has five characteristics [9]:
  - weight: amount of work the issuing node has invested in the transaction
  - cumulative weight: weight of transaction (tx) plus all transaction weights that approve tx directly and indirectly
  - height: length of longest oriented path to the genesis transaction
  - depth: length of longest path from self to a tip
  - score: sum of weight of self plus all transactions approved by self directly and indirectly

Appendix-5

- A bundle on Tangle can have four types of transactions [9]:
  - output tx: IOTA tx are sent to another address
  - input tx with positive value: transfer to a new address in senders wallet
  - input tx with negative value: tx completely spends balance in that account
  - meta tx: stores data on tangle using signatureMessageFragment
- Either all transactions in a bundle are accepted or none
- All transactions are tryte encoded where each tryte has one of 27 characters [A-Z and 9]
- Each transaction has 2673 tryte encoded chars which are 1.59kBytes
  - Message field (2187 trytes) [9]: For input and output tx contains the signature. For meta tx it contains data
  - Tag field (27 trytes): used for searching transactions

Appendix-6

- To choose a tip to approve each node performs a random walk from genesis node till it reaches a tip
- Random walk favors transactions with higher cumulative weight
- Bias factors α decides this favoring
- high α leads to higher tips in Tangles