Attacks on the IOTA protocol

Abstract

Modern Internet of Things (IoT) devices consume low energy, and provide low performance. Therefore, optimizing resource consumption is a huge need for large organizations to tackle performance and scalability issues. Existing schemes, therefore, consume more energy, processing, and response time, increase communication load, and use high computational power, which is significantly lost in a real-time scenario while processing enormous authentication requests.

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 datastructure named "Tangle". The main idea of the tangle is the following: to issue a transaction, users must work to approve other transactions by doing a Proof-of-work [3]. Therefore, users who issue a transaction are contributing to the network's security.

Objectives

To make sure that the Coordicide solution is resistant to 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

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
- 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

Planned Contribution

- Verify both the security and usability of the Coordicide scheme by formally defining the attacking model, adversary capabilities, and evaluation criteria.
- Test cordicide protocol against two possible attack scenarios on IOTA viz. parasite chain attack and splitting attack
- Perform quantitative analysis with use of AVISPA and ProVerif simulation.
- Identify vulnerability resistance of IOTA to quantum computations
- Study effect of end-to-end delay on Masked Authenticated Messaging (MAM) in Tangle

References

[1] Serguei Popov. The tangle. *cit. on*, page 131, 2016.

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

[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.