Evaluation of Ginga's CC-Web-Service Module

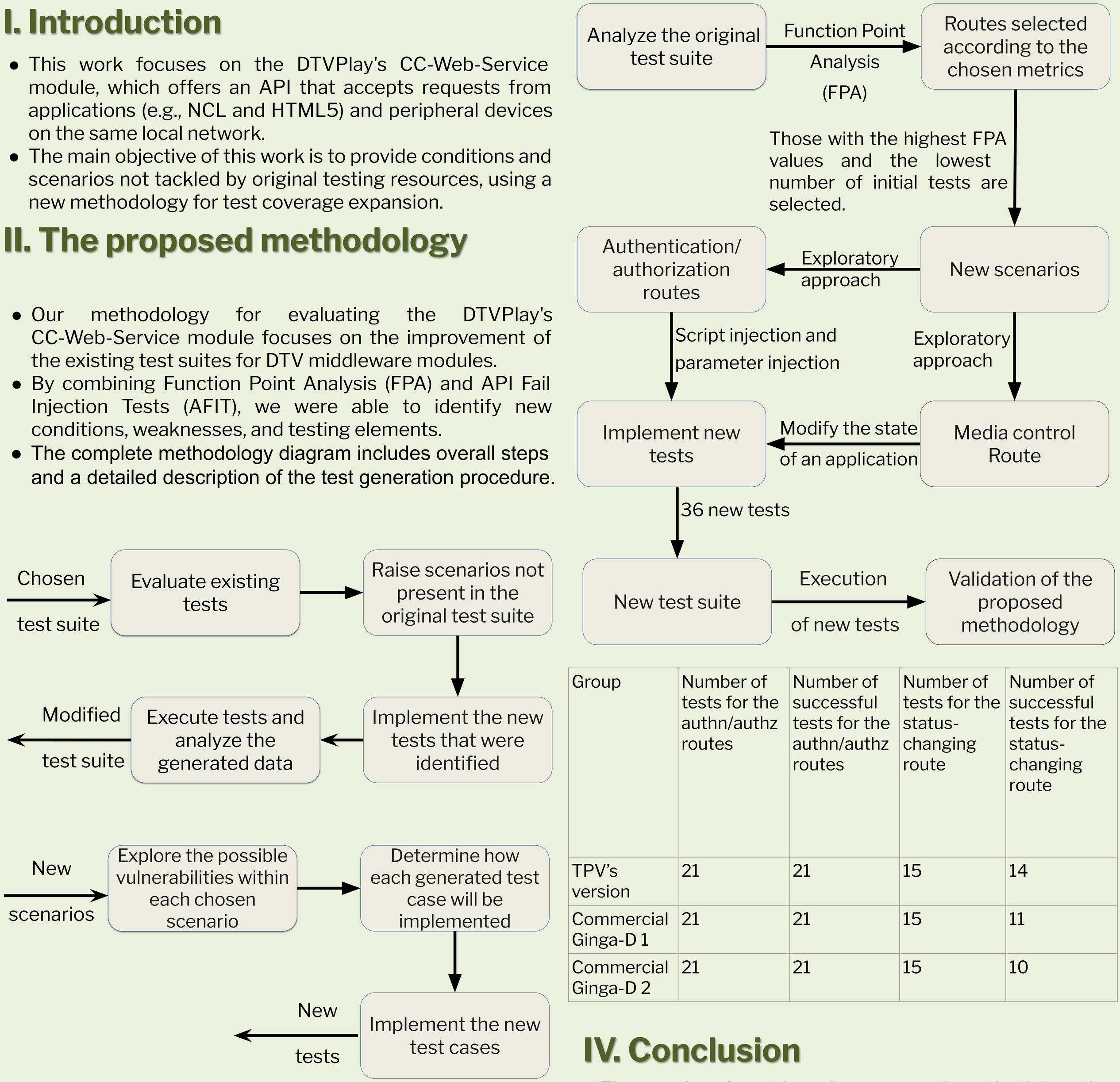
S. Barroso Oliveira[1], A. R. da Silva Conceição[1], E. de Lima Filho[1] and L. Cordeiro[2]
[1]TPV Technology, Manaus, Brazil, [2]University of Manchester, UK
{sergillam.oliveira, andre.conceicao, eddie.filho}@tpv-tech.com
lucas.cordeiro@manchester.ac.uk

I. Introduction

- This work focuses on the DTVPlay's CC-Web-Service module, which offers an API that accepts requests from applications (e.g., NCL and HTML5) and peripheral devices on the same local network.
- The main objective of this work is to provide conditions and scenarios not tackled by original testing resources, using a new methodology for test coverage expansion.

II. The proposed methodology

- Our methodology for evaluating the DTVPlay's CC-Web-Service module focuses on the improvement of the existing test suites for DTV middleware modules.
- By combining Function Point Analysis (FPA) and API Fail Injection Tests (AFIT), we were able to identify new conditions, weaknesses, and testing elements.
- The complete methodology diagram includes overall steps and a detailed description of the test generation procedure.



III. Experiments

- Two groups of the original SBTVD's test suite were tackled:
  - authorization/authentication, which includes routes 8.1.1, 8.1.2, 8.7.1, and 8.7.2;
  - application environment control, which includes route 8.3.10.
- Their descriptions can be found in the associated standard ABNT NBR 15606-11.
- Three commercial versions of Ginga-D executed the modified test suite.

Group	Number of tests for the authn/authz routes	Number of successful tests for the authn/authz routes	Number of tests for the status-changing route	Number of successful tests for the status-changing route
TPV's version	21	21	15	14
Commercial Ginga-D 1	21	21	15	11
Commercial Ginga-D 2	21	21	15	10

IV. Conclusion

- The results show that the proposed methodology is effective and that the chosen middleware versions are robust regarding authorization/authentication.
- However, they may face frozen interface, crash, and reboot events when attacked using routes that change the status of a running application.
- Notice that commercial Ginga-D 1 and commercial Ginga-D 2 are used by many Brazilian DTV-receiver manufacturers, which reveals a great number of defective devices that may suffer successful attacks.

Sponsors:

TPV VISION INNOVATOR

UFAM