The Name of the Title is Hope

TBD and TBD, University of Colorado Boulder

(1) What is the technical problem you are addressing?
    We intend to explore one method of compositional testing of protocols used in the control-plane of cellular communication infrastructure.
(2) Why is addressing the problem important?
    The architecture and design of the cellular-communication-network is fast evolving to handle the needs of IoT and 5G communication. With the increase in scale, comes the need to update the different protocols used to control-coordinate decision making in the control-plane. While the protocols get updated, the implementations of the protocols need to be evaluated for compliance with older versions, for the sake of backward compatibility. Current methodoly of testing doesn't help to address this challenge.
(3) Why is solving this problem hard?
    There has been an interest in the community to adopt formal methods to specify and to ensure correct implementations of protocols within the software and internet-network domain. There hasn't been any prior work that does this within the cellular domain. The current intention is not provide a formal-translation of the natural-lanaguage specification, but rather to provide an on-the-wire specification of the protocol, with little or no emphasis on the internal-mechanisms that are to be satisfied by the different entitites.
(4) What is your expecgted contribution?
    Ourr contribution is to transfer the tools and techniques that's being adopted for internet-protocols, to the domain of control-plane protocols within cellular communications, with a particular focus on the interaface between the Radio part and the Core part of the network.

(1) What is the problem?
    We intend to provide a formal specification of the S1AP protocol that forms the basis of communication between the Evolved Packet Core (EPC) of the cellular communications core network and E-nodeB (base-station) and use this specification to generate automated randomized testers for implementations of S1AP.
(2) Why is the problem important?
    If the implemented code does not exactly follow the protocol, communication using the protocol cannot be correctly performed. However, it is not easy to write the code for the protocol because the protocol definition document is complicated.
(3) Why is the problem hard?
    This is because we need to understand the complex protocol, implement the code according to the developed IVy language for verification, and consider various error cases.
(4) What is your contribution?
    Our automatic testers can quickly find errors in the S1AP implementation process to minimize errors that can occur in the actual communication process.
(5) What follows from your contribution?
    By building a correct LTE network simulation environment with S1AP protocol, we can perform research to improve network performance, such as speed improvement.

Authors' address: TBD, tbd@colorado.edu; TBD, tbd@colorado.edu, University of Colorado Boulder.

1 INTRODUCTION

Introduction - Define the problem and state the contributions. That is, expand the sentences from the abstract into paragraphs covering primarily questions 1-4.

(1) Define the problem you'll solve :
   We intend to extend the applicatiton of Compositional Verification of Internet-protocols to the domain of celluar communication networks, with a specific focus on the interface between the e-NodeB and the Core-Network. Instead of translating the 3GPP protocol specification for the S1-Application Protocol(S1AP) and the Non-Stratum Access(NAS) protocol, we intend to demonstrate the methodology for specifying on-the-wire messages that are exchanged between the entities while interacting over a stateful-protocol. We shall focus on implementing one of the primary procedures facilitated by the EPC, the UE-Attach Procedure. In this procedure, the EPC facilities the connection of a UE(mobile phone/IoT device) to the cellular network, to permit data-transmission over IP.

(2) What is the general approach you intend to use to solve the problem?
   We intend to use the IvY tool for providing a formal-specification of the S1AP/NAS protocol. In addition, we intend to test the MME component(server) of the Core-Network while generating test-messages that shall be sent by the e-NodeB(Client, Radio-link).

(3) Why do you think the approach will sovle the problem?
   This approach has been successfully used to verify a complex stateful internet-protocol, QUIC, which runs as an application-layer protocol, while using UDP to send/transmit messages over the network. This use case is very similar to the domain of cellular-communication networks, where the control-plane protocols are executed as application-layer protocols, executing over an underlying SCTP transport-layerr protocol, which is used to communicate messages on-the-wire.

(4) How do you plan to demonstrate the idea?
   We plan to demonstrate it by encoding the specification of the protocol in the IvY tool, and to adopt its automated-test-message generation process to evaluate some open-source implementations of cellular-core-network (e.g OpenEPC).

(5) How will you evaluate your idea? What will be the measure of success?
   The measure of success would be the following:
   (a) Implementation of SCTP transport protocol within IvY, to facilitate message transmisison between the IvY system and the EPC-implementation(server). The functionality shall be evaluated by the ability to transmit "S1-Setup Request Message" and also to receive "S1-Setup Response" message.
   (b) Specification of subset of S1AP/NAS protocol that enables the "UE-Attach Procedure". This shall be evaluated by a successful simulation of a UE-Attach by an arbitrary UE with the EPC.

2 OVERVIEW

Overview - Showing your contribution through an example (and a bit of why hard).

3 (CONTRIBUTION 1)

4 (CONTRIBUTION 2)

5 EMPIRICAL EVALUATION

6 RELATED WORK

The primary research exercise that we undertake is to determine an good methodology for providing a formal-specification for the control-plane protocols used in the cellular communication infrastrucuture. When we think about task for formalizing a specification for a protocol, there are two main use-cases: (1) to use the specification as an input for verifying that a particular model of its implementation satisfies some desriable properties, and (2) to enable the development of correct by construction implementations of the protocol. In our work, we explore the domain of specification as a means to conduct testing of an implementation, by facilitating a mechanism of automated generation of test-messages that shall be used to test the communication interface between two entities. Most of the related research have focused on the issue of formal-verification of correctness and security properties that are provided by the authentication protocols used in this domain. A formal methodology of testing of a communication protocol has been attempted within this domain. An interesting research project, that aligns with our endeavour, is the Project Everest, which attempts to create a formally verified stack to guarantee verified low-level implementations of the HTTPS stack.

7 CONCLUSION

ACKNOWLEDGMENTS

TBD