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.

ACM Reference Format:
TBD and TBD. 2020. The Name of the Title is Hope. CSCI 5535, Spring 2020 (April 2020), 4 pages.

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.

[Prasanth: Questions to address in introduction:

(1) What is the Cellular Core System? Which part of the system are you handling?
(2) What is S1AP? What is NAS?
(3) How is S1AP/NAS specified?
(4) What is the current process for determining the correctness of the protocol?
(5) What are the current issues?
(6) What do we need?
(7) what do we offer? Why is this more challenging?
(8) what shall you be implementing and demonstrating?
(9) what did you learn from this process?
(10) what are the drawbacks/negatives of this procedure?

]

(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

[Prasanth: We attempt to extend the formal specification based testing methodology introduced in [] to the domain of control-plane application layer protocols. In [], while describing the experience of verifying the QUIC protocol, the authors have reviewed the different approahces to generating adversarial tests for network protocols. Some of the methods can be summarized as follows.

We may observe a taxonomy of classification of the approaches for testing network-protocols as constituting of two main branches, one based on formal specifications and the other not based on formal specification. The latter branch consists of methods like "fuzz testing", in which , and "white-box testing", in which one extracts traces of the internal control flow paths of the target system,that is then used to discover input-values(via SMT solvers or symbolic execution methods) that stimulate code-branches that were previously ignored.

One of the testing frameworks based on formal specification of the protocols, include model-based testing(MBT) and its precedents within the field of protocol-conformance testing. The protocols are specified as finite-state machines(FSMs), which are then explored to generate test-scenarios in an online or offline operational scenario. These methods require procedures to fill in concrete data parameters of messages, which leads to significant complexity in these formalisms.

The compositional testing methodology, introduced in [], does not model the protocol as a FSM. It instead, adopts a constrained-random approach to generating tests based on an assume-guarantee formulation, which is a non finite-state specification. Further, the approach focuses on developing a global representation of the protocol, rather than separate specifications based on the role of an entity within the protocol. In this way, a single specification is used for the generation of tests to verify targets playing different roles within the protocol. By adopting an assume-guarantee based specification for the protocol, as used within the domain of program-analysis, this methodology avoids the constraint of general finite-state machine models to describe only some restricted aspect of the protocol. Though, the assume-guarantee/compositional testing methodology has been used successfully for software and hardware verification, it's application to the network-protocol verification faces new challenges introduced by the presence of data which constitutes the specification state and the messages.

An alternative to using a testing-methodology for examining the correctness of a network protocol, is to construct formally verified reference implementations or to prove properties of an existing implementtaiton. These implementations are assumed to be built to compliance to a reference standard specification. They only way they can be used to guarantee compliance to a common standard, is when they are used as targets within an interoperability testing framework.

Another alternative to examining the correctness of protocols, is to infer protocol specifications from message traces that are recorded on the wire. In the Network Semantics Project, the formal

specification is used as a test-oracle to examine the compliance of observed message traces. In a similar vein, there has been prior work in which software API specifications, restricted to a finite-state abstraction, have been inferred automatically from run-time traces.

The above alternatives to proving correctness of network protocols, stands apart from the larger body of work related to the abstract modeling and analysis of network protocols, in that they are more grounded to practice and examining real-world systems. The latter theoretical approaches are often confined to asserting theoretical properties of the system, which is often separated from any concerns of a workable system in practice.

]

[Prasanth: Questions/TODO:

(1) What are the works related to Testing of Cellular Application Protocols?
(2) What does it mean to check for compliance with a common standard? How is that guaranteed by the compositional testing methodology?

]

[Prasanth: To be reviewed:

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