CSCI 5535 Project Proposal

Prasanth Prahladan and Taeho Kim

1. Define the problem that you will solve as concretely as possible. Provide a scope of expected and potential results. Give a few example programs that exhibit the problem that you are trying to solve.

   - **Define 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-stations). We intend to do so, with an intention of creating an Executable Test-Oracle for evaluating various implementations of EPC.
   - **Provide scope of expected and potential results**: In particular, we intend to formally describe the aspects of the following two protocols:
     - S1AP - protocol between eNodeB and MME
     - NAS - protocol between UE and MME

     Messages based on the above two protocols shall be incorporated into the **[UE-Initial Attach]** procedure within S1AP. We intend to formulate test-cases for evaluating the following in relation to existing EPC implementations:
     - Provide a formal/mathematical specification of S1AP protocol
     - Conformance to S1AP standards specifications for Initial UE Attach procedure
     - Identify errors in Standards that provides a security-risk when considering UE attachment to the MME.
   - **Give a few example programs that exhibit the problem**: Our program generates automated test cases, so we give a few example test cases.
     - E-UTRAN Radio Access Bearer (E-RAB) setup/modify/release verification
     - Initial Context Transfer successful/unsuccessful operation
     - MME Direct Information Transfer test
     - Warning Message Transmission Procedure verification

2. What is the general approach that you intend to use to solve the problem?
   Compositional Testing methodology formulated by Ken McMillan, for the purpose of evaluating Network protocols like QUIC [1]; Distributed Consensus protocols, etc.

3. Why do you think that approach will solve the problem? What resources (papers, book chapters, etc.) do you plan to base your solution on? Is there one in particular that you plan to follow? What about your solution will be similar? What will be different?

   - The QUIC protocol is a transport protocol of significant complexity, which has been evaluated using this methodology and the Ivy Tool [2].
   - The resources we plan to base our solution on:
     - Deductive verification in decidable fragments with Ivy
     - **Compositional testing of internet protocols**

- **Formal specification and testing of QUIC**

(the ones in bold are the ones we intend to follow)

- **Similar aspects of solution**:
  - The methodology of Compositional testing and the tool used for specifying the protocol
  - We believe the protocol shall have shared features with QUIC, which shall facilitate the specification process.
- **Different aspects of solution**:
  - The protocol we shall handle lies in the domain of cellular communication, rather than internet communication protocols.
  - The S1AP protocol verification requires that the UE-Identifier data is generated from a fixed set that is already contained in a database shared between the UE and the MME. This requirement did not exist in the QUIC protocol. It would be a novel contribution to determine how this shared-data may be represented.
  - The S1AP is also strongly related to User Equipments (UE) as well as the relationship between eNB and MME. We need to process the NAS protocol between UE and MME. Meanwhile, the QUIC is considering the transport layer and the application layer.
  - Our solution does not need to consider the relationship between multiple layers.

4. How do you plan to demonstrate your idea?
   Run the executable formal-specification for S1AP using the Ivy tool, to generate test-cases that shall be sent out to evaluate an EPC implementation.

5. How will you evaluate your idea? What will be the measurement for success?
   We shall use the above mentioned test-bench constituting an EPC implementation, and create a bug in one of the steps of the protocol. If the corresponding test-case generated by the Ivy tool fails, we can determine the success of our specification.

References

[1] Kenneth L McMillan and Lenore D Zuck. Formal specification and testing of quic. In *Proceedings of the ACM Special Interest Group on Data Communication*, pages 227–240. 2019. https://dl.acm.org/doi/abs/10.1145/3341302.3342087.

[2] Kenneth L McMillan and Lenore D Zuck. Compositional testing of internet protocols. In *2019 IEEE Cybersecurity Development (SecDev)*, pages 161–174. IEEE, 2019. https://ieeexplore.ieee.org/abstract/document/8901577.