Name: Md Mazharul Islam

Hard Problem Area:
Developing open interface and engine for a decision-making controller, *ActiveSDN*, that enables implementing Network Functions Virtualizations (NFVs) for adaptive cyber defense and cyber agility capabilities rapidly and safely on Software Defined Networks.

Overall Research Goal(s):
We are working to create a new dimension in the foundation of cyber agility and active cyber defense. The main thrust of our research can be described as following:

- *ActiveSDN*, Active Cyber Defense using Software-defined networking (SDN).
- Stealthy DDoS Attack mitigation, e.g. Crossfire and Link Flooding Attack mitigation.
- Moving Target Defense.
- CLIPS Policy Builder.

Broad Impact:
Internet was built as an open system without security in mind. Hence the assets, services, in general the infrastructure of ‘Internet’ remain vulnerable and susceptible to many stealthy attacks.

Cyber defense techniques are mostly non-adaptive and takes long time to respond (hours, months and days). Moreover, the defense techniques are rigid and does not provide agility capability to mitigate threat proactively. Existing cyber defense policies (such as firewalls and IDS) requires too specific description of the attacks signature and lack of the ability to investigate and hypothesize.

Developing agility on cyber defense is highly complex tasks and it requires significant effort in management and orchestration.

Our research hypothesis is to build a framework, *ActiveSDN*, that can:

- Actively respond to defend any kind of cyber-attack both reactively and proactively within seconds.
- Using Solvers e.g. constraints satisfaction solvers known as brain in ActiveSDN to resolve computationally hard problem.
- Using verification module to verify user defined Policy specification so that no misconfiguration can take place using the framework.
- ActiveSDN is capable of mitigating different class of stealthy DDoS attacks through investigation and configuration actions.
- ActiveSDN can defend against reconnaissance attack with effectiveness approximately 70%. That means 70% of the data collected by the attacker in the reconnaissance phase will be wrong.
Specific Research Goals:
We've implemented several NFVs using Software-defined networking (SDN) for Moving Target Defense, different class of stealthy DDoS attacks, e.g. IP Mutation (Random Host Mutation), Path Mutation (Random Route Mutation), Redirect, Reroute, Secure Tunneling, Path Migration etc. To evaluate the performance of these NFVs, we use OpenFlow protocol (for Open vSwitch) in OpenDaylight controller.

We developed a CLIPS based policy language (CPL), which will be used to build security policies (SP) to defend many well-known cyber-attacks as well as to provide network facilities for active cyber defense. CPL is designed and written in a very fine grain manner so that user can easily fit any policy into it.

The infrastructure of our framework is as following:

1. We use Mininet virtual network at the bottom of our framework.
2. The OpenDaylight controller communicates with this virtual network using Openflow protocol.
3. In the controller, we implement our defined ActiveSDN NFVs.
4. We provide a well-defined user friendly API.

For future work:
1. We will provide a CLIPS environment which mainly comprise with:
   a. CLIPS policy interface,
   b. CLIPS verifier,
   c. A CLIPS translator.
2. User can provide any policy to the CLIPS environment by:
   a. Manually,
   b. From third party,
   c. Build their own using our GUI included with the framework.
3. The given policy will be verified and then translated into a proper semantic using the CLIPS environment so that it can be used by the ActiveSDN API.
4. Through the API, the policy will be deployed into the virtual network to test and evaluate the feasibility of the policy.
5. We will also extend our research by including Adaptive Computing, Game Theory and Solvers (e.g., constraints satisfaction solvers) in CPL and ActiveSDN Controller.

Proposed Data Collection (if applicable):
Currently we are using Mininet, a virtual network creator for SDN, to build different topologies and test our framework instead of using any physical network. So, no active data collections are applicable at this phase of our research.

Success Criteria:
We are continuing our research as planned. As a result, we have already done the following:
- Successfully implemented ActiveSDN.
- Implemented several NFVs, e.g. IP Mutation, Path Mutation, Redirect, Reroute, Secure Tunneling, Path Migrate etc.
- Provided API for ActiveSDN.
- Created different policy examples, e.g., stealthy DDoS mitigation, Active Continuous Monitoring using CLIPS policy language and through ActiveSDN API, deployed them into different virtual network topologies to test the feasibility of the policies.

**Anticipated Difficulties, Limitations, and Criticisms:**
Developing an adaptive cyber defense environment considering fine tuning of the agility action parameters in order to achieve measurable effectiveness and provide a high-level user friendly interfaces is challenging.

The most challenging part is to integrate a policy verifier and solver into the framework. Even if a rock-solid software can malfunction because of misconfiguration, so that we are planning to provide a verifier which will find and fix if any misconfiguration occurs using our framework. The solver will be used to find solution for computationally hard problem.

Another challenge is the continuous adaptiveness of the framework.

To overcome these challenges, we will use divide and conquer methodology. We have already build our ActiveSDN controller. Now we will implement a verifier separately and test as many as possible cases for that verifier. Then we will integrate the verifier into our framework. We will use Satisfiability Modulo Theories (SMT) for the solver and Adaptive Computing including Game Theory to achieve the adaptiveness of our framework.