


text here
deployed on each link in the spanning tree, which makes the cost unacceptable.

Figure 1c shows a deployment that cuts the budget. Using the single firewall, the network operator has to manually set up forwarding tables for every switches, to ensure traffic is directed to the firewall. This is a complex and error-prone task especially when the network becomes large.

Full SDN enhances security by using the controller to analyze the traffic. Figure 1d shows an OpenFlow network example. When an OpenFlow switch receives packets from end hosts, it sends a PacketIn message to the controller to forward the packet to the controller. The controller then analyzes the packet with its SNFs to decide whether or not to drop it. However, similar to the FW deployment in Figure 1b, full SDN upgrade is cost-prohibitive [2]. Moreover, forwarding packets to the controller degrades the performance.

3 SYSTEM DESIGN
As shown in Figure 2, Clé comprises three main components: the Device Upgrader, the Unified Controller, and the Clé Dataplane. The key idea behind Clé’s Unified Controller and Dataplane are automatically "attracting" traffic from LSes to PSSes without manual inferences, and PSS can inspect traffic decide the action.

- **Device Upgrader** is responsible for identifying the "Critical" Legacy Switches (CLSes), and the total number of CLSes is the minimum. And once upgrading CLSes to PSSes, we can achieve full SDN security enhancement. Identifying the CLSes is a placement problem that studies how to place SDN switches on the legacy network. The objective of the problem is to minimize the overall upgrade cost, which is minimizing the number of PSSes. The constraint for the problem is that each flow’s path should have a PSS, where a flow is a (source host, destination host) pair.

  - **Unified Controller** attracts traffic to PSSes. It i) gathers address information from the ARP (Address Resolve Protocol) message and ii) uses the information to calculate the routes to each flow. iii) By using the calculated routing information, the controller broadcasts "decoy" ARP messages in the network and tells LSes the PSS knows where to send packets to the destination host. iv) Also, the unified controller generates flow tables to instruct PSSes forwarding packets. v) Upon receiving traffic, PSSes parse packets and detect possible threats with SNFs.

  - **Clé Dataplane** can be categorized into two parts. One is PSSes, and another is LSes. Clé does not modify anything on LSes. PSSes leverage the benefit of programmability and combine the basic forwarding functionality with SNFs. We use P4 [1] switches as our PSS and use the P4 language to implement the SNFs. Our PSSes also support security service function chaining that chains multiple SNFs together. We implement simple rule-based FW and IDS on PSSes. Stricter security enhancement may require deep packet processing logic. To this end, we forward the packet to the unified controller with the PacktIn message to make further detection.

4 CONCLUSION AND FUTURE WORK
We propose a PD enabled hybrid SDN based network security enhancement solution called Clé. It achieves the minimum cost by smartly selecting CLSes to upgrade and realizes full SDN-like security enhancement and simple network management without introducing the performance penalty by using the proposed unified controller along with the SNFs combined PD. Clé is now under development, we present Clé to inspire readers to leverage the benefit of partial SDN deployment and programmable dataplane.

ACKNOWLEDGEMENT
The work was supported by the National Natural Science Foundation of China under Grant No. U1536112 and the China Scholarship Council under Grant No. 201806470060, and in part by US NSF under Grants CNS-1411636, CNS-1618339, CNS-1617729, CNS-1814322, and CNS-1836772.

REFERENCES