Privacy-Preserving Validation of Reachability

Cross Multiple Software Defined Networks for Smart Grids

Ang Li, Rakesh Kumar, David M. Nicol

Objectives

- Validating the network reachability for a given path across multiple Software Defined Networks (SDN) for smart grids
- Preserve the privacy of network configuration information belongs to different domains

Motivation

- SDN has been widely deployed in smart grid, which offers flexibility of configuration and fine-grained control for security
- For reliable operation of the smart grid, it is necessary to integrate data from separate domains without privacy leakage
- Network reachability is crucial for monitoring network behavior and detecting the violation of security policies
- Collecting reachability information across multiple domains is very challenging due to the privacy and security concerns

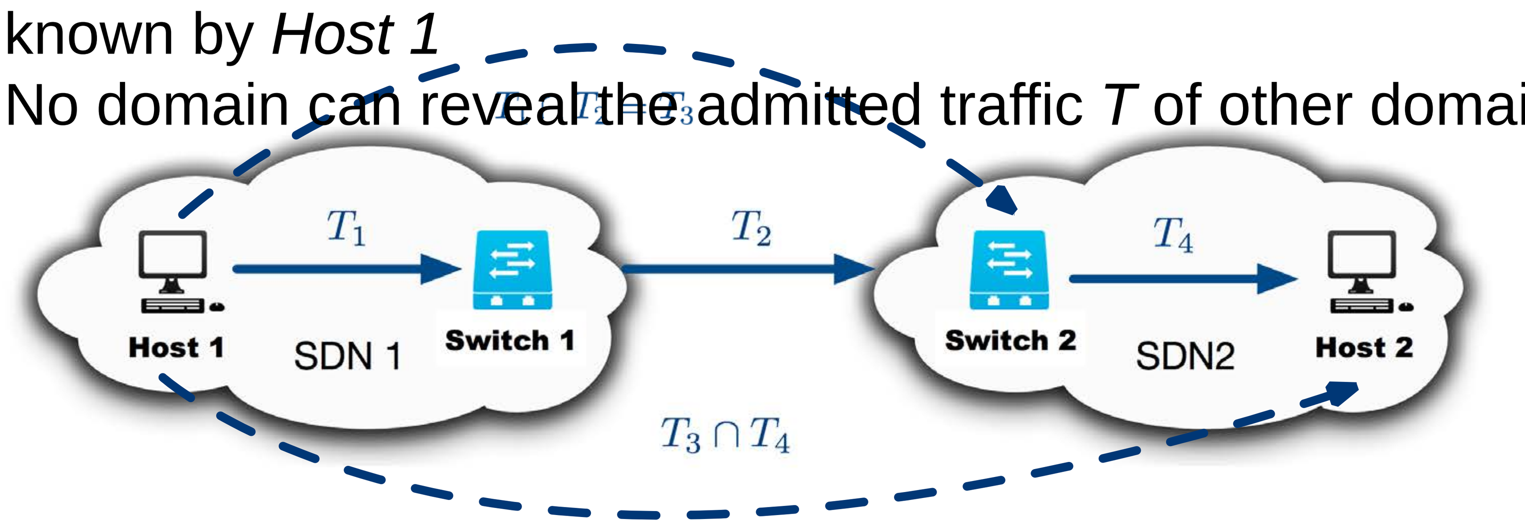
Problem Statement

Assumption

- For each domain, the reachability information is converted to *admitted traffic set* [1], representing the traffic carried from source to the destination node. For example, T_1 represents the admitted traffic from *Host 1* to *Switch 1*
- Let *M(T)* denote the set of packets that constitute admitted traffic *T*
- Inside admitted traffic set is private for each domain, such as T_1 and T_4. But the intermediate admitted traffic is available for each domain, such as T_2
- Each packet $p \in M(T)$ consists of *n* fields F_1, ..., F_n, such as *source IP*, *destination IP*, etc.

Privacy-Preserving Protocol

- Enables *Host 1* to validate the reachability to *Host 2* by computing $M(T_3) \cap M(T_4)$, since $M(T_1) \cap M(T_2) = M(T_3)$ is known by *Host 1*
- No domain can reveal the admitted traffic *T* of other domains



Threat Model

Semi-Honest Model

- Each domain must follow our protocol step by step
  - ➢ Input its admitted traffic *T* and *M(T)* correctly
  - ➢ Follow the process of our protocol
- Each domain may try to learn *M(T)* of other domains
  - ➢ Analyze the intermediate information during running the validation process

Prefix Membership Verification

P_1: [4, 7] → Prefix format → S([4,7])={100, **1****} → Prefix numericalization → N(S([4,7]))={1001, **1100**}

P_2: 5 → Prefix family → T(5)={101, 10*, **1****,***} → Prefix numericalization → N(T(5))={1011,1010, **1100**,1000}

If N(S([4,7]))∩N(T(5)) ≠ ∅, then 5∈[4, 7]

Range Intersection

- Suppose the domain of this field is [0, 15]

P1: [4, 7] → Generate ranges → [0, 3] , [4, 7], [8, 15] → Prefix format and numericalize → N(S([0,3])), N(S([4,7]), N(S([8, 15]))

P2: [2, 5] → Retrieve boundaries → 2, 5 → Prefix family and numericalize → N(T(2)), N(T(5))

Because (1) N(S([0,3]))∩N(T(2)) ≠ ∅, then 2∈[0, 3]
(2) N(S([4,7]))∩N(T(5)) ≠ ∅, then 5∈[4, 7]

From 2∈[0, 3] and 5∈[4, 7], we have
[4, 7] ∩ [2, 5] = [4, 5]

Privacy-Preserving Range Intersection

Commutative encryption [2, 3]

- For a number *x*, $((x)_{k1})_{k2} = ((x)_{k2})_{k1}$
- Let $(x)_{k12}$ denote $((x)_{k1})_{k2}$, namely $(x)_{k12} = (x)_{k21}$

P_1 (K_1): [4, 7] → N(S([0,3])) , N(S([4,7]), N(S([8, 15])) → (1) Encrypt by P_1 (2) Encrypt by P_2 → $N(S([0,3]))_{K12}$, $N(S([4,7]))_{K12}$, $N(S([8, 15]))_{K12}$

P_2 (K_2): [2, 5] → N(T(2)), N(T(5)) → (1) Encrypt by P_2 (2) Encrypt by P_1 → $N(T(2))_{K21}$, $N(T(5))_{K21}$

If P_1 does the comparison, it can conclude that [4,7] ∩ [2, 5] = [4, the original number of $N(T(5))_{K21}$]

Conclusion and Future Work

- Propose a secure protocol to validate the reachability cross multiple SDNs for smart grids
- This initial effort can be extended in several directions
  - ➢ Implement a prototype and evaluate the performance of proposed protocol
  - ➢ Refine the protocol for adaptation to topological variations of networks, such as links go down and new links get added
  - ➢ In addition to reachability, we propose to validate other security properties (e.g., link length) in the context of multiple SDNs for smart grids.

References

[1] Kumar, Rakesh, and David M. Nicol. "Validating resiliency in Software Defined Networks for smart grids." *Smart Grid Communications (SmartGridComm), 2016 IEEE International Conference on*. IEEE, 2016.

[2] Chen, Fei, Bezawada Bruhadeshwar, and Alex X. Liu. "Privacy-preserving cross-domain network reachability quantification." *Network Protocols (ICNP), 2011 19th IEEE International Conference on*. IEEE, 2011.

[3] Pohlig, Stephen, and Martin Hellman. "An improved algorithm for computing logarithms over GF (p) and its cryptographic significance (Corresp.)." *IEEE Transactions on information Theory* 24.1 (1978): 106-110.

SCIENCE OF SECURITY
VIRTUAL ORGANIZATION
Funded by the National Security Agency.

INFORMATION TRUST INSTITUTE