Automated Verification of Safety Properties of Declarative Networking Programs

Chen Chen
University Of Pennsylvania
chenche@seas.upenn.edu

Lay Kuan Loh
Carnegie Mellon University
lkloh@cmu.edu

Limin Jia
Carnegie Mellon University
liminjia@cmu.edu

Wenchao Zhou
Georgetown University
wzhou@cs.georgetown.edu

Boon Thau Loo
University Of Pennsylvania
boonloo@cis.upenn.edu

Abstract

Networks are complex systems that unfortunately are ridden with errors. Such errors can lead to disruption of services, which may have grave consequences. Verification of networks is key to eliminating errors and building robust networks. In this paper, we propose an approach to verify networks using declarative networking, where networks are specified in NDLog, a declarative language. We focus on analyzing safety properties. We develop a technique to statically analyze NDLog programs: first, we build a dependency graph of the predicates of NDLog programs; then, we build a summary data structure called a derivation pool to represent all possible derivations and their associated constraints for predicates in the program; finally, properties specified in first-order logic are checked on the data structure with the help of the SMT solver Z3. We build a prototype tool and demonstrate the effectiveness of the tool in validating and debugging several SDN applications.

Keywords: Declarative networking, static analysis

1. Introduction

As more and more services are offered over the Internet, ensuring the security and stability of networks has become increasingly important. Unfortunately, networks are complex systems that are ridden with errors. Such errors can lead to disruption of services, which may have grave consequences. Verification of networks is key to eliminating errors and building robust networks. Much work on network verification has focused on verifying topological-specific network configurations [18, 22, 33, 38]. Practical testing tools for finding undesired behavior in protocol implementation have also been proposed [16, 25]. With the emerging technology of software-defined networking (SDN), modeling networks as programmable software has gained unprecedented popularity. Researchers began to apply program verification techniques to the verification of SDNs [8, 9].

Our goal is to develop a general automated technique that can be applied to network verification. The first step towards that goal is to find the right abstraction for networks. Declarative networking [31] is one of the first research efforts to demonstrate that high-level languages can be used to program networks. In declarative networking, network protocols are written in a declarative language NDLog, which is a distributed Datalog. Declarative networking techniques have been used in several domains including fault tolerance protocols [45], cloud computing [4], sensor networks [13], overlay network compositions [34], anonymity systems [44], mobile ad-hoc networks [27, 36], wireless channel selection [26], network configuration management [12], and forensic analysis [53–55]. An open-source declarative networking system called RapidNet [43] has been integrated with the ns-3 [39] simulator, so protocols can be tested. It has also been shown that network verification can be carried out using the declarative network framework [10, 47, 48].

In summary, NDLog is a great intermediary language for bridging the gap between network specification, verification, and implementation, so we use NDLog as our specification language for networks.

Unfortunately, all of the verification tools related to NDLog require manual proofs, which makes verification very labor intensive. What is worse is that when the proofs cannot be constructed, it is nontrivial to find out what went wrong. Either there are bugs in the program, or the invariants used in the proofs are not correct. There is little tool support for identifying problems under these circumstances. In this paper, we develop an automated static analysis technique to analyze the safety properties of NDLog programs. When properties do not hold, our tool provides a concrete counterexample to further aid program debugging. The properties that we are interested in include invariants of the network and desirable behavior of nodes in the network. For instance, we would like to know if every forward entry corresponds to a route announcement packet, or if a successfully delivered packet indicates proper forwarding to the destination of nodes in the network. For instance, we would like to know if every forward entry corresponds to a route announcement packet, or if a successfully delivered packet indicates proper forwarding to the destination of nodes in the network. For instance, we would like to know if every forward entry corresponds to a route announcement packet, or if a successfully delivered packet indicates proper forwarding to the destination of nodes in the network. For instance, we would like to know if every forward entry corresponds to a route announcement packet, or if a successfully delivered packet indicates proper forwarding to the destination of nodes in the network.

Our static analysis examines the structure of the NDLog program and builds a summary data structure for all derivations of that program. Properties specified in the restricted format of first-order logic are checked on the summary data structure with the help of the SMT solver Z3 [50]. The challenge is how to deal with recursive programs. For such programs, the number of possible derivations for recursive predicates is infinite. We use a concise representation for recursive predicates, so all possible derivations can be finitely represented. To evaluate our analysis, we built a prototype tool, and verified several safety properties of a number of SDN controller programs, where the SDN’s controller program and switch logic are specified in NDLog.

This paper makes the following technical contributions.

- We developed algorithms for automatically analyzing a class of safety properties of NDLog programs.
• We proved the correctness (soundness and completeness) of our algorithms for non-recursive programs and proved the soundness of our algorithms for recursive programs.

• We implemented a prototype tool and verified a number of safety properties of SDN controller programs.

The rest of this paper is organized as follows. In Section 2, we review declarative networks and NDLog, and describe our analysis at a high-level. Then, we explain our algorithm for non-recursive programs in Section 3. Next, we extend the algorithm to handle recursive programs in Section 4. The case studies are described in Section 5. We discuss related work in Section 6 and then conclude.

Due to space constraints, we omit many technical details. They can be found in our companion technical report [11].

2. Overview
We first review declarative networking and NDLog through examples. Then, we present an overview of our analysis.

2.1 Declarative Networking
Declarative networks are specified using Network Datalog (NDLog), which is a distributed recursive query language used for querying network graphs. Declarative queries are a natural and compact way to implement a variety of routing protocols and (over)-lay networks. For example, traditional routing protocols such as path vector and distance-vector protocols can be expressed in a few lines of code [29], and the Chord distributed hash table in 47 lines of code [28]. When compiled and executed, these NDLog programs perform efficiently relative to imperative implementations.

NDLog is based on Datalog [42]. A Datalog program consists of a set of declarative rules. Each rule has the form \( p :- q_1, q_2, \ldots, q_n, \ldots, q_m \), which can be read as \("q_1, q_2, \ldots, q_n\) implies \( p\)." Here, \( p \) is the head of the rule, and \( q_1, q_2, \ldots, q_n \) is a list of literals that constitutes the body of the rule. Literals are either predicates with attributes (which are bound to variables or constants), or Boolean expressions that involve function symbols (including arithmetic) applied to attributes, which we call constraints.

Datalog rules can refer to one another in a mutually recursive fashion. Commas are interpreted as logical conjunctions. The names of predicates, function symbols, and constants begin with a lowercase letter, while variable names begin with an uppercase letter. The following example NDLog program computes full reachability between any pair of nodes. In the runtime, derived predicates are stored as tuples in database tables, so we use predicate and tuple interchangeably for the rest of this paper.

**Reachable:**

\[
\begin{align*}
d1 & \text{ reachable}(\langle X, Y, C \rangle) :- \text{ link}(\langle X, Y, C \rangle). \\
d2 & \text{ reachable}(\langle X, Y, C \rangle) :- \text{ link}(\langle X, Z, C1 \rangle), \text{ reachable}(\langle Z, Y, C2 \rangle), C=C1+C2. \\
d3 & \text{ reachable}(\langle X, Y, C \rangle) :- \text{ link}(\langle X, Z, C1 \rangle), \text{ link}(\langle Z, Y, C2 \rangle), C=C1+C2. \\
\end{align*}
\]

The program `reachable` takes as input \( \text{link}(\langle X, Y, C \rangle) \) tuples, where each tuple corresponds to a copy of an entry in the neighbor table, and represents an edge from the node itself (\( X \)) to one of its neighbors (\( Y \)) of cost \( C \). NDLog supports a location specifier in each predicate, expressed with a symbol followed by an attribute. This attribute is used to denote the source location of each corresponding tuple. For example, \( \text{link} \) tuples are stored based on the value of the \( X \) field. The program `reachable` derives `reachable(\( \langle X, Y, C \rangle \)` tuples, where each tuple represents the fact that \( X \) has a path to \( Y \) with cost \( C \). Rule `d1` derives `reachable` tuples from direct links. Rule `d2` and `d3` compute transitively reachable: if there exists a link from \( X \) to \( Z \) with cost \( C1 \), and \( Z \) knows about a path to \( Y \) with cost \( C2 \), then, \( X \) can reach \( Y \) with cost \( C1+C2 \). Rule `d3` is similar to `d2`.

As our driving example, we will use the following erroneous program. The following non-recursive set of rules computes one-, two-, and three-hop reachability information within a network. There is an error in rule `r2`, where `onehop X Z C2` should be `onehop Z Y C2`, thus this program cannot derive three-hop paths.

**Threehops (with a deliberate error in `r2`):**

\[
\begin{align*}
r1 & \text{ onehop}(\langle X, Y, C \rangle) :- \text{ link}(\langle X, Y, C \rangle). \\
r2 & \text{ twohops}(\langle X, Z, C \rangle) :- \text{ link}(\langle X, Z, C \rangle), \text{ onehop}(\langle X, Z, C1 \rangle), \text{ onehop}(\langle X, Z, C2 \rangle), C = C1+C2. \\
r3 & \text{ threehops}(\langle X, Y, C \rangle) :- \text{ onehop}(\langle X, Z, C1 \rangle), \text{ twohops}(\langle Z, Y, C2 \rangle), C = C1+C2. \\
r4 & \text{ threehops}(\langle X, Y, C \rangle) :- \text{ twohops}(\langle X, Z, C1 \rangle), \text{ onehop}(\langle Z, Y, C2 \rangle), C = C1+C2. \\
\end{align*}
\]

2.2 Analysis Overview
The static analysis mainly consists of two processes: a process that summarizes all derivations of predicates in an auxiliary data structure, which we call a derivation pool, and a process that queries properties on the derivation pool. NDLog programs are represented abstractly as dependency graphs. Recursive programs are more complicated than non-recursive programs, so we explain the algorithms for non-recursive programs first, before we discuss extensions to support recursive programs. The dependency graph and the properties to be checked are of the same form for both recursive and non-recursive programs. Next, we formally define the dependency graph and the format of the properties.

**Dependency graph** A dependency graph has two types of nodes, predicate nodes, denoted \( N_p \) and rule nodes, denoted \( N_r \). Each predicate node corresponds to a tuple in the program. A predicate node consists of a unique ID for the node, the name of the predicate and its type, and a tag indicating whether the predicate is on a cycle or not. Each rule node corresponds to a rule in the program. A rule node consists of a unique ID, the head of the rule, the body of the rule, which is a list of predicates, and the constraints. The edges, denoted \( E \), are directional. Each edge points either from a rule node to the predicate node which is the head of that rule node, or from a predicate node to a rule node where the predicate is in the rule body.

**Predicate type** \( \tau \) := \( \text{Pred} \) \& \( | \text{bt} \supset \tau \)

**Dependency graph** \( G \) := \( \{ N_p \}, N_r, E \) List

**Predicate node** \( N_p \) := \( \{ nID, p, \tau, cyc \} \)

**Rule node** \( N_r \) := \( \{ rID, hd, body, c \} \)

**Edge** \( E \) := \( \{ rID, nID \} \)

**Rule head** \( hd \) := \( p(\bar{x}) \)

**Rule body** body := \( p_1(x_1), \ldots, p_n(x_n) \)

**Rule constraints** c := \( e_1 \& e_2 \& c_1 \& c_2 \& c_3 \& \exists r. c \)

To make variable substitutions easier, each predicate takes unique variables as arguments. For instance, the following two NDLog rules are equivalent, but we use \( r1 \) as the normal form.

\[
\begin{align*}
r1: & p(x,y) :- q(x_1), s(y_1), x_1=y_1, x=x_1, y_1=y_2. \\
r2: & p(x,y) :- q(x), s(y), x=y. \\
\end{align*}
\]

**Properties** We focus on safety properties, which state that bad things have not happened yet. We use trace-based semantics of NDLog [10, 40]. The advantage of trace-based semantics over fixed point semantics is that the order in which predicates are derived can be clearly specified using traces. Fixed point semantics only care about what is derivable in the end, and are not precise enough to capture transient faults that appear only in the middle of the execution of network protocols.

To make it possible for automated analysis, we restrict the form of properties to be the following:

\[
\phi = \forall x_1. p_1(x_1) \land \cdots \land \forall x_n. p_n(x_n) \land c_p(x_1 \cdots x_n) \supset \exists y_1. q_1(y_1) \land \cdots \land \exists y_m. q_m(y_m) \land c_q(x_1 \cdots x_n, y_1 \cdots y_m)
\]
The meaning of the property is the following: if all of the predicates $p_i$ are derivable, and their arguments satisfy constraint $c_p$, then each of the predicate $q_j$ must be in one of the derivations of $p_i$, and the constraint $c_q$ must be true. We implicitly require $q_j$ to be derived before $p_i$. A lot of the correctness properties can be specified using formulas of this form. For instance, we can specify derivable for some threehops rule of the derivation, the conclusion of that rule is inductively defined. The base tuples, denoted $\Delta$, forms the set of all derivation trees rooted at that predicate. It is derivable for some $x, y, z$. Q1 states that to derive threehops $x y z$, it is necessary to derive twohops $x' y'$ for some $x'$ and $y'$. Q1 does not hold because there are two ways to derive threehops and one of them does not contain such a twohops tuple as a sub-derivation. Q2 states that to derive a threehops tuple, three links connecting those two nodes are necessary. Q3 should hold. Q3 states that threehops tuple is derivable for some $x, y,$ and $z$.

3. Analyzing Non-recursive Programs

In this section, we first explain how to compute the derivation pool for a non-recursive NDLLog program. Then, we show how to check properties. Next, we show how to incorporate network constraints into our property checking algorithm. Finally, we prove the correctness of our algorithm and analyze its time complexity.

3.1 Derivation Pool Construction

For a non-recursive program, its derivation pool maps each predicate to the set of all derivation trees rooted at that predicate. It is formally defined as follows:

\[
\begin{align*}
\text{Derivation pool} & \quad dpool ::= \cdot \\
\text{Entries} & \quad \Delta ::= \cdot \\
\text{Derivation} & \quad D ::= (BT, p(\vec{x})) \mid (rID, p(\vec{x}), D, List)
\end{align*}
\]

We write $dpool$ to denote derivation pools. We write $\Delta$ to denote lists of pairs of a constraint and a derivation tree, denoted $D$. At a high-level, $D$ can be instantiated to be a valid derivation of $p(\vec{t})$ using rules in the program, if $c$ is satisfiable. A derivation tree, $D$, is inductively defined. The base tuples, denoted $(BT, p(\vec{x}))$, are the leaf nodes. A non-leaf node consists of the unique rule ID of the last rule of the derivation, the conclusion of that rule $p(\vec{x})$, and the list of derivation trees for the body predicates of that rule ($D, List$). We write $dpool(p)$ to denote $dpool((nID, p, \tau), \Delta)$, which returns $\Delta$.

Figure 1 and 2 present the main functions used for constructing a derivation pool from a dependency graph. The top-level function GENDPPOOL is defined in Figure 1. This function follows the topological order of the nodes in the dependency graph $G$. We keep track of a working set $P$, which is the set of nodes whose derivations can be summarized currently. We also keep track of the set of edges that have not traversed yet. The function terminates when all of the edges in the dependency graph have been traversed and the derivations for all of the predicates in the dependency graph are built. In the body of GENDPPOOL, we remove one predicate node from $P$, and build all derivations for it. A base tuple’s only possible derivation is one with itself as the leaf node. The constraint associated with this derivation is the trivial true constraint $\top$ (Line 8). When $p$ is not a base tuple, derivations for tuples that $p$’s derivations depend on have been stored in $dpool$. The GENDS function constructs derivations for $p$ given the dependency graph and the current derivation pool (explained later).

After the derivations for a predicate $p$ are constructed, outgoing edges from $p$ are removed (Line 13), so predicates that depend on $p$ can be processed in later iterations. Function REMOVEEDGES removes outgoing edges from $p$, and outgoing edges from rule nodes that now do not have incoming edges. This may result in predicates enqueued into $P$ for the next iteration of processing.

Function GENDS (Figure 2) takes the dependency graph, the derivation pool that has been constructed so far, and a predicate $p$, as arguments, and returns all derivation pool entries for $p$. The body of GENDS calls GENDRULE to construct derivations for each rule that derives $p$. The function GENDRULE makes use of List map and fold operations to construct all possible derivations of $p$ from a rule of the form $r: p(\vec{x}) :- q_1(y_1), \ldots, q_n(y_n), c$. $dpool$ has already stored all possible derivations for each $q_i$. We need to compute all combinations of the derivations for $q_i$s. The LOOKUp function on line 11 collects the list of derivations for one body tuple and the list map function returns the list of derivations for all body tuples. More precisely, the LOOKUp function returns a list of tuples of the form $(\sigma, c, d)$, where $d$ is a derivation, $c$ is the constraint associated with that derivation, and $\sigma$ is a variable substitution. The domain of $\sigma$ is $q_i$‘s arguments in the rule node, and the range of $\sigma$ is $q_i$‘s arguments in the conclusion of the derivations. We need these substitutions because we alpha-rename the derivations. The constraint in the rule node needs to use the correct variables. Line 12 uses list fold operation to generate all possible derivations. Function MERGEDDLL and MERGEDL are helper functions to generate the list of derivations. Function MERGED is the function that takes as arguments, the list of derivations from $q_m$ to $q_{m+1}$ and one derivation for $q_i$, and prepends the derivation for $q_i$ to the list of derivations from $q_m$ up to $q_i$. Here, the substitutions need to be merged and the resulting constraint is the conjunction of the two constraints. Finally on line 14, function COMPLETED generates a well-formed derivation for $p$ using the rule ID and the list of derivations for $q_i$s. The constraint associated with this derivation of $p$ is the conjunction of constraints for the derivation of $q_i$ and the constraint in the rule body. The substitutions are applied to the constraint $c$, because all derivations are alpha-renamed and use fresh variables.

3.2 Property Query

Figure 3 shows the property query algorithm for non-recursive programs. The top-level function CKPROP takes the derivation
1: function GENDS(\(G\), \(dpool\), \((nID, p; \tau)\))
2: \(\Delta \leftarrow \{\}\)
3: for each rule with ID \(rID\) where \((rID, nID)\) in \(G\) do
4: \(\Delta \leftarrow \Delta \cup \text{GENDRULE}(\(G\), \(dpool\), \((nID, p; \tau), rID\))
5: return \(\Delta\)
6: end function
7: function GENDRULE(\(G\), \(dpool\), \((nID, p; \tau)\), \(rID\))
8: \((p(\bar{g}), Q, c_r) \leftarrow G(rID)\)
9: (* \(Q = q_1 \cdots q_m\))
10: \(D\) is the list of list of derivations for \(q_1 \cdots q_m\)*
11: \(D \leftarrow \text{LIST.MAP} (\text{LOOKUP} dpool) Q\)
12: \(D' \leftarrow \text{LIST.FOLDRIGHT MERGEDIVISION} D \text{ nil}\)
13: \(\bar{x} \leftarrow \text{fresh}(p(\bar{g}))\)
14: return \text{LIST.MAP} (\text{COMPLETED} c_r, \(rID\), \(p(\bar{g})\), \(\bar{x}\)) \(D'\)
15: end function
16: function MERGEDIVISION(\(c_d\), \(d_{c_2}\))
17: (* \(d_{c_2}\) is a derivation for \(q_0 \cdots q_{k+1}\)
18: \(dc_i\) is a possible derivation of \(q_i\)*)
19: \((\sigma_2, c_2, d_{22}) \leftarrow d_{c_2}\)
20: \((\sigma_1, c_1, d_i) \leftarrow dc_i\)
21: (* \(\sigma_i\) substitutes new vars in \(q_i\) for old ones*)
22: \((\sigma'_i, \sigma'_i, d'_i) \leftarrow \text{fresh}(c_i, d_i)\)
23: return \((\sigma, \sigma'_i \cup \sigma_2, c_2 \land c_2, d'_i:d_{22})\)
24: end function
25: function LOOKUP(dpool, \(q(\bar{x})\))
26: function EXTRACTD(\(q, (c, d)\))
27: return \(\text{COMPLETE}(c_r, \(rID\), \(p(\bar{g})\), \(\bar{x}\), \(d)\))
28: end function
29: end function
30: function COMPLETE(\(c_r\), \(rID\), \(p(\bar{g})\), \(\bar{x}\), \(d)\))
31: return \((c \land c_r[\bar{x}/\bar{g}]: \text{MAP}(\bar{x})(\bar{g})\), \(rID\), \(p(\bar{x}), d)\))
32: end function

Figure 2. Generate derivation pool for one predicate

pool and the property as arguments. On line 3, we separate the property into the list of predicates to the left of the implication \((P)\), the constraint to the left of the implication \((c_p)\), the list of predicates to the right of the implication \((Q)\), and the constraint to the right of the implication \((c_q)\). Next, similar to the derivation pool construction, we construct all possible combinations of the derivations of all the \(p_i\)s in \(P\) between lines 5 to 9. We omit the definition of MERGEDIVISION, as it is similar to MERGEDIVIDATION. The only difference is that we do not need to alpha-rename the derivations. Next, we check that for each possible derivation of \(p_i\)s in \(P\), each of \(q_i\)s appear in the derivation, and the constraint \(c_p\) holds (lines 10 to 14) using function CKPROP. If for all possible derivations of \(p_i\)s, we can always find derivations of \(q_i\)s such that the constraint \(c_p\) holds, \(P\) holds (line 14).

The function CKPROP checks that in the list of derivations \(D\), with constraints \(c_q\), whether all the predicates in \(Q\) appear in \(D\), and \(c_q\) is true. On Line 18, we first check whether all the \(p_i\)s are derivable and constraint \(c_p\) is satisfiable. If the conjunction of the derivation constraint \(c_q\) and \(c_p\) is not satisfiable, then the precedent of \(\varphi\) is false, so \(\varphi\) is trivially true for that derivation. So, we return valid in the else branch (line 38). If the conjunction is satisfiable, then there are substitutions for variables so that all the \(p_i\)s are derivable and the constraint \(c_p\) is satisfiable. Next, we need to check whether all \(q_i\)s are derivable. On line 20, function UNIFY identifies a list of occurrences of \(q_i\) in the derivation \(d\). That is, for each \(q_i(\bar{y})\) appearing in \(d\), UNIFY returns the list of substitutions: \((\bar{y}_i/\bar{x}):(\bar{y}_i/\bar{x})::\cdots::(\bar{y}_i/\bar{x})::\text{nil}\), where \(\bar{x}\) is \(q_i\)’s arguments in \(\varphi\). The list map function returns the list of the list of occurrences for all the \(q_i\)s in \(Q\). We call it “UNIFY” because we unify the variables that are \(q_i\)’s arguments in \(\varphi\) with \(q_i\)’s arguments in the derivation \(d\). This substitution will be applied to constraint \(c_q\) later. If some \(q_i\) does not appear in \(d\), then UNIFY will return an empty list nil. Therefore, on line 21, we check whether each \(q_i\) will appear at least once in \(d\). If it is not the case, then we return invalid with the current derivation and one satisfying substitution that makes \(p_i\)s true for constructing a counterexample. Otherwise, we check whether the constraint \(c_p\) can be satisfied. Before doing so, on line 29, we first compute the list of all possible combinations of occurrences of \(q_i\)s. Again, the function MERGEDIVIDATION is similar to MERGEDIVISION and we omit the details. Now on line 30, for each possible appearance of \(q_i\)s in \(d\), \(\Sigma_q\) is a list of substitutions, each of which, when applied to \(c_q\), makes \(c_q\) use the same variables as those in the derivation. We ask whether the negation of \(c_q\) together with the derivation constraint and the constraint on the arguments of \(p_i\)s are satisfiable.
function CKPROPDC(c_d, c_p, d, Q, c_q, β, c_b)
if CHECK SAT c_d ∧ c_p = (sat, σ_p)
(* find all occurrences of b
Σ_b ← LIST.MAP (UNIFY d) β
(* Σ_b is a list of substitutions. Each substitution
in Σ_b corresponds to one combination of b in d *)
Σ_b ← MERGE LL Σ_b
(* Given Σ_b = σ_1:1 · · · :σ_m, c_b = ∨_i=1^m c_bσ_d^i *)
c_b ← CONS (Σ_b, c_b)
(* find all occurrences of q in d *)
Σ ← LIST.MAP (UNIFY d) Q
if nil ∈ Σ then
(* check network constraints *)
if CHECK SAT c_d ∧ c_p ∧ (c_b) = (sat, σ_c)
(* Network constraints are met *)
return valid
else
return invalid (d, σ_c)
else
(* Find all possible combinations for q_1 · · · :q_m
Σ_q is a list of substitutions of form σ_q_1: · · · :σ_q_m
σ_q_d = Σ_q is a substitution for variables in one
appearance of q_1 to q_m in d, for variables that
appear in Q *)
Σ_q ← MERGE LL Σ_q
(* c_q is unsat for any substitutions that make
q_m appear in d *)
c_q ← c_d ∧ c_p ∧ ∨_i=1^m ¬c_q σ_d^i
if CHECK SAT c_q = (sat, σ_q)
(* Network constraints are met *)
return invalid (d, σ_q)
else
return valid
else
(* c_q is sat *)
return valid
else
(* Constraints for p_1 · · · :p_n and c_q are unsat *)
return valid
end function

Figure 4. Property query with network constraints

If this is not satisfactory, then we know that there exists a substitution for variables so that the property ϕ holds. Otherwise, we return the derivation and the satisfying substitution that makes p_1 and q_m derivable, but c_q false for counterexample construction.

3.3 Network Constraints
Sometimes, the network being analyzed has certain network constraints; for instance, every node in the network has only one outgoing link. Our property query algorithm needs to take into consideration these network constraints. If we ignore these constraints, the counterexample generated by the tool may not be useful as the counterexample could violate the network constraints.

Network constraints that our analysis can handle have similar form as the properties: ∀x_1 b_1 (x_1) ∧ · · · ∧ ∀x_k b_k (x_k) ⊇ c_0 (x_0 · · · :x_k), where b_i is a base tuple. Figure 4 shows the algorithm for checking properties on networks with constraints. For clarity, we explain the case with one network constraint. Extending the algorithm to handle multiple constraints is straightforward.

The top-level function CKPROPDC (omitted here) is almost the same as CKPROP, except that it takes a network constraint (ϕ_net) as an additional argument and uses the function CKPROPDC, which additionally checks network constraints compared to CKPROP. The function CKPROPDC takes as additional arguments, a list base tuples B and the constraint c_b in the network constraint. In the body of CKPROPDC, we first check whether the constraint on p_1 is satisfiable. If it is not, then this derivation does not violate the property we are checking. Next, between lines 3 to 10, we find all occurrences of the base tuples in the constraint ϕ_net. We find all possible combinations of substitutions for these base tuples as they appear in the derivation d. For each occurrence of the base tuples, the constraint c_b needs to be true, so we compute the conjunction of all the c_b. To give an example, if the constraint is ∀x_1, b(x_1) ≥ x_0. If d has two occurrences of b, b(y) and b(z), then c_b = y ≥ 0 ∧ z ≥ 0.

Next, we collect the list of the occurrences of q_m, the same as before. If some q_m does not appear in d (line 13), we additionally check whether this derivation d satisfies the network constraint (line 15). If it is the case, then we find a counterexample. Otherwise, d does not violate the property being checked.

Then, we compute the combination of all possible occurrences of q_m (line 21) as usual. For each substitution that makes all q_m appear in d, we check whether c_q is satisfiable. Between lines 30 to 33, c_q is satisfiable, so we need check that the network constraint is satisfied. If this is the case, d satisfies the property being checked. Otherwise, we have to try the next substitution that makes all q_m appear in d. On line 34, we finished the loop and c_q is not satisfiable for any of the substitutions that make q_m appear in d. Again, we check the network constraints on d, and report an error only if d satisfies the network constraint.

3.4 Analysis of the Algorithms
Correctness. We first prove that our derivation pool construction is correct. Lemma 1 states that an entry for a predicate p in the derivation pool maps to a valid derivation of ϕ if the constraints of that derivation is satisfiable; and that if a predicate p is derivable, then there must be a corresponding entry in the derivation pool. The function DGRAPH generates a dependency graph for prog, which can be straightforwardly defined. The semantics of NDLog programs are bottom up, so a set of base tuples B is needed to start the execution of the program. We write σ ≥ ϕ to mean that σ extends ϕ. B denotes a set of ground base tuples of prog. We write prog, B = d · p(ϕ) to mean that d is a derivation of p(ϕ) using program prog and base tuples B. We write (c, d · p(ϕ)) ∈ dpool (p) to mean that (c, d) is an entry in the derivation pool dpool for the predicate p and that d is a derivation tree with p(ϕ) as the root.

Lemma 1 (Correctness of derivation pool construction).
DGRAPH (prog) = G and GEN DPOOL (G) = dpool

1. If prog, B = d · p(ϕ), then exists σ where dom (σ) = x_d and (c (x_d), d (x_d); p(ϕ)) ∈ dpool (p) s.t. d (x_d)σ · p (ϕ) = d · p (ϕ) and = c (x_d)σ.

2. If (c (x_d), d (x_d); p(ϕ)) ∈ dpool (p) and = c (x_d)σ, then exists σ. B where dom (σ) = x_d and (c (x_d)σ) = (c (x_d)σ), and B = {b | b is a base tuple, b appears in d (x_d)} s.t. prog, B = d (x_d)σ · p (ϕ)σ.

Using the result of Lemma 1, we prove our property checking algorithm is correct with regard to the formula semantics.

Theorem 2 (Correctness of property query).
ϕ = ∀x_1 · p_1 (x_1) · · · ∧ ∀x_k · p_k (x_k) · · · ∧ c_p (x_1 · · · x_k) ⊇ ∃y_1 · q_1 (y_1) · · · ∧ ∃y_m · q_m (y_m) ⊇ c_q (x_1 · · · x_n) · y_1 · · · y_m
DGRAPH (prog) = G and GEN DPOOL (G) = dpool,

1. CKPROP (dpool, ϕ) = valid implies ∀B, prog, B = ϕ.
2. \( \text{CkProp}(dpool, \phi) = \text{invalid}(d, \sigma) \implies \exists B \text{ s.t. } \text{prog}, B \not\equiv \phi \).

When network constraints are provided, we prove that the property checking algorithm is correct with regard to the network constraints on base tuples.

**Theorem 3** (Correctness of property query with constraints),
\[
\phi = \forall \vec{x}, p_1(\vec{x}) \land \cdots \land \forall \vec{x}, p_n(\vec{x}) \land c_\phi(\vec{x}, \cdots, \vec{y}) \supset \exists y_1(q_1(y_1)) \land \cdots \land \exists y_m(q_m(y_m)) \land c_\phi(\vec{x}, \cdots, y_1, \cdots, y_m)
\]
\[
\varphi_{nxt} = \forall \vec{x}, \vec{b}_1(\vec{u}_1) \land \cdots \land \forall \vec{x}, \vec{b}_k(\vec{u}_k) \land c_\phi(\vec{u}_1, \cdots, \vec{u}_k)
\]
\[
\varphi_{rec} = \forall \vec{x}, \vec{c}(\vec{u}_1, \cdots, \vec{u}_k) \land c_\phi(\vec{u}_1, \cdots, \vec{u}_k)
\]
\[
\text{Dgraph}(\text{prog}) = \mathcal{G} \text{ and } \text{GenDPool}(\mathcal{G}) = dpool,
\]
1. \( \text{CkPropC}(dpool, \varphi_{nxt}, \varphi) = \text{valid implies } \forall B, \text{ either } B \not\equiv \varphi_{nxt} \text{ or } \text{prog}, B \equiv \phi \).
2. \( \text{CkPropC}(dpool, \varphi_{rec}, \varphi) = \text{invalid}(d, \sigma) \implies \exists B \text{ s.t. } \text{prog}, B \not\equiv \varphi \text{ and } \text{prog}, B \equiv \varphi_{rec} \).

**Time complexity.** We give an upper bound on the time complexity of the property query algorithm (Figure 3). Given an NDL program with \( R \) rules; each rule contains at most \( W \) body tuples. Also assume \( |Q| = m \) and \( |P| = n \). The time complexity of our algorithm is \( O((R^m W^n) n^m W^m) \). In practice, \( R \) and \( W \) are usually small. For example, in our case study, \( R \) is bounded by 11 and \( W \) is bounded by 5. In this case, \( R \) and \( W \) can be viewed as constants.

4. **Extension to Recursive Programs**

The dependency graph for a recursive program contains cycles. The derivation pool construction algorithm presented in Figure 1 does not work for recursive programs because it relies on the topological order of nodes in the dependency graph. In this section, we show how to augment our data structures and algorithms to handle recursive programs.

4.1 **Derivation Pool for Recursive Predicates**

When \( p \) is recursively defined, \( dpool \) maps \( p \) to a pair \((c, \Delta)\), where \( \Delta \) has the same meaning as before. The additional constraint \( c \) is an invariant of \( p \); \( c \) is satisfiable if and only if \( p \) is derivable.

\[
\begin{align*}
\text{Constraint pool} & \quad dpool \ ::= \cdots \mid dpool, (nID, p; \tau) \rightarrow (c, \Delta) \\
\text{Derivation pool} & \quad D \ ::= \cdots \mid \{\text{rec, } p(\vec{z})\} \\
\text{Annotation} & \quad A \ ::= \cdots \mid \{\text{rec, } p(\vec{z})\} \rightarrow (\vec{x}, c)
\end{align*}
\]

Derivation trees include a new leaf node \((\text{rec, } p(\vec{z}))\), where \( p \) appears on a cycle in the dependency graph. This leaf node is a place holder for the derivation of \( p \). We write \( A \) to denote annotations for recursive predicates, provided by the user. \( A \) maps a predicate \( p \) to a pair \((\vec{x}, c)\), where \( \vec{x} \) is the arguments of \( p \) and \( c \) is the constraint which is satisfiable if and only if \( p \) is derivable.

The structure of the derivation pool construction remains the same. We highlight the changes in Figure 5. The main difference is that now when a cycle is reached, the annotations are used to break the cycle. The working set \( P \), which contains the set of nodes that can be processed next, includes not only predicate nodes that do not have incoming edges, but also includes nodes that depend on only body tuples that have annotations. Consider the following scenario: Rule \( r_1 \) derives \( p \) and has two body tuples \( q_1 \) and \( q_2 \). Let’s assume that there is no edge from \( q_1 \) to \( r_1 \), as \( q_1 \) has been processed and \( q_2 \) has an annotation in \( A \). In this case, we will place \( p \) in the working set. The above mentioned change is encoded in the new \text{RemoveEdges} function.

The second change is in constructing derivation pool entries for a predicate \( p \). In the non-recursive case, each derivation tree of a predicate \( p \) corresponds to the application of a rule to the list of derivation trees for the body tuples of that rule. In the recursive case, if one of the body tuples, say \( q \), is on a cycle, when we process \( p \), \( q \)'s entries in \( dpool \) have not been constructed. However, the constraint under which \( q \) can be derived is given in the annotation \( A \). In this case, we use \((\text{rec, } q(\vec{z}))\) as a place holder for derivations of \( q \), and use the constraint in \( A \) as the constraint for this derivation. The change is reflected in the \text{LookUp} function for collecting possible derivations of the body predicates (lines 21-23). Finally, annotations need to be verified. The \text{GenD} function checks the correctness of the annotations after all the predicates have been processed (lines 5-15). For a recursive predicate, the derivation pool maps it to a summary constraint and a list of possible derivations (a pair \((c, \Delta)\)). The requirement of the summary constraint for \( p \) is that it has to be satisfiable if and only if there is at least one derivation for the recursive predicate \( p \). That is, this summary constraint has to be logically equivalent to the disjunction of the constraints associated with all possible derivations of \( p \) in \( \Delta \).

We consider two cases for a predicate on a cycle of the dependency graph: (1) there is an annotation for it in \( A \) and (2) there is no annotation. For both cases, we need to collect all the possible constraints for deriving \( p \) from \( \Delta \). Function \text{EX_Disj} computes the disjunction of constraints in \( \Delta \). Each constraint is existentially quantified over the arguments that do not appear in \( p \). For case (1), we need to check that the annotation is logically equivalent to the disjunction of the constraints for all possible derivations of \( p \) (line 10). If this is the case, then the annotated constraint together with \( \Delta \) is returned; otherwise, an error is returned, indicating that the invariant doesn’t hold. For case (2), we return the disjunctive formula returned by \text{EX_Disj} (lines 15). When \( p \) is not recursive, only \( \Delta \) is returned (line 17).

4.2 **Property Query**

We use the same property query algorithm for non-recursive programs. This obviously has limitations, because the derivations of
recursive predicates are not expanded. The imprecision of the analysis comes from the following two sources. The first is that derivations represented as \((\text{rec}, p(x))\) may contain predicates needed by the antecedent of the property (the \(q_s\) in \(\varphi\)). Without expanding these derivations, the algorithm may report that \(\varphi\) is violated because \(q_s\) cannot be found, even though this is not the case in reality. The second is that network constraints cannot be accurately checked. When we find a suitable derivation \(d\) that contains all the \(q_s\) such that \(c_p\) holds, checking the network constraints on \(d\) requires us to expand \((\text{rec}, p(x))\) in \(d\). The algorithm may report that the property holds, even though, the witness it finds does not satisfy the network constraints. Similarly, when the algorithm reports that the network property does not hold, the counterexample may not satisfy the network constraints. For the analysis to be precise, we would need annotations for recursive predicates to provide invariants for recursive predicates. Our case studies do not require annotations. Expanding the algorithm to handle recursive predicates precisely remains our future work.

4.3 Analysis of the Algorithms

Correctness. Similar to the non-recursive case, we prove the correctness of derivation pool construction. We only prove the soundness of the query algorithm. Because derivations of recursive predicates are summarized as \((\text{rec}, p(x))\), the correctness of the derivation pool construction needs to consider the unrolling of \((\text{rec}, p(x))\). First, we define a relation \(dpool \vdash d, \sigma \rightsquigarrow_k d', \sigma'\) to mean that a derivation \(d\) with the substitution \(\sigma\) can be expanded using derivations in \(dpool\) to another derivation \(d'\) of depth \(k\) and a new substitution \(\sigma'\).

\[
\sigma' \geq \sigma \quad dpool \vdash (BT, p(x)), \sigma \rightsquigarrow_0 (BT, p(x)), \sigma'
\]

\[
\forall j \in [1, n], \ dpool \vdash d_j, \sigma \rightsquigarrow_k d'_j, \sigma'
\]

\[
dpool \vdash (rID, p(x), d_1; \cdots d_n; \text{nil}), \sigma \rightsquigarrow_{k+1} (rID, p(x), d'_1; \cdots d'_n; \text{nil}), \sigma'
\]

\[
dpool (p) = (c, \Delta) \quad (c_i, d_p) \in \Delta \quad \vdash c_i \sigma'
\]

\[
dpool \vdash d_{p}, \sigma \rightsquigarrow_{k} d_{p}, \sigma''
\]

The first rule applies to the base tuples. Here, no unrolling is needed and the depth of the derivation is 0. The second rule unrolls the premises of a derivation \(d\). The depth of \(d'\) is \(k + 1\). The last rule is the key rule that unrolls the derivation of recursive predicate \(p((\text{rec}, p(x))) using one of the possible derivations of \(p\) from \(\Delta\). Here, the unrolling can only use the derivation in \(\Delta\), whose constraint can be satisfied.

Lemma 4 shows that the derivation pool construction algorithm is correct with respect to an unrolling of the derivation. If a predicate \(p\) is derivable, then the derivation pool should have an entry for \(p\) that can be unrolled into that derivation. In the other direction, for every entry in the derivation pool, it either unrolls into a finite derivation, or can be further unrolled. This lemma allows the unrolling to be infinite.

Lemma 4 (Correctness of derivation pool construction (recursive)). DGRAPH\((prog) = \mathcal{G}\), and GENDPool\((\mathcal{G}, A) = dpool\)

\[
1. \text{If } prog, B \models d : p(\bar{x}) \text{ then } \]

\[
(a) \text{ either } p \text{ is not on a cycle in the dependency graph and exists } \sigma \text{ and } (c, d': p(\bar{x})) \in dpool(p) \text{ s.t. } dpool \vdash d', \sigma \rightsquigarrow_{|d|} d_1, \sigma, d = d_1 \sigma \text{ and } \vdash \sigma.
\]

\[
(b) \text{ or } p \text{ is on a cycle in the dependency graph and exists } \sigma \text{ and } (c_p, \Delta_p) \in dpool(p) \text{ s.t. } dpool \vdash (\text{rec}, p(\bar{x})), \sigma \rightsquigarrow_{|d|} d_1, \sigma, d_1 \sigma = d \text{, and } \vdash c_p \sigma.
\]

2. \(a) \text{ If } (c, d: p(\bar{x})) \in dpool(p) \text{ and } \vdash \sigma, \text{ then } \forall n, m \leq n, \text{ dpool } \vdash d, \sigma \rightsquigarrow_m d', \sigma', \text{ either } d' \text{ does not contain } \text{(rec, q(y))}, \text{ and exists } B, \text{ s.t. prog, } B \models d' \sigma' : p(\bar{x}) \sigma' \text{ or } d' \text{ contains } \text{(rec, q(y))}, \text{ and replacing all of the } \text{(rec, q(y))} \text{ derivations with a derivation } \sigma' \text{ in } d' \text{ results in a derivation for } p(\bar{x}) \sigma'.
\]

\(b) \text{ If } (c_p, \Delta_p) \in dpool(p) \text{ and } \vdash c_p \sigma \text{ then } \forall n, m \leq n, \text{ dpool } \vdash (\text{rec}, p(\bar{x})), \sigma \rightsquigarrow_m d', \sigma', \text{ either } d' \text{ does not contain } \text{(rec, q(y))}, \text{ and exists } B, \text{ s.t. prog, } B \models d' \sigma' : p(\bar{x}) \sigma' \text{ or } d' \text{ contains } \text{(rec, q(y))}, \text{ and replacing all of the } \text{(rec, q(y))} \text{ derivations with a derivation } \sigma' \text{ in } d' \text{ results in a derivation for } p(\bar{x}) \sigma'.
\]

As we discussed in Section 4.2, we cannot show a general correctness theorem without annotations for recursive predicates. We can only prove the soundness of the algorithm when there is no network constraint.

Lemma 5 (Soundness of property query).

\[
\varphi = \forall x_1, p_1(x_1) \land \cdots \land \forall x_m, p_m(x_m) \land c(x_1 \cdots x_n) \supset
\]

\[
\exists y_1, q_1(y_1) \land \cdots \land \exists y_m, q_m(y_m) \land c_0(x_1 \cdots x_n, y_1 \cdots y_m)
\]

DGRAPH\((prog) = \mathcal{G}\) and GENDPool\((\mathcal{G}, A) = dpool\), and CXP\(\text{Prop}(dpool, \varphi) = \text{valid implies } prog \models \varphi\).

Time complexity. The time complexity of the property query algorithm on recursive programs is the same as that of non-recursive programs. Observe that the height of a derivation in the derivation pool is still bounded by \(R\) (the number of rules in the program). This is because in the derivation pool construction algorithm (Figure 5), each rule node is processed at most once. Therefore a path in a derivation from the root predicate to any leaf predicate could have at most \(R\) rules.

5. Case Study

We apply our tool to the verification of software-defined networking (SDN) applications. SDN is an emerging networking technique that allows network administrators to program the network through well-defined interfaces (e.g., OpenFlow protocol [35]). SDNs intentionally separate the control plane and the data plane of the network. A centralized controller is introduced to monitor and manage the whole network. The controller provides an abstraction of the network to network administrators, and establishes connections with underlying switches. Recently, declarative programming languages have been used to write SDN controller applications [38]. Like any program, these applications are not guaranteed to be bug-free. We show the effectiveness of our tool in validating and debugging several SDN applications. We demonstrate that the tool can unveil problems in the process of SDN application development, ranging from software bugs, incomplete topological constraints and incorrect property specification. All verifications in our case study are completed within one second.

5.1 Verification process

We first provide a high-level description of the verification process. When analyzing a property, the user is expected to provide three types of inputs: (1) formal specification of the property in the form discussed in Section 2; (2) formal specification of initial network constraints (e.g., topological constraints and switch default setup); and (3) formal specification of invariants on recursive tuples.

Our tool takes the above user specifications along with the NDLog program as inputs. It first checks the correctness of the invariants on recursive tuples. After invariants are validated, the tool runs the main algorithm for verification, and outputs either “True” if the property holds, or “False” if the property is not valid. For invalid properties, the tool also generates a concrete counter example to help the programmer debug the program.
Controller installs a flow entry on the switch to match on the source address of the incoming packet.

Updates the local flow table under the instruction of the controller

Switch does not have a hit in its flow entry table for a packet that appeared on it, send by host with mac address SrcMac to target host with mac address DstMac. Therefore, Switch forwarded the packet to Controller to ask it how to proceed.

Controller generates and sends this tuple to switch Switch to allow it to install host with mac address SrcMac into its flow entry table.

A packet that appeared on switch Switch via port InPort, from host with mac address SrcMac, with target host of mac address DstMac, and priority Priority.

Controller forwards the packet to the switch that it connects to via Port.

Controller learns the position of an end host through packets relayed by host with mac address SrcMac.

5.2 Ethernet Source Learning

The first case study we consider is Ethernet source learning, which allows switches in a network to remember the location of end hosts through incoming packets. More specifically, three kinds of entities are deployed in the network: (1) end hosts (servers or desktops) at the edge of the network that send packets to the network through connected switches, (2) switches that forward a packet if the packet matches a flow entry in the forwarding table, or relay the packet to the controller for further instruction if there is a table miss, and (3) a controller that connects to all switches in the network. The controller learns the position of an end host through packets relayed from a switch, and installs a corresponding flow entry in the switch for future forwarding.

Encoding We encode the behaviors of each component in ND-Log. Due to space limitation, we omit the full program and just provide a summary of the program in Table 2.

In a typical scenario, an end host initiates a packet and sends it to the switch that it connects to (rs1). The switch recursively looks up its forwarding table to match against the received packet (rs1, rs2). If a flow entry matches the packet, it is forwarded to the port indicated by the “Action” part of the entry (rs3). Otherwise, the switch wraps the packet in an OpenFlow message, and relays it to the controller for further instruction (rs5). On receiving the OpenFlow message, the controller first extracts the location information of the source address in the packet (the OpenFlow message registers incoming port for each packet), and installs a flow entry matching the source address in the switch (rc1). The controller then instructs the switch to broadcast the mismatched packet to all its neighbors other than the upstream neighbor who sent the packet (rc2). Rules rs5 and rs6 specify the reaction of the switch corresponding to Rules rc1 and rc2 respectively — the switch either inserts a flow entry into the forwarding table (rs5) or broadcasts the packet (rs6) as instructed.

Network constraints We use the following basic network constraints to limit the topology of the network that runs Ethernet source learning.

\[
\begin{align*}
\forall_{\text{net}_1} \quad & \text{initPacket}(\text{Host}, \text{Switch}, \text{Src}, \text{Dst}) \supset \text{Host} \neq \text{Switch} \land \text{Host} = \text{Src} \land \\
& \text{Host} \neq \text{Dst} \land \text{Switch} \neq \text{Dst}, \\
\forall_{\text{net}_2} \quad & \text{ofconn}(\text{Controller}, \text{Switch}) \supset \text{Controller} \neq \text{Switch}, \\
\forall_{\text{net}_3} \quad & \text{swToHst}(\text{Switch}, \text{Host}, \text{Port}) \supset \text{Switch} \neq \text{Host} \land \text{Switch} \neq \text{Port} \land \text{Host} \neq \text{Port}, \\
\forall_{\text{net}_4} \quad & \text{swToHst}(\text{Switch}, \text{Host}_1, \text{Port}_1) \land \\
& \text{swToHst}(\text{Switch}_2, \text{Host}_2, \text{Port}_2) \supset \\
& (\text{Switch}_1 = \text{Switch}_2 \land \text{Host}_1 = \text{Host}_2) \supset \\
& \text{Port}_1 = \text{Port}_2 \land \\
& (\text{Switch}_1 = \text{Switch}_2 \land \text{Port}_1 = \text{Port}_2 \supset \text{Host}_1 = \text{Host}_2). 
\end{align*}
\]

We demand that an end host always initiates packets using its own address as source, and the switch it connects to cannot be the source or the destination (constraints on initPacket). In addition, the controller cannot share addresses with switches (constraints...
on ofconn), and a switch cannot have a link to itself (constraints on single swToHst). Also, each switch should have only one link connecting the neighbor host, and no two hosts can connect to the same port of a switch (constraints on any two swToHsts).

**Verification results** We verify a number of properties that are expected to hold in a network running the Ethernet Source Learning program. We discuss two properties in detail.

The first property specifies that whenever an end host receives a packet not destined to it, the switch that it connects to has no matching flow entry for the destination address in the packet. Formally:

$$\varphi_{ESL2} =$$

$$\forall EndHost, Switch, SrcMac, DstMac, InPort,$$

$$OPort, Outport, Mac, Priority,$$

$$packet(EndHost, Switch, SrcMac, DstMac)$$

$$\land swToHst(Switch, EndHost, OPort)$$

$$\land flowEntry(Switch, Mac, Outport, Priority)$$

$$\land DstMac \neq EndHost$$

$$\land Mac \neq DstMac$$

Though this property is seemingly true, our tool returns a negative answer, along with a counterexample shown in Figure 6. The counter example reveals a scenario where an end host (H4) receives a broadcast packet destined to another machine (H3) (Execution trace (1) in Figure 6), but the switch it connects to (S1) has a flowEntry that matches the destination MAC address in the packet (Execution trace (2) in Figure 6).

In the counter example, switch S1 receives a packet \langle Src : H6, Dst : H3 \rangle through port 2 from the upstream switch S2 (Q). Since S1 does not have a flowEntry for the destination address H3, it relays the packet wrapped in an OpenFlow message (i.e. ofPacket) to the controller C1(2). The controller then instructs S1 to broadcast the packet to all neighbors except S2 (3). However, before Server H4 receives the broadcast packet, a new packet \langle Src : H3, Dst : H4 \rangle could reach switch S1(4), triggering an ofPacket message to the controller (5). The controller would then set up a new flow entry at switch S1, matching destination H3 (6, 7). It is possible that due to network delay, server H4 receives its copy of the broadcast packet just now(8). Therefore, the execution trace generates packet (H4,S1,H6,H3), swToHst(S1,H4,1) (i.e. the link between S1 and H4), and flowEntry (S1,H3,2,1), with Mac == DstMac (H3 = H3).

Our tool also generates a counterexample for another seemingly correct property. This second property specifies that whenever an end host receives a packet destined to it, the switch it connects to has a flowEntry matching the end host’s MAC address. Formally:

$$\varphi_{ESL3} =$$

$$\forall EndHost, Switch, SrcMac, DstMac, OPort,$$

$$packet(EndHost, Switch, SrcMac, DstMac)$$

$$\land swToHst(Switch, EndHost, OPort)$$

$$\land DstMac = EndHost$$

$$\exists Switch', Mac, Outport, Priority,$$

$$flowEntry(Switch', Mac, Outport, Priority)$$

$$\land Switch' = Switch \land Mac = DstMac$$

The generated counter example (Figure 7) shows that a packet could reach the correct destination by means of broadcast — a corner case that can be easily missed with manual inspection. In the counter example, switch S1 receives a packet destined to server H4(1). Since there is no flow entry in the forwarding table to match the destination address, switch S1 informs the controller of the received packet (2), and further broadcasts the packet under the controller’s instruction (3). In this way, server H4 does receive a packet destined to it (4), but switch S1 does not have a flow entry matching H4.

With further inspection, the above counter examples, are attributed to incorrect specification of network properties, rather than bugs in the programs. In the first case, a stricter property would specify that a received broadcast message indicates an earlier table miss. While in the second one, the property fails to consider the possibility of specific broadcast messages in the execution.

### 5.3 Firewall

Our second case study is a stateful firewall, which is usually deployed at the edge of a corporate network to filter untrusted packets from the Internet. Compared to a stateless firewall, which makes decision purely based on specific fields of a packet, a stateful firewall allows richer access control depending on flow history. For example, the firewall can allow traffic from an outside end host to reach machines inside the local domain only if the communication was initiated by the internal machines. We implement a SDN-based stateful firewall, which can set up filtering policies under the instruction of the controller. The controller registers traffic traversal information and installs appropriate filtering entries.

**Verification results** We verify a number of properties about the stateful firewall. We discuss one property here (shown below).

$$\varphi_{WeakFW} =$$

$$\forall Host, Port, Src, SrcPort, Switch,$$

$$pktReceived(Host, Port, Src, SrcPort, Switch)$$

$$\exists Cntrl, trustedControllerMemory(@Cntrl, Switch, Src)$$

The above property specifies that source destinations of all packets reaching internal machines are trusted by the controller. Surprisingly, our tool gives a counterexample for this property (Figure 8), which depicts the scenario that an internal machine H3 sends a packet to another internal machine H4 in the same domain through the firewall F1. Because the controller C1 never registers local machines, the property is violated.

In spite of its simplicity, we find the counterexample interesting, because it can be interpreted in different ways; each corresponds to a different approach to fixing the problem. The counterexample can be viewed as a revelation of a program bug. The programmer can add a patch to the program and re-verify the property over the updated program. Alternatively, the counterexample could be linked to incomplete specification of network constraints that internal machines should never send internal traffic to the firewall. The fix would then be to insert extra constraints over base tuples of the program. In addition, the problem could also stem from the property specification, since users may only care about traffic from outside the domain. In this case, we can change the property specification, to specify that if a packet is from an external machine, then the source address must be registered at the controller before.

In real deployment, it is up to the programmer to decide which interpretation is most appropriate.

### 5.4 Load Balancing

The third case study is load balancing. When receiving packets to a specific network service (e.g., web page requests), a typical load balancer splits the packets on different network paths to balance traffic load. There are a number of strategies for load balancing, e.g., static configuration or congestion-based adjustment. In our case study, we implement a load balancer which load balances traffic towards a specific destination address, and determines the path of a packet based on the hash value of its source address.

**Verification result** The property that we verify for load balancing is called flow affinity, that is, if two servers receives packets requesting the same service—which means the packets share the same initial destination address—the source addresses of the packets must be different.

The property does not hold in the given protocol specification, and a counterexample is given by our tool. In the counterexample, two load balancers responsible for different network service could
co-exist in the network, and if a server sends packets to both load-balancers, requesting the same service, it is possible that the packets are routed to different servers.

Similar to the case of the firewall, the programmer can fix the counter example of the load balancer by patching the program, adding network assumption (e.g., assuming no server is connected to two load-balancers), or changing property specification (e.g., "load-balanced packets that are forwarded out of different ports of the load balancer do not share the same source address").

5.5 Ethernet Address Resolution

The final case study we focus on is the Address Resolution Protocol (ARP) in an Ethernet network. End hosts use ARP to request the destination MAC address corresponding to an IP address that they want to communicate to. Traditionally, the ARP requests are broadcast through the domain. In our case study, we replace the broadcast with a centralized controller that answers ARP requests.

Verification results We verify a number of safety properties on ARP, and all these properties prove to be true. The detailed results can be found in Table 3.

5.6 Discussion

We discuss our experience of using the tool and insights obtained from the case studies.

Cause of property violation The counter examples we discuss above reveal a common pattern: when a predicate in the program has multiple derivations, proving properties over the predicate becomes harder. The situation is even worse when a property involves multiple predicates, each with multiple derivations. The increased complexity of predicate derivations makes it error-prone for human programmers to write correct programs or specify correct properties, and serves as the core cause of property violation. Naturally, the fixes we proposed for counter examples generally fall into two categories: (1) enriching the property specification to include the missing derivations, or (2) changing the program to remove the uncovered derivations.

Iterative application development Another observation is that reasonable network assumptions (e.g., topological constraints) helps prune scenarios that would not appear in actual executions, and generate insightful counter examples. For example, a counter example may suggest a topology where a switch has a link to itself. A programmer may start with trivial network assumptions and let the tool guide the exploration of corner cases and gradually add (implicit) network assumptions that are not obvious to the programmer. In fact, our tool enables the programmer to iteratively develop applications. The generated counter examples could help the programmer understand (1) applicable domain of the program (feedback of missing network constraints); (2) implementation correctness (feedback of bugs in the program); and/or (3) expected behavior of the program (feedback of incorrect property specification). After the programmer fix the problem, she or he can redo the verification repeatedly until the specified property holds.

6. Related Work

Network verification. In recent years, formal verification has received much attention in the network community. There has been a cloud of prior work on network verification focusing on several different aspects. One aspect is the verification of network configurations, where the proposed solutions detect network configuration errors either 1) through static analysis of the configuration file [2, 17, 18, 37, 49], or 2) by analyzing snapshots of the data plane—reflecting the aggregate impact of all configurations—during system execution [22, 23, 33, 51]. These solutions rely heavily on application-specific network models and property specifications, which limits its adoption in more general scenarios. The second aspect is to leverage proof-based and model-checking techniques to verify the correctness of both the design and implementation of network protocols [16, 19, 25, 47, 48]. Such solutions often demand participation of system administrators during the verification phase, and require domain-specific expertise. The third aspect focuses on security properties, such as origin and route authenticity.
properties, in secure networking protocols that use cryptographic primitives [5, 6, 10, 14, 52].

Most closely related to ours is the work on verifying network protocol design using declarative networking [10, 47, 48]. The general approach of the prior work share similarities with the one of ours—both model the network behavior using trace semantics, and properties are specified and verified on the trace-based model. However, the proposed solution in this paper enables automated static analysis of safety properties and generates counterexamples for debugging purposes, whereas the prior work relies on manual proofs and therefore can handle a richer set of properties.

**SDN verification.** One special case of network verification is SDN verification [1, 8, 9, 21, 24, 41, 46]. For example, VeriCon [8] defines its own special language for modeling SDN controller and switches [8]. A hoare-logic is developed on this language to prove properties of SDN controllers. The proof obligations are translated to constraints and solved by the SMT solver. NICE is a testing tool for SDN controllers written in Python [9]. NICE combines symbolic execution of the controller programs with state-exploration-based model checking. An alternative approach is to verify network configurations generated by SDN controllers in realtime, instead of verifying the protocol directly [24, 33]. For instance, Anteater reduced SDN data plane verification into SAT problems so that SAT solvers can solve them effectively in practice [33]. NetKAT is a high-level language designed specifically for programming SDN. Its semantics are based on Kleene algebra. The correctness properties of networks programming using NetKAT are tightly connected to the semantics of Kleene algebra, for instance, reachability, way points and traffic separation.

All of these tools are specially designed to analyze SDN controllers or data planes. Modeling and verifying SDN controllers is one example application of our analysis; our analysis can be applied to analyzing other distributed systems expressible in NDLog. On the other hand, in the current state, we can only check simple safety properties, while VeriCon, NICE, and NetKAT can handle more expressive properties.

**Verification of declarative programs.** Declarative languages have been proposed to model systems in a variety of domains such as networks, mobile agent programming, and algorithms for graph structures (e.g., Network Datalog (NDLog) [30], MELD [7], Linear Meld [15], Netlog [20], DAHL [32], Dedalus [3]). However, there has been few work on analyzing low-level correctness properties of declarative programs. Notably, Wang et al. [47, 48] developed a proof system for proving correctness properties of networking protocols specified in NDlog, where programs are translated into equivalent first-order logic axioms, that is, all the body tuples are derivable if and only if the head tuple is derivable.

### Table 3. Results of checking safety properties of $\text{prog}_{ARP}$ on our tool

<table>
<thead>
<tr>
<th>Property</th>
<th>Property description</th>
<th>Formal Specification</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\varphi_{\text{ARP}}_1$</td>
<td>If any controller sends an ARP response for IP address $IP_A$, then some end host had sent a broadcast ARP request message for $IP_A$.</td>
<td>$\forall \text{Controller}, IP_A, \text{Mac}_A, \text{DstIP}, \text{DstMac}, \text{arpReply}(\text{Controller}, IP_A, \text{Mac}_A, \text{DstIP}, \text{DstMac}) \supset \exists \text{Qmac}, \text{arpRequest}(\text{Host}, \text{SrcIP}, \text{Qmac}, \text{DstIP}, \text{DstMac}, IP_A, Qmac) \land Qmac = 255$</td>
<td>true</td>
</tr>
<tr>
<td>$\varphi_{\text{ARP}}_2$</td>
<td>If any controller has a map between IP address $IP_A$ and MAC address $\text{Mac}_A$, then host $A$ has sent a broadcast ARP request.</td>
<td>$\forall \text{Controller}, IP_A, \text{Mac}_A, \text{arpMapping}(\text{Controller}, IP_A, \text{Mac}_A) \supset \exists \text{Host}, \text{SrcIP}, \text{SrcMac}, \text{DstIP}, \text{DstMac}, \text{arpReply}(\text{Host}, IP_A, \text{Mac}_A, \text{DstIP}, \text{DstMac}) \land \text{DstMac} = 255$</td>
<td>true</td>
</tr>
</tbody>
</table>

### 7. Conclusion

We presented an automated approach to analyzing and debugging network protocols using declarative networking. By focusing on a specific class of safety properties, we are able to analyze NDLog programs with few annotations. Our algorithm reduces property checking to constraint solving that can be automatically checked by the SMT solver Z3. We analyzed formal properties of our algorithms and implemented a prototype tool on top of RapidNet, a compilation and execution framework for NDLog. Using our tool, we analyzed a number of real-world SDN network protocols. Our tool can unveil problems ranging from software bugs, incomplete topological constraints, and incorrect property specification. When a given safety property is violated, our tool can provide meaningful counterexamples to help debug the protocol specification.

### 8. Acknowledgment

We thank the anonymous reviewers for their invaluable comments. This work is supported in part by NSF CNS-1218066, CNS-1117052, CNS-1115706, CNS-0845552, CNS-1453392 and AFOSR Young Investigator Award FA9550-12-1-0327.

### References
