Applying Formal Methods to Networking: Theory, Techniques, and Applications

Junaid Qadir and Osman Hasan

***Abstract*—Despite its great importance, modern network infrastructure is remarkable for the lack of rigor in its engineering. The Internet, which began as a research experiment, was never designed to handle the users and applications it hosts today. The lack of formalization of the Internet architecture meant limited abstractions and modularity, particularly for the control and management planes, thus requiring for every new need a new protocol built from scratch. This led to an unwieldy ossified Internet architecture resistant to any attempts at formal verification and to an Internet culture where expediency and pragmatism are favored over formal correctness. Fortunately, recent work in the space of clean slate Internet design—in particular, the software defined networking (SDN) paradigm—offers the Internet community another chance to develop the right kind of architecture and abstractions. This has also led to a great resurgence in interest of applying formal methods to specification, verification, and synthesis of networking protocols and applications. In this paper, we present a self-contained tutorial of the formidable amount of work that has been done in formal methods and present a survey of its applications to networking.**

***Index Terms*—Computer networks, formal specifications, formal verification.**

I. Introduction

THE networking industry in a way is a victim of its own popularity. Internet, which began as a research experiment in the late 1960s, became popular before many aspects of Internet's design could be formally contemplated and designed [1]. The overwhelming success of the Internet led to the need of rapid innovations in applications and protocols. This has helped develop a culture that values engineering judgment, heuristics, and running code[1] more than it values sound engineering and rigorous verification. Unfortunately, the expedient rapid innovations resulting from this approach has resulted in a hit-and-trial hacking based software development culture. In contrast to well-honed verification and testing tools available for other fields such as ASIC hardware design, large-scale software systems, the networking industry has a very primitive testing tool-chain. The lack of rigor in networking industry, on the other hand, can be observed by the fact that simulation based testing—which is inherently a trial-and-error process—is routinely used to "establish" the correctness of networking protocols, software, and hardware. With exponential number of possibilities, exhaustive testing is almost always impossible and thus subtle bugs remain unchecked and undetected until they manifest themselves at invariably inopportune times where the consequences of bugs in the wild can be drastic [2], [3]. Such a lack of rigor is unacceptable in other mature engineering or manufacturing fields, and the networking community is increasingly realizing the need for better tools and techniques for verification and testing.

Formal methods allow us to not only verify the properties of protocols and systems, but also will help us deepen our conceptual understanding of large classes of protocols. With the emergence of large-scale computer systems such as data centers, and the emergence of cloud computing paradigm using which consumers can access resources on a pay-per-usage basis, computing is increasingly being democratized. However, the cost of failure of such large-scale computing systems is huge which motivates the use of formal methods to provide an increased level of system reliability and correctness [4].

There are many prominent examples of huge losses accruing from failing systems, protocols, and services [4]. For example, a recently published white paper by Rapid7 [5] identifies some vulnerabilities in the commonly used Universal Plug and Play (UPnP) protocol, i.e., a communication protocol for routers, smart TVs, network-attached storage etc. According to the report [5], these issues can endanger about 50 million network-enabled devices that are using UPnP. Similarly, due to the incorrect operation of a network card, over 15 000 flights were grounded at the Los Angeles International Airport in 2007 and no one was allowed to enter or leave the US via this airport for about 8 hours [6]. At times such undetected bugs in the design phase can also compromise the privacy of the Internet users. For example, various vulnerabilities have been identified in the programs running in the web servers of the social media giant Facebook; a recent one [7] involves a program that the company has been running since 2011 and allows someone to access arbitrary files on the company's web server. Facebook paid a bug bounty of $33 500 to the engineer reporting this case [7]. In addition to vulnerabilities in software and protocols, a large share of failing network services is due to operator errors (which includes configuration errors) [8].

Manuscript received November 18, 2013; revised March 7, 2014 and June 4, 2014; accepted August 2, 2014. Date of publication August 7, 2014; date of current version March 13, 2015.

The authors are with School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Islamabad 44000, Pakistan (e-mail: junaid.qadir@seecs.edu.pk; osman.hasan@seecs.edu.pk).

Digital Object Identifier 10.1109/COMST.2014.2345792

[1]The ethos of the Internet research is reflected in the famous quote of David Clark: "We reject: kings, presidents and voting. We believe in: rough consensus and running code."

A standard technique to manage complexity in computer systems is to utilize abstractions and modularity. Apart from the lack of a developed verification tool-chain, the Internet also suffers from a paucity of useful abstractions, especially for the control plane, which has led to accumulation of a "big bag of protocols" [9]. This is in contrast with other fields of computer science: e.g., the software industry has matured to incorporate a hierarchy of abstractions designed to simplify the task of programming while ensuring correctness—e.g., in software development, the high-level end-to-end requirements are separated from the low-level machine code by various abstractions such as algorithms, programming languages, compilers, tracers and debuggers, static analysis tools, etc. The lack of abstractions has resulted in an unwieldy complex Internet architecture, with under-developed underlying principles and theoretical foundations, that is totally ill-suited to the kind of dependence that is expected of the modern Internet.

Formal methods—computer techniques based on mathematical logic—are poised to play a central role in future networking as the research community increasingly converges towards a firm realization that traditional informal methods are grossly inadequate for *specification*, *analysis*, and *validation* of networking protocols [10]. Formal methods have been extensively applied to the *verification* of hardware design [11], communication protocols [12], [13] (e.g., routing protocols [14]), secure software systems [15], engineering systems [16], programming languages [17], network simulations [18], large software programs [19], etc. Likewise, formal methods have also been used in the networking domain with promising results. For example, the lightweight formal modeling and verification tool, Alloy, has been successfully used to discover some major issues with the widely used Chord protocol [20]. These issues could not be identified with over a decade of research on the Chord protocol using the traditional analysis methods. Similarly, the network simulator J-Sim, extended with the bounded model checking capability, was able to detect an unknown bug in an earlier J-Sim implementation of the Ad-Hoc On-Demand Distance Vector (AODV) protocol [21]. Another notable example of detecting errors in widely used telecommunication systems using formal methods include the usage of the higher-order-logic theorem prover Coq for identifying several bugs in the implementation of the open source Netgear WNR3500L wireless router firmware [22].

Despite the above-mentioned results, there has been an impression in the networking community that formal methods do not return benefits commensurate with the effort to use them. Vint Cerf has written that "Formal methods have not yielded results commensurate with the effort to use them. They are overblown, verbose, hard to use, hard to understand." [23]. This criticism has unfortunately resulted from the lack of appreciation of advances in formal verification and sometimes due to poor communication between the formal verification community and the networking community. It is imperative in today's world, and it will become increasingly important in the future, to move away from manual error-prone methods of testing and verification and automate as much of the testing and verification tasks as we can [24]. Formal methods are still useful even if they do not meet the utopian "gold standards" of complete automation and complete generality of mathematical proofs—in particular, interactive theorem proving, abstracted models, and light-weight methods are highly suited to certain niche applications [10]. Advances in modern technology has fortunately facilitated development of many automatic and semi-automatic tools that can be conveniently used by practitioners with limited specialized background knowledge of formal methods.

With the increasingly central role networks play in all aspects of our lives (business, personal, entertainment, etc.), the correct functioning of networking protocols and systems has never been more important. In recent times, there has been significant interest in the application of formal methods to networking [25], not only due to the importance of this subject, but also due to the possibilities created by recent architectural developments in the networking community. In particular, the software defined networking (SDN) architecture, which proposes splitting of the control/data planes and the management of multiple data planes through a centralized controller to allow programming the network in a software-like fashion, makes networking accessible via formal methods. This has accentuated the networking community's interest in applying formal methods to networking [26]. With the use of formal methods in networking, the field of network verification looks set to evolve from the current set of ad-hoc verification tools and emerge as an engineering discipline.

Contributions of this work: In this paper, we provide a self-contained tutorial covering the vast amount of work that has been done in the area of formal methods with a special focus on their applications in the domain of networking. Due to the great breadth of the subject, and vast amount of works in associated fields, we cannot hope to be comprehensive in every respect—nonetheless, we provide an extensive, self-contained, description of application of formal methods to networking with an adequate background on logic, programming languages, automatic verification, etc. This work is different from existing surveys [27]–[30] in its exclusive focus on application of formal methods to networking and incorporation of new trends that have emerged with recent network architectural developments (such as the development of the SDN networking architecture). The emergence of SDN, and other recent innovations, have spurred a surge of interest in the application of formal methods to networking [31]. Our paper is timely since, despite the recent focus and interest in our subject area, there does not exist a unified survey paper that a networking researcher can use to develop a high-level broad understanding of formal methods and techniques and learn about their applications in the context of networking. This paper attempts to fill this void, and will be valuable to networking researchers who wish to exploit the large amount of work done in the formal methods community to build reliable future networks whose correctness is formally verifiable.

The remainder of this paper is organized as follows. Sections II–IV serve to provide the necessary background to various topics in formal methods and verification make this paper self-contained. The necessary background on logic is provided in Section II. Different techniques for specification and modeling, such as finite-state-machines, Kripke structures,

binary decision diagrams, etc., are described in Section III. Different techniques for formal verification, such as model checking, theorem proving, static analysis, etc., are described in Section IV. After discussing the necessary background, the stage is set for the three main sections of this paper (Sections V–VII) in which we describe the various application of formal methods in the context of networking in detail. In the section *formal verification techniques in networking* (Section V), we present a formal verification technique based categorization of applications of formal methods in networking; we also present a discussion on the suitability of various techniques for different verification tasks in networking as well as a discussion on common pitfalls. We provide a broad-ranging overview of application domains of formal methods in networking in *application domains of formal methods in networking* (Section VI). We then focus on developments in SDN and detail how formal methods, logic, and programming languages can be used in such networks in section *applications of formal methods in SDN* (Section VII). Various open issues and future works are then identified in Section VIII. Finally, this paper is concluded in Section IX.

II. Logic—The Foundation of Formal Methods

Logic is the branch of knowledge that focuses on systemizing truth, reasoning, and inference. Studied by generations of philosophers (Socrates, Plato, Aristotle, Kant, etc.), logic has a rich ancient tradition in philosophy [32]. Logic was developed in ancient Greece as a device for systematizing *deduction* through which true statements, or *conclusions*, could be derived from *premises*—statements that are *assumed* to be correct. Although, utilized in mathematics at least since Euclid (2300 BC), the incorporation of logic into a mathematical framework has occurred mostly in the last two centuries [33] through the efforts of Frege, Peano, and Russell to axiomatize mathematics. In the field of computer science, logic has been referred to as "the calculus of computer science"[2] [34] to highlight its pivotal, and indeed "unusually effective" [35], role in the fields of formal methods [36], artificial intelligence [37], and theoretical computer science [38]. Formal methods, which utilize logic for modeling and reasoning about computer systems, have been extensively for formal verification of computer systems (both hardware and software) [36].

What is logicism? As per Aristotle's definition, logic is new and necessary reasoning—*new* since we learn what we did not know, and *necessary* because the conclusions are inescapable. Leibniz dreamed of such a mechanical system of reasoning which he called *calculus ratiocitinator* to calculate new and necessary conclusions from facts described in a logical symbolic language, which Leibniz called *characteristica universalis*. Frege devised a set-based logical language for developing Mathematics on a solid footing. Frege (1848–1925) conceived of an ambitious project, called *logicism*, which aimed at deducing mathematics (more specifically, set theory, number theory, and analysis) from laws of logic [39]. This project after Frege was taken up most notably by Russell, along with Whitehead, who embarked on an ambitious project to put mathematics on firm foundations. The use of symbolic notation, an integral component of Russell's attempt to formalize mathematics, allowed rapid progress and allowed emphasis on the structure and the form of reasoning.

The "failure" of logicism: It was discovered by Russell that a logical language based on naive set theory—which defined sets to be a collection of objects and allowed sets to contain sets (including possibly itself) as elements—could not be used as the foundation of all mathematics because it suffered from paradoxes. Russell showed the following simple example, known as Russell's paradox, to illustrate this: does the set S of all sets that do not contain itself contain the set S itself? This riddle exposed that naive set theory is not sufficient to act as a foundation of mathematics leading to axiomatized set theory and various typed set theory to deal with the self-referential that created the Russell's paradox. In mathematics, the standard form of axiomatic set theory is the Zermelo–Franenkel set theory with the axiom of choice (ZFC) which acts as the most common foundation of mathematics. Eventually, Fregian logic also had to be restricted—into what is now known as first-order logic—to deal with Russell's paradox, and this restricted logic was incorporated by ZF set theory. In 1931, Godel dealt a deathly blow to logicism when he proved that any axiomatic system capable of expressing the laws of arithmetic is *incomplete*—i.e., there will always be some truth of arithmetic that cannot be proved using the axioms of the system. While logicism "failed" in its aim of deducing arithmetic from the axioms of logic, it was instrumental in establishing the limits of computation and of "formal reasoning." It helped identify the limits of computation and of axiomatized logic systems.

Components of logical reasoning: In modern terms, every logic-based language is defined in terms of three components: syntax, semantics, and proof theory. The *syntax* of a language specifies all the components that can be part of a well-formed formulae. The purpose of standardizing a syntax is to aid in understanding, communicating, and reasoning. The *semantics* of a language, informally speaking, deals with the "meaning" of the formulae, or sentence, formatted according to the language's syntax. In logic, the semantics of a language specifies the truth of a formulae with respect to each possible world [37]. As an example, $x + y = 2$ is true when x and y are both equal to 1 but false in a world where x and y are both equal to 2. More formally, the term "model"—which is used in the name of a technique known as "model checking" that we shall see later in Section IV-C—is used in logic in place of "possible world." The meaning of a statement $\mathcal{M}$ is a model of α (commonly depicted as $\mathcal{M} \models \alpha$, and read as $\mathcal{M}$ models α) is that the formulae α is true in situation represented by model $\mathcal{M}$. The concept of *logical entailment* is similar: we can denote in notation $\alpha \models \beta$, i.e., the formulae α entails the formulae β if and only if every model in which α is true, β is true as well. In other words, logical entailment $\alpha \models \beta$ implies that if α is true, β must also be true. Lastly, *proof theory* is concerned with manipulating formulae according to certain rules.

In the remainder of this section, we will provide *background* information about some important logics relevant to the overall

[2]In a metaphorical reference to the central place calculus occupies in natural sciences.

TABLE I
TRUTH-TABLE OF TRUTH-FUNCTIONAL CONNECTIVES

α	β	$\alpha \wedge \beta$	$\alpha \vee \beta$	$\alpha \rightarrow \beta$	$\alpha \leftrightarrow \beta$	$\neg\alpha$	$\neg\beta$
T	T	T	T	T	T	F	F
T	F	F	T	F	F	F	T
F	T	F	T	T	F	T	F
F	F	F	F	T	T	T	T

problem of formal specification and verification of computer networks. A discussion of the *applications* of various logics in the context of networking is presented later in Section VII-B.

A. Propositional Logic

Propositional logic, also called propositional calculus or sentential logic, was developed into a formal logic by Chrysippus and developed further by the Stoics and eventually by Leibniz.[3] Propositional logic differs from syllogistic logic, proposed by Aristotle, in that it focuses on propositions which are declarative sentences that can only take values of *True* or *False*. Since the propositions are akin to Boolean variables, propositional logic is also known as Boolean logic [37]. Propositional logic is important for two main reasons. Firstly, it is fundamentally important for computer systems since it is the theory behind digital circuits. Moreover, most of the advanced logics (such as first-order logic, also called predicate logic, which is covered in Section II-B) build upon propositional logic.

In propositional logic, new propositions are generated from old through *truth-functional connectives* [40], which define the formal grammar of propositional logic, such as the *not* operator ($\neg$), the *and* operator ($\wedge$), the *or* operator ($\vee$), the *if, or implies, or the conditional* operator ($\rightarrow$), and the *iff, or equivalence, or the biconditional* operator ($\leftrightarrow$). Although, the Boolean propositional operators have intuitive analogues in natural language, they are defined formally. Sometimes, the mathematical terminology has a direct analogue with our intuition: e.g., the Boolean operator *and* is an operator that is defined to give a *true* value if and only if applied to two expressions whose values are true [33]. At other times, the mathematical terminology may extend our intuitive interpretation: e.g., mathematical usage of the implication logical connective extends the intuitive concept of implication by divorcing the concept of causality from implication [41]. Similarly, the Boolean operator *or*, when applied to two expressions, has the intuitive analogue of *inclusive or*, i.e., any one or both expressions are true. It is important to stress that these operators are formally defined through a truth table, and these operators may not exactly match our everyday understanding of these words. The truth tables of the logical connectives used in propositional logic can be seen in Table I.

Propositional logic formulae: The formulae of a formal language built on propositional logic are expressions that can be recursively built from propositional variables by using connectives. There are four important concepts that apply to formulae. Two of these concepts are important *properties* of a formulae: *i*) being a tautology, *ii*) being a contradiction, while the remaining two concepts refer to *relations* between formulae: *iii*) tautological implication, and *iv*) tautological equivalence.

There are two fundamental concepts that deal with formulae of all logics: *i) satisfiability*—is this formula *ever* true? and *ii) validity*—is this formula always true? It may be noted that the satisfiability problem is very general, indeed various computer science problems can be reduced to a satisfiability formulation. Determining the satisfiability of sentences in propositional logic was the first problem that was proved to be NP-complete [37]. Similarly, determining the validity of logic formulae is an extremely important problem. Another important problem that deals with propositional logic is the propositional tautology or equivalence checking.

B. Predicate Logic

Developed initially by Frege and Peirce, predicate logic [36], [40] enhances propositional logic—which only allows propositional symbols and operators—with *i*) propositional symbols, *ii*) predicates, *iii*) functions and constant symbols, *iv*) quantifiers (universal quantifier, $\forall$, meaning "for all," and an existential quantifier, $\exists$ meaning "for some"), *v*) equality, and, *vi*) variables [37]. The prime motivation behind developing predicate logic is that the truth-functional connectives of propositional logic (such as *not, and, or, if, iff*, etc.) alone are not rich enough to capture the much richer logical structure of natural language which often uses quantifiers, or modifiers, such as "there exists," "all," "some," "among," "only," etc.

It is worth emphasizing the difference between a proposition and a predicate. A proposition is a statement that is either true or false—for example, IPv4 addresses are 32 bits long is a *true* statement. A predicate, on the other hand, is used to capture relation(s) or dependence on some input parameter(s)—a predicate evaluates to true or false depending on some input parameters. In the case of a *unary predicate*—e.g., x is a philosopher—the truth of the statement depends on the a solitary input variable. For *binary predicates*, however, the truth of a statement depends on two input variables—e.g., $x > y$, depends on the values of both x and y. In general, predicate logic may have n-ary relations between objects [37]. Predicate logic is extremely important, especially for our subject topic of formal verification of communication systems, as it can be used to formalize the semantics of programming languages, and to specify and verify programs.

C. First-Order Logic

Predicate logic can be categorized into various orders depending on how the quantifiers are used in predicate logic. In first-order logic, it is assumed that the world contains objects (such as switches, routers, users, etc.), relations (faster than, happens after, etc.), functions (one more than, next hop of, etc.), and quantifiers through which facts can be expressed about some or all the objects in the universe [37]. In first-order logic, quantifiers can range over individuals, whereas in higher-order logic, the quantifiers can also range over sets, or relations. Higher-order logic can also be defined, with ω-order logic being essentially the simple theory of types. While

[3]Leibniz is also credited for being the developer of symbolic logic, along with his more famous contributions towards development of calculus.

predicate logic subsumes first-order logic, second-order logic, or infinitary logic, etc., the unqualified use of predicate logic typically refers to first-order logic.

First-order logic was delineated by Hilbert, and then Skolem who proposed building set-theory on the basis of first-order logic. First-order logic, like propositional logic, is a complete system [39] (first proved by Godel in his completeness theorem). There are various useful verification tools that are based on first-order logic including the Alloy analyzer (which we will discuss later in Section IV-D).

In 1928, David Hilbert proposed the *Entscheidungsproblem*, German for the "decision problem" [42], which asked for an algorithm which will take a statement of a first-order logic as input, and answer if the statement is universally valid—i.e., valid in every structure satisfying the axioms—with a "yes" or a "no." Hilbert's intent was to find a system for completely axiomatizing, and formalizing, all mathematical knowledge and proofs. In 1936, Alonzo Church and Alan Turing independently showed that a general solution to the Entscheidungsproblem is impossible—thus, no mechanical, or algorithmic, method can prove the validity of arbitrary predicate logic statements. The Church-Turing result for the Entscheidungsproblem also has significant implications for the use of *automatic theorem proving methods for software systems*. In particular, we cannot write a program (written in any common language such as Java, C, etc.) which will be able to always answer the decision question: Is a given logical formula ϕ in predicate logic true for all its valuations, i.e., does $\models \phi$ hold, yes or no?

The unfortunate implication of this is that no automatic deductive verification tool can exist that will work with any arbitrary predicate logic formula instance as an input and always terminate while producing a correct "yes"—corresponding to a valid input formula—or a "no" answer corresponding to an invalid input formula [36]. This poses a fundamental, and insurmountable, problem to the automatic theorem proving approach of verification, also known as automatic deductive verification. Therefore, first-order logic, unlike propositional logic is only a semi-decidable theory—i.e., there exists an effective method for telling if any arbitrary given formula is in the theory, but it may give either a negative answer or no answer at all when the formula is not in the theory.

D. Higher-Order Logic

A *higher-order logic* (HOL) is more expressive than first-order logic as it allows a more general usage of quantifiers along with stronger semantics. Unlike first-order logic in which variables cannot denote predicates, variables in second-order logic can denote predicates allowing the logic to talk about itself more easily. There can be higher-orders beyond second-order logic. The main strength of HOL is that it is highly expressive, and can express any mathematical theory, like multi-variable calculus [43] and probability [44], in its true form. The higher expressiveness associated with higher-order logic, however, is tempered with the downside that model-theoretic properties of higher-order logic are less well-behaved than those of first-order logic. In particular, validity in higher-order logic is not even semi-decidable (or anywhere in the arithmetical hierarchy).

E. Hoare Logic

Hoare logic (also known as *Floyd–Hoare logic* or *program logic*) is a formalism that defines logical rules—i.e., axioms and inference rules—to provide an axiomatic basis for verifying computer programming [45]. The central construct used in Hoare logic is the partial correctness specification in the form of a *Hoare triple*:[4] $\{P\}C\{Q\}$ where P is the pre-condition, Q is the post-condition, and C is the command. Hoare logic builds upon other conventional logic, e.g., first-order logic, for specifying the pre- and post-conditions.

Hoare Logic is a deductive proof system for Hoare triples $\{P\}C\{Q\}$. The partial correctness specification $\{P\}C\{Q\}$ means that whenever C is executed in a state satisfying P, and if the execution of C terminates, then the terminating state after C's will satisfy Q. Hoare logic deals with verification of partial correctness of a command, and termination of a program has to be separately proved to show total correctness. The generality of Hoare's approach is based on its characterization of programming constructs as transformations of states which can universally apply to any imperative programming language construct. The underlying semantics of a program can be viewed a set of transformations from an initial state to a final state. Since a sequential program can also be envisioned as a transformational system, Hoare logic is particularly suited to analysis and verification of sequential computer programs. Hoare logic is a sound system (every provable formula is true) but not a complete system (i.e., not all true statements are provable). More details about Hoare logic can be found in [46].

Hoare logic, and the use of Hoare-style pre-conditions and post-conditions, is commonly used in many settings. As an example, the Java Modeling Language (JML) defines a specification language for Java programs, following the design by contract paradigm, which uses Hoare style pre-conditions and post-conditions and invariants for extended static checking. The same style is inherited by ESC/Java.

F. Modal Logic

Modal logic is an expressive form of logic that uses additional quantifiers. Modal logic was originally developed by philosophers to study different "modes of truth"—e.g., an assertion P may be false in the present world, however, the assertion "possibly P" will be true if the assertion P is true in some alternate world [47]. Temporal logics essentially have two kinds of operators: logical operators (loaned from traditional the logic framework in which temporal logic is used) and modal operators. The modal operators capture in modal logic the intuitive notions of *necessarily, always, possibly, sometimes*, etc. The symbols N, F, G, A, E represent ***N**ext*, ***F**uture*, ***G**lobally*, ***A**ll*, and ***E**xists*, respectively. In typical notational terms, the box symbol is used to represent *necessity*, while the diamond symbol is used to represent *possibility*. For example, Gp would mean always p; Fp will mean sometimes p; $\diamond p$ means possibly p; $\Box p$ means necessarily p.

[4]The Hoare triple is also known as partial correctness assertion or PCA and is partially based on Floyd's intermediate assertion method.

Modal claims can be understood semantically in a theory of "possible worlds"—an idea commonly attributed to Leibniz which was advanced by Saul Kripke in the late 1950s. Kripke advanced Leibniz's conception of the actual world being one "possible world" amongst other, by proposed a mathematical theory of models (now known as Kripke models) for possible worlds. A statement is "possible" in modal logic if it is true in at least one possible world; a statement is "necessary" if it is true in all possible worlds. We will see later that "model checking" (covered in Section IV-C) depends fundamentally on the concept of possible worlds and utilizes Kripke models.

G. Temporal Logic

The use of temporal logic, a special type of modal logic, for formal specification and verification of computer systems was proposed by Amir Pnueli in a highly influential paper [48] in 1977. In this paper, Pnueli argued that temporal logic—a formalism for dealing with how truth values of assertions change over time—is especially appropriate for describing reactive systems such as operating systems and network communication protocols. In a reactive system, which contrast with sequential terminating programs that essentially transform the input to the output and then terminate, the normal behavior is to engage in a nonterminating computation that continuously interacts with the environment. Examples of reactive systems include operating systems and network communication protocols. Temporal logic is especially invaluable in the field of model checking finite-state *concurrent* programs [49]: Leslie Lamport, in his highly cited paper "what good is temporal logic?," has highlighted that the main utility of temporal logic is in modeling concurrent systems [50].

Temporal logic formulae differ from ordinary Boolean formula in that the temporal formulae have new modal operators—which allow qualitative description of temporal events by implicitly incorporating temporal ordering of events—in addition to the traditional Boolean operators—"and," "or," "not," and "implies" [51], [52]. The usage of temporal logic has been widely adopted for use with finite-state programs with algorithmic methods available that can verify the temporal-logic properties of finite-state systems. While the capacity to only include finite states may appear too limiting, it turns out that a wide range of systems, especially, hardware systems and communication protocols, can be modeled as finite-state programs. Some (linear) temporal logic operators include G (*Globally*), F (*Eventually, Finally*), X (*Next*), and U (*Until*). For example, we may want to reason about the temporal properties of a protocol in the following way: a message is not received unless one is sent, a message that is sent is eventually received, etc.

Temporal logic has been extensively applied to computer systems, and is a key component of the popular model checking approach (discussed in Section IV-C), because it can capture two keys notions of computer performance. Firstly, temporal logic can capture the "*liveness*" property that some good thing will happen in the future—i.e., the form Fp, which indicates that some proposition will be true in the *future* in the course of the computation. Secondly, the "*safety*" property of the form Gp can capture the desire that globally p is ensured which incorporates the proposition that undesirable states are never obtained. In addition, the "*fairness*" property is also defined which states given certain conditions, an event will occur, or will fail to occur, infinitely often. The fairness property is often expressed with Gp (infinitely often) and Fp (eventually always).

There are two important subtypes of temporal logic: linear temporal logic (e.g., LTL)—where each moment in time has a unique future trajectory or possible future—and branching temporal logic [53] in which each moment can be split into many different possible futures. *Linear temporal logic (LTL)* is a subset of the more complex CTL that additionally allows branching time and quantifiers. LTL is also sometimes called propositional temporal logic, abbreviated PTL. LTL can use both propositional and first-order forms. *Computation tree logic* (CTL) is an example of branching temporal logic that has additional path quantifiers such as A (for all paths $\forall$) and E (there exists a path) that denote universal and existential quantification over paths starting in a certain state, respectively. CTL is used mostly for applications in hardware verification, while LTL is used mostly for applications in software verification. While CTL and LTL do have overlapping expressiveness, each logic can express properties outside the domain of the other—e.g., LTL can express fairness properties which CTL cannot, but CTL can express the so-called reset property which LTL cannot.

H. Other Logics

Relational Logic: The logic used in the Alloy analyzer [54] is a relational logic that combines the quantifiers of first-order logic with the operators of the relational calculus. Relational logic extends first-order logic by incorporating transitive closure allowing greater expressiveness. Since first-order logic is undecidable, the focus of the Alloy analyzer is in *model finding* rather that exhaustive model checking—in particular, not finding a model does not preclude a model in a larger scope. Most tools for relational notation, other than Alloy analyzer, e.g., PVS etc., focus instead on theorem proving and are thus not fully automated. Kodkod [55] is an example tool that is based on the relational logic of Alloy. The inclusion of "transitive closure" enables expressiveness (beyond that offered by first-order logic) that can be used to encode common reachability constraints. Since the relational logic of Alloy uses multi-arity relations instead of functions over sets, it is first-order and thus amenable to automatic analysis due to its simplicity.

Router Logic: Feamster *et al.* [56] proposed *routing logic* to define a set of rules that can be used to determine if a routing protocol satisfies various properties. Feamster *et al.* also utilized this logic for analyzing the behavior of BGP protocol under various conditions. Importantly, Feamster *et al.* suggested that in addition to analysis of existing configurations, router logic can be used to synthesize network-wide router configurations from a high-level description.

I. Algebra and Logic

An algebra is a structure that consists of sets and operations that act on those sets. Using the tools of algebra, logical statements can incorporate unknowns, symbols, and formulas. Mathematical logic, or symbolic logic, has improved upon the

logic of Aristotle by exploiting symbolic manipulations defined essentially by methods of algebra. This symbolic calculus enables correct reasoning with economy of mental effort[5] and has led to rapid development in mathematical knowledge.

While algebra is mostly associated with axioms of simple numbers, computer protocols and programs, with all their inherent complexity, are also surprisingly amenable to algebraic analysis. Algebra can be applied to large scale concurrent systems evolving in parallel as well as to micro-level manipulation of program code. As such algebra, along with logic, provides an invaluable tool for modeling and verifying distributed protocols and systems. We will very briefly outline some of the more important algebra that are fundamental to verification of computer systems and networks.

Boolean Algebra: The algebra of logic was founded by George Boole (1815 to 1864), and perfected by later logicians, to formalize the "laws of thought." Boolean algebra is essentially the "algebraization" of classical propositional logic and the bridge between logic and algebra.

Relational Algebra: The field of databases extensively utilizes ideas from relational algebra. Relational algebra, an offshoot hybrid of first-order logic and of algebra of sets, essentially deals with manipulations of relations. The formalism of relational algebra, proposed by E.F. Codd in the 1970s, can be used as a query language for relations and serves as a theoretical foundation of databases.

Kleene Algebra: The study of semantics and logics of programs utilizes Kleene algebra which defines algebraic structures with operators $+$, ., $*$, 0, and 1 satisfying certain axioms. Kleene algebras arise in many diverse contexts: relational algebra, semantics and logics of programs, etc. Kleene algebra was extended to incorporate tests to produce *Kleene algebra with tests* (KAT) [57]. KAT has recently been used in the NetKat [58] project to provide consistent reasoning principles about network applications in the setting of SDN.

Process Algebra: Process algebra is a widely used formalism used for specifying and verifying distributed concurrent software systems (including computer protocols). In process algebra, a system is specified in the provides syntax, and the composed system is then verified against the desired properties axiomatically [59]. Finite state automata theory models a process as an automaton which has a number of states and transitions. The automata model lacks in that it does not incorporate the notion of interaction. In parallel and distributed systems (such as computer protocols), which are also called reactive systems, support for concurrency and interaction is required. Process algebra is essentially an algebraic approach to providing support for concurrent interaction between distributed parallel computer systems.

[5]To paraphrase Alfred Whitehead, symbolism facilitates understanding and tracking of transitions in reasoning almost mechanically by the eye without undue taxing of the brain.

III. Techniques for Formal Specification and Modeling

The formal verification of a system mainly requires two inputs from the user, i.e., the given system description and the corresponding properties that need to be verified. All formal verification tools support a specification language that is used to express the system, or its abstracted model, and the properties. The relationship between the formally specified system and its properties is then formally verified using computer-based tools. In this section, we will study techniques for specifying and modeling systems in Section III-A and for specifying properties in Section III-B. We will cover verification methods later in Section IV.

A. Modeling Systems

Systems can be divided into two broad classes. *Transformational systems* may be modeled as black boxes that take certain input and produce a final result as output and terminate. Such systems can modeled in terms of their input/output relations. Formal methods developed for such transformational systems include the Floyd–Hoare logic (Section II-E), which allow reasoning about such systems through pre- and post-conditions, and specification languages like Z (which we will cover in Section III-B). *Reactive systems*, on the other hand, maintain an ongoing interaction with their environment, and thus such systems must be specified and verified in terms of their ongoing behaviors. Formal methods proposed for such reactive systems have to use more sophisticated techniques than those provided by the pre- and post-conditions in notations such as Z. In particular, label transition systems (called Kripke structure) based on the concept of finite state machines (FSMs) and temporal logic have been proposed for modeling reactive systems.

In the following subsections, we will discuss various approaches for modeling systems. We will cover FSMs, Kripke structures, binary decision diagrams (BDDs), and model extraction from code in Section III-A1–A4, respectively.

1) Finite State Machines: The mathematical formalism of finite state machine (FSM), or finite state automaton, is commonly used in the study of the design of computer programs and sequential circuits [76]. An FSM can be conceived as an abstract machine having finite states in which the machine can be in only one state at any given time. The FSM can make a transition—i.e., change its state from the *current state* to another state when triggered by some event or condition. A given FSM is defined by its set of states, and the triggering conditions for each transition. The "state transition model" of FSM has been extensively used in formal verification and serves as the basis of system modeling in "model checking." The state transition model is amenable to mechanical automated verification, but suffers from the "state space explosion" problem, which describes the case when the number states of the system model becomes so large that it becomes infeasible to exhaustively explore the state-space using the available computational resources.

Broadly speaking, there are two kinds of FSMs: *i*) the more general *Mealy machines*, in which the output depends not only on the system state but also on the system input, and

ii) *Moore machines*, which are special cases of Mealy machines, in which the output is determined by only the system state. A FSM is deterministic if the next state and the output are uniquely determined by the current state and input, otherwise, the FSM is non-deterministic if a given state and input can non-deterministically lead to one of many possible next states and outputs. Non-deterministic FSM (NFSM) can be viewed as a generalization of deterministic FSM.

A protocol specification can be translated into a FSM model, with each asynchronous process coded as a separate FSM, extended by message queues and variables if necessary. The system remains finite and amenable to exhaustive search if the queue size and the range of variables is bounded. The system is non-deterministic in general since in each system state a number of transitions may be simultaneously executable. There are two important structural properties of FSMs when used to represent protocols [77]. Firstly, the state space is sparse, i.e., the set of effectively reachable state is much less than the number of potentially reachable states with a ratio of 1 in 10^9 being typical. Secondly, the state space is tightly connected, i.e., the states are usually reachable by mildly different paths that differ only in the order in which the execution of the asynchronous protocol is interleaved. Unfortunately, the FSM verification problem is PSPACE-complete, and therefore is computationally very complex. The problem, however, reduces to be NP-complete if the FSM can be formulated as a combinational logic network.

Automata Theory is a field of theoretical computer science that has been used in the study of computability and languages [78]. Finite automata constitute an important formalism in theoretical computer science. It is useful for modeling a wide variety of systems that have a finite number of states (e.g., communication protocols, for lexical analysis as used in compilers, for scanning text, for expression pattern matching, etc.). An automaton can be envisioned as a special case of Moore machines in which only two outputs—ACCEPT and REJECT—are defined. Variations on the general theme of automata, with varying degrees of expressiveness, have been proposed [76]: e.g., timed-automata [79], Petri nets [80], etc. These formalisms have been adopted in the field of formal verification: e.g., Petri nets have been commonly used for representing concurrent network protocols [81] while timed-automatons have been used for verifying timing properties of network protocols and real-time systems in time-automata based model checking tools (to be discussed later in Section IV-C) such as UPPAAL [82].

2) Kripke Structure: Kripke structure is a labeled state transition graph that can adequately capture the temporal behavior of reactive systems. From a practical point of view, the Kripke structure is nothing but a *labeled* FSM extended to incorporate a labeling function that maps states to sets of atomic propositions making it possible to specify simple propositional properties on the FSM. When used in conjunction with some temporal operators, these propositional properties can be used to specify properties like "from a state labeled *REQ*, the state labeled *ACK* will eventually be reached" [83]. Kripke structure can easily model diverse kinds of systems that are described using formulae of first-order logic.

Kripke structures are often used to model reactive systems that interact with the environment in a continuous fashion without terminating [84]. Since such systems do not terminate, input-output transformation characterization is not sufficient. Instead, it is important to capture the *state* of the system, and how the system state changes as a result of some action. One way of doing this is by identifying the transition of the system—which describes the system state before an action occurs and after it occurs, respectively.

More formally, Kripke structures consist of a set of states, set of transitions between states, and labels for each states defining properties that are true in that state. A Kripke structure $\mathcal{M}$ over AP, representing a set of atomic propositions, is a 4-tuple $\mathcal{M} = (S, S_0, R, L)$ where *i*) S is the *finite* set of states, *ii*) S_0 is the set of initial states, *iii*) R is the transition relation, and *iv*) L is a labeling function that labels every state with the set of atomic propositions that are true in that state.

3) Binary Decision Diagrams (BDDs): The concept of "binary decision diagrams" (BDDs) is quite old but was popularized by Bryant in 1992 [85] as an efficient method for representing state transition systems [86], [87]. It has been pointed out earlier that techniques like model checking suffer from the problem of state explosion which is quite likely to occur if the system under study is composed of components that can perform transitions in parallel. This can cause the system states to grow exponentially leading many experts to be skeptic about the ability of model checking to scale to large systems. Model checking owes most of its success to the development of the data structure of BDDs which allows efficient verification of large transition systems. Computer science luminary Don Knuth cites BDDs as one of the most fundamental data structure development in the last 25 years which allows solutions to problems previously imagined as intractable [87]. The BDD data structure allows concise representation of large transition systems and easy manipulation, and is therefore an important component of many logic synthesis and formal verification systems [87], [88].

Bryant also observed that reduced ordered BDDs (OBDDs) are a canonical representation of Boolean functions. The use of reduction and ordering is common in BDDs, and in fact, the term BDD is commonly understood to refer to reduced ordered BDDs [87]. BDDs are able to reduce the space required for storing state transition systems by identifying redundancies through the following three rules: *i*) merge equivalent leaves, *ii*) merge isomorphic nodes, and lastly *iii*) to eliminate redundant tests.

It was noted in [89] that the rule sets that network administrators typically write lead to small BDDs. BDD is a very popular data structure that can be used, along with efficient graph algorithms for BDDs, to significantly improve the computing time and space efficiency of algorithms [90], [91].

4) Model Extraction From Code: One of the hindrances in the popularization of formal verification is the tediousness of the task of creating system models. A possible solution to this problem for the specific case of *software systems* is to apply verification methods not to models of code, but to implementation code directly through some automated model extraction technique. Some example efforts in this domain include extension

of the SPIN model checker for support of embedded software in abstract models [92], formal verification of device driver code at Microsoft [93] through automatic predicate abstraction of C programs [94], extracting code written in F# to implement the TLS security protocol to process models in applied pi-calculus [95], and CMC tool at Stanford that works directly with C code [96].

B. Formal Specification

Formal specification can be used by the formal verification process to verify that the desired properties are held by the system model. For the purpose of formal verification, *equivalence checking* can be used to match an implementation against a full specification of what a program must do. However, due to the significant overhead involved in writing a full specification, formal verification is often done with partial specification that describes only some desired behavior of the program. This endeavor which contrasts with equivalence checking is known as *property checking*. Most property checking tools use either logical deductive interference or model checking, and report a counterexample when a property violation is seen. It is worth emphasizing that correctness is not an unqualified concept since correctness measures the relation between two entities: a specification and an implementation, or a property and a design [97]. Thus verification is only as good as the specification, making specification an extremely important part of verification.

Broadly speaking, *formal specification techniques* can be categorized into three types based on the underlying formalism. Firstly, in the *mathematical or language-based techniques*, commonly a predicate calculus based approach is taken to represent protocols. Secondly, in the *FSM-based techniques*, an existing programming language may be extended to incorporate the representation of a state machine and associated rules. Techniques like extended FSMs, Petri nets, abstract state machines fall under this category. Lastly, in the *temporal logic techniques*, which are especially useful for reactive systems, in which the protocol is described in terms of statements that implicitly incorporate the relative ordering of events and their actions. IEEE's "property specification language" (PSL) (IEEE 1850 standard) is an example specification language rooted in temporal logic that is commonly used in hardware design where it is a common practice to augment design with assertions serving to specify correct behavior.

IV. Techniques for Formal Verification

In this section, we will provide background information about the various techniques that have been proposed for formal verification. We will first discuss the SAT problem which deals with satisfiability of logic formulae and will see how it has become a very versatile verification technique. In general, formal verification approaches include both automated and interactive techniques. We will discuss theorem proving—a technique that can be automated for decidable logics such as propositional or first-order logic, but which works in concert with a human expert for dealing with the undecidable higher-order logic as a proof-assistant—in Section IV-B. We discuss model checking as an example automated method in Section IV-C. In the later part of this section, we will discuss light-weight formal methods, static analysis, and symbolic execution and simulation in Section IV-D–F, respectively. Finally, we will provide a taxonomy of formal verification techniques in Section IV-G.

We note here that our focus in this section is on providing the necessary background on various formal verification techniques. The *applications in the context of networking* of various formal verification techniques are presented later in Section V-B in a unified fashion.

A. Satisfiability of Logic Formulae: The SAT Problem

A fundamental concept that applies to all logic formulae is the concept of *satisfiability*: is this formula ever true? The Boolean satisfiability (abbreviated as SAT) problem is an important problem in theoretic computer science having a wide-range of applications. The SAT problem can be defined as: Given any arbitrary formula, find a satisfying assignment or prove that no satisfying assignment is possible. Such an assignment may not always exist—in which case, we will say that the problem is over-constrained, and the solver will report that satisfying the formula is not possible. The SAT problem was the first problem shown to be NP-complete,[6] and many practical problems can be reduced to a SAT formulation [98] and solved through off-the-shelf SAT solvers. The SAT problem is at the very heart of the problems of design, specification and verification of computer systems [36] for diverse logics.

A formula is *satisfiable* if it has an interpretation that makes it logically true. Whereas, a logical formula is *valid* if it is logically true in all possible interpretations. Conversely, a propositional formula is valid *if and only if* its negation is unsatisfiable. As an example, consider a Boolean variable p. The formula $p \wedge \neg p$ is unsatisfiable since it is not true in any interpretation—in other words, it does not have any model. The formulas p and $\neg p$, on the other hand, are satisfiable but not valid since they are true in some, but not all, interpretation(s). Finally, the formula $p \vee \neg p$ is valid since it is true in all interpretations. In the SAT problem, we seek a *satisfying assignment* for a given propositional formula on a set of Boolean variables which assigns values to the variables such that the formula evaluates to *True*.

The main idea behind the traditional SAT solving based verification, depicted in Fig. 1, is to express the verification problem, i.e., $\mathcal{M} \models \phi$ where $\mathcal{M}$ is a *model* of a system and ϕ is a specification expressing what should be true in situation $\mathcal{M}$, in propositional logic. This propositional logic relationship is then negated and transformed to conjunctive normal form (CNF), i.e., a conjunction of disjunction of literals (usually termed as the sums of products in digital circuit design), in such a way that ascertaining the satisfiability of this CNF allows us to deduce the validity of $\mathcal{M} \models \phi$ as shown in Fig. 1. This CNF

[6] Any instance of NP-complete problem can be transformed into an instance of another NP-complete problem quite easily. As an example, both graph coloring and SAT problems are NP-complete, and an instance of the former problem (i.e., graph coloring) can easily be transformed into an instance of the latter (i.e., SAT).

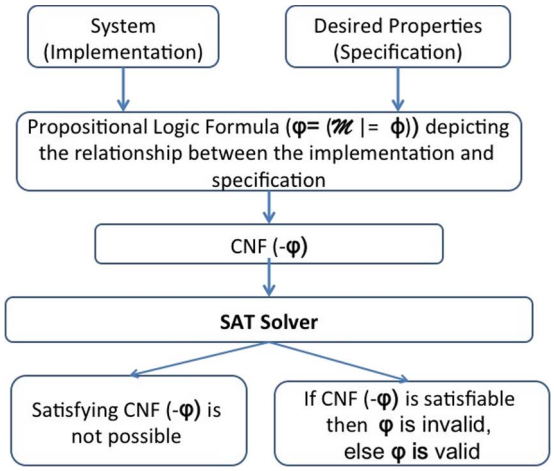

Fig. 1. Formal verification using SAT solvers.

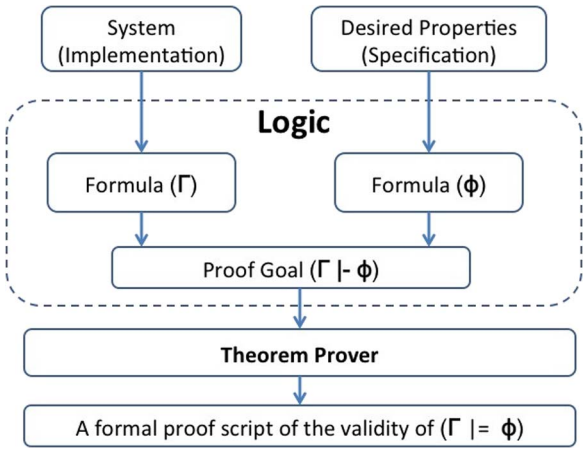

Fig. 2. Formal verification using theorem proving.

form is then given to the SAT solver in the corresponding syntax to automatically check its satisfiability.

Broadly speaking, there are *two ways to use a SAT solver*. The first, and simplest way, is the *eager approach* for the application to generate a Boolean formula for the SAT solver so that it may determine that the satisfiability of the formula. Alternatively, the application can use the *lazy approach* to reduce a problem to a series of inter-related SAT queries, in which the SAT solver incrementally solves subsequent queries dynamically generated based on the results of previous queries [99]. Much of the improvement in SAT solver performance in recent years has been driven by several improvements to the basic DPLL algorithm such as *i*) non-chronological backjumping and learning conflict clauses, *ii*) optimization of constraint propagation rules, *iii*) heuristics for picking split variables (even restarting with a different split sequence), and *iv*) highly efficient data structures. A detailed account of various algorithms for solving the SAT problem is presented in [100], whereas recent advances in SAT-based formal verification can be viewed at [101], [102]. A comparison of propositional satisfiability and the related field of constraint programming can be seen in [99]. Modern tools can solve practical industrial SAT problems having millions of variables and constraints in mere seconds. In practice, such approaches can help avoid the daunting proposition of redeveloping algorithmic solutions for solving new problems, thus enabling a wide variety of application areas to benefit.

While we are mostly interested in propositional satisfiability due to its tractability, the concept of satisfiability can be generalized to other Boolean logics—in particular, the quantified Boolean formulas (QBF) problem generalizes the SAT problem[7] and refers to the problem of deciding the satisfiability of quantified Boolean formulae, or QBF, in which the variables can be either universally or existentially quantified. The ability to utilize universal and existential quantifiers in arbitrary ways makes QBF considerably expressive than SAT. It must be noted that SAT is NP-complete which means any NP problem can be encoded in SAT. Similarly, QBF is PSPACE-complete, i.e., any PSPACE problem can be encoded in QBF. Unfortunately, current QBF solvers do not scale, and therefore, our primary focus will be on the SAT problem and solvers.

The SAT problem has many interesting variations. For example, the MaxSAT problem is the application of SAT problem to optimization theory, the AllSAT problem aims to determine all satisfying assignments, etc. Motivated by the success of SAT solvers, researchers have recently given significant attention to Satisfiability Modulo Theories (SMT). While SAT solvers determine the satisfiability of propositional formulas, SMT solvers can, on the other hand, check the satisfiability of formulas in some decidable first-order theory (e.g., linear arithmetic, array theory, uninterpreted functions, bit-vectors, etc.) [103]. SMT is seeing rapid progress and initial commercial use in software verification [104].

Various SAT/SMT tools have been proposed with rapid progress in this field being sustained by Moore's law and consistent advances in algorithms, data structures, and decision heuristics [105]. Example SAT/SMT solver tools include MiniSAT [106], Chaff [107], and the Z3 tool from Microsoft [108]. Due to the great generality of SAT/SMT solvers, it is remarkable that various contemporary verification tools that differ in terms of source language, methodology, and degree of automation, eventually fall back on these solvers for the core task of checking validity and satisfiability. With their impressive generality, scalability, and maturity, SAT/SMT solvers look set to play a significant role in future formal verification technology.

B. Theorem Provers

In the theorem proving paradigm of formal verification, we are interested in a deductive proof of $\Gamma \vdash \phi$, where Γ is a *set of formulas* representing the system behavior (implementation) in a suitable logic, and ϕ is another formula representing the system property (specification) that needs to be checked. As depicted in Fig. 2, this relationship is verified as a proof goal using a computer-based tool theorem prover, which is sound and complete. The term soundness has a background in mathematical logic where a system is said to be sound if it can only prove valid arguments with respect to a semantics. Completeness, in contrast, implies that there will be no *false*

[7]In the SAT problem, all the variables are implicitly existentially quantified.

positives which require exhaustive analysis of every possible scenario.

The dream of having automated theorem provers is a long-standing dream of many an ambitious scientists starting from Leibniz, to Peano and Hilbert [109]. Herbrand in 1930 provided a mechanical method for proving theorems but due to lack of appropriate computing facilities the method was difficult to apply. In 1936 Church and Turing showed that it is impossible to devise a generic method of verifying the validity of first-order logic. First-order logic is said to be semi-decidable in that methods exist for verifying validity of a formula if it is indeed valid, however, such methods will never terminate in general for invalid formulae. This has defined the limits of automatic theorem proving. In the 1960s, Herbrand's method was implemented on a digital computer, followed by an even more efficient Davis–Putnam–Logemann–Loveland (DPLL) algorithm [110]. The resolution principle, proposed by Robinson in 1965, has been a major step forward. The DPLL algorithm is important for many applications including automated theorem proving and satisfiability modulo theories (SMT). The DPLL algorithm is used to solve the CNF-SAT problem—i.e., determine the satisfiability of propositional logic formulae in conjunctive normal form (CNF).

Despite the theoretic complexity of automated reasoning in expressive logics, in practice, *interactive theorem provers*—also known as proof assistants—which solve the proof verification problem are useful in many settings. Interactive theorem provers differ from automatic theorem proving in that it requires human assistance. A proof assistant is a program that takes a formalized mathematical statement and a plausible proof, and checks whether the proof is valid. There are three key ingredients of a proof assistant. Firstly, it needs to incorporate an expressive formal language and logic—which is typically, but not always, a variant of higher-order logic. Secondly, it needs to have support for checking proofs and in aiding proof construction. Lastly, it needs to have a programming language—typically a functional programming language—that allows extending the system with new proof procedures (e.g., decision procedures). There are various interactive theorem provers that have been proposed including tools that are based on first-order logic (e.g., ACL2 [111], Microsoft's Z3 tool [108]—which uses many-sorted first-order logic, etc.) and others that are based on higher-order logic (e.g., Isabelle [112], HOL [113], PVS [114], Coq [115], etc.).

C. Model Checking

Developed independently in 1980's by Clarke and Emerson[8] [49], and by Queille and Sifakis [118], model checking can be envisioned as an automated debugging, or exhaustive simulation and testing, technique useful for checking any property violations (i.e., bugs or errors) [119]. While formal verification has traditionally been associated with logic-based axiomatic or deductive techniques for establishing proofs of correctness,

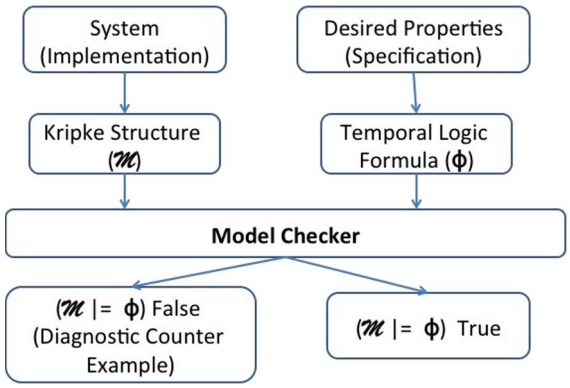

Fig. 3. Formal verification using model checking.

model checking has been the first step towards engineerization of this field [84], [119].

The main insight of model checking is that proof construction—a tedious and non-trivial task requiring good deal of ingenuity and guidance from the user—is not necessary for the case of finite state concurrent systems. In model checking, we are interested in showing that $\mathcal{M} \models \phi$ where $\mathcal{M}$ represents a Kripke structure[9] or a labeled transition graph, as a model of system description while the specification is still a formula (typically written in propositional temporal logic). As depicted in Fig. 3, the model checking problem is (from [120]): "Let $\mathcal{M}$ be a Kripke structure (i.e., a state transition graph), ϕ be a formula of temporal logic (i.e., the specification). Find all states s of $\mathcal{M}$, such that $\mathcal{M}, s \models \phi$ (i.e., $\mathcal{M}$ has property ϕ at that state s)." As discussed earlier in Section III-A2, Kripke structures are *labeled* FSM with the states labeled with a sets of atomic propositions that are true in this case; all other unlabeled propositions are assumed false according per the "closed-world" assumption. This model checking can be performed for finite state systems algorithmically, unlike proof systems, in a push-button fashion. In model checking, the verification procedure intelligently searches through the entire state space of the design in an exhaustive fashion [49], and thus this technique is applicable for finite state systems.[10] Although this looks limiting, many interesting systems (e.g., hardware devices, communication protocols, etc.) can be modeled as FSMs in practice.

It is important to ensure that the term "model" in "model checking" is not confused with its everyday usage of being an abstraction of the actual system under study. In the case of "model checking," the inventors of this method were interested in the model-theoretic interpretation [121], [122] of the term "model"—i.e., determining that $\mathcal{M}$, representing the system interpreted as an automaton, is a (Kripke) *model* for the temporal logic formula ϕ representing the desired property [120]. It should be noted that when we say that $\mathcal{M}$ is a model for the formula ϕ, we really are paraphrasing our intention of saying "ϕ, when interpreted as in $\mathcal{M}$, is true." Noting the distinction between the various interpretations of models can alleviate any

[8]For a historical account of the development of model written, the interested reader is referred to [116] and [117] (written by Emerson from his personal perspective).

[9]A Kripke structure, proposed by Saul Kripke, is a nondeterministic automaton representing a system's behavior. Kripke structures are commonly used in model checking for interpreting temporal logics.

[10]Infinite state can only be analyzed with abstraction [83] and induction.

unnecessary confusions. To summarize, model checkers are named such because they check whether a system, interpreted as an automaton, is a (Kripke) model of a property expressed as a temporal logic formula.

Model checking is a rigorous method which, unlike testing, verifies a property only if it is true for all possible executions. This is a very useful feature as the verification engineer does not need to think about creating smart test cases to identify system problems. Similarly, model checking has many benefits over deductive proof techniques which makes it preferable wherever it is applicable. Some compelling benefits of model checking [120] include: *i*) it is fast compared to other rigorous methods; *ii*) it provides diagnostic counterexamples; *iii*) it can work well with partial specifications/properties; *iv*) logics can easily express various concurrency properties; finally, *v*) it does involve any human-guided proofs.

Buchi automata has been used in model checking as a bridge between automata theory and temporal logic. In particular, Buchi automata can provide an automata-theoretic formalization of a linear temporal logic, or LTL, formula. It was shown in the mid 1980s that there exists for every temporal logic formula a Buchi automaton that accepts precisely those runs that satisfy the formula. There are algorithms that can mechanically convert any temporal logic formulae into the equivalent Buchi automaton. Typically, the property invariants are expressed as LTL formulas, and a negated version is converted to Buchi automata to be used in the model checking algorithm to detect violation of the desired property.

Scalability of Model Checking: The state explosion problem limits the application of model checking to large scale problems. Various approaches have been proposed for coping with this issue including symbolic model checking, bounded model checking, and statistical model checking. These approaches are covered next.

a) Symbolic model checking: The main insight of symbolic model checking is that it is more efficient to consider large number of states simultaneously at a single step instead of traversing enumerated reachable states one at a time. Symbolic model checking facilitates such a state space traversal by allowing representations of states set and transition relations as Boolean encoded formulas, BDDs, or related data structures. This allows handling of much larger designs containing hundreds of state variables [123]–[125]. Symbolic algorithms can thus work with the FSM represented implicitly as a formula in quantified propositional logic without the need of explicitly building a FSM graph. Symbolic model checking is the most commonly used variant of model checking in industrial scale model checking tools. The first symbolic model checking tool, SMV, was developed by McMillan in 1992 and used BDDs to combat the state explosion problem [126]. More recently, SMV has been extended and reimplemented as NuSMV and NuSMV2 [127].

b) Bounded model checking: Symbol model checking can also be performed through SAT procedures [128]. SAT procedures can operate on Boolean expressions without requiring canonical forms and without the potential space explosion of BDDs. Various efficient implementations are available for solving SAT problems. Bounded model checking (BMC) uses a SAT procedure instead of BDDs [129]. A Boolean formula is constructed that is satisfiable *iff* there is a counterexample of length k. By incrementing the bound k, longer counterexamples can be searched. After some number of iterations, we may conclude that no counterexample exists and the specification holds. The state explosion problem is thus handled by focusing on falsification rather than exploring all reachable states. Incorporation of the falsification approach into a SAT based framework in a BMC allows scaling to much larger number of states. BMC techniques using the falsification approach are very useful since in many practical scenarios, we are more interested in finding bugs as early as possible in the design rather than in formally proving the correctness of the design. SAT-based BMC for falsification is a very popular model checking technique in the industry. As an example, safety property may be verified by increasing the number of iterations to the bound defined by the diameter of the FSM. The advantage of the bounded model checking approach is that it can quickly find counterexamples due to the depth first nature of SAT search procedures. Secondly, since the bound is increased incrementally, the approach finds the counterexample of minimum length which leads to better diagnostics. Finally, it also uses lesser space as compared to BDD-based approaches. The NuSMV2 tool [127] incorporates both BDD-based and SAT-based model checking. BMC can also be performed using SMT tools [130]. BMC tools include a CBMC [131] which is a bounded model checker for ANSI-C and C++ programs.

c) Statistical model checking: Statistical model checking is a proposal that can allow model checking to scale to large systems by relaxing the requirements of formal correctness. The key insight is to use hypothesis testing with a simulation based approach to deduce from some sample executions if the system under test satisfies the specification [132].

d) Probabilistic model checking: Various approaches have been proposed for building probabilistic model checking tools [133]–[135]. PRISM is an example probabilistic model checking tool that can be used for reachability analysis [136] and protocol verification [137]. While traditionally, establishing performance evaluation and correctness have been orthogonal tasks, a promising new direction in formal methods research is to develop probabilistic methods that can allow joint analysis of both correctness and performance [138].

e) Model checking for software: Model checking is not inherently well suited for verifying software due to the asynchronous and unstructured nature of software. While, the early successes of model checking were mainly in hardware verification, recent progress has made model checking viable for software verification [139]. Popular model checking softwares include Java Pathfinder [140], Microsoft's Slam Toolkit [93], UC Berkeley's BLAST [141]. The interested reader is referred to a detailed survey on model checking for software for more details [139].

D. Light-Weight Formal Methods

"Full-blown" formal methods, such as model checkers and proof systems, have some limitations due to which there is interest in alternative "light-weight" formal methods [142].

Proof systems, like theorem provers, have the deficiency that they cannot be fully automated due to fundamental limits of computation. Model checkers, on the other hand, face the state explosion problem and cannot deal with indirection, which is a fundamental concept of software [54]. Lightweight formal methods [143] tend to overcome these limitations by exploiting advances in technologies such as SAT solvers.

The *Alloy analyzer* works by translating constraints to be solved from Alloy into Boolean constraints which are then fed to an off-the-shelf SAT solver. Alloy is also known as a *model-finding* tool since it aims to find an instance of a counterexample, known as a model in logic theory, quickly rather than for completeness. Alloy defines both a language for describing structures and also a tool for exploring them—in particular, it specifies a new high-level language, inspired from Z [144], for specifying the behavior of software; secondly, it uses an automated SAT-solver based analyzer to work through all the possible scenarios. The software design modeled with a high-level notation is then analyzed over billions of possible executions to catch any pathological conditions. The important consequence is that subtle design errors are caught even before the design is coded. The design, once thoroughly tested, can then be constructed with much more confidence. Alloy represents a new generation of software analysis engines similar in principle to tools traditionally used for verification of hardware designs [145].

E. Static Analysis

Static analysis is a class of techniques concerned with extracting information about the run-time behavior of a program, or a configuration file, without actually executing the source file. Static analysis, which means analysis without execution (e.g., SLAM [93]), is to be contrasted with dynamic analysis, which involves executing the program (e.g., Verisoft [17]). Static analysis can discover bugs in configuration files, or software systems, before they are activated or executed thus obviating the reflexive debugging that results from discovery of bugs after deployment. Due to the fundamental limits imposed by the theory of computation (cf. Turing's halting problem which is notorious for being undecidable), static analyzers *cannot* extract run-time behavior of all programs perfectly. Static analyzer attempt to defy the undecidability of the halting problem by not focusing on *completeness* or *soundness* but instead on quick and efficient debugging. The key insight used by static analysis is to utilize an approximate interpretation, or an abstract interpretation, of the program. In many cases, this approximate interpretation is finite, and thus amenable to analysis.

In the context of debugging, soundness means the ability to detect *all* possible errors of a certain class, or not miss a bug if one exists—in other words, a sound debugger will give no *false negatives*. An effective static analyzer, thus, has to balance three desirable, but often competing, costs: *i*) the cost of false negatives due to being unsound, *ii*) the computational cost of analysis, and *iii*) the usability of the tool (which can be measured in total time investment of the user) [146]. In particular, it turns out that soundness and completeness have a tradeoff. For *assurance* based projects where soundness is needed (i.e., if told that there are no errors, we should be sure that there are none), we are limited to accepting incompleteness, or to accept false alarms or false positives. The presence of false alarms is usually irritating for customers of debugging tools—who aim incidentally to reduce the number of bugs and not necessarily eliminate all of the bugs—who often give up on soundness to reduce the number of false alarms. Most commercial debugging tools (such as Coverity, etc.) are neither sound nor complete, but perform well in practice catching many errors with lesser number of false alarms.

It is instructive to compare static analysis with model checking directly [147]. In general, model checking has some benefits that are hard for static analysis to match: e.g., *i*) it can check the implication of code, and not just surface-visible properties, *ii*) it gives stronger correctness results, etc. A major drawback of model checking approach is the need to create a correct working environment model—this restrictions makes model checking infeasible for many networking verification tasks [148] and adds significant overhead even when feasible especially for large scale systems. Also, no model is as good as the implementation itself, and the abstraction in the modeling process is a potential for producing false positives or missing critical errors. Static analysis is more useful than model checking in some aspects: e.g., *i*) it is quicker, *ii*) it can easily check millions of lines of code, *iii*) it can find thousands of errors. Some of these comparisons are direct outcomes of the fact that static analysis does not run any code, while model checking does [147]. Static analysis is a widely used technique used in many software testing tools (e.g., Coverity, FindBugs, etc.) that can analyze extremely large code-bases [149].

Static analysis is known to all programmers in its most basic form of typechecking in compilers (e.g., a Java compiler will catch errors such as adding a number to a Boolean, etc.) This kind of static analysis focuses on simple checking with no false alarms and thus only scratches at the surface of what can be achieved with static analysis. More extensive static analysis requires more computation but can check a wider range of properties—e.g., runtime exceptions due to division by zero, array bounds violation, etc. can be detected.

Extended static checking defines a powerful paradigm for program checkers in which verification conditions—i.e., a logical formula that is valid iff the program is free of the classes of error under consideration—are defined, and then counterexamples to the verification condition are searched mechanically [150]. Extended static checking for Java (ESC/Java) [151] is a compile time program checker that performs formal verification of properties of Java source code through theorem proving. ESC/Java is an annotation language, which is effectively a subset of Java Modeling Language (JML). It allows the programmer to add Hoare-style preconditions and postconditions and loop invariants into the program with special comments in the source code.

F. Symbolic Simulation and Execution

Symbolic execution [152], also called symbolic evaluation, is a "abstract interpretation" method for analyzing a program

TABLE II
TAXONOMY OF FORMAL VERIFICATION TECHNIQUES

Technique	*Soundness*	*Automation*	*Counter Examples*	*Generic*
SAT Solvers	✓	✓	✓	✗
Interactive Theorem Provers	✓	✗	✗	✓
Model Checkers	✓	✓	✓	✗
Light-weight Formal Methods	✗	✓	✓	✗
Static Analysis	✗	✓	✓	✗
Symbolic Simulation & Execution	✗	✓	✓	✗

assuming symbolic values for inputs rather that actual inputs that would arise through the normal execution of the program. Symbol execution is essentially a technique for generating an optimized test suite that satisfies a customizable coverage criteria using which deep errors in software applications may be identified. Although the idea of symbolic execution is quite old (proposed by King in 1976 [153]), symbolic execution has emerged as an effective tool recently with advanced in constraint satisfaction tools. Symbolic execution proceeds by exploring as many program paths as it can in a given time budget, thereby creating a logical formula encoding the explored paths. A constraint solver is then used to calculate feasible execution paths. Symbolic execution are much more powerful than dynamic execution techniques, such as those incorporated in popular debugging tools like Valgrind [154], since it can find a bug if there exists *any* buggy input on a path without depending on a concrete input that triggers the bug. Symbolic simulation [155] is an extension of the idea of symbolic execution to hardware systems. Simulation is a time-test tool for formal verification. Simulation can be generalized in two different ways: *i*) ternary simulation [156]—where we have a "don't care" value X in addition to 0 and 1; *ii*) symbolic simulation—where Boolean variables can act as input parameters and outputs are functions of these parameters. Ternary symbolic simulation unfortunately suffers from the problem of large growth in the state space leading researchers to look for alternative techniques in recent times [30].

G. Taxonomy of Formal Verification Techniques

In this section, we classify common formal verification techniques based on the basis of four main characteristics. The first characteristic is *soundness*: a technique is termed sound if the results verified by it are always true. The second characteristic is *automation* which refers to an automatic push-button type verification process which does not require user guidance. The third characteristic is the *provisioning of illustrative counterexamples* in case of finding a bug. Finally, the last characteristic we will use in our classification is the *ability to verify generic properties* that are universally quantified. A taxonomy constructed on the basis of this classification is presented in Table II. The techniques are arranged in the order of their increasing complexity in terms of usage.

Referring to Table II, the three full-blown formal verification techniques (SAT solvers, theorem proving and model checking) are sound while the other three techniques (light-weight formal methods, static analysis, and symbolic simulation and execution) compromise on soundness to provide more user friendly alternatives. The results of light-weight formal methods cannot be termed as sound due to the partial nature of modeling and analysis. However, these techniques usually support automatic analysis and provide debugging support by providing counter examples. Most of the static analysis tools compromise the soundness to improve completeness of the analysis. Symbolic techniques have not been identified as sound since for real-world systems the number of possible input combinations is usually very high and the whole range cannot be covered even in the symbolic form. Failing test cases provide counter examples, which are very useful for debugging the system. While interactive theorem provers require explicit user guidance in the verification process and thus are very cumbersome to use and also do not provide counter examples, interactive theorem provers provide the most powerful verification technique in terms of tackling a wide range of verification problems and is the sole technique that supports verifying generic theorems as well.

V. FORMAL VERIFICATION TECHNIQUES IN NETWORKING

In this section, we will describe various applications of formal verification methods to networking. We will initially focus on highlighting the applicability of various verification techniques to various problem domains in networking in Section V-A. We will then provide a detailed technique-categorized description of application of formal verification techniques in networking in Section V-B. Finally, some common pitfalls in applying formal methods are highlighted in Section V-C.

A. Applicability of Verification Techniques in Networking

Networks include many components—such as hardware including digital circuits and software including operating system and communication protocols—that must work correctly in harmony for the holistic correctness of the networking service. The appropriate choice of technique depends on the networking subsystems we are trying to formally model and verify. Due to the diversity of the subsystems, it is envisioned that multiple verification techniques would be used in the field of networking: e.g., BDDs and model checking would be useful for digital circuit verification, static analysis would be useful for checking for overflow and bugs in software, model checking can be used for communication protocol verification, etc.

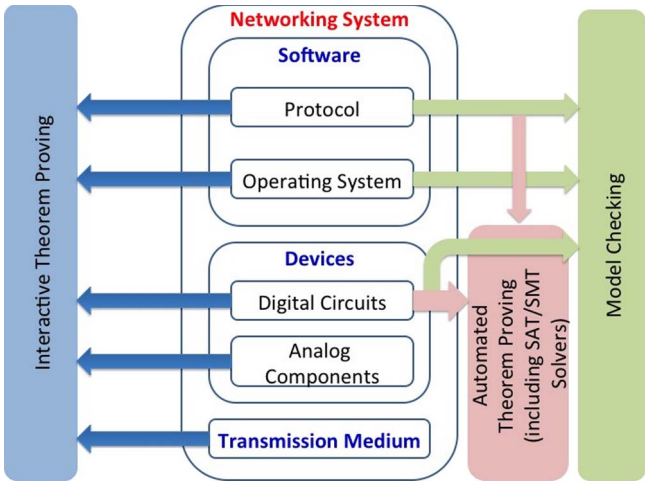

Fig. 4. Applicability of core formal verification techniques in networking.

Before we indulge into the detailed discussion of the applications of various formal verification techniques in networking, it is important to note that *simulation or testing* is a very effective analysis technique and formal methods should never be thought of as an alternative to simulation. Both the techniques complement one another and thus have to play together for an effective, realistic and complete analysis. It is a very common occurrence that some sub-systems of the given system are more safety-critical, e.g., the correctness of the protocol ensuring the reliable communication in a network is more important than the graphical user interface module. Thus, it is more viable in terms of verification time and effort to use simulation for analyzing the non-critical blocks and formal verification for analyzing the safety-critical sub-systems only. Moreover, simulation offers a very viable solution for verifying complete system models, which, due to their large size and complexity, are almost impossible to be modeled and verified using formal methods. Finally, formal methods are based on mathematical foundations and thus cannot be used to reason about properties for which closed form solutions do not exist. Thus, these aspects are also handled by simulation or numerical methods.

Techniques such as *light-weight formal methods, static analysis*, and *symbolic simulations*, bridge the gap between formal methods and traditional simulations. Their analysis results are trust worthier than traditional simulations but cannot be termed as sound and complete as the ones that are obtained via model checking or theorem proving. On the other hand, these verification methods are user friendlier than the core formal verification techniques. These techniques can be used at various abstraction levels and models and have shown promising results in reachability and returnability analysis of networks.

Using powerful abstractions, the core formal verification techniques of theorem proving and model checking have also been used in the literature to analyze almost all key aspects of networking. In order to highlight the strengths of these core formal verification methods, the Fig. 4 connects a particular sub-system of a networking system to a formal verification method only if the method allows to analyze the sub-system including all the required details, i.e., without using any abstractions. In this figure, we are focusing on the applicability of core verification techniques of theorem proving and model checking, which are both sound and complete, and do not include other techniques such as SAT solving, light-weight formal methods which are generic solutions. The figure is not intended as a final say in this matter, but represents the authors opinion regarding which technique is best suited to various problems of verification in networking.

Automated theorem provers (and SAT solvers) for propositional and some subsets of first-order logic allows us to automatically analyze models of the given systems. The only requirement for this kind of verification is to translate the system behavior and the desired properties in the target logic. The verification can then be done in an automatic push-button fashion. The main limitation of propositional logic is its limited expressiveness as it cannot be used to represent verification problems for all sorts of systems (like the systems including the notion of time and continuous systems). Thus, they are quite well suited for analyzing system models at a higher abstraction level during the early design phases. Besides that, automatic theorem provers can only be used to verify the combinational circuits of the digital blocks of the networking devices and some basic protocols, which can be described completely in propositional logic.

Model checking is primarily used as a verification technique for reactive systems, i.e., the systems that exhibit a behavior that is dependent on time and their environment, like communication protocols. These kinds of behaviors cannot be assessed using automated theorem provers and thus the most suitable approach to tackle the verification of networking protocols (essentially all the protocols used in the seven layers of the OSI model) and the sequential logic of digital circuits of networking devices is model checking. Moreover, many aspects of real-time operating systems, such as mutual exclusiveness during common file sharing, can be checked using model checking. The verification involves translating the behavior of the given system in the language supported by the model checker and the desired properties in temporal logic. The model checker can then check if the properties hold for the model automatically and in the case of failures can also provide error traces, which are quite useful for debugging. The verification is again is automatic. Due to the enormous involvement of protocols in networking systems, model checking is undoubtedly one of the most widely used formal verification technique in this domain. Besides the functional verification, probabilistic model checking allows us to tackle the verification of performance related characteristics of networking systems as well. However, in this case, we cannot model the continuous behaviors of the medium and thus a discretized model of the medium is used.

Model-checking is limited to systems that can only be expressed as finite state machines. Another major limitation of the model checking approach is state space explosion. Similarly, due to its inherent nature, model checking cannot be used to verify generic mathematical expressions and deal with continuous models. *Interactive theorem provers*, with higher-order logic, allows us to overcome all these limitations. Thus, interactive theorem provers can be used to verify communication protocols, their performance, and reason about the correctness of networking systems while considering physical

TABLE III
REPRESENTATIVE SUMMARY OF VERIFICATION APPLICATIONS CATEGORIZED BASED ON **TECHNIQUE** USED

Technique	*Project & Reference*	*Brief Summary*
Model Checkers		
	Al-Shaer et al. [91]	'Network configuration in a box' using BDD/ CTL with Symbolic Model Checking
	Holzmann et al. [77]	Protocol verification
	Narain et al. [157]	Proposed a method for managing (i.e., formalizing, and automating, reasoning about) network configuration with 'model finding' using the Alloy analyzer
	ConfigChecker [91]	Symbolic reachability analysis with BDD/CTL-based model checking using the Alloy tool
	Ritchey et al. [158]	Using model checking to analyze network vulnerabilities
	NICE [159]	Performs symbolic execution of OF applications while applying model checking to explore the entire state space of the network
Static Analysis		
	HSA [61]	HSA provides a protocol-agnostic method for finding data plane bugs in networks by jointly studying the header space of packets and transformations applied to it by networking boxes
	FlowChecker [160], Anteater [161]	These tools perform static verification of the data plane of a network using static analysis techniques based on a snapshot of network state
	Xie et al.[162]	Proposed a graph-theoretic algorithm for static Analysis of IP networks with support for ACL policies
Theorem Provers		
	Frenetic	The Coq tool has been used for verifying the network controller
	Frenetic	Verifying a featherweight version of the OpenFlow protocol [163] using the Coq tool
	Paulson et al. [112]	BGP policy verification was performed using Isabelle/ HOL
	Hasan et al. [164]	Performance analysis of the Stop-and-Wait protocol using HOL theorem prover
	Elleuch et al. [165]	Formally analyzed coverage-based random scheduling algorithm for WSNs using HOL theorem prover
SAT and SMT solvers		
	FlowChecker [160]	Uses SAT/ SMT to verify the reachability and security of OpenFlow federated infrastructures
	Anteater	Anteater builds upon Xie et al. [162], *implements* a tool for checking invariants in the data plane by transforming invariants into SAT instances to be checked against network state by a SAT solver
	FLOVER [166]	Verifies the network's security policy is not violated in an an OpenFlow network
	NetSAT [167]	NetSAT is a data plane verification project that is SAT based

and randomized aspects associated with the medium, like noise. Moreover, due to its ability to reason about continuous aspects, theorem proving can also be used to formally verify physical components, like analog and mixed signal devices and optical networks, in communication devices. This technique is also expressive enough to handle reactive systems, like communication protocols, and complete operating systems. However, this flexibility comes at the cost of manual verification where specific user guidance is required to verify all formulas expressed in higher-order-logic, due to its un-decidable nature. Thus, the interactive theorem provers are only suitable if the verification of some very safety-critical sub-block of a system, with continuous or randomized behavior, is required.

B. Technique-Based Categorization of Applications

In this subsection, we will discuss the application of formal verification techniques discussed in Section IV in the context of networking. In particular, we will discuss applications of model checking, theorem provers, light-weight formal methods, static analysis, and symbolic simulation and execution in this particular order. A representative summary of applications of these techniques, categorized per technique, is presented in Table III for easy reference.

1) Applications of SAT/SMT Solvers in Networking: Recent advances in SAT/SMT solvers have significantly advanced the state of the art in formal verification, and SAT/SMT tools for various logics are routinely used in network verification projects. There has been a remarkable upsurge of interest in propositional logic SAT solving since a diverse class of problems (including scheduling, planning, problems) can be expressed as propositional satisfiability problems. While propositional satisfiability (SAT) problem is the canonical NP-complete problem which makes it intractable in theory, it can fortunately be solved efficiently in practice.

There are various applications of SAT/SMT solvers in the literature of formal verification for networking. We present a few works as examples. Zhang *et al.* have presented an approach for verifying and synthesis of firewalls using SAT and QBF [168]. FLOVER, a model checking system, implemented using the Yices SMT solver [169], verifies that the networks security policy is not violated by the aggregate of flow policies instantiated within an OpenFlow network [166]. Recently, there has been work in verifying the data plane through SAT solvers. Anteater [161] verifies the data plane by translating connectivity invariants into SAT problems that are checked against the data plane by a general SAT solver to return a counter example in case of violation of invariants. NetSAT is another data plane verification project that is SAT based [167].

2) Applications of Model Checking in Networking: There are a great number of *model checking tools* that have been devised with some popular model checkers being SPIN [170], NuSMV [127], and Alloy [54]. SPIN, developed in early 1980s by Holzmann for assuring dependability in complex telephone switching systems, is a popular award-winning[11] *explicit-state* model checking tool. SPIN was the first model checker developed, with its initial focus being on telecommunication systems and protocol verification. SPIN is now used for diverse applications from hardware verification to distributed control software used in nuclear power plants and spacecrafts. The IEEE Futurebus cache coherence protocol is the first IEEE protocol whose specification was debugged successfully through model checking. NuSMV, in contrast to SPIN, is a *symbolic* model checking tool that also incorporates features of *bounded* model checking. NuSMV was the first implementation of symbolic model checking and was developed by McMillan in 1992 [126]. NuSMV

[11]The SPIN model checker has been awarded the ACM Software System Award http://www.acm.org/announcements/ss_2001.html.

TABLE IV
REPRESENTATIVE SUMMARY OF VERIFICATION **TOOLS** CATEGORIZED BASED ON TECHNIQUE USED

Tool	*Technique*	*Brief Summary*
Microsoft's Z3 [108]	SAT/ SMT	Z3 is a state of the art SMT solver from Microsoft Research
Kodkod [55]	SAT/ SMT	Kodkod is a SAT-based constraint solver that can work with first-order logic with relations, transitive closure, etc.
YICES [169]	SAT/ SMT	Yices is an efficient SMT solver that can also act as a SAT and MaxSAT solver
SPIN [170]	Model Checking	SPIN is a mostly automated tool for verifying distributed and concurrent systems
NuSMV [127]	Model Checking	NuSMV, an extension of the original symbolic model checking tool SMV, is a model checking tool based on BDDs
PRISM [136]	Model Checking	PRISM is a probabilistic model checker suitable for systems that exhibit probabilistic behavior
Uppaal [82]	Model Checking	UPPAAL is a model-checking based tool-box, based on timed-automata formalism, used for verification of real-time systems
SMC-Uppaal [171]	Model Checking	Statistical extension of Uppaal which supports composition of timed automata and/or probabilistic automata
Edinburgh LCF [75]	Theorem Proving	Interactive theorem prover proposed in 1972 which introduced ML language as a metalanguage for writing proving tactics
HOL [113]	Theorem Proving	HOL represents a family of interactive theorem provers that are based on higher-order logics and strategies
Isabelle [112]	Theorem Proving	A popular LCF-style theorem prover (written in Standard ML) that can work with various logics
ACL2 [111]	Theorem Proving	ACL2 is a mechanical theorem prover with a Common Lisp-variant programming language, and an extensive first-order logic based theory
PVS [114]	Theorem Proving	PVS is an automated theorem prover with an integrated specification language with multiple support tools
Coq [115]	Theorem Proving	Coq is an interactive theorem prover that assists in finding proofs, and in extracting a certified program from the constructive proof
Alloy [54]	Light-Weight Formal Methods	Alloy analyzer is a light-weight formal method that can analyze user specified properties of a (partial) model
ESC/Java [151]	Static Analysis	ESC/ Java is a theorem proving based compile time program checker for formal verification of properties of Java code
Coverity, FindBugs	Static Analysis	These tools can statically analyze extremely large code-bases [149]
Margrave [172]	Static Analysis	Firewall analysis
rcc [148]	Static Analysis	BGP configuration fault detection
HSA/ Hassell [173]	Symbolic Simulation	HSA/ Hassell uses ternary symbolic simulation implementation for verifying various properties such as reachability, loop detection, etc
NICE [159]	Symbolic Simulation	NICE is a symbolic execution and model checking based framework for catching bugs which works by exploring symbolically all possible code paths

can utilize both BDD-based and SAT-based techniques. Alloy is also a symbolic model checker that translates constraints into Boolean formulas which are then solved through an external SAT-solver. SPIN and NuSMV support temporal logic for property specifications with SPIN supporting propositional LTL and NuSMV supporting CTL. For model specification, SPIN uses the PROMELA language (which is inspired by C) while NuSMV uses the SMV description language to specify finite state machines. Alloy uses first-order logic for both model specification and property specification. A detailed comparison of SPIN, NuSMV, and Alloy, and some other model checking tools, is presented in [174]. Popular model checking tools are listed in Table IV, along with other popular formal verification tools, for quick reference. Apart from SPIN, NuSMV, and Alloy, it is worthwhile to mention two other popular types of model checking tools. The PRISM tool [136] is a probabilistic model checking tool, while the UPPAAL tool [82] is a model checking tool based on timed-automata which can be used for verification of real-time systems.

Model checking techniques and tools have been extensively applied in the context of networking, and we will present a representative sample. Zave *et al.* have used model checking to understand SIP [175]. Al-Shaer *et al.* have used model checking for configuration analysis for general networks [91] and for SDN networks having federated OpenFlow infrastructures [160]. In [160], network routing tables are represented as BDDs and reachability predicates are computed using model checking. In other works for OpenFlow networks, Canini *et al.* present the model checking based NICE platform for verification [159], and Son *et al.* present a model checking based security invariant property checker [166]. In a recent work [176], three state-of-the-art VM based open-source cloud management platforms have been formally analyzed and verified using the technique of bounded model checking using the SAT/SMT solvers SMT-Lib and Z3Solver.

Most of the model checking work has focused on verifying safety property since verifying liveness property entails computing an infinite long trace of states in which the desired property is never reached with heuristics-based MaceMC being a notable exception [177]. A summary of various tools that are used in this regard is presented separately in Table IV.

3) Applications of Theorem Provers in Networking: Theorem provers have many applications in networking research. As specific examples, we will discuss three theorem proving tools that are popularly used in networking research. The Coq tool, which incorporates higher-order logic along with richly-typed functional programming language, defines a system for manipulating and mechanical verification of formal mathematical proofs by machines [115]. Coq also supports extracting certified programs to popular functional languages like OCaml, Haskell, etc. The Coq tool has been used for verifying the network controller in SDN environments [163] and for ensuring per-packet and per-flow consistency of network updates [178]. The Z3 tool from Microsoft, which uses a portfolio ofx solvers, is another popular theorem prover used in many software testing, analysis and verification projects [108]. Finally, the Isabelle/HOL theorem prover has been used for network verification and the BGP policy verification [112] is a notable example in this regard.

Besides the functional verification, theorem provers have also been used for the formal performance analysis of network applications based on the higher-order-logic formalizations of probability theory [44] and Markov Chains [179]. Some notable examples in this regard include the performance analysis of the Stop-and-Wait protocol [164], scheduling algorithms of

Wireless sensor networks [165], the memory contention problem in multiprocessor systems [180] and the quantitative analysis of information flow in a network [181].

4) Applications of Light-Weight Formal Methods in Networking: Light-weight formal methods in general, and particularly the Alloy tool, have been widely deployed to solve a wide variety of problems ranging from security analysis [157] to the design of telephone switching networks [10], [182]. The main attraction of using light-weight formal methods is in their ease of use and their operational orientation towards non-specialists.

5) Applications of Static Analysis in Networking: Static analysis has also been used in networking context most notably for reachability analysis in IP networks [162], firewall analysis (e.g., Margrave [172], etc.), BGP configuration fault detection [148], [183], etc. Static analysis can It can also be used for debugging of networking software using static analysis techniques described for software verification (described earlier in Section IV-E).

6) Applications of Symbolic Simulation in Networking: Header Space Analysis (HSA) [173] is an example ternary symbolic simulation implementation proposed recently for verifying various properties such as reachability, loop detection, etc. for SDNs. Canini *et al.* have proposed a symbolic execution and model checking based NICE framework for catching bugs which works by exploring symbolically all possible code paths [159]. In another work, Bishop *et al.* [184] have proposed symbolic evaluation testing of TCP implementation against a HOL specification.

C. Common Pitfalls Applying Formal Methods

In this subsection, we will describe some common pitfalls that network practitioners must avoid while applying formal methods in networking.

1) Selecting Inappropriate Techniques: As highlighted in this work, there is a vast amount of work that has been done in the field of formal methods. There are various logics, notations and technologies available, each making its own claim of superiority, that may be utilized. Many of the claims are valid in that certain techniques do certain excel in niche areas; however, each technique has its disadvantages as well. As Keshav has pointed out [185], the choice of the most appropriate tool is certainly non-trivial even for an established researcher, let alone for a graduate student. It is important to use the most appropriate specification language for the task, as noted in the 10 commandments stated in [186].

Technique selection directly impacts the verification effort and complexity. For example, while verifying a communication protocol, we can use automated theorem provers, model checking and theorem proving. While using automated theorem provers, the model needs to be abstracted so that it can be captured by the logic (with limited expressiveness.) supported by the theorem prover. Model checking can also handle this protocol but due to the state-space explosion problem, we would be limited by the number of nodes in the verification. A generic expression for the desired characteristic quantified over all possible number of nodes can be verified using an interactive theorem prover but this would be very time consuming. This decision is generally made based on the desired properties and models and time and resources at hand. It is always recommended to use automated verification methods whenever possible. In an industrial case study, we usually use various techniques for verifying the complete system. In such cases, integrating the results obtained via various techniques is also a main challenge.

2) Using Mismatching Tools: We have multiple tools supporting a single formal verification technique and each tool is optimized in certain aspect. For example, the SPIN model checker and supports LTL while nuSMV supports both LTL and CTL. On the other hand, nuSMV does not support abstraction over entity instances [174]. Similarly, UPPAAL allows us to verify real-time systems, which the above-mentioned model checking tools are not capable of verifying. Similarly, the higher-order-logic theorem prover HOL-Light provides support for multivariable calculus but do not support probabilistic reasoning, which is available in the HOL theorem prover. Thus, one of the foremost jobs of a verification engineer is to identify the desired features of the tools that are required in the selected technique. This kind of an upfront analysis is very critical since an inappropriate selection of a tool can cause unnecessary delays in the verification process.

With research in network verification recently starting to flourish, it is important to determine the right tools for various verification tasks in network verification. Two tools that are immediately useful for a networking researcher are Alloy and SPIN: a practical comparison of these two tools is presented in [187].

3) Naïve Overreliance on Unfaithful Models: In formal verification, we always work with models instead of real systems. For example, while verifying a piece of code written in C++, it needs to be translated to an appropriate logic for using theorem proving or the language supported by the model checker for model checking based verification. The first challenge is the assurance that this model faithfully captures the behavior of the given system. Since, if the model is incorrect then the whole purpose of using formal verification is lost. Even though we can never be 100% sure that the model depicts the system correctly, the verification process can certainly raise the confidence level in our model. It is usually recommended to verify as many properties as possible during the verification phase as it is very less likely that a correct property will be verified for a wrong model.

VI. Application Domains of Formal Methods in Networking

In the history of the Internet, formal correctness has mostly taken a backseat to practical expediency and pragmatic considerations. The development, standardization, and deployment process is cumbersome and inflexible leading to an environment which only just works [188]. As an example of the unfortunate adhocism that pervades the culture of network protocols, it is noted that BGP, despite any lack of convergence guarantees, is often used in service as an interior-gateway routing protocol (IGP) [189]. While there were some initial successes in the application of formal methods to networking [182], the networking enterprise quickly transformed into a complex behemoth

impervious to any attempts at formal analysis and verification. In addition to the inherent complexity of networking protocols, the vertical integration of control and data planes meant lack of modularity and a paucity of useful abstractions [9]. With the tools of formal methods unable to tame the staggering complexity of networking, the resulting frustration bred skepticism leading to a widespread critical view, enunciated by Vint Cerf [23], that formal methods are "overblown, verbose, hard to use, (and) hard to understand." Fortunately, modern attempts at redesigning the Internet ossified architecture—and more specifically, the SDN movement—create new abstractions by separating the control and data planes and thus allow a great opportunity for incorporating formal methods in networking. With the utility of Internet firmly entrenched in all aspects of modern life, the use of formal methods for ensuring correctness of specification and operation is anticipated to be incorporated into mainstream Internet operations.

Traditionally, the focus of formal verification community has been on hardware systems or software systems, and relatively less on network verification. Networked systems comprise a software component (implementing the node OS, protocols, applications, etc.) and a hardware component (featuring the range of hardware configuration such as microprocessors, general purpose processors, DSPs, ASICs, etc.). Networked system are in fact distributed systems composed of end hosts that use the network as well as networking nodes (such as routers, switches, and various middleboxes such as firewall, load balancers etc.) that implement the network. In previous work, network verification is considered as essentially a state machine verification problem [30]—i.e., a communication network can be visualized as a finite network of FSMs. Although, this problem is quite complex theoretically—PSPACE-complete for the general problem of verification of network of FSMs—structural properties of networks as we shall see fortunately enable efficient practical techniques.

We will now discuss various applications of formal methods and verification techniques in networks categorized according to the application domain. We will initially discuss protocol verification, and will follow it up with a discussion on the verification of network properties (such as reachability, isolation, absence of loop, etc.). We will thereafter discuss network configuration management and network security. A discussion on techniques for formal specification and synthesis of protocol follows. We will follow it with a discussion of using formal methods for verifying implementations and hardware. Finally, we will discuss the SDN architecture, and how its emergence is acting as a boon to the adoption of formal methods in networking. A summary of the following discussion is tabulated in Table V for easy reference.

A. Formal Specification

There are many benefits in formally specification including the clarity accompanying rigorous specification of high-level specification of the target networking problem along with the ability to employ mechanized correctness checking to weed out trivial mistakes through techniques such type-checking. It has been shown in research that informal specification of protocols can lead to incorrect reasoning and implementation [20] and ambiguity [175].

In networking protocols, it is important that protocols are defined unambiguously. Traditionally, the specification process adopted by Internet Engineering Task Force (IETF) is based largely on specification through informal English prose, with implementations also serving as an informal specification surrogate. Although in the early 1980s, various IETF standards have been formally specified by various academics (including an Estelle [201] description of Transport Control Protocol, TCP), the IETF has not embraced the use of formal description techniques and continues to specify protocols informally relying primarily on the implementation as the specification. The tendency to use the implementation as the specification has the drawback of not cleanly separating what is part of the protocol and must be conformed to and what is system and implementation dependent. The lack of the emphasis on formal specifications for Internet protocols has created a problem where it is considered acceptable to create software without fully understanding the implications leading to an ad-hoc hit-and-trial based software development culture [144]. Experience with Internet protocols has shown that simple informal English prose is insufficient for specifying and communicating protocols [10]. Many of the problems that arise due to informal specifications can be redressed through formal methods for specification which aid not only in verification and communication, but also in analysis [1]. In particular, analytical tools can analyze the formal description to ensure that absence of protocol deadlock, data loss, races, hazards, and other pathological behaviors.

There are many standard *formal description languages* for protocols [27]. The Estelle language [201] and the SDL language [217], specified by CCITT/ITU, are based on a extended state model. The LOTOS language [218], on the other hand, is based on a temporal logic model. The Z (pronounced Zed) language [144] is a popular formal specification language useful for describing *transformational* systems such as sequential programs in Hoare style using pre- and post-conditions. PROMELA is a specification language used for specifying LTL formulas that can be used for validation of *reactive* systems with the SPIN model checker. The interested reader is referred to a tutorial article [27] for more details about formal description and specification techniques such as SDL, Estelle, PROMELA, LOTOS, etc.

In order to create a correctly performing implementation, it is worthwhile to invest time and effort in *design verification*. Various approaches can be explored including specialized meta-theories specific to routing and forwarding [189], axiomatic logic-based formalisms [219], or declarative programming frameworks [220], [221], to specify the design. These formalisms can then be analyzed used methods like theorem provers, model checking, SAT/SMT solvers, lightweight formal methods etc. to verify the correctness of the design and thereby guide the implementation.

B. Protocol Verification

In layered communication networks, protocols define the set of rules governing exchange of messages between interacting

TABLE V
SUMMARY OF APPLICATION OF FORMAL METHODS IN NETWORKING CATEGORIZED ON THE BASIS OF **APPLICATION DOMAINS**

Project and Reference	*Technique*	*Brief Summary*
Protocol Verification		
Bishop et al. [184]	Symbolic Evaluation	Proposed symbolic evaluation testing of TCP implementation against a HOL specification
Ridge et al. [190]	HOL proof assistant	Proposed a rigorous approach for modeling and verifying TCP using the HOL proof assistant
Reachability Analysis		
Xie et al.[162]	Static Checking	Proposed a graph-theoretic algorithm (transitive closure) for static analysis of IP networks with support for ACL policies
Khakpour et al. [191]	Static Checking	Proposed a tool Quarnet comprising algorithms for quantifying reachability based on network configuration (incorporated ACL) and for querying network reachability
Al-Shaer et al. [91]	(Symbolic) Model Checking	Proposed a BDD/ CTL based symbolic model checking approach for performing 'network configuration in a box'
Lopes et al. [30]	SAT solvers	New SAT based solutions for the reachability set predicate
HSA [173]	SAT solvers; Static Checking	HSA provides a protocol-agnostic method for finding data plane bugs in networks by jointly studying the header space of packets and transformations applied to it by networking boxes
NetPlumber [61]	SAT solvers; Static Checking	HSA-based real-time policy checker for networks that works with incremental recomputation
VeriFlow [192]	Mininet, Depth-first search, Tries	Implemented as a layer between SDN controller and switches, VeriFlow verifies network-wide invariants in real-time dynamically as a forwarding rule is added
AP Verifier [90]	Atomic Predicates Verifier	AP verifier reduces the set of predicates representing packet filters to minimal atomic predicates, using which AP verifier dramatically improves computation of network reachability
Loop Detection		
HSA, NetPlumber, VeriFlow, AP Verifier	See above	These tools provide support for loop checking as well.
Isolation Verification		
AP Verifier [90]	Atomic Predicates Verifier	AP verifier, discussed above, can also be used to verify slice isolation [90]
"Splendid Isolation" [193]	Model Checking	Proposes a slices abstraction for SDNs with automatically verifiable formal isolation properties (expressed in CTL and checked through NuSMV tool)
Configuration Management		
rcc [148]	Static Analysis	Static analysis tool for detecting BGP configuration faults proactively before deployment
Qie et al. [183]	Static Analysis	Proposed using service grammar, incorporating a requirements language containing global high-level constraints, for detecting BGP configuration errors
Narain et al. [157]	(Lightweight) Model Checking; Scenario Finding	Proposed a method for managing (i.e., formalizing, and automating, reasoning about) network configuration with 'model finding' using the Alloy analyzer
ConfigChecker [91]	(Symbolic) Model Checking	Performs firewall verification with BDD-based model checking to perform symbolic reachability analysis
FlowChecker [160]	(Symbolic) Model Checking	The FlowChecker tool can be used to verify the correctness of OpenFlow federated infrastructures and debug reachability and security problems
Anteater [161]	SAT solvers; Static Checking	Anteater, builds upon Xie et al. [162], *implements* a tool for checking invariants in the data plane by transforming invariants into SAT instances to be checked against network state by a SAT solver
Paulson et al. [112]	Theorem Prover	BGP policy verification was performed using Isabelle/ HOL prover
Network Security		
FLOVER [166]	Model-Checking; SMT solvers	Verifies that the aggregate of flow policies instantiated within an OpenFlow network does not violate the networks security policy
MulVAL [194]	Logic-based Analysis	A logic-based network security analyzer
Zhang et al. [168]	SAT and QBF solvers	A SAT based technique for comparing the equivalence and inclusion relationship between two firewalls, and also propose Quantified Boolean Formula (QBF) based ACL optimization
Margrave [172]	SAT solvers & Scenario Finding	Firewall analysis tool that allows tracing behavior to specific rules and verification against security goals
Al-Shaer et al. [195]	Tree based model	Proposed a "Firewall Policy Advisor" for managing firewall filtering rules, and for detecting all anomalies in single or multiple firewall environments
Kothari et al. [196]	Symbolic Execution & Model Checking	Studies protocol manipulation attacks in which adversaries induce honest players into undesirable behaviors
Ritchey et al. [158]	Model Checking	Uses model checking to analyze network vulnerabilities
Gouda et al. [197]	Firewall Decision Diagrams	Presented a structured firewall design ensuring consistency, completeness and compactness. Also, proposed firewall decision diagram (FDD) for modeling firewall specification formally
Automatic Synthesis		
FVN project [198]	Logic-based framework	FVN presents a approach towards unifying the design, specification, implementation, and verification of networking protocols based on a logic language NDLog
Noyes et al. [199]	Model Checking	Proposed techniques for synthesis of network updates using NuSMV and OCaml tools
Wang et al. [200]	Reactive Synthesis & Model Checking	Proposed techniques for automated synthesis of reactive controllers for SDNs

processes which serve two related goals: firstly, to provide service to the local protocol layers above, secondly, to interact according to a defined protocol with remote peer partners on other machines. In terms of specification, the former goal is defined through service specification, while the latter is defined through protocol specification. Both these specifications—service-specification and protocol-specification—can be verified against their design or implementation. Verification at the design stage is more useful as it can avoid unnecessary incorrect implementation [222].

There are three main ways in which protocols can fail [13], [223]: *deadlocks*—when all the protocols stall waiting for conditions that can never be fulfilled; *livelocks*—when execution sequences keep getting repeated indefinitely without the protocol making any effective progress, and *improper terminations*—when the protocol completes execution without satisfying the proper terminating conditions. The general problem of finding deadlocks in protocols is known to be complex, i.e., PSPACE-complete at best which makes it undecidable for unbounded message queues. Thus any method that relies exclusively on an exhaustive search of state space method is bound to fail, thus prompting much research on alternate non-exhaustive methods that exploit symmetry and abstraction. Also, due to the inherent complexity of the problem, we set a

TABLE VI
REPRESENTATIVE SUMMARY OF **PROTOCOL VERIFICATION** EFFORTS

Reference	*Protocol*	*Network Type*	*Method*	*Tool*
Medium Access Control Protocols (Link Layer)				
Kwiatkowska et al. [137]	802.11 DCF	WLAN	Probabilistic Model Checking	PRISM
Fehnker et al. [203]	LMAC	WSN	Model Checking	UPPAAL
Ballarini et al. [204]	S-MAC	WSN	Model Checking	PRISM
Routing Protocols (Network Layer)				
Bhargavan et al. [14]	RIP/AODV	General	Interactive Theorem Proving/ Model Checking	HOL/ SPIN
Malik et al. [205]	OSPF	Data Centers	SMT/SAT	Z3
De Renesse et al. [206]	WARP	MANET	Model Checking	SPIN
Fehnker et al. [207]	AODV	WMN/ MANET	Model Checking	UPPAAL
Xiong et al. [208]	AODV (generalizable)	WMN/ MANET	Colored Petri Nets (CPNs)	Occ CPN tool
Hofner et al. [209]	AODV and DYMO (AODV v2)	WMN/ MANET	Statistical Model Checking	SMC-Uppaal
Reliability Protocols (Link Layer & Transport Layer)				
Bergstra et al. [210]	ABP [211]	General	Process Algebra	Algebra of Communicating Processes (ACP)
Suzuki et al. [212]	ABP	General	Temporal Petri Nets	
Billington et al. [213]	Stop and Wait Protocol (SWP)	General	Colored Petri Nets with hand proofs and automatic techniques	DesignCPN
Billington et al. [214]	TCP	General	Colored Petri Nets	DesignCPN/ CPNTools
Bishop et al. [184]	TCP	General	Symbolic Model Checking with HOL	HOL
Hasan et al. [215]	ARQ	General	HOL models for Stop-and-Wait, Go-Back-N and Selective-Repeat ARQ protocols	HOL
Other Protocols (Application Layer & Security Protocols)				
Zave [175]	SIP	General	Model Checking	Promela/ SPIN
Vsimovnak et al. [216]	TFTP	General	Petri Nets	ACP2Petri, PATool
Bhargavan et al. [95]	TLS	General	Use model-extraction and verification tools	ProVerif/ CryptoVerif
Armando et al. [217]	Various Security Protocols	General	SAT-based Model Checking	SATMC

more conservative target in protocol verification of detecting the presence of errors—should they exist—with high probability instead of striving to prove the absence of errors with certainty.

Various works have been proposed for protocol verification and a representative summary is presented in Table VI. As noted in Table VI, while certain works have focused on protocols in narrowly specified networking environments such as wireless LANs (WLANs) [137], wireless sensor networks (WSNs) [202], [203], wireless mesh networks (WMNs) [208], mobile ad-hoc networks (MANETs) [205], [207], modern data centers and clouds [176], [204] etc., most of the formal verification work in networking applies generally to all kinds of networks. There also has been work on verification of protocols across the layered TCP/IP networking stack as can be seen in Table VI including work at the link-layer, network-layer, transport-layer, and application-layer.

Many formal verification works [209], [211], [224] have prototyped their modeling and verification work on a simple reliability protocol known as the "*alternating bit protocol*" (ABP) [210] which was designed to provide reliable full-duplex data transfer over an unreliable half-duplex physical transmission line over which messages may be lost or corrupted in a detectable way but may not be duplicated or reordered. Amongst other work for the *link-layer*, there also has been a lot of work on the formal verification of medium access control (MAC) protocols. Kwiatkowska *et al.* have utilized the probabilistic model checking tool PRISM for the verification of the IEEE 802.11 DCF protocol [137]. Fehnker *et al.* [202] have utilized the UPPAAL model checking tool for the verification of LMAC protocol proposed for WSNs. Ballarini *et al.* have also utilized the technique of model checking (using the tool PRISM) for verification of the S-MAC protocol proposed for WSNs [203].

There also has been work on verifying *network layer protocols*. Bhargavan *et al.* [14] have utilized the techniques of interactive theorem proving and model checking (using the tool HOL and SPIN) for verifying the RIP and AODV routing protocols. Malik *et al.* [204] have utilized SMT/SAT solvers for verifying the OSPF routing protocol in data center environments. In other works of verification of routing protocols, various researchers have used the technique of model checking. De Renesse *et al.* [205] have used the model checking tool SPIN for verifying the wireless adaptive routing protocol (WARP) routing protocol. Fehnker *et al.* [206] have utilized the model checking tool UPPAAL for verifying the AODV protocol which is very popular in WMN and MANETs. Hofner *et al.* [208] have utilized the statistical model checking tool SMC-UPPAAL for verifying AODV and DYMO (AODV v2).

Petri Nets (including Colored Petri Nets or CPNs) are popular modeling tools for protocols. CPNs and the tool occ-CPN has been used by Xiong *et al.* [207] for analyzing the AODV routing protocol. CPNs, and the tool DesignCPN, have been used by Billington for verifying the stop-and-wait (SWP) and TCP transport layer protocols. Petri Nets have also been used by Vsimovnak *et al.* using the tools ACP2Petri and PATool for verifying the application layer protocol TFTP.

A lot of work has also focused on verifying *transport layer protocols* including work on stop and wait protocols (SWPs) [212], general ARQ techniques including go-back-N and sliding window protocols [214] and on the TCP protocol [184], [190], [213]. A variety of techniques have been used for verifying transport layer protocols including modeling with

Petri Nets with hand proofs and automated techniques [212], [213], interactive theorem proving using higher-order logic [214], and symbolic model checking and execution [184]. There also has been work on formally verifying *application layer protocols* with work being done on modeling and verifying various properties of (boundedness, liveness, deadlock freeness) of trivial FTP protocol (TFTP) [215] and SIP [175]. The techniques and tools used by these works is summarized in Table VI.

In addition, there has been significant research in the field of *security protocol verification*. Security protocols are defined as a protocol/program which aims to secure communications on insecure networks utilizing cryptographic primitives and find ubiquitous use in modern networks (with an example being the TLS protocol used for secure communication using the HTTPS protocol). Security protocols verification is especially challenging and can evade functional software tests since many security errors arise when a malicious adversary abuses the protocol. Automatic tools for security protocol verification is thus highly desirable and this is an actively researched area [225].

There are various security related properties with *secrecy* and *authentication* representing two key properties that are required by most security protocols. Secrecy, or confidentiality, implies that an adversary cannot obtain any information on data manipulated by the protocol, while authentication implies that two participants A and B talking to each other apparently share the same values of a protocols parameters [225]. In order to prove the correctness of security protocols, two security protocol models are used (the details of which are outside the scope of this paper). The symbolic model is the simpler model which is amenable to relatively easy automatic proofs, while the computational model is much more realistic, and more commonly used by cryptographers, but its proofs have been limited to being manual until recently. Numerous verification techniques exist for automatic verification of security protocols in the symbolic model including model checking, SAT-based model checking [225]. Various techniques have been proposed for modeling security protocols (such as through model extraction [95]) and for verifying security protocols (such as through SAT-based model checking [216]).

As depicted in Fig. 4, the techniques of automated theorem proving (including SAT/SMT solvers), interactive theorem proving and model checking, are all well suited to the task of protocol verification. As can be seen in Table VI, protocol verification work has been done across the TCP/IP layering stack with a wide variety of formal verification techniques being used (including model checking, symbolic evaluation, interactive theorem proving such as HOL, and SAT/SMT solvers).

There have been a few survey papers written focusing on communication protocols [12], [226], including a FSM-based protocol verification survey [222] and a survey documenting experience with protocol description [10]. Various tools have been used for protocol verification including the theorem proving tool Isabelle [112] for BGP policy verification and the proof assistant Coq tool [115] for creating a featherweight version of the OpenFlow protocol [163].

C. Network Property Verification

There is great interest and intent in the research community to develop technological support for automatic verification of various properties of protocols and systems. When we are verifying the property of a system, we are essentially interested in two kinds of properties: *i) Safety property* where we are mainly interested that "bad" things will not occur, *ii) Liveness property* where we are mainly interested in that "good" things will eventually occur [97]. In general, safety property bugs are easier to discover by finding a counterexample, while liveness property violations are difficult to obtain—in particular, a liveness violation example would require finding an infinitely long execution trace in which the desired "good" property never happens [177]. Recent works such as Anteater [161], Header Space Analysis (HSA) [61], FlowChecker [160], VeriFlow [192] use an automatic solver to check properties of a logical representation of switch configurations.

In the remainder of this section, we will cover example properties of reachability analysis, loop detection, and isolation verification, packet destination control.

a) Reachability analysis: Reachability analysis is a powerful method widely used for formal verification of protocols [77] and concurrent distributed systems. Unfortunately, reachability analysis suffers, like all methods based on finite state machines, from the state-explosion problems. Reachability analysis can benefit from symbolic methods which work without inspecting all the reachable states of the system to scale to large networks—e.g., BDD-based symbolic traversals have been proposed for reachability analysis of large finite state machines [227]. An example work that utilizes BDD-based symbolic model checking for reachability analysis is the ConfigChecker tool proposed as part of the "Network configuration in a box" project by Al-Shaer *et al.* [91].

There is a well-developed theory for verification of FSMs: e.g., reachable states, and equivalence, etc., that can readily be exploited for network verification tasks. In particular, reachability of states is very relevant in a networking context. The FSM formalism has been extensively used in formal verification works for networking [61], [91], [160], [178]—in these works, the packet is considered as an FSM. Many network verification projects model the network as a large state machine (see description in [29] and [30]).

In a networking context, reachability analysis was first proposed for IP networks by Xie *et al.* [162]. The technique proposed utilized a static snapshot of network configuration, culled from configuration state from each of the network routers, for determining reachability between applications running on end-hosts. This reachability information is very useful in network troubleshooting and management for verifying the implementation of the intent of the network designer, and for troubleshooting reachability problems. Xie *et al.* reduced the reachability problem to a classical graph theoretic problem of computing the transitive closure which can be solved in polynomial time. Transitive closure is a standard graph-theoretic technique which, intuitive speaking, provides an efficient method for answering the reachability question "where can we get from here?". A non-formal intuitive depiction of the transitive closure problem

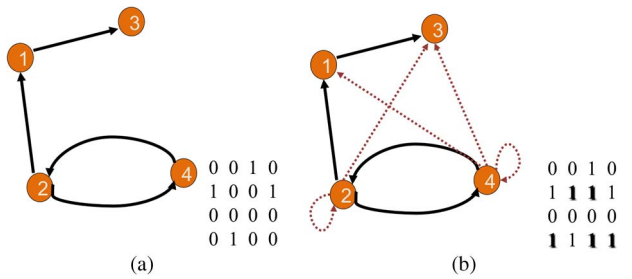

Fig. 5. Reachability analysis performed by a graph theoretic transitive closure algorithm such as Warshall's algorithm. (a) Input graph connecting directly reachable nodes. (b) output graph connecting directly or indirectly reachable nodes.

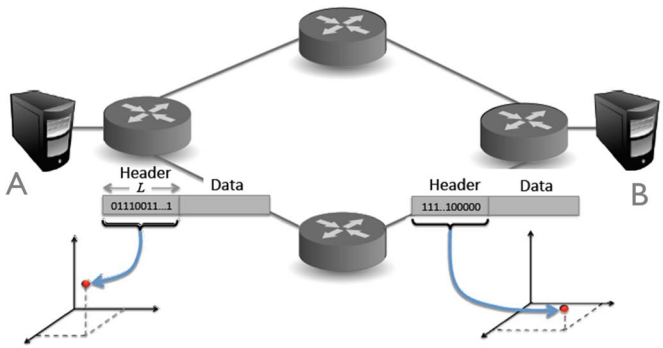

Fig. 6. The geometric transformation of a packet's header in header space analysis by network boxes from one geometrical point to another in the header space [173].

is presented in Fig. 5. The input graph is shown in Fig. 5(a) which is a network graph with edges connecting two directly connected nodes (with the associated matrix incorporating the same information by showing its i, jth element as a 1 if i can reach j directly or 0 otherwise). We are interested in computing reachability from various nodes: i.e., which of the other nodes can a node reach directly or indirectly. A transitive closure algorithm like the Warshall's algorithm can solve this problem in polynomial time to provide a graph like the one shown in Fig. 5(b) which is connecting every node to all nodes reachable from it (directly or indirectly). Recently, advances in SAT technology have popularized the use of transitive closure algorithm for reachability analysis problems [30], [167].

Kazemian *et al.* have proposed a general protocol-agnostic static checking framework for networks based on *header space analysis* (HSA) [173]. The basic insight of HSA is to model a packet by its header by treating the entire header field as a concatenation of bits without any associated semantics—instead, the packet may be considered as a (geometric) point in the $\{0, 1\}^L$ geometric space where L is the maximum length of the packet header. The network is then modeled as being composed of network boxes (such as routers, switches, etc.) that transform packets from one point to another point, or possibly set of points (assuming multicast). This transformation from a point in header space to another point in header space is represented in Fig. 6. This geometric approach taken by HSA (i.e., of representing the packet as a point in a subspace) allows the Hassel tools to check for a variety of failure conditions (reachability failures, forwarding loops, and traffic isolation failures) in a protocol-agnostic way. Using HSA, we can easily *i*) find all packets that can reach from a point A to another point B, *ii*) find loops regardless of the protocol/layer, *iii*) prove that two sites are isolated. Unlike model checking, HSA is not limited to providing a single counterexample in case of a failure detection, but can importantly provide information about the full set of failed packets.

Tracking the transformation of every possible packet (there are 2^L possible headers) sounds complicated; fortunately, group of packets tend to have the same behavior—e.g., all the traffic destined to port 80 gets dropped, or all packets going to a particular destination go through a particular next hop, etc.—thus reducing the number of geometric transformations that we need to track making header space analysis tractable. The grouping of the packets can be done in HSA without knowing packet semantics or prior knowledge about packet fields. In HSA, the processing by network boxes is modeled through box transfer functions that transform subspaces of the L-dimensional space to other subspaces. The changes to a packet enroute its flow through the network is captured by composing transfer functions along the path. In addition to modeling individual network boxes, HSA also uses a network transfer function Ψ (which combines individual box functions into a single integrated function representing the network behavior) and a topology transfer function Γ (which models the links that connects ports together). HSA provides an interesting abstract forwarding model that is independent of the protocol and can seamlessly incorporate new protocols and technologies. By providing algebraic support for basic set operations (intersection, union, complementation, difference, etc.) on the header space, HSA can act as a foundation over which reachability analysis, loop detection tools can be easily built.

Lopes *et al.* [30] have recently proposed extending the reachability predicate ("Can a packet from node A reach node B?") to a generalized abstraction of *reachability set* ("What are all the packets that can reach node B from node A?"). It is highlighted in [30] that reachability sets are useful for two reasons: *incremental computation* and *intelligibility*. In general, the tools for calculating reachability sets are less developed, although some languages like Datalog provide out of the box support for computation of reachability sets. The technique of incremental computation is useful for dynamic verification (i.e., when a new rule is being added) and has been recently proposed for real-time verification of SDN networks [61], [192]. The main insight underlying such an approach is the realization that a single rule change is unlikely to change the underlying network state machine drastically. Therefore, small modifications are necessary to the "reachability set" to incorporate the changes introduced by the addition of the new rule. Reachability set is also more intelligible as it produces a more general counter example—e.g., it can provide a set of packets being dropped.

In a promising recently proposed work [90], Yang and Lam present "Atomic Predicate (AP) Verifier," which reduces the set of predicates representing network packet filters to a set of atomic predicates that is provably both minimum and unique, which can be used to dramatically improve the computation of network reachability. The basic insight of this work is that atomic predicates have the following key property: Any given

predicate is equal to the disjunction of the a subset of atomic predicates, and thus can be stored and represented as a set of integers identifying the atomic predicate. The conjunction (or the disjunction) of two predicates can be computed quickly as the intersection (or union) of two sets of integers. As an example, Yang and Lam show that while the Stanford network has 71 ACLs and 1584 rules, there were only 21 atomic predicates for these ACLs and rules (due to great redundancy in the forwarding and ACL rules). By encoding the rules in terms of atomic predicates (in the form of BDDs which can be manipulated through well-known graph BDD algorithms), this unnecessary redundancy is removed leading to much greater space and time efficiency. In their performance evaluation, Yang and Lam compare AP Verifier with Hassel in C and NetPlumber to demonstrate that AP verifier is significantly more time and space efficient [90].

Property verification also includes questions about *packet destination control*: can a packet *i*) get out of the network, *ii*) get dropped, *iii*) go through certain switches, or *iv*) never pass through certain links. Model checking as well as ternary symbolic simulation techniques can be used for packet destination control [29].

b) Loop detection: Header Space Analysis (HSA) [173] defines a "network algebra" which captures the manipulation of packet headers by network routers and switches. In the HSA framework, packet headers, represented as n-dimensional bit fields, are operated upon by the function defined by routers and switches which effectively transform the packet headers. HSA, in addition to doing reachability analysis, can also pinpoint all packet headers that will loop. Given a network transfer function, loops are detected by injecting a special packet header (all of whose bits are wild-carded) from each port in the network with a loop being reported if the packet returns to the original port it was injected from [173]. HSA can verify a range of properties such as connectivity, reachability between ports, absence of any loops, and isolation between groups, etc.

Various other approaches have been proposed in literature for loop detection including ConfigChecker [91], AP Verifier [90], etc. In recent work, the NetPlumber tool [61] (which is based on HSA [173]) and the VeriFlow tool [192] (which is based on verification of network invariants) can also be used for detection of routing loops in *real time*.

c) Isolation verification: For various reasons (such as security, confidentiality, etc.), it is sometimes desirable to ensure that certain kinds of traffic are isolated from each other. In current Internet, this is managed by various ad-hoc mechanisms often requiring manual intervention. For example, techniques used for ensuring isolation include: *i*) low level mechanisms such as VLANs or ACLs requiring configuration, *ii*) special purpose devices such as firewalls, *iii*) or complex hypervisors such as the FlowVisor system [228] for OpenFlow networks. It is desirable to have more fundamental abstractions that can be exploited to provide verifiable isolation between traffic as desired.

Header space analysis [173] can be used to help create network slices that are guaranteed to be isolated. Alternatively, header space analysis can also be used for diagnostic purposes for detecting slices that should be isolated but are leaking traffic. Another work in this regard geared towards SDNs in the "splendid isolation" project [193] proposed as part of the Frenetic project [229]. In this work, a slice abstraction is presented and algorithms for compiling slices is presented along with a tool for automatic verification of formal isolation properties. In other works, AP Verifier can also verify slice isolation as reported in [90].

D. Network Configuration Management

Configuration errors can create numerous connectivity, security, performance, and reliability problems. It has been pointed out in literature that the bulk of network downtime is in fact due to manual errors [230] and misconfiguration of devices [29]. The problem is especially acute since it is not far fetched for a misconfiguration of a single device to cripple an entire network. Various problems can arise from bugs due to misconfiguration including access control failures, isolation guarantee failures, routing loops, reachability failures, blackholes, etc. The presence of such problems can have debilitating effect on network performance and efficiency, thus motivating a more rigorous and formal management of network configuration. In configuration management, we would like to have multiple abstractions, incorporating correctness checks, between the high-level global end-to-end requirements and low-level distributed configuration at individual devices.

Static analysis has been used extensively for detecting configuration faults. Feamster *et al.* proposed a static analysis tool *rcc* for detecting BGP configuration faults [148]. The *rcc* tool allowed proactive analysis of network configurations before deployment in an operational network by checking that BGP configuration satisfies a set of constraints, based on the correctness specification. The *rcc* tool, like most practical static analysis tools, is neither complete nor sound—i.e., it can miss problematic configurations, and may complain about harmless deviations from the best practices. Nevertheless, *rcc* was able to find many important classes of errors to make it useful in practice. Qie *et al.* [183] proposed an approach based on "service grammar" for BGP which incorporated a requirements language using which the network operator can specify high-level requirements against which the system may be checked. Unfortunately, the proposed grammar was rather low-level thus having possibilities of erroneous specification. In another work, Narain *et al.* proposed managing network configuration through model finding [157] while using the Alloy analyzer [54]. In yet other work, ConfigChecker [91] performs firewall verification with BDD-based model checking to perform symbolic reachability analysis. Configuration management has been a fertile area for application for formal verification methods with various proposals in literature [157], [160], [161], [231].

E. Network Debugging

As mentioned before, networks are composed of both hardware and software components and are managed in many cases manually. Due to this reason, networks can fail in a variety of ways making the job of debugging and troubleshooting a

network very complex. Traditionally, networking has a very primitive toolset for troubleshooting comprising few ad-hoc tools such as ping, traceroute, etc. usually complemented by the painstaking manual process of inspecting log files. Broadly speaking, debugging can take place either statically or dynamically. Static debugging—akin to compile-time checking—works by inspecting network configuration and settings through static analysis tools, model checking, SAT solvers, etc. Dynamic checking—similar to run-time checking—works by checking if the data plane is behaving as it should (techniques for data plane verification have earlier been discussed in Section VII-E). Dynamic checking can catch errors that arise from reasons other that erroneous configurations, e.g., it can help in the case of *i*) hardware errors, *ii*) link failure, *iii*) congestion, *iv*) intermittent problems, etc. Heller *et al.* have proposed systematic troubleshooting of SDNs by establishing equivalence of network views at different layers [232]. In particular, Heller *et al.* proposed comparing *i*) actual network behavior vs. policy, *ii*) the policy vs. device state, *iii*) the device state vs. the hardware state, etc. By comparing these diverse network views systematically, more efficient troubleshooting can be performed which will allow identification of faults and systematic tracking down root causes.

Handigol *et al.* [233] have proposed the ndb (network debugger) tool, analogous to the software debugging gdb tool, that aims to capture and reconstruct the sequence of events that leads to buggy behavior. In particular, it allows users to define a "network breakpoint" in the form of (header, switch) filter to identify the errant behavior, and then produces a packet backtrace, which includes historical information about the path taken by the packet as well as the state of the flow tables at each switch, to aid in troubleshooting of networks [234]. In a similar vein, Wundsam *et al.* [235] have proposed the OFRewind framework which is useful for capturing and reproducing the sequence of problematic OpenFlow command sequence. In another work, Scott *et al.* have proposed using correspondence checking and simulation based causal inferencing to isolate and localize software faults in SDN [236]. In networked systems, erroneous behavior can manifest itself due to the various issues related to distributed computing such as asynchrony, concurrency, and partial failures leading to time-consuming troubleshooting and considerable angst [237]. Various debugging tools have been proposed for debugging general distributed systems: e.g., Pip [238], etc., and automatic debugging techniques specific to SDN have been proposed in [239].

F. Network Security

The domain of network security is a very broad area which deals with ensuring that networks, and the programs that utilize the network, work securely as desired by the network operator and the network users. In this context, it is important that security properties such as secrecy, isolation, and authentication can be verified. Ensuring secure functioning of programs, especially when they communicate over a network, is an important aspect of ensuring network security. As discussed earlier in Section VI-B, security protocol verification is an extremely important and active area of research. The readers are referred to Section VI-B for a broad overview of the field of security protocol verification.

Designing an error-free security protocol is very challenging and many security protocols have been implemented and deployed with a design flaw being discovered years later. For example, the Needham–Schroeder authentication protocol was found vulnerable 17 years after being proposed [240]. Even discounting attacks that depend on breaking cryptography, security protocols can have other sources of errors that arise due to complex interleaving of protocol sessions and the presence/interference of malicious adversaries. Since these errors are hard to find just by inspecting protocol specification or by testing, there is a strong motivation of using formal methods for verification of security protocols. With security protocols being at the heart of security-sensitive applications in a variety of settings (e.g., e-banking, e-governance, etc.), security protocol verification serves as a strong example of an application that can benefit from the use of formal methods (in contrast to non-formal techniques) to fix the problems that non-formal techniques cannot solve.

There has been a lot of work in firewall verification and synthesis and vulnerability analysis. There are various important subproblems of firewall verification and synthesis [168]. Firstly, the *firewall equivalence checking* problem focuses on determining if two firewalls have identical behavior—i.e., they drop and permit the same set of packets. Secondly, the *firewall inclusion checking* problem compares two firewall policies and can verify that one policy is inclusive, i.e., more strict, than the other policy. Thirdly, the *firewall rule redundancy checking* problem focuses on determining redundant rules—i.e., rules that can be deleted without affecting the behavior of the firewall. Lastly, the *firewall synthesis* problem focuses on synthesizing a firewall with minimum number of rules install that matches exactly the behavior of another given firewall.

A variety of techniques have been utilized for firewall verification and synthesis and vulnerability analysis including static analysis [241], model based analysis [242], [243], logic-based analysis [194], SAT solvers, model checking [158], [166], new abstractions (e.g., firewall decision diagrams or FDD [197], atomic predicates (AP) verifier [90], etc.). While a comprehensive review of these techniques is outside the scope of this paper, we will provide a high level overview of three sample works in this domain next. The interested reader is referred to a detailed description of related work in [172] and [197].

Gouda *et al.* [197] presented a structured firewall design ensuring consistency, completeness and compactness, and also proposed firewall decision diagrams (FDD) as a formalism for modeling firewall specification. The proposed structured firewall design consists of two steps. Firstly, instead of defining firewall configuration as a sequence of possibly conflicting rules, the design is specified using the FDD. Secondly, the FDD is converted into a functionally-equivalent compact sequence of rules (using combination rules such as FDD deduction and FDD marking as well as a firewall compaction algorithm). Since FDDs are designed to be conflict-free, the method of structured firewall design ensures consistency. The formalism of FDD also enforces completeness because of its syntactic requirements. In another important recent work, Margave tool [172] provides

powerful features for firewall analysis, verification against security goals, and detection of overlaps and conflicts. Margrave's modus operandi is scenario finding: when a user inputs a query, Margrave returns the (typically exhaustive) set of scenarios that witness the queried behavior. Margrave models policies in first order logic with Margrave's backend producing sets of solutions to first-order logic formulae using the SAT-solving based Kodkod tool [55]. Lastly, the Datalog based MulVAL tool [194] models a network system to perform automatic network vulnerability analysis. MulVAL can incorporate bug databases into its framework using Datalog and can perform "what-if" analysis using Prolog programs.

G. Formal Synthesis

There also has been work in synthesizing protocol implementations from formal specifications. An example work in this regard is the "formally verifiable networking" (FVN) project [198]. In another work, the synthesis of network updates have been proposed [199]. Recently Lopes *et al.* [30] have indicated building a synthesis tool for Microsoft Azure firewalls as their future work—such a tool can enable synthesis of low-level rules from a high-level specification and thus network operators can forego the error-prone access control list (ACL) configuration CLI.

H. Implementation Verification

Having studied techniques that can be used to verify design in previous subsections, we will now see that a variety of techniques, described earlier in Section IV, can be used to verify *implementations*. In particular, we can make use of static checking as well as dynamic checking. In static validation, correctness properties are defined as invariants or constraints which are then checked to find out any system faults. In certain cases, a pre-processing stage may be necessary to transform the real system into an intermediate more checkable form. Static analysis and model checking are static validation tools. While most model checking tools work with specification models, some model checking tools (such as MaceMC [177], VeriSoft [17], and CMC [96]) can work directly with implementation code making them very valuable for verifying implementations. In dynamic validation, on the other hand, we rely on runtime verification and testing—which per se are not really formal verification tools but nonetheless perform a complementary role.

I. Hardware Verification

Formal verification methods have been used for hardware verification of networking devices. Some sample works in hardware verification in networking include verification of: *i*) the lookup machine of a hardware router [244], *ii*) the Fairisle ATM switching element [245], *iii*) network-on-chip [246], [247]. A more detailed treatment of this topic survey application of formal verification techniques in hardware design can be found at [11].

VII. Applications of Formal Methods in SDN

In this section, we will discuss new opportunities offered for incorporating programming and verification advances into the networking context by the SDN architecture. We will initially provide some necessary background on programming languages and verification in Section VII-A. We will then discuss the applications of logic and programming languages in the context of networking in Section VII-B. We will then discuss new degrees of freedom offered by SDN in Section VII-C. We will discuss SDN programming languages in Section VII-D and will thereafter talk about data plane and control plane verification in Sections VII-E and F, respectively. A tabulated summary of the application of formal methods in SDN is presented in Section VII for quick reference.

A. Background: Programming Languages and Verification

In recent times, the networking industry is observing a profound paradigm shift driven by the "software defined networking" (SDN) architecture which promises to bring programming and software to the very heart of networking. With software taking a central role in future networking, as foreseen by leading networking experts [31], there is a great upsurge in the interest of applying formal methods to networking and exploiting the vast amount of formal verification work done in the domain of programming languages (particularly for declarative programming, logic programming, and functional programming). In the remainder of this section, we will introduce the necessary background regarding the grammar of languages, declarative programming, logic programming, and functional programming in Section VII-A1, A2, A2a, and A2b, respectively. We will discuss the applications of these programming styles in the context of networking later on in Section VII-B.

Before delving into the other topics, we will provide a brief introduction to the semantics of computer programs. Broadly speaking, there are three ways to establish the meaning, or *semantics*, of computer programs [60]. In *operational semantics*, the program is modeled by execution on an abstract machine—this interpretation is useful for implementing compilers and interpreters. In *axiomatic semantics*, pioneered by Hoare and Floyd, the program is modeled by the logical formulas it obeys—this interpretation is useful for proving program correctness. In *denotational semantics*, the program is modeled by mathematical objects—this interpretation is useful for developing theoretical foundations of programming.

1) Grammar of Languages: The most common type of grammar used for specifying languages is known as the *context-free grammar*, which is expressive enough to capture the recursive syntactic structure of most languages of our interest. The core component of a context-free grammar is a set of rules where a rule typically defines a name and an expansion for that name. The Backus–Naur form (BNF) is a formal notation used for encoding the grammar of a language in a form amenable to human consumption. The BNF notation is used by many programming languages, protocols or formats in their specification. A rule of the BNF notation has the following structure: "$name ::= expansion$" where the symbol ::= means "expands

to" or "may be replaced with." Every name in BNF is enclosed in angle brackets, $\langle\,\rangle$. Choice is indicated by a vertical bar, $|$. For more details about the BNF format, the interested reader is referred to [36]. In the context of networking, the BNF format has been used to specify network programming languages in FlowExp (short for Flow Expression) [61], NetCoreLib for Frenetic [62], [63], etc.

2) Declarative Programming: Declarative programming is a programming style in which we specify what the program must do without specifying how to do it. The imperative programming style adopted by imperative languages such as C, Java, etc., in contradistinction, focuses on specifying algorithmically how the computer must do its job. It may be highlighted that the imperative programming style harmonizes with the imperative procedural (how to) approach typically adopted in computer science while the declarative programming style dovetails with a mathematical or logic-based approach which emphasized declarative (what is) knowledge [64]. Imperative programming style involves the use of mutable state variables which makes reasoning and verification a difficult task. Declarative programming style, in contrast, eschews maintenance of state variables and avoids invisible side-effects and relies instead of mathematical logic and evaluation of mathematical functions and logic formulae. Declarative programming is intimately tied to mathematical logic—programs in a declarative frameworks can be thought of as theories of formal logic, and computations as deductions in that logic space. Examples of declarative languages include SQL, frameworks such as: functional programming languages, logic programming languages, constraint logic programming, etc. In recent times, there has been a lot of interest in declarative languages, and in their use in networking especially cloud networking [65], since declarative languages are well-suited to parallel programming[12] [67].

a) Logic programming: Logic programming provides many advantages including programmability at a very high level and natural support for formal semantics. Logic languages, such as Prolog, Lisp, have been very popular in the AI community for knowledge representation and automated reasoning. Prolog, an example declarative logic programming language designed primarily for AI based systems, works by stating and querying the logical relations between entities. Prolog like languages are also useful in formal verification for automated theorem proving. Logic programming languages are also popular in the databases community of computer science due to their support for declarative querying and symbolic manipulation. Datalog, an example database-based logic programming language, facilitates declarative definition of properties and relationships between objects with the language framework providing support for computing with these objects (including querying about objects declaratively).

The declarative programming style is superior to the procedural style in some significant ways—especially, in the context of formal verification [68]. The declarative style emphasizes the intent of a program and the static description of relationships and properties that hold in a program regardless of the computing context, thus easing understanding a computer program and reasoning about it. Unlike procedural languages, the effect of logic programming statements is not dependent on the context (i.e., the state of the computer when the preceding statements were executed).

b) Functional programming: The functional programming paradigm considers computation to be the evaluation of mathematical functions—that are not dependent on state and will always provide the same output for the same input. The main reason for the importance of functional programs is due to their direct correspondence with mathematical objects, which makes it easier to reason about them [69]. The functional paradigm avoids variables, or more technically—mutable state (i.e., variables whose values can be changed), and encourages a function-based programming worldview instead. By avoiding mutable state, the source of numerous subtle bugs in imperative-style programming languages, verification of programs become more simple. In functional programming, execution of a program means evaluation of the expression represented by the functional program. The functional programming style makes no use of variables. Instead of loops, the functional program makes use of recursive functions (i.e., functions that are defined in terms of themselves).

The main downfall of imperative programming is in race conditions when concurrency is supported. Race conditions are much harder to detect and fix since they may arise of nondeterministic interleavings of concurrent threads (which may interleave in a myriad different ways). Imperative programming is always vulnerable to race conditions since it relies on mutable state. Functional programming puts up much better with such race conditions since a pure functional language has no mutable state. Since the future of programming is in concurrency and parallelism, functional programming is increasingly migrating from fringes of the programming world to the mainstream [66]. In summary, mutations allowed in the imperative programming paradigm severely limit any opportunities for automatic parallel execution, while the lack of dependencies in the (purely) functional paradigm presents great opportunities for automatic parallel execution.

The functional programming is based on the theoretical underpinnings of Alonzo Church's *lambda calculus* [70], proposed in the 1930's, which defines rules about using unnamed functions for representing and evaluating expressions. Lambda calculus, although originally intended as a formal logical system for mathematics is in fact a completely general programming language and defines a family of prototype programming languages. Many modern programming languages C++, Python, JavaScript, Ruby, Java 8, etc. borrow from the programming style of lambda calculus, following the lead of the Lisp programming language—which was the first mainstream language to include anonymous functions known as lambda functions. Two important features of lambda calculus is that it is functional—i.e., it is based on the concept of a mathematical function and include notation for function application and abstraction—and that is higher-order—i.e., it provides a systematic formalism and notation to deal with operators whose

[12] Almost every successful large-scale application of parallelism, e.g., SQL server, LINQ, MapReduce, etc., has been declarative and value-oriented [66]. This trend bodes well for the use of declarative programming, especially functional programming, in parallel computing.

input and output may be other operators. The lambda calculus model significantly differs from the Turing model of a store with evolving state [71]. Interestingly, the Turing model and lambda calculus were invented in the same year, 1936. Turing showed in 1937 that both these models were equivalent and in fact defined the same class of computable functions. In any case, computer programs and mathematical proofs are directly related as the system of formal logic and computational calculi are analogous—the famous "Curry–Howard correspondence" expresses the isomorphism between proof structures and functional spaces [72].

Popular functional programming languages include Lisp, invented by the AI pioneer John McCarthy, Haskell [73], Caml, OCaml, Scala, etc. Historically, most successful languages have been written for specific purposes—e.g., Lisp was created for artificial intelligence, Fortran for numerical computation, and Prolog for natural language processing. The *raison d'etre* for ML has been the need of an efficient language for theorem proving [74]. ML originated as the metalanguage (thus its name ML) of the famous theorem proving system called Edinburgh LCF [75] for writing theorem proving algorithms in formal deductive calculus. ML was designed to have the full power of higher-order functional programming so that it could represent necessary inference rules and proof strategies. Since early time, functional languages and theorem proving (and formal verification in general) have been intimately intertwined. (Edinburgh) ML has spawned a wide range of ML-based descendant languages including Standard ML (SML) and OCaml. OCaml is a programming language specifically designed for writing theorem provers, with numerous major systems being written in it (e.g., SLAM verification system from Microsoft, HOL Light theorem prover, etc.). The OCaml language, being perfectly suited for symbolic manipulations, is used extensively by the Coq proof assistant which is used extensively for the verification of purely functional programs. Similarly, the SLAM verification system, proposed by Microsoft, also used OCaml programming language. The ACL2 ("A Computational Logic for Applicative Common Lisp") theorem prover is also composed of a first-order, purely functional subset of Common Lisp.

B. Application of Logic and Programming Languages in Networking

1) Algebra and Logic in Networking: In networking context, algebra can be viewed as a concise language useful for describing combinatorial problems. Researchers have applied algebraic ideas to network routing through algebraic path finding methods that exploit the fact that numerous practical network problems are in fact instances of the same abstract "algebraic path problem" (e.g., a classical example of an abstract algebraic path problem is shortest path routing) [248]. Routing algebra meta-language (RAML), which builds upon Sobrinho's *Routing algebra* [249], was proposed by Griffin in the "metarouting" project [189]. Metarouting aims at equipping network operators with the ability to define their own routing protocols in a high-level declarative manner using a domain-specific language customized for specification, verification, and implementation of routing path metrics. Sobrinho's Routing algebra [249], which can be understood as generalization of shortest path routing, is expressive enough to adequately model complex policy-based routing typified by ubiquitous the Border Gateway Protocol (BGP) routing protocol. A key feature of the metalanguage proposed for metarouting, which is especially relevant to our subject topic, is that algebraic properties required for guaranteeing correctness can be automatically derived.

2) Declarative Programming in Networking: Adoption of declarative programming languages is a manifestation of a contemporary trend in networking, brought on by the need to fix an ailing inflexible network architecture—and by software defined networking in particular, in which advanced programming techniques and database techniques are increasingly being applied to networking [220]. We present two examples of SDN declarative languages: *i*) the flow management language (FML) is a declarative language for SDN [250] designed for network operators so that static network policies may be written and maintained more efficiently; *ii*) the NetCore language [63] is a high-level declarative language proposed for SDN that allows programmer to describe what behavior is desired and not necessarily describe how to realize the implementation of that behavior. We will discuss SDN programming languages in more detail in Section VII-D.

a) Logic programming in networking: There has been a lot of interest in using declarative logic programming languages for simplifying the implementation of Internet protocols. They have been previously used for writing parsers (like the "yet another compiler-compiler" (yacc) parser tool [251]) for application layer protocols [252], declarative routing [253], and declarative networking [220]. The basic insight behind declarative networking is the realization that recursive query languages are a natural fit for network protocols which essentially deal with computing and maintaining distributed state (such as information about routes, sessions, etc.) across the network. Network Datalog (NDlog) is a data and query model that has been proposed for declarative networking. NDlog, which implements a network specific subset of Datalog and supports distributed programming, exposes the partitioning of data across nodes and the link graph of the network. This makes the implementation much more amenable to static analysis and verifiable using other formal verification techniques such as general-purpose theorem provers. It has been shown that declarative implementations of popular protocols can be done much more concisely and efficiently while also allowing extensibility and safety [220]. Logic programming languages have recently been proposed for SDNs [254], FlowLog: [255], with researchers also exploring declarative network verification [256]. In another work, Kazemian *et al.* have implemented a FML-like language in a Prolog frontend to enable network administrators to specify high-level policies [61].

b) Functional programming in networking: With the recent paradigm shift in networking brought on by SDN, a clear trend of preferring high-level declarative languages, domain-specific languages (DSL), functional languages—and more specifically, *functional reactive programming* (FRP)—for programming SDNs (both the SDN controller as well as SDN

applications) is emerging. Much of the recent work in SDN programming has followed the declarative programming coupled with the FRP paradigm [62], [257], [258]. This trend is helped by ample foundational research in these fields in the programming and databases community, and by the verifiability properties of functional languages. Nettle [221] is a SDN specific language implemented as a domain-specific language in the functional programming language Haskell. Nettle adopts the design methodology of domain-specific languages (DSL) research, and is built in the paradigm of FRP [259]. Nettle has been used for providing a comprehensive abstraction calculation constructs for configuring BGP policies. In a similar work, Procera [257] is a domain-specific language embedded in Haskell that can be used to specify high-level dynamic reactive network control policies. In other work, the Frenetic project [229] defines a family of domain-specific languages for specifying high-level network policies. In the initial work in the Frenetic project [62], two sub-languages were proposed: *i*) a high-level declarative network query language—which enable Frenetic programs to read the network state using constructs for filtering, grouping, splitting, limiting, aggregating, etc., and *ii*) a general purpose FRP-based network policy management library—using which the policy to govern the forwarding of packets through the network can be defined. The Frenetic framework borrows extensively from the FRP languages like Yampa [260], etc., and reuses many of the proposed primitives. In more recent work, Pyretic [258] is an example DSL in the Frenetic family which supports composable policies constructed from a set of fundamental constructs such as basic policies and combinators along with associated techniques for compiling these techniques to OpenFlow switches.

C. What is New About SDN

In traditional networking, the complex intricacies of a vertically integrated network architecture largely ruled out applications of formal methods to the domain of networking. This resulted in ad-hoc management of networks by "masters of complexity" [31]—network administrators who kept networks running mainly through intuition and judgment honed through experience with a very limited tool-set. Fortunately, the recent SDN architecture is much cleaner and offers an opportunity at rethinking networking management and troubleshooting [232]. There are three reasons for the optimistic evaluation of verification prospects of SDNs: firstly, the control plane that previously ran as distributed algorithms across individual devices has now been refactored into a single program that runs on the controller; secondly, the heterogeneity in traditional networking—in devices, configuration interfaces, vendors, and softwares—has given way to stock programmable switches supporting standard interfaces with precise semantics [63]; lastly, it is envisioned that the core network, or the *fabric*, in the new SDN architecture will be purely hardware (finite state) and is thus amenable to efficient application of verification techniques [29]. These new degrees of freedom enabled by SDN have ignited a renewed resolve in the networking community of applying formal methods to networking and to put networking on a solid theoretical foundation [163], [263], [264].

D. SDN Programming Languages

As pointed out earlier, there is an increasing trend in using declarative programming techniques, and techniques that have been successful in deductive databases community, in networking. The use of such techniques also enables importantly the ability to perform network verification. There has been some work in this regard [256] in which the task of formal specification is performed through declarative networking code, using Network Datalog (NDLog), a distributed variant of Datalog, while verification is done through a general-purpose theorem prover.

Various SDN specific programming languages have been proposed recently (e.g., Frenetic [229], NetCore [63], [265], Pyretic [258], and NetKat [58], etc.). These network programming languages enable programmers, in line with the vision of software defined networks, to define the desired network behavior at a high-level and the compiler then translates the high level abstract description to rules that are installed on the underlying hardware devices. The NetCore language [265] was initially designed to provide support for parallel composition and was later extended by Pyretic [258] for sequential composition. NetCore provides a rich set of programming primitives including predicates for filtering packets, actions for modifying and forwarding packets, and (parallel and sequential) composition operators for building elaborate policies from simpler ones. NetCore has even been formalized in Coq. NetKat is similar to NetCore and Pyretic, but additionally provides formal axiomatic semantics and a compiler based on an equational theory for reasoning about programs. NetKat is based on *Kleene algebra with tests* which is a mature framework that combines Kleene algebra—useful for reasoning about network structure—and Boolean algebra which is useful for reasoning about the predicates that define switch behavior. NetKat provides consistent reasoning principles that other network programming languages lack. In contrast to fore-mentioned languages, which have a functional bent and are suited for programming of centralized controllers, the DataLog[13] based declarative network programming language *NDLog* [220], [253] is a logic programming language suited to distributed programming.

E. Data Plane Verification

Various approaches have been proposed for data plane verification including *i*) static checking—in which the correctness is verified independently, *ii*) dynamic checking—in which new forwarding state is checked before being added, *iii*) automatic testing—where the correct behavior of the dataplane is checked automatically, and *iv*) interactive debugging—which aims at finding bugs in operational networks. The Anteater [161], FlowChecker [160], and Hassell [173] tools are example *static checking tools*. Various real-time *dynamic checking tools* have been proposed in literature including NetPlumber [61] and VeriFlow [192]. The NetPlumber tool uses a novel header space

[13]Datalog is a declarative logic programming language used as a query language for deductive databases. It is a simplified form of Prolog, and can be envisioned as a subset of Prolog sans the complex terms allowed by Prolog.

TABLE VII
SUMMARY OF APPLICATION OF FORMAL METHODS CATALYZED BY EMERGENCE OF SOFTWARE DEFINED NETWORKING (SDN)

Project and Reference	*Technique*	*Brief Summary*
Data Plane Verification		
FlowChecker [160], Anteater [161], HSA [173]	Static Checking	These tools perform static verification of the data plane of a network based on a snapshot of network state
NetPlumber & VeriFlow [192]	Dynamic Checking	These tools perform dynamic verification of the data plane using incremental recomputation techniques
ATPG [262]	Automatic Testing	ATPG is an automatic testing tool for generating test packets
NetSigtht, ndb [234]	Interactive Debuggers	Interactive debugging tools that operates passively
Control Plane Verification		
Scott et al. [238]	'Retrospective Causal Inference'	Proposed improving SDN troubleshooting by automatically identifying the minimum sequence of inputs responsible for causing a control software bug
Guha et al. [63]	Theorem Proving	Proposed a featherweight version of the OpenFlow protocol, and used the Coq tool for verifying the network controller [163]
Reitblatt et al.	Theorem Proving	Ensuring per-packet and per-flow consistency of network updates using the Coq prover
NICE [159]	Symbolic Execution & Model Checking	Performs symbolic execution of OpenFlow applications while applying model checking to explore the entire state space of the network
FlowLog [256]	Model Checking	Proposed a declarative finite-state language for programming SDN controllers that balances expressiveness and analysis and is amenable to model checking
Sethi et al. [263]	Model Checking	Proposed new abstractions for model checking SDN controllers

analysis for performing a real time network policy check, while the VeriFlow tool verifies network invariants—e.g., lack of access control violations, absence of routing loops, blackholes, etc.—in real time and presents a diagnostic report in case of a violation. The Automatic Test Packet Generation (ATPG) tool is an automatic testing tool that automatically generates test packets [261]. The ATPG verifies full reachability in a network, using minimal network of test packets by using a heuristic solver for the min-set-cover problem, and detects anomalies by looking for persistent packet drops that are indicative of some software or hardware errors. Finally, the NetSigtht and the Network Debugger (ndb) tools are *interactive debugging tools* that operate passively without generating any new packets unlike the ATPG tool. The ndb tool [233]—the analogue of gdb debugger for programming—is like a network-wide path-aware tcpdump that builds packet histories which can be exploited by network analysis applications to verify the policy compliance of network data plane behavior.

F. Control Plane Verification

Various projects have aimed at verification of the control plane functionality of SDNs. In the SDN architecture, it is envisioned that network programs will run as SDN applications on top of a northbound API exposed by SDN controller. This will allow SDN applications to leverage the services of the SDN controller, which will be responsible for managing the distributed state through a southbound API like OpenFlow, while the SDN application can focus on using the state for the task it wishes to perform. It is anticipated that this architecture will allow innovation to flourish and the development of numerous network based applications. In such an environment, it is necessary to ensure that we have tools available for testing and verifying such SDN applications. Canini *et al.* present their NICE framework for testing OpenFlow applications [159]. Kuzniar *et al.* have proposed another framework, named SOFT, for verifying OpenFLow switch interoperability. There also has been work on computationally verifying network programs in the Coq mechanical proof tool [266].

There also has been work on isolating fault inducing inputs to SDN control software [237], controller verification [63], and ensuring per-packet and per-flow consistency of network updates [178]. The problem of verifying a generic SDN controller—which in its general setting is Turing complete (e.g., NOX, Floodlight, etc.)—is undecidable. Guha *et al.* have proposed a method of using for machine verification of network controllers [63]. FlowLog [255] is a declarative, finite-state, language for programming SDN controllers that balances expressiveness and analysis and is amenable to model checking. In another model checking based work, Sethi *et al.* [262] have proposed new data state and network state abstractions that can be used for model checking SDN controllers more efficiently. The Frenetic framework [229] incorporates features to help achieve per-packet and per-flow consistency during network updates [178]. The safe update protocol proposed in [178] builds upon approaches that use incremental recomputation (e.g., Anteater [161], VeriFlow [192], etc.), which may have a transient stage in which the property to be verified may be violated, by ensuring that the property under check also holds during the transient stage.

A representative summary of the applications of formal verification techniques for data plane and control plane verification is presented separately in Table VII.

VIII. OPEN ISSUES AND FUTURE WORK

The area of formal methods and verification is vast with various mature tools and techniques available. With networking being fundamentally important to all aspects of life including government, defence, industry, finance, etc., networks are in dire need of provably correct mechanisms. Notwithstanding the lack of any major breakthroughs made by formal methods in traditional networking, architectural support from SDN along with its clean abstractions provide a source of optimism for the future of formal methods in networking. The nascent field of network verification is wide open and is ripe for further exploration. In this section, we will point a few important open issues and highlight possible future work.

A. Scalable Formal Verification for Large Networks

Advanced in technologies such as BDDs and SAT solvers have extended the state of the art considerably in recent years.

However, more work needs to be done for current formal verification techniques to scale to large networks and to verify large software systems (such as network applications and protocol implementations). An approach that has been proposed in literature for scaling to large networks is to utilize incremental recomputation thereby avoiding the overhead of redoing expensive static calculations. For example, NetPlumber [173] improves HSA [173], and Veriflow [192] improves Anteater [161], by supporting incremental computation. The incorporation of incremental recomputations techniques have allowed these tools to scale to reasonably large networks. In recent work, Yang and Lam have proposed an efficient real-time verifier of network properties using atomic predicates [90]. More work is needed in this area to exploit these recent works so that network verification for large networks can become both practical and efficient.

B. Automated Synthesis of Protocols and Configuration

Synthesis which promises to automatically derive implementations from specifications is an extremely important future goal that can improve programmer productivity. The problem of automated synthesis is at the frontier of verification research today [30]. Some important works in this regard include synthesis of network updates [199], synthesis of network controllers [200], synthesis of finite state controllers from temporal logic specifications, and synthesis of programs from examples by exploiting domain specific knowledge, etc. [138]. In the context of networking, more work needs to be done so that subsystems such as protocols, configurations, hardware may be synthesized through a high-level formal specification only in a user-friendly manner.

C. Specialized Network Verification Tools

In contrast to sophisticated well-honed design automation tools that are available for general hardware[14] and software industries, networking industry has almost no rigorous tools for verification. The vision of building a network CAD was articulated by McKeown. Encouragingly, as the SDN architecture is becoming mainstream, there is renewed interest in building specialized tools that will allow automated debugging, verification, and analysis. Some important issues that need to be addressed before such a vision can be realized are [232]: *i*) incorporating program semantics into network troubleshooting tools; *ii*) improved techniques for checking invariants; *iii*) development of new abstractions, especially in the SDN context, to facilitate troubleshooting.

D. Verification Abstractions for Modern Architectures

With the emergence of data centers and cloud computing, the programming world is undergoing a silent revolution with a growing trend towards parallel programming. Although, there are various approaches that have been proposed to support verification of concurrent programs, more research needs to be done to propose new clean simplified abstractions for building verified concurrently executing programs that can exploit modern multi-core and multi-processor architectures, and parallel programming style suited to data centers and cloud computing.

[14]The electronic design automation (EDA) industry in hardware design is a big market catering to a multi-billion dollar industry.

IX. Conclusion

We are in an exciting time in the networking world with recent innovations such as software defined networking and cloud computing fundamentally altering the landscape of the networking world. Keeping in mind the criticality of the Internet infrastructure, assuring the correct behavior of various subsystems of the Internet has become essential. There is great interest in applying the vast amount of work that has been done in the community of formal methods and verification to networks. The work in formal methods draws upon many diverse fields such as logic, theoretical computer science, programming languages, mathematics, etc., and hence appears daunting to a non-specialist. In this work, we present a detailed description of the various techniques used in formal methods and verification while providing necessary background and references to important works. We also present a detailed survey of the application of formal methods in the networking context. Finally, we have also identified some important research directions that can be pursued in future work.

References

[1] J. Day, *Patterns in Network Architecture: A Return to Fundamentals*. Englewood Cliffs, NJ, USA: Prentice-Hall, 2007.
[2] S. Garfinkel, "History's worst software bugs," Wired News, Nov. 2005.
[3] G. Tassey, "The economic impacts of inadequate infrastructure for software testing," National Inst. Std. Technol., Gaithersburg, MD, USA, 2002, vol. 7007, RTI Project.
[4] S. U. Malik and S. U. Khan, "Formal methods in large-scale computing systems," *ITNOW*, vol. 55, no. 2, pp. 52–53, 2013.
[5] HD Moore, Security Flaws in Universal Plug and Play: Unplug, Don't Play, Jan. 2013. [Online]. Available: https://community.rapid7.com/community/infosec/blog/2013/01/29/security-flaws-in-universal-plug-and-play-unplug-dont-play
[6] C. Barker, "The top 10 IT disasters of all time," [Online]. Available: http://www.zdnet.com/news/the-top-10-it-disasters-of-all-time/177729. Accessed: 2013-02-21.
[7] M. Cabural, "Facebook Inc (FB) Awards Biggest Bug Bounty To Brazilian Engineer," [Online]. Available: http://www.valuewalk.com/2014/01/facebook-inc-fb-awards-biggest-bug-bounty/. Accessed: 2013-02-21.
[8] D. Oppenheimer, A. Ganapathi, and D. A. Patterson, "Why do Internet services fail, and what can be done about it?" in *Proc. USENIX Symp. Internet Technol. Syst.*, Seattle, WA, USA, 2003, vol. 4, pp. 1–15.
[9] J. Rexford and P. Zave, "Report of the DIMACS working group on abstractions for network services, architecture, and implementation," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 1, pp. 56–59, Jan. 2012.
[10] P. Zave, "Experiences with protocol description," in *Proc. WRIPE*, 2011, pp. 1–6.
[11] C. Kern and M. R. Greenstreet, "Formal verification in hardware design: A survey," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 4, no. 2, pp. 123–193, Apr. 1999.
[12] G. Bochmann and C. Sunshine, "Formal methods in communication protocol design," *IEEE Trans. Commun.*, vol. COM-28, no. 4, pp. 624–631, Apr. 1980.
[13] G. J. Holzmann, "Design and validation of protocols: A tutorial," *Comput. Netw. ISDN Syst.*, vol. 25, no. 9, pp. 981–1017, Apr. 1993.
[14] K. Bhargavan, D. Obradovic, and C. A. Gunter, "Formal verification of standards for distance vector routing protocols," *J. ACM*, vol. 49, no. 4, pp. 538–576, Jul. 2002.
[15] J. Jürjens, *Secure Systems Development With UML*. Berlin, Germany: Springer-Verlag, 2005.

[16] D. M. Buede, *The Engineering Design of Systems: Models and Methods*, vol. 55. Hoboken, NJ, USA: Wiley, 2011.

[17] P. Godefroid, "Model checking for programming languages using VeriSoft," in *Proc. 24th ACM SIGPLAN-SIGACT Symp. Principles Program. Lang.*, 1997, pp. 174–186.

[18] K. Bhargavan *et al.*, "Verisim: Formal analysis of network simulations," *IEEE Trans. Softw. Eng.*, vol. 28, no. 2, pp. 129–145, Feb. 2002.

[19] H. Chen, D. Dean, and D. Wagner, "Model checking one million lines of C code," in *Proc. NDSS*, 2004, vol. 4, pp. 171–185.

[20] P. Zave, "Using lightweight modeling to understand chord," *SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 2, pp. 49–57, Apr. 2012.

[21] A. Sobeih, M. Viswanathan, D. Marinov, and J. Hou, "Finding bugs in network protocols using simulation code and protocol-specific heuristics," in *Formal Methods and Software Engineering*, vol. 3785, *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 2005, pp. 235–250.

[22] Z. Lu, C. Steinmuller, and S. Mukhopadhyay, "Towards formal verification of a commercial wireless router firmware," in *Proc. IEEE 37th Annu. COMPSAC*, Jul. 2013, pp. 639–647.

[23] "Running code vs. formal testing methods," [Online]. Available: http://www.ietf.org/mail-archive/web/ietf/current/msg10577.html. Accessed: 2013-09-30.

[24] G. Holzmann, "OOPSLA keynote: Scrub and SPIN: Stealth use of formal methods in software development," in *Proc. 24th ACM SIGPLAN Conf. Companion Obj. Orient. Program. Syst. Lang. Appl.*, 2009, p. 4.

[25] "International Conference on Formal Techniques for Networked and Distributed Systems," [Online]. Available: http://www.informatik.unitrier.de/~ley/db/conf/forte/. Accessed: 2013-09-12.

[26] [Online]. Available: http://www.cs.cornell.edu/conferences/formalnetworks/. Accessed: 2013-10-1.

[27] F. Babich and L. Deotto, "Formal methods for specification and analysis of communication protocols," *IEEE Commun. Surveys Tuts.*, vol. 4, no. 1, pp. 2–20, 2002.

[28] J. Woodcock, P. G. Larsen, J. Bicarregui, and J. Fitzgerald, "Formal methods: Practice and experience," *Proc. ACM CSUR*, vol. 41, no. 4, p. 19, Oct. 2009.

[29] S. Zhang, S. Malik, and R. McGeer, "Verification of computer switching networks: An overview," in *Automated Technology for Verification and Analysis*. Berlin, Germany: Springer-Verlag, 2012, pp. 1–16.

[30] N. Lopes, N. Bjørner, P. Godefroid, and G. Varghese, "Network verification in the light of program verification," 2013.

[31] "Scott Shenker's talk at Stanford," 2013. [Online]. Available: http://www.youtube.com/watch?v=WabdXYzCAOU. Accessed: 2013-09-12.

[32] H. Scholz, *Concise History of Logic*, vol. 94. New York, NY, USA: Philosophical Library, 1961.

[33] M. Ben-Ari, *Mathematical Logic for Computer Science*. New York, NY, USA: Springer-Verlag, 2012.

[34] A. R. Bradley and Z. Manna, *The Calculus of Computation: Decision Procedures With Applications to Verification*. Berlin, Germany: Springer-Verlag, 2007.

[35] J. Y. Halpern *et al.*, "On the unusual effectiveness of logic in computer science," *Bull. Symbolic Logic*, vol. 7, no. 2, pp. 213–236, Jan. 2001.

[36] M. Huth and M. Ryan, *Logic in Computer Science: Modelling and Reasoning About Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[37] S. Russell, *Artificial Intelligence: A Modern Approach, 2/E*. Chennai, India: Pearson Education India, 2003.

[38] K. J. Devlin, *Logic and Information*. Cambridge, U.K.: Cambridge Univ. Press, 1995.

[39] J. Franco and J. Martin, "A history of satisfiability," in *Handbook Satisfiability*, vol. 185. Amsterdam, The Netherlands: IOS Press, 2009, pp. 3–74.

[40] D. Makinson, *Sets, Logic and Maths for Computing*. London, U.K.: Springer-Verlag, 2012.

[41] K. Devlin, *Sets Functions, and Logic: An Introduction to Abstract Mathematics*. Boca Raton, FL, USA: CRC Press, 2003.

[42] O. Strichman, *Decision Procedures: An Algorithmic Point of View*. Berlin, Germany: Springer-Verlag, 2010.

[43] J. Harrison, "The HOL light theory of Euclidean space," *J. Autom. Reason.*, vol. 50, no. 2, pp. 173–190, Feb. 2013.

[44] T. Mhamdi, O. Hasan, and S. Tahar, "Formalization of measure theory and Lebesgue integration for probabilistic analysis in HOL," *Proc. ACM Trans. Embedded Comput. Syst.*, vol. 12, no. 1, pp. 13:1–13:23, Jan. 2013.

[45] C. A. R. Hoare, "An axiomatic basis for computer programming," *Commun. ACM*, vol. 12, no. 10, pp. 576–580, Oct. 1969.

[46] K. R. Apt, "Ten years of Hoare's logic: A survey—Part I," *ACM Trans. Programm. Lang. Syst.*, vol. 3, no. 4, pp. 431–483, Oct. 1981.

[47] E. A. Emerson, "Temporal and modal logic," in *Handbook of Theoretical Computer Science, Volume B: Formal Models and Sematics (B)*. Cambridge, MA, USA: MIT Press, 1990, pp. 995–1072.

[48] A. Pnueli, "The temporal logic of programs," in *Proc. IEEE 18th Annu. Symp. Found. Comput. Sci.*, 1977, pp. 46–57.

[49] E. M. Clarke, E. A. Emerson, and A. P. Sistla, "Automatic verification of finite-state concurrent systems using temporal logic specifications," *ACM Trans. Programm. Lang. Syst.*, vol. 8, no. 2, pp. 244–263, Apr. 1986.

[50] L. Lamport, "What good is temporal logic?" in *Proc. IFIP Congr.*, 1983, vol. 83, pp. 657–668.

[51] D. M. Gabbay, I. Hodkinson, M. Reynolds, and M. Finger, *Temporal Logic: Mathematical Foundations and Computational Aspects*. Oxford, U.K.: Clarendon, 2000.

[52] Z. Manna and A. Pnueli, *Temporal Logic*. Berlin, Germany: Springer-Verlag, 1992.

[53] L. Lamport, "The temporal logic of actions," *ACM Trans. Programm. Lang. Syst.*, vol. 16, no. 3, pp. 872–923, May 1994.

[54] D. Jackson, "Software abstractions: Logic," in *Language, and Analysis*. Cambridge, MA, USA: MIT Press, 2006.

[55] E. Torlak and D. Jackson, "Kodkod: A relational model finder," in *Tools and Algorithms for the Construction and Analysis of Systems*. Berlin, Germany: Springer-Verlag, 2007, pp. 632–647.

[56] N. Feamster and H. Balakrishnan, "Towards a logic for wide-area Internet routing," in *Proc. ACM SIGCOMM Comput. Commun. Rev.*, 2003, vol. 33, pp. 289–300.

[57] D. Kozen, "Kleene algebra with tests," *ACM Trans. Programm. Lang. Syst.*, vol. 19, no. 3, pp. 427–443, May 1997.

[58] C. J. Anderson *et al.*, "NetKAT: Semantic foundations for networks," in *Proc. 34th Annu. ACM SIGPLAN Conf. Programm. Lang. Des. Implementation*, Seattle, WA, USA, 2013, pp. 113–126.

[59] J. C. Baeten, T. Basten, T. Basten, and M. Reniers, *Process Algebra: Equational Theories of Communicating Processes*, vol. 50. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[60] H. R. Nielson and F. Nielson, *Semantics With Applications: An Appetizer*. London, U.K.: Springer-Verlag, 2007.

[61] P. Kazemian *et al.*, "Real time network policy checking using header space analysis," in *Proc. USENIX Symp. NSDI*, 2013, pp. 99–112.

[62] N. Foster *et al.*, "Frenetic: A network programming language," *ACM SIGPLAN Notices*, vol. 46, no. 9, pp. 279–291, Sep. 2011.

[63] A. Guha, M. Reitblatt, and N. Foster, "Machine-verified network controllers," in *Proc. PLDI*, 2013, pp. 483–494.

[64] H. Abelson, G. Sussman, and J. Sussman, *Structure and Interpretation of Computer Programs*. Cambridge, MA, USA: MIT Press, 1985.

[65] P. Alvaro *et al.*, "Boom analytics: Exploring data-centric, declarative programming for the cloud," in *Proc. 5th Eur. Conf. Comput. Syst.*, 2010, pp. 223–236.

[66] S. P. Jones, "The future is parallel, the future of parallel is declarative," 2012.

[67] J. M. Hellerstein, "The declarative imperative: Experiences and conjectures in distributed logic," *ACM SIGMOD Rec.*, vol. 39, no. 1, pp. 5–19, Mar. 2010.

[68] D. Maier and D. Warren, *Computing With Logic*. Redwood City, CA, USA: Benjamin Cummings, 1988.

[69] J. Harrison, "Introduction to Functional Programming," Univ. Cambridge, Cambridge, U.K., 1997, Lecture Notes.

[70] D. S. Scott, "λ-calculus: Then & now," in *Proc. ACM Turing Centenary Celebration*, 2012, pp. 1–33.

[71] R. Herken, *The Universal Turing Machine: A Half-Century Survey*, vol. 2. New York, NY, USA: Springer-Verlag, 1995.

[72] Z. Luo, *Computation and Reasoning: A Type Theory for Computer Science*. London, U.K.: Oxford Univ. Press, 1994.

[73] S. Thompson, *Haskell: The Craft of Functional Programming*, vol. 2. Reading, MA, USA: Addison-Wesley, 1999.

[74] L. C. Paulson, *ML for the Working Programmer*. Cambridge, U.K.: Cambridge Univ. Press, 1996.

[75] M. J. Gordon, R. Milner, and C. P. Wadsworth, *Edinburgh LCF: A Mechanised Logic of Computation*, vol. 78. New York, NY, USA: Springer-Verlag, 1979.

[76] D. Lee and M. Yannakakis, "Principles and methods of testing finite state machines—A survey," *Proc. IEEE*, vol. 84, no. 8, pp. 1090–1123, Aug. 1996.

[77] G. J. Holzmann, "An improved protocol reachability analysis technique," *Softw. Pract. Exp.*, vol. 18, no. 2, pp. 137–161, Feb. 1988.

[78] J. E. Hopcroft, *Introduction to Automata Theory, Languages, and Computation*. Chennai, India: Pearson Education, 2008.

[79] R. Alur, "Timed automata," in *Computer Aided Verification*. Berlin, Germany: Springer-Verlag, 1999, pp. 8–22.

[80] T. Murata, "Petri nets: Properties, analysis and applications," *Proc. IEEE*, vol. 77, no. 4, pp. 541–580, Apr. 1989.

[81] J. Billington, M. Diaz, and G. Rozenberg, *Application of Petri Nets to Communication Networks: Advances in Petri Nets*, vol. 1605. Berlin, Germany: Springer-Verlag, 1999.

[82] K. G. Larsen, P. Pettersson, and W. Yi, "UPPAAL in a nutshell," *Int. J. Softw. Tools Technol. Transf.*, vol. 1, no. 1/2, pp. 134–152, Dec. 1997.

[83] C. Wang, G. D. Hachtel, and F. Somenzi, *Abstraction Refinement for Large Scale Model Checking*. New York, NY, USA: Springer-Verlag, 2006.

[84] E. M. Clarke, O. Grumberg, and D. A. Peled, *Model Checking*. Cambridge, MA, USA: MIT Press, 1999.

[85] R. E. Bryant, "Symbolic Boolean manipulation with ordered binary decision diagrams," *ACM Comput. Surveys*, vol. 24, no. 3, pp. 293–318, Sep. 1992.

[86] H. R. Andersen, "An introduction to binary decision diagrams," IT Univ. Copenhagen, Copenhagen, Germany, 1997, Lecture Notes, Available Online.

[87] D. Knuth, *The Art of Computer Programming: Bitwise Tricks & Techniques; Binary Decision Diagrams, Volume 4, Fascicle 1*. Reading, MA, USA: Addison-Wesley, 2009.

[88] R. E. Bryant, "Binary decision diagrams and beyond: Enabling technologies for formal verification," in *Proc. IEEE/ACM ICCAD Dig. Tech. Papers*, 1995, pp. 236–243.

[89] R. McGeer, "New results on BDD sizes and implications for verification," in *Proc. Int. Workshop Logic Synthesis*, Berkeley, CA, USA, Jun. 2012. [Online]. Available: http://www.iwls.org/iwls2012/program.html

[90] H. Yang and S. S. Lam, "Real-time verification of network properties using atomic predicates," in *Proc. IEEE ICNP*, 2013, pp. 1–11.

[91] E. Al-Shaer, W. Marrero, A. El-Atawy, and K. ElBadawi, "Network configuration in a box: Towards end-to-end verification of network reachability and security," in *Proc. 17th IEEE ICNP*, 2009, pp. 123–132.

[92] G. J. Holzmann and M. H. Smith, "Automating software feature verification," *Bell Labs Tech. J.*, vol. 5, no. 2, pp. 72–87, Apr.–Jun. 2000.

[93] T. Ball and S. K. Rajamani, "The SLAM toolkit," in *Computer Aided Verification*. Berlin, Germany: Springer-Verlag, 2001, pp. 260–264.

[94] T. Ball, R. Majumdar, T. Millstein, and S. K. Rajamani, "Automatic predicate abstraction of C programs," in *Proc. ACM SIGPLAN Notices*, 2001, vol. 36, pp. 203–213.

[95] K. Bhargavan, C. Fournet, R. Corin, and E. Zalinescu, "Cryptographically verified implementations for TLS," in *Proc. 15th ACM Conf. Comput. Commun. Security*, 2008, pp. 459–468.

[96] M. Musuvathi, D. Y. Park, A. Chou, D. R. Engler, and D. L. Dill, "CMC: A pragmatic approach to model checking real code," *ACM SIGOPS Operat. Syst. Rev.*, vol. 36, no. SI, pp. 75–88, 2002.

[97] P. Camurati and P. Prinetto, "Formal verification of hardware correctness: Introduction and survey of current research," *Computer*, vol. 21, no. 7, pp. 8–19, Jul. 1988.

[98] A. Biere, *Handbook of Satisfiability*, vol. 185. Amsterdam, The Netherlands: IOS Press, 2009.

[99] L. Bordeaux, Y. Hamadi, and L. Zhang, "Propositional satisfiability and constraint programming: A comparative survey," *ACM Comput. Surveys*, vol. 38, no. 4, p. 12, 2006.

[100] J. Gu, P. W. Purdom, J. Franco, and B. W. Wah, *Algorithms for the Satisfiability (SAT) Problem*. New York, NY, USA: Springer-Verlag, 1999.

[101] M. R. Prasad, A. Biere, and A. Gupta, "A survey of recent advances in SAT-based formal verification," *Int. J. Softw. Tools Technol. Transf.*, vol. 7, no. 2, pp. 156–173, Apr. 2005.

[102] M. K. Ganai and A. Gupta, "SAT-based verification framework," in *SAT-Based Scalable Formal Verification Solutions*. New York, NY, USA: Springer-Verlag, 2007, pp. 247–261.

[103] L. De Moura and N. Bjørner, "Satisfiability modulo theories: Introduction and applications," *Commun. ACM*, vol. 54, no. 9, pp. 69–77, Sep. 2011.

[104] C. W. Barrett, R. Sebastiani, S. A. Seshia, and C. Tinelli, "Satisfiability modulo theories," in *Handbook Satisfiability*, vol. 185. Amsterdam, The Netherlands: IOS Press, 2009, pp. 825–885.

[105] C. P. Gomes, H. Kautz, A. Sabharwal, and B. Selman, "Satisfiability solvers," in *Handbook of Knowledge Representation. Foundations of Artificial Intelligence*, vol. 3. New York, NY, USA: Elsevier, 2008, pp. 89–134.

[106] N. Een and N. Sörensson, "Minisat: A SAT solver with conflict-clause minimization," in *Proc. SAT*, 2005, vol. 5, pp. 1–2.

[107] M. W. Moskewicz, C. F. Madigan, Y. Zhao, L. Zhang, and S. Malik, "Chaff: Engineering an efficient SAT solver," in *Proc. 38th Annu. Design Autom. Conf.*, 2001, pp. 530–535.

[108] L. De Moura and N. Bjørner, "Z3: An efficient SMT solver," in *Tools and Algorithms for the Construction and Analysis of Systems*. Berlin, Germany: Springer-Verlag, 2008, pp. 337–340.

[109] C.-L. Chang and R. C.-T. Lee, *Symbolic Logic and Mechanical Theorem Proving*, vol. 67. New York, NY, USA: Academic, 1973.

[110] M. Davis, G. Logemann, and D. Loveland, "A machine program for theorem-proving," *Commun. ACM*, vol. 5, no. 7, pp. 394–397, Jul. 1962.

[111] B. Brock, M. Kaufmann, and J. S. Moore, "ACL2 theorems about commercial microprocessors," in *Formal Methods in Computer-Aided Design*. Berlin, Germany: Springer-Verlag, 1996, pp. 275–293.

[112] L. C. Paulson and M. Wenzel, *Isabelle/HOL: A Proof Assistant for Higher-Order Logic*, vol. 2283. Berlin, Germany: Springer-Verlag, 2002.

[113] M. J. Gordon, *HOL: A Proof Generating System for Higher-Order Logic*. New York, NY, USA: Springer-Verlag, 1987.

[114] S. Owre, J. M. Rushby, and N. Shankar, "PVS: A prototype verification system," in *Automated DeductionCADE-11*. Berlin, Germany: Springer-Verlag, 1992, pp. 748–752.

[115] Y. Bertot and P. Castèran, *Interactive Theorem Proving and Program Development: Coq'Art: The Calculus of Inductive Constructions*. New York, NY, USA: Springer-Verlag, 2004.

[116] O. Grumberg and H. Veith, *25 Years of Model Checking: History, Achievements, Perspectives*, vol. 5000. Berlin, Germany: Springer-Verlag, 2008.

[117] E. A. Emerson, "The beginning of model checking: A personal perspective," in *25 Years of Model Checking*. Berlin, Germany: Springer-Verlag, 2008, pp. 27–45.

[118] T. A. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine, "Symbolic model checking for real-time systems," in *Proc. 7th Annu. IEEE Symp. LICS*, 1992, pp. 394–406.

[119] C. Baier *et al.*, *Principles of Model Checking*. Cambridge, MA, USA: MIT Press, 2008.

[120] E. M. Clarke, "The birth of model checking," in *25 Years of Model Checking*. Berlin, Germany: Springer-Verlag, 2008, pp. 1–26.

[121] "Webpage on 'Model Theory' in Stanford's Encyclopedia of Philosophy," [Online]. Available: http://plato.stanford.edu/entries/model-theory/. Accessed: 2013-10-3.

[122] D. Marker, *Model Theory: An Introduction*. New York, NY, USA: Springer-Verlag, 2002.

[123] K. L. McMillan, *Symbolic Model Checking*. New York, NY, USA: Springer-Verlag, 1993.

[124] E. Clarke, K. McMillan, S. Campos, and V. Hartonas-Garmhausen, "Symbolic model checking," in *Computer Aided Verification*. Berlin, Germany: Springer-Verlag, 1996, pp. 419–422.

[125] J. R. Burch, E. M. Clarke, K. L. McMillan, D. L. Dill, and L.-J. Hwang, "Symbolic model checking: 10^{20} states and beyond," *Inf. Comput.*, vol. 98, no. 2, pp. 142–170, Jun. 1992.

[126] K. L. McMillan, "The SMV system, symbolic model checking-an approach," Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU-CS-92-131, 1992.

[127] A. Cimatti *et al.*, "NuSMV 2: An opensource tool for symbolic model checking," in *Computer Aided Verification*. Berlin, Germany: Springer-Verlag, 2002, pp. 359–364.

[128] A. Biere, A. Cimatti, E. Clarke, and Y. Zhu, *Symbolic Model Checking Without BDDs*. Berlin, Germany: Springer-Verlag, 1999.

[129] E. Clarke, A. Biere, R. Raimi, and Y. Zhu, "Bounded model checking using satisfiability solving," *Formal Methods Syst. Des.*, vol. 19, no. 1, pp. 7–34, Jul. 2001.

[130] A. Armando, J. Mantovani, and L. Platania, "Bounded model checking of software using SMT solvers instead of SAT solvers," *Int. J. Softw. Tools Technol. Transf.*, vol. 11, no. 1, pp. 69–83, Jan. 2009.

[131] E. Clarke, D. Kroening, and F. Lerda, "A tool for checking ANSI-C programs," in *Tools and Algorithms for the Construction and Analysis of Systems*. Berlin, Germany: Springer-Verlag, 2004, pp. 168–176.

[132] A. Legay, B. Delahaye, and S. Bensalem, "Statistical model checking: An overview," in *Runtime Verification*. Berlin, Germany: Springer-Verlag, 2010, pp. 122–135.

[133] R. Fagin and J. Y. Halpern, "Reasoning about knowledge and probability," *J. ACM*, vol. 41, no. 2, pp. 340–367, Mar. 1994.

[134] C. Baier, B. Haverkort, H. Hermanns, and J.-P. Katoen, "Modelchecking algorithms for continuous-time Markov chains," *IEEE Trans. Softw. Eng.*, vol. 29, no. 6, pp. 524–541, Jun. 2003.
[135] M. Kwiatkowska, G. Norman, and D. Parker, "Stochastic model checking," in *Formal Methods for Performance Evaluation*. Berlin, Germany: Springer-Verlag, 2007, pp. 220–270.
[136] M. Kwiatkowska, G. Norman, and D. Parker, "PRISM: Probabilistic model checking for performance and reliability analysis," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 36, no. 4, pp. 40–45, Mar. 2009.
[137] M. Kwiatkowska, G. Norman, and J. Sproston, *Probabilistic Model Checking of the IEEE 802.11 Wireless Local Area Network Protocol*. Berlin, Germany: Springer-Verlag, 2002.
[138] R. Alur, T. A. Henzinger, I. Austria, and M. Y. Vardi, "Theory in Practice for System Design and Verification," 2013.
[139] R. Jhala and R. Majumdar, "Software model checking," *ACM Comput. Surveys*, vol. 41, no. 4, p. 21, Oct. 2009.
[140] K. Havelund and T. Pressburger, "Model checking Java programs using Java Pathfinder," *Int. J. Softw. Tools Technol. Transf.*, vol. 2, no. 4, pp. 366–381, Mar. 2000.
[141] T. A. Henzinger, R. Jhala, R. Majumdar, and G. Sutre, "Software verification with BLAST," in *Model Checking Software*. Berlin, Germany: Springer-Verlag, 2003, pp. 235–239.
[142] S. Agerholm and P. G. Larsen, "A lightweight approach to formal methods," in *Applied Formal Methods—FM-Trends 98*. London, U.K.: Springer-Verlag, 1999, pp. 168–183.
[143] D. Jackson, "Lightweight formal methods," in *FME 2001: Formal Methods for Increasing Software Productivity*. Berlin, Germany: Springer-Verlag, 2001, pp. 1–1.
[144] J. Jacky, *The Way of Z: Practical Programming With Formal Methods*. Cambridge, U.K.: Cambridge Univ. Press, 1996.
[145] D. Jackson, "Dependable software by design," *Sci. Amer.*, vol. 294, no. 6, pp. 68–75, Jun. 2006.
[146] Y. Xie, M. Naik, B. Hackett, and A. Aiken, "Soundness and its role in bug detection systems," in *Proc. Workshop Eval. Softw. Defect Detection Tools*, Chicago, IL, USA, 2005. [Online]. Available: http://www.cs.umd.edu/~pugh/SoftwareDefectWorkshop05/BugWorkshop05.pdf
[147] D. Engler and M. Musuvathi, "Static analysis versus software model checking for bug finding," in *Verification, Model Checking, Abstract Interpretation*. Berlin, Germany: Springer-Verlag, 2004, pp. 191–210.
[148] N. Feamster and H. Balakrishnan, "Detecting BGP configuration faults with static analysis," in *Proc. 2nd Conf. Symp. Netw. Syst. Design Implementation*, 2005, vol. 2, pp. 43–56.
[149] A. Bessey *et al.*, "A few billion lines of code later: Using static analysis to find bugs in the real world," *Commun. ACM*, vol. 53, no. 2, pp. 66–75, Feb. 2010.
[150] K. R. M. Leino, "Extended static checking: A ten-year perspective," in *Informatics*. Berlin, Germany: Springer-Verlag, 2001, pp. 157–175.
[151] C. Flanagan *et al.*, "Extended static checking for Java," *ACM Sigplan Notices*, vol. 37, no. 5, pp. 234–245, May 2002.
[152] C. Cadar and K. Sen, "Symbolic execution for software testing: Three decades later," *Commun. ACM*, vol. 56, no. 2, pp. 82–90, Feb. 2013.
[153] J. C. King, "Symbolic execution and program testing," *Commun. ACM*, vol. 19, no. 7, pp. 385–394, Jul. 1976.
[154] N. Nethercote and J. Seward, "Valgrind: A framework for heavyweight dynamic binary instrumentation," *ACM Sigplan Notices*, vol. 42, no. 6, pp. 89–100, Jun. 2007.
[155] R. E. Bryant, "Symbolic simulation—Techniques and applications," in *Proc. 27th ACM/IEEE Design Autom. Conf.*, 1991, pp. 517–521.
[156] R. E. Bryant and C.-J. H. Seger, "Formal verification of digital circuits using symbolic ternary system models," in *Computer-Aided Verification*. Berlin, Germany: Springer-Verlag, 1991, pp. 33–43.
[157] S. Narain, "Network configuration management via model finding," in *Proc. LISA*, 2005, vol. 5, pp. 15–15.
[158] R. W. Ritchey and P. Ammann, "Using model checking to analyze network vulnerabilities," in *Proc. IEEE Symp. S P*, 2000, pp. 156–165.
[159] M. Canini, D. Venzano, P. Peresini, D. Kostic, and J. Rexford, "A nice way to test openflow applications," in *Proc. NSDI*, Apr. 2012, p. 10.
[160] E. Al-Shaer and S. Al-Haj, "Flowchecker: Configuration analysis and verification of federated openflow infrastructures," in *Proc. 3rd ACM Workshop Assurable Usable Security Config.*, 2010, pp. 37–44.
[161] H. Mai *et al.*, "Debugging the data plane with anteater," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 290–301, Aug. 2011.
[162] G. G. Xie *et al.*, "On static reachability analysis of IP networks," in *Proc. IEEE 24th Annu. Joint INFOCOM*, 2005, vol. 3, pp. 2170–2183.
[163] A. Guha, M. Reitblatt, and N. Foster, "Formal foundations for software defined networks," presented at the Open Net Summit, Santa Clara, CA, USA, 2013.
[164] O. Hasan and S. Tahar, "Performance analysis and functional verification of the stop-and-wait protocol in HOL," *J. Autom. Reason.*, vol. 42, no. 1, pp. 1–33, Jan. 2009.
[165] M. Elleuch, O. Hasan, S. Tahar, and M. Abid, "Formal analysis of a scheduling algorithm for wireless sensor networks," in *Formal Engineering Methods*, vol. 6991, *LNCS*. Berlin, Germany: Springer-Verlag, 2011, pp. 388–403.
[166] S. Son, S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "Model checking invariant security properties in openflow," in *Proc. IEEE ICC*, 2013, pp. 1974–1979.
[167] S. Zhang and S. Malik, "SAT based verification of network data planes," in *Automated Technology for Verification and Analysis*. Zürich, Switzerland: Springer-Verlag, 2013, pp. 496–505.
[168] S. Zhang, A. Mahmoud, S. Malik, and S. Narain, "Verification and synthesis of firewalls using SAT and QBF," in *Proc. 20th IEEE ICNP*, 2012, pp. 1–6.
[169] B. Dutertre and L. De Moura, "The YICES SMT solver," vol. 2, p. 2, 2006. [Online]. Available: http://yices.csl.sri.com/tool-paper.pdf
[170] G. J. Holzmann, "The model checker SPIN," *IEEE Trans. Softw. Eng.*, vol. 23, no. 5, pp. 279–295, May 1997.
[171] P. Bulychev *et al.*, "UPPAAL-SMC: Statistical model checking for priced timed automata," arXiv preprint arXiv:1207.1272, 2012.
[172] T. Nelson, C. Barratt, D. J. Dougherty, K. Fisler, and S. Krishnamurthi, "The Margrave tool for firewall analysis," in *Proc. USENIX Large Install. Syst. Admin. Conf.*, 2010, pp. 1–115.
[173] P. Kazemian, G. Varghese, and N. McKeown, "Header space analysis: Static checking for networks," in *Proc. NSDI*, Apr. 2012, p. 9.
[174] M. Frappier, B. Fraikin, R. Chossart, R. Chane-Yack-Fa, and M. Ouenzar, "Comparison of model checking tools for information systems," in *Formal Methods and Software Engineering*. Berlin, Germany: Springer-Verlag, 2010, pp. 581–596.
[175] P. Zave, "Understanding SIP through model-checking," in *Principles, Systems and Applications of IP Telecommunications. Services and Security for Next Generation Networks*. Berlin, Germany: Springer-Verlag, 2008, pp. 256–279.
[176] S. Malik, S. Khan, and S. Srinivasan, "Modeling and analysis of state-of-the-art VM-based cloud management platforms," *IEEE Trans. Cloud Comput.*, vol. 1, no. 1, pp. 1–1, Jan.–Jun. 2013.
[177] C. Killian, J. W. Anderson, R. Jhala, and A. Vahdat, "Life, death, the critical transition: Finding liveness bugs in systems code," in *Proc. NSDI*, 2007, pp. 243–256.
[178] M. Reitblatt, N. Foster, J. Rexford, C. Schlesinger, and D. Walker, "Abstractions for network update," in *Proc. ACM SIGCOMM Conf. Appl., Technol., Architect., Protocols for Comput. Commun.*, 2012, pp. 323–334.
[179] L. Liu, O. Hasan, and S. Tahar, "Formal reasoning about finite-state discrete-time Markov chains in HOL," *J. Comput. Sci. Technol.*, vol. 28, no. 2, pp. 217–231, Mar. 2013.
[180] L. Liu, O. Hasan, and S. Tahar, "Formal analysis of memory contention in a multiprocessor system," in *Formal Methods: Foundations and Applications*, vol. 8195, *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 2013, pp. 195–210.
[181] T. Mhamdi, O. Hasan, and S. Tahar, "Quantitative analysis of information flow using theorem proving," in *Formal Methods and Software Engineering*, vol. 7635, *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 2012, pp. 119–134.
[182] P. Zave, Formal Methods and Networking: Former Success, Current Failure 2012.
[183] X. Qie and S. Narain, "Using service grammar to diagnose BGP configuration errors," *Sci. Comput. Programm.*, vol. 53, no. 2, pp. 125–141, Nov. 2004.
[184] S. Bishop *et al.*, "Engineering with logic: HOL specification and symbolic-evaluation testing for TCP implementations," *ACM SIGPLAN Notices*, vol. 41, no. 1, pp. 55–66, Jan. 2006.
[185] S. Keshav, "Editor's message: Modeling," *Comput. Commun. Rev.*, vol. 42, no. 3, p. 3, Jul. 2012.
[186] J. P. Bowen and M. G. Hinchey, "Ten commandments of formal methods," *Computer*, vol. 28, no. 4, pp. 56–63, Apr. 1995.
[187] P. Zave, "A practical comparison of alloy and SPIN," in *Proc. IFIP Working Group 2.3 Programm. Methodol.*, 2012, pp. 1–9.
[188] M. Handley, "Why the Internet only just works," *BT Technol. J.*, vol. 24, no. 3, pp. 119–129, Jul. 2006.
[189] T. G. Griffin and J. L. Sobrinho, "Metarouting," in *Proc. ACM SIGCOMM Comput. Commun. Rev.*, 2005, vol. 35, pp. 1–12.

[190] T. Ridge, M. Norrish, and P. Sewell, "A rigorous approach to networking: TCP, from implementation to protocol to service," in *FM 2008: Formal Methods*. Berlin, Germany: Springer-Verlag, 2008, pp. 294–309.

[191] A. R. Khakpour and A. X. Liu, "Quantifying and querying network reachability," in *Proc. IEEE 30th ICDCS*, 2010, pp. 817–826.

[192] A. Khurshid, W. Zhou, M. Caesar, and P. Godfrey, "Veriflow: Verifying network-wide invariants in real time," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 4, pp. 467–472, Sep. 2012.

[193] S. Gutz, A. Story, C. Schlesinger, and N. Foster, "Splendid isolation: A slice abstraction for software-defined networks," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw.*, 2012, pp. 79–84.

[194] X. Ou, S. Govindavajhala, and A. W. Appel, "MulVAL: A logic-based network security analyzer," in *Proc. 14th USENIX Security Symp.*, 2005, pp. 1–16.

[195] E. S. Al-Shaer and H. H. Hamed, "Discovery of policy anomalies in distributed firewalls," in *Proc. IEEE 23rd Annu. Joint Conf. INFOCOM*, 2004, vol. 4, pp. 2605–2616.

[196] N. Kothari, R. Mahajan, T. Millstein, R. Govindan, and M. Musuvathi, "Finding protocol manipulation attacks," *SIGCOMM–Comput. Commun. Rev.*, vol. 41, no. 4, pp. 26–37, Aug. 2011.

[197] M. G. Gouda and A. X. Liu, "Structured firewall design," *Compu. Netw.*, vol. 51, no. 4, pp. 1106–1120, Mar. 2007.

[198] A. Wang *et al.*, "Formally verifiable networking," in *Proc. HotNets ACM SIGCOMM*, 2009, pp. 1–42.

[199] A. Noyes, T. Warszawski, and N. Foster, "Toward synthesis of network updates," in *Proc. Workshop SYNT*, 2013, pp. 1–16.

[200] A. Wang, S. Moarref, U. Topcu, B. T. Loo, and A. Scedrov, "Automated synthesis of reactive controllers for software-defined networks," in *Proc. 3rd Int. WRIPE*, 2013, pp. 1–6.

[201] S. Budkowski and P. Dembinski, "An introduction to Estelle: A specification language for distributed systems," *Comput. Netw. ISDN Syst.*, vol. 14, no. 1, pp. 3–23, Mar. 1987.

[202] A. Fehnker, L. Van Hoesel, and A. Mader, "Modelling and verification of the LMAC protocol for wireless sensor networks," in *Integrated Formal Methods*. Berlin, Germany: Springer-Verlag, 2007, pp. 253–272.

[203] P. Ballarini and A. Miller, "Model checking medium access control for sensor networks," in *Proc. IEEE 2nd ISoLA, Verification Validation*, 2006, pp. 255–262.

[204] S. U. R. Malik, S. K. Srinivasan, S. U. Khan, and L. Wang, "A methodology for OSPF routing protocol verification," in *Proc. 12th Int. Conf. ScalCom*, Changzhou, China, 2012, pp. 1–5.

[205] F. De Renesse and A. Aghvami, "Formal verification of ad-hoc routing protocols using SPIN model checker," in *Proc. 12th IEEE MELECON*, 2004, vol. 3, pp. 1177–1182.

[206] A. Fehnker *et al.*, "Automated analysis of AODV using UPPAAL," in *Tools and Algorithms for the Construction and Analysis of Systems*. Berlin, Germany: Springer-Verlag, 2012, pp. 173–187.

[207] C. Xiong, T. Murata, and J. Leigh, "An approach for verifying routing protocols in mobile ad hoc networks using Petri nets," in *Proc. IEEE 6th Circuits Syst. Symp. Emerging Technol.—Frontiers Mobile Wireless Commun.*, 2004, vol. 2, pp. 537–540.

[208] P. Höfner and A. McIver, "Statistical model checking of wireless mesh routing protocols," in *NASA Formal Methods*. Berlin, Germany: Springer-Verlag, 2013, pp. 322–336.

[209] J. A. Bergstra and J. W. Klop, "Verification of an alternating bit protocol by means of process algebra protocol," in *Mathematical Methods of Specification and Synthesis of Software Systems'85*. Berlin, Germany: Springer-Verlag, 1986, ser. Proceedings of the International Spring School Wendisch-Rietz, GDR, April 22–26, 1985, pp. 9–23.

[210] K. A. Bartlett, R. A. Scantlebury, and P. T. Wilkinson, "A note on reliable full-duplex transmission over half-duplex links," *Commun. ACM*, vol. 12, no. 5, pp. 260–261, May 1969.

[211] I. Suzuki, "Formal analysis of the alternating bit protocol by temporal Petri nets," *IEEE Trans. Softw. Eng.*, vol. 16, no. 11, pp. 1273–1281, Nov. 1990.

[212] J. Billington and G. E. Gallasch, *How Stop and Wait Protocols Can Fail Over the Internet*. Berlin, Germany: Springer-Verlag, 2003.

[213] J. Billington and B. Han, "Modelling and analysing the functional behaviour of TCPs connection management procedures," *Int. J. Softw. Tools Technol. Transf.*, vol. 9, no. 3/4, pp. 269–304, May 2007.

[214] O. Hasan and S. Tahar, "Performance analysis of ARQ protocols using a theorem prover," in *Proc. IEEE ISPASS*, 2008, pp. 85–94.

[215] S. Šimoňák, "Verification of communication protocols based on formal methods integration," *Acta Polytech. Hungarica*, vol. 9, no. 4, pp. 117–128, 2012.

[216] A. Armando and L. Compagna, "Automatic sat-compilation of protocol insecurity problems via reduction to planning," in *Formal Techniques for Networked and Distributed Sytems—FORTE 2002*. London, U.K.: Springer-Verlag, 2002, pp. 210–225.

[217] F. Belina and D. Hogrefe, "The CCITT-specification and description language SDL," *Comput. Netw. ISDN Syst.*, vol. 16, no. 4, pp. 311–341, Mar. 1989.

[218] T. Bolognesi and E. Brinksma, "Introduction to the ISO specification language LOTOS," *Comput. Netw. ISDN Syst.*, vol. 14, no. 1, pp. 25–59, Mar. 1987.

[219] M. Karsten, S. Keshav, S. Prasad, and M. Beg, "An axiomatic basis for communication," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 4, pp. 217–228, Oct. 2007.

[220] B. T. Loo *et al.*, "Declarative networking," *Commun. ACM*, vol. 52, no. 11, pp. 87–95, Nov. 2009.

[221] A. Voellmy and P. Hudak, "Nettle: Taking the sting out of programming network routers," in *Practical Aspects of Declarative Languages*. Berlin, Germany: Springer-Verlag, 2011, pp. 235–249.

[222] M. C. Yuang, "Survey of protocol verification techniques based on finite state machine models," in *Proc. Comput. Netw. Symp.*, 1988, pp. 164–172.

[223] G. J. Holzmann, *Design and Validation of Computer Protocols*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1991.

[224] J.-P. Queille and J. Sifakis, "Specification and verification of concurrent systems in CESAR," in *Proc. Int. Symp. Programm.*, 1982, pp. 337–351.

[225] B. Blanchet, "Security protocol verification: Symbolic and computational models," in *Proc. 1st Int. Conf. POST*, 2012, pp. 3–29.

[226] R. Lai, "A survey of communication protocol testing," *J. Syst. Softw.*, vol. 62, no. 1, pp. 21–46, May 2002.

[227] G. Cabodi, P. Camurati, and S. Quer, "Improved reachability analysis of large finite state machines," in *Proc. IEEE/ACM Int. Conf. Computer-Aided Design*, 1997, pp. 354–360.

[228] R. Sherwood *et al.*, "Carving research slices out of your production networks with openflow," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 1, pp. 129–130, Jan. 2010.

[229] "The Frenetic Research Project," [Online]. Available: http://www.frenetic-lang.org. Accessed: 2013-09-12.

[230] "What's Behind Network Downtime?—IBM," [Online]. Available: www-05.ibm.com/uk/juniper/pdf/200249.pdf. Accessed: 2013-09-30.

[231] N. Feamster, "Practical verification techniques for wide-area routing," *ACM Sigcomm Comput. Commun. Rev.*, vol. 34, no. 1, pp. 87–92, Jan. 2004.

[232] B. Heller *et al.*, "Leveraging SDN layering to systematically troubleshoot networks," in *Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw.*, 2013, pp. 37–42.

[233] N. Handigol, B. Heller, V. Jeyakumar, D. Maziéres, and N. McKeown, "Where is the debugger for my software-defined network?" in *Proc. 1st Workshop Hot Topics Softw. Defined Netw.*, 2012, pp. 55–60.

[234] N. A. Handigol, "Using packet histories to troubleshoot networks," Ph.D. dissertations, Stanford Univ., Stanford, CA, USA, 2013.

[235] A. Wundsam, D. Levin, S. Seetharaman, and A. Feldmann, "Ofrewind: Enabling record and replay troubleshooting for networks," in *Proc. USENIX ATC*, 2011, p. 29.

[236] R. C. Scott, A. Wundsam, K. Zarifis, and S. Shenker, "What, where, when: software fault localization for SDN," EECS Dept., Univ. California, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2012-178, 2012.

[237] C. Scott *et al.*, "How did we get into this mess? Isolating fault-inducing inputs to SDN control software," EECS Dept., Univ. California, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2013-8, 2013.

[238] P. Reynolds *et al.*, "PIP: Detecting the unexpected in distributed systems," in *Proc. NSDI*, 2006, vol. 6, pp. 115–128.

[239] C. Scott *et al.*, "Automatic troubleshooting for SDN control software," 2013.

[240] G. Lowe, "Breaking and fixing the Needham–Schroeder public-key protocol using FDR," in *Tools and Algorithms for the Construction and Analysis of Systems*. Berlin, Germany: Springer-Verlag, 1996, pp. 147–166.

[241] B. Chess and J. West, *Secure Programming With Static Analysis*. Boca Raton, FL, USA: Pearson Education, 2007.

[242] C. Ramakrishnan and R. Sekar, "Model-based analysis of configuration vulnerabilities," *J. Comput. Security*, vol. 10, no. 1/2, pp. 189–209, 2002.

[243] D. M. Nicol, W. H. Sanders, and K. S. Trivedi, "Model-based evaluation: From dependability to security," *IEEE Trans. Dependable Secure Comput.*, vol. 1, no. 1, pp. 48–65, Jan.–Mar. 2004.

[244] D. Antoš, V. Rehak, and J. Korenek, "Hardware router's lookup machine and its formal verification," in *Proc. ICN*, 2004, vol. 2, pp. 1–002.

[245] P. Curzon, The Formal Verification of the Fairisle ATM Switching Element 1994.
[246] D. Borrione, A. Helmy, L. Pierre, and J. Schmaltz, "A formal approach to the verification of networks on chip," *EURASIP J. Embedded Syst.*, vol. 2009, p. 2, 2009.
[247] T. van den Broek and J. Schmaltz, "Towards a formally verified network-on-chip," in *Proc. FMCAD*, 2009, pp. 184–187.
[248] J. S. Baras and G. Theodorakopoulos, "Path problems in networks," *Synthesis Lect. Commun. Netw.*, vol. 3, no. 1, pp. 1–77, 2010.
[249] J. L. Sobrinho, "An algebraic theory of dynamic network routing," *IEEE/ACM Trans. Netw.*, vol. 13, no. 5, pp. 1160–1173, Oct. 2005.
[250] T. L. Hinrichs, N. S. Gude, M. Casado, J. C. Mitchell, and S. Shenker, "Practical declarative network management," in *Proc. 1st ACM Workshop Res. Enterprise Netw.*, 2009, pp. 1–10.
[251] S. C. Johnson, "YACC: Yet another compiler-compiler," Bell Lab., Murray Hill, NJ, USA, 1975, vol. 32.
[252] R. Pang, V. Paxson, R. Sommer, and L. Peterson, "binpac: A yacc for writing application protocol parsers," in *Proc. 6th ACM SIGCOMM Conf. Internet Meas.*, 2006, pp. 289–300.
[253] B. T. Loo, J. M. Hellerstein, I. Stoica, and R. Ramakrishnan, "Declarative routing: Extensible routing with declarative queries," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 35, no. 4, pp. 289–300, Oct. 2005.
[254] N. P. Katta, J. Rexford, and D. Walker, "Logic programming for software-defined networks," in *Proc. Workshop Cross-Model Design Validation (XLDI)*, 2012, pp. 1–3.
[255] T. Nelson, A. Guha, D. J. Dougherty, K. Fisler, and S. Krishnamurthi, "A balance of power: Expressive, analyzable controller programming," in *Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw.*, 2013, pp. 79–84.
[256] A. Wang, P. Basu, B. T. Loo, and O. Sokolsky, "Declarative network verification," in *Practical Aspects of Declarative Languages*. Berlin, Germany: Springer-Verlag, 2009, pp. 61–75.
[257] A. Voellmy, H. Kim, and N. Feamster, "Procera: A language for high-level reactive network control," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw.*, 2012, pp. 43–48.
[258] C. Monsanto, J. Reich, N. Foster, J. Rexford, and D. Walker, "Composing software defined networks," in *Proc. NSDI*, Apr. 2013, pp. 1–14.
[259] Z. Wan and P. Hudak, "Functional reactive programming from first principles," *ACM SIGPLAN Notices*, vol. 35, no. 5, pp. 242–252, May 2000.
[260] P. Hudak, A. Courtney, H. Nilsson, and J. Peterson, "Arrows, robots, functional reactive programming," in *Advanced Functional Programming*. Berlin, Germany: Springer-Verlag, 2003, pp. 159–187.
[261] H. Zeng, P. Kazemian, G. Varghese, and N. McKeown, "Automatic test packet generation," in *Proc. 8th Int. Conf. Emerging Netw. Exp. Technol.*, 2012, pp. 241–252.
[262] D. Sethi, S. Narayana, and S. Malik, "Abstractions for model checking SDN controllers," in *Proc. Formal Methods Comput. Aided Design*, 2013, pp. 145–148.
[263] M.-K. Shin, K.-H. Nam, M. Kang, and J.-Y. Choi, "Formal specification and programming for SDN," in *Proc. IETF 84*, 2012, pp. 1–19.
[264] R. W. Skowyra, A. Lapets, A. Bestavros, and A. Kfoury, "Verifiably-safe software-defined networks for CPS," in *Proc. 2nd ACM Int. Conf. High Confidence Netw. Syst.*, 2013, pp. 101–110.
[265] C. Monsanto, N. Foster, R. Harrison, and D. Walker, "A compiler and run-time system for network programming languages," *ACM SIGPLAN Notices*, vol. 47, no. 1, pp. 217–230, Jan. 2012.
[266] G. Stewart, "Computational verification of network programs in coq," Certified Programs and Proofs 2013.

Junaid Qadir received the B.S. degree in electrical engineering from the University of Engineering and Technology, Lahore, Pakistan, and the Ph.D. degree in 2008 from the University of New South Wales, Sydney, Australia. He is currently an Assistant Professor at the School of Electrical Engineering and Computer Sciences (SEECS), National University of Sciences and Technology, Islamabad, Pakistan. He leads the Cognet Lab, SEECS, which is focused on solving algorithmic/networking problems in the domain of cognitive radio networks, wireless networks, and software-defined networks. His research interests span the fields of networking, algorithms, artificial intelligence, machine learning, and formal methods.

Osman Hasan received the Ph.D. degree from Concordia University, Montreal, QC, Canada. He is an Assistant Professor at the School of Electrical Engineering and Computer Sciences (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan. He is the Lab Director of the System Analysis and Verification (SAVE) Lab, SEECS. Prior to joining SEECS, NUST, he did his post-doctoral fellowship from the Hardware Verification Group, Concordia University. His main research interests include formal verification, interactive theorem proving, and higher-order logic.