Formal Methods for Mobile Ad Hoc Networks: A Survey

Wan Fokkink[1*] and Rob van Glabbeek[2]

[1*]Department of Computer Science, Vrije Universiteit Amsterdam, De Boelelaan 1111, 1081 HV Amsterdam, The Netherlands.
[2]School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh, EH8 9AB, United Kingdom.

*Corresponding author(s). E-mail(s): w.j.fokkink@vu.nl;
Contributing authors: rvg@cs.stanford.edu;

Abstract

In a mobile ad hoc network (MANET), communication is wireless and nodes can move independently. Properly analyzing the functional correctness, performance, and security of MANET protocols is a challenging task. A wide range of formal specification and analysis techniques have been employed in the analysis of MANET protocols. This survey presents an overview of rigorous formal analysis techniques and their applications, with a focus on MANET routing protocols. Next to functional correctness, also real-time properties and security are considered. Moreover, an overview is given of formal frameworks that target MANETs specifically, as well as mobility models that underlie performance analyses of MANET protocols. The aim is to give a comprehensive and coherent overview of this rather scattered field, in which a variety of rigorous formal methods have been applied to analyze different aspects of a wide range of MANET protocols.

Keywords: Formal methods, mobile ad hoc networks

1 Introduction

A mobile ad hoc network, abbreviated to MANET, is a wireless network in which the nodes are free to move independently, so that the network topology changes over time. Its origins date back to the 1970s, when the U.S. Defense Research developed the Packet Radio NETwork [1] and its follow-on the SURvivable Adaptive Network

[2]. Interest in MANETs has grown significantly over the last two decades, owing to the common availability of wireless communication devices, connecting e.g. cell phones and laptops. MANETs may dynamically self-organize and self-configure, which facilitates their employment for e.g. mobile robots and in dire circumstances such as an earthquake area. They are currently widely used in practice, notably in disaster relief and maritime applications.

Network connectivity in a MANET is typically based on broadcast communication, in which a message is received by all nodes within a certain range of the sender. A key challenge is to let nodes continuously maintain information needed to route data traffic through the network, over multiple hops from the source to the destination of a data packet. This is complicated by the fact that MANETs can grow very large and their nodes often have only restricted resources and need to share limited communication bandwidth.

A wide range of MANET protocols have been developed over the last 25 years. Their functional correctness and performance were mostly analyzed by means of simulations, through for instance the widely employed simulator ns-3. This offers a convenient way to evaluate and compare the performance of MANET protocols in large-scale networks of thousands of nodes and reproduce experiments [3]. However, adequately simulating wireless mobility is a tall order because important corner cases may easily be missed in the large spectrum of possible behaviors, and performance results tend to be sensitive to networking and user traffic profiles [4]. Furthermore, due to their open and dynamic nature, MANETs are vulnerable to attacks by malicious intruders, which makes it extra important to analyze their protocols from a security perspective. In view of these challenges, formal specification and analysis techniques have been applied to analyze MANET protocols. An additional advantage is that formal methods provide precise, unambiguous protocol specifications, compared to the informal textual descriptions of protocol standards.

Different formal modeling frameworks, especially a significant number of process calculi, were developed that target the specification and verification of MANET protocols. In particular, their languages include mechanisms to specify connectivity between network nodes and to let the network topology evolve over time. These frameworks have been applied successfully in the analysis of MANET protocols, in particular for routing. Not only were many of these protocols proven correct formally, also these analyses led to the detection of flaws and security vulnerabilities that induced adaptations in MANET protocol standards.

Coping with the huge number and unpredictability of possible mobility scenarios in a MANET is the key challenge in analyzing its protocols. Therefore it is of the essence to employ mathematical mobility models that are on the one hand comprehensive and at the other hand compact. Different mobility models of nodes in a MANET have been developed and employed in particularly performance analyses of MANET protocols.

The aim of the current survey is to give a comprehensive and coherent overview of this rather scattered field, in which a variety of formal methods have been applied to analyze different aspects of a wide range of MANET protocols, using different mobility models. We discuss analyses of routing protocols for MANETS using existing formal methods, addressing functional correctness as well as real-time and security properties.

It is also explained how these analyses have impacted specific protocol standards. We moreover consider several formal frameworks developed specifically for MANETs, with an emphasis on process calculi. Finally, different mobility models are discussed, capturing how nodes move through a network, and explain how such probabilistic models impact performance analyses of MANET protocols.

To arrive at an exhaustive list of research papers in this domain, we took the following steps. First, we performed searches in the DBLP database and Google Scholar with as search terms combinations of firstly formal/model/analysis and secondly MANET or a variant of this acronym (mobile/dynamic/ad hoc network). Furthermore, publication lists of prolific researchers in the field were scrutinized. Next, we performed snowballing by investigating for each selected paper on the one hand its reference list to look for older relevant papers, and on the other its Google Scholar entry to look for later relevant papers that cite the one at hand. An Achilles heel of this methodology is that it focused mostly on titles of papers, which is mitigated by the fact that in Google Scholar also bodies of papers were taken into account. The selected papers were grouped in coherent story lines, that show how the research field has progressed over the past 25 years. We discuss formal analysis techniques and tools developed especially for MANET protocols as well as notable case studies, and provide some directions for future research.

Formal methods are characterized by three ingredients: syntax, semantics, and analysis technique (see e.g. [5]). Formal methods come with an exactly defined syntax and a rigorous semantics. Analysis techniques that allow to provide a rigid correctness proof, notably theorem proving, or that perform an exhaustive analysis of the state space of model, notably model checking, are in [6] contrasted with what are called lightweight formal methods. Typical examples of the latter category, which do not provide an exhaustive analysis, are static code analysis and model animation. This survey focuses on the first category of rigorous, exhaustive formal methods, whereby we do take into account some techniques that are tilted toward the second category, notably statistical model checking and model-based conformance testing.

It should be kept in mind that formal analysis techniques tend to be applied to abstractions of protocol standards. First, because specifying such a standard in full detail is cumbersome. Second, because it can be infeasible to prove a formal model of the entire standard correct formally. This holds true especially for MANETs, for which the vast range of possible mobility scenarios can give rise to huge state spaces of protocol behavior. The aim of an abstraction is that all key aspects of the standard are included in the formal model, but inevitably an abstraction leads to a loss of information. In some cases a specification of a MANET protocol was proven correct formally, while the protocol later turned out to be flawed, due to the fact that the abstraction employed in the correctness proof lacked vital ingredients.

The formal analysis of MANET networks is a huge challenge, which has given rise to the development of important new concepts and featured many success stories, but is still an ongoing research effort. This survey gives an overview of work done in this area during the last two decades and discusses some challenges that lie ahead.

This survey is organized as follows. Section 2 gives an overview of analyses of MANET protocols using existing formal methods, i.e., not tailored to MANETs. This

section emphasizes routing protocols, and distinguishes functional correctness, real-time properties, and security aspects. Section 3 presents formal frameworks that were designed specifically for analyzing MANET protocols, with an emphasis on process calculi. Section 4 discusses different ways of modeling mobility in a MANET and how these are used in performance analyses of protocols. Finally, Section 5 provides conclusions and possible avenues for future research.

2 Analysis of Routing Protocols with Existing Formal Methods

Initially, formal verifications of MANETs focused on the specification and analysis of specific network protocols using existing formal methods that are not tailored to MANETs. In particular, the functional correctness, real-time performance, and security of routing protocols has been studied widely, as these constitute key challenges for MANETs. In link-state routing protocols, such as the Optimized Link State Routing (OLSR) protocol [7], nodes continuously gather information on the local network topologies at other nodes to build a view of the global topology, so that at all times routes can be computed locally. By contrast, on-demand protocols, such as the Ad-hoc On-Demand Distance Vector (AODV) routing protocol [8, 9], build a multi-hop path by letting the source node of this path send exploration messages through the network toward the destination node. These route request messages carry a hop count to keep track of the length of the path, in order to find a shortest path and abort the attempt if the destination is not found within a certain limit. In case an exploration message reaches the destination, route reply messages travel from the destination toward the source via the established path. If a link break is detected by a node, it sends a route error message in the opposite direction of affected routes, so that nodes on such paths cancel these routes.

Initially, especially model checking and theorem proving were promoted to analyze MANET protocols. Model checking allows one to generate the entire state space of a protocol for one particular network topology and automatically check whether certain requirements, formulated in some temporal logic, are satisfied in the entire state space. With interactive theorem one can prove such requirements mathematically for general network topologies, whereby the human verifier and the theorem proving tool work hand in hand.

2.1 Functional Correctness

AODV served as case study in a string of papers, in some cases formally proving its correctness, in others uncovering flaws, in particular concerning the formation of cyclic paths called loops. In early works [10, 11], case studies on a high-level specification of AODV highlight the strength of at that time novel model checking techniques. The first paper presents a novel predicate abstraction method to turn infinite-state systems into finite-state ones. The second paper propagates the strength of software model checking, where a piece of software is verified instead of an abstract model.

A notable early paper is [12], in which both the model checker SPIN [13] and the interactive theorem prover HOL [14] are used for the analysis of a preliminary

version of the AODV protocol. SPIN is applied to find different scenarios for AODV in which loops are formed. Moreover, loop freedom is proved for a stricter specification of AODV, with extra conditions that avoid these scenarios. The verification with HOL, under the assumption that nodes never delete routes, is based on an abstraction of hop counts and of sequence numbers, which indicate the freshness of routes. Correctness of this abstraction is left as an open question. In [15, p. 124] it is shown that a key invariant (i.e., a property that is satisfied in all reachable states) in this correctness proof, in essence originating from [8], does not hold for AODV.

Formal proofs of loop freedom for an updated version of AODV are presented in [16, 17]. In [18] however it is shown that loops can occur in this version of AODV. The reason for this discrepancy is that in [16, 17], route reply messages generated at intermediate nodes on a path are abstracted away.

In a Petri net tokens concurrently travel through a directed graph; in a colored Petri net [19] tokens are data values. AODV and its successor AODVv2 [20] (also known as DYMO) are modeled in [21] and analyzed in [22] using colored Petri nets. In the latter paper several underspecifications and issues in the AODV2 standard are reported, notably with regard to the content of route request messages. In [23] the model from [22] is optimized so that its state space is reduced considerably. Four ambiguities in the AODV specification are revealed in [18], in particular concerning how to act at the receipt of a route reply or route error message. Possible interpretations of these ambiguities are considered exhaustively, and it is shown that certain interpretations of these ambiguities give rise to unwanted behavior. Experimentation with five existing open source implementations of AODV show that they deal with these ambiguities in different ways. For more than 5000 interpretations it is verified whether they are loop-free, as explained in [15], demonstrating how this formal reasoning approach can be adapted conveniently for protocol variants. In [24] AODVv2 is specified in AWN, a process calculus that will be discussed in Section 3.2, and it is shown that some problems of AODV were resolved in AODVv2 but new shortcomings were introduced. Notably, route request messages may be lost in AODV; a fix of this problem causes the loss of both route request and reply messages in AODVv2. The latter protocol is proven to be loop-free in [25] using a graph grammar framework, but is later shown to suffer from loops in [26, 27]. The latter two papers suggest improvements and formally prove loop freedom for these adapted versions. It is worth noting that the specification issues reported in [22, 23] and the detected loop formations in [12, 18, 26, 27] led to adaptations in the official AODV standard.

Other MANET routing protocols have also been analyzed using model checking, on very small networks to cope with state space explosion. The underlying idea is that flaws in these protocols may already occur with only a few nodes. In [28] the refinement checker FDR [29] is used to analyze the Cluster-Based Routing Protocol (CBRP) [30] on networks of five nodes. In [31] the Lightweight Underlay Network Ad hoc Routing (LUNAR) protocol [32] is analyzed with SPIN for networks of seven nodes, with respect to a few specific mobility scenarios. In [33] the Wireless Adaptive Routing Protocol (WARP) [34] is analyzed for networks of five nodes. General mobility is taken into account, leading to huge state spaces. Therefore a simplified version of the protocol is considered and so-called bitstate hashing is employed, meaning that roughly 98%

of the state space is covered in the analysis. In [35] it is explained how connection properties within ad hoc wireless sensor networks can be analyzed using SPIN. In [36] several functional properties of the OLSR protocol, including loop freedom, are verified with SPIN on networks of four nodes. Byzantine node failures are taken into account, in which case the verification provides an execution trace to the failure.

Different techniques have been developed to cope with the state space explosion problem inherent to MANET protocols. In [37] the intermediate nodes in a route are lumped together. SPIN is applied to the abstracted state spaces of three routing protocols, the Location Aided Routing (LAR) protocol [38], the Distance Routing Effect Algorithm for Mobility (DREAM) [39], and OLSR, leading to the detection of flaws in all three protocols. A symbolic reachability algorithm for MANET protocols is introduced in [40], based on a constraint language for representing topologies. In [41] the transitions in the state space of a MANET protocol are endowed with topological connectivity information. Model checking is performed, using the mCRL2 toolset [42], with regard to a temporal logic that takes into account connectivity. In a mobility-preserving abstraction of a state space of a MANET protocol from [43], the transitions are labeled by connectivity information, and model checking can be performed with regard to a three-valued temporal logic. In [44] it is demonstrated on AODVv2 that it may suffice to prove global invariants for arbitrarily large dynamic networks of similar nodes on a small "cutoff" network. In [45] AODV serves as running example for a novel approach to reduce state spaces of MANET routing protocols by considering only the last attempt of a source node trying to establish a route to some destination.

Model-based conformance testing verifies whether execution traces of a system implementation conform to a formal model of the desired system behavior. A methodology for conformance testing of MANET routing protocols is presented in [46], which tries to address the challenge of interpreting the outcomes of test executions against unpredictable underlying topology changes. The notion of self-similarity from [47] is exploited: nodes on the same paths of forwarded packets are collapsed, to obtain small networks that are representative of the entire network. The approach is used to test an implementation of the Dynamic Source Routing (DSR) protocol [48, 49] against a model of this protocol in the Specification and Description Language (SDL) [50]. Many test verdicts unfortunately remain inconclusive, due to the huge number of possible mobility patterns. In [51] this framework is employed to passively test the OLSR protocol, meaning that input and output events of the implementation under test are observed at run-time without stimulating the implementation. In [52] this experiment is repeated to showcase the formal tool DataMonitor for passively testing MANET routing protocols.

2.2 Real-time Properties

With regard to the formal analysis of real-time properties of MANET protocols, again [12] is a notable starting point. Next to functional correctness of the Routing Information Protocol (RIP) [53], a sharp real-time upper bound on the computation of paths is proved using SPIN and HOL, under the assumption that the network topology remains stable. In [31] the LUNAR protocol is analyzed on networks of up to five nodes, with respect to some specific mobility scenarios, using the model checker

UPPAAL for real-time properties [54]. In the follow-up paper [55], by abstracting away some messages that are redundant in establishing a route, this is pushed up to networks with a diameter of eleven hops. In [56] an UPPAAL analysis of AODV shows that in paths with twelve intermediate nodes, a node may give up waiting for a route reply message too quickly. Their suggestion to make this delay dependent on the network diameter has been incorporated in a subsequent version of the AODV standard.

In [57] a formal model from [58] of the Better Approach to Mobile Ad hoc Networks (B.A.T.M.A.N.) routing protocol [59] is considered. Some ambiguities in the protocol standard are resolved and functional correctness is shown using UPPAAL. An adaptation of this protocol standard is proposed, and it is shown by means of simulations that this adaptation leads to significantly fewer suboptimal routes. In [60] the latter analysis is confirmed using UPPAAL, considering dynamic topologies in a 4×4 grid. In [61] OLSR is analyzed using UPPAAL. Next to functional properties on stable networks, also route discovery times are analyzed on dynamic networks, for networks of five nodes. In [62] this work is extended by proposing a new error message for OLSR and showing with UPPAAL that this halves recovery time in case of a link failure.

A method to alleviate the state space explosion problem for real-time model checking is proposed in [63]. Hard delay bounds for MANET protocols are derived by applying model checking for each individual node only and abstracting node interactions to arrival curves which express upper and lower bounds on the number of events that may arrive over a specified time interval, using Sensor Network Calculus [64]. This method is applied to the Real-Time X-layer Protocol (RTXP) [65], a routing protocol with guaranteed bounded end-to-end delays.

In [66] a novel method is proposed to build an efficient peer-to-peer overlay network on top of a MANET, by selecting physically near and fresh peer-to-peer neighbors. Several safety and liveness properties for this framework, such as absence of deadlock and successful termination of transmissions, are verified using UPPAAL, allowing to take into account timeouts at the network nodes.

Statistical model checking mixes traditional model checking with simulation. Execution runs of a model checker on the state space of the specified system are monitored with respect to some property, to obtain a statistical estimate on the validity of the property. In [67] this approach is advocated for the analysis of real-time properties of MANETs, to combat the state space explosion problem. A comparison is made between the performance of AODV and AODVv2 on networks with static topologies by means of the stochastic timed model checker UPPAAL SMC [68]. In these experiments, AODV performs better than AODVv2 on networks of five nodes. Moreover, it is shown that this analysis could scale to networks of up to a hundred nodes. In [69] this experiment is repeated on 4×3 toroidal networks with lossy communication, in which case by contrast AODVv2 performs significantly better than AODV. An explanation for these different experimental outcomes is that on very small networks AODVv2 does not benefit from an optimization called path accumulation, meaning that messages accumulate information about the nodes they visit and distribute this information to their recipients. In [70] it is analyzed how an upgrade of AODVv2 to resolve loop formations, called AODVv2-16, impacts performance, on 3×3 grid networks. It is found that the old version performs significantly better, especially in case

of a high rate of message loss. In [71] it is explained how UPPAAL SMC can be used in a structured way to model MANET protocols, by building reusable components for such protocols. This framework is applied to analyze the probability of packet delivery for AODV, B.A.T.M.A.N., and OLSR on different network topologies of nine nodes, at different rates of link failures.

2.3 Security

A protocol is considered secure if it is robust against malicious attackers. In a MANET, nodes must be able to trust the intermediate nodes in a route. A malicious node should not be able to secretly inject itself into the network or overhear private information, in spite of the dynamic and open nature of MANETs and wireless communication being vulnerable to malicious activity such as eavesdropping. The importance of an in-depth security analysis of MANET protocols is underscored by the wide range of security issues in the OLSR protocol reported in [72].

A strand space [73] is a graph structure of events generated by causal interaction. It exploits that security protocols typically exhibit nonbranching behavior, as the participants tend to execute a fixed sequence of events. The tool Athena [74] automatically checks security properties of strand spaces using a combination of model checking and theorem proving. In [75] the strand space model and Athena are extended to capture the branching behavior of MANET routing protocols and search for insider attacks. As a case study it is shown on a network of four nodes that in AODV an attacker can forge a route reply message.

Ariadne [76] intends to be a secure MANET routing protocol. In [77] however attacks on this protocol are revealed, in which the malicious intruder redirects routes through nodes under its own control, and an adaptation called endairA (the reverse of Ariadne) is proposed. While in Ariadne a route request message is digitally signed, in endairA all intermediate nodes sign a route reply message. The endairA protocol is proven correct using simulations of a mathematical model of the protocol. In [78] however another attack is exposed on endairA, in which adversarial nodes exploit nonexisting links to transfer data (such as signatures). It is argued that the mathematical framework put forward in [77] for analyzing the security of MANET routing protocols needs to be extended to take into account such hidden channels. A posterior analysis of endairA in [79] with the model checker AVISPA [80], which targets security protocols, inadvertently misses the attack uncovered in [78] because hidden channels are not included in the model.

The Authenticated Routing for Ad hoc Networks (ARAN) secure MANET routing protocol [81] is based on a public key signature scheme. In [82] a man-in-the-middle spoofing attack on ARAN is revealed by means of ProVerif [83], an automatic cryptographic protocol verifier that transforms a protocol specification into Horn clauses. It is also explained how ARAN can be adapted to avoid this attack that constructs false routes. An analysis of this improved version of ARAN with AVISPA in [84] does not reveal any flaws. It is however reported that AVISPA does not terminate on some requirements in case of a network of five nodes. A later AVISPA analysis of the same

protocol in [79] does reveal attacks, in which routes are prevented from being discovered or existing routes are tampered with. In [85] an analysis of ARAN with the symbolic model checker AlPiNa [86] rediscovers all known attacks on this protocol.

In [87] the Open Shortest Path First (OSPF) routing protocol is analyzed using the model checker CBMC [88] for C programs, on networks of a few nodes. A spoofing attack is uncovered, as well as a attack in which the buffer of a node is filled with fake messages. Moreover, a known attack from [89] is revealed. The same approach leads to the discovery of another attack in [90], in which nonexisting links are included in routing tables, giving rise to patches by most OSPF route vendors. In [91] detailed Uppaal models of OSPF are analyzed, leading to the automated detection of aforemenioned attacks.

Dedicated methods have been developed to facilitate the verification of security properties for MANET protocols by means of model checking. In [92] automation of model checking routing protocols is increased by evaluating all potential message sequences an attacker may use to change routing information during route discovery (in a given network). Additionally, automatic topology generation and reduction techniques are developed. Furthermore, a topology equivalence is defined to cluster network topologies with the same security vulnerabilities, allowing an exhaustive analysis for networks of six nodes. SPIN analyses of Ariadne and a secure version of DSR, using the Secure Routing Protocol from [93], show how an attack revealed in [77] can be discovered in an automated way. In [94] it is shown that for a large class of security properties of routing protocols, including validity of routes, it suffices to consider only five topologies consisting of four nodes. As examples, the secure version of DSR and the Secure, Disjoint, Multipath Source Routing (SDMSR) protocol [95] are analyzed using ProVerif, again showing that an attack revealed in [77] can be discovered in an automated way. In the aforementioned paper [87] it is shown how a so-called abstract topology can, from a security perspective, capture a family of topologies of greater complexity.

3 Modeling Frameworks for MANET Protocols

Existing formal modeling languages have been extended and new formalisms have been developed to specifically target MANET networks. They played an important role in pushing forward the boundaries of formal analyses of MANET protocols. Typically, in these frameworks a message sent by a node is received only by the nodes in its range, and mobility is incorporated by letting neighborhoods of nodes evolve over time.

The majority of the frameworks targeting MANETs are in the form of a process calculus, in which the individual network nodes are specified in the form of algebraic terms and their behavior is defined by means of a formal semantics, which is often operational, meaning that transitions in the state space are defined on the basis of logical inference rules. A wide range of equivalences have been defined to distinguish such process behaviors.

This section starts with a general overview of process calculi for MANETs. Next, it is explained in some detail how broadcast communication has been modeled in these calculi. The section is completed with an overview of adaptations of other formalisms

to specify MANET protocols, notably Object-Z, Abstract State Machines, and Petri Nets.

3.1 Process Calculi

In the Calculus of Broadcasting Systems with mobility (CBS$^{\#}$) [96], which targets MANET protocols, connectivity changes are captured in the semantics: every send event expresses which nodes are connected at that moment, and the transitions in the generated state space must satisfy a topology invariant. Process behavior is considered modulo what is called mediated equivalence, which identifies nodes with respect to their capabilities to store items from other nodes. A static analysis is proposed that by overapproximating network behavior allows to automatically analyze in how far an attacker can influence the network topology. A simplified version of SAODV, a secure variant of AODV, is specified in CBS$^{\#}$, and it is shown that this specification is not what is called topology consistent: even in the presence of a filter that rejects incorrect paths, a network under attack is not mediated equivalent to this network without an attacker. In [97] a process calculus inspired by CBS$^{\#}$ is defined to analyze the security of MANET routing protocols. Moreover, it is shown how to automatically search for network topologies that allow an attack, using constraint solving techniques. The approach is demonstrated on the aforementioned secure version of DSR.

In the Calculus of Mobile Ad hoc Networks (CMAN) [98, 99] as well as in the Calculus of Mobile ad hoc Networks (CMN) [100], each network node is equipped with a location and communicates with other nodes using a spatially oriented broadcast. In CMAN arbitrary node mobility is expressed both in the semantics and syntactically through a static binding operator, while in CMN it is captured only in the semantics. For both process calculi, next to an operational semantics also a reduction semantics is provided, and the two semantics are shown to coincide with respect to a notion of weak bisimulation equivalence. The strength of CMAN is in [98] exemplified by means of the aforementioned attack on the ARAN secure routing protocol revealed in [82]. In [101] a variant of CMN is proposed that allows one to express different levels of trust.

In Restricted Broadcast Process Theory (RBPT) [102] connectivity changes are captured in the semantics, making sure that received messages in a broadcast are in sync with network connectivity. The notion of network bisimulation equivalence is introduced, which takes into account network connectivity. RBPT is provided with an equational theory in [103]. In [104] it is exemplified on a simplified version of the AODV protocol that this framework can be used to reason about MANET protocols on networks consisting of an unbounded number of nodes. A variant of RBPT in which communication is considered reliable, presented in [105], aims at the detection of conceptual flaws in protocol designs that are not due to lossy communication. In the Calculus for Systems with Dynamic Topology (CSDT) [106], which is similar in spirit to RBPT, nodes can broadcast at two different transmission ranges. The belief of nodes about who are their neighbors is continuously updated. A hiding construct allows one to observe networks at different levels of abstraction. A theory of confluence is developed and the framework is applied to verify the Vasudevan-Kurose-Towsley leader election algorithm for MANETs [107]. In a stochastic extension of RBPT [108], delay functions are assigned to events, while the semantics captures the interplay of

a MANET protocol with stochastic dynamic behavior of the data-link and physical networks layers. A continuous-time Markov chain, expressing the probability with which a certain state will change to another state, is derived using a novel notion of weak Markovian network bisimulation equivalence. This framework is imployed to analyze expected election times for the Vasudevan-Kurose-Towsley leader election algorithm.

A large body of work has been developed for the Algebra for Wireless Networks (AWN) [109], which offers reliable local broadcast, a conditional unicast operator whose behavior depends on whether a message can be delivered, and rich datastructures. In [109–111] the core of AODV is modeled in AWN, including data handling aspects such as maintaining route tables. Moreover, properties such as loop freedom and packet delivery are (dis)proved, both manually and with UPPAAL, culminating in a detailed specification and proofs in [112]. This work is underpinned in [113] by a formalization of proofs using the theorem prover Isabelle/HOL [114]. A mechanization of the calculus AWN in Isabelle/HOL is presented in [115], together with a novel technique to lift global invariants from individual nodes to networks. By an automatic translation in [116] from AWN to mCRL2, this formal verification toolset can be applied to AWN specifications.

A timed extension of AWN (T-AWN) is presented in [117] and used to show that premature deletion of invalid routes and a too quick restart of a node after a reboot can lead to loops in AODV. Boundary conditions are given that resolve this problem. T-AWN is used in [118] to give an unambiguous specification of the OLSRv2 protocol. In [119] a detailed T-AWN specification is given of OSPF, providing an unambiguous interpretation of this standard. Moreover, the specification is translated to an UPPAAL model, serving as the basis for the aforementioned security analysis of OSPF in [91].

The Calculus of Wireless Systems (CWS) [120] aims at modeling nonmobile wireless networks. An extension of CWS with mobility and time, called Timed Calculus for Mobile ad hoc Networks (TCMN), is proposed in [121] and used to analyze two collision-avoidance protocols, Carrier Sense Multiple Access (CSMA) and Multiple Access with Collision Avoidance Receiver-Transmitter (MACA/R-T). It is shown that CSMA is not robust with regard to mobility while MACA/R-T is.

In [122] the Calculus of the Internet of Thing [123] is extended with node mobility and broadcast communication. A transformation from the extended calculus to timed automata is presented, which is employed to verify six temporal properties for smart homes using UPPAAL.

3.2 Extensions of the π-Calculus

The π-calculus [124] is a process calculus in which channel names can be communicated along the channels themselves. This makes it a convenient platform for expressing mobility. A primary process calculus inspired by the π-calculus that takes the movement of nodes into account explicitly is the ambient calculus [125]. Locations are represented by a topology of boundaries, interaction between nodes is by shared location within a common boundary, and security is expressed by the inability to cross boundaries. Nomadic π [126] adds communication primitives to the π-calculus for interaction between mobile agents in a two-level framework; the lower level defines

location-dependent primitives, the higher layer defines location-independent primitives using underlying primitives. Nomadic π serves as the basis for Nomadic Pict [127], a distributed programming language for prototyping overlay network algorithms.

In three other extensions of the π-calculus, the $b\pi$-calculus [128], the Mobile Broadcasting System (MBS) calculus [129], and the ω-calculus [130], two nodes can communicate if they belong to the same group. Mobility is captured through the creation of new groups and allowing a node to move to another group. In [128] a theoretical framework for this group communication paradigm is developed, including three behavioral equivalences. In [130] it is shown how one can verify a model against mobility scenarios using invariants that constrain mobility, which is applied to analyze AODV and the Vasudevan-Kurose-Towsley leader election algorithm. The psi-calculus [131], a parametric framework for extensions of the π-calculus, is in [132] provided with dynamic broadcast communication. This framework is demonstrated by verifying a reachability property for LUNAR.

Some extensions of the π-calculus target the security of MANETs. The Distributed Broadcast SPI-calculus (DBSPI) [133] combines elements of the Distributed π-calculus [134], which adds a network layer and a primitive mobility construct to the π-calculus, and the Spi-calculus [135], which is a cryptographic extension of the π-calculus. DBSPI offers a type system, i.e., a logical system of inference rules, that ensures correctness of authentication for MANET protocols. This framework is applied to prove the Mobile IP registration protocol [136] correct. The bAπ-calculus [137] adds mobility to the applied π-calculus [138], an extension of the π-calculus that targets security protocols. The bAπ-calculus allows one to reason about an unbounded number of nodes. Its reduction semantics, describing interactions between a sender and receivers, coincides with its operational semantics modulo a novel behavioral equivalence called barbed weak congruence. In [139] a variant of the applied π-calculus is extended to analyze privacy-type properties for MANET routing protocols. Using this framework it is demonstrated that the ANonymous On-Demand Routing (ANODR) protocol [140] violates source anonymity: an attacker can retrieve the identity of a node trying to establish a route.

3.3 Modeling Broadcast Communication

We now discuss in more detail, based on [15, section 11.1], the ways in which broadcast communication has been modeled in the process calculi mentioned in the previous two sections. These calculi all include some form of broadcast communication in their operational semantics, in which a message emitted by a node can be received by multiple other nodes. Typically this is expressed by two symmetric operational rules such as

$$\frac{M \xrightarrow{\texttt{broadcast}(m)} M' \qquad N \xrightarrow{\texttt{receive}(m)} N'}{M \| N \xrightarrow{\texttt{broadcast}(m)} M' \| N'} \qquad \frac{M \xrightarrow{\texttt{receive}(m)} M' \qquad N \xrightarrow{\texttt{broadcast}(m)} N'}{M \| N \xrightarrow{\texttt{broadcast}(m)} M' \| N'}$$

which originate from the nonmobile Calculus of Broadcasting Systems (CBS) [141]. Process terms M and N represent two subnetworks and $M \| N$ their composition. The

premises at the top of the two operational rules express that in one of the subnetworks message m is broadcast, while nodes in the other subnetwork can receive this message. The conclusion at the bottom of each rule expresses that then in the composed network these same nodes can receive m. In these rules the broadcast action in the conclusion is simply inherited from the broadcasting argument of the parallel composition, so that it remains available for the composition with yet another receiver.

To capture the receipt of a broadcast messages m properly, an additional operational rule is needed, expressing that multiple subnetworks can receive this message concurrently:

$$\frac{M \xrightarrow{\texttt{receive}(m)} M' \qquad N \xrightarrow{\texttt{receive}(m)} N'}{M \| N \xrightarrow{\texttt{receive}(m)} M' \| N'}$$

This rule is missing in CMN and the ω-calculus. In [15] it is observed that this omission leads to technical problems in both calculi.

To model lossy communication in MANETS, the bAπ-calculus, CMAN, CMN, the ω-calculus, and RBPT contain operational rules to express that one subnetwork may nondeterministically miss a message m broadcast by another subnetwork, even if they are within each other's ranges, such as the following two symmetric rules:

$$\frac{M \xrightarrow{\texttt{broadcast}(m)} M'}{M \| N \xrightarrow{\texttt{broadcast}(m)} M' \| N} \qquad \frac{N \xrightarrow{\texttt{broadcast}(m)} N'}{M \| N \xrightarrow{\texttt{broadcast}(m)} M \| N'}$$

A drawback of this approach is that it becomes impossible to verify properties such as "if there is a path from some source node to some destination node and the topology remains stable, then data packets from the source will eventually reach their destination" for routing protocols, because each packet may be lost on the way. AWN and RRBPT, a variant of RBPT, allow to express reliable communication and thus to verify such properties.

In the operational semantics of the bπ-calculus, CBS$^{\#}$, CWS and an optional augmentation of AWN [109], a broadcast message m is only dropped by nodes that are not ready to receive it, which can be specified using a negative premise:

$$\frac{M \xrightarrow{\texttt{broadcast}(m)} M' \qquad N \xrightarrow{\texttt{receive}(m)}\!\!\!\!\!\!\rightarrow}{M \| N \xrightarrow{\texttt{broadcast}(m)} M' \| N} \qquad \frac{M \xrightarrow{\texttt{receive}(m)} M' \qquad N \xrightarrow{\texttt{receive}(m)}\!\!\!\!\!\!\rightarrow}{M \| N \xrightarrow{\texttt{receive}(m)} M' \| N}$$

and two more symmetric operational rules. The negative premise $N \xrightarrow{\texttt{receive}(m)}\!\!\!\!\!\!\rightarrow$ expresses that process term N is not able to perform the event $\texttt{receive}(m)$. This makes these calculi nonblocking, meaning that a sender cannot be delayed in transmitting a message, even if potential recipients are not ready to receive it. The default version of AWN does allow for blocking, although it has facilities to prevent this in applications.

3.4 Other Formalisms

An early work where an existing formalism, not tailored to MANETS, is adapted to cope with mobility is [142], which extends the UNITY proof logic for distributed systems [143]. Transient interactions are added to capture that nodes can communicate with each other only when they are within range, and the proof logic is extended to cover mobility. A baggage delivery system serves as running example.

Object-Z [144], a state-oriented formal specification language with object-oriented concepts, is in [145] extended to dynamic networks whereby connections are mutable references between nodes. In [146] Object-Z is used to formalize the route discovery process in AODV, where broadcast communication is modeled by simultaneous changes in local variables of the sender and all of its connected receivers. Loop freedom is proved under a dynamic network topology. In [147] the UPPAAL model of the OLSR protocol from [61] is transposed to Event-B [148], to formally model this protocol through incremental stepwise refinements and prove functional properties with Event-B's interactive theorem prover Rodin. In [149] the experiences with this translation and the two models are the basis for some guidelines on when to use UPPAAL or Event-B for formal modeling and analysis. In [150] Event-B is combined with the evolving graphs formalism from [151] that aims to model dynamic graphs. The obtained framework to specify correct-by-construction MANET protocols is exemplified on a simple centralized counting algorithm.

In an Abstract State Machine (ASM) [152] states are data structures, equipped with functions and relations. A distributed ASM (DASM) [153] is provided with a location service and position-based routing, to enable modeling MANET routing protocols. In [154] this formalism is extended further with a logical topology and a protocol to let each node maintain the location information of its logical neighbors. In [155] it is shown how the resulting formalism can be carried over to the specification language SDL [156]. In [157] AODV is modeled as a DASM and two correctness properties, starvation-freedom and that the correct packet is received back by the initiator of a route, are briefly argued based on this model. This work is in [158] extended by proposing and formally proving correct a variant of AODV that prevents blackhole attacks, in which false information is sent toward the initiator.

An Algebraic Higher-Order (AHO) net [159] allows the tokens in a Petri net to be dynamic structures, such as graphs or Petri nets. An architecture for AHO nets from [160] enables nodes in a MANET to collaborate effectively through workflows, by means of a coordination layer that maintains network connections and modifies the workflow schema at run-time. In [161] it is proposed to divide this architecture into three layers: a workflow layer, a mobility layer, and a team layer, which maps the activities of individual nodes to the workflow and mobility layers. In [162] this approach is extended by making the mapping dynamic.

In [163] it is investigated how topology control of wireless sensor networks can be modeled in two graph-based formalisms, Graph Transformation Systems [164] and Bigraphical Reactive Systems [165]. In [166] bigraphs are used to model part of the Routing Protocol for low-power and Lossy Networks (RPL) [167], meant for wireless sensor networks. Bigraphs allow developers to draw the protocol updates. A model

checking analysis of their (nonprobabilistic) model is performed using PRISM to verify a reachability property, discovery of optimal routes, and loop freedom.

4 Mobility Models and Performance

A mobility model captures how nodes move through a MANET. This may be random or guided by some probability distribution. In [168] it is shown that the choice of mobility model has a significant effect on the outcome of simulation experiments on MANETs to measure the performance of protocols. Different probabilistic formal frameworks have been proposed in which mobility models can be expressed explicitly.

An early work on mobility models is [169], in which a pathset algebra is put forward, where a pathset is a graph structure of all paths from some source to some destination. It is coupled with an algebraic approach from [170] to model dynamic multi-agent systems. The framework is demonstrated on a small payroll application. In [171] an algebra of routing tables for MANET routing protocols is developed that allows to algebraically reason about for instance packet delivery.

In [172] a simple wireless process calculus is provided with mobility functions. Its operational semantics incorporates a notion of global time passing. This framework allows one to express and compare various mobility models with respect to weak simulation and bisimulation equivalences. In [173] this mobility model is extended with group mobility and the ability to let movement patterns change over time, and this framework is applied to prove some properties for a simplified version of the Wireless HIerarchical Routing protocoL (WHIRL) [174], which includes group mobility. In [175] a mobile process calculus is proposed where messages may be lost with some probability. How the network distribution evolves depends on which nodes receive a broadcast message. Node mobility is ruled by a probabilistic function and the calculus is considered modulo a weak bisimulation equivalence that takes this mobility function into account. The framework is applied to analyze the probability of address collision for a simplifies version of [176], a protocol for assigning unique IP addresses to nodes in a self-configuring local area network. In [177] the mobility function is generalized by allowing it to change multiple connections at the same time. Furthermore, the process calculus is extended to express mobility models with stochastically timed behavior. This enhanced framework is demonstrated by a specification of the Vasudevan-Kurose-Towsley leader election algorithm.

[178] offers a framework to evaluate the performance of MANET protocols, capturing the interplay between stochastic behavior of protocols deployed at different network layers and the underlying topology. A link connectivity model specifies link up and down lifetimes. Transitions are annotated by network restrictions, expressing the topologies in which an event is possible. A continuous-time Markov chain is generated to evaluate performance by means of the probabilistic model checker PRISM [179]. A simple flooding protocol to find the largest ID in the network serves as running example. In [180] the unreliable nature of radio links is considered, where links may frequently appear and disappear. A method is presented to produce the set of topologies with a probability distribution and check the probability that a certain property holds. This method is applied to check some time properties on an Uppaal model

of f-MAC [181], a real-time protocol for access control of nodes in a wireless network to a shared medium. In [182] the influence of uncertainty (such as packet loss rates, collisions) on the probability to establish short routes in AODV is analyzed using a formal model of probabilistic timed automata and the MODEST toolset [183].

In [184] a topology-based mobility model is proposed that abstracts away physical behavior and models mobility as probabilistic changes in the topology. These probabilities are distilled from either the random walk or the random waypoint model. The approach is applied, using UPPAAL, in a performance analysis of AODV and of the energy-efficient Lightweight Medium Access Control (LMAC) protocol [185] for wireless sensor networks.

The Calculus for Wireless sensor networks from Quality perspective (CWQ) [186] is extended with mobility in [187] and the resulting calculus mCWQ is provided with an operational semantics. It offers a parametric framework to describe how node movement patterns evolve over time. A simple ad hoc network for vehicles serves as case study. In [188] mCWQ is provided with a denotational semantics. In [189] a proof system for mCWQ is provided, based on Hoare Logic [190] extended with some time primitives.

In [191], different mobility models are specified in Real-Time Maude [192], a specification language for real-time and hybrid systems based on rewriting logic. This framework is used to analyze the route discovery process in AODV and the Vasudevan-Kurose-Towsley leader election algorithm using Real-Time Maude's timed model checker [193]. This analysis uncovers a spurious behavior in the latter protocol, due to a subtle interplay between communication delays, node movement, and neighbor discovery.

PEBUM [194] is an energy-aware process calculus for MANETs. A probabilistic bisimulation equivalence is defined to verify whether two networks exhibit the same observable behavior. Moreover, an energy-aware preorder is defined to compare the energy consumption of different but behaviorally equivalent networks. The framework is applied, using PRISM, to analyze how the performance of the LAR protocol depends on the network topology, and to compare the energy consumption of two error control protocols, stop-and-wait and go-back-N. This approach to turn a PEBUM specification into a discrete-time Markov chain and then apply PRISM is in [195] applied to analyze energy consumption of different communication strategies for the gossip-based routing protocol from [196]. In [197] PEBUM is studied in the setting of a probabilistic reduction semantics from [120] that takes into account interference caused by simultaneous transmissions of multiple nodes in overlapping transmission areas, leading to loss of messages at the receiver side. This offers a framework to analyze network connectivity and measure the level of interference in a MANET. As a case study it is proven that, under mild assumptions on node mobility, the LAR protocol has the same probability to discover a path as a simple flooding approach.

5 Conclusions

This survey aims to give an exhaustive overview of research performed in the context of rigorous formal methods for analyzing MANET protocols. Formal modeling and

analysis of MANETs has led to a significant body of research, including the development of innovative formalisms, semantics, and behavioral equivalence notions. These frameworks have been applied successfully to a wide range of MANET protocols, especially for routing, revealing many ambiguities and inconsistencies in their specifications as well as flaws in their designs, often leading to the adaptation of protocol standards. These imperfections would generally have been very difficult to spot with traditional methods such as visual inspection or testing an implementation of the standard, because they typically concern corner cases that rarely come to the surface and may require specific mobility scenarios.

A key aspect of these formalisms has been the invention of novel ways to express broadcast communication and mobility. Furthermore, the formal analysis of MANET protocols has benefited considerably from optimized verification techniques that specifically target MANETs. Symbolic methods have been of particular importance, because the exponential increase in possible mobility scenarios with the growth of a network seriously hampers model checking approaches, which require generation of the state space.

Summarizing, the following types of models and methods can be distinguished.

- *State-based model checking*: The system is represented as a collection of states and transitions between them, and model checking is employed to verify temporal logic formulas. General strengths of this approach are that it is relatively simple and intuitive, and well-supported by mature and automated tools such as SPIN. Typical use of this method in the context of this survey therefore is logical verification of protocol correctness on small MANET instances, including correctness of route discovery or packet delivery. General weaknesses are that only instances of networks can be verified, and the state explosion problem. The latter is particularly poignant for MANETs, due to poor scalability in case of many network nodes or dynamic topologies.
- *Timed and hybrid*: Timed Automata, which include real-time clocks, can be used to model protocol timeouts and delays. Such models can be analyzed using a timed model checker such as Uppaal. This is of importantance in the context of this survey because MANET routing often depends on timing constraints, e.g., route discovery completion within a time bound. Hybrid Automata include continuous variables which allow to combine discrete protocol logic with continuous mobility dynamics (e.g., node movement equations). The obvious weakness of both formalisms is that the state space explosion problem becomes even more severe. This can be alleviated by time abstraction or approximation of continuous behavior, but such measures tend to increase model complexity as well as the uncertainty of verification results.
- *Probabilistic and stochastic*: Formalisms such as Probabilistic Automata and continuous-time Markov chains allow to represent uncertainty in transitions (e.g., mobility, link failure, packet loss), and thus capture randomness and reliability. This enables the employment of probabilistic model checkers such as PRISM for quantitative verification of robustness and reliability under uncertainty, e.g., whether a delivery probability is beyond a certain threshold. Typical use of such models in the context of MANET protocols is for analyzing reliability, packet loss, and expected

route duration. General weaknesses are that this approach does not scale well to large state spaces and that it tends to require accurate probabilistic parameters.

- *Petri net*: The system is modeled using events (transitions) and local states (places), with tokens modeling data moving through the network. Extensions such as Colored and Stochastic Petri nets provide more structure to tokens or probabilities to transitions. In the context of MANETs, tokens typically represent packets, while transitions model events like packet transmission or route discovery. General strengths are that this formalism allows to model parallelism, resource sharing, and synchronization of distributed and concurrent systems in a natural fashion. Moreover, the specification language is graphical and intuitive. Typical use of this formalism in the context of MANETS is for performance-oriented verification of concurrent behaviors in routing, and for studying packet flow, buffer management, and route establishment. General weaknesses are a limited expressiveness for complex logical properties, and that analysis can be computationally expensive.
- *Process algebra*: The system is specified in an algebraic format, in which each network node is modeled as a concurrent process communicating through channels. General strengths of this framework are that it is good for reasoning about process interactions and synchronization. Strengths in the context of MANETs are that it naturally models concurrency and mobility, which is especially true for the π-calculus. The latter formalism is therefore particularly suited for MANETs where node connections change over time. Typical use of this method is to formally reason about communication and concurrency in MANET protocols, and to analyze protocol interaction patterns and message-passing correctness. General weaknesses are that the abstract mathematical formalism requires a steep learning curve, and that it can be hard to take into account quantitative aspects like timing or probabilities.
- *Interactive proof assistant*: The user and the prover, such as Isabelle/HOL, collaborate to build a proof, whereby the user applies tactics or commands to break down goals into simpler subgoals and the prover checks each step for logical correctness and generates new subgoals if necessary. This typically entails the formulation and proof of invariants, e.g., sequence-number monotonicity for AODV. Existing libraries of lemmas and definitions can be exploited in the process. This approach avoids the state space explosion problem and can provide a formal correctness proof of MANET protocols for arbitrary networks, but often requires abstractions for mobility. Modeling realistic mobility and probabilistic loss in a proof assistant is possible but increases proof complexity significantly. The overall compute cost tends to be relatively low, but the human effort is high in terms of formalization and proof development, and requires skilled users. Building the right invariants is hard; here model checking can offer support through the discovery of counterexamples to refine invariants.

Process calculi sit between model checking and theorem proving in several respects: they give strong compositional and concurrency/mobility abstractions (very useful for MANETs), but they also incur non-trivial human cost (formal modeling + proof/analysis) and limited off-the-shelf automation compared with model checkers. They are especially attractive when you want protocol-level reasoning, compositional proofs (e.g., modular correctness, equivalence, refinement) and a natural treatment

of dynamic link structure, but they are less convenient for brute-force counterexample search, tight timing/probabilistic analysis, or large concrete instance exploration. A process algebraic specification offers a useful first step toward a proof with an interactive proof assistant.

If priorities are modular design, correctness under dynamic topology, or reasoning about protocol refinements, invest in process calculi: they pay off conceptually and in proofs of equivalence/refinement. If priorities are fast bug discovery, timed/probabilistic metrics, or low-barrier automation, start with model checking. If you need machine-checked, parameterized guarantees for deployment or certification, plan for theorem proving — but bootstrap it from process calculus models and model checking counterexamples. For many MANET verification projects, a hybrid pipeline (model checking → process calculus → interactive proof assistant) may give the best cost/benefit balance.

The advancement of this research field is somewhat impeded by the fact that developed frameworks are often used only by their inventors. Preferably the rich body of work would lead to a single formalism that becomes the main vehicle for the formal analysis of MANET protocols. Process calculi seem to be best suited for this purpose, because they can conveniently express a combination of mobility as well as real-time, probabilistic, and security aspects. Furthermore, their algebraic nature allows to conveniently specify rich datastructures and efficiently perform both model checking and theorem proving analyses. Other important avenues for further research are techniques that target formal performance and security analyses of MANET protocols.

Formal analysis techniques regarding the functional correctness of MANET protocols have reached a level where complex, real-life protocol standards can be verified in a thorough fashion, exemplified by the detailed analysis of AODV in the process calculus AWN. A challenge is to develop the formalisms and techniques in such a way that they can be conveniently included and employed by protocol developers and software engineers in the development and implementation process of MANET protocol standards.

References

[1] Jubin, J., Tornow, J.D.: The DARPA packet radio network protocols. Proc. IEEE **75**(1), 21–32 (1987) https://doi.org/10.1109/PROC.1987.13702

[2] Shacham, N., Westcott, J.: Future directions in packet radio architectures and protocols. Proc. IEEE **75**(1), 83–99 (1987) https://doi.org/10.1109/PROC.1987.13707

[3] Das, S.R., Castañeda, R., Yan, J.: Simulation-based performance evaluation of routing protocols for mobile ad hoc networks. Mob. Networks Appl. **5**(3), 179–189 (2000) https://doi.org/10.1023/A:1019108612308

[4] Cavin, D., Sasson, Y., Schiper, A.: On the accuracy of MANET simulators. In: Proc. 1st Workshop on Principles of Mobile Computing (POMC), pp. 38–43. ACM, New York (2002). https://doi.org/10.1145/584490.584499

[5] Roggenbach, M., Schlingloff, B.-H., Schneider, G.: Formal methods. In: Roggenbach, M., Cerone, A., Schlingloff, B.-H., Schneider, G., Shaikh, S.A. (eds.) Formal Methods for Software Engineering: Languages, Methods, Application Domains, pp. 1–46. Springer, Heidelberg (2022). https://doi.org/10.1007/978-3-030-38800-3

[6] Kulik, T., Dongol, B., Larsen, P.G., Macedo, H.D., Schneider, S., Tran-Jørgensen, P.W.V., Woodcock, J.: A survey of practical formal methods for security. Formal Aspects Comput. **34**(1), 1–39 (2022) https://doi.org/10.1145/3522582

[7] Clausen, T.H., Jacquet, P.: Optimized Link State Routing Protocol (OLSR). RFC 3626. IETF, (2003). IETF. http://www.ietf.org/rfc/rfc3626

[8] Perkins, C.E., Royer, E.M.: Ad-hoc on-demand distance vector routing. In: Proc. 2nd Workshop on Mobile Computer Systems and Applications (WMCSA), pp. 90–100. IEEE, New York (1999). https://doi.org/10.1109/MCSA.1999.749281

[9] Perkins, C.E., Royer, E.M., Das, S.R.: Ad Hoc On-Demand Distance Vector (AODV) Routing. RFC 3561. IETF, (2003). IETF. https://datatracker.ietf.org/doc/html/rfc3561

[10] Das, S., Dill, D.L.: Counter-example based predicate discovery in predicate abstraction. In: Proc. 4th Conference on Formal Methods in Computer-Aided Design (FMCAD). LNCS, vol. 2517, pp. 19–32. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-36126-X_2

[11] Engler, D.R., Musuvathi, M.: Static analysis versus software model checking for bug finding. In: Proc. 5th Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI). LNCS, vol. 2937, pp. 191–210. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24622-0_17

[12] Bhargavan, K., Obradovic, D., Gunter, C.A.: Formal verification of standards for distance vector routing protocols. JACM **49**(4), 538–576 (2002) https://doi.org/10.1145/581771.581775

[13] Holzmann, G.J.: The model checker SPIN. IEEE Trans. Software Eng. **23**(5), 279–295 (1997) https://doi.org/10.1109/32.588521

[14] Gordon, M.J.C., Melham, T.F. (eds.): Introduction to HOL: A Theorem Proving Environment for Higher Order Logic. Cambridge University Press, Cambridge (1993)

[15] Fehnker, A., van Glabbeek, R.J., Höfner, P., McIver, A., Portmann, M., Tan, W.L.: A process algebra for wireless mesh networks used for modelling, verifying and analysing AODV. Technical Report 5513, NICTA (2013). https://doi.org/10.48550/arXiv.1312.7645

[16] Wu, X., Xu, Q., Zhu, H.: Formal analysis of AODV using rely-guarantee. In: Proc. 7th Symposium on Theoretical Aspects of Software Engineering (TASE), pp. 45–48. IEEE, New York (2013). https://doi.org/10.1109/TASE.2013.14

[17] Zhou, M., Yang, H., Zhang, X., Wang, J.: The proof of AODV loop freedom. In: Proc. 1st Conference on Wireless Communications and Signal Processing (WCSP), pp. 1–5. ACM, New York (2009). https://doi.org/10.1109/WCSP.2009.5371479

[18] van Glabbeek, R.J., Höfner, P., Tan, W.L., Portmann, M.: Sequence numbers do not guarantee loop freedom: AODV can yield routing loops. In: Proc. 16th Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), pp. 91–100. ACM, New York (2013). https://doi.org/10.1145/2507924.2507943

[19] Jensen, K.: Coloured Petri nets and the invariant-method. Theor. Comput. Sci. **14**, 317–336 (1981) https://doi.org/10.1016/0304-3975(81)90049-9

[20] Perkins, C.E., Ratliff, S., Dowdell, J.: Dynamic MANET On-Demand (AODVv2) Routing. Draft. IETF, (2013). IETF. https://datatracker.ietf.org/doc/html/draft-ietf-manet-aodvv2-02

[21] Xiong, C., Murata, T., Tsai, J.: Modeling and simulation of routing protocol for mobile ad hoc networks using colored Petri nets. In: Proc. Workshop on Formal Methods Applied to Defense Systems. Conferences in Research and Practice in Information Technology, vol. 12, pp. 145–153. Australian Computer Society, Sydney (2002). https://dl.acm.org/doi/abs/10.5555/846335.846350

[22] Espensen, K.L., Kjeldsen, M.K., Kristensen, L.M.: Modelling and initial validation of the DYMO routing protocol for mobile ad-hoc networks. In: Proc. 29th Conference on Applications and Theory of Petri Nets (PETRI NETS). LNCS, vol. 5062, pp. 152–170. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-68746-7_13

[23] Billington, J., Yuan, C.: On modelling and analysing the dynamic MANET on-demand (DYMO) routing protocol. Trans. Petri Nets Other Model. Concurr. **3**, 98–126 (2009) https://doi.org/10.1007/978-3-642-04856-2_5

[24] Edenhofer, S., Höfner, P.: Towards a rigorous analysis of AODVv2 (DYMO). In: Proc. 20th Conference on Network Protocols (ICNP), pp. 1–6. IEEE, New York (2012). https://doi.org/10.1109/ICNP.2012.6459942

[25] Saksena, M., Wibling, O., Jonsson, B.: Graph grammar modeling and verification of ad hoc routing protocols. In: Proc. 14th Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS). LNCS, vol. 4963, pp. 18–32. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78800-3_3

[26] Namjoshi, K.S., Trefler, R.J.: Loop freedom in AODVv2. In: Proc. 35th IFIP WG 6.1 Conference on Formal Techniques for Distributed Objects, Components, and Systems (FORTE). LNCS, vol. 9039, pp. 98–112. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-319-19195-9_7

[27] Yousefi, B., Ghassemi, F., Khosravi, R.: Modeling and efficient verification of wireless ad hoc networks. Formal Aspects Comput. **29**(6), 1051–1086 (2017) https://doi.org/10.1007/s00165-017-0429-z

[28] Zakiuddin, I., Goldsmith, M., Whittaker, P., Gardiner, P.H.B.: A methodology for model-checking ad-hoc networks. In: Proc. 10th Workshop on Model Checking Software (SPIN). LNCS, vol. 2648, pp. 181–196. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-44829-2_12

[29] Lawrence, J.: Practical application of CSP and FDR to software design. In: Communicating Sequential Processes: The First 25 Years. LNCS, vol. 3525, pp. 151–174. Springer, Heidelberg (2004). https://doi.org/10.1007/11423348_9

[30] Jiang, M., Li, J., Tay, Y.C.: Cluster Based Routing Protocol (CBRP) Functional Specification. Draft. IETF, (1998). IETF. https://tools.ietf.org/id/draft-ietf-manet-cbrp-spec-00.txt

[31] Wibling, O., Parrow, J., Pears, A.N.: Automatized verification of ad hoc routing protocols. In: Proc. 24th IFIP WG 6.1 Conference on Formal Techniques for Networked and Distributed Systems (FORTE). LNCS, vol. 3235, pp. 343–358. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-30232-2_22

[32] Tschudin, C., Gold, R., Rensfelt, O., Wibling, O.: LUNAR: A lightweight underlay network ad-hoc routing protocol and implementation. In: Proc. 5th Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking (NEW2AN), pp. 38–43 (2004). https://www.researchgate.net/publication/228870993_LUNAR_a_lightweight_underlay_network_ad-hoc_routing_protocol_and_implementation

[33] de Renesse, R., Aghvami, A.H.: Formal verification of ad-hoc routing protocols using SPIN model checker. In: Proc. 12th Mediterranean Electrotechnical Conference (IEEE MELECON), pp. 1177–1182. IEEE, New York (2004). https://doi.org/10.1109/MELCON.2004.1348275

[34] Khengar, P., Aghvami, A.H.: WARP - The wireless adaptive routing protocol. In: Proc. 10th IST Mobile Summit, pp. 480–485 (2001)

[35] Oleshchuk, V.A.: Modeling, specification and verification of ad-hoc sensor networks using SPIN. Comput. Stand. Interfaces **28**(2), 159–165 (2005) https://doi.org/10.1016/j.csi.2005.01.017

[36] Steele, M.F., Andel, T.R.: Modeling the optimized link-state routing protocol

for verification. In: Proc. Spring Simulation Multiconference (SpringSim), pp. 1–8. SCS/ACM, New York (2012). https://dl.acm.org/doi/abs/10.5555/2346616.2346651

[37] Câmara, D., Ferreira Loureiro, A.A., Filali, F.: Methodology for formal verification of routing protocols for ad hoc wireless networks. In: Proc. 8th Global Communications Conference (GLOBECOM), pp. 705–709. IEEE, New York (2007). https://doi.org/10.1109/GLOCOM.2007.137

[38] Ko, Y., Vaidya, N.H.: Location-aided routing (LAR) in mobile ad hoc networks. Wirel. Networks **6**(4), 307–321 (2000) https://doi.org/10.1023/A:1019106118419

[39] Basagni, S., Chlamtac, I., Syrotiuk, V.R., Woodward, B.A.: A distance routing effect algorithm for mobility (DREAM). In: Proc. 4th Conference on Mobile Computing and Networking (MOBICOM), pp. 76–84. ACM, New York (1998). https://doi.org/10.1145/288235.288254

[40] Singh, A., Ramakrishnan, C.R., Smolka, S.A.: Query-based model checking of ad hoc network protocols. In: Proc. 20th Conference on Concurrency Theory (CONCUR). LNCS, vol. 5710, pp. 603–619. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04081-8_40

[41] Ghassemi, F., Fokkink, W.J.: Model checking mobile ad hoc networks. Formal Methods Syst. Des. **49**(3), 159–189 (2016) https://doi.org/10.1007/s10703-016-0254-7

[42] Groote, J.F., Keiren, J., Stappers, F.P.M., Wesselink, W., Willemse, T.A.C.: Experiences in developing the mCRL2 toolset. Softw. Pract. Exp. **41**(2), 143–153 (2011) https://doi.org/10.1002/spe.1021

[43] Nanz, S., Nielson, F., Nielson, H.R.: Static analysis of topology-dependent broadcast networks. Inf. Comput. **208**(2), 117–139 (2010) https://doi.org/10.1016/j.ic.2009.10.003

[44] Namjoshi, K.S., Trefler, R.J.: Analysis of dynamic process networks. In: Proc. 21st Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS). LNCS, vol. 9035, pp. 164–178. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46681-0_11

[45] Kojima, H., Nagashima, Y., Tsuchiya, T.: Model checking techniques for state space reduction in MANET protocol verification. In: Proc. IPDPS Workshop on Advances in Parallel and Distributed Computational Models, pp. 509–516. IEEE, New York (2016). https://doi.org/10.1109/IPDPSW.2016.122

[46] Maag, S., Grepet, C., Cavalli, A.R.: A formal validation methodology for MANET routing protocols based on nodes' self similarity. Comput. Commun.

31(4), 827–841 (2008) https://doi.org/10.1016/j.comcom.2007.10.031

[47] Djouvas, C., Griffeth, N.D., Lynch, N.A.: Testing self-similar networks. In: Proc. 2nd Workshop on Model Based Testing (MBT). ENTCS, vol. 164, pp. 67–82. Elsevier, Amsterdam (2006). https://doi.org/10.1016/j.entcs.2006.09.007

[48] Hu, Y.-C., Maltz, D.A., Johnson, D.B.: The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. RFC 4728. IETF, (2007). IETF. https://datatracker.ietf.org/doc/rfc4728/

[49] Johnson, D.B., Maltz, D.A., Broch, J.: DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. In: Ad Hoc Networking, pp. 139–172. Addison-Wesley, Boston (2001). https://www.microsoft.com/en-us/research/publication/dsr-dynamic-source-routing-protocol-multi-hop-wireless-ad-hoc-networks/

[50] Belina, F., Hogrefe, D.: The CCITT-specification and description language SDL. Comput. Netw. ISDN Syst. **16**(4), 311–341 (1989) https://doi.org/10.1016/0169-7552(89)90078-0

[51] Andrés, C., Maag, S., Cavalli, A.R., Merayo, M.G., Núñez, M.: Analysis of the OLSR protocol by using formal passive testing. In: Proc. 16th Asia-Pacific Software Engineering Conference (APSEC), pp. 152–159. IEEE, New York (2009). https://doi.org/10.1109/APSEC.2009.37

[52] Lalanne, F., Maag, S.: Datamonitor - A formal approach for passively testing a MANET routing protocol. In: Proc. 9th Wireless Communications and Mobile Computing Conference (IWCMC), pp. 207–212. IEEE, New York (2013). https://doi.org/10.1109/IWCMC.2013.6583560

[53] Hedrick, C.: Routing Information Protocol. RFC 1058. IETF, (1988). IETF. https://datatracker.ietf.org/doc/html/rfc1058

[54] Larsen, K.G., Pettersson, P., Yi, W.: Uppaal in a nutshell. Int. J. Softw. Tools Technol. Transf. **1**(1-2), 134–152 (1997) https://doi.org/10.1007/s100090050010

[55] Wibling, O., Parrow, J., Pears, A.N.: Ad hoc routing protocol verification through broadcast abstraction. In: Proc. 25th IFIP WG 6.1 Conference on Formal Techniques for Networked and Distributed Systems (FORTE). LNCS, vol. 3731, pp. 128–142. Springer, Heidelberg (2005). https://doi.org/10.1007/11562436_11

[56] Chiyangwa, S., Kwiatkowska, M.Z.: A timing analysis of AODV. In: Proc. 7th IFIP WG 6.1 Conference on Formal Methods for Open Object-Based Distributed Systems (FMOODS). LNCS, vol. 3535, pp. 306–321. Springer, Heidelberg (2005). https://doi.org/10.1007/11494881_20

[57] Chaudhary, K., Fehnker, A., Mehta, V.: Modelling, verification, and comparative performance analysis of the B.A.T.M.A.N. protocol. In: Proc. 2nd Workshop on Models for Formal Analysis of Real Systems (MARS@ETAPS). EPTCS, vol. 244, pp. 53–65 (2017). https://doi.org/10.4204/EPTCS.244.3

[58] Furlan, D.: Improving B.A.T.M.A.N. routing stability and performance. Master's thesis, Universtità degli Studi di Trento (2012). https://www.semanticscholar.org/paper/Improving-B.A.T.M.A.N.-Routing-Stability-and-Cigno-Furlan/e73b1615721f5c2adb4d0f2129d10419b133e7f7

[59] Neumann, A., Aichele, C., Lindner, M., Wunderlich, S.: Better Approach To Mobile Ad-hoc Networking (B.A.T.M.A.N.). Draft. IETF, (2008). IETF. https://datatracker.ietf.org/doc/html/draft-wunderlich-openmesh-manet-routing-00

[60] Fehnker, A., Chaudhary, K., Mehta, V.: An even better approach - Improving the B.A.T.M.A.N. protocol through formal modelling and analysis. In: Proc. 10th NASA Formal Methods Symposium (NFM). LNCS, vol. 10811, pp. 164–178. Springer, Heidelberg (2018). https://doi.org/10.1007/978-3-319-77935-5_12

[61] Kamali, M., Höfner, P., Kamali, M., Petre, L.: Formal analysis of proactive, distributed routing. In: Proc. 13th Conference on Software Engineering and Formal Methods (SEFM). LNCS, vol. 9276, pp. 175–189. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-319-22969-0_13

[62] Kamali, M., Petre, L.: Improved recovery for proactive, distributed routing. In: Proc. 20th Conference on Engineering of Complex Computer Systems (ICECCS), pp. 178–181. IEEE, New York (2015). https://doi.org/10.1109/ICECCS.2015.27

[63] Mouradian, A., Augé-Blum, I.: Formal verification of real-time wireless sensor networks protocols: Scaling up. In: Proc. 26th Euromicro Conference on Real-Time Systems (ECRTS), pp. 41–50. IEEE, New York (2014). https://doi.org/10.1109/ECRTS.2014.12

[64] Schmitt, J.B., Roedig, U.: Sensor network calculus - A framework for worst case analysis. In: Proc. 1st Conference in Distributed Computing in Sensor Systems (DCOSS). LNCS, vol. 3560, pp. 141–154. Springer, Heidelberg (2005). https://doi.org/10.1007/11502593_13

[65] Mouradian, A., Augé-Blum, I., Valois, F.: RTXP: A localized real-time MAC-routing protocol for wireless sensor networks. Comput. Networks **67**, 43–59 (2014) https://doi.org/10.1016/j.comnet.2014.03.020

[66] Hammal, Y., Seddiki, M., Benchaïba, M., Abdelli, A.: Formal specification and analysis of a cross-layer overlay P2P construction protocol over MANETs. In: Proc. 18th Wireless Communications and Networking Conference (WCNC), pp.

1–6. IEEE, New York (2017). https://doi.org/10.1109/WCNC.2017.7925622

[67] Höfner, P., McIver, A.: Statistical model checking of wireless mesh routing protocols. In: Proc. 5th NASA Formal Methods Symposium (NFM). LNCS, vol. 7871, pp. 322–336. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38088-4_22

[68] David, A., Larsen, K.G., Legay, A., Mikučionis, M., Poulsen, D.B.: Uppaal SMC tutorial. Int. J. Softw. Tools Technol. Transf. **17**(4), 397–415 (2015) https://doi.org/10.1007/s10009-014-0361-y

[69] Dal Corso, A., Macedonio, D., Merro, M.: Statistical model checking of ad hoc routing protocols in lossy grid networks. In: Proc. 7th NASA Formal Methods Symposium (NFM). LNCS, vol. 9058, pp. 112–126. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-319-17524-9_9

[70] Kamali, M., Merro, M., Dal Corso, A.: AODVv2: Performance vs. loop freedom. In: Proc. 44th Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM). LNCS, vol. 10706, pp. 337–350. Springer, Heidelberg (2018). https://doi.org/10.1007/978-3-319-73117-9_24

[71] Kamali, M., Fehnker, A.: Adaptive formal framework for WMN routing protocols. In: Proc. 15th Conference on Formal Aspects of Component Software (FACS). LNCS, vol. 11222, pp. 175–195. Springer, Heidelberg (2018). https://doi.org/10.1007/978-3-030-02146-7_9

[72] Herberg, U., Clausen, T.H.: Security issues in the optimized link state routing protocol version 2 (OLSRv2). Int. J. Netw. Secur. Appl. **2**(2), 162–181 (2010) https://doi.org/10.5121/ijnsa.2010.2213

[73] Thayer, F.J., Herzog, J.C., Guttman, J.D.: Strand spaces: Proving security protocols correct. J. Comput. Secur. **7**(1), 191–230 (1999) https://doi.org/10.3233/JCS-1999-72-304

[74] Song, D.X.: Athena: A new efficient automatic checker for security protocol analysis. In: Proc. 12th Computer Security Foundations Workshop (CSFW), pp. 192–202. IEEE, New York (1999). https://doi.org/10.1109/CSFW.1999.779773

[75] Yang, S., Baras, J.S.: Modeling vulnerabilities of ad hoc routing protocols. In: Proc. 1st Workshop on Security of Ad Hoc and Sensor Networks (SASN), pp. 12–20. ACM, New York (2003). https://doi.org/10.1145/986858.986861

[76] Hu, Y., Perrig, A., Johnson, D.B.: Ariadne: A secure on-demand routing protocol for ad hoc networks. Wirel. Networks **11**(1-2), 21–38 (2005) https://doi.org/10.1007/s11276-004-4744-y

[77] Ács, G., Buttyán, L., Vajda, I.: Provably secure on-demand source routing in

mobile ad hoc networks. IEEE Trans. Mob. Comput. **5**(11), 1533–1546 (2006) https://doi.org/10.1109/TMC.2006.170

[78] Burmester, M., de Medeiros, B.: On the security of route discovery in MANETs. IEEE Trans. Mob. Comput. **8**(9), 1180–1188 (2009) https://doi.org/10.1109/TMC.2009.13

[79] Benetti, D., Merro, M., Viganò, L.: Model checking ad hoc network routing protocols: ARAN vs. endairA. In: Proc. 8th Conference on Software Engineering and Formal Methods (SEFM), pp. 191–202. IEEE, New York (2010). https://doi.org/10.1109/SEFM.2010.24

[80] Armando, A., Basin, D.A., Boichut, Y., Chevalier, Y., Compagna, L., Cuéllar, J., Hankes Drielsma, P., Héam, P., Kouchnarenko, O., Mantovani, J., Mödersheim, S., von Oheimb, D., Rusinowitch, M., Santiago, J., Turuani, M., Viganò, L., Vigneron, L.: The AVISPA tool for the automated validation of internet security protocols and applications. In: Proc. 17th Conference on Computer Aided Verification (CAV). LNCS, vol. 3576, pp. 281–285. Springer, Heidelberg (2005). https://doi.org/10.1007/11513988_27

[81] Sanzgiri, K., LaFlamme, D., Dahill, B., Levine, B.N., Shields, C., Belding-Royer, E.M.: Authenticated routing for ad hoc networks. IEEE J. Sel. Areas Commun. **23**(3), 598–610 (2005) https://doi.org/10.1109/JSAC.2004.842547

[82] Godskesen, J.C.: Formal verification of the ARAN protocol using the applied π-calculus. In: Proc. 6th IFIP WG 1.7 Workshop on Issues in the Theory of Security (WITS) (2006). http://www.itu.dk/~jcg/Papers/ARAN-APPpi.pdf

[83] Blanchet, B.: Automatic verification of security protocols in the symbolic model: The verifier ProVerif. In: Foundations of Security Analysis and Design VII (FOSAD), Tutorial Lectures. LNCS, vol. 8604, pp. 54–87. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-319-10082-1_3

[84] Pura, M., Patriciu, V.V., Bica, I.: Simulation of an identity-based cryptography scheme for ad hoc networks. In: Proc. 6th Conference on Security and Cryptography (SECRYPT), pp. 135–139. INSTICC Press, Lisbon (2009). https://www.naun.org/main/UPress/cc/19-311.pdf

[85] Pura, M., Buchs, D.: Symbolic model checking of security protocols for ad hoc networks on any topologies. Trans. Petri Nets Other Model. Concurr. **10**, 109–130 (2015) https://doi.org/10.1007/978-3-662-48650-4_6

[86] Hostettler, S., Marechal, A., Linard, A., Risoldi, M., Buchs, D.: High-level Petri net model checking with AlPiNA. Fundam. Informaticae **113**(3-4), 229–264 (2011) https://doi.org/10.3233/FI-2011-608

[87] Sosnovich, A., Grumberg, O., Nakibly, G.: Finding security vulnerabilities in

a network protocol using parameterized systems. In: Proc. 25th Conference on Computer Aided Verification (CAV). LNCS, vol. 8044, pp. 724–739. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39799-8_51

[88] Clarke, E.M., Kroening, D., Lerda, F.: A tool for checking ANSI-C programs. In: Proc. 10th Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS). LNCS, vol. 2988, pp. 168–176. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24730-2_15

[89] Nakibly, G., Kirshon, A., Gonikman, D., Boneh, D.: Persistent OSPF attacks. In: Proc. 19th Network and Distributed System Security Symposium (NDSS). The Internet Society, Reston (2012). https://www.ndss-symposium.org/wp-content/uploads/2017/09/P01_3.pdf

[90] Nakibly, G., Sosnovich, A., Menahem, E., Waizel, A., Elovici, Y.: OSPF vulnerability to persistent poisoning attacks: A systematic analysis. In: Proc. 30th Annual Computer Security Applications Conference (ACSAC), pp. 336–345. ACM, New York (2014). https://doi.org/10.1145/2664243.2664278

[91] Darville, C., Höfner, P., Ivankovic, F., Pam, A.: Advanced models for the OSPF routing protocol. In: Proc. 5th Workshop on Models for Formal Analysis of Real Systems (MARS@ETAPS). EPTCS, vol. 355, pp. 13–26 (2022). https://doi.org/10.4204/EPTCS.355.2

[92] Andel, T.R., Back, G., Yasinsac, A.: Automating the security analysis process of secure ad hoc routing protocols. Simul. Model. Pract. Theory **19**(9), 2032–2049 (2011) https://doi.org/10.1016/j.simpat.2011.05.008

[93] Papadimitratos, P., Haas, Z.J.: Secure routing for mobile ad hoc networks. In: Proc. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), pp. 1–13 (2002)

[94] Cortier, V., Degrieck, J., Delaune, S.: Analysing routing protocols: Four nodes topologies are sufficient. In: Proc. 1st Conference on Principles of Security and Trust (POST). LNCS, vol. 7215, pp. 30–50. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-28641-4_3

[95] Berton, S., Yin, H., Lin, C., Min, G.: Secure, disjoint, multipath source routing protocol (SDMSR) for mobile ad-hoc networks. In: Proc. 5th Conference on Grid and Cooperative Computing (GCC). IEEE, New York (2006). https://doi.org/10.1109/GCC.2006.86

[96] Nanz, S., Hankin, C.: A framework for security analysis of mobile wireless networks. Theor. Comput. Sci. **367**(1-2), 203–227 (2006) https://doi.org/10.1016/j.tcs.2006.08.036

[97] Arnaud, M., Cortier, V., Delaune, S.: Modeling and verifying ad hoc routing

protocols. Inf. Comput. **238**, 30–67 (2014) https://doi.org/10.1016/j.ic.2014.07.004

[98] Godskesen, J.C.: A calculus for mobile ad hoc networks. In: Proc. 9th Conference on Coordination Models and Languages (COORDINATION). LNCS, vol. 4467, pp. 132–150. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-72794-1_8

[99] Godskesen, J.C.: A calculus for mobile ad-hoc networks with static location binding. In: Proc. 15th Workshop on Expressiveness in Concurrency (EXPRESS). ENTCS, vol. 242, pp. 161–183. Elsevier, Amsterdam (2008). https://doi.org/10.1016/j.entcs.2009.06.018

[100] Merro, M.: An observational theory for mobile ad hoc networks (full version). Inf. Comput. **207**(2), 194–208 (2009) https://doi.org/10.1016/j.ic.2007.11.010

[101] Merro, M., Sibilio, E.: A calculus of trustworthy ad hoc networks. Formal Aspects Comput. **25**(5), 801–832 (2013) https://doi.org/10.1007/s00165-011-0210-7

[102] Ghassemi, F., Fokkink, W.J., Movaghar, A.: Restricted broadcast process theory. In: Proc. 6th Conference on Software Engineering and Formal Methods (SEFM), pp. 345–354. IEEE, New York (2008). https://doi.org/10.1109/SEFM.2008.25

[103] Ghassemi, F., Fokkink, W.J., Movaghar, A.: Equational reasoning on mobile ad hoc networks. Fundam. Informaticae **105**(4), 375–415 (2010) https://doi.org/10.3233/FI-2010-371

[104] Ghassemi, F., Fokkink, W.J., Movaghar, A.: Verification of mobile ad hoc networks: An algebraic approach. Theor. Comput. Sci. **412**(28), 3262–3282 (2011) https://doi.org/10.1016/j.tcs.2011.03.017

[105] Ghassemi, F., Fokkink, W.J.: Reliable restricted process theory. Fundam. Informaticae **165**(1), 1–41 (2019) https://doi.org/10.3233/FI-2019-1775

[106] Kouzapas, D., Philippou, A.: A process calculus for dynamic networks. In: Proc. Joint 13th IFIP WG 6.1 Conference on Formal Methods for Open Object-Based Distributed Systems and 31st IFIP WG 6.1 Conference on Formal Techniques for Distributed Systems (FMOODS/FORTE). LNCS, vol. 6722, pp. 213–227. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-21461-5_14

[107] Vasudevan, S., Kurose, J.F., Towsley, D.F.: Design and analysis of a leader election algorithm for mobile ad hoc networks. In: Proc. 12th Conference on Network Protocols (ICNP), pp. 350–360. IEEE, New York (2004). https://doi.org/10.1109/ICNP.2004.1348124

[108] Ghassemi, F., Talebi, M., Movaghar, A., Fokkink, W.J.: Stochastic restricted broadcast process theory. In: Proc. 8th European Performance Engineering

Workshop (EPEW). LNCS, vol. 6977, pp. 72–86. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24749-1_7

[109] Fehnker, A., van Glabbeek, R.J., Höfner, P., McIver, A., Portmann, M., Tan, W.L.: A process algebra for wireless mesh networks. In: Proc. 21st European Symposium on Programming (ESOP). LNCS, vol. 7211, pp. 295–315. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-28869-2_15

[110] Fehnker, A., van Glabbeek, R.J., Höfner, P., McIver, A., Portmann, M., Tan, W.L.: Automated analysis of AODV using UPPAAL. In: Proc. 18th Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS). LNCS, vol. 7214, pp. 173–187. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-28756-5_13

[111] Höfner, P., van Glabbeek, R.J., Tan, W.L., Portmann, M., McIver, A., Fehnker, A.: A rigorous analysis of AODV and its variants. In: Proc. 15th Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), pp. 203–212. ACM, New York (2012). https://doi.org/10.1145/2387238.2387274

[112] van Glabbeek, R.J., Höfner, P., Portmann, M., Tan, W.L.: Modelling and verifying the AODV routing protocol. Distributed Comput. **29**(4), 279–315 (2016) https://doi.org/10.1007/s00446-015-0262-7

[113] Bourke, T., van Glabbeek, R.J., Höfner, P.: A mechanized proof of loop freedom of the (untimed) AODV routing protocol. In: Proc. 12th Symposium on Automated Technology for Verification and Analysis (ATVA). LNCS, vol. 8837, pp. 47–63. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-319-11936-6_5

[114] Paulson, L.C.: Isabelle - A Generic Theorem Prover. LNCS, vol. 828. Springer, Heidelberg (1994). https://doi.org/10.1007/BFb0030541

[115] Bourke, T., van Glabbeek, R.J., Höfner, P.: Mechanizing a process algebra for network protocols. J. Autom. Reason. **56**(3), 309–341 (2016) https://doi.org/10.1007/s10817-015-9358-9

[116] van Glabbeek, R.J., Höfner, P., van der Wal, D.: Analysing AWN-specifications using mCRL2 (extended abstract). In: Proc. 14th Conference on Integrated Formal Methods (IFM). LNCS, vol. 11023, pp. 398–418. Springer, Heidelberg (2018). https://doi.org/10.1007/978-3-319-98938-9_23

[117] Bres, E., van Glabbeek, R.J., Höfner, P.: A timed process algebra for wireless networks with an application in routing (extended abstract). In: Proc. 25th European Symposium on Programming (ESOP). LNCS, vol. 9632, pp. 95–122. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49498-1_5

[118] Barry, R., van Glabbeek, R.J., Höfner, P.: Formalising the optimised link state

routing protocol. In: Proc. 4th Workshop on Models for Formal Analysis of Real Systems (MARS@ETAPS). EPTCS, vol. 316, pp. 40–71 (2020). https://doi.org/10.4204/EPTCS.316.3

[119] Drury, J., Höfner, P., Wang, W.: Formal models of the OSPF routing protocol. In: Proc. 4th Workshop on Models for Formal Analysis of Real Systems (MARS@ETAPS). EPTCS, vol. 316, pp. 72–120 (2020). https://doi.org/10.4204/EPTCS.316.4

[120] Lanese, I., Sangiorgi, D.: An operational semantics for a calculus for wireless systems. Theor. Comput. Sci. **411**(19), 1928–1948 (2010) https://doi.org/10.1016/j.tcs.2010.01.023

[121] Wang, M., Lu, Y.: A timed calculus for mobile ad hoc networks. In: Proc. 1st Workshop on Formal Techniques for Safety-Critical Systems (FTSCS). EPTCS, vol. 105, pp. 118–134 (2012). https://doi.org/10.4204/EPTCS.105.9

[122] Chen, N., Zhu, H.: IoT modeling and verification: From the CaIT calculus to Uppaal. IEICE Trans. Inf. Syst. **106**(9), 1507–1518 (2023) https://doi.org/10.1587/TRANSINF.2022EDP7223

[123] Lanotte, R., Merro, M.: A semantic theory of the Internet of Things. Inf. Comput. **259**(1), 72–101 (2018) https://doi.org/10.1016/J.IC.2018.01.001

[124] Milner, R., Parrow, J., Walker, D.: A calculus of mobile processes, I + II. Inf. Comput. **100**(1), 1–77 (1992) https://doi.org/10.1016/0890-5401(92)90008-4

[125] Cardelli, L., Gordon, A.D.: Mobile ambients. Theor. Comput. Sci. **240**(1), 177–213 (2000) https://doi.org/10.1016/S0304-3975(99)00231-5

[126] Sewell, P., Wojciechowski, P.T., Pierce, B.C.: Location-independent communication for mobile agents: A two-level architecture. In: Proc. ICCL Workshop on Internet Programming Languages. LNCS, vol. 1686, pp. 1–31. Springer, Heidelberg (1998). https://doi.org/10.1007/3-540-47959-7_1

[127] Sewell, P., Wojciechowski, P.T., Unyapoth, A.: Nomadic Pict: Programming languages, communication infrastructure overlays, and semantics for mobile computation. ACM Trans. Program. Lang. Syst. **32**(4), 12–11263 (2010) https://doi.org/10.1145/1734206.1734209

[128] Ene, C., Muntean, T.: A broadcast-based calculus for communicating systems. In: Proc. 6th IPDPS Workshop on Formal Methods for Parallel Programming: Theory and Applications (FMPPTA). IEEE, New York (2001). https://doi.org/10.1109/IPDPS.2001.925136

[129] Prasad, K.V.S.: A prospectus for mobile broadcasting systems. In: Proc. Workshop "Essays on Algebraic Process Calculi" (APC 25). ENTCS, vol. 162, pp.

295–300. Elsevier, Amsterdam (2006). https://doi.org/10.1016/j.entcs.2005.12.096

[130] Singh, A., Ramakrishnan, C.R., Smolka, S.A.: A process calculus for mobile ad hoc networks. Sci. Comput. Program. **75**(6), 440–469 (2010) https://doi.org/10.1016/j.scico.2009.07.008

[131] Bengtson, J., Johansson, M., Parrow, J., Victor, B.: Psi-calculi: A framework for mobile processes with nominal data and logic. Log. Methods Comput. Sci. **7**(1) (2011) https://doi.org/10.2168/LMCS-7(1:11)2011

[132] Borgström, J., Huang, S., Johansson, M., Raabjerg, P., Victor, B., Pohjola, J.Å., Parrow, J.: Broadcast psi-calculi with an application to wireless protocols. In: Proc. 9th Conference on Software Engineering and Formal Methods (SEFM). LNCS, vol. 7041, pp. 74–89. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24690-6_7

[133] Godskesen, J.C., Hüttel, H., Kühnrich, M.: Verification of correspondence assertions in a calculus for mobile ad hoc networks. In: Proc. 7th Workshop on the Foundations of Coordination Languages and Software Architectures (FOCLASA). ENTCS, vol. 229, pp. 77–93. Elsevier, Amsterdam (2009). https://doi.org/10.1016/j.entcs.2009.06.030

[134] Hennessy, M.C.B.: A Distributed Pi-calculus. Cambridge University Press, Cambridge (2007). https://doi.org/10.1017/CBO9780511611063

[135] Abadi, M., Gordon, A.D.: A calculus for cryptographic protocols: The spi calculus. In: Proc. 4th Conference on Computer and Communications Security (CCS), pp. 36–47. ACM, New York (1997). https://doi.org/10.1145/266420.266432

[136] Perkins, C.E.: IP Mobility Support. RFC 2002. IETF, (1996). IETF. https://datatracker.ietf.org/doc/html/rfc2002

[137] Godskesen, J.C.: Observables for mobile and wireless broadcasting systems. In: Proc. 12th Conference on Coordination Models and Languages (COORDINATION). LNCS, vol. 6116, pp. 1–15. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13414-2_1

[138] Abadi, M., Fournet, C.: Mobile values, new names, and secure communication. In: Proc. 28th Symposium on Principles of Programming Languages (POPL), pp. 104–115. ACM, New York (2001). https://doi.org/10.1145/360204.360213

[139] Chrétien, R., Delaune, S.: Formal analysis of privacy for routing protocols in mobile ad hoc networks. In: Proc. 2nd Conference on Principles Of Security and Trust (POST). LNCS, vol. 7796, pp. 1–20. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36830-1_1

[140] Kong, J., Hong, X.: ANODR: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks. In: Proc. 4th Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 291–302. ACM, New York (2003). https://doi.org/10.1145/778415.778449

[141] Prasad, K.V.S.: A calculus of broadcasting systems. Sci. Comput. Program. **25**(2-3), 285–327 (1995) https://doi.org/10.1016/0167-6423(95)00017-8

[142] Roman, G., McCann, P.J., Plun, J.Y.: Mobile UNITY: Reasoning and specification in mobile computing. ACM Trans. Softw. Eng. Methodol. **6**(3), 250–282 (1997) https://doi.org/10.1145/258077.258079

[143] Chandy, K.M., Misra, J.: Parallel Program Design: A Foundation. Addison-Wesley, Boston (1988)

[144] Smith, G.: The Object-Z Specification Language. Advances in Formal Methods. Kluwer, Alphen aan den Rijn (2000). https://doi.org/10.1007/978-1-4615-5265-9

[145] Smith, G.: A framework for modelling and analysing mobile systems. In: Proc. 27th Australasian Computer Science Conference (ACSC2004). CRPIT, vol. 26, pp. 193–202. Australian Computer Society, Sydney (2004). http://crpit.scem.westernsydney.edu.au/abstracts/CRPITV26Smith.html

[146] Wu, X., Sanders, J.W., Zhu, H.: Formal modelling and analysis of AODV. In: Proc. 18th Conference on Engineering of Complex Computer Systems (ICECCS), pp. 93–100. IEEE, New York (2013). https://doi.org/10.1109/ICECCS.2013.22

[147] Kamali, M., Petre, L.: Modelling link state routing in Event-B. In: Proc. 21st Conference on Engineering of Complex Computer Systems (ICECCS), pp. 207–210. IEEE, New York (2016). https://doi.org/10.1109/ICECCS.2016.035

[148] Abrial, J.-R.: Modeling in Event-B: System an Software Design. Cambridge University Press, Cambridge (2010). https://doi.org/10.1017/CBO9781139195881

[149] Kamali, M., Petre, L.: Uppaal vs Event-B for modelling optimised link state routing. In: Proc. 11th Conference on Verification and Evaluation of Computer and Communication Systems (VECoS). LNCS, vol. 10466, pp. 189–203. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-319-66176-6_13

[150] Fakhfakh, F., Tounsi, M., Kacem, A.H., Mosbah, M.: Towards a formal model for dynamic networks through refinement and evolving graphs. In: Revised Selected Papers from Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNDP). Studies in Computational Intelligence, vol. 612, pp. 227–243. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-319-23509-7_16

[151] Ferreira, A.: Building a reference combinatorial model for MANETs. IEEE Netw. **18**(5), 24–29 (2004) https://doi.org/10.1109/MNET.2004.1337732

[152] Gurevich, Y.: Evolving algebras 1993: Lipari guide. In: Börger, E. (ed.) Specification and Validation Methods, pp. 9–36. Oxford University Press, Oxford (1993). https://www.researchgate.net/publication/2241959_Evolving_Algebras_1993_Lipari_Guide

[153] Benczúr, A.A., Glässer, U., Lukovszki, T.: Formal description of a distributed location service for mobile ad hoc networks. In: Proc. 10th Workshop on Abstract State Machines, Advances in Theory and Practice (ASM). LNCS, vol. 2589, pp. 204–217. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-36498-6_11

[154] Glässer, U., Gu, Q.: Formal description and analysis of a distributed location service for mobile ad hoc networks. Theor. Comput. Sci. **336**(2-3), 285–309 (2005) https://doi.org/10.1016/j.tcs.2004.11.009

[155] Glässer, U., Prinz, A.: ASM and SDL models of geographic routing in mobile ad hoc networks. In: Proc. 12th SDL Forum. LNCS, vol. 3530, pp. 162–173. Springer, Heidelberg (2005). https://doi.org/10.1007/11506843_11

[156] Rockström, A., Saracco, R.: SDL-CCITT specification and description language. IEEE Trans. Commun. **30**(6), 1310–1318 (1982) https://doi.org/10.1109/TCOM.1982.1095599

[157] Bianchi, A., Pizzutilo, S., Vessio, G.: Suitability of abstract state machines for discussing mobile ad-hoc networks. Global Journal of Advanced Software Engineering **1**, 29–38 (2014). https://www.researchgate.net/publication/268813941_Suitability_of_Abstract_State_Machines_for_Discussing_Mobile_Ad-hoc_Networks

[158] Bianchi, A., Pizzutilo, S., Vessio, G.: Intercepting blackhole attacks in MANETs: An ASM-based model. In: Proc. 1st Workshop on Formal Approaches for Advanced Computing Systems (FAACS). LNCS, vol. 10729, pp. 137–152. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-319-74781-1_10

[159] Hoffmann, K., Mossakowski, T.: Algebraic higher-order nets: Graphs and Petri nets as tokens. In: Proc. 16th Workshop on Recent Trends in Algebraic Development Techniques (WADT). LNCS, vol. 2755, pp. 253–267. Springer, Heidelberg (2002). https://doi.org/10.1007/978-3-540-40020-2_14

[160] Bottoni, P., De Rosa, F., Hoffmann, K., Mecella, M.: Applying algebraic approaches for modeling workflows and their transformations in mobile networks. Mob. Inf. Syst. **2**(1), 51–76 (2006) https://doi.org/10.1155/2006/704187

[161] Padberg, J., Hoffmann, K., Ehrig, H., Modica, T., Biermann, E., Ermel, C.:

Maintaining consistency in layered architectures of mobile ad-hoc networks. In: Proc. 10th Conference on Fundamental Approaches to Software Engineering (FASE). LNCS, vol. 4422, pp. 383–397. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-71289-3_29

[162] Biermann, E., Hoffmann, K., Padberg, J.: Layered architecture consistency for MANETs: Introducing new team members. Electron. Commun. Eur. Assoc. Softw. Sci. Technol. **12** (2008) https://doi.org/10.14279/tuj.eceasst.12.269

[163] Archibald, B., Kulcsár, G., Sevegnani, M.: A tale of two graph models: A case study in wireless sensor networks. Form. Asp. Comp. **33**(6), 1249–1277 (2021) https://doi.org/10.1007/s00165-021-00558-z

[164] Ehrig, H., Pfender, M., Schneider, H.J.: Graph-grammars: An algebraic approach. In: Proc. 14th Symposium on Switching and Automata Theory, pp. 167–180. IEEE, New York (1973). https://doi.org/10.1109/SWAT.1973.11

[165] Milner, R.: Bigraphical reactive systems. In: Proc. 12th Conference on Concurrency Theory (CONCUR). LNCS, vol. 2154, pp. 16–35. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44685-0_2

[166] Albalwe, M., Archibald, B., Sevegnani, M.: Modelling and analysing routing protocols diagrammatically with bigraphs. Formal Aspects Comput. **36**(3), 17–11725 (2024) https://doi.org/10.1145/3685934

[167] Alexander, R., Brandt, A., Vasseur, J.P., Hui, J., Pister, K., Thubert, P., Levis, P., Struik, R., Kelsey, R., Winter, T.: RPL: IPv6 Routing Protocol for Low-power and LossyNetworks. RFC 6550. IETF, (2012). IETF. https://www.rfc-editor.org/info/rfc6550

[168] Camp, T., Boleng, J., Davies, V.: A survey of mobility models for ad hoc network research. Wirel. Commun. Mob. Comput. **2**, 483–502 (2002) https://doi.org/10.1002/wcm.72

[169] Patsouris, P.A.: Algebraic modeling of an ad hoc network for mobile computing. J. Parallel Distributed Comput. **61**(7), 884–897 (2001) https://doi.org/10.1006/jpdc.2000.1718

[170] Romanowska, A.B., Smith, J.D.H.: Modal Theory: An Algebraic Approach to Order, Geometry, and Convexity. Heldermann Verlag, Berlin (1983)

[171] Höfner, P., McIver, A.: Hopscotch - Reaching the target hop by hop. J. Log. Algebraic Methods Program. **83**(2), 212–224 (2014) https://doi.org/10.1016/j.jlap.2014.02.009

[172] Godskesen, J.C., Nanz, S.: Mobility models and behavioural equivalence for

wireless networks. In: Proc. 11th Conference on Coordination Models and Languages (COORDINATION). LNCS, vol. 5521, pp. 106–122. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-02053-7_6

[173] Wu, X., Liu, S., Zhu, H., Zhao, Y.: Reasoning about group-based mobility in MANETs. In: Proc. 20th Pacific Rim Symposium on Dependable Computing, (PRDC), pp. 244–253. IEEE, New York (2014). https://doi.org/10.1109/PRDC.2014.39

[174] Pei, G., Gerla, M., Hong, X., Chiang, C.: A wireless hierarchical routing protocol with group mobility. In: Proc. Wireless Communications and Networking Conference, (WCNC), pp. 1538–1542. IEEE, New York (1999). https://doi.org/10.1109/WCNC.1999.796996

[175] Song, L., Godskesen, J.C.: Probabilistic mobility models for mobile and wireless networks. In: Proc. 6th IFIP WG 2.2 Conference on Theoretical Computer Science (IFIP TCS). IFIP Advances in Information and Communication Technology, vol. 323, pp. 86–100. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-15240-5_7

[176] Cheshire, S., Aboba, B., Guttman, E.: Dynamic Configuration of IPv4 Link-Local Addresses. RFC 3927. IETF, (2005). IETF. https://datatracker.ietf.org/doc/html/rfc3927

[177] Song, L., Godskesen, J.C.: Broadcast abstraction in a stochastic calculus for mobile networks. In: Proc. 7th IFIP WG 2.2 Conference on Theoretical Computer Science (IFIP TCS). LNCS, vol. 7604, pp. 342–356. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-33475-7_24

[178] Ghassemi, F., Movaghar, A., Fokkink, W.J.: Towards performance evaluation of mobile ad hoc network protocols. In: Proc. 10th Conference on Application of Concurrency to System Design (ACSD), pp. 85–92. IEEE, New York (2010). https://doi.org/10.1109/ACSD.2010.20

[179] Hinton, A., Kwiatkowska, M.Z., Norman, G., Parker, D.: PRISM: A tool for automatic verification of probabilistic systems. In: Proc. 12th Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS). LNCS, vol. 3920, pp. 441–444. Springer, Heidelberg (2006). https://doi.org/10.1007/11691372_29

[180] Mouradian, A., Augé-Blum, I.: Formal verification of real-time wireless sensor networks protocols with realistic radio links. In: Proc. 21st Conference on Real-Time Networks and Systems (RTNS), pp. 213–222. ACM, New York (2013). https://doi.org/10.1145/2516821.2516833

[181] Roedig, U., Barroso, A.M., Sreenan, C.J.: f-MAC: A deterministic media access control protocol without time synchronization. In: Proc. 3rd European Workshop

on Wireless Sensor Networks (EWSN). LNCS, vol. 3868, pp. 276–291. Springer, Heidelberg (2006). https://doi.org/10.1007/11669463_21

[182] Kamali, M., Katoen, J.: Probabilistic model checking of AODV. In: Proc. 17th Conference on Quantitative Evaluation of Systems (QEST). LNCS, vol. 12289, pp. 54–73. Springer, Heidelberg (2020). https://doi.org/10.1007/978-3-030-59854-9_6

[183] Bohnenkamp, H.C., D'Argenio, P.R., Hermanns, H., Katoen, J.: MODEST: A compositional modeling formalism for hard and softly timed systems. IEEE Trans. Software Eng. **32**(10), 812–830 (2006) https://doi.org/10.1109/TSE.2006.104

[184] Fehnker, A., Höfner, P., Kamali, M., Mehta, V.: Topology-based mobility models for wireless networks. In: Proc. 10th Conference on Quantitative Evaluation of Systems (QEST). LNCS, vol. 8054, pp. 389–404. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40196-1_32

[185] van Hoesel, L.F.W., Havinga, P.J.M.: A lightweight medium access protocol (LMAC) for wireless sensor networks: Reducing preamble transmissions and transceiver state switches. In: Proc. 1st Workshop on Networked Sensing Systems (INSS), pp. 205–208 (2004). https://www.researchgate.net/publication/242150051_A_Lightweight_Medium_Access_Protocol_LMAC_for_Wireless_Sensor_Networks_Reducing_Preamble_Transmissions_and_Transceiver_State_Switches

[186] Wu, X., Zhu, H.: A calculus for wireless sensor networks from quality perspective. In: Proc. 16th Symposium on High Assurance Systems Engineering (HASE), pp. 223–231. IEEE, New York (2015). https://doi.org/10.1109/HASE.2015.40

[187] Wu, X., Zhao, Y., Zhu, H.: Integrating a calculus with mobility and quality for wireless sensor networks. In: Proc. 17th Symposium on High Assurance Systems Engineering (HASE), pp. 220–227. IEEE, New York (2016). https://doi.org/10.1109/HASE.2016.29

[188] Wu, X., Zhu, H., Xie, W.: UTP semantics of a calculus for mobile ad hoc networks. In: Proc. 7th Symposium on Unifying Theories of Programming (UTP). LNCS, vol. 11885, pp. 198–216. Springer, Heidelberg (2019). https://doi.org/10.1007/978-3-030-31038-7_10

[189] Xie, W., Zhu, H., Wu, X., Vinh, P.C.: Formal verification of mCWQ using extended Hoare logic. Mob. Networks Appl. **24**(1), 134–144 (2019) https://doi.org/10.1007/s11036-018-1142-8

[190] Hoare, C.A.R.: An axiomatic basis for computer programming. Commun. ACM **12**(10), 576–580 (1969) https://doi.org/10.1145/363235.363259

[191] Liu, S., Ölveczky, P.C., Meseguer, J.: Modeling and analyzing mobile ad hoc networks in Real-Time Maude. J. Log. Algebraic Methods Program. **85**(1), 34–66 (2016) https://doi.org/10.1016/j.jlamp.2015.05.002

[192] Ölveczky, P.C., Meseguer, J.: Real-Time Maude: A tool for simulating and analyzing real-time and hybrid systems. In: Proc. 3rd Workshop on Rewriting Logic and Its Applications (WRLA). ENTCS, vol. 36, pp. 361–382. Elsevier, Amsterdam (2000). https://doi.org/10.1016/S1571-0661(05)80134-3

[193] Lepri, D., Ábrahám, E., Ölveczky, P.C.: Sound and complete timed CTL model checking of timed Kripke structures and real-time rewrite theories. Sci. Comput. Program. **99**, 128–192 (2015) https://doi.org/10.1016/j.scico.2014.06.006

[194] Gallina, L., Marin, A., Rossi, S.: Connectivity and energy-aware preorders for mobile ad-hoc networks. Telecommun. Syst. **63**(2), 307–333 (2016) https://doi.org/10.1007/s11235-015-0122-6

[195] Gallina, L., Marin, A., Rossi, S., Han, T., Kwiatkowska, M.Z.: A process algebraic framework for estimating the energy consumption in ad-hoc wireless sensor networks. In: Proc. 16th Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), pp. 255–262. ACM, New York (2013). https://doi.org/10.1145/2507924.2507958

[196] Haas, Z.J., Halpern, J.Y., Li, L.: Gossip-based ad hoc routing. IEEE/ACM Trans. Netw. **14**(3), 479–491 (2006) https://doi.org/10.1109/TNET.2006.876186

[197] Bugliesi, M., Gallina, L., Hamadou, S., Marin, A., Rossi, S.: Behavioural equivalences and interference metrics for mobile ad-hoc networks. Perform. Evaluation **73**, 41–72 (2014) https://doi.org/10.1016/j.peva.2013.11.003