Overview of Applications of Passive Testing Techniques*

Iosif Itkin[1] and Rostislav Yavorskiy[2]

[1] Exactpro Systems
Suite 3.02, St Clements House, 27 Clements Lane
EC4N 7AE, London, UK
E-mail: iosif.itkin@exactprosystems.com
[2] Surgut State University
Lenina, 1, Surgut
Khanty-Mansiyskiy avtonomnyy okrug, 628403, Russia
E-mail: javorski_re@surgu.ru

Abstract. We present here the overview of recent research on passive testing methods and tools, which covers 104 manually selected papers most relevant to this topic. The papers were classified according to their approaches, methods, and application areas. Each class is summarized in a separate section. Besides, statistics is provided for the publication time, authorship and most popular topics.

1 Introduction

Testing is the most widely used technique to analyze the correctness of complex software systems. Passive testing or monitoring is a process of detecting faults in a system under test (SUT) by observing its behavior without interrupting its normal operations. Logs produced by SUT are recorded and checked against expected behavior according to the specification. Passive testing techniques become highly relevant when there is no access to the system interface or when the system cannot be interrupted from its normal operation. An important aspect of passive monitoring is that observations are obtained from an unknown state in the middle of the execution of the system.

In order to model the SUT behavior many authors use formalism such as finite state machines (FSM) or its extensions (EFSM). Many works use a set of invariants to formalize the expected behaviour of the system. Invariants express the facts that each time the system under test performs a given sequence of actions, it must exhibit a behavior reflected in the invariant. Early passive testing techniques only considered control portions of exchanged packets and ignored data parts. Now testing for data constraints and relations between packets is becoming more and more essential, which requires application of new methods and tools from data science and machine learning. Sometimes active testing

techniques are used alongside the passive testing, while other studies are focused on passive testing only.

1.1 Methodology of the overview

Here we present an overview of recent research on passive testing. In order to gather the collection of relevant papers for the analysis the following three sources were used:

- Google Scholar[4],
- ACM digital library[5],
- IEEE Xplore[6].

Search results for "passive testing" query were analyzed and 104 the most relevant papers were selected. Then, the papers were classified according to their approaches, methods, and application areas. Each class is summarized in a dedicated section below.

1.2 Publications timing and authorship

As it was already mentioned above the data set consists of 104 research papers. Fig. 1 shows distribution of the papers by publication year.

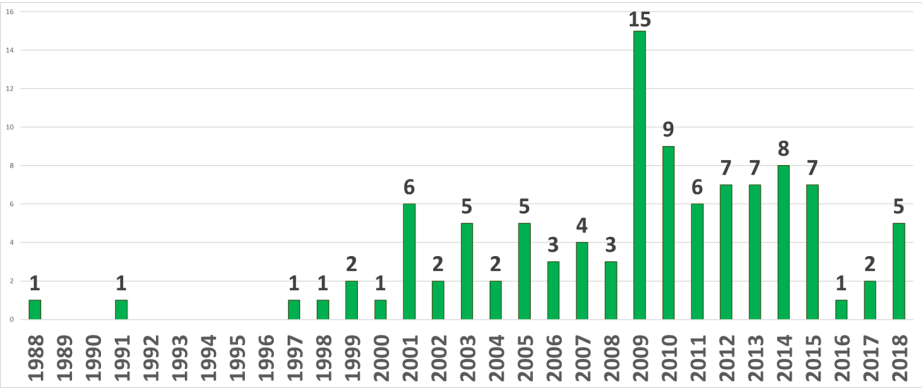

Fig. 1. Distribution of the papers by publication year

The co-authorship graph is presented on Fig. 2. The graph nodes represent authors. Size of node is proportional to the number of papers in the collection, which are co-authored by the researcher. Also, this number is explicitly displayed

[4] https://scholar.google.ru/
[5] https://dl.acm.org/
[6] https://www.ieee.org/publications/xplore/

after the author name. Edge between nodes stands for the collaboration relation. Thickness of the edges indicates the number of the joint papers. If it is 2 or more, then the number is displayed next to the edge.

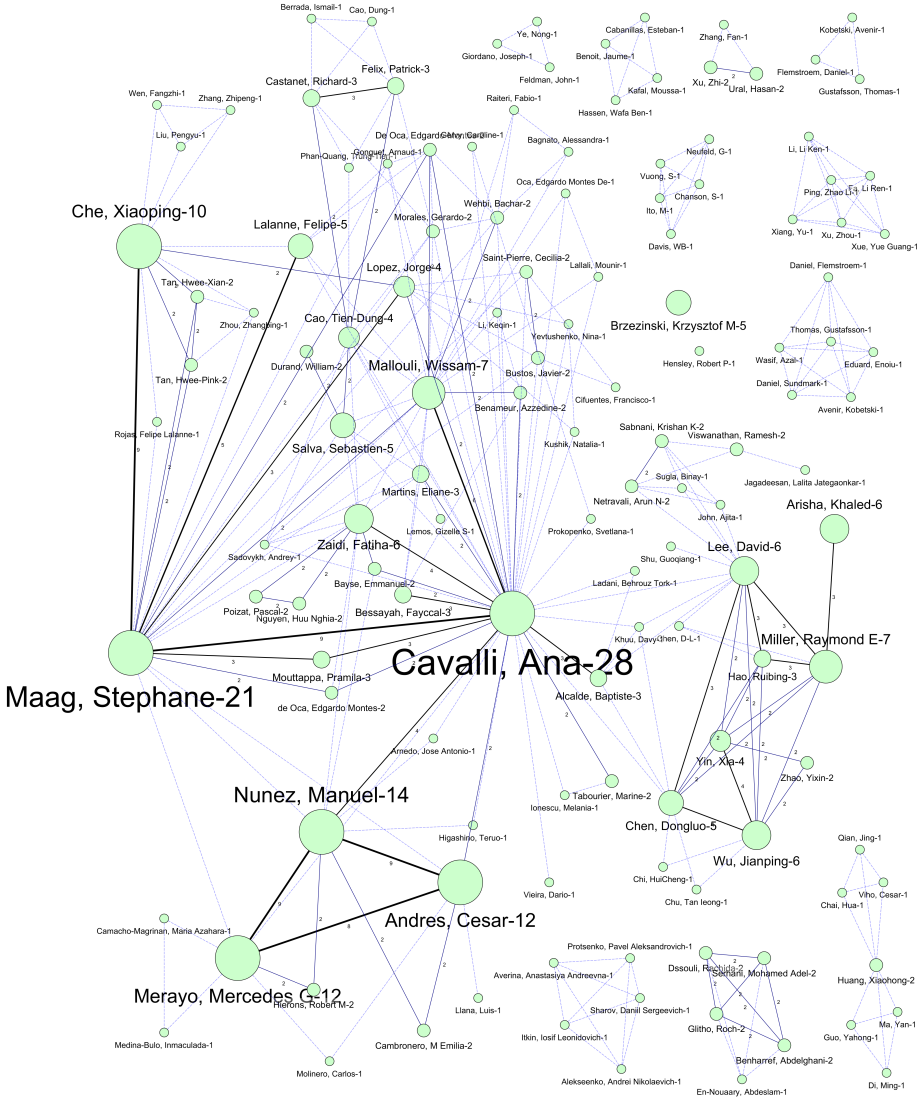

Fig. 2. The co-authorship graph

Word cloud diagram on Fig. 3 is used to visualize the most frequent topics in the collection. One can see that majority of papers are devoted to network

protocols, algorithms for trace analysis, formal requirements and specifications, finite state machines, invariants etc.

1.3 Structure of the paper

The remaining part of this paper presents compilation of manually processed abstracts of the selected papers. From the collection of 104 relevant papers on passive testing we included here those, which have clear focus on application of the technique in practical settings. The text is organized in the following way. Section 2 summarizes papers focused on network protocol testing. Section 3 surveys research on testing of web services. Section 4 is devoted to internet of things applications. Security related testing is covered in section 5. Other specific cases of application of passive testing are collected in section 6.

Fig. 3. The most frequent words in the abstracts of the papers

2 Network Protocol Testing

This section summarizes papers focused on application of passive testing to network protocols.

In [36] Protocol Integrated Test System is introduced to test routing protocols. The system under test is modeled as a black box with windows. The testing covers multiple channels and ports. A passive testing is applied in production field for conformance, interoperability and performance testing. Protocol state machine is used to cover routing information manipulation. OnLine Test System

(OLTS) presented in [39] additionally introduces topology analysis and internal process simulation to perform testing of BGP, OSPF and RIP protocols.

In [25] passive testing algorithm based on extended FSM is applied to TCP protocol. The paper runs experiment to analyse the resulting test coverage for state transitions.

Passive testing on protocols can be applied to detect faults in network devices [26]. Linear programming is used to determine the ranges of the variables to reveal transitions covered by the testing and monitoring.

Practical aspects of testing and monitoring are considered in [9]. The paper presents its own independent approach to practical testing, own protocol monitor and own syntax description tool.

In [6] a passive testing approach based on invariants is introduced. A set of invariants represent the most relevant expected properties of the implementation under test. The presented pattern matching algorithm allows to decide correctness of the proposed variants with respect to a given specification. In additional to theoretical framework a TestInv tool is developed and applied to Wireless Application Protocol (WAP).

Papers [30] and [18] address non-deterministic network protocol specifications and both present case studies applied to Internet protocol and Managed Session Protocol accordingly. The first one is based on implementation machines and the second one enhances the use of a set of invariants that implementation under test should fulfill.

A methodology based on contextual signatures and passive testing with invariants is presented in [38]. The concept of contextual signature offers a framework to add information on the states, the values of parameters and logical connectors to increase the expressive power of invariants. This allows to cover properties related to different layers of the protocol stack and end-to-end communication between distant entities. A correlation algorithm is defined to enable interoperability testing between events collected from different network views.

Process mining and passive testing are applied in [35] to detect anomalies in DNS protocol traces. Multi-actor modeling is based on the sequence of structured activities, queries and responses by clients and servers. A practical example illustrated approach application to identify mail bonnet attack in Internet Life DNS traces.

3 Testing of Web Services

A detailed survey on formal approaches to active and passive testing with applications to the cloud is presented in [19]. Here we mention the most relevant articles.

An approach for EFSM-based passive testing of web services was suggested in see [7]. The authors present an approach to speed up state recognition of EFSM-based observers designed for observation of Web Services. The approach is based on combining observed events and backward walks in the EFSM model to recognize states and appropriately initialize variables.

Efficient traces collection mechanisms for passive testing of web services was suggested in [8]. The authors consider management of Web Services by passive testing where the tester itself is a Web Service. They propose different architectures for observation of simple and composite Web Services. They also study a set of online traces collection mechanisms and discuss their performances in terms of required CPU/RAM resources and introduced network overhead. These performances are then maximized by selecting best locations of observers. Observation considers both functional and non-functional (QoS) properties of Web Services.

Paper [12] proposes an approach to test (actively and passively) Web services composition described in BPEL using TGSE (Test Generation, Simulation and Emulation), that is a tool for generating test cases for Communicating Systems (CS). TGSE implements a generic generation algorithm allowing either test cases derivation or traces checking. It supports the description of one or several components with data and temporal constraints. First, in order to model the BPEL behaviors, the timing constraints, and data variables, the BPEL specification is transformed into the Timed Extended Finite State Machines (TEFSM) model. TGSE can check whether a trace is valid according the specification or not. The Loan Web Service is used as a case study.

In paper [31] the authors choose a non-intrusive approach based on monitoring to propose a conformance passive testing methodology to check that a composed Web service respects its functional requirements. This methodology is based on a set of formal invariants representing properties to be tested including data and time constraints. Passive testing of an industrial system (that uses a composition of Web services) is briefly presented to demonstrate the effectiveness of the proposed approach.

Paper [3] presents a methodology to perform passive testing based on invariants of distributed systems with time information. This approach is supported by the following idea: A set of invariants represents the most relevant expected properties of the implementation under test. Intuitively, an invariant expresses the fact that each time the system under test performs a given sequence of actions, then it must exhibit a behavior reflected in the invariant. These invariants are called local because they only check the correctness of the logs that have been recorded in each isolated system. The type of errors that are undetectable by using only local invariants is discussed. In order to cope with these limitations, this paper introduces a new family of invariants, called globals to deal with more subtle characteristics. They express properties of a set of systems, by making relations between the set of recorded local logs. It is shown that global invariants are able to detect the class of undetected errors for local invariants.

Paper [15] presents a methodology and a set of tools for the modelling, validation and testing of Web service composition, conceived and developed within the French national project WebMov. This methodology includes several modelling techniques, based mainly on some variations of Timed Extended Finite State Machines (TEFSM) formalism, which provide a formal model of the BPEL description of Web services composition. These models are used as a reference for

the application of different test generation and passive testing techniques for conformance and robustness checking. The whole WebMov methodology is integrated within a dedicated framework, composed by a set of tools that implement the model representation, the test generation and passive testing algorithms. This framework also permits the interaction of these tools to achieve specific modelling and testing activities in a complementary way. A case study based on a real service, a Travel Reservation Web Service, is presented as well as the results of the application of the proposed WebMov methodology and tools.

Paper [14] presents a methodology to perform passive testing of behavioural conformance for the web services based on the security rule. The proposed methodology can be used either to check a trace (offline checking) or to runtime verification (online checking) with timing constraints, including future and past time. In order to perform this: firstly, the authors use the Nomad language to define the security rules. Secondly, they propose an algorithm that can check simultaneously multi instances. Afterwards, with each security rule, graphical statistics is proposed, with some fixed properties, that helps the tester to easy assess about the service. In addition to the theoretical framework a software tool is developed, called RV4WS (Runtime Verification engine for Web Service), that helps in the automation of the passive testing approach. In particular the algorithm presented in this paper is fully implemented in the tool. The authors also present a mechanism to collect the observable trace in this paper.

Article [5] describes the application of the TestInv-P passive testing tool as part of the testing phase of TXT e-tourism Web application. TestInv-P is a passive testing tool that monitors communication traces of an application during run-time and verifies whether it satisfies certain security-related invariants derived from SHIELDS models.

Paper [2] presents a formal framework to perform passive testing of service-oriented systems. The approach uses the historical interaction files between web services to check the absence of faults. The authors assume that a global log is not available. They show how to use local logs (recorded in each web service) in order to check local properties and how to combine them in order to check global properties.

Paper [13] presents two tools for conformance testing of web services. One tool for unit testing that is implemented by an on-line approach. This tool can be used to test a web service-based and/or an orchestration by simulating its partners. The other focuses on verification of a timed trace with respect to a set of constraints. Specially, one can use this tool to verify on-line or off-line a timed trace. A real-life case study, Product Retriever, is presented by combining the two tools.

Two related papers, [34] and [33] on conformance testing of web service choreographies were published in 2012. The passive testing approach is prefered due to its non-intrusiveness, support for black-box peers without source code being available, and both local and global conformance. In [34] Chor specification language is chosen, which can be seen as an abstraction of the standard Web service choreography language, WS-CDL. The formal framework of the approach and

the tool support for one possible implementation model, Web service choreographies, are presented. Collaborations within a chaoreography are usually achieved through information exchange, thus taking data into account during the testing process is necessary. In [33] the authors address this issue by using a non-intrusive passive testing approach based on functional properties. A property can express a critical (positive or negative) behavior to be tested on an isolated peer (locally) or on a set of peers (globally). They support online verification of these kind of properties against local running traces of each peer in a distributed system where no global clock is needed.

4 Testing for Internet of Things

In a series of papers published in 2009 the authors apply a passive conformance testing technique to a Mobile ad hoc network (MANET) routing protocol, OLSR, which supports a dynamically changing topology and absence of centralized management. In [16] a formal passive testing method to test the conformance and reliability of the protocol is proposed. Paper [17] is taking into account the OLSR formal specification, formal description of properties and collected traces of the implementation. In order to precisely express new properties in multi-node environments a new kind of invariants is introduced in [4].

In [21] and [22] the authors present a logic-based approach to test the conformance and performance of XMPP protocol through real execution traces and formally specified properties. Two related papers, [24], and [23], propose a logic-based approach to formal specification of functional requirements for WSN routing protocol. An algorithm to evaluate these properties on collected protocol execution traces is suggested.

Prof. Brzezinski in [11] presents a tester that is built around an Arduino-class microcontroller and is programmed in a test language that re-creates the basic semantics of the standardized test language TTCN-3. The approach is intended for the validation of IoT-class distributed systems involving humans-in-the-loop, especially for long-term unobtrusive supervision of in-the-wild behaviour change experiments in an instrumented home/work facility.

5 Security testing

A process model of a security-aware computer and network system is presented in [37]. For each entity in the model a history of activities that have occurred to the entity is recorded. Two major categories of attack-detection techniques are discussed: anomaly detection and attack signature recognition. Anomaly detection is used as a complement, to detect novel attacks with unknown signatures.

In [10] the author suggests using Testing and Test Control Notation as a platform for Intrusion Detection systems on the example of the Smurf attack.

In [29] a passive testing approach to check whether a system respects its security policy is proposed. To specify this policy Nomad formal language is

used, which is based on deontic and temporal logics. The methodology is applied to an industrial case study provided by SAP group.

In [20] a passive testing approach is used for security monitoring of web services. The authors propose a passive testing approach for SOA, encompassing a non-intrusive module that gathers selected traces for web services for centralized and decentralized workflows, and also a passive tester that analyzes the distributed collected traces against security requirements. The proposed methodology is applied to a Loan Origination Process using BPEL workflow.

In [32] the authors propose a novel approach to define protocol properties in terms of Input-Output Symbolic Transition Systems (IOSTS) and show how they can be tested on real execution traces taking into account the both, data portions and control portions. These properties can be designed to test the conformance of a protocol as well as security aspects. A parametric trace slicing approach is defined to match trace and property. The approach is illustrated on a set of execution traces extracted from an automotive Bluetooth framework with functional and security properties.

6 Other applications

In [28] the authors propose a conformance passive testing approach to check that implementation of IP Multimedia Subsystem Push over Cellular (PoC) service respects OMA standard requirements. First, formal invariants representing the most relevant properties to be tested are verified against the service specification. Then their are tested on the PoC collected execution traces.

Paper [1] is devoted to passive testing tools for certification of trading systems, which are connected by means of financial protocols (such as FIX/FAST, ITCH, or specialized binary access interfaces) to an exchange or a broker. The distinctive feature of the tool is a unified way of supporting multiple protocols.

In [27] the authors use Orthogonal Multi-tone Time Domain Reflectometry (OMTDR) for fault detection and location in live smart grids. Several approaches have been proposed and applied for reconstructing the topology of an unknown network in an on-line live mode. Passive testing approach is highly relevant here because a wide range of wiring networks embedded in critical systems as power grids and power-plants can not be easily shutdown for testing purposes.

References

1. Andrei Nikolaevich Alekseenko, Anastasiya Andreevna Averina, Daniil Sergeevich Sharov, Pavel Aleksandrovich Protsenko, and Iosif Leonidovich Itkin. Usage of passive testing tools for certification of trading systems clients. *Sistemy i Sredstva Informatiki [Systems and Means of Informatics]*, 24(2):83–98, 2014.
2. César Andrés, M Emilia Cambronero, and Manuel Nunez. Formal passive testing of service-oriented systems. In *Services Computing (SCC), 2010 IEEE International Conference on*, pages 610–613. IEEE, 2010.

3. César Andrés, M Emilia Cambronero, and Manuel Núnez. Passive testing of web services. In *International Workshop on Web Services and Formal Methods*, pages 56–70. Springer, 2010.
4. César Andrés, Stéphane Maag, Ana Cavalli, Mercedes G Merayo, and Manuel Núñez. Analysis of the olsr protocol by using formal passive testing. In *Software Engineering Conference, 2009. APSEC'09. Asia-Pacific*, pages 152–159. IEEE, 2009.
5. Alessandra Bagnato, Fabio Raiteri, Wissam Mallouli, and Bachar Wehbi. Practical experience gained from passive testing of web based systems. In *Software Testing, Verification, and Validation Workshops (ICSTW), 2010 Third International Conference on*, pages 394–402. IEEE, 2010.
6. Emmanuel Bayse, Ana Cavalli, Manuel Núñez, and Fatiha Zaïdi. A passive testing approach based on invariants: application to the wap. *Computer networks*, 48(2):247–266, 2005.
7. Abdelghani Benharref, Rachida Dssouli, Mohamed Adel Serhani, Abdeslam En-Nouaary, and Roch Glitho. New approach for efsm-based passive testing of web services. In *Testing of Software and Communicating Systems*, pages 13–27. Springer, 2007.
8. Abdelghani Benharref, Rachida Dssouli, Mohamed Adel Serhani, and Roch Glitho. Efficient traces collection mechanisms for passive testing of web services. *Information and Software Technology*, 51(2):362–374, 2009.
9. Krzysztof M Brzezinski. Towards practical passive testing. In *Parallel and Distributed Computing and Networks*, pages 177–183, 2005.
10. Krzysztof M Brzezinski. Intrusion detection as passive testing: linguistic support with ttcn-3. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 79–88. Springer, 2007.
11. Krzysztof M Brzeziński. Tiny ttcn-inspired testing tools for experimenting with hybrid iot systems. In *2018 11th International Conference on Human System Interaction (HSI)*, pages 261–267. IEEE, 2018.
12. Dung Cao, Patrick Felix, Richard Castanet, and Ismail Berrada. Testing web services composition using the tgse tool. In *WS-Testing 2009*, pages 187–194, 2009.
13. Tien-Dung Cao, Richard Castanet, Patrick Felix, and Gerardo Morales. Testing of web services: tools and experiments. In *Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific*, pages 78–85. IEEE, 2011.
14. Tien-Dung Cao, Trung-Tien Phan-Quang, Patrick Felix, and Richard Castanet. Automated runtime verification for web services. In *Web Services (ICWS), 2010 IEEE International Conference on*, pages 76–82. IEEE, 2010.
15. Ana Cavalli, Tien-Dung Cao, Wissam Mallouli, Eliane Martins, Andrey Sadovykh, Sébastien Salva, and Fatiha Zaidi. Webmov: A dedicated framework for the modelling and testing of web services composition. In *Web Services (ICWS), 2010 IEEE International Conference on*, pages 377–384. IEEE, 2010.
16. Ana Cavalli, Stephane Maag, and Edgardo Montes de Oca. A passive conformance testing approach for a manet routing protocol. In *Proceedings of the 2009 ACM symposium on Applied Computing*, pages 207–211. ACM, 2009.
17. Ana Cavalli, Stephane Maag, Edgardo Montes de Oca, and Fatiha Zaidi. A formal passive testing approach to test a manet routing protocol. In *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on*, pages 1–6. IEEE, 2009.

18. Ana Cavalli and Dario Vieira. An enhanced passive testing approach for network protocols. In *Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on*, pages 169–169. IEEE, 2006.
19. Ana R Cavalli, Teruo Higashino, and Manuel Núñez. A survey on formal active and passive testing with applications to the cloud. *annals of telecommunications-annales des télécommunications*, 70(3-4):85–93, 2015.
20. Ana Rosa Cavalli, Azzedine Benameur, Wissam Mallouli, and Keqin Li. A passive testing approach for security checking and its practical usage for web services monitoring. In *NOTERE 2009: 9e Conférence Internationale sur Les NOuvelles TEchnologies de la REpartition*, 2009.
21. Xiaoping Che and Stephane Maag. A passive testing approach for protocols in internet of things. In *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*, pages 678–684. IEEE, 2013.
22. Xiaoping Che and Stephane Maag. Testing protocols in internet of things by a formal passive technique. *Science China Information Sciences*, 57(3):1–13, 2014.
23. Xiaoping Che, Stephane Maag, Hwee-Xian Tan, and Hwee-Pink Tan. Passively testing routing protocols in wireless sensor networks. In *Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), 2015 IEEE 12th Intl Conf on*, pages 270–277. IEEE, 2015.
24. Xiaoping Che, Stephane Maag, Hwee-Xian Tan, Hwee-Pink Tan, and Zhangbing Zhou. A passive testing approach for protocols in wireless sensor networks. *Sensors*, 15(11):29250–29272, 2015.
25. Dongluo Chen, Jianping Wu, and HuiCheng Chi. Passive testing on tcp. In *Communication Technology Proceedings, 2003. ICCT 2003. International Conference on*, volume 1, pages 182–186. IEEE, 2003.
26. Dongluo Chen, Jianping Wu, and Tan Ieong Chu. An enhanced passive testing tool for network protocols. In *Computer Networks and Mobile Computing, 2003. ICCNMC 2003. 2003 International Conference on*, pages 513–516. IEEE, 2003.
27. Wafa Ben Hassen, Moussa Kafal, Esteban Cabanillas, and Jaume Benoit. Power cable network topology reconstruction using multi-carrier reflectometry for fault detection and location in live smart grids. In *2018 Condition Monitoring and Diagnosis (CMD)*, pages 1–5. IEEE, 2018.
28. Felipe Lalanne, Stephane Maag, Edgardo Montes De Oca, Ana Cavalli, Wissam Mallouli, and Arnaud Gonguet. An automated passive testing approach for the ims poc service. In *Automated Software Engineering, 2009. ASE'09. 24th IEEE/ACM International Conference on*, pages 535–539. IEEE, 2009.
29. Wissam Mallouli, Fayçal Bessayah, Ana Cavalli, and Azzedine Benameur. Security rules specification and analysis based on passive testing. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–6. IEEE, 2008.
30. Raymond E Miller, D-L Chen, David Lee, and Ruibing Hao. Coping with nondeterminism in network protocol testing. In *IFIP International Conference on Testing of Communicating Systems*, pages 129–145. Springer, 2005.
31. Gerardo Morales, Stephane Maag, Ana Cavalli, Wissam Mallouli, Edgardo Montes De Oca, and Bachar Wehbi. Timed extended invariants for the passive testing of web services. In *Web Services (ICWS), 2010 IEEE International Conference on*, pages 592–599. IEEE, 2010.

32. Pramila Mouttappa, Stephane Maag, and Ana Cavalli. Monitoring based on iosts for testing functional and security properties: application to an automotive case study. In *Computer Software and Applications Conference (COMPSAC), 2013 IEEE 37th Annual*, pages 1–10. IEEE, 2013.
33. Huu Nghia Nguyen, Pascal Poizat, and Fatiha Zaïdi. Online verification of value-passing choreographies through property-oriented passive testing. In *High-Assurance Systems Engineering (HASE), 2012 IEEE 14th International Symposium on*, pages 106–113. IEEE, 2012.
34. Huu Nghia Nguyen, Pascal Poizat, and Fatiha Zaïdi. Passive conformance testing of service choreographies. In *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, pages 1528–1535. ACM, 2012.
35. Cecilia Saint-Pierre, Francisco Cifuentes, and Javier Bustos-Jiménez. Detecting anomalies in dns protocol traces via passive testing and process mining. In *Communications and Network Security (CNS), 2014 IEEE Conference on*, pages 520–521. IEEE, 2014.
36. Jianping Wu, Yixin Zhao, and Xia Yin. From active to passive: Progress in testing of internet routing protocols. In *International Conference on Formal Techniques for Networked and Distributed Systems*, pages 101–116. Springer, 2001.
37. Nong Ye, Joseph Giordano, and John Feldman. A process control approach to cyber attack detection. *Communications of the ACM*, 44(8):76–82, 2001.
38. Fatiha Zaidi, Emmanuel Bayse, and Ana Cavalli. Network protocol interoperability testing based on contextual signatures and passive testing. In *Proceedings of the 2009 ACM symposium on Applied Computing*, pages 2–7. ACM, 2009.
39. Yixin Zhao, Xia Yin, and Jianping Wu. Online test system, an application of passive testing in routing protocols test. In *Networks, 2001. Proceedings. Ninth IEEE International Conference on*, pages 190–195. IEEE, 2001.