Traffic-aware Stress Testing of Distributed Systems Based on UML Models

Vahid Garousi‡, Lionel C. Briand‡§ and Yvan Labiche‡
‡ Carleton University
Department of Systems and Computer Engineering
Software Quality Engineering Laboratory
1125 Colonel By Drive
Ottawa, ON K1S5B6, Canada
{vahid, briand, labiche}@sce.carleton.ca
§ Simula Research Laboratory
Department of Software Engineering
Martin Linges v 17, Fornebu
P.O.Box 134,
1325 Lysaker, Norway
briand@simula.no

ABSTRACT
A stress test methodology aimed at increasing chances of discovering faults related to network traffic in distributed systems is presented. The technique uses the UML 2.0 model of the distributed system under test, augmented with timing information, and is based on an analysis of the control flow in sequence diagrams. It yields stress test requirements that are made of specific control flow paths along with time values indicating when to trigger them. Different variants of our stress testing technique already exist (they stress different aspects of a distributed system) and we focus here on one variant that is designed to identify and to stress test the system at the instant when data traffic on a network is maximal. Using a real-world distributed system specification, we design and implement a prototype distributed system and describe, for that particular system, how the stress test cases are derived and executed using our methodology. The stress test results indicate that the technique is significantly more effective at detecting network traffic-related faults when compared to test cases based on an operational profile.

Categories and Subject Descriptors

General Terms
Algorithms, Reliability, Verification.

Keywords
Stress testing, model-based testing, distributed systems, UML, network traffic.

1. INTRODUCTION
Distributed Systems (DS) are becoming more important to our everyday life. Examples include command and control systems, aircraft aviation systems, robotics, and nuclear power plan systems [28]. The development and testing of a DS is difficult and takes more time than the development and testing of a non-distributed system, which runs on a single computer [30]. Furthermore, DSs often have real-time constraints which increase the testing complexity of such systems.

Sources of failures in the United States Public Switched Telephone Network (PSTN) are investigated in [16]. It is reported that in the 1992-1994 time period, although only 6% of the outages were overloads, they led to 44% of the PSTN’s service downtime. In the system under study, overload was defined as the situation in which service demand exceeds the designed system capacity. So it is evident that although overloads do not happen frequently, the failure resulting from them can be quite expensive.

Therefore the motivation for our work can be stated as follows: Because DS are by nature concurrent and are often real-time, there is a need for methodologies and tools for testing and debugging DS under stress conditions such as heavy user loads and intense network traffic. These systems should be tested under stressing conditions before being deployed in the field in order to assess their robustness to distribution-specific problems. In this work, our focus is on network traffic, one of the fundamental factors affecting the behavior of DS.

Distributed nodes of a DS regularly need to communicate with each other to perform system functionality. Network communications are not always successful and on time as problems such as congestion, transmission errors, or delays might occur. On the other hand, many real-time and safety-critical systems have hard deadlines for many of their operations, where if the deadlines are not met, serious or even catastrophic consequences will happen.

Furthermore, a DS might behave well with normal network traffic loads (e.g., in terms of amount of data, number of requests), but the communication might turn out to be poor and unreliable if many network messages or high loads of data are concurrently transmitted over a particular network or towards a particular node.

Since 1997, UML has become the de facto standard for modeling object-oriented software for nearly 70 percent of IT industry [25]. The new version of UML, version 2.0 [22] offers an improved modeling language compared to UML 1.x versions. Some of the high level improvements are: enhanced architecture modeling, improved extensibility mechanism, support for component-based development, modeling of relationships and model management [25]. As we expect UML to be increasingly used for DS, it is therefore important to develop automatable UML model-driven,
stress test techniques and this is the main motivation for the work reported here.

Assuming that the UML design model of a DS is in the form of Sequence Diagrams (SD) annotated with timing information, and the system’s network topology is given in a specific modeling format, we propose a technique to derive test requirements to stress the DS with respect to network traffic in a way that will likely reveal robustness problems. Note that, for a DS where several concurrent objects are running on each distributed node and objects communicate frequently with each other, the number of all possible object interaction interleavings on a network is extremely large. Testing all these interleavings is in general not feasible. We thus introduce a systematic technique to automatically generate an interleaving that will stress the network traffic on a network or a node in a System Under Test (SUT) so as to analyze the system under strenuous but valid conditions. If any network traffic-related failure is observed, designers will be able to apply any necessary fixes to increase robustness before system delivery.

Though the stress test technique reported in this article targets distributed systems, there are important aspects of real-time systems that we do not address here. As we further discuss in Section 6.6, such systems often have to react to external or internal events that exhibit arrival patterns (e.g., periods). Such patterns impose constraints on the time instant when interactions between distributed objects can take place. These issues are addressed in [14] where a more sophisticated optimization technique based on Genetic Algorithms is proposed. The current paper, however, focuses on the modeling issues to enable such optimization and a simpler optimization approach when no arrival pattern constraints are present.

The contributions of this work can be summarized as: (1) an approach for UML model-based network traffic usage analysis in DS, and (2) a stress test strategy aiming at increasing chances of discovering faults related to network traffic.

The remainder of this article is structured as follows. Related works are discussed in Section 2. An overview of the stress test methodology is given in Section 3. The assumed input system models for the methodology are described in Section 4. Section 5 discusses how a stress test model is built to support automation. The use of the stress test model to derive test requirements is described in Section 6. The results of applying the methodology to a case study system are described in Section 7, which shows the applicability and assesses the effectiveness of the methodology in revealing faults related to network traffic. Finally, Section 8 concludes the article and discusses some of the future research directions.

2. RELATED WORKS

To the best of our knowledge, no existing work addresses the automated derivation of test requirements from UML models for performance stress testing of DS from the perspective of maximizing the chance of exhibiting network traffic faults. There have not been many works on systematic generation of stress and load test suites for software systems, with the notable exception of [1, 4, 31, 32].

Authors in [1] propose a class of load test case generation algorithms for telecommunication systems which can be modeled by Markov chains. The black-box techniques proposed are based on system operational profiles. The Markov chain that represents a system’s behavior is first built. The operational profile of the software is then used to calculate the probabilities of the transitions in the Markov chain. The steady-state probability solution of the Markov chain is then used to guide the generation process of the test cases according to a number of criteria, in order to target specific types of faults. For instance, using probabilities in the Markov chain, it is possible to ensure that a transition in the chain is involved many times in a test case so as to target the degradation of the number of calls that can be accepted by the system. From a practical standpoint, targeting only systems whose behavior can be modeled by Markov chains can be considered a limitation of this work. Furthermore, using only operational profiles to test a system may not lead to stressing situations.

Yang propose a technique [31] to identify potentially load sensitive code regions to generate load test cases. The technique targets memory-related faults (e.g., incorrect memory allocation/de-allocation, incorrect dynamic memory usage) through load testing. The approach is to first identify statements in the module under test that are load sensitive, i.e., they involve the use of malloc() and free() statements (in C) and pointers referencing allocated memory. Then, data flow analysis is used to find all Definition-Use (DU)-pairs that trigger the load sensitive statements. Test cases are then built to execute paths for the DU-pairs.

Briand et al. [4] propose a methodology for the derivation of test cases that aims at maximizing the chances of deadline misses within a system. They show that task deadlines may be missed even though the associated tasks have been identified as schedulable through appropriate schedulability analysis. The authors note that although it is argued that schedulability analysis simulates the worst-case scenario of task executions, this is not always the case because of the assumptions made by schedulability theory. The authors develop a methodology that helps identify performance scenarios that can lead to performance failures in a system.

Zhang et al. [32] describe a procedure, similar to ours, for automating stress test case generation in multimedia systems. The authors consider a multimedia system consisting of a group of servers and clients connected through a network as a SUT. Stringent timing constraints as well as synchronization constraints are present during the transmission of information from servers to clients and vice versa. The authors identify test cases that can lead to the saturation of one kind of resource, namely CPU usage of a node in the distributed multimedia system. The authors first model the flow and concurrency control of multimedia systems using Petri-nets coupled with timing constraints. A specific flavor of temporal logic is used to model temporal constraints. The following are some of the limitations of their technique: (1) The technique cannot be easily generalized to generate test cases to stress test other kinds of resources, such as network traffic, as this would require important changes in the test model; (2) The resource utilization (CPU) of media objects is assumed to be constant over time, although such utilization would likely depend on the requests the server receives for example; (3) Although the objective is similar to ours, i.e., maximizing resource usage at a given time instant, no variation of the technique is proposed or

1 A network interaction interleaving is a possible sequence of network interactions among a subset of objects on a subset of nodes.
even mentioned to stress test over a specific period of time. A system may only exhibit failures if stress testing is prolonged for a period of time; (4) If this technique is applied in a UML-based development, it requires additional knowledge (Petri Nets and a specific flavor of temporal logic) which can be an impediment to its use.

3. OVERVIEW OF THE METHODOLOGY

An overview of our model-based stress test methodology is presented using an activity diagram in Figure 1. Note that only the steps in gray background are addressed by the current paper.

The detailed steps of Figure 1 are described in the next sections:

- Input models (Section 4)
- Building the test model (Section 5)
- Derivation of stress test requirements (optimization algorithm) – (Section 6)

4. INPUT SYSTEM MODEL

The input model consists of a number of UML diagrams. Some of them are standard in mainstream development methodologies (class diagram, sequence diagrams, and system context diagram [15]). Others are needed to describe the distributed architecture of the SUT (Network Deployment Diagram) and sequential constraints among SDs, i.e., their respective use cases (Modified Interaction Overview Diagram). The next subsections describe the latter two diagrams.

4.1 Network Deployment

The structure of the distributed architecture of a SUT as we need it to be described is shown in Figure 2 as a metamodel. Such network information is paramount as one of our objectives is to stress, not only nodes in a network, but also (sub-)networks. An example of a distributed architecture is depicted in Figure 3-(a) which shows networks in a hierarchical structure (each network can have many subnets and only one supernet), nodes belonging to networks, and objects distributed on nodes, e.g., node1 connected to node3 through the network path <Network1, SystemNetwork, Network2> in Figure 3-(a).

We want to describe such a distributed architecture using UML 2.0 so as to be able to use it as an input for our testing methodology in the context of a UML-based development. When compared to UML 1.x [25], UML 2.0 [22] shows significant improvements with respect to modeling application architecture, nodes, and communication paths. However, modeling a hierarchical set of networks and their inter-connectivity is not directly addressed in the UML 2.0 specification [22].

We thus decided to model the system network as a package diagram where the entire system network is the root (high level) package and other networks and nodes are the sub-packages in a hierarchical manner. We refer to such a diagram as a Network Deployment Diagram (NDD). As an example, the architecture in Figure 3-(a) is modeled by the NDD in Figure 3-(b). Packages represent networks of the system and containment (nested) relationships among the packages denote nested networks. Note that the deployment locations of objects are not specified in NDDs, but in sequence diagrams (Section 5.1)

4.2 Modified Interaction Overview

The naming of Modified Interaction Overview Diagram (MIOD) comes from the UML 2.0’s Interaction Overview Diagram (IOD) [22]. To model which actor can trigger a particular SD, we modify IODs to include activity partitions: one partition per actor. A MIOD is used to model sequential and conditional constraints between SDs (inter-SD constraints): activities (i.e., nodes in the diagram) are SDs and edges depict those sequential constraints [3, 6, 8, 20]. Taking such constraints into account is important while defining stress tests since executing an arbitrary sequence of SDs in a SUT might not be always valid or possible. The business logic of a SUT might enforce a set of constraints on the sequence (order) of SDs and also certain conditions may have to be satisfied before a particular SD can be executed, e.g., the Login SD of an ATM system should be executed before the Withdrawal SD (Figure 4). For example, the MIOD of a simplistic ATM system...
(Figure 4) has two partitions to model which actor (e.g., user) can trigger (or interact with) SDs.

\[ \text{Login} \]

\[ \text{Object}2 \]

\[ \text{[login successful]} \]

Fragments in a SD. For example, the fork node after node entailed by asynchronous messages and parallel combined Join and fork nodes are used to represent concurrent control flow names in Figure 5), and edges between nodes denote the flow of Figure 5. In a CCFG, nodes correspond to messages of the CCFG is similar to the concept of inter-procedural CFG [18]. As another SD, there are control flow edges connecting their generated for each SD. In cases where a SD calls (refers to) another SD, their corresponding CCFGs to form an inter-SD CCFG. An inter-SD CCFG is similar to the concept of inter-procedural CFG [18]. As an example, the CCFG in Figure 6 corresponds to the SD in Figure 5. In a CCFG, nodes correspond to messages of the SD (e.g., message B follows message A). Join and fork nodes are used to represent concurrent control flow entailed by asynchronous messages and parallel combined fragments in a SD. For example, the fork node after node C (Figure 6) corresponds to the concurrent control flow entailed by the asynchronous message C.

The concept of Concurrent Control Flow Path (CCFP), formally presented in [13], is similar to the conventional CFPs, except that they account for concurrent control flows as they are derived from CCFGs. A CCFP is a path from the start node of a CCFG to its final node. In our notation for CCFPs, parentheses denote concurrent control flow, and can be nested. For example, four of the CCFPs of the CCFG in Figure 6 are represented in Figure 7.

\[ \rho = \rho_B \left( \left( \rho_D \left( \rho_E \right) \right) \right) \]

\[ \rho = \rho_A \left( \left( \rho_F \left( \rho_G \right) \right) \right) \]

\[ \rho = \rho_A \left( \left( \rho_B \left( \rho_C \right) \right) \right) \]

\[ \rho = \rho_A \left( \left( \rho_B \left( \rho_C \right) \right) \right) \]

The symbol \( \rho \) (Figure 7) will be used in the rest of this article to refer to CCFPs. The four CCFPs in Figure 7 are due to the decision node corresponding to a loop in the CCFG. Following a strategy similar to what is done for code coverage, a loop can either be bypassed (if possible), taken only once, a representative or average number of times, and a maximum number of times. These situations correspond to CCFPs \( \rho_1, \rho_2, \rho_3 \), and \( \rho_4 \), respectively.

\[ \rho_1 = \rho_B \left( \left( \rho_D \left( \rho_E \right) \right) \right) \]

\[ \rho_2 = \rho_A \left( \left( \rho_F \left( \rho_G \right) \right) \right) \]

\[ \rho_3 = \rho_A \left( \left( \rho_B \left( \rho_C \right) \right) \right) \]

\[ \rho_4 = \rho_A \left( \left( \rho_B \left( \rho_C \right) \right) \right) \]

5.2 Network Interconnectivity Tree

A Network Interconnectivity Tree (NIT) is a data structure built from a NDD (Section 4). The motivation for NITs is to easily identify the subset of nodes and networks that are relevant for deriving stress test cases and the network path between any two given nodes. The root of the tree is always the entire system.
network while system networks and nodes are its children. In a NIT, networks and nodes are shown as rectangles and circles, respectively. For example, the NIT of the NDD in Figure 3-(b) is shown in Figure 8-(a). Then, assuming a tester’s goal is to stress test the SUT only with respect to Network2, the test strategy will only consider the messages going through Network2 in the NIT.

Figure 8. (a): NIT built from the NDD in Figure 3-(b). (b): Derivation of network path between two nodes using getNetworkPath().

To identify the network path between any two given nodes, we define the network path function getNetworkPath(n1,n2) where n1 and n2 are the sender and the receiver nodes of a message, respectively. (An algorithm for this function can be found in [14].) For example, the derivation of the network path between n1 (the sender) and n2 (the receiver) is depicted in Figure 8-(b) and is formally represented as:

getNetworkPath(n1, n2)=<Network1, SystemNetwork, Network2>

5.3 Network Traffic Usage Pattern

A network traffic usage pattern is the pattern describing how a CCFP entails traffic on a network. As discussed in Section 5.1, the network traffic usage of each CCFP can be different from other CCFPs. We present in this section a resource usage analysis (RUA) technique to measure the traffic usage for each CCFP. The measurement heuristics are described first and the formalized.

5.3.1 Heuristics

In order to analyze the usage pattern of each CCFP, we need to analyze the traffic usage entailed by its messages. Only distributed messages in SDs are of interest here (not local messages) since they are the only ones entailing network traffic.

A Distributed CCFP (DCCFP) is a CCFP where only distributed messages are modeled. For example, considering ρ1 in Figure 7, since all messages except A and B are distributed, the transformation to obtain a DCCFP is:

\[
\rho_1 = ABC \left[ \frac{DE}{FG} \right] \Rightarrow DCCFP(\rho_1) = C \left[ \frac{DE}{FG} \right]
\]

where DCCFP(ρ) denotes a function returning the corresponding DCCFP of a CCFP.

In order to measure the traffic entailed by each distributed message, we measure the data sizes of the parameters of a call message or the return values of a reply message. For a distributed signal message, we consider the size of the signal object (sum of the attributes size) as the size of the signal message. We define the data size of an object to be the summation of sizes (in bytes) of the attributes in its class.

Admittedly, other measures (perhaps more accurate) of network traffic can be considered. We however consider our measurement as a reasonable surrogate for network traffic.

5.3.2 Formalizing Messages

In order to precisely define how we perform traffic analysis of SDs, we formally define SD messages. Similar to the tabular representation of messages, proposed by UML 2.0 [22], each message annotated with timing information (using the UML-SPT profile [24]) can be represented as a tuple:

\[
\text{message} = (\text{sender}, \text{receiver}, \text{methodOrSignalName}, \text{parameterList}, \text{returnList}, \text{startTime}, \text{endTime}, \text{msgType})
\]

where

- \text{sender} denotes the sender of the message and is itself a tuple of the form sender=(object, class, node), where:
  - object is the object (instance) name of the sender.
  - class is the class name of the sender.
  - node is where the sender object is deployed.
- \text{receiver} denotes the receiver of the message and is itself a tuple of the same form as \text{sender}.
- \text{methodOrSignalName} is the name of the method on the message or the signal class name in case of a signal message.
- \text{parameterList} is the list of parameters for call messages. parameterList is a sequence of the form \langle (p_1, C_1, \text{in/out}), ..., (p_o, C_o, \text{in/out}) \rangle, where \(p_i\) is the \(i\)-th parameter of class type \(C_i\) and \text{in/out} defines the kind of the parameter. For example, if the call message is \text{m}(o_1:C_1, o_2:C_2), then the ordered parameters set will be \langle (o_1, C_1, \text{in}), (o_2, C_2, \text{in}) \rangle. If the method call has no parameter, this set is empty.
- \text{returnList} is the list of return values on reply messages. It is empty in other types of messages. UML 2.0 assumes that there may be several return values for a reply message. We show returnList in the form of a sequence \langle (\text{var}_1=\text{val}_1, C_1), ..., (\text{var}_o=\text{val}_o, C_o) \rangle, where \text{val}_i is the return value for variable \text{var}_i with type \(C_i\).
- \text{startTime} is the start time of the message (modeled by UML-SPT profile’s RTstart tagged value).
- \text{endTime} is the end time of the message (modeled by UML-SPT profile’s RTEnd tagged value).
- \text{msgType} is a field to distinguish between signal, call and reply messages. Although the messageSort attribute\(^3\) of each message in the UML metamodel can be used to distinguish signal and call messages, the metamodel does not provide a built-in way to separate call and reply messages. Further explanations on this and an approach to distinguish between call and reply messages can be found in [13].

5.3.3 Network Traffic Usage Function

We present a Network Traffic Usage (NTU) function in Equation 1, which is used to measure the amount of traffic entailed by a distributed message. A dash (-) symbol indicates that a field can take any arbitrary value (a “don’t care” field). NTU is a function

\[\text{NTU}(\text{message}) = \text{parameterList} + \text{returnList} + \text{startTime} + \text{endTime} + \text{msgType}\]

\(^2\) In UML 2.0, in the case of a message of type signal, the arguments of the message must correspond to the attributes of the signal class. The data carried by a signal message is represented as attributes of the signal instance.

\(^3\) The messageSort attribute of a message specifies the type of communication reflected by the message [22], and can be any of these values: synchCall (synchronous call), synchSignal (synchronous signal), asynchCall, or asynchSignal.
from the set of messages to real values (data traffic). The data traffic (DT) value depends on the type of the message.

For a signal message (function SignalDT is used), DT is equal to the data sizes of all the attributes of the signal class referred by the message. For a call message (function CallDT is used), DT is the sum of data sizes of all the attributes of each parameter. For a reply message (function ReplyDT is used), DT is the sum of data sizes of all attributes of each member of the return list.

\[
\text{NTU}(\text{msg}) = \text{CallDT}(\text{msg}) = \text{dataSize}(\text{A}) + \text{dataSize}(\text{B})
\]

Equation 1. Network Traffic Usage (NTU) function.

As an example, suppose call message msg has parameterList=\langle(a_1,A),(a_2,B)\rangle, where classes A and B are defined in the class diagram of Figure 9.

![Figure 9. Two classes with data fields.](image-url)

Using the class specifications of A and B, we can estimate the size of the message as:

\[
\text{NTU}(\text{msg}) = \text{CallDT}(\text{msg}) = \text{dataSize}(\text{A}) + \text{dataSize}(\text{B}) = (8\times(100+500)) + (8\times100+2\times100) = 5.8\text{ KB (kilobytes)}
\]

where long and char are among the primitive data types in Java. Data size of a long and a char variable in Java are eight and two bytes, respectively.

5.3.4 Usage Pattern of Distributed Concurrent Control Flow Paths

Using NTU, we present a Network Traffic Usage Pattern (NTUP) function for DCCFPs in Equation 2. NTUP is a function from the set of DCCFPs, networks, and time domain to real values (usage pattern values). The usage pattern of a DCCFP ρ on a network net at a particular time instant t is the sum of NTU values of the subset of the DCCFPs’ messages whose start/end time interval includes t and that go through net (using getNetworkPath() in Section 5.2). Dur(t) denotes the time duration of a message and since a message can span over several time units, our definition for the data traffic value of a message at a given time unit is its total data size divided by its duration, which yields the average message traffic per time unit.

As an example, Figure 10-(a) shows the NTUP values of DCCFP(ρi) at different time instants (DCCFP(ρi) is discussed in Section 5.3.1). The message durations are extracted from the SD in Figure 5. The NTU values, shown in Figure 10-(b), are example values used when computing this NTUP. Figure 10-(a) shows that the maximum traffic entailed by this DCCFP is 80 KB at time instance = 13 ms.


\[
\text{NTUP}(\rho, \text{net}, t) = \sum_{\text{msg}} \text{NTU}(\text{msg}) / \text{Dur}(\text{msg}), \text{msg}_\text{start} \leq t \leq \text{msg}_\text{end}
\]

Figure 10. (a): Network Traffic Usage Pattern of a DCCFP. (b): Network Traffic Usage values of the messages.

5.4 Inter-Sequence Diagram Constraints

As discussed in Section 4.2, a MIOD (Modified Interaction Overview Diagram) is used to model sequential and conditional constraints between SDs, referred to as inter-SD constraints.

The goal of our stress test technique is to choose the maximum number of SDs (to create maximum possible traffic) which can realistically be run concurrently, according to the MIOD, and schedule them such that their maximum traffic messages run at the same time. To comply with inter-SD constraints while considering the maximum number of SDs, we introduce the concept of Independent SD Set (ISDS). Two SDs are independent if there is no path (inter-SD constraints) between them in the MIOD (e.g., SDs A and B in Figure 11-(a) are independent). An ISDS is the largest (maximal) set of SDs, in which any two SDs are independent, thus enabling all the SDs in the set to run concurrently. A MIOD can lead to several ISDSs and, as discussed in Section 6, the ISDS with maximum traffic (among all the ISDSs for a given MIOD) will be chosen to generate stress test requirements.

![Figure 11. (a): The MIOD of a power system. (b): The corresponding Independent-SDs Graph (ISDG). (c): One of the maximal-complete subgraphs of the ISDG (shown with dashed edges).](image-url)

To derive the set of ISDSs of a MIOD, we first build a graph, referred to as a Independent-SDs Graph (ISDG); nodes are SDs and there is an edge between two nodes if and only if the two corresponding SDs are independent. Finding the ISDSs is then a graph-based problem. More specifically, every maximal-complete...
subgraph in this graph is an ISDS. (More details can be found in [14].) Standard algorithms can then be used to find those maximal-complete subgraphs. For example, the MIOD of a power distribution controller system (used as a case study in Section 7) is shown in Figure 11-(a). For the ISDG in Figure 11-(b), four ISDSs are identified:

- $SD_1 = \{ A, B, D, E \}$
- $SD_2 = \{ A, B, F \}$
- $SD_3 = \{ C, D, E \}$
- $SD_4 = \{ C, F \}$

The stereotype «HRT» in Figure 11-(a) is a specialization to the UML-SPT’s $RT_action$ stereotype to model hard real-time constraints and it will be discussed and used in Section 7. This extension is needed since the UML-SPT does not have separate stereotypes for hard and soft real-time constraints. For brevity, SDs are labeled alphabetically in the MIOD.

6. DERIVATION OF STRESS TEST REQUIREMENTS

This section describes how stress test requirements are derived from our test model.

6.1 Heuristics

Given a specific network to stress test, we identify a message (or a set of messages) in a DCCFP of a SD which imposes maximum traffic on the network. Let us refer to such messages as maximum stress messages. Then, using the start times of the maximum stress messages selected in each DCCFP, the selected set of DCCFPs can be scheduled in such a way that the maximum stressing messages are all sent concurrently. This concurrent schedule of DCCFPs will cause a maximum possible traffic on the selected network, in turn will increase the probability of exhibiting distributed traffic-related faults in the system under stress test. Only SDs (i.e., their respective DCCFPs) that are members of an ISDS are considered in order to ensure we comply with inter-SD constraints. The heuristic can be informally visualized by the example in Figure 12.

![Figure 12. An example illustrating the heuristic.](image)

Given the usage patterns of the DCCFPs of SDs in an ISDS, the heuristic is to first find the DCCFP, among all DCCFPs of a SD, which has a message with the maximum traffic. In Figure 12, we assume we have three SDs and the corresponding DCCFPs are denoted $DCCFP_i$, i uniquely identifying SDs. The DCCFPs are then scheduled such that their maximum stressing messages are sent at the same time (right-hand side diagram in Figure 12). Note that the NIT is used to determine if a distributed message between two nodes goes through the selected network.

6.2 Formulation as an Optimization Problem

According to the heuristic defined above, we formulate the stress test requirements derivation process as the optimization problem [12] in Figure 13.

![Figure 13. Formulation as an optimization problem.](image)

Note that multiple concurrent invocations of a SD might be allowed in a system, e.g., a SD which is triggered by five sensors concurrently. Therefore multiple DCCFP instances of such a SD can be executed to maximize stress during testing. Our technique derives the number of multiple invocations of a SD from the information specified in a system context diagram [15], i.e., a diagram specifying actors interacting with the system and their expected numbers at run-time. For example, if five instances of an actor can trigger a SD, it implies that five instances of the SD (i.e., one of its corresponding DCCFPs) can run concurrently.

6.3 Output Stress Test Requirements

Assuming that a SUT has $n$ SDs ($SD_1, …, SD_n$), a test requirement will be a schedule of a selected set of DCCFPs in the form of $< (\rho_{l_{max}} \alpha_{l_{max}}, …, (\rho_{l_{max}} \alpha_{l_{max}}) >$, where for the $i$-th entry of the sequence, $\rho_{l_{max}}$ is a DCCFP in the DCCFP set of $SD_i$, $DCCFP(SD_i)$, that entails the maximum traffic over the selected network. $\alpha_{l_{max}}$ is the start time of $\rho_{l_{max}}$, i.e., the time to trigger $\rho_{l_{max}}$. Intuitively, if none of the DCCFPs of $SD_i$ has any message going through the given network, it means that that $SD_i$ does not have any traffic on the network and hence it will not be included in the test requirement. In such a case, the $i$-th entry is null.

6.4 Algorithm

We now present the algorithm which solves the optimization problem in Figure 13 and generates test requirements to stress test data traffic in a network at any time instant, referred to as StressNetInsInsDT($net$). The main steps of the algorithm are presented using the activity diagram in Figure 14. The algorithm is best explained by applying it to an example.

Suppose the test model of a SUT with four ISDSs and six SDs as described in Figure 11 is built as specified in Section 5. Further assume that each SD $X$ has two CCFPs (and DCCFPs), labeled $\rho_{X,1}$, $\rho_{X,2}$. Step 1 of the algorithm in Figure 14, which is to find DCCFPs for SDs with maximum network traffic, identifies DCCFPs $\rho_{A,2}$, $\rho_{B,1}$, $\rho_{B,2}$, $\rho_{C,1}$, $\rho_{D,1}$, and $\rho_{E,2}$ for SDs A to F, respectively. Note that in order to find those DCCFPs, Step 1 first finds the maximum traffic messages and determines the start times of such messages, which are used in Step 3. Step 1.2 selects the DCCFP with maximum traffic value, which is used for stress testing purposes. In our example, the maximum traffic values of

---

4 A maximal-complete subgraph is a complete subgraph that is not contained in any other complete subgraph. A complete subgraph of a graph is a subgraph in which there exists an edge between any pair of nodes.
DCCFPs (labeled $\max DT(p_{xj})$ for each SD $X$ and DCCFP $j$) are specified below in KB:

\[
\max DT(p_{xj}) = \begin{cases} 
10 & \text{for } X = A \text{ and } j = 1 \\
15 & \text{for } X = B \text{ and } j = 1 \\
12 & \text{for } X = A \text{ and } j = 2 \\
35 & \text{for } X = B \text{ and } j = 2 \\
80 & \text{for } X = C \text{ and } j = 2 \\
45 & \text{for } X = D \text{ and } j = 2
\end{cases}
\]

Using ISDS$_{A}$ as an example, Step 2 then calculates the total traffic of each ISDS as follows:

\[
\max DT(ISDS_{A}) = \sum_{j=1}^{\text{ISDS}_{A}} \max DT(p_{xj}) = 140\text{KB}
\]

and similarly:

\[
\max DT(ISDS_{B}) = 70 \\
\max DT(ISDS_{C}) = 127 \\
\max DT(ISDS_{D}) = 57
\]

The ISDS with maximum DT value is then chosen: ISDS$_{A}$. The last step (Step 3) is to schedule the DCCFPs of ISDS$_{A}$ ($p_{A,1}$, $p_{A,2}$, $p_{A,3}$, $p_{A,4}$) so that their maximum stress messages happen at the same time. Assume that start times of maximum traffic messages for $p_{A,1}$, $p_{A,2}$, $p_{A,3}$, and $p_{A,4}$ are 5 ms, 10 ms, 15 ms, and 20 ms, respectively (Figure 15, left). Then the four DCCFPs are scheduled at times 15 ms, 10 ms, 5 ms, and 0 ms, respectively (Figure 15, right). Thus, since $C$ and $F$ are not part of the selected ISDS, the output stress test requirements will be:

\[
\langle p_{A,1}, 15\text{ms}, p_{B,1}, 10\text{ms}, \text{null}, p_{D,1}, 5\text{ms}, p_{C,1}, 0\text{ms}, \text{null}\rangle
\]

**6.5 Algorithm Complexity**

Based on the variables description in Table 1, the average-case time complexity of the algorithm StressNetInsDT(net) is in $O(s \times p \times m + y)$. The algorithm is therefore quite scalable, since the $s \times p$ term is the dominating factor in the complexity expression and, fortunately, the number of SDs ($s$), and average number of DCCFPs per SD ($p$) are usually small. Refer to [14] for further details.

**6.6 Discussions**

Note that, due to space constraints, we only discussed one of our stress test methodologies in this paper, which is stress testing data traffic of a network in a single time instant. Alternatively, a network could be stress tested in a period of time. These tests might reveal different types of faults in a DS, as discussed in [14]. Our methodology has a set of 32 different test strategies to test different nodes and network in a DS, such as instant stress testing towards a node, or period stress testing from a node. All these strategies share a common set of heuristics (Section 6.1) and have the same test model components to derive test requirements while complying with arrival-pattern constraints of a network Traffic Usage Pattern (NTUP) functions (Section 5.3.3). The stress test parameters in Figure 1 are used to specify the type of testing strategy desired by a tester and other specific parameters of the strategy, such as the network to be tested for the strategy discussed in this article.

Furthermore, we presented the simplified version of our methodology in this paper where only sequential and conditional constraints were considered between SDs. DS usually have another type of constraints, referred to as arrival-pattern constraints [24], which relate to the timing of SDs. The time instant when a SD can start running might be constrained. Each single SD might only be allowed to execute in some particular time instants. For example, consider a SD which is triggered by a timer on a periodic basis, say every 5 seconds. In such a case, it is not possible to trigger the SD (or any of its DCCFPs) in time instant 4 seconds. As we discuss in [14], taking into account the arrival-pattern class of constraints requires more advanced optimization techniques, since they bring a new set of complex constraints into the optimization problem [14]. We present a more sophisticated optimization technique in [14], to derive stress test requirements while complying with arrival-pattern constraints of a DS (in addition to sequential and conditional ones).

**7. CASE STUDY**

Our stress test methodology can be used to stress test distributed systems with, perhaps, an emphasis on safety-critical and data-intensive systems. Distributed Control Systems (DCS) [17] and Supervisory Control and Data Acquisition (SCADA) Systems [10] are two kinds of such systems.

We surveyed numerous existing systems (e.g. [7, 9, 11]) to choose a suitable case study. Selection criteria were that it should be possible to run a system on a standard hardware/software platform, the design model and source code of the system should be available, and also the system should be accessible for use. Since no public domain system met all the above requirements,
we decided to analyze, design and build a prototype system based on a real-world specification.

SCAPS (our prototype system) is a SCADA-based power system (e.g. [5, 26, 29]) which controls the power distribution grid across a nation consisting of several provinces, composed of cities and regions. Each city and region has several local power distribution grids, each with a Tele-Control unit (TC), which gathers the grid data and can also be controlled remotely. There is a nation-wide central server, and each province has one central server that gathers the SCADA data from TCs from all over the province and sends them to the central server. The central server performs the following real-time data-intensive safety-critical functions as part of the Power Application Software [27]: (1) Overload monitoring and control, (2) Detection of separated power systems and (3) Power restoration after network failure.

We designed SCAPS so that it meets all the suitability criteria for a case study (Section 4). The UML model was defined and the system was implemented using Borland Delphi [2], which is a well-known Integrated Development Environment for Rapid Application Development.

The objective of our case study was to compare the durations for SDs D and E in Figure 11-(a), SCAPS’ MIOD, by running Operational Profile Tests (OPT) and Stress Tests (ST). Recall there was a time constraint on these SDs’ executions and our goal is to assess whether stress testing can help detect violations of this constraint. We considered OPTs as a useful baseline of comparison as this is a common testing practice to assess a system based on its expected usage in the field [19]. To derive operational profile test cases, we assumed an operational profile for SCAPS, which takes into account its business logic in the context of SCADA-based power systems. For example, overload and power failure situations are expected to be fairly rare in a power grid [27].

Recall that we modeled a HRT constraint in the MIOD of SCAPS in Figure 11-(a). This specifies the maximum acceptable value for the durations of SDs D and E: it should be less than 1,300 ms (milliseconds). Figure 16 shows the observed values of this duration by running 500 Operational Profile Tests (OPT) and 500 Stress Tests (ST). The X-axis is the test type and the Y-axis is duration in milliseconds. The quantile regions and the histograms of the two distributions are also depicted, and reported in Table 2.

Due to indeterminism in distributed environments, it is expected the duration of distributed messages can be different across different executions. Figure 16 shows that, despite such a variation, all OPTs executions satisfy the HRT constraint above, since all their durations are less than 1,300 ms (bold horizontal line). However, showing sharply different results, the constraint is violated in %96.4 (482/500) of stress test cases. These results suggest that our ST strategy is much more effective at stressing the system to exhibit violations of our HRT constraint than standard, operational profile-based testing.

When the experiments show that there can be scenarios in which one or more of the RT constraints can be violated in a DS, such as in our example above, performance engineering techniques should be applied to redesign the system and/or increase resources (for example, network capacities) or change the RT constraint values to more realistic levels.

| Table 2. Quantiles (ms) of the distribution in Figure 16. |
|---|---|---|---|---|---|---|---|
| Level | Min. | 10% | 25% | Median | 75% | 90% | Max. |
| OPT | 953 | 1029 | 1059 | 1094 | 1125 | 1156 | 1241 |
| ST | 1276 | 1305 | 1317 | 1329 | 1344 | 1358 | 1382 |

Figure 16. Maximum execution time of SDs D and E in Figure 11-(a) by running Operational Profile Tests (OPT) and Stress Tests (ST).

8. CONCLUSIONS

A stress test methodology aimed at increasing chances of discovering faults related to network traffic in distributed systems was presented. The technique uses the UML 2.0 model of a system, augmented with timing information. In particular we were very careful to design an adequate and realistic input test model precisely, which is one of the main contributions of this article. It mainly entails (1) a Network Deployment Diagram (following the UML package notation) that describes the distributed architecture in terms of system nodes and networks and (2) a Modified Interaction Overview Diagram (following the UML 2.0 interaction overview diagram notation) that describes execution constraints between sequence diagrams. Our stress testing technique relies on a careful identification of the control flow in UML 2.0 Sequence Diagrams and the network traffic they entail. These data are used to generate stress test requirements composed of specific control flow paths (in Sequence Diagrams) along with time values indicating when those paths have to be triggered so as to stress the network to the largest extent possible.

Using the specification of a real-world distributed system, we designed and implemented a prototype system and described how the stress test cases were derived and executed. We furthermore reported the results of applying our stress test methodology on the prototype system and discussed its effectiveness in detecting violation of a hard real-time constraint when compared to test cases based on an operational profile. Our first results are promising as they suggest that our stress test cases can help to increase the probability of exhibiting network traffic-related faults in distributed systems.

Some of our future works include: (1) Experimenting with the other 31 stress testing techniques that we mentioned as being defined; (2) Generalizing the methodology to other distributed-type faults, such as distributed unavailability of networks and nodes, and other resources such as CPU, memory and database; (3) Specifying, visualizing, and analyzing stress test requirements and stress test process using the UML 2.0 Testing Profile [23]; (4) Performing a risk assessment and fault analysis of distributed-type faults; and (5) Improving our tool support. We also plan to stress
test more complex distributed systems and investigate the effectiveness of the methodology.

ACKNOWLEDGMENTS
This work was in part supported by Siemens Corporate Research, Princeton, NJ and a Canada Research Chair grant. Lionel Briand and Yvan Labiche were further supported by NSERC operational grants.

REFERENCES