Journal of Universal Computer Science, vol. 14, no. 2 (2009),444-464
submitted: 20/10/08, accepted: 25/1/09, appeared: 28/1/09 © J.UCS

Stability in Heterogeneous Multimedia Networks under Adversarial Attacks[1]

Dimitrios Koukopoulos
(University of Ioannina, Ioannina, Greece
dkoukopoulos@cc.uoi.gr)

Abstract: A distinguishing feature of today's large-scale platforms for multimedia distribution and communication, such as the Internet, is their heterogeneity, predominantly manifested by the fact that a variety of communication protocols are simultaneously running over different hosts. A fundamental question that naturally arises for such common settings of heterogeneous multimedia systems concerns the presence (or not) of stability properties when individual greedy, contention-resolution protocols are composed in a large packet-switched multimedia network. A network is stable under a greedy protocol (or a composition of protocols) if, for any adversary of injection rate less than 1, the number of packets in the network remains bounded at all times. We focus on a basic adversarial model for packet arrival and path determination for which the time-averaged arrival rate of packets requiring a single edge is no more than 1. Within this framework, we study the property of stability under various compositions of contention-resolution protocols (such as LIS (*Longest-in-System*), FIFO (*First-In-First-Out*), FFS (*Furthest-from-Source*), and NTG (*Nearest-to-Go*)) and different packet trajectories trying to characterise this property in terms of network topologies. Such a characterisation provides us with the family of network topologies that, under specific compositions of protocols, can be made unstable by some adversarial traffic pattern. Finally, we present an experimental evaluation of the stability behaviour of specific network constructions with different protocol compositions under an adversarial strategy. Interestingly, some of our results indicate that such a composition leads to worst stability behaviour than having a single unstable protocol for contention-resolution. This suggests that the potential for instability incurred by the composition of protocols may be worse than that of any single protocol.

Keywords: Multimedia Communication Networks, Adversarial Attacks, Network Stability, Adversarial Queueing Theory
Categories: C.2.0, C.2.4, D.4.6, K.6.5

1 Introduction

1.1 Motivation and Framework

Motivation. Nowadays, the development and distribution of multimedia products are fast and inexpensive because of the rapid deployment of electronic technology and large-scale communication platforms. Some of the most important features of contemporary large-scale platforms for multimedia distribution and communication, such as the Internet, are their robustness and heterogeneity. Robustness is the ability of communication despite adversarial attacks, while heterogeneity comes around in

[1] Part of this work has appeared in the 2008 International Workshop on Multimedia Security in Communication (MUSIC'08), Hangzhou, China, August 2008, Paper id: 3769.

many different flavours. For example, different traffic sources over the Internet (due to varying mechanisms for supporting different service qualities) result in a heterogeneous mix of traffic traces. Moreover, although, conceptually, the Internet uses a unified set of protocols, in practice each protocol has been implemented with widely varying features. Thus, heterogeneity is a crucial feature that makes it difficult to model, verify and analyse the behaviour of such large-scale multimedia networks. As the Internet evolves into a ubiquitous communication infrastructure that supports multiple protocols running on different network hosts, its dependability on the presence of various adversarial attacks becomes critical. These attacks can degrade system performance and lead to service disruption. Thus, the study of performance and correctness properties of heterogeneous multimedia systems which suffer from adversarial attacks becomes a necessity.

One crucial aspect of the performance properties of heterogeneous multimedia networks relates to stability. Stability requires that the number of packets in the network remains bounded at all times. Adversarial attacks that can lead a network to instability can be seen as a type of denial of service attacks since their purpose is to flood the network (or a subnetwork) with packets whose sole purpose is to overload the local system in order to hamper (or prevent) legitimate users from having access to the system. If a network is proven to be stable its users are ensured that this network is secure against malicious attacks. Therefore, the users can trust the network. Roughly speaking, trust can be considered as a notion central to stable multimedia networks. Within this context, when something is proven to be stable, it is *trusted*. Studying the stability behaviour of a network is not an easy task. However, this study could help researchers detect and understand and even avoid the conditions which lead systems to unstable behaviour. Thus, the researchers will not only be informed of a better design for establishing and maintaining a trustworthy heterogeneous multimedia system, but they will also be assisted in the understanding of the concept of trust in a heterogeneous multimedia environment.

Objectives. We are interested in the behaviour of packet-switched multimedia networks in which packets arrive dynamically at the nodes and they are routed at discrete time steps across the links. Recent years have witnessed a vast amount of work on analysing packet-switched networks under non-probabilistic assumptions. We work within a model of worst-case continuous packet arrivals, originally proposed in [Borodin et al. 2001] and termed Adversarial Queueing Theory to reflect the assumption of an adversarial way of packet generation and path determination. A major issue that arises in such a setting is that of network stability-- will the number of packets in the network remain bounded at all times against any adversary under a single contention-resolution protocol or a composition of protocols? (By composition of contention-resolution protocols, we mean the simultaneous use of different such protocols at different queues of the network.). The answer to this question is non-trivial; since the property of network stability under a certain protocol (or composition of protocols) is a predicate quantified over all adversaries. It may depend on the network structure, the traffic pattern defined by the adversary and the composition of protocols employed to resolve packet conflicts. The traffic pattern controls where and how packets are injected into the network, and defines their path (trajectory).

Framework of Adversarial Queueing Theory. We consider a packet-switched communication network in which packets arrive dynamically at the nodes with predetermined paths, and they are routed at discrete time steps across the edges (links). Roughly speaking, the Adversarial Queueing Theory model views the time evolution of a packet-switched multimedia network as a game between an adversary and a protocol. At each time step, the adversary may inject a set of packets into some nodes. For each packet, the adversary specifies a path that the packet must traverse; when the packet arrives to its destination, it is absorbed by the system. When more than one packets wish to cross a queue at a given time step, a contention-resolution protocol is employed to resolve the conflict. A crucial parameter of the adversary is its injection rate *r*, where ($0 < r < 1$). Among the packets that the adversary injects in any time interval *I*, at most $r \mid I \mid$ can have paths that contain any particular edge. In this work, we embark on a study of the impact of the topological structure of the multimedia networks on their correctness and performance properties. In particular, we wish to pose the general question of whether it would be possible to detect network stability under specific compositions of protocols against various adversarial attacks using the knowledge of the topological structure of the network. This subfield of study was initiated in [Andrews et al. 2001] where it is proved that the family of undirected-path universally stable graphs is minor-closed and that there exists a finite set of basic undirected graphs such that a graph is stable, if and only if it does not contain any of the graphs of that set as a minor.

Stability. Roughly speaking, a protocol (or a composition of protocols) *P* is stable on a network *G* against an adversary *A* of rate *r* if there is a constant *B* for which the number of packets in the system is bounded at all times by *B* [Borodin et al. 2001]. On the other hand, a protocol (or a composition of protocols) *P* is universally stable, if it is stable against any adversary of rate less than 1 and on any network [Borodin et al. 2001]. We also say that a network *G* is universally stable, if any greedy protocol is stable against any adversary of rate less than 1 on *G* [Borodin et al. 2001]. Moreover, the property of network stability can be viewed under two different approaches; we refer to simple-path stability when packets follow simple paths (paths do not contain repeated edges and vertices), while we refer to stability when packets follow non-simple paths (paths do not contain repeated edges, but they can contain repeated vertices) [Alvarez et al. 2004].

Protocol name	*Which packet it advances:*	*Universally Stable*
LIS (*Longest-In-System*)	The least recently injected packet into the network	Yes [Andrews et al. 2001]
NTG (*Nearest-To-Go*)	The nearest packet to its destination	No [Andrews et al. 2001]
FFS (*Furthest-From-Source*)	The furthest packet from its origin	No [Andrews et al. 2001]
FIFO (*First-In-First-Out*)	The earliest arrived packet at the queue	No [Andrews et al. 2001]

Table 1: Greedy protocols considered in this paper

Greedy Contention-Resolution Protocols. We consider only greedy protocols—that is protocols that always advance a packet across a queue whenever at least one packet resides in the queue. The protocol specifies which packet will be chosen. We study four greedy protocols all of which enjoy simple implementations [Tab. 1]. All these protocols require some tie-breaking rule in order to be unambiguously defined. Here, we assume FIFO as a tie breaking rule for the adversary.

Approach. We consider all the compositions of NTG with LIS and FFS protocols. We examine whether the corresponding protocol composition is stable on the set of forbidden subgraphs for universal stability and simple-path universal stability [Fig. 1, Fig. 2]. For each forbidden subgraph, we demonstrate an adversary for which the composition is not stable on the subgraph. In addition, in order to qualitatively evaluate how unstable the compositions are, we consider the FIFO protocol, which is known not to be universally stable in general, but it is stable against the network *U*1. We measure the instability of the composition of FIFO with NTG against that of FIFO. Finally, we present an experimental evaluation of the stability properties of the set of forbidden subgraphs for universal stability and simple-path universal stability with different protocol compositions under an adversarial strategy in order to strengthen our theoretical results.

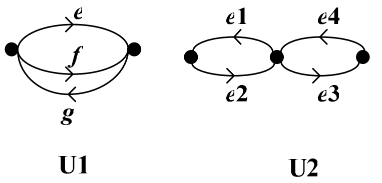

Figure 1: Forbidden subgraphs for universal stability

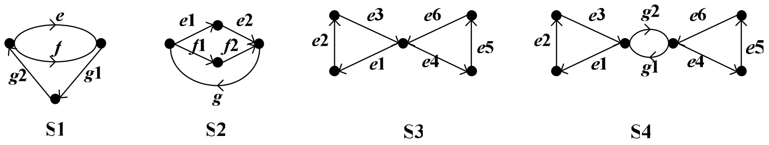

Figure 2: Forbidden subgraphs for simple-path universal stability

1.2 Contribution

Our work interestingly shows how the network structure precisely affects the stability behaviour of multimedia packet-switched networks under specific compositions of protocols, such as NTG, LIS, FFS, and FIFO, running on top of them, when they face various adversarial attacks. Our results are three-fold; they are summarised as follows:

- We demonstrate adversarial constructions that lead the set of subgraphs that are forbidden for universal stability and simple-path universal stability under a single protocol to instability when different compositions of contention-resolution protocols (NTG, LIS), (NTG, FFS), and (NTG, FFS, LIS) are composed on the network nodes. These results show for the first time that the forbidden subgraphs for universal stability and simple-path universal stability under a single protocol are also unstable when specific compositions of protocols are used for contention-resolution on network queues. Surprisingly, the compositions of NTG with LIS and FFS in some network constructions result in lower bounds on the injection rate for network instability compared to the instability bounds obtained from the usage of a single protocol into the same networks.

- We establish that, the composition of FIFO with NTG is not stable on the set of forbidden subgraphs for universal stability and simple-path universal stability. Not only does this result prove that the composition of FIFO with another protocol can result in instability even for the simple graphs that belong to the set of forbidden subgraphs for universal stability and simple-path universal stability, but it also shows that the subgraph $U1$, which has been proved stable for FIFO [Weinard 2006], can become unstable under a composition of FIFO with another protocol. These results together may modestly suggest that the composition of two protocols may turn out to exhibit more unstable behaviour than the usage of a single protocol that is already known not to be universally stable (such as FIFO).

- We present an experimental evaluation of the stability properties of the networks that are forbidden subgraphs for universal stability and simple-path universal stability under different adversarial strategies and various scenarios of protocol compositions. The experimental evaluation agrees with the theoretical results and provides an important insight into the understanding of the impact of heterogeneity on the performance properties of large-scale communication multimedia networks such as the Internet.

1.3 Related Work

The issue of composing distributed protocols (resp., objects) to obtain other protocols (resp., objects), and the properties of the resulting protocols (resp., objects), has a rich record in Distributed Computing Theory [Lynch 1996]. For example, Herlihy and Wing [Herlihy and Wing 1990] establish that a composition of linearizable memory objects (possibly distinct), each managed by its own protocols, preserves linearizability. In the community of Security Protocols, the statement that security is not compositional is considered to be folklore.

Adversarial environments can be used to model intrusion attacks as an intruder can behave like an adversary that tries to change network environment parameters concerning network topology, packet service rate or the used contention-resolution protocols. In particular, adversarial attacks that attempt to lead a network to instability aiming at flooding the network with packets whose sole purpose is to overload the local system. Such attacks can be seen as a type of denial of service attacks. In the community of Security, the study of intrusion detection and the proposal of methods for quality service protection against various attacks received a lot of interest [Kumar 1995, Levine and Kessler 2002, Moore et al. 2006, Oh et al. 2005, Yau et al. 2005].

In the community of stability Adversarial Queueing Theory model [Borodin et al. 2001] received a lot of attention in the study of network performance issues [Alvarez et al. 2004, Andrews et al. 2001, Koukopoulos et al. 2002, Weinard 2006]. The universal stability of various natural greedy protocols such as LIS was established in [Andrews et al. 2001]. Also, several greedy protocols such as NTG and FFS have been proved unstable [Andrews et al. 2001]. The instability of FIFO has been proved in [Andrews et al. 2001].

The subfield of study of the stability properties of compositions of protocols was introduced in [Koukopoulos et al. 2002] where the compositions of LIS with any of SIS (*Shortest-In-System*), NTS (*Nearest-To-Source*) and FTG (*Furthest-To-Go*) protocols have been proved unstable.

The existence of a finite set of basic undirected network graphs was proved in [Andrews et al. 2001] for which a graph G is stable for any r if and only if none of these graphs is a minor of G. A characterization was given in [Alvarez et al. 2004] for the universal stability of directed networks when the packets follow simple paths and non-simple paths. According to this characterization, a directed network graph where packets are injected in non-simple paths is universally stable if and only if it does not contain as subgraph any extension of the subgraphs $U1$ or $U2$ [Fig. 1]; while a directed graph where packets are injected in simple paths is universally stable if and only if it does not contain as subgraph any extension of the subgraphs $S1$ or $S2$ or $S3$ or $S4$ [Fig. 2]. Also, adversarial constructions were specified in [Alvarez et al. 2004] that lead to instability the network subgraphs $U1$, $U2$, $S2$, $S3$, and $S4$ for $r \geq 0.841$ and $U1$ for $r \geq 0.871$ when a single protocol is used for contention-resolution on the network queues. Moreover, the subgraph $U1$ has been proved stable for FIFO [Weinard 2006].

1.4 Roadmap

The rest of this paper is organized as follows. [Section 2] presents model definitions. [Section 3] demonstrates the stability properties of forbidden subgraphs for universal and simple-path universal stability under certain protocol compositions. [Section 4] shows the stability behaviour of the composition of FIFO and NTG protocols on forbidden subgraphs. [Section 5] makes an experimental evaluation of the stability behaviour of forbidden subgraphs. [Section 6] concludes our results. [Section 7] has a discussion of some open problems.

2 Theoretical Framework

The model definitions are patterned after those in [Borodin et al. 2001]. We consider that a routing network is modelled by a directed graph G on n vertices and m edges, $G = (V, E)$. Each vertex $x \in V$ represents a communication switch (node), and each edge $e \in E$ represents a link between two switches. In each node, there is a queue associated with each outgoing link. Time proceeds in discrete time steps. Queues store packets that are injected into the network with a route, which is a simple directed path in G. A packet is an atomic entity that resides at a queue at the end of any step. A packet must travel along paths in the network from its source to its destination, both of which are nodes in the network. When a packet is injected, it is placed in the queue of the first link on its route. When a packet reaches its destination, we say that it is *absorbed*. During each step, a packet may be sent from its current node along one of the outgoing edges from that node.

Any packets that wish to travel along an edge *e* at a particular time step, but they are not sent, they wait in a queue for the edge *e*. At each step, an *adversary* generates a set of requests. A *request* is a *path* specifying the route that will be followed by a packet. In this work, it is assumed, as it is common in packet routing, that there are two types of paths: simple paths where edges and vertices cannot be overlapped and non-simple paths where edges cannot be overlapped, while vertices can be overlapped [Alvarez et al. 2001]. We say that the adversary generates a set of packets when it generates a set of requested paths. Also, we say that a packet *p requires* an edge *e* at time step *t* if the edge *e* lies on the path from its position to its destination at time step *t*. There are no computational restrictions on how the adversary chooses its requests at any given time step.

The definition of a *bounded adversary A* of rate (*r*, *b*) (where $b \geq 1$ is a natural number and $0 < r < 1$) [Borodin et al. 2001] requires that for any edge *e* and any time interval *I*, the adversary injects no more than $r \mid I \mid + b$ packets during *I* that require edge *e* at their time of injection. Such a model allows for adversarial injection of packets that are "bursty" using the integer $b > 0$.

When we consider adversarial constructions for proving instability of specific protocol compositions in which we want to derive lower bounds, it is advantageous to have an adversary that is as weak as possible. Thus, for these purposes, we say that an adversary *A* has injection rate *r* if for any $t \geq 1$, any interval *I* of *t* steps, and any edge *e*, it injects no more than $r \mid t \mid$ packets during *I* that require edge *e* at the time of their injection.

In order to formalise the behaviour of a network, we use the notions of *system* and *system configuration*. A triple of the form <*G*, *A*, *P*> where *G* is a network, *A* is an adversary and *P* is the used protocol (or composition of protocols) on the network queues is called a system. The execution of the system proceeds in global time steps numbered 0, 1,…. Each time-step is divided into two sub-steps. In the first sub-step, one packet is sent from each non-empty queue over its corresponding link. In the second sub-step, packets are received by the nodes at the other end of the links; they are absorbed (eliminated) if that node is their destination, otherwise they are placed in the queue of the next link on their respective routes. New packets are injected in the second sub-step.

In every time step *t*, the current configuration C^t of a system <*G*, *A*, *P*> is a collection of sets $\{ S_e^t : e \in G \}$ where S_e^t is the set of packets waiting in the queue of the edge *e* at the end of time step *t*. If the current system configuration is C^t, we obtain the system configuration C^{t+1} for the next time step as follows: (i) Addition of new packets to some of the sets S_e^t, each of which has an assigned path in *G*, and (ii) for each non-empty set S_e^t deletion of a single packet $p \in S_e^t$ and its insertion into the S_f^{t+1} where *f* is the edge following *e* on its assigned path (if *e* is the last edge on the path of *p*, then *p* is not inserted into any set.). A time evolution of the system is a sequence of such configurations C^1, C^2,…. An execution of the adversary's construction on a system <*G, A, P*> determines the time evolution of the system configuration.

In the adversarial constructions we study here for proving instability, we split time into *phases*. In each phase, we study the evolution of the system configuration by considering corresponding *time rounds*. For each phase, we inductively prove that the number of packets of a specific subset of queues in the system increases in order to guarantee instability. This inductive argument can be applied repeatedly, thus showing instability.

Furthermore, we assume that there is a sufficiently large number of packets s_0 in the initial system configuration. This will imply instability results for networks with an empty initial configuration, as it was established in [Andrews et al. 2001]. For simplicity, and in a way similar to that in [Andrews et al. 2001], we omit floors and ceilings from our analysis, and we, sometimes, count time steps and packets only roughly. This may only result to loosing small additive constants, while it implies a gain in clarity.

3 Unstable Compositions of NTG with FFS and LIS

In this section we show lower bounds on injection rate that guarantee instability for specific networks [Fig. 1, Fig. 2] under the composition of NTG with FFS and LIS protocols when packets are injected with non-simple and simple paths.

3.1 Stability Behavior of U1 Network

First, consider the network $U1$ [Fig. 1] that uses the composition of NTG with LIS protocol where packets are injected with non-simple paths. We have:

Theorem 1. For the network $U1$, there is an adversary A of rate $r \geq 0.841$ such that the system <$U1$, A, (NTG, LIS)> is unstable.

Proof. The edge f uses LIS protocol, while the edges e, g use NTG protocol. *Inductive hypothesis*: At the beginning of phase j, there are s_j packets (called S set of packets) in the queues e, f requiring to traverse the edges e, g and f, g correspondingly. *Induction Step*: At the beginning of phase j+1 there will be more than s_j packets, $s_{j+1}> s_j$, in the queues e, f requiring to traverse the edges e, g and f, g correspondingly.

We will construct an adversary A such that the induction step will hold. Proving that the induction step holds, we ensure that the inductive hypothesis will hold at the beginning of phase j+1 with an increased value of s_j, $s_{j+1} > s_j$. In order to prove that the inductive argument works, we consider that there is a large enough number of packets s_j in the initial system configuration. During phase j the adversary plays four rounds of injections.

Round 1: It lasts $|T_1| = s_j$ time steps. During this round, the adversary injects in g a set Z1 of $|Z_1| = r|T_1|$ packets wanting to traverse the edges g, f. S packets have priority over Z1 packets in g.

Round 2: It lasts $|T_2| = r|T_1|$ time steps. During this round, the adversary injects a set Z_2 of $|Z_2| = r|T_2|$ packets in g requiring to traverse the edges g, e and a set Z_3 of $|Z_3| = r|T_2|$ packets in f requiring to traverse f. Z_1 packets have priority over Z_2 packets in g. All Z_1 packets arrive at queue f along with Z_3 packets. The total number of packets arriving at f during this round is $|Z_1| + |Z_3|$ packets. However, the duration of the round is $|T_2|$ time steps. Therefore, $|T_2|$ packets traverse f during this round. Thus, at the end of this round, there will be a set X of $|X| = r|T_2|$ packets in f wanting to traverse f and $|Z_2| = r|T_2|$ packets in g wanting to traverse g, e.

Round 3: It lasts $|T_3| = r|T_2|$ time steps. During this round, the adversary injects a set Z4 of $|Z_4| = r|T_3|$ packets in f requiring to traverse f and a set Z_5 of $|Z_5| = r|T_3|$ packets in e requiring to traverse e, g. X packets have priority over Z_4 packets in f because X packets are longer in the system than Z_4 packets. Thus at the end of this round, there are $|Z_4| = r|T_3|$ packets in f wanting to traverse f. Also, the Z_2 packets have priority over Z_5 packets in e. Thus, at the end of this round, there will be $|Z_5|$ packets in e wanting to traverse e, g.

Round 4: It lasts $|T_4| = r|T_3|$ time steps. During this round, the adversary injects a set Z_6 of $|Z_6| = r|T_4|$ packets in e requiring to traverse e and a set Z_7 of $|Z_7| = r|T_4|$ packets in f requiring to traverse f, g. Z_4 packets have priority over Z_7 packets in f because they are longer in the system than Z_7 packets. Also, Z_6 packets have priority over Z_5 packets in e, because Z_6 packets are nearest to their destination than Z_5 packets. At the end of this round, there are $|Y| = |Z_5| + |Z_6| - |T_4|$ packets in e wanting to traverse e, g. Therefore, at the end of this round, the number of packets in e, f requiring to traverse e, g and f, g is $s_{j+1} = |Z_7| + |Y| = 2r|T_4|$.

In order to have instability, we must have $s_{j+1} > s_j$. This holds for $2r|T_4| > |T_1|$, i.e. $r \geq 0.841$. This argument can be repeated for an infinite and unbounded number of phases ensuring that the number of packets in e, f requiring to traverse the edges e, g and f, g at the end of a phase is larger than at the beginning of the phase. □

Similarly to Theorem 1 we can prove Theorem 2. For the system <U1, A, (NTG, FFS)> the queue f of U1 uses FFS and e, g use NTG. For the system <U1, A, (NTG, LIS, FFS)> the queue f uses LIS, g uses FFS and e uses NTG. The strategy of the adversary is the same in both of the systems.

Adversary's strategy. We consider that each phase consists of four distinguished time rounds. The inductive argument states that if at the beginning of a phase j, there are s_j packets in the queues e, f requiring to traverse the edges e, g and f, g correspondingly, then at the beginning of phase j+1 there will be more than s_j packets in the same queues requiring to traverse the same edges. The adversary's strategy during a phase j follows:

Round 1: It lasts $|T_1| = s_j$ time steps. During this round, the adversary injects in g a set Z_1 of $|Z_1| = r|T_1|$ packets wanting to traverse the edges g, f.

Round 2: It lasts $|T_2| = r|T_1|$ time steps. During this round, the adversary injects a set Z_2 of $|Z_2| = r|T_2|$ packets in g requiring to traverse the edges g, e and a set Z_3 of $|Z_3| = r|T_2|$ packets in f requiring to traverse f.

Round 3: It lasts $|T_3| = r|T_2|$ time steps. During this round, the adversary injects a set Z_4 of $|Z_4| = r|T_3|$ packets in f requiring to traverse f and a set Z_5 of $|Z_5| = r|T_3|$ packets in e requiring to traverse e, g.

Round 4: It lasts $|T_4| = r|T_3|$ time steps. During this round, the adversary injects a set Z_6 of $|Z_6| = r|T_4|$ packets in e requiring to traverse e and a set Z_7 of $|Z_7| = r|T_4|$ packets in f requiring to traverse f, g.

Theorem 2. For the network U1 there is an adversary A of rate $r \geq 0.841$ such that the system <U1, A, N_i> is unstable where $i = \{1, 2\}$ and $N_i = \{$(NTG, FFS), (NTG, FFS, LIS)$\}$.

3.2 Stability Behavior of U2 Network

We consider network $U2$ [Fig. 1]. Similarly to Theorem 1 we can prove Theorem 3. For the system <$U2$, A_2, (NTG, LIS)> and the system <$U2$, A_2, (NTG, FFS)> the queue $e4$ uses LIS and FFS protocol correspondingly and the rest queues use NTG. For the system <$U2$, A_2, (NTG, LIS, FFS)> the queue $e4$ uses LIS, $e1$ uses FFS and $e2$, $e3$ use NTG. The strategy of the adversary is the same in these three systems.

Adversary's strategy. We consider that each phase consists of three distinguished time rounds. The inductive argument states that if at the beginning of a phase j, there are s_j packets in the queues $e2$, $e3$ requiring to traverse the edges $e2$, $e1$ and $e3$, $e4$, $e1$, then at the beginning of phase j+1 there will be more than s_j packets in the same queues requiring to traverse the same edges. We consider that each phase consists of three distinguished time rounds. The adversary's strategy during a phase j follows:

Round 1: It lasts $|T_1| = s_j$ time steps. During this round, the adversary injects in $e1$ a set Z_1 of $|Z_1| = r|T_1|$ packets wanting to traverse $e1$, $e2$, $e3$.

Round 2: It lasts $|T_2| = r|T_1|$ time steps. During this round, the adversary injects a set Z_2 of $|Z_2| = r|T_2|$ packets in $e2$ requiring to traverse $e2$ and a set Z_3 of $|Z_3| = r|T_2|$ packets in $e3$ requiring to traverse $e3$, $e4$, $e1$.

Round 3: It lasts $|T_3| = r|T_2|$ time steps. During this round, the adversary injects a set Z_4 of $|Z_4| = r|T_3|$ packets in $e2$ requiring to traverse $e2$, $e1$ and a set Z_5 of $|Z_5| = r|T_3|$ packets in $e3$ requiring to traverse $e3$.

Theorem 3. For the network $U2$ there is an adversary A_2 of rate $r \geq 0.794$ such that the system <$U2$, A_2, N_i> is unstable where i = {1, 2, 3} and N_i = {(NTG, LIS), (NTG, FFS), (NTG, FFS, LIS)}.

3.3 Stability Behavior of S1, S2, S3, S4 Networks

Now, we consider the networks $S1$, $S2$, $S3$ and $S4$ [Fig. 2]. Then, similarly to Theorem 1 we can prove Theorem 4.

Adversary's strategy in network $S1$. For the system <$S1$, A_1, (NTG, LIS)> and the system <$S1$, A_1, (NTG, FFS)> the queue f uses LIS and FFS protocol correspondingly and the rest queues use NTG. For the system <$S1$, A_1, (NTG, LIS, FFS)> the queue f uses LIS, $g1$ uses FFS and e, $g2$ use NTG. The strategy of the adversary is the same in these three systems. We consider that each phase consists of four distinguished time rounds. The inductive argument states that if at the beginning of a phase j, there are s_j packets in the queues e, f requiring to traverse the edges e, $g1$ and f, $g1$, then at the beginning of phase j+1 there will be more than s_j packets in the same queues requiring to traverse the same edges. The adversary's strategy during a phase j follows:

Round 1: It lasts $|T_1| = s_j$ time steps. During this round, the adversary injects in $g1$ a set Z_1 of $|Z_1| = r|T_1|$ packets wanting to traverse $g1$, $g2$.

Round 2: It lasts $|T_2| = r|T_1|$ time steps. During this round, the adversary injects a set Z_2 of $|Z_2| = r|T_2|$ packets in $g2$ requiring to traverse $g2$, e.

Round 3: It lasts $|T_3| = r|T_2|$ time steps. During this round, the adversary injects a set Z_3 of $|Z_3| = r|T_3|$ packets in $g2$ requiring to traverse $g2$, f and a set Z_4 of $|Z_4| = r|T_3|$ packets in e requiring to traverse e, $g1$.

Round 4: It lasts $|T_4| = r|T_3|$ time steps. During this round, the adversary injects a set Z_5 of $|Z_5| = r|T_4|$ packets in e requiring to traverse e and a set Z_6 of $|Z_6| = r|T_4|$ packets in f requiring to traverse f, $g1$.

*Adversary's strategy in network S*2. For the system <$S2$, A_2, (NTG, LIS)> and the system <$S2$, A_2, (NTG, FFS)> the queue g uses LIS and FFS protocol correspondingly and the rest queues use NTG. For the system <$S2$, A_2, (NTG, LIS, FFS)> the queue g uses FFS, $f2$ uses LIS and $e1$, $e2$, $f1$ use NTG. The strategy of the adversary is the same in these three systems. We consider that each phase consists of four distinguished time rounds. The inductive argument states that if at the beginning of a phase j, there are s_j packets in the queues $e2$, $f2$ requiring to traverse the edges $e2$, g and $f2$, g correspondingly, then at the beginning of phase j+1 there will be more than s_j packets in the same queues requiring to traverse the same edges. The adversary's strategy during a phase j follows:

Round 1: It lasts $|T_1| = s_j$ time steps. During this round, the adversary injects in g a set Z_1 of $|Z_1| = r|T_1|$ packets wanting to traverse g, $e1$.

Round 2: It lasts $|T_2| = r|T_1|$ time steps. During this round, the adversary injects a set Z_2 of $|Z_2| = r|T_2|$ packets in queue $e1$ requiring to traverse $e1$, $e2$ and a set Z_3 of $|Z_3| = r|T_2|$ packets in queue g requiring to traverse g, $f1$.

Round 3: It lasts $|T_3| = r|T_2|$ time steps. During this round, the adversary injects a set Z_4 of $|Z_4| = r|T_3|$ packets in $f1$ requiring to traverse $f1$, $f2$ and a set Z_5 of $|Z_5| = r|T_3|$ packets in $e2$ requiring to traverse $e2$, g.

Round 4: It lasts $|T_4| = r|T_3|$ time steps. During this round, the adversary injects a set Z_6 of $|Z_6| = r|T_4|$ packets in $e2$ requiring to traverse $e2$ and a set Z_7 of $|Z_7| = r|T_4|$ packets in $f2$ requiring to traverse $f2$, g.

*Adversary's strategy in network S*3. For the system <$S3$, A_3, (NTG, LIS)> the queues $e1$, $e2$ use LIS protocol and the rest queues use NTG. For the system <$S3$, A_3, (NTG, FFS)> the queues $e1$, $e2$ use FFS protocol and the rest queues use NTG. For the system <$S3$, A_3, (NTG, LIS, FFS)> the queue $e6$ uses LIS, the queues $e1$, $e2$ use FFS and the queues $e3$, $e4$, $e5$ use NTG. The strategy of the adversary is the same in these three systems. We consider that each phase consists of four distinguished time rounds. The inductive argument states that if at the beginning of a phase j, there are s_j packets in the queues $e3$, $e5$ requiring to traverse the edges $e3$, $e1$ and $e5$, $e6$, $e1$, then at the beginning of phase j+1 there will be more than s_j packets in the same queues requiring to traverse the same edges. The adversary's strategy during a phase j follows:

Round 1: It lasts $|T_1| = s_j$ time steps. During this round, the adversary injects in $e1$ a set Z_1 of $|Z_1| = r|T_1|$ packets wanting to traverse $e1$, $e2$.

Round 2: It lasts $|T_2| = r|T_1|$ time steps. During this round, the adversary injects a set Z_2 of $|Z_2| = r|T_2|$ packets in $e2$ requiring to traverse $e2$, $e3$, $e4$, $e5$.

Round 3: It lasts $|T_3| = r|T_2|$ time steps. During this round, the adversary injects a set Z_3 of $|Z_3| = r|T_3|$ packets in $e2$ requiring to traverse $e2$, $e3$ and a set Z_4 of $|Z_4| = r|T_3|$ packets in $e5$ requiring to traverse $e5$, $e6$, $e1$.

Round 4: It lasts $|T_4| = r|T_3|$ time steps. During this round, the adversary injects a set Z_5 of $|Z_5| = r|T_4|$ packets in $e3$ requiring to traverse $e3$, $e1$ and a set Z_6 of $|Z_6| = r|T_4|$ packets in $e5$ requiring to traverse $e5$.

*Adversary's strategy in network S*4. For the system <$S4$, A_4, (NTG, LIS)> the queues $e1$, $e2$ use LIS protocol and the rest queues use NTG. For the system <$S4$, A_4, (NTG, FFS)> the queues $e1$, $e2$ use FFS protocol and the rest queues use NTG. For the system <$S4$, A_4, (NTG, LIS, FFS)> the queue $e6$ uses LIS, the queues $e1$, $e2$ use FFS and the queues $e3$, $e4$, $e5$, $g1$, $g2$ use NTG. The strategy of the adversary is the same in these three systems. We consider that each phase consists of four distinguished time rounds. The inductive argument states that if at the beginning of a phase j, there are s_j packets in the queues $e3$, $e5$ requiring to traverse the edges $e3$, $e1$ and $e5$, $e6$, $g1$, $e1$, then at the beginning of phase j+1 there will be more than s_j packets in the same queues requiring to traverse the same edges. The adversary's strategy during a phase j follows:

Round 1: It lasts $|T_1| = s_j$ time steps. During this round, the adversary injects in $e1$ a set Z_1 of $|Z_1| = r|T_1|$ packets wanting to traverse $e1$, $e2$.

Round 2: It lasts $|T_2| = r|T_1|$ time steps. During this round, the adversary injects a set Z_2 of $|Z_2| = r|T_2|$ packets in $e2$ requiring to traverse $e2$, $e3$, $g2$, $e4$, $e5$.

Round 3: It lasts $|T_3| = r|T_2|$ time steps. During this round, the adversary injects a set Z_3 of $|Z_3| = r|T_3|$ packets in $e2$ requiring to traverse $e2$, $e3$ and a set Z_4 of $|Z_4| = r|T_3|$ packets in $e5$ requiring to traverse $e5$, $e6$, $g1$, $e1$.

Round 4: It lasts $|T_4| = r|T_3|$ time steps. During this round, the adversary injects a set Z_5 of $|Z_5| = r|T_4|$ packets in $e3$ requiring to traverse $e3$, $e1$ and a set Z_6 of $|Z_6| = r|T_4|$ packets in $e5$ requiring to traverse $e5$.

Theorem 4. For the network Si there is an adversary A_i of rate $r \geq 0.841$ such that the systems <Si, A_i, (NTG, LIS)>, <Si, A_i, (NTG, FFS)> and <Si, A_i, (NTG, LIS, FFS)> are unstable where $i = \{1,2,3,4\}$.

4 Instability of FIFO and NTG Compositions

In this section we show lower bounds on injection rate that guarantee instability for specific networks [Fig. 1, Fig. 2] under the composition of FIFO and NTG protocols when packets are injected with non-simple and simple paths. First, consider the network $U1$ [Fig. 1] where packets are injected with non-simple paths. We have:

Theorem 5. For the network $U1$ there is an adversary A of rate $r \geq 0.841$ such that the system <$U1$, A, (NTG, FIFO)> is unstable.

Proof. The edge e uses FIFO protocol, while the edges f, g use NTG protocol. *Inductive hypothesis*: At the beginning of phase j, there are s_j packets (called S set of packets) in the queues e, f requiring to traverse the edges e, g and f, g correspondingly. *Induction Step*: At the beginning of phase j+1 there will be more than s_j packets, $s_{j+1}>s_j$, in the queues e, f requiring to traverse the edges e, g and f, g correspondingly.

We will construct an adversary A such that the induction step will hold. Proving that the induction step holds, we ensure that the inductive hypothesis will hold at the beginning of phase j+1 with an increased value of s_j, $s_{j+1}>s_j$. In order to prove that the inductive argument works, we consider that there is a large enough number of packets s_j in the initial system configuration. During phase j the adversary plays four rounds of injections.

Round 1: It lasts $|T_1| = s_j$ time steps. During this round, the adversary injects in queue g a set Z_1 of $|Z_1| = r|T_1|$ packets wanting to traverse the edges g, f. S packets have priority over Z_1 packets in g.

Round 2: It lasts $|T_2| = r|T_1|$ time steps. During this round, the adversary injects a set Z_2 of $|Z_2| = r|T_2|$ packets in queue g requiring to traverse the edges g, e and a set Z_3 of $|Z_3| = r|T_2|$ packets in queue f requiring to traverse the edge f. Z_1 packets have priority over Z_2 packets in g. Therefore, all Z_1 packets arrive at f along with Z_3 packets. The total number of packets arriving at f during this round is $|Z_1| + |Z_3|$ packets. However, the duration of this round is $|T_2|$ time steps. Therefore, $|T_2|$ packets traverse f during this round. At the end of the round, there will be a set X of $|X| = r|T_2|$ packets in f wanting to traverse f and $|Z_2| = r|T_2|$ packets in g wanting to traverse the edges g, e.

Round 3: It lasts $|T_3| = r|T_2|$ time steps. During this round, the adversary injects a set Z_4 of $|Z_4| = r|T_3|$ packets in queue e requiring to traverse e and a set Z_5 of $|Z_5| = r|T_3|$ packets in f requiring to traverse the edges f, g. X packets have priority over Z_5 packets in f. At the end of this round, there are $|Z_5| = r|T_3|$ packets in f wanting to traverse f, g. Also, the Z_4 packets arrive at e along with Z_2 packets. The total number of packets arriving at e during this round is $|Z_4| + |Z_2|$ packets. However, the duration of this round is $|T_3|$ time steps. Therefore, $|T_3|$ packets traverse e during this round. Thus, at the end of this round, there will be a set Y of $| Y | = r|T_3|$ packets in e wanting to traverse e and $|Z_5| = r|T_3|$ packets in f wanting to traverse f, g.

Round 4: It lasts $|T_4| = r|T_3|$ time steps. During this round, the adversary injects a set Z_6 of $|Z_6| = r|T_4|$ packets in e requiring to traverse the edges e, g and a set Z_7 of $|Z_7| = r|T_4|$ packets in f requiring to traverse the edge f. Z_7 packets have priority over Z_5 packets in f. Thus at the end of this round, there are $|Z_8| = r|T_4|$ packets in f wanting to traverse f, g. Also, Y packets have priority over Z_6 packets in e, because Y packets are longer time in e than Z_6 packets. At the end of this round, there are $s_{j+1} = |Z_6| + |Z_8|$ packets in e, f requiring to traverse e, g and f, g.

In order to have instability, we must have $s_{j+1} > s_j$. This holds for $2r|T_4| > |T_1|$, i.e. $r \geq 0.841$. This argument can be repeated for an infinite and unbounded number of phases ensuring that the number of packets in e, f requiring to traverse e, g and f, g at the end of a phase is larger than at the beginning of the phase forever. □

Now, consider the network $U2$ [Fig. 1]. Similarly to Theorem 5 we can prove Theorem 6. For the system <$U2$, A_2, (NTG, FIFO)> the queues $e2$, $e4$ use FIFO, and the queues $e1$, $e3$ use NTG. The inductive argument and the adversary's strategy for the system <$U2$, A_2, (NTG, FIFO)> during a phase j is the same as for the systems <$U2$, A_2, N_i> in Theorem 3.

Theorem 6. For the network $U2$ there is an adversary A_2 of rate $r \geq 0.867$ such that the system <$U2$, A_2, (NTG, FIFO)> is unstable.

Now, we consider the networks $S1$ and $S2$, [Fig. 2]. Then, similarly to Theorem 5 we can prove Theorem 7. For the system <$S1$, A_1, (NTG, FIFO)> the queue f uses FIFO and e, $g1$, $g2$ use NTG. For the system <$S2$, A_2, (NTG, FIFO)> the queue $f2$ uses FIFO and the queues $f1$, g, $e1$, $e2$ use NTG. The inductive argument and the adversary's strategy for the systems <$S1$, A_1, (NTG, FIFO)> and <$S2$, A_2, (NTG, FIFO)> is the same as for the systems <$S1$, A_1, (NTG, LIS)> and <$S2$, A_2, (NTG, LIS)> in Theorem 4 correspondingly.

Theorem 7. For the network *Si* there is an adversary Ai of rate $r \geq 0.908$ such that the system <*Si, A_i*, (NTG, FIFO)> is unstable where $i = \{1, 2\}$.

Now, we consider the networks *S*3 and *S*4 [Fig. 2]. Then, similarly to Theorem 5 we can prove Theorem 8. For the system <*S*3, A_3, (NTG, FIFO)> the queues *e*3, *e*6 use FIFO and the queues *e*1, *e*2, *e*4, *e*5 use NTG. For the system <*S*4, A_4, (NTG, FIFO)> the queues *e*3, *e*6 use FIFO and the queues *e*1, *e*2, *e*4, *e*5, *g*1, *g*2 use NTG. We consider that each phase consists of four distinguished time rounds. For the system <*S*3, A_3, (NTG, FIFO)> (<*S*4, A_4, (NTG, FIFO)>) the inductive argument states that if at the beginning of a phase *j*, there are s_j packets in the queues *e*3, *e*5 (*e*3, *e*5) requiring to traverse the edges *e*3, *e*1 (*e*3, *e*1) and *e*5, *e*6, *e*1 (*e*5, *e*6, *g*1, *e*1) correspondingly, then at the beginning of phase *j*+1 there will be more than s_j packets in the same queues requiring to traverse the same edges. The adversary's strategy for the systems <*S*3, A_3, (NTG, FIFO)> and <*S*4, A_4, (NTG, FIFO)> during the first two rounds of a phase *j* is the same as for the systems <*S*3, A_4, (NTG, LIS)> and <*S*4, A_4, (NTG, LIS)> in Theorem 4 correspondingly.

For the system <*S*3, A_3, (NTG, FIFO)> the adversary's construction during the last two rounds of a phase *j* is as follows:

Round 3: It lasts $|T_3| = r|T_2| = r^2 s_j$ time steps. During this round, the adversary injects a set Z_3 of $|Z_3| = r|T_3|$ packets in *e*3 requiring to traverse *e*3 and a set Z_4 of $|Z_4| = r|T_3|$ packets in *e*5 requiring to traverse *e*5, *e*6, *e*1.

Round 4: It lasts $|T_4| = r|T_3|$ time steps. During this round, the adversary injects a set Z_5 of $|Z_5| = r|T_4|$ packets in *e*3 requiring to traverse *e*3, *e*1 and a set Z_6 of $|Z_6| = |T_4| - |T_3| + |T_3|^{2} / (|T_3| + |Z_3|)$ packets in *e*5 requiring to traverse *e*5.

For the system <*S*4, A_4, (NTG, FIFO)> the adversary's construction during the last two rounds of a phase *j* is as follows:

Round 3: It lasts $|T_3| = r|T_2| = r^2 s_j$ time steps. During this round, the adversary injects a set Z_3 of $|Z_3| = r|T_3|$ packets in *e*3 requiring to traverse *e*3 and a set Z_4 of $|Z_4| = r|T_3|$ packets in *e*5 requiring to traverse *e*5, *e*6, *g*1, *e*1.

Round 4: It lasts $|T_4| = r|T_3|$ time steps. During this round, the adversary injects a set Z_5 of $|Z_5| = r|T_4|$ packets in *e*3 requiring to traverse *e*3, *e*1 and a set Z_6 of $|Z_6| = |T_4| - |T_3| + |T_3|^{2} / (|T_3| + |Z_3|)$ packets in *e*5 requiring to traverse *e*5.

Theorem 8. For the network *Si* there is an adversary A_i of rate $r \geq 0.9$ such that the system <*Si, A_i*, (NTG, FIFO)> is unstable where $i = \{3, 4\}$.

5 Experimental Evaluation

In order to evaluate our theoretical results [Section 3, Section 4] about the stability properties of forbidden subraphs for universal stability and simple-path universal stability under various protocol compositions we carried an experimental study. All of our implementations follow closely the network constructions, the adversarial strategies and the properties of contention-resolution protocols we described in [Section 3] and [Section 4]. They have been implemented as C++ classes by using C++ Builder.

The simulation environment that we developed is based on the Adversarial Queueing Model presented in Section 2 and allows us to perform an experiment having taken into account specific parameters: symmetric or non-symmetric network construction, the packet injection rate, the adversarial strategy, the used contention-resolution protocol or composition of protocols, the number of phases and the amount of initial packets in the network along with their placement into the network queues. The experiments were conducted on a Windows box (Windows XP, Pentium III at 933MHz, with 512MB memory at 133MHz) using C++ Builder.

	(NTG, LIS)	(NTG, FFS)	(NTG, LIS, FFS)	(NTG, FIFO)
*U*1	LIS: [*f*] ($r \geq 0.841$)	FFS: [*f*], ($r \geq 0.841$)	LIS: [*f*], FFS: [*g*], ($r \geq 0.841$)	FIFO: [*e*], ($r \geq 0.841$)
*U*2	LIS: [*e*4], ($r \geq 0.794$)	FFS: [*e*4], ($r \geq 0.794$)	LIS: [*e*4], FFS: [*e*1], ($r \geq 0.794$)	FIFO: [*e*2, *e*4], ($r \geq 0.867$)

Table 2: Instability of protocol compositions of forbidden subraphs for universal stability

We are interested in the behaviour of the number of packets in the network queues in successive phases for various compositions of protocols. If the total number of packets in the network queues increases at any time, then the network is unstable. In [Fig. 3, Fig. 4, Fig. 5] we illustrate our experiments with respect to the worst estimated injection rate for instability under all protocol compositions studied here.

	(NTG, LIS)	(NTG, FFS)	(NTG, LIS, FFS)	(NTG, FIFO)
*S*1	LIS: [*f*], ($r \geq 0.841$)	FFS: [*f*], ($r \geq 0.841$)	LIS: [*f*], FFS: [*g*1], ($r \geq 0.841$)	FIFO: [*f*], ($r \geq 0.908$)
*S*2	LIS: [*g*], ($r \geq 0.841$)	FFS: [*g*], ($r \geq 0.841$)	LIS: [*f*2], FFS: [*g*], ($r \geq 0.841$)	FIFO: [*f*2], ($r \geq 0.908$)
*S*3	LIS: [*e*1, *e*2], ($r \geq 0.841$)	FFS: [*e*1, *e*2], ($r \geq 0.841$)	LIS: [*e*6], FFS: [*e*1, *e*2], ($r \geq 0.841$)	FIFO: [*e*3, *e*6], ($r \geq 0.9$)
*S*4	LIS: [*e*1, *e*2], ($r \geq 0.841$)	FFS: [*e*1, *e*2], ($r \geq 0.841$)	LIS: [*e*6], FFS: [*e*1, *e*2], ($r \geq 0.841$)	FIFO: [*e*3, *e*6], ($r \geq 0.9$)

Table 3: Instability of protocol compositions of forbidden subraphs for simple-path universal stability

The results of our experiments are summarized in [Tab. 2] and [Tab. 3]. The information of which protocol is used in each queue for contention-resolution is included into the tables. For example, in [Tab. 2], in the cell that corresponds to the composition (NTG, LIS) on *S*1, the line LIS: [*f*], ($r \geq 0.841$) means that all the queues use NTG except from the queue *f* which uses LIS protocol and the injection rate lower bound that guarantees instability is $r \geq 0.841$.

Generally, we formulated our experiments assuming that initially there are s_0=1000 packets in the system. In addition, all of the experiments are executed for 80 phases. We start the experimentation by considering the effect of the composition of NTG with LIS, FFS, and FIFO protocols on the stability properties of networks *U*1 and *U*2. [Fig. 3b, Fig. 3d] depict the total number of packets into the queues of *U*1 and *U*2 correspondingly under the compositions of NTG with LIS, FFS, (LIS, FFS), and FIFO protocols. Furthermore, for comparison reasons, we estimate the evolution of the number of packets into the network when FIFO or NTG is used for contention-resolution on all queues of *U*1 [Fig. 3a] and *U*2 [Fig. 3c].

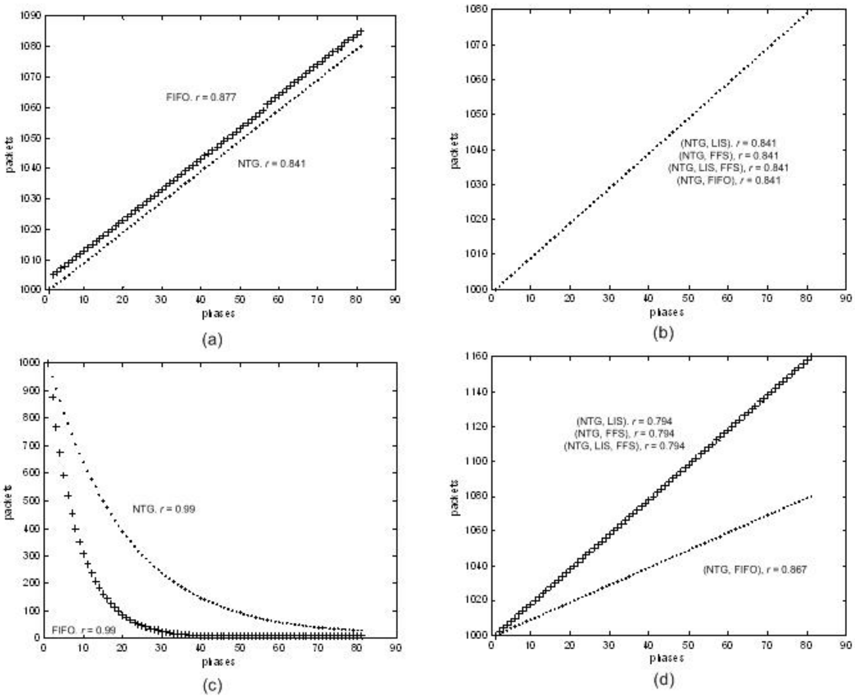

Figure 3: Instability Curves of U1and U2 under a protocol or a composition of protocols: (a) NTG and FIFO on U1, (b) compositions (NTG, LIS), (NTG, FFS), (NTG, LIS, FFS), (NTG, FIFO) on U1, (c) NTG and FIFO on U2, (b) compositions (NTG, LIS), (NTG, FFS), (NTG, LIS, FFS), (NTG, FIFO) on U2

The results of the experiments on networks *U*1 and *U*2 [Tab. 2] agree with the theoretical results obtained in Theorems 1, 2, 3, 5 and 6. Those results [Tab. 2] show that the instability properties of the set of forbidden subgraphs for universal stability (*U*1 and *U*2) under a single protocol are maintained, even though we use protocol compositions for contention resolution on different network queues. Even in the case of composing an unstable protocol (NTG) with a universally stable protocol (LIS) on networks *U*1 and *U*2 we obtain instability. Surprisingly, in the case of the composition pairs (NTG, LIS), (NTG, FFS) and (NTG, LIS, FFS) on network *U*2 we found an instability bound on the injection rate ($r \geq 0.794$) lower than the one specified in [Alvarez et al. 2004] ($r \geq 0.841$) where only a single protocol is applied on U2. Furthermore, applying the same adversarial strategy on network *U*2, either we use a single protocol for contention resolution (FIFO or NTG) on all network queues, or we use a composition of NTG with any of LIS, FFS, (LIS, FFS) and FIFO, we observe that the stability properties of U2 are different [Fig. 3c, Fig. 3d]. In particular, when we use a single contention-resolution protocol, the network is stable, while using any of the above protocol compositions the network becomes unstable. This is an indication that networks face worst stability behaviour under protocol compositions.

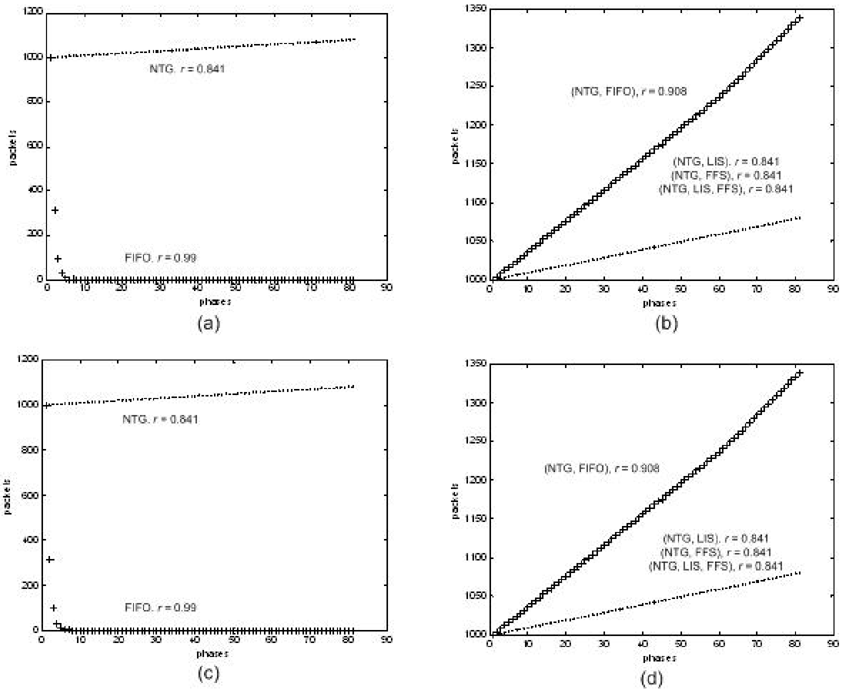

Figure 4: Instability Curves of S1 and S2 under a protocol or a composition of protocols: (a) NTG and FIFO on S1, (b) compositions (NTG, LIS), (NTG, FFS), (NTG, LIS, FFS), (NTG, FIFO) on S1, (c) NTG and FIFO in S2, (d) compositions (NTG, LIS), (NTG, FFS), (NTG, LIS, FFS), (NTG, FIFO) on S2

After studying the stability properties of networks *U*1 and *U*2, we study the effect of composing protocols NTG with LIS, FFS, and FIFO on networks *S*1 and *S*2. [Fig. 4b, Fig. 4d] depict the total number of packets into the queues of *S*1 and *S*2 correspondingly under the compositions of NTG with LIS, FFS, (LIS, FFS), and FIFO protocols. Furthermore, for comparison reasons, we estimate the evolution of the number of packets into the network when FIFO or NTG is used for contention-resolution on all queues of *S*1 [Fig. 4a] and *S*2 [Fig. 4c].

The results of the experiments on networks $S1$ and $S2$ [Tab. 3] agree with the theoretical results obtained in Theorems 4 and 7. Those results [Tab. 3] show that the instability properties of the subset of forbidden subgraphs for simple-path universal stability ($S1$ and $S2$) under a single protocol are maintained, even though we use protocol compositions for contention resolution on different network queues. Even in the case of composing an unstable protocol (NTG) with a universally stable protocol (LIS) on networks $S1$ and $S2$ we obtain instability. Surprisingly, in the case of the composition pairs (NTG, LIS), (NTG, FFS) and (NTG, LIS, FFS) on network $S1$ we found an instability bound on the injection rate ($r \geq 0.841$) lower than the one specified in [Alvarez et al. 2004] ($r \geq 0.871$) where only a single protocol is applied on $S1$. Furthermore, we observe that by applying the same adversarial strategy on network $S1$ using either FIFO on all network queues for contention resolution or the composition of NTG with FIFO, the stability properties of $S1$ are different [Fig. 4a, Fig. 4b]. In particular, when we use only FIFO for contention resolution $S1$ is stable, while composing NTG with FIFO makes the network unstable. The same observation holds in the case of network $S2$ [Fig. 4c, Fig. 4d]. Again, this is an indication that networks face worst stability behaviour under protocol compositions.

Finally, we experiment with the effect of composing protocols NTG with LIS, FFS, and FIFO on networks $S3$ and $S4$. [Fig. 5b, Fig. 5d] depict the total number of packets into the queues of $S3$ and $S4$ correspondingly under the compositions of NTG with LIS, FFS, (LIS, FFS), and FIFO. Furthermore, for comparison reasons, we estimate the evolution of the number of packets into the network when FIFO or NTG is used for contention-resolution on all queues of $S3$ [Fig. 5a] and $S4$ [Fig. 5c]

The results of the experiments on networks $S3$ and $S4$ [Tab. 3] agree with the theoretical results obtained in Theorems 4 and 8. Those results [Tab. 3] show that the instability properties of the subset of forbidden subgraphs for simple-path universal stability ($S3$ and $S4$) under a single protocol are maintained, even though we use protocol compositions for contention resolution on different network queues. Even in the case of composing an unstable protocol (NTG) with a universally stable protocol (LIS) on networks $S3$ and $S4$ we obtain instability. Furthermore, we observe that by applying the same adversarial strategy on network $S3$ using either FIFO on all network queues for contention resolution or the composition of FIFO with NTG, the stability properties of $S3$ are different [Fig. 5a, Fig. 5b]. In particular, when we use only FIFO for contention resolution $S3$ is stable, while composing NTG with FIFO makes the network unstable. The same observation holds in the case of network $S4$ [Fig. 5c, Fig 5d]. This is another indication that networks face worst stability behaviour under protocol compositions.

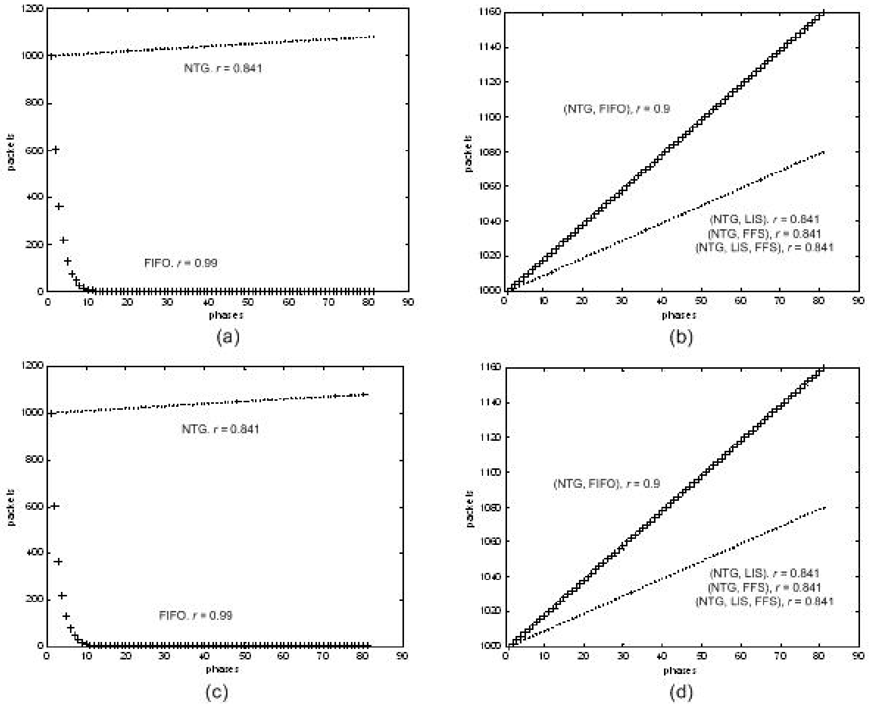

Figure 5: Instability Curves of S3 and S4 under a protocol or a composition of protocols: (a) NTG and FIFO on S3, (b) compositions (NTG, LIS), (NTG, FFS), (NTG, LIS, FFS), (NTG, FIFO) on S3, (c) NTG and FIFO on S4, (d) compositions (NTG, LIS), (NTG, FFS), (NTG, LIS, FFS), (NTG, FIFO) on S4

6 Conclusions

In this work, we study how efficiently the property of stability under the composition of specific protocols ((NTG, LIS), (NTG, FFS), (NTG, LIS, FFS), (NTG, FIFO)) can be characterised considering directed graphs where packets are injected with non-simple or simple paths under the Adversarial Queueing Model. In particular, we prove that the set of subgraphs that are forbidden for universal stability and simple-path universal stability under a single protocol maintain their instability when specific compositions of contention-resolution protocols are composed on the network queues. Interestingly, some of the compositions on some network constructions result in lower bounds on injection rate for network instability compared to the usage of a single protocol.

Also, we show that the stability properties of FIFO networks are not preserved when FIFO is composed with NTG. In particular, network constructions that are stable when FIFO is used as the only contention-resolution protocol become unstable when FIFO is composed with NTG under the same adversarial constructions. Even, the subgraph *U*1 that is stable for FIFO under any adversarial construction [Weinard 2006] becomes unstable composing FIFO with NTG. Thus, we can suggest that the instability properties of a protocol that is not universally stable can become worse when it is composed with another protocol on the same network.

Finally, in order to evaluate our theoretical results we proceed in the experimental analysis of the stability of forbidden subgraphs for universal stability and simple-path universal stability under different adversarial strategies and various scenarios of protocol compositions. We feel that this study is a nice complement to our theoretical analysis and gives a better understanding of how an adversary/intruder can exploit the topological structure of a large-scale heterogeneous multimedia network in order to flood the network with packets degrading system performance and leading to service disruption.

7 Future Work

A lot of problems remain open. Our results suggest that the instability properties of a protocol that is not universally stable can become worse when it is composed with another protocol on the same network. Proving (or disproving) this remains an open problem. Also, we show that the forbidden network subgraphs for universal stability and simple-path universal stability under a single contention-resolution protocol maintain their instability properties when we use protocol compositions for contention-resolution on different network queues. However, it is an open question, whether there are not other subgraphs that are forbidden for universal stability and simple-path universal stability when compositions of protocols are used for contention-resolution on different network queues. Another avenue for further research is whether there are upper bounds on the injection rate that guarantee stability for forbidden subgraphs when we use protocol compositions for contention-resolution. An interesting problem is to characterise the stability of the compositions of LIS with any of SIS, NTS and FTG protocols that have been proved unstable for specific networks in [Koukopoulos et al. 2002]. Finally, it is worth giving attention to the study of the stability behaviour of networks and protocols in environments where the adversary controls the movement of the network nodes.

References

[Alvarez et al. 2004] Alvarez, C., Blesa, M., Serna, M.: "A Characterization of Universal Stability in the Adversarial Queuing Model"; SIAM J. on Computing, 34 (2004), 41-66.

[Andrews et al. 2001] Andrews, M., Awerbuch, B., Fernandez, A., Kleinberg, J., Leighton, T., Liu, Z.: "Universal Stability Results for Greedy Contention-Resolution Protocols"; J. of the ACM, 48 (2001), 39-69.

[Borodin et al. 2001] Borodin, A., Kleinberg, J., Raghavan, P., Sudan, M., Williamson, D.: "Adversarial Queueing Theory"; J. of the ACM, 48 (2001), 13-38.

[Floyd and Paxson 2001] Floyd, S., Paxson, V.: "Difficulties in Simulating the Internet"; IEEE/ACM Trans. on Networking, 9 (2001), 392-403.

[Herlihy and Wing 1990] Herlihy, M. P., Wing, J.: "Linearizability: A Correctness Condition for Concurrent Objects"; ACM Trans. on Programming Languages and Systems, 12, 3 (1990), 463-492.

[Koukopoulos et al. 2002] Koukopoulos, D., Mavronicolas, M., Nikoletseas, S., Spirakis, P.: "On the Stability of Compositions of Universally Stable, Greedy, Contention-Resolution Protocols"; Proc. 16th Int. Symposium on DIStributed Computing, LNCS 2508, Springer, Toulouse (2002), 88-102.

[Kumar 1995] Kumar, S.: "Classification and detection of computer intrusions"; Ph.D. Dissertation, Dept. Computer Science, Purdue University, USA (1995).

[Levine and Kessler 2002] Levine, D., Kessler, G.: "Chapter 11 - Denial of Service Attacks, Computer Security Handbook, 4th Edition"; John Wiley & Sons (2002).

[Lynch 1996] Lynch, N.: "Distributed Algorithms"; Morgan Kaufmann (1996).

[Moore et al. 2006] Moore, D., Shannon, C., Brown, D. J., Voelker, G.M., Savage, S.: "Inferring Internet Denial-of-Service Activity"; ACM Trans. on Computer System, 24, 2 (2006), 115-139.

[Oh et al. 2005] Oh, J.-T., Park, S.K., Jang, J.-S., Jeon, Y. -H.: "Detection of DDoS and IDS Evasion Attacks in a High-Speed Networks Environment"; Int. J. of Computer Science and Network Security, 7, 6 (2005), 124-131.

[Weinard 2006] Weinard, M.: "Deciding the FIFO Stability of Networks in Polynomial Time"; Proc. 8th Int. Conf. on Algorithms and Complexity, LNCS 3998, Springer, Rome (2006), 81-92.

[Yau et al. 2005] Yau, D. K. Y., Lui, J.C.S., Liang, F., Yam, Y.: "Defending against Distributed Denial-of-Service Attacks with Max-Min Fair Server-Centric Router Throttles"; IEEE/ACM Trans. on Networking, 13, 1 (2005), 29-42.