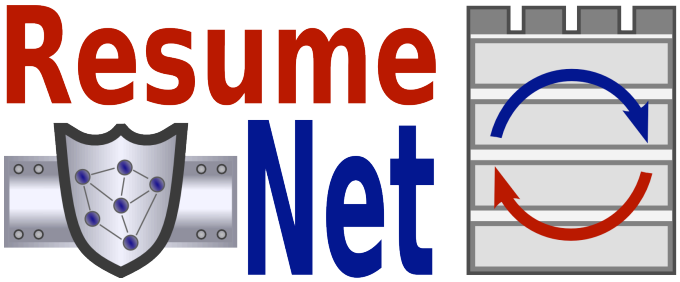
Resilience and Survivability for future networking: framework, mechanisms, and experimental evaluation



Deliverable number	2.1a
Deliverable name	First draft on defensive measures for resilient networks
WP number	2
Delivery date	30/11/2009
Date of Preparation	15/12/2009
Editor	E. Gourdin
Contributor(s)	C. Doerr (TUD), E. Gourdin (FT), G.G. Popa (ETHZ), J. Omic (TUD), J.P.G. Sterbenz (KU), J.P. Rohrer (KU), T. Taleb (NEC), P. Van Mieghem (TUD)
Internal reviewer	D. Hutchison (ULANC), M. Karaliopoulos (ETHZ), H. de Meer and A. Fischer (UP)

For ResumeNet project internal and PO use only

Summary

This is the first deliverable concerning defensive measures for network resilience. Being the first D in the D^2R^2+DR framework, defensive measures are also the first step toward building resilient networks. *Defensive measures* include all actions that can be performed before the challenges effectively occur so that the network is sufficiently well-armed to resist most of these challenges without considerable performance degradation. In this deliverable, we concentrate on selected defensive measures in these areas that are being addressed in ResumeNet. These measures include the network design process (define the topology and dimension the links), the choice of efficient routing mechanisms, and a protection strategy assessed by relevant models.

Contents

1 Introduction

In this deliverable, we are concerned with defensive measures for network resilience. By *defensive measures*, we mean everything that can be done before the challenges effectively occur. The question of resilience can be addressed at almost any phase during the design of a new network or the deployment of new service. It "simply" consists in asking whether the network or the service can still remain operational (or at least, at a certain level), if a challenge occurs. Among the various challenges that can be considered, a first major distinction can be made between *unintentional events* and *intentional actions*. Events in the first category include equipment failures, resource shortage, unpredicted traffic conditions, erroneous maintenance operations, environmental disaster, and many others. Actions in the second category include intentional attacks of persons or entities wishing to harm a network or a system, and actions of people or entities in competition for the usage of the same resources. Broadly speaking, unintentional events can be handled with deterministic or stochastic models, either by enumerating discrete scenarios with occurrence probability, or using continuous distributions; whereas intentional actions often require, in addition, game theoretical models.

When designing networks taking into account defensive measures, there are usually three contradictory criteria or families of criteria that are crucial aspects of QoS (Quality of Service):

- **cost** of the network, that is often to be minimized, or sometimes to be kept within a given budget constraint;
- **performance**, which includes a broad range of distinct metrics (delay, jitter, packet loss, availability,...);
- **security**, which covers everything that makes the data transfer and delivery reliable and safe.

Obviously, these three criteria are often contradictory. For instance, a natural solution to enhance the performance would be to increase the network connectivity and the routing infrastructure, thereby increasing the cost. Likewise, increasing the security might involve, either reducing the connectivity to limit the security leaks, or increasing filtering, detection and various additional processing tasks that will end up slowing the performances. These numerous contradictions can be summarized in the following picture:

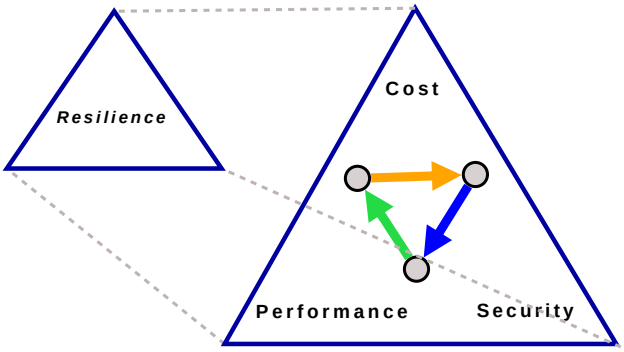


Figure 1: The three conflicting objectives hidden behind the concept of resilience

The expressions "designing a network" or "deploying a service" are drastic short-cuts for very complex real-case situations. There are many different types of networks, often composed

of successive layers, each one responsible for different functionalities, realized through different protocols, having different characteristics and deployed and managed over different time-scales. As a result, it is impractical to address all aspects of potential defensive measures for all possible networks in this deliverable. Instead, the focus is on key concepts and defensive actions. Some of the presented approaches are sufficiently generic to be applied to a wide range of different networks; whereas, others are more specifically tuned for specifics types of networks. Particular attention is paid to the wireless mesh networks (WMNs). WMNs have to cope up with a much wider range of challenges than wired networks and offer themselves as valuable study cases, through which a lot of concepts can be studied and analyzed.

2 Scope of the deliverable

Task 2.1 covers a broad range of defensive measures ranging from topological choices and structural design to traffic engineering and deployment of protection mechanisms:

- Topology and dimensioning aspects: here, we address the question of the network structure. Designing a suitable topology with certain connectivity requirements and sufficient capacity provisioning can already help the network to confront a number of challenges, including failures and traffic bursts, while maintaining a reasonable operational level.
- Routing protocols and strategies: given the network structure, a set of well-chosen routing mechanisms with fine tuned parameters should provide the network with additional capability to sustain similar events.
- Security protocols and mechanisms: since the environment is typically multi-agent and competitive, it is of utmost importance to model hostile or selfish behaviors and be able to determine how to optimally deploy curing, filtering or protection mechanisms to increase security without impacting too much the other important metrics (cost, QoS).

In each of these three fields, specific problems will be analyzed and mathematical models will be derived to capture and provide insight to real-world use cases. New algorithmic tools will be proposed to assess the models or solve the problems. This first deliverable of Task 2.1 introduces the various problems, formulates the respective research questions and provides the related state-of-the-art. It also reports some preliminary results.

3 State of the art, first results and future production plan

The defensive measures will benefit from different contributors (ETHZ, FT, KU, NEC and TUDelft), each one with different background and different expertise. The scientific tools that are used in the research activities include game and graph theory, optimization, markovian models, but also simulation. In this deliverable, several quite different types of defensive measures have been analyzed and partially addressed by the different contributors. For some of them important results have already been produced. The detailed results of the deliverable are contained in the papers (at various stages of publication) attached in the appendix. This section provides summaries of the various papers in each different research area.

3.1 Topological conditions for collaboration in wireless mesh network

Wireless multi-hop networks (WMNs) usually involve nodes operated by different administrative entities or end users that voluntarily avail resources for their formation and operation. Besides challenges related to the communication environment, such as wireless error-prone links and radio interference, WMNs are particularly vulnerable to node selfishness phenomena. Selfishness points to nodes that do not consistently participate in fundamental network operations, e.g., data routing and forwarding or radio resource sharing. It is motivated by the desire to obtain better performance from the network or the need to preserve some scarce resources, such as the node battery or storage space. concerns about the node resources. The non-perfect node cooperation has been shown to result in network performance degradation and may threaten the very basic capability of the network to form and operate. Therefore, specific countermeasures have to be built in the network in order to alleviate as much as possible node selfishness. Since *reactive* monitoring and punishment mechanisms against selfishness are difficult to implement, realistic countermeasures will have to take the form of proactive/preventive measures that add to the network *defense*.

Focusing on the network layer, completely decentralised networks such as wireless mesh networks and DTNs rely on every node to provide packet forwarding services for normal operation. The lack of a central entity to supervise the activity of the nodes in these networks highlights the central role of collaboration in such environments. In many cases, the networks we are analyzing are composed of mobile, battery-powered devices. Therefore, a power-preserving strategy, sometimes combined with bandwidth constraints, may lead to denial of packet forwarding services for other nodes (*forwarding selfishness*). Therefore, nodes could depart from the established protocol in order to gain some advantages.

The initial research efforts, noticing the similarities with selfishness issues in P2P networks, have focused on reputation mechanisms [MGLB00, BB02b, BB02a], which unfortunately do not offer stability to the system and underline the difficulties of obtaining correct reputation information. It did not take long to realize that the addressed problem (forwarding selfishness in wireless networks) displays characteristics that are easily modeled by using game theory. Since mechanisms with money have been the main area of study for game theory research, they have been the most used theoretical tools for studying selfishness.

Following the idea of offering monetary (virtual currency) incentives to nodes in exchange for forwarding services, the literature has given a lot of attention to Vickrey-Clarke-Groves (VCG) mechanisms. Unlike the usual auctions, VCG auctions satisfy one major goal of mechanism design: they cannot be strategically manipulated by individual nodes. In [AE03] a way to adapt the VCG mechanism for the purpose mentioned above is presented. The idea of using VCG-style auctions has been extended in [ZLLY05], where routing and forwarding are regarded as subgames, thus acknowledging the fact that the two are inseparable from a game theoretical perspective. Following the same line, [LWX+08] adds a new layer by examining one of the fundamental challenges of decentralized wireless networks, namely the observability of nodes' actions and the availability of information necessary for selecting a specific strategy.

Recently, a number of authors have questioned the feasibility of implementing such a game theoretic incentive mechanism in the network. The problem stems from the fact that payment-based incentive mechanisms are impractical or extremely inefficient in large-scale distributed systems [MS09]. In addition, [MS09] also proposes a creditability mechanism in order to avoid making payments, at the cost of creating a central authority that should offer the proper payment promises.

Our approach to the selfishness problem draws on [BFH06], where the traffic flows and node forwarding services in static wireless mesh networks are modeled by dependency cycles. The conclusion is that in the absence of an incentive scheme, one cannot avoid situations where nodes *defect*; namely, they do not participate in forwarding since they do not see any advantage in doing so. Part of our work goes one step further in this direction. It seeks to characterize the traffic matrix requirements generating such a dependency graph that naturally induces good collaboration amongst network nodes.

We revisit the idea of using a form of barter or reciprocation by exploiting the dependencies between nodes or flows. In order to ease the examination of dependency relations in wireless mesh networks, we have made a number of assumptions regarding the topology and the traffic matrix. First of all, each node is assumed to be either a source or a destination of a single data flow, with the option of having also the role of relay on one or more routes. This way, the assumptions are largely simplified as the flow activity is considered to be synchronized and the dependencies between flows can be studied irrespective of time constraints.

¿From the connectivity graph and the route arrangements, a dependency graph can be derived, considering that both sources and destinations are dependent on all the relay nodes on their route. This has the meaning that relay nodes can ask for the same forwarding service in exchange from the sources and destinations of served flows, in any combination.

Under this particular assumptions, we seek to find the optimal route placement that will enable full collaboration, as well as the additional topological constraints that should be necessary. After this step, the problem is to be revisited while removing topological and time constraints and adapting the findings to the new assumptions.

The following work has been initiated by ETH Zurich:

1. *Examining the topological conditions for collaboration in wireless mesh networks – ongoing*

   The current work focuses on analyzing how the topology and the traffic matrix can influence the collaboration in decentralized networks. More precisely, the routes are considered to induce a dependency graph G_{dep} on top of the connectivity graph G. The collaboration condition between the nodes of this network is found to be the membership in strongly connected components of G_{dep} with no outgoing edges. Then, the collaboration is evaluated, considering that a relay node will forward data on a specific path if it collaborates with either the source or the destination of the flow. Preliminary results have been obtained for random graphs and for routes chosen to be shortest paths in terms of hop count. While this evaluation shows the number of multi-hop flows that are actually active is low, the cause has been identified to be intersection with one-hop flows, which will have to be avoided. The goal is to construct the proper optimization (under reasonable assumptions) that will give the flow assignment for the maximum possible collaboration degree. For the moment the issue is being examined under the assumption that a central entity is able to observe the network and communicate topology information to the nodes.

2. *Reciprocation protocol for wireless mesh networks – ongoing*

   We aim at creating a protocol building on game theoretic mechanisms that is able to take advantage of the dependencies that occur between nodes in a wireless mesh network. While it is not yet clear how to build it, the previous item should offer not only an upper bound on the performance that can be obtained, but also a good insight into

the problem. Ideally, this would offer a way to design an implementable, distributed selfish-thwarting mechanism.

The following collaboration opportunities will need to be evaluated:

- **With FT:** the use of MIP models is considered for optimally placing the routes in the described dependency graph model in order to obtain the highest collaboration and evaluating the imapact of selfishness in wireless networks;
- **With TU Delft:** elaboration of a game theoretic mechanism for overcoming (at least partially) the forwarding selfishness.

3.2 Optimization models for resilient network design

We are interested here in models and algorithmic approaches allowing the design of least cost telecommunication networks, with a special attention on resilience (the topology and the installed capacity are chosen to accommodate an reasonable set of potential challenges). By "design", we mean the choice of a suitable topology and the dimensioning of links and nodes. We will heavily rely on the well-known multi-commodity flow model: given a capacitated undirected graph $G = (V, E, C)$, where C_e is the capacity of edge $e \in E$ and a set of commodities $\{(s^k, t^k, d^k)\}_{k \in K}$, where s^k and t^k are the origin and destination nodes and d^k is the demand volume of commodity $k \in K$, a solution to the multicommodity flow problem is a set of paths containing at least one path for each commodity (i.e., joining the origin and the destination). We will call routing pattern and denote $\mathcal{R}$ such a solution. For such a routing pattern, denote by $F^k(\mathcal{R})$ the total amount of flow routed between s^k and t^k and by $F_e(\mathcal{R})$ the total resulting flow on each edge $e \in E$. A routing pattern $\mathcal{R}$ is said feasible if:

$$F^k(\mathcal{R}) \geq d^k, \quad k \in K, \tag{1}$$

$$F_e(\mathcal{R}) \leq C_e, \quad e \in E. \tag{2}$$

The *demand constraints* (1) impose that at least d^k unit of flow are routed on the paths joining s^k and t^k. The *capacity constraints* (2) guarantee that the flow on each edge $e \in E$ does not exceed the capacity of the edge.

Besides the underlying graph G itself, a multicommodity flow problem is essentially defined by the the demand vector $\{d^k\}_{k \in K}$ and the capacity vector $\{C_e\}_{e \in E}$. Assuming one set is fixed (as input data) and the second is variable or uncertain, we can distinguish two families of problems:

- **Network design problems** are problems where the demand is given and the network must be designed in a way that the demands can be routed in the graph.
- **Robust routing problems** are problems where the design is given (topology and capacities) and the commodities must be routed so that a set of different traffic demands can be routed in the graph.

The family of network design problems is a very broad family of graph problems that have been extensively studied with mathematical programming and combinatorial optimization tools. Note, that deciding the capacity vector implies two decisions that are sometimes considered separately: deciding on which edges non-zero capacities are installed is a *topological decision*

(which topology or sub-topology of G will be used), and deciding what are the values of the non zero capacities is a *dimensioning decision*. Problems where only the topological aspect is taken into account are sometimes described as *uncapacitated* since each time an edge is chosen, it is implicitly assumed to carry an infinite value capacity. Uncapacitated network design problems are hence mainly concerned with connectivity issues.

Network design problems where each edge (and in some cases, each node) can fail, are called **survivable network design problems** (SND). These problems have also been quite intensively studied over the past thirty years [OPTW07]. Uncapacitated SND problems are concerned with generalization of simple connectivity problems [GMS93] [KM05]. There is a wide variety of capacitated SND problems according to the choice of protection and/or rerouting strategy.

In the second family of problems, the capacities are given (and fixed) and the demand vector is variable. There are two motivations for such problems: (a) the case where the traffic demands vary dynamically over time and, (b) the case where the traffic demands are not known exactly (uncertain). Problems addressing case (a) are sometimes called multi-period or multi-hour network problems. Problems addressing case (b) belong to a broader family of optimization problems where some of the input data are uncertain. To model such uncertainties, the "traditional" approach was to rely on *stochastic programming* techniques [BL97]. Recently, alternative approaches have been proposed to capture uncertainties in input data with a significant improvement regarding the tractability of the resolution approaches. These approaches are known under the term *robust optimization* [KY97] [BS03] and some have already been applied to **robust network design problems** (RND).

Problems considering both the survivability of the design and robustness to face uncertainties in the demands have not yet been studied in depth. There is mainly a recent but nonetheless pioneering work in 2005 [AK05] and a few subsequent publications.

The main contribution of FT (Orange Labs) in this first deliverable is a state of the art trying to survey the most significant results concerning both survivable network design and robust network optimization (see appendix, paper not yet submitted).

The working plan for the future is to investigate network optimization problems where the design is both survivable to network failures and robust to demand uncertainties. More specifically, we plan to address the following issues:

- The objective of the *Maximum Concurrent Flow* problem (MCF) consists in maximizing the common share of all traffic demands that can be routed simultaneously in the network (while satisfying the capacity constraints) [SM91]:

  $$\max\{\lambda : \ F^k(\mathcal{R}) \geq \lambda d^k, F_e(\mathcal{R}) \leq C_e\}.$$

  As such, MCF naturally conveys some ideas of robustness: the same network can accommodate an increase of λ of all demands. Our intention is first to analyze the links between such problems with a sort of implicit robustness feature and the standard robustness optimization models. In particular, these assumptions should be translated into a probability distribution for the demand volumes. These observations and comparisons should also be extended to other robustness routing models, such as the *oblivious routing* model where the same routing scheme is applied to all possible demand scenarios [YAR04]. Other links can be established with previous routing models exhibiting some max-min fairness properties and which can be seen as a lexicographic MCF [DNL06].

- In a second line of research, we will address an extension of MCF where the network,

instead of being fixed and given as an input, as to be designed, for instance, with a limited budget constraint:

$$\max\{\lambda : \ F^k(\mathcal{R}) \geq \lambda d^k, F_e(\mathcal{R}) \leq C_e y_e, \sum_{e \in E} y_e \leq p\}.$$

3.3 Diversity in topology and end-to-end mechanisms

The work at KU directly relates to defensive measures in three areas. The work on diversity in end-to-end reliability mechanisms is the most mature and will be discussed first, followed by brief descriptions of the work in modeling realistic physical network topologies, and modeling geographic attacks and challenges.

3.3.1 End-to-end problem description

The ResumeNet resilience strategy involves taking defensive measures at every layer of the network stack. In the end-to-end context, this involves implementing diverse mechanisms to mitigate the effects of transport protocol data unit (TPDU) corruption and loss, and taking a context aware approach to making appropriate decisions about which mechanisms to enable in an adaptive manner. These requirements lead to a couple of broad questions which we seek to answer in our current research.

- What is the minimal set of operational modes that comprehensively addresses possible application requirements and network conditions?
- What are the set of mechanisms required to support each operational mode?

While investigating these questions, it becomes apparent that multipath mechanisms could yield greater benefits if incorporated in the end-to-end (transport) context, and not only on a hop-by-hop (forwarding) basis. It is also evident that there is much more research needed on the end-to-end multipath mechanism when compared with some of the other areas (e.g. ARQ and congestion avoidance) that have been more thoroughly explored in the past.

3.3.2 Research work and approach

Our current research has two main thrusts, first the identification and characterization of *multiple reliability modes*, and second *Path Diversification*, a heuristic approach to selecting multiple end-to-end paths for simultaneous or failover use. The precursor to identifying reliability modes is to enumerate the classes of traffic that should be given particular types of service.

Service types In the past the transport layer has had little instrumentation from the network and lower layers about path conditions. In this approach, we apply the principle of *translucency* [SH] by making key pieces of information upwardly visible from the network to allow the transport layer to make intelligent decisions about the E2E data transfer. In doing this we have several service types in mind, with the selection indicated by the active application:

- **Delay-bounded** data is that for which the utility curve as a function of latency decreases over a relatively short interval. An example of this is VoIP, in which the data is no longer

useful after more than a few hundred milliseconds. This kind of traffic requires a low-latency path with high reliability since retransmissions are not generally an option, but the data rate is often low enough to allow for some additional overhead in the form of FEC or erasure coding.

- **Bandwidth-inelastic** traffic has a primary requirement in terms of the peak and average data rate for the flow. A large file transfer is an example of this type of service requirement, and the transport protocol will send the data over a path composed of high-capacity uncongested links, aggregating bandwidth from multiple disjoint paths if possible. Due to the high data-rates involved, it may be preferable to correct errors via retransmission as opposed to incurring the overhead of FEC.
- **Best effort** service is for delay and bandwidth insensitive applications, such as email, in which the data should be delivered before the user gets impatient, but is not as time sensitive as a packetised telephone call. An important consideration for this type of communication is minimal resource usage at the end nodes since a server could be managing tens of thousands of connections at any given time. UDP [Pos80] is essentially designed to provide this kind of *best effort* service, but because it does not use cross-layer information, it cannot provide the application layer with any details about the service being provided, nor can it make intelligent decisions on how to deal with lost or delayed packets [FCG+06].

Reliability modes Based on the application requirements, there may be a number of data classes being transferred over the network. For this reason we define multiple *reliability modes* that are mapped from different service types and form the generic counterpart of the domain-specific reliability modes used in AeroTP [RPS08]. We call the generic protocol ResTP (Resilient Transport Protocol) and it assumes the presence of a thin internetworking layer (PoMo) [BCG+06]) also being developed by KU and partner institutions. The first two modes are connection-oriented, and the last two are connectionless:

- **Reliable** mode uses end-to-end acknowledgements from the destination to the source as the only way to *guarantee* delivery. This carries the penalty of requiring the end nodes to maintain state regarding each packet in flight over the entire E2E path, which can be substantial in high bandwidth-$\times$-delay product environments.
- **Near-reliable** mode is highly reliable, but does not *guarantee* delivery, instead using the custody transfer [SB07] approach, which splits the ACK loop at intermediate realms at the cost of buffering ResTP segments in each PoMo gateway until acknowledged by the next realm along the path. Since the gateway uses split ARQ and immediately returns TCP ACKs to the source, the assumption is that ResTPs reliable ARQ-based delivery will succeed using SNACKs (selective negative acknowledgements) [DMT96] supplemented by a limited number of (positive) ACKs. This can be more bandwidth-efficient than full source–destination reliability. However, the possibility exists of confirming delivery of data that the gateway cannot actually deliver to its final destination.
- **Quasi-reliable** mode uses only open-loop error recovery mechanisms such as FEC and erasure coding across multiple paths if available [McA90], thus eliminating ACKs and ARQ entirely. In this mode the strength of the coding can be tuned using cross-layer optimizations based on the quality of the channel being traversed, available bandwidth, and the application's sensitivity to data loss. This mode provides an arbitrary level of statistical reliability but without absolute delivery guarantees.

- **Unreliable** mode relies exclusively on the FEC of the link layer to preserve data integrity and does not use any error correction mechanism at the transport layer. Cross-layering is used to vary the link FEC strength.

The multipath mechanism may be useful in implementing any of the *reliability modes*, depending on the *service type* selected, and the graph of the underlying topology.

Path diversification The path diversification model is made up of several components. First we establish a quantitative measure of *path diversity*. We then use an exponential aggregator function to calculate the *effective path diversity*. Finally, we do the path selection itself, based on these values and a criterion derived from the service type being provided.

Path Diversity Since the primary motivation for implementing the path diversification mechanism is to increase resilience, paths should be chosen such that they will not experience correlated failures. To this end, we define a measure of diversity (originally introduced in [RNS09]) that quantifies the degree to which alternate paths share the same nodes and links. Note that in the WAN context in which we are concerned with events and connections on a large geographic scale, a node may be thought of as representing an entire POP, and a link as the physical bundle of fibers buried in a given right-of-way. This distinction between WAN and LAN component identifiers affects only the population of the path database, not the usage of the diversity metric.

Definition 1 (Path) *Given a (source, destination) node pair, a path P between them is a vector containing all links L and all intermediate nodes N traversed by that path, or*

$$P = L \cup N \tag{3}$$

and the length of this path, $|P|$ is the combined total number of elements in L and N.

Definition 2 (Path diversity) *Let the shortest path between a given (source, destination) pair be P_0. Then, for any other path P_k between the same source and destination, we define the diversity function $D(x)$ with respect to P_0 as:*

$$D(P_k) = 1 - \frac{|P_k \cap P_0|}{|P_0|} \tag{4}$$

The path diversity has a value of 1 if P_k and P_0 are completely disjoint and a value of 0 if P_k and P_0 are identical. For two arbitrary paths P_a and P_b the path diversity is given as:

$$D(P_b, P_a) = 1 - \frac{|P_b \cap P_a|}{|P_a|} \tag{5}$$

where $|P_a| \leq |P_b|$.

It has been claimed [MEFV08] that measuring diversity (referred to as novelty) with respect to *either* nodes *or* links is sufficient, however we assert that this is not the case. Figure 2 shows the shortest path, P_0, along with the alternate paths P_1 and P_2 both of which have a novelty of 1. However, given a failure on node 1, both P_0 and P_2 will fail. In our approach, $D(P_2) = \frac{2}{3}$, which reflects this vulnerability. P_1 on the other hand has both a novelty of 1 and a diversity of 1, and does not share any common point of failure with P_0. Similarly, the wavelengths or fibers from multiple nodes may in fact be spliced into a single physical link.

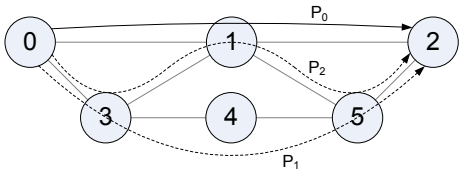


Figure 2: shortest path P_0 and alternatives P_1 and P_2

Effective path diversity Effective path diversity (EPD) is an aggregation of path diversities for a selected set of paths between a given node-pair (S,D). To calculate EPD we use an exponential function

$$\mathrm{EPD} = 1 - e^{-\lambda k_{sd}} \tag{6}$$

where k_{sd} is a measure of the added diversity defined as

$$k_{sd} = \sum_{i=1}^{k} D_{\min}(P_i) \tag{7}$$

where $D_{\min}(P_i)$ is the minimum diversity of path *i* when evaluated against all previously selected paths for that pair of nodes. λ is an experimentally determined constant that scales the impact of k_{sd} based on the utility of this added diversity. A high value of λ (> 1) indicates lower marginal utility for additional paths, while a low value of λ indicates a higher marginal utility for additional paths. Using EPD allows us both to bound the diversity measurement on the range [0,1) (an EPD of 1 would indicate an infinite diversity) and also reflect the decreasing marginal utility provided by additional paths in real networks. This property is based on the aggregate diversity of the paths connecting the two nodes.

Measuring graph diversity The total graph diversity (TGD) is simply the average of the EPD values of all node pairs within that graph. This allows us to quantify the diversity that can be achieved for a particular topology, not just for a particular flow. For example, a star topology will always have a TGD of 0, while a ring topology will have a TGD of 0.6 given a λ of 1.

Path selection In this section we use three different modes for choosing a set of diverse paths for a given node pair: number of paths, diversity threshold, and stretch limit. The objective in the first mode is to find k maximally diverse paths. We first find the shortest fully disjoint paths, and, if additional paths are required, we continue finding paths that add maximum diversity as calculated using equation 7. The second mode selects as many maximally diverse paths as are required to achieve the desired EPD. Finally, the third mode selects all maximally diverse paths with stretch less than the stretch limit. In all modes, the set of maximally diverse paths are found using the Floyd-Warshall algorithm with modified edge weights [Bha98]. In this algorithm, only those paths are used which increase the EPD for the node pair in question. Recall that only paths with one or more disjoint elements (links, nodes) will result in non-zero $D_{\min}$ and consequently increase EPD.

3.3.3 Modeling Physical Network Topologies

Realistic topology generators are crucial to numerous aspects of networking research. In particular, there are three distinct applications of topology generators: understanding the graphical properties of the network and evaluating the performance of protocols and services over a given topology; resilience and survivability analysis of the network to determine how well the network will react to challenges; and finally, a tool for network architects, providing alternate topologies that meet certain constraints during the design and engineering phase. It should be noted that research in the past has rigorously studied the first application by modeling the graphical properties of the network and to some extent have addressed the survivability issues. However the existing research focuses on independent single link failures as opposed to geographically correlated link failures. Finally, to our knowledge there is very little effort on the third application - development of a practical tool to be used in the network design process.

Two important issues that are not sufficiently addressed by current topology generators are node-positioning and cost considerations. The utility of the existing models could be vastly improved by incorporating these two features. This project aims at developing a new network topology generator, which enables node positioning and cost constraints on the topologies generated with several well-known graph generation models. Our approach incorporates network design practices in topology generation, thereby enabling a tool that can be used to generate viable alternate topologies during the network design and engineering phase. Further, we consider the representativeness of the generated topologies using several graphical properties such as degree distribution, shortest path distribution, link length distribution, and spectrum of the graph amongst several others.

3.3.4 Modeling Network Attacks and Challenges

An essential aspect to the evaluation of network resilience and design of resilient networks is to understand how various architectures, designs, and protocols respond to challenges. These challenges to normal operation include: unintentional misconfiguration or operational mistakes, large scale natural disasters, attacks from an intelligent adversary, environmental challenges, unusual but legitimate traffic, service failure at a lower level.

In order to simulate a wide variety of challenges, complex simulation scripts are needed that model both the network topology, protocols, as well as the challenges. Challenge simulation requires manual and careful modification of the simulation script, for example by disabling links and nodes for the duration of the challenge. For c challenges to n networks this requires c?n simulation files. We are looking at a new approach that decouples the network model from the challenge description, resulting in c challenge descriptions applied to n networks, for a total of c+n input files, thus increased efficiency of simulation generation. This is accomplished by feeding network topology (via an adjacency matrix) and geographical coordinates of nodes to C++ based ns-3 simulation script. The network topology file that is fed to the simulation model can be organic or synthetically generated via KU-LoCGen.

Publications The work published along this line of research includes:

- Justin P. Rohrer, Abdul Jabbar and James P.G. Sterbenz, "Path Diversification: A Multipath Resilience Mechanism", The 7th IEEE International Workshop on the Design of Reliable Communication Networks (DRCN) 2009, Washington, DC October 2009.

- Justin P. Rohrer, Ramya Naidu and James P.G. Sterbenz, "Multipath at the Transport Layer: An End-to-End Resilience Mechanism", International Workshop on Reliable Networks Design and Modeling (RNDM) 2009, St. Petersburg, Russia, October 2009.
- Justin P. Rohrer and James P.G. Sterbenz, Performance and "Disruption Tolerance of Transport Protocols for Airborne Telemetry Networks", International Telemetering Conference (ITC) 2009, Las Vegas, NV October 2009 (to appear).
- Justin P. Rohrer, Abdul Jabbar, Erik Perrins, and James P.G. Sterbenz, "Cross-Layer Architectural Framework for Highly-Mobile Multihop Airborne Telemetry Networks", Proceedings of IEEE Military Communications Conference (MILCOM'08), San Diego, November 2008.
- Justin P. Rohrer, Erik Perrins, and James P.G. Sterbenz, "End-to-End Disruption-Tolerant Transport Protocol Issues and Design for Airborne Telemetry Networks", International Telemetering Conference (ITC) 2008, San Diego, October 2008.

Publications currently under review include:

- Abdul Jabbar, Egemen K. Cetinkaya, Qian Shi, and James P.G. Sterbenz, "Towards Modeling Physical Network Topologies: Challenges and Principles", SIGCOMM Computer Communications Review (CCR), ACM.
- Egemen K. Cetinkaya, Abdul Jabbar, Rabat Mahmood, James P. G. Sterbenz, "Modelling Network Attacks and Challenges: A Simulation-based Approach", Eighth European Dependable Computing Conference (EDCC), Valencia, Spain, April 28-30, 2010.

3.3.5 Work plan for the next 6 months

Over the course of the following six months, the following tasks will be carried out.

- Determine specifications for cross-layering communication and header fields used between ResTP and PoMo.
- Implement a model of the ResTP protocol in the ns-3 simulation environment.

3.4 QoS^2: Integrating QoS with Quality of Security

3.4.1 Research Background & Motivation

Protection mechanisms obviously belong to the set of defensive measures that should be deployed in a network, but, at the same time, they should be tuned in such a way to preserve a sufficient level of performance. The rational behind the work we intend carrying out in this specific task, stems from the observations we have made in some of our previous research work, pertaining to detection of Internet worms in large scale network [STW$^+$09] and detection and trace back of sophisticated attacks using encryption protocols. The observations indicated that the adopted level of security has an important impact on the overall QoS of the network [FTV$^+$].

In [STW$^+$09], a two-layer hierarchical worm detection architecture is envisioned. The network topology is divided into a number of metropolitan areas; each is administrated by a

metropolitan security manager (MSM) and consists of a number of local networks, managed by their respective local security managers (LSMs). A global security manager controls the whole network and directly communicates with MSMs. LSMs search for any worm-like or suspicious e-mails propagating in their networks, and report such emails to their corresponding metropolitan managers. A MSM uses cluster analysis to sort worms out of the suspicious contents transmitted by its local managers. The MSM then automatically generates signature from the sorted worms and sends the generated signature to the GSM. Upon receiving signatures from MSMs, the GSM relays the generated signature to all local networks via MSMs. Whilst for signature generation, LSMs and MSMs need only to sniff inbound and outbound traffic, for the detection of worms, they need to carefully filter each inbound and outbound flow. Conducting a number of simulations using real-life network traces, the general observation we made, is that the longer the generated signature is, the more accurate the detection is, however the longer the end-to-end delay becomes. This clearly, and sometime significantly, impacts the overall Quality of Experience (QoE) of users.

In [FTV$^+$], we devised an Intrusion Detection System (IDS) capable of detecting attacks against cryptographic protocols. The devised IDS uses strategically distributed Monitoring Stubs (MSs) that sniff the encrypted traffic, extract features for detecting these attacks and construct normal usage behavior profiles. Upon detecting suspicious activities due to the deviations from these normal profiles, the MSs notify the victim servers, which may then take necessary actions. Depending on the detected attack, such actions may introduce additional delays to the end-to-end delay to disable attackers from making accurate estimates of the processing time required for the decryption of a particular key (e.g., remote time attack). Such actions may also involve a random discarding of packets (e.g., password attack). All in all, such counter measures may have side impact on the overall QoS of the system. It is thus imperative to deploy security requirements along with their QoS counterparts.

A leading illustration of how security may be integrated as a dimension to existing QoS frameworks can be found in the middleware adaptation proposed in [HN06]. The users of IEEE 802.11-based wireless ad-hoc networks are presented with a set of security requirements and end-to-end QoS delay requirements. Depending on a user's chosen level of security and delay requirements, the middleware adaptor attempts to attain the minimum end-to-end delay while offering the user the highest possible security level, which is proportional to the encryption key-length. Thus, it achieves a balance between delay and security levels under varying network loads. Although this tunable QoS/QoP framework for QoS delay and security requirements serves as a pioneering work, it is not without its shortcomings. Especially, a bandwidth consuming attack may exploit the manner in which the encryption key-lengths are downgraded dynamically to maintain a reasonable end-to-end delay requirement for the user. The attacker may then launch remote timing like attacks more effectively and quickly owing to the weakened encryption level. In our work [FTN$^+$09], we illustrated the significance of the problem of dynamically adjusting the lengths of the encryption keys with varying end-to-end delays.

3.4.2 Research Objectives

As a continuation to the work presented in [FTN$^+$09], where the problem of security impact on QoS is stated, the objective of our research work is to design an "agile" framework that ensures high protection for the network from malicious usage and attacks. However, in the absence of a potential threat, the framework, in an autonomic way, relaxes the system's overall security requirements in case the required QoS are not met under the current security settings. The

basic concept of the framework is depicted in Fig. 3. The figure shows a "network security advisory system" with a number of threat levels ranging from low to severe. The security advisory system defines the threat level of the network based on the events reported by IDSs and/or other entities, such as firewalls and IDSs of other collaborating networks. It analyzes the events in specific timeslots and constantly updates the threat level. For each threat level and each associated security level, a particular defensive measure can be applied. Threat level one (i.e., low) corresponds to a normal network state when no malicious activities are reported. In contract, threat level "severe" implies that the system is either under potential attack or is in a grave danger of encountering a particular attack. The threat level of a given timeslots may be decided by considering, for example, *i)* the total number of events observed in the timeslot with respect to a pre-defined event threshold, and *ii)* the increasing or decreasing tendency of the number of events with respect to previous timeslots. Based on the alert level indicated by the security advisory system, we are interested in devising a security / QoS policy control that indicates the security level that should correspond to a desired QoS level. When under the indicated threat level, the security advisory system recommends a range of security levels (e.g., range of encryption/decryption key lengths, anomaly detection score, worm signature lengths, etc), we are interested in finding out the highest security level that should be selected in a way that the QoS requirements of users are not compromised. If for a particular security level from within the recommended range, the QoS requirements of users can not be satisfied (i.e., this can be inferred from a learning phase), the security / QoS policy control unit asks for security relaxation. It should be noted here that if the network is under potential attack and the security advisory system recommends the highest security level, the system has to stick to the recommended level although this decision may compromise the required QoS. QoS relaxation becomes thus mandatory and that is using different mechanisms

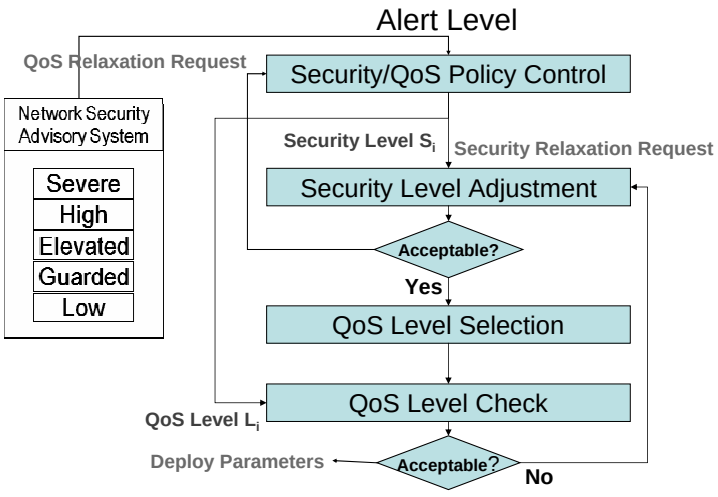


Figure 3: Basic concept of the intended research work.

3.4.3 Problem Formulation

The problem can be formulated as follows. We assume there is a number M of QoS parameters (e.g., bandwidth, delay, packet drops, fairness, etc). Intuitively, the set of envisaged QoS parameters depends on the type of the considered application and/or traffic. For each particular security defensive measure F, there is also a number N_f of security levels, each characterized by R different metrics (e.g., encryption/decryption key length, anomaly detection score, worm signature generation, etc). Additionally, there are also P QoS satisfaction levels, each characterized by a value (or a range of values) for each of the M QoS parameters. For example, QoS satisfaction level X can be defined as such when users experience an end-to-end delay less or equal to D_x and the guaranteed bandwidth is larger or equal to BW_x. The matching of each QoS satisfaction level with the values of its corresponding QoS metrics can be done during an initial learning phase and can be constantly updated during the service course time of the network. The network operator also relates each security defensive measure (e.g., encryption/decryption mechanism) with a given granularity defining the security level (e.g., encryption key length) with a list of values of corresponding QoS parameters (e.g., delay, bandwidth) that may be experienced by users when the security defensive measure is applied using the same granularity.

The objective of our work is to minimize the distance between the performance vector composed of normalized measured QoS when a security defensive measure is applied with adjustable security metrics, and the ideal values of the same normalized QoS metrics (e.g., minimum loss rate, E2E delay, maximum throughput, etc) that characterizes the desired QoS satisfaction level. This optimization can be achieved by selecting the best possible security level characterized by adequate security metrics. In the event that the security advisory system does not tolerate any further relaxation of the security level, relaxation of QoS requirements may be requested. This QoS relaxation certainly should be carried out while ensuring an acceptable satisfaction level to users. Regarding this point, we will be particularly addressing "adaptive real time" traffic where relaxation of QoS requirements is possible. Note that in case of hard real time traffic such relaxation is not permissible and that there are no strong QoS requirements in case of non-real time traffic.

3.4.4 Conclusion and future work

To reiterate, the objectives of our work are to explore inter-correlation between QoS and Security requirements and to envision a framework that efficiently integrates the two. For this purpose, we intend to conduct research following these three steps.

- Investigate further about correlation between QoS and security parameters and that is per application and traffic type.
- Find adequate "multi-objective utility" functions to formulate QoS level and security level using different QoS metrics and security parameters, respectively.
- Incorporate Multi-Attribute Decision Making (MADM) concept in the QoS/security level selection procedure and define an Adaptive Decision Making Mechanism that retrieves the best possible security level to ensure the best possible QoS when the network is applying a particular security defensive measure against a particular event.

3.5 Protection against malicious information spread

Each system in a network, prone to various types of challenging situations, needs apart from detection also protection mechanisms. Tasks 2.1.3 aims to determine the level of protection in each system in the network against malicious attacks or any type of epidemic spreading. Given a certain network topology and the strength of the malicious spread, we determine at each node the level of protection (e.g. the required level of efficiency of anti-virus software) in order to prevent further spread of the malicious attacks.

The problem consists of two main aspects: the epidemic spreading on a network and optimization/game theoretical problem of protection distribution. While extensive studies have been done on spreading processes in networks, its optimization/game theoretic perspectives has hardly been considered. Epidemics on computer networks were studied in [AJB00], [KW91], [PSV01] and [WCF$^+$03]. The SIS (Susceptible Infected Susceptible) model and the influence of the topology on the spreading process were extensively studied in [GMT05], [GG03], [CEM05] and [Asa00].

Network security under a game theoretical setting was considered in [ACY06]. That study addressed the interplay between protection and infection and noted the influence of the underlying topology. However, it focused on the case of just two simple strategies, namely being fully protected or totally unprotected. In particular, if a node chooses the fully protected strategy, its security level does not depend on that of its neighbors. A framework that is closer to the present study is that of IDS (Interdependent security games) [KH03], [KO03]. As opposed to [ACY06], in IDS games security levels of agents are interdependent even when they choose the protected strategy. However, the IDS framework does not consider the influence of the underlying topology, as it restricts its attention to the case of a complete graph.

Global optimization of network protection was studied in [BCGS09], but the discussion was limited to the epidemic threshold. For effective spreading rates below the epidemic threshold, the virus contamination in the network dies out - the mean epidemic lifetime is of order $O(log(N))$, where N is the size of the network. For effective spreading rate above the epidemic threshold, the virus is prevalent, i.e. a persisting fraction of nodes remains infected with the mean epidemic lifetime [GMT05] of the order $O(e^{N^\alpha})$, where α is a positive constant.

We shall employ the N-intertwined model, proposed and studied in [MOK09], to model the spreading process. The N-intertwined epidemic model takes into account the topology of the relation network. Each host stores IP addresses, e-mail accounts and passwords of other hosts and systems. This stored information defines a relation between hosts. If a host is compromised, then all reachable hosts can be attacked. The relation network is an abstraction that determines the hosts that can be infected. The relation topology is a significant aspect of the spreading process [GMT05], [PSV01], [WCF$^+$03]. For given curing strategies of the individual nodes, it is possible to calculate the probability of infection and the average infection time for individual nodes [MOK09].

The following work has been done at Delft University of Technology:

1. *Design and study of the homogeneous N-intertwined model which captures the influence of the network structure on the spreading process. [MOK09] - published*

   The influence of the network characteristics on the virus spread is analyzed in a new – the N-intertwined Markov chain – model, whose only approximation lies in the application of mean field theory. The mean field approximation is quantified in detail. The N-intertwined model has been compared with the exact 2^N-state Markov model and with

previously proposed "homogeneous" or "local" models. The sharp epidemic threshold τ_c, which is a consequence of mean field theory, is rigorously shown to be equal to $\tau_c = \frac{1}{\lambda_{\max}(A)}$, where $\lambda_{\max}(A)$ is the largest eigenvalue – the spectral radius – of the adjacency matrix A. A continued fraction expansion of the steady-state infection probability at node j is presented as well as several upperbounds.

2. *Extend the model to heterogeneous virus spread in networks - general topology. [MO08] - published*

   Our N-intertwined model [MOK09] for virusspread in any network with N nodes is extended to a full heterogeneous setting. The metastable steady-state nodal infection probabilities are specified in terms of a generalized Laplacian, that possesses analogous properties as the classical Laplacian in graph theory. The critical threshold that separates global network infection from global network health is characterized via an N dimensional vector that makes the largest eigenvalue of a modified adjacency matrix equal to unity. Finally, the steady-state infection probability of node i is convex in the own curing rate δ_i, but concave in the curing rates δ_j of the other nodes $1 \leq j \neq i \leq N$ in the network.

3. *Apply the extended model of heterogeneous virus spread in networks to regular and bipartite graphs - optimization problem. [OKM09] - published*

   We examine the influence of heterogeneous curing rates for a SIS model, used for malware spreading on the Internet, information dissemination in unreliable networks, and propagation of failures in networks. The topology structures considered are the regular graph which represents the homogeneous network structures and the complete bi-partite graph which represents the hierarchical network structures. We find the threshold in a regular graph with m different curing rates.

   Further, we consider a complete bi-partite graph with 2 curing rates and find the threshold for any distribution of curing rates among nodes. In addition, we consider the optimization problem and show that the minimum sum of the curing rates that satisfies the threshold equation is equal to the number of links in the graph. The optimization problem is simplified by assuming fixed curing rates δ_1, δ_2 and optimization of the distribution of curing rates among different sets of nodes.

4. *Study how the game theoretical approach can be used in order to model the influence of topological characteristics of the underlying structure in the case of Internet security problems. [OOM09] - published*

   Security breaches and attacks are critical problems in today's networking. A key-point is that the security of each host depends not only on the protection strategies it chooses to adopt but also on those chosen by other hosts in the network. The spread of Internet worms and viruses is only one example. This class of problems has two aspects. First, it deals with epidemic processes, and as such calls for the employment of epidemic theory. Second, the distributed and autonomous nature of decision-making in major classes of networks (e.g., P2P, ad-hoc, and most notably the Internet) call for the employment of game theoretical approaches. Accordingly, we propose a unified framework that combines the N-intertwined, SIS epidemic model with a noncooperative game model.

   We determine the existence of a Nash equilibrium of the respective game and characterize its properties. We show that its quality, in terms of overall network security, largely depends on the underlying topology. We then provide a bound on the level of system inefficiency due to the noncooperative behavior, namely, the "price of anarchy" of the

game. We observe that the price of anarchy may be prohibitively high, hence we propose a scheme for steering users towards socially efficient behavior.

The following activities are initiated at Delft University of Technology:

1. *Optimization of Network Protection. [OGKM09] - not published*

   In todays networks, each system (node) in the network has different protection mechanisms (antivirus software, firewall). The level of node security influences neighbors - nodes that can be attacked using information from the compromised node. All the nodes in the network form global network security. We are interested into optimizing overall security by strategic distribution of protection among individual systems. We have found that the optimization problem is of sum of ratios functional programming type. We have also concluded that protection proportional to the node degree in the case where network is not fully protected - above the threshold - is not the optimal. Further work will concentrate on finding bounds on the optimal solution and optimization for some specific networks.

2. *Application: Malware Spread in Social Networks*

   Typically, a virus or malware that requires user interaction to infect a computer or network component is more successful when it can exploit social information about the victim, e.g., one is more likely to click on an attachment if the sender is known by the targeted receiver. For this reason, the recently emerged social media platforms such as Facebook, LinkedIn, or myspace are very valuable for attackers as they provide information about the user's social environment openly, and with the introduction of user-uploaded web-applications therefore become a source for highly viral worms. We will therefore investigate the mechanics and dynamics of social networks as possible spreading ground for malware.

3.6 Future work and integration activities

Elements of the future work plan have been sketched within each research topic. Several additional convergence areas have also been clearly identified and some problems, among the ones listed below, will be addressed with combined tools and complementary skills:

- **ETHZ with FT:** the use of MIP models is considered for optimally placing the routes in the described dependency graph model in order to obtain the highest collaboration and evaluate the impact of selfishness in wireless networks.
- **ETHZ with TUDelft:** elaboration of a game theoretic mechanism for overcoming (at least partially) the forwarding selfishness.
- **FT with TUDelft**: use Mixed Integer Programming (MIP) models to solve as efficiently as possible some graph problems such as cuts. The impact of node degree constraints coming from virus spreading analysis could also be integrated in network design models.
- **FT with NEC**: use bi-criteria optimization tools to solve and evaluate network design problems driven by two contradictory objectives, namely, the cost on one side, and the efficiency, or QoS, on the other side.

4 Conclusions

Although this is the first deliverable on defensive measures for resilient networks, there are already several important results available:

- A framework for studying collaboration of individual nodes with a tendency to act selfishly.
- A survey of models and methods for survivable and robust networks design problems arising as optimization problems.
- A set of efficient mechanisms to enforce network resilience using path diversity.
- An efficient mechanism to fight against attacks using encrypted protocols.
- Homogeneous and heterogeneous models for virus spreading in bipartite, regular graphs and general networks.
- Game theoretical approaches to assess optimal anti-virus deployment strategies.

There are several more or less obvious ways to combine these results in order to broaden the scope of problems addressed within this task. One obvious way consists in combining some approaches within a cyclic framework: approach A uses the data x^k and provides a solution y^k, then approach B uses y^k as an input and provides a solution x^{k+1}. Figure 4 shows some of such obvious collaboration cycles.

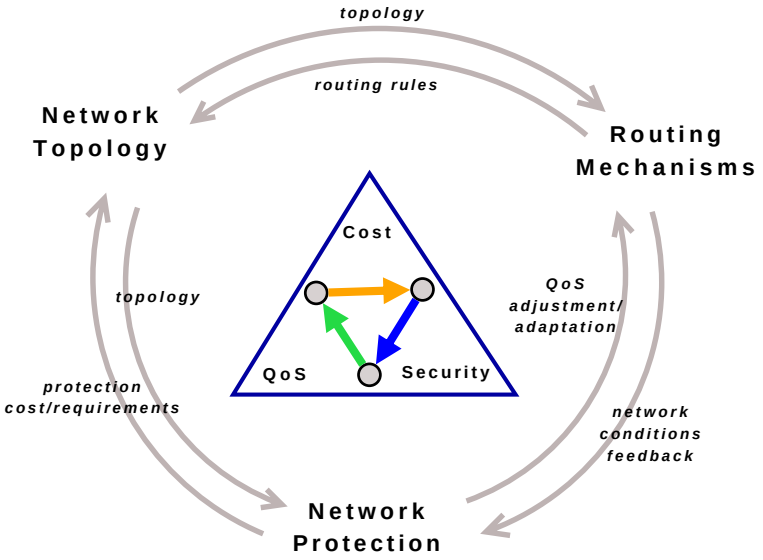


Figure 4: Potential exchanges of data between the three main network components

It is however hopeless to think all bricks could be combined together to solve the "big picture". There are several reasons for that, a major one being the intractability of large scope problems. Another reason is that, in the real world, problems very often occur at different levels and at different time scales. It is hence very reasonable to consider providing a set of models, methods and tools to cover a variety of more specific problems. In summary, these are the topics addressed by Task 2.1. The final deliverable will offer a complete image of the proposed defensive measures.

Appendix: **list of publications**

- Topological conditions for collaboration in wireless mesh network:
  - "Topological conditions for collaboration in wireless mesh networks", G.G. Popa, technical report ETH Zürich, Nov. 2009
- Optimization models for resilient network design:
  - "A quick overview of optimization models for the design of resilient networks", E. Gourdin, technical report Orange Labs, Nov. 2009
- Diversity in topology and end-to-end mechanisms:
  - "Towards Modeling Physical Network Topologies: Challenges and Principles", A. Jabbar, E.K. Cetinkaya, Q. Shi, J.P.G. Sterbenz, SIGCOMM Computer Communications Review (CCR), ACM.
  - "Modelling Network Attacks and Challenges: A Simulation-based Approach", E.K. Cetinkaya, A. Jabbar, R. Mahmood, J.P.G. Sterbenz, Eighth European Dependable Computing Conference (EDCC), Valencia, Spain, April 28-30, 2010.
- QoS^2: Integrating QoS with Quality of Security:
  - "DTRAB: combating against attacks on encrypted protocols through traffic-feature analysis", Z.M. Fadlullah, T. Taleb, A. Vasilakos, M. Guizani, N. Kato, submitted to IEEE/ACM Transactions on Networking
  - "Exploring the security requirements for quality of service in combined wired and wireless networks", Z.M. Fadlullah, T. Taleb, N. Nasser, N. Kato, IWCMC'09
  - "A connection stability aware handoff management scheme", T. Taleb, Z.M. Fadlullah, M. Schöller, K. Ben Letaief, 2009 IEEE Intern. Conf. on Wireless and Mobile Computing, Networking and Communications
- Protection against malicious information spread:
  - "Virus spread in networks", P. Van Mieghem, J. Omic, R.E. Kooij, IEEE/ACM Trans. Netw., Vol. 17(1), pp. 1-14, 2009
  - "In-homogeneous Virus spread in Networks", P. Van Mieghem, J. Omic, Technical report 20080801, TUDelft, 2008
  - "Protecting Against Network Infections: A Game Theoretic Perspective", J. Omic, A. Orda, P. Van Mieghem, Proceedings of IEEE INFOCOM 2009
  - "Heterogeneous Protection in Regular and Complete Bi-partite Networks", J. Omic, R.E. Kooij, P. Van Mieghem, NETWORKING '09: Proceedings of the 8th International IFIP-TC 6 Networking Conference, pp. 92–103]

References

[ACY06] J. Aspnes, K. Chang, and A. Yampolskiy. Inoculation strategies for victims of viruses and the sum-of-squares partition problem. *jcss*, 72(6):1077–1093, sep 2006.

[AE03] L. Anderegg and S. Eidenbenz. Ad hoc-vcg: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. In *MobiCom '03: Proceedings of the 9th annual international conference on Mobile computing and networking*, pages 245–259, New York, NY, USA, 2003. ACM.

[AJB00] R. Albert, H. Jeong, and A.-L. Barabasi. Error and attack tolerance of complex networks. *Nature*, 406:378, 2000.

[AK05] W. Ben Ameur and H. Kerivin. Routing of uncertain demands. *Optimization and Engineering*, 6(3):283–313, 2005.

[Asa00] C. Asavathiratham. The influence model: A tractable representation for the dynamics of networked markov chains. Technical report, in Dept. of EECS. 2000, 2000.

[BB02a] S. Buchegger and J.-Y. Le Boudec. Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks. In *Tenth Euromicro PDP (Parallel, Distributed and Network-based Processing)*, pages 403 – 410, 2002.

[BB02b] S. Buchegger and J.-Y. Le Boudec. Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks). In *MobiHoc 2002*, 2002.

[BCG+06] B. Bhattacharjee, K. Calvert, J. Griffioen, N. Spring, and J. Sterbenz. Postmodern internetwork architecture. Technical Report ITTC-FY2006-TR-45030-01, Information and Telecommunication Center, 2335 Irving Hill Road, Lawrence, KS 66045-7612, February 2006.

[BCGS09] C. Borgs, J. Chayes, A. Ganesh, and A. Saberi. How to distribute antidote to control epidemics. 2009.

[BFH06] L. Buttyan, M. Felegyhazi, and J.-P. Hubaux. Nash equilibria of packet forwarding strategies in wireless ad hoc networks. *IEEE Transactions on Mobile Computing*, 5(5):463–476, 2006.

[Bha98] R. Bhandari. *Survivable Networks: Algorithms for Diverse Routing*. Kluwer Academic Publishers, Norwell, MA, USA, 1998.

[BL97] J.R. Birge and F. Louveaux. *Introduction to Stochastic Programming*. Springer-Verlag, 1997.

[BS03] D. Bertsimas and M. Sim. Robust discrete optimization and network flows. *Mathematical Programming*, 98:49–71, 2003.

[CEM05] G. Canright and K. Engoe-Monsen. Spreading on networks: a topographic view. In *Proceedings of the European Conference on Complex Systems*, nov 2005.

[DMT96] R. C. Durst, G. J. Miller, and E. J. Travis. TCP extensions for space communications. In *Proc. ACM MOBICOM '96*, pages 15–26, New York, NY, USA, November 1996. ACM Press.

[DNL06] E. Gourdin D. Nace, H.-L. Doan and B. Liau. Computing optimal max-min fair resource allocation for elastic flows. *IEEE/ACM Transaction on Networking*, 14(6):1272–1281, 2006.

[FCG+06] S. Farrell, V. Cahill, D. Geraghty, I. Humphreys, and P. McDonald. When TCP breaks: Delay- and disruption- tolerant networking. *IEEE Internet Computing*, 10(4):72–78, July-Aug. 2006.

[FTN+09] Z. Fadlullah, T. Taleb, N. Nasser, N., and Kato. Exploring the security requirements for quality of service in combined wired and wireless networks. In *Proc. ACM IWCMC '09*, Leipzig, Germany, June 2009.

[FTV+] Z. Fadlullah, T. Taleb, A. Vasilakos, M. Guizani, N., and Kato. DTRAB: Combating Against Attacks on Encrypted Protocols through Traffic-Feature Analysis. *in ACM/IEEE Transactions on Networking. (currently under submission)*, –.

[GG03] M. Garetto and W. Gong. Modeling malware spreading dynamics. In *In Proceedings of IEEE INFOCOM*, pages 1869–1879, 2003.

[GMS93] M. Grötschel, C. Monma, and M. Stoer. *Design of Survivable Networks*, volume Networks of *Handbooks in Operations Research and Management Science*, chapter 10, pages 617–672. North-Holland, Amsterdam, 1993.

[GMT05] A.J. Ganesh, L. Massouli, and D.F. Towsley. The effect of network topology on the spread of epidemics. In *INFOCOM*, pages 1455–1466. IEEE, 2005.

[HN06] W. He and K. Nahrstedt. An integrated solution to delay and security support in wireless networks. In *Proc. IEEE WCMC '06*, Las Vegas, USA, April 2006.

[KH03] H. Kunreuther and G. Heal. Interdependent security. *Journal of Risk and Uncertainty*, 26(2-3):231–49, March-May 2003.

[KM05] H. Kerivin and A. Mahjoub. Design of survivable networks: A survey. *Networks*, 46(1):1–21, 2005.

[KO03] M.J. Kearns and L.E. Ortiz. Algorithms for interdependent security games. In *NIPS*, 2003.

[KW91] J.O. Kephart and S.R. White. Directed-graph epidemiological models of computer viruses. *Security and Privacy, IEEE Symposium on*, 0:343, 1991.

[KY97] P. Kouvelis and G. Yu. *Robust discrete optimization and its applications*. Kluwer Academic Publishers, 1997.

[LWX+08] X.-Y. Li, Y.W. Wu, P. Xu, G.H. Chen, and M. Li. Hidden information and actions in multi-hop wireless ad hoc networks. In *MobiHoc '08: Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing*, pages 283–292, New York, NY, USA, 2008. ACM.

[McA90] A. J. McAuley. Reliable Broadband Communication Using a Burst Erasure Correcting Code. *SIGCOMM Computer Communications Review*, 20(4):297–306, 1990.

[MEFV08] M. Motiwala, M. Elmore, N. Feamster, and S. Vempala. Path splicing. In *Proc. ACM SIGCOMM '08*, pages 27–38, New York, NY, USA, August 17-22 2008. ACM.

[MGLB00] S. Marti, T.J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 255–265, New York, NY, USA, 2000. ACM.

[MO08] P. Van Mieghem and J. Omic. In-homogeneous virus spread in networks. Technical report, Technical report 20080801, TUDelft, 2008.

[MOK09] P. Van Mieghem, J. Omic, and R.E. Kooij. Virus spread in networks. *IEEE/ACM Trans. Netw.*, 17(1):1–14, 2009.

[MS09] T. Moscibroda and S. Schmid. On mechanism design without payments for throughput maximization. In *INFOCOM 2009. The 28th Conference on Computer Communications. IEEE*, pages 972–980, April 2009.

[OGKM09] J. Omic, A.J. Ganesh, R.E. Kooij, and P. Van Mieghem. Optimization of network protection. Technical report, On going work, TUDelft, 2009.

[OKM09] J. Omic, R.E. Kooij, and P. Van Mieghem. Heterogeneous protection in regular and complete bi-partite networks. In *NETWORKING '09: Proceedings of the 8th International IFIP-TC 6 Networking Conference*, pages 92–103, Berlin, Heidelberg, 2009. Springer-Verlag.

[OOM09] J. Omic, A. Orda, and P. Van Mieghem. Protecting against network infections: A game theoretic perspective. In *Proceedings of IEEE INFOCOM*, 2009.

[OPTW07] S. Orlowski, M. Pióro, A. Tomaszewski, and R. Wessäly. SNDlib 1.0–Survivable Network Design Library. In *Proceedings of the 3rd International Network Optimization Conference (INOC 2007), Spa, Belgium*, April 2007. http://sndlib.zib.de.

[Pos80] J. Postel. User Datagram Protocol. RFC 768 (Standard), August 1980.

[PSV01] R. Pastor-Satorras and A. Vespignani. Epidemic spreading in scale-free networks. *Phys Rev Lett*, 86(14):3200–3203, January 2001.

[RNS09] J. P. Rohrer, R. Naidu, and J. P.G. Sterbenz. Multipath at the transport layer: An End-to-End resilience mechanism. In *RNDM'09 - International Workshop on Reliable Networks Design and Modeling*, St. Petersburg, Russia, October 2009. to appear.

[RPS08] J. P. Rohrer, E. Perrins, and J. P. G. Sterbenz. End-to-end disruption-tolerant transport protocol issues and design for airborne telemetry networks. In *Proc. International Telemetering Conference*, San Diego, CA, October 27–30 2008.

[SB07] K. Scott and S. Burleigh. Bundle Protocol Specification. RFC 5050 (Experimental), November 2007.

[SH] J. P. G. Sterbenz and D. Hutchison. Resilinets: Multilevel resilient and survivable networking initiative wiki (http://wiki.ittc.ku.edu/resilinets).

[SM91] F. Shahrokhi and D.W. Matula. On solving large maximum concurrent flow problems. *Journal of the ACM*, 37:318–334, 1991.

[STW+09] K. Simkhada, T. Taleb, Y. Waizumi, A. Jamalipour, Y., and Nemoto. Combating against Internet worms in large-scale networks: an autonomic signature-based solution. *Wiley InterScience Journal on Security and Communication Networks, Vol. 2, No. 1, pp. 11-28*, Jan/Feb. 2009.

[WCF+03] Y. Wang, D. Chakrabarti, C. Faloutsos, C. Wang, and C. Wang. Epidemic spreading in real networks: An eigenvalue viewpoint. In *In SRDS*, pages 25–34, 2003.

[YAR04] A. Fiat H. Kaplan Y. Azar, E. Cohen and H. Räcke. Optimal oblivious routing in polynomial time. *J. Comput. Syst. Sci.*, 69:383–394, 2004.

[ZLLY05] S. Zhong, L.(E.) Li, Y. G. Liu, and Y.R. Yang. On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks: an integrated approach using game theoretical and cryptographic techniques. In *MobiCom '05: Proceedings of the 11th annual international conference on Mobile computing and networking*, pages 117–131, New York, NY, USA, 2005. ACM.