Future Network and MobileSummit 2010 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2010
ISBN: 978-1-905824-18-2

On Realising a Strategy for Resilience in Opportunistic Networks

Marcus Schöller[1], Paul Smith[2], Christian Rohner[3], Merkouris Karaliopoulos[4]
Abdul Jabbar[5], James P.G. Sterbenz[2,5], and David Hutchison[2]
[1]*NEC Europe, Kurfürsten-Anlage 36, Heidelberg, 69115, Germany*
Email: marcus.schoeller@neclab.eu
[2]*Lancaster University, InfoLab21, Lancaster, LA1 4WA, UK*
Email: $\{p.smith|jpgs|dh\}$*@comp.lancs.ac.uk*
[3]*Uppsala Universitet, Box 337, 751 05 Uppsala, Sweden*
Email: christian.rohner@it.uu.se
[4]*ETH Zürich, Gloriastrasse 35, 8092 Zürich, Switzerland*
Email: karaliopoulos@tik.ee.ethz.ch
[5]*The University of Kansas, Lawrence, KS 66045-7612, US*
Email: $\{jpgs|jabber\}$*@ittc.ku.edu*

Abstract: Because of our increased dependence on communication networks, resilience needs to be a fundamental property of the future Internet. We define resilience as the ability of a network to provide an acceptable level of service in the light of various challenges, such as episodic connectivity or malicious actors. There have been many helpful point solutions to improve resilience in the Internet, yet a systematic approach is necessary to make resilience a first class citizen of the future Internet.
In this paper, we apply our general resilience strategy, called $\mathsf{D}^2\mathsf{R}^2 + \mathsf{DR}$, to an opportunistic networking scenario, showing how it can be used to address the challenge of selfish nodes. The strategy describes a real-time control loop to allow dynamic adaptation of the networked system in response to challenges, and an off-line loop that aims to improve the performance of the network via a process of reflection. We briefly describe our approach to quantifying resilience, and its use in our scenario. Initial simulation results indicate the promise of our approach.

Keywords: Opportunistic networks, resilience, survivability, DTN

1. Introduction

Society increasingly depends on networks in general and the Internet in particular for many aspects of our daily lives. Consumers use the Internet to access information, obtain products and services, manage finances, and communicate. Business entities use the Internet to conduct business with their customers and with one another. Nations rely on the Internet to conduct government affairs, deliver services to their citizens, and, to some extent, manage homeland security and conduct military operations. As its reach and scope continue to extend, the Internet increasingly subsumes services previously implemented on separate networks.

With this increasing dependence on the Internet and the integration of services within it, the disruption of networked services may lead to severe consequences. Lives of individuals, the economic viability of businesses and organizations, and the security of nations are directly linked to the resilience, survivability, and dependability of data networks. Unfortunately, the increased sophistication and interdependence of services render the Internet more vulnerable to industrial espionage, information warfare, and cyber-crime in general. In parallel, its expansion to the mobile wireless domain exposes the network to the challenges of error-prone links and intermittent network connectivity, raising additional concerns with respect to its robustness and scalability.

The Internet community realised those challenges early, and in many cases has responded to them with resounding success. After all, the very first design choice of datagram routing and maximum flexibility in route retrieval was motivated exactly by the need for high network robustness. Mechanisms such as optical ring restoration, for example, have further signified the attempts to strengthen the network operation tolerance to failures. Nevertheless, there is consensus in the community that the majority of the previous, clearly valuable, efforts have largely been done in isolation rather than as part of an overall systematic approach.

In this paper, we outline an approach to network resilience, based on a general resilience strategy being investigated as part of the EU-funded ResumeNet project [1]. We define network resilience as the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation [2]; effectively, resilience can be viewed as a superset of commonly used definitions for survivability, dependability, and fault tolerance. The strategy describes a real-time control loop to allow dynamic adaptation of a networked system in response to challenges, and an off-line control loop that aims to improve the performance of the network (including the real-time loop) via a process of reflection.

We apply this general resilience strategy to an opportunistic networking scenario, and attempt to illustrate its value. In addition to the application of the strategy to opportunistic networks, we have previously demonstrated its general utility when considering problems of resilience in other contexts, for example, to mitigate the effects of flash crowd events [3] or for weather disruption in millimeter wave wireless mesh networks [4]. Here, however, we show how our opportunistic transport protocol implementation fits into the overall strategy, following the two control loops. These two control loops are triggered by the introduction of an additional challenge to the simulation scenario, namely malicious nodes that do not behave according to the transport service specification, by not forwarding data. We have inserted this challenge into our simulation environment together with mechanisms that aim to allow the system to maintain an acceptable level of service. In the evaluation section we assess the impact of such malicious nodes, as well as the success of our potential remedy, including its costs.

This paper is organized as follows. Our general resilience strategy is described in Section 2. This strategy is investigated within the study case on opportunistic networking in Section 3. Thereafter, the experimentation results derived by our opportunistic networking emulator are presented in Section 4. Our conclusions and an outlook to future work close the paper in Section 5.

2. A General Strategy for Network Resilience – $\mathsf{D}^2\mathsf{R}^2 + \mathsf{DR}$

Our research is based on a general strategy for multi-level network resilience, called $\mathsf{D}^2\mathsf{R}^2 + \mathsf{DR}$ [2]. The strategy involves two nested control loops. The inner loop is a real-time adaptation control loop consisting of the Defence, Detection, Remediation, and Recovery stages. The outer loop contains the stages of Diagnosis and Refinement. This strategy was developed by the ResiliNets Initiative [5] and is partly based on a number of previous strategies, including ANSA [6], CMU-CERT [7], and SUMOWIN [8]

It is common practice to protect networked systems by providing defensive measures. With respect to resilience, two lines of *defence* can be drawn. The first line attempts to prevent challenges from affecting the system, e.g. firewalls. A second line of defence aims to limit erroneous behaviour within a service and tries to prevent failures propagating to other services or to the application. However, since it is impossible to forecast all potential challenges and discover every system fault, defensive measures alone are not sufficient to build a resilient network. Therefore, *detection* mechanisms must be put in place to identify deviations from the specified operational service. The (optimal) result of the detection stage is an informed report about a detected challenge. Based on this report the *remediation* stage applies a resilience strategy in order to maintain the desired level of delivered service, despite the adverse operational condition; or at least it will provide a graceful degradation of the affected service. As soon as the challenge ceases, the activated remediation mechanisms should be discontinued in order to free the resources they consume. We call this deactivation *recovery*.

The outer control loop deals with the long-term improvement of the system. The idea is to assess how successful the real-time control loop was in ensuring network resilience through the various stages outlined above. This is done in the *diagnosis* stage. In the *refinement* stage, the system is improved in response to the outcome of diagnosis, and also includes, for example, reporting to the operator about challenges that cannot be mitigated with the installed resilience mechanisms.

The general strategy abstracts many of the complexities of building resilient networked systems, such as the need for a distributed monitoring system. Many of these complexities are specific to the deployment environment, such as the opportunistic networking scenario presented here. The next section presents details of the system enhancements we have developed for our simulator, in which these control loops are implemented, and we then present the simulation results.

3. Resilience for Opportunistic Networks

We now describe the application of our resilience strategy to an opportunistic networking scenario. Access to the world's networks has become a commodity in a large number of countries, where infrastructure, such as optical fibres, is readily available. However, there are vast regions, often remote, sparsely populated, and with a relatively poor economic base, where the deployment of constant connectivity is not a viable option. Projects like N4C [9] or ZebraNet [10] aim to provide basic e-mail and (cached) Web access to such remote areas using opportunistic networks.

3.1 Service Specification of a Store-Carry-Forward Transport

In opportunistic networks, typically mobile nodes store, carry, and forward messages when they encounter other nodes, using short- range communication. A store-carry-forward (SCF) transport service [8] allows the flow of data in the network despite the absence of end-to-end paths. Data instead travels over *space-time paths*, comprised of sets of links that become available in different time instants in the network. Node mobility is thus important for data dissemination; it creates contact opportunities between different nodes and allows nodes physically to transport data to areas where no connectivity might be available.

A misbehaving node may break this service specification by not forwarding data when a space-time path exists. It is important to note that this service specification assumes unlimited storage capacity. The results presented below are also based on this assumption. We are currently working on incorporating node buffer limitations in the simulator to reflect a more realistic opportunistic network. However, this also introduces complications, which we detail in Section 5. pointing to our future work.

3.2 *Realising the $D^2R^2 + DR$ Strategy*

Based on the resilience strategy described in Section 2., we now illustrate how the opportunistic network can be enhanced to cope with misbehaving nodes. An evaluation of this implementation is provided in the subsequent section. Our overall strategy for mitigating misbehaving nodes is depicted in Figure 1. In summary, we start by understanding the potential capabilities of the network, e.g. in terms of delivery ratio, delay, and number of replicas related to various proposed data forwarding schemes. We do this with the help of simulations and analytical modelling. If we detect a deviation from the expected behavior because of misbehaving nodes, we remediate by adapting the configuration of the store-carry-forward (SCF) transport mechanism. A more detailed description of the realisation of the strategy is as follows.

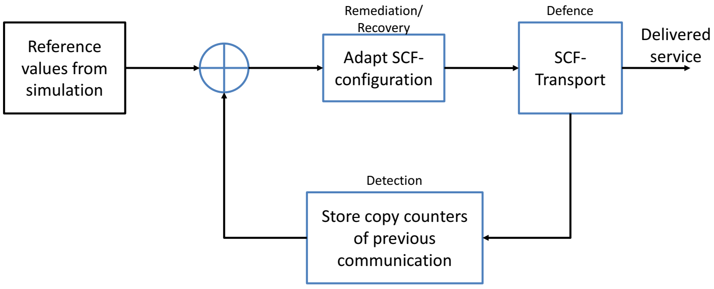

Figure 1: Control loop steering the transport protocol

Defence A network for opportunistic communication using a SCF transport service has inherent defence against the challenge of episodic connectivity. The mobility of nodes gives rise to a diversity of space-time paths. Depending on how aggressive a data forwarding scheme is, the network can exploit all or part of it, at the expense of resource consumption. Epidemic forwarding, for example, makes use of all possible space-time paths in the network and achieves minimum message transfer delay; yet, it generates a very high number of message replicas in the network. Two-hop forwarding, on the other hand, exploits only part of this diversity, limiting the length of feasible space-time paths to two hops [11]. This same diversity can be the counter-measure against misbehaving nodes, whether selfish or malicious, which fail to contribute to the transport service. Likewise, the network defence against selfish behaviours could be strengthened by implementing game-theoretic mechanisms with or without money to promote or enforce node cooperation. An example of a mechanism without money is given in [12]; a similar approach is being developed in the ResumeNet project.

Detection The implementation of challenge detection mechanisms is one of the most difficult parts in an opportunistic network, precisely because of their intermittent connectivity. To detect the presence of misbehaving (or unhelpful) nodes, sources would need to maintain a history of the nodes that participated in the delivery of a message. In turn, receiver nodes should maintain a list of nodes they have seen and nodes that successfully delivered a message to them. Then the sender and receiver nodes would need to exchange their state, either upon a direct contact or during an off-line period, e.g., when the devices are attached to some infrastructure. Using that information, the sender could deduce which nodes cooperated in forwarding a given message, and which did not; and out of them, which nodes did so because they never saw the receiver, and which ones chose not to transmit the message.

Extensions of this algorithm include nodes sharing their local knowledge about the utility of various nodes – by disseminating information about unhelpful nodes and those that are useful for certain destinations. The utility of this algorithm in different forwarding scenarios and the effect of various parameters of the algorithm on its utility (e.g. the amount of state to maintain) require further investigation.

Remediation If a node detects the presence of misbehaving nodes, it adapts the SCF transport service configuration to enable a more aggressive forwarding mechanism. For example, it could shift from two-hop to epidemic forwarding. Effectively, in this way, it restores some or all of the space-time diversity that is lost due to the existence of misbehaving nodes.

Recovery The use of epidemic forwarding as a remedy against misbehaving nodes brings the associated cost of increased energy consumption and buffer utilisation at the network nodes (see Section 4. for details). Therefore, the SCF transport service should recover to its normal operation using two-hop forwarding as soon as the malicious nodes have disappeared from the system. This requires additional detection capabilities, which are currently under further investigation.

Diagnosis The diagnosis step includes the understanding of the impact of node misbehaviours on the network performance and the ability of the remediation solution to cope with it. For example, when the remediation is implemented via use of the epidemic forwarding scheme, all data can be forwarded to its destination and the delivery delay is decreased. However, the diagnosis also reveals the high costs that this forwarding scheme places on the system.

Refinement Based on the diagnosis step, measures for better balancing between the resource usage of the scheme and the achievable end-user performance can be designed. An ageing mechanism for efficiently managing the node forwarding storage is such an example. Messages older than a certain threshold will be deleted from the store. The results of this measure are also shown below.

3.3 Resilience Metrics for Opportunistic Networking

One of the difficult tasks is the quantitative characterisation of resilience in order to evaluate the *efficacy* of architectures and developed mechanisms. This is an especially hard problem because of the numerous 'levels' within networks and the interaction between these levels. Given our multi-level resilience approach, we are developing a framework that enables resilience evaluation at any arbitrary level. First, we define a service at any given layer boundary. We then quantify the resilience of the network at this boundary using a two-dimensional state-space model [13]. Along one dimension, we characterise the *service* at a given layer boundary using the metrics that are desired from such a service (e.g. storage size). Along the other dimension, metrics that define the *operational* state at the layer boundary (i.e. metrics that affect those defined in the service dimension) are specified (e.g. data delivery ratio). Finally, we quantify resilience as a measure of service degradation in the presence of challenges (perturbations) to the operational state of the network.

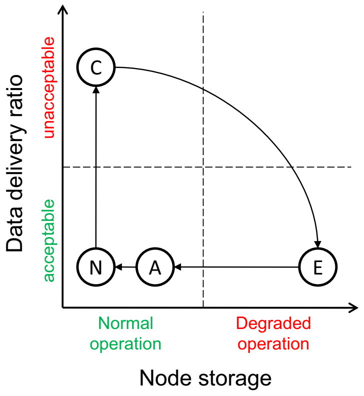

Figure 2: Resilience metric state space

In Figure 2, this approach is depicted for our opportunistic networking scenario.

The system's normal operation (N) is affected by the presence of misbehaving nodes, which degrade the provided service (C). Applying epidemic forwarding as a remedy allows the system to deliver the desired service again, but at an increased cost (E). Introducing ageing during the refinement phase improves the system to maintain the specified service, while reducing the cost again (A). Finally, recovery brings the system back into its normal mode of operation (N).

4. Evaluation

We sketch an opportunistic network scenario to evaluate the proposed resilience strategy. The experimental results are obtained with the Haggle experimentation architecture [14] running on 20 (virtual) nodes with controlled connectivity. Connectivity between two nodes follows a two state Markov model with typical average contact time and average inter-contact time of 30 seconds and 150 seconds respectively. This topology avoids large connected clusters but still gives enough contact opportunities to exchange data. The nodes generate data every 2 seconds with a random destination among the 20 nodes. Our emulator offers the possibility of dynamically changing the forwarding strategy and resource management policies, for example to age out data carried for a long time. We use the two-hop forwarding scheme [11] with no data ageing as the default configuration (as normal operation).

Our experiment considers four operational states: *normal* operation with all nodes using the two-hop forwarding strategy, *challenged* operation with 8 out of the 20 nodes refusing to forward data of other nodes, as an expression of selfish behaviour. Assuming perfect detection, we pass into the, third, *remediation* phase by activating epidemic forwarding on the remaining co-operating nodes. Finally, we enter the *refinement* phase by periodically ageing data based on the time they stay in a node's data buffer; thus, we compensate for the additional redundancy introduced by epidemic forwarding. For our evaluation we consider the amount of data received at the destination, the end-to-end delay for all received data, and the amount of data in the buffer of a co-operating node, measured over a period of 90 seconds. The results are summarized in Table 1.

scenario	delivered data	end-to-end delay	buffer
normal (N)	227	37 s	127
challenged (C)	134 (−41%)	31 s (−16%)	n/a
remediation (E)	226 (±0%)	18 s (−51%)	942 (+642%)
refinement (A)	246 (+8%)	17 s (−54%)	177 (+39%)

Table 1: Evaluation results.

Selfish behaviour of 8 out of the 20 nodes reduces the number of delivered data significantly to 59% of the data delivered during normal operation. The end-to-end delay of delivered data is reduced by a few seconds, because data with a longer delivery time in normal operation is not delivered at all in challenged operation and thus does not contribute to the result. By using epidemic forwarding as a remediation mechanism, the co-operating nodes compensate for the impact of selfish nodes, achieving almost the same delivery of data as in normal operation. Furthermore, end-to-end delay of the delivered data is much smaller because the restriction for redundancy of two-hop forwarding no longer applies, but data may reach the destination over longer space-time paths. However, because redundancy is no longer restricted, the amount of data on the inspected node increases dramatically from 127 units during normal operation to 942 during the remediation phase. The refinement process takes account of that aspect by ageing data that was stored on a node for more than 45 seconds. As a result, the stored data is reduced to 177 units, which is again close to the normal operation. End-to-end delay was not affected, while the number of delivered messages actually improves.

This latter aspect is explained as follows: our emulation software ranks - in order of importance – the data to be transferred to another node, and transfers only some of the data to help limit congestion. Also, the longer data is in the buffer of a node, the higher the likelihood that it already has been delivered to the destination by other nodes. By ageing older data, we thus give priority to the transfer of newer data.

5. Conclusion

In this paper, we have argued that resilience is a necessary building block for any future network. Despite the fact that many resilience mechanisms have been added to networks, especially to the Internet, a systematic approach to resilience has not so far been developed in order to increase its availability and survivability. We have introduced a general strategy that aims to embed resilience systematically into networked systems. We have applied our strategy to an opportunistic networking scenario, showing some of our early results and how this strategy can enhance the network over time.

Future work will refine the service specification for the store-carry-forward transport service to reflect realistic resource limitations of the network nodes. Due to this limitation several complications arise; these impact the detection mechanisms, i.e. how to detect misbehaving nodes, in contrast to nodes which dropped data as a result of limited storage. Moreover, epidemic forwarding as a remediation mechanism can worsen the system performance compared to normal two-hop forwarding in the presence of some misbehaving nodes. Repeatedly applying our strategy to the simulator should enable us to find suitable mechanisms and more importantly validate more completely the suitability of our resilience strategy.

Acknowledgements

The research was supported in part by the European Commission under grant FP7-224619 (ResumeNet) and US NSF FIND under grant CNS-0626918. The authors would like to thank members of these projects for their input into the ideas in this paper.

References

[1] "The EU FP7 Resumenet Project." `http://www.resumenet.eu`.

[2] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer Networks*, 2010. (to appear).

[3] L. Xie, P. Smith, D. Hutchison, M. Banfield, H. Leopold, A. Jabbar, and J. P. G. Sterbenz, "From detection to remediation: A self-organized system for addressing flash crowd problems," in *IEEE ICC 2008*, pp. 5809–5814.

[4] A. Jabbar, J. P. Rohrer, A. Oberthaler, E. K. Çetinkaya, V. S. Frost, and J. P. G. Sterbenz, "Performance comparison of weather disruption-tolerant cross-layer routing algorithms," in *IEEE INFOCOM 2009*, pp. 1143–1151.

[5] "The ResiliNets Initiative." `https://wiki.ittc.ku.edu/resilinets`.

[6] N. Edwards, "Building dependable distributed systems," Technical report APM.1144.00.02, ANSA, February 1994.

[7] R. J. Ellison *et al.*, "Survivable network systems: An emerging discipline," Tech. Rep. CMU/SEI-97-TR-013, PA, 1999.

[8] J. P. G. Sterbenz *et al.*, "Survivable mobile wireless networks: issues, challenges, and research directions," in *ACM WiSE 2002*, pp. 31–40.

[9] "The N4C project." `http://www.n4c.eu`.

[10] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. S. Peh, and D. Rubenstein, "Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with zebranet," *SIGOPS Oper. Syst. Rev.*, vol. 36, no. 5, pp. 96–107, 2002.

[11] M. Grossglauser and D. N. Tse, "Mobility increases the capacity of ad hoc wireless networks," in *IEEE/ACM Trans. on Networking*, vol. 10, pp. 477–486, August 2002.

[12] L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda, "Barter trade improves message delivery in opportunistic networks," *Ad Hoc Net.*, vol. 8, no. 1, pp. 1–14, 2010.

[13] A. J. Mohammad, D. Hutchison, and J. P. Sterbenz, "Poster: Towards quantifying metrics for resilient and survivable networks," in *IEEE ICNP 2006*, pp. 17–18.

[14] E. Nordström, P. Gunningberg, and C. Rohner, "A search-based network architecture for mobile devices," Tech. Rep. 2009-003, Uppsala Univ., 2009.