Displays xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

Displays

journal homepage: www.elsevier.com/locate/displa

Sonification of a network's self-organized criticality for real-time situational awareness ☆

Paul Vickers [a,*], Chris Laing [b,1], Tom Fairfax [c]

[a] Northumbria University, Newcastle upon Tyne NE1 8ST, UK
[b] Sciendum Ltd, 20-22 Wenlock Road, London N1 7GU, UK
[c] SRM Solutions, The Grainger Suite, Dobson House, Regent Centre, Gosforth, Newcastle upon Tyne NE3 3PF, UK

ARTICLE INFO

Article history:
Received 28 October 2015
Received in revised form 21 April 2016
Accepted 6 May 2016
Available online xxxx

Keywords:
Auditory display
Sonification
Information visualization
Self-organized criticality
Network monitoring

ABSTRACT

Communication networks involve the transmission and reception of large volumes of data. Research indicates that network traffic volumes will continue to increase. These traffic volumes will be unprecedented and the behaviour of global information infrastructures when dealing with these data volumes is unknown. It has been shown that complex systems (including computer networks) exhibit self-organized criticality under certain conditions. Given the possibility in such systems of a sudden and spontaneous system reset the development of techniques to inform system administrators of this behaviour could be beneficial. This article focuses on the combination of two dissimilar research concepts, namely sonification (a form of auditory display) and self-organized criticality (SOC). A system is described that sonifies in real time an information infrastructure's self-organized criticality to alert the network administrators of both normal and abnormal network traffic and operation. It is shown how the system makes changes in a system's SOC readily perceptible. Implications for how such a system may support real-time situational awareness and post hoc incident analysis are discussed.

1. Introduction

With the large volumes of traffic passing across networks it is important to know about the state of the various components involved (servers, routers, switches, firewalls, computers, network-attached storage devices, etc.) and the types and volume of the data traffic passing through the network. In the case of the hardware, network administrators need to know if a component has failed or is approaching some capacity threshold (e.g., a server has crashed, a hard drive has become full, etc.) so that appropriate action can be taken. Likewise, the administrators need to be aware of traffic type and flow. For example, a large increase in traffic volume (perhaps as would occur if the network were to broadcast a live stream of a major sporting event) might require extra servers to be brought online to handle and balance the load. A sudden increase in certain types of traffic (such as small UDP packets) might indicate that a distributed denial-of-service attack is in progress, for example, and corrective action would need to be taken to protect the network.[2]

Given the large volume of traffic passing through a network every second in the form of data packets and the fact that each packet will be associated with particular sender and receiver IP addresses and port numbers, understanding what is happening to a network requires information about the traffic data to be aggregated and presented to the network administrator in an easy-to-understand way. This problem of information presentation and interpretation, or 'situational awareness', was addressed by the military leading to Boyd's OODA (observe, orient, decide, act) model (see [1]), and others have followed (notably Endsley's three-level model [2]). Situational awareness, as Cook put it, "requires that various pieces of information be connected in space and time" (Nancy Cooke in McNeese [3]).

Computer networks possess high tempo and granularity but with low visibility and tangibility. Administrators rely on complex data feeds which typically need translation into language that can be understood by decision makers. Each layer of analytical tools that is added can increase the margin for error as well as adding

☆ This paper was recommended for publication by Richard H.Y. So.

* Corresponding author.
E-mail addresses: paul.vickers@northumbria.ac.uk (P. Vickers), christopher.laing@sciendum.org.uk (C. Laing), tom.fairfax@srm-solutions.com (T. Fairfax).

[1] This work was done while Chris Laing was at Northumbria but he is now at sciendum.org.uk.

[2] UDP, or user datagram protocol, is a way of sending internet packets without handshaking. It means that packets can be lost, but in some real-time systems (e.g., online gaming) it is preferable to lose a packet than to wait for a delayed one.

http://dx.doi.org/10.1016/j.displa.2016.05.002
0141-9382/

Clausewitzian friction (see von Clausewitz's '*On War*', 1873). Furthermore, it is practically impossible for most administrators to watch complex visual data feeds concurrently with other activity without quickly losing effectiveness [4].

In military circles there is debate about whether cyberspace has become the fifth warfighting domain (the others being sea, land, air, and space) [4]. Computer networks are increasingly coming under strain both from adversarial attacks (warfighting in military parlance) and from load and traffic pressures (e.g., increased demand on web services).

Another term that has made its way from the military lexicon into the wider world of network administration is situational awareness. Endsley [2, p. 36] defined situational awareness (SA) as the "perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future". So, SA facilitates an administrator in becoming aware of a network's current state. The perception phase of SA comprises the recognition of situational events and their subsequent identification. Sonification is a process of computational perceptualisation which Vickers [5] suggested is well suited to the monitoring of time-dependent processes and phenomena such as computer networks.

Fairfax et al. [4] noted that the cyber environment is increasingly being viewed as the fifth warfighting domain (alongside land, sea, air, and space). They stated the challenge for maintaining situational awareness in the cyber environment as:

> ...whilst land, sea, air and space are physically distinct and are defined by similar criteria, cyberspace is defined in a different way, existing on an electronic plane rather than a physical and chemical one. Some would argue that cyber space is a vein which runs through the other four warfighting domains and exists as a common component rather than as a discrete domain. One can easily see how cyber operations can easily play a significant role in land, sea, air or space warfare, due to the technology employed in each of these domains [4, p. 335].

Thus, in this environment where human perception is constrained, adversaries and protagonists alike are dependent on tools for their perception and understanding of what is going on. Many tools on which we rely for situational awareness are focused on specific detail. The peripheral vision (based on a range of senses) on which our instinctive threat models are based is very narrow when canalised by the tools we use to monitor the network environment. The majority of these tools use primarily visual cues (with the exception of alarms) to communicate situational awareness to operators. Put simply, situational awareness is the means by which protagonists in a particular environment perceive what is going on around them (including hostile, friendly, and environmental events), and understand the implications of these events in sufficient time to take appropriate action.

When network incidents occur experience shows that the speed and accuracy of the initial response are critical to a successful resolution of the situation. Operators observe the indicators, orient themselves and their sensors to understand the problem, decide on the action to be taken, and act in a timely and decisive way. Traditional approaches to monitoring can hinder this by not making the initial indication and its context clear thus requiring an extensive orientation stage. An ineffective initial response is consistently seen to be one of the hardest things for people to get right in practice [4]. D'Amico (see McNeese [3]) put the challenge of designing visualizations for situational awareness this way:

> ...visualization designers must focus on the specific role of the target user, and the stage of situational awareness the visualizations are intended to support: perception, comprehension, or projection.

While work has been carried out to use information visualization techniques on network data we note that the *perceive* and *comprehend* stages in Endsley's three-level situational awareness model (the third being *project*) [2] align themselves with Pierre Schaeffer's two fundamental modes of musical listening, *écouter* (hearing, the auditory equivalent of perception) and *entendre* (literally 'understanding', the equivalent of comprehension). Vickers [6] demonstrated how Schaeffer's musical context can be applied sonification. This paper proposes a sonification tool as one of the means by which real-time situational awareness in network environments may be facilitated. A more detailed discussion of situational awareness and its relationship to network monitoring (specifically within a cybersecurity and warfighting context) can be found in Fairfax et al. [4].

1.1. Sonification for network monitoring

Sonification has been applied to many different types of data analysis (for a recent and broad coverage see *The Sonification Handbook* [7]). One task for which it seems particularly well suited is live monitoring, as would be required in situational awareness applications [5]. The approach described in this article provides one way of addressing the challenges outlined above by enabling operators to monitor networks concurrently with other tasks using additional senses. This has the potential to increase operators' available bandwidth without overloading individual cognitive functions, and could provide an immediate and elegant route to practical situational awareness.

It has been suggested that understanding the patterns of network traffic is essential to the analysis of a network's survivability [8]. Typically, analysis takes place post hoc through an inspection of log files to determine what caused a crash or other network event. Lessons would be learned and counter measures put in place to prevent a re-occurrence.

For the purpose of keeping a network running smoothly load balancing can sometimes be achieved automatically by the network itself, or alerts can be posted to trigger a manual response by the network administrators. Guo et al. [8] observed that "from the perspective of traffic engineering, understanding the network traffic pattern is essential" for the analysis of network survivability.

Often, the first the administrators know about a problem on a network is after an attack, or other destabilizing event, has taken place or the network has crashed. Here, the traffic logs would be examined to identify the causes and steps would be taken to try to protect against the same events in future. Live monitoring of network traffic assists with situational awareness and could provide administrators either with advanced warning of an impending threat or with real-time intelligence on network threatening events in action.[3]

Real-time network monitoring offers a challenge in that, except for alarms for discrete events, the administrator must be looking at a console screen to observe what is happening. To identify changes in traffic flow would this require attention to be devoted to the console [4]. Vickers [5, p. 455] categorised monitoring tasks as direct, peripheral, or serendipitous-peripheral:

> In a direct monitoring task we are directly engaged with the system being monitored and our attention is focused on the system as we take note of its state. In a peripheral monitoring task, our primary focus is elsewhere, our attention being diverted to the monitored system either on our own volition at intervals by scanning the system ...or through being interrupted by an exceptional event signalled by the system itself.

[3] By threat, we do not only mean a hacking/DDoS attack, but also include 'natural' disasters such as component failures, and legitimate traffic surges.

Please cite this article in press as: P. Vickers et al., Sonification of a network's self-organized criticality for real-time situational awareness, Displays (2016), http://dx.doi.org/10.1016/j.displa.2016.05.002