



SENIOR LEADER PERSPECTIVE: SOFTWARE VIRTUAL NETWORKS



Dr. Rajive Bagrodia

NSCI's Lindsay Trimble recently interviewed Dr. Rajive Bagrodia, president and chief executive officer of Scalable Network Technologies, and Maj. Gen. (ret.) George "Nordie" Norwood, president and chief executive officer of Norwood & Associates. In 1999, Bagrodia founded Scalable Network Technologies (SNT) – a software and services company. Norwood is retired from the U.S. Air Force after more than 30 years of service and has served on SNT's Board of Directors since 2002.



Maj. Gen. (ret.) George "Nordie" Norwood

SNT develops and supports evaluation software that can represent physical wireless networks as software virtual networks – exact digital replicas with full functionality that behave exactly like live networks. In this interview, Bagrodia and Norwood explain how software virtual networks will be influential in cyber defense training and preparation – in industry, the government and the military.

NSCI: Dr. Bagrodia, in your recent article on "wireless cyber warfare," you say that wireless networks – specifically mobile networks – are "the most critical component of tactical communication infrastructure," but also "the most neglected network security domain, in terms of spending." In general, spending is often associated with the likelihood and severity of the threat. Can you talk a little bit about the likelihood and severity of the threat to military and/or commercial mobile networks?

BAGRODIA: Absolutely. Wireless networks are – plain and simple – harder to protect than wired networks. For one thing, it's easier to provide physical security for wired networks. But because wireless networks transmit over an open and shared medium, they are much more vulnerable to threats and acts of destruction.

The second part of the problem is that the next generation of military and commercial wireless networks involve what we call multi-hop wireless communications. This multi-hop aspect opens up security holes in the communication protocol stack. These holes were not present in the previous generation of communication networks, where intermediate radios were basically used to relay traffic from one point to another. This new capability of routing traffic opens up new vulnerabilities.

Because we're talking about concepts of the Global Information Grid, or GIG – which potentially ties in communication at the tactical edge to the larger communication network – disruption at the



tactical edge of a mobile ad hoc network would lead not only to a loss of communication, and consequently disrupt decision-making at the tactical end, but could potentially disrupt communications at the higher-command levels as well.

These sets of vulnerabilities make the problems of securing multi-hop communication networks much more critical.

NSCI: What do you recommend as defense against cyber attacks on mobile networks?

BAGRODIA: Let me paraphrase the old real estate adage: The best way to defend against attacks to mobile networks is preparation, preparation, preparation.

There are various ways we can prepare against that eventuality. First, we prepare the communication infrastructure itself to handle the “type” of cyber threats that we know. Second, we prepare the processes, protocols and countermeasures to survive cyber threats once they are launched against us. Last, we prepare and train our personnel to identify and respond to cyber threats in the best time-efficient manner possible.

If we can prepare along these three dimensions, I think we are in a much better position to respond to attacks on our communication infrastructure. From our perspective, the adoption of software virtual networks is a crucial goal in the other types of preparation – in training environments, analysis, role playing work stations for cyber professionals, and so on.

NSCI: General Norwood, as the need increases for real-time news and information, and wireless devices are increasingly common in government and industry, how is the military adapting to the need for a different – and more complex – type of network security?

NORWOOD: The military need is not just for news and information; it’s really about getting actionable intelligence in the hands of a warfighter – at all levels. This all happens over networks that are made up of this complex mix of both mobile wireless and wired devices and equipment. All commanders, especially those of expeditionary and mobile force, rely heavily on the wireless networks for secure voice, data and video. These large, mobile ad hoc networks bring together new communication devices and equipment, but they’re coupled with legacy systems, and so they make for a complex and vulnerable system.

NSCI: When combat operations begin, is there data comparing mobile/wireless communication criticality to fixed/wired communication criticality?

NORWOOD: I’m not aware of a study that actually compares criticality of mobile/wireless versus fixed/wired systems – maybe vulnerability, but not necessarily criticality. Because these modern networks that we’re talking about rely on a complex combination of mobile/wireless and fixed/wired communication, all elements of that network are both critical *and* vulnerable. That’s why we must account for the inherent vulnerabilities of the mobile portion of the network. Really, it’s the entire network that must be protected and defended. Enemy forces – the red force attackers – will exploit any and all vulnerabilities they find, anywhere in the system.



NSCI: Dr. Bagrodia, how are software virtual networks (SVNs) changing the security environment?

BAGRODIA: Software virtual networks are exact digital replicas of the live network. They can be used to replace a live network such that any application, system components – even humans – can interact with the SVN just as if they were interacting with the actual network. So you can embed this SVN to represent a communication network and hook up applications, humans and other systems to interact with it. This allows us to place our cyber defense professionals in front of the actual environment, have the “network” they’re monitoring subjected to attacks by someone playing the role of the red side, and see how the cyber ops personnel respond to the attack and prepare their countermeasures. We could additionally have the red side detect the countermeasures and modify the type of attacks; thus you can have a very realistic cyber war game being played where the red side is not artificially disadvantaged.

We need our training to be as realistic as possible, which means giving the red side a lot more freedom to be able to inject increasingly refined attacks. This will provide a training environment that prepares our cyber professionals to effectively respond as the war game unfolds in a highly realistic setting.

NSCI: Just to clarify, people play the roles on both sides – red and blue?

BAGRODIA: Exactly. SVNs can be used to represent different types of communication networks. We could, for instance, pretend that the red side is using a standard commercial cellular telephone network to launch an attack. We represent the blue side communication using whatever mix of military technologies that would be used in the field and see how the red side would inject their attacks.

The second important component of this is that we can deploy actual applications – the battle command or situational awareness, or any other applications that we would use on the corresponding physical network – on an SVN. When an attack is launched on the red side, we can expose trainees to how the applications really behave and respond in the presence of those attacks. There may be major differences between how the underlying communication network manifests the problems during an attack – as opposed to how the application manifests those network problems.

What the SVNs allow us to do is to directly reflect the impact of computer network attacks in the context of our battle command applications. This provides a significantly higher degree of realism, allowing us to prepare responses and fall-back plans in a very realistic setting.



NSCI: What are some of the benefits of SVNs?

BAGRODIA: There are three primary benefits: cost, flexibility and providing a controlled environment.

Let's look at cost: With digital representations, if we want a communication network with hundreds or even thousands of radios, all that is required is the software and an appropriate hardware platform, which may be a parallel computer with some tens of processors. That's it! Then we can do the training or the analysis using the digital environment, rather than a significantly more expensive physical test-bed.

With respect to flexibility, suppose we want to create a scenario of attack and then replay it in an urban context. What this means is I must recreate how radio transmissions behave in the presence of buildings, huts or whatever type of physical environment. Trying to recreate that environment digitally is much easier and more economical than trying to do that in the corresponding physical context. Doing it in a physical test-bed would certainly increase realism, but because a multitude of different physical environments can be recreated effectively in a digital context, SVNs allow us to expose the trainee to the effect of cyber attacks and countermeasures in many different settings. This flexibility, combined with cost savings, is very important.

The third thing is providing a repeatable, controlled environment. Let's say we launch a particular type of attack and the blue side didn't respond as effectively as desired. We can recreate that attack again to figure out where the problems are rooted. This is ideal for training purposes, as opposed to live – where such repeatability may be much harder to achieve.

NSCI: Can you tell us how SVNs improve network security day-to-day operations, training and experimentation?

BAGRODIA: Because an SVN is an exact digital replica, we can create a shadow representation of the network, and use that to conduct a "dress rehearsal" of day-to-day operations. We can do a number of "what if" analyses, and even extrapolate some trends noticed in physical networks to see if they might indicate a potential problem in its operation.

For instance, if we see the network traffic increasing at a certain rate over a time period, we can extrapolate that rate of increase over a slightly longer time period to see how it might affect the operation of the network. With any critical system, it's important to have a shadow of that system that can be replayed in a "back room" to detect potential flaws and vulnerabilities or to find ways to improve its performance.