On Information Assurance in Nanoscale Networks

Stephen F. Bush, *Senior Member, IEEE*
GE Global Research Center, Niskayuna, NY, 12309, USA
bushsf@research.ge.com

***Abstract*–An intersection of two worlds, emerging nano-technologies and network/communication theory, is poised to change the nature of information assurance. New communication paradigms will be derived from the transition from micro- to nano-scale devices. The related degrees of freedom and constraints associated with these new technologies will change our notions about efficient networks, system design and the nature of information assurance. Work is ongoing on a multi-disciplinary front towards new techniques in modeling, design, simulation, and fabrication of network and communication systems at the nano-scale. This paper reviews the state of the art and considers the challenges and implications for information assurance.**

***Index Terms*–nanotechnology communication networks, and information assurance.**

I. INTRODUCTION

Networks communicating nformation exist on a nanoscale [1]. Interconnected carbon nanotubes, micrometers in length and nanometers in diameter, convey signals across areas of tens of square micrometers [25]. The Nano-Net conference [35] focuses on aspects familiar to those researching today's macro-scale communication systems such as efficient coding, routing, quality of service, but within nanoscale networks. Wireless transmission and reception among components on a single chip have been designed in [34] and patented in [33]. Nanoscale wireless security issues will need to be addressed at some point. Thus, while it is still early in the development of nanoscale networks, it may be worth considering that information warfare and network security may have to be considered at the nanoscale, just as they are on the macro scale.

Information security is typically comprised of *confidentiality*: assurance that information is shared only among authorized persons or organizations, *integrity*: assurance that the information is authentic and complete, and *availability*: assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them. How are these impacted when entire, or at least significant portions, of communication networks are reduced to the nano scale?

First, consider the impact of the extreme difference in scale between today's networks and nanoscale networks. In Fig. 1 the size of a wireless mote sensor is to a nanotube as the length of a large bridge (or approximately an Ethernet segment) is to a finger on the human hand. Thus, it is clearly much easier to manipulate and replace components in today's Internet.

In terms of nanoscale sensor networks, the network components are on the same scale as the individual molecules of the sensed elements. This close relationship in scale between sensed targets and the communication network has significant implications for information security. Management of the complexity of such systems becomes significantly more difficult. The ability to detect and mitigate malicious behavior is thus more difficult. The problems are twofold: (1) the significant increase in the complexity of nano-scale systems due to their larger number of components within a compact space (2) the mismatch in the size of the networking components, making them individually more difficult to detect and handle.

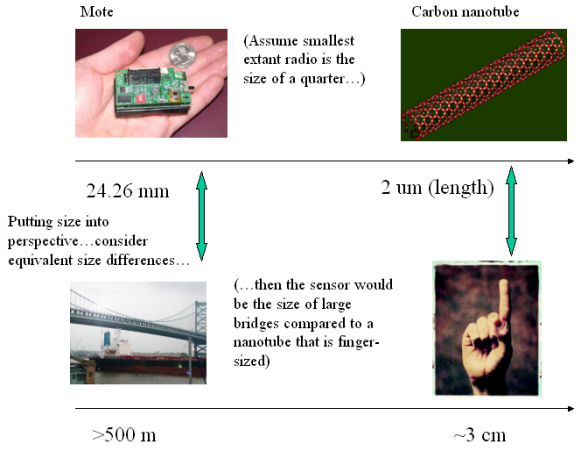

Fig. 1. Comparison of macro and nanoscale networking. The size of a wireless mote sensor is to a nanotube as the length of a large bridge (or an Ethernet segment) is to a finger on the human hand.

As specific examples, consider several manifestations of nanoscale networks: (1) biological networking (2) nanotube interconnections (3) quantum communication. The nature of attacks at the nanoscale will utilize the nature of both the small scale and the strong relationship to fundamental physical objects: real viruses in biological systems may compromise a molecular communication system, eavesdropping may occur by tapping into nanoscale networks with the attacker's network sensors at the same scale, denial of service may be accomplished by flooding nanoscale networks with small physical matter, careful and controlled induced faults in the physical nature of the

nanoscale network in order to discreetly corrupt the integrity of the information.

II. NANOROBOTICS AND SECURITY

There are two major research thrust areas [31]. The first area deals with design, simulation, control, and coordination of robots with nanoscale dimensions. The second research area focuses on overall miniaturization of mobile robots down to μm overall sizes. Nanorobots, nanomachines, and other nanosystems are objects with overall dimensions at or below the micrometer range and are made of assemblies of nanoscale components with individual dimensions ranging approximately between 1 to 100 nm. In these mobile robotic systems, overall system size is very limited, which induces severe constraints in actuators, sensors, and motion mechanisms; power sources, computing power, and wireless communication capability. When scaling down, the surface-to-volume ratio increases and surface forces dominate volume-based forces. At nm scales, inter-atomic forces or surface chemistry plays a significant role in robot mechanics. Thus, inertial forces and weight are almost negligible and micro/nanoscale surface inter-atomic forces, fluid dynamics, heat transfer, surface chemistry, and adhesion-based contact mechanics and friction dominate robot mechanics. These micro/nanoscale forces have many different characteristics compared to macroscale ones [30]. Our focus is on the information transmission among such nanomachines [32] and whether the nanoscale forces have an impact upon the fundamentals of communication and its corresponding security. Research into nanorobotics is well underway [29] and one can easily imagine such robots programmed to carry out the mission of discreetly compromising a nanoscale network. Defense against nanorobots is likely to lead towards a new integration of information and physical security.

III. NANOSCALE NETWORKS

Source and channel coding as well as cryptography require computational overhead which (1) grow very rapidly with the large scale of nano networks and (2) network processing power is reduced at the nanoscale because there is limited processing that can be packed into a ever smaller volumes. Given this limitation, more of the computation will have to be done by non-traditional means, perhaps by utilizing network topology as part of the computation.

Nanoscale networking has been driven by several factors, a significant one being the fact that industry is reaching limits regarding the speed of processors that can be placed onto an integrated circuit chip with acceptable properties of power consumption, current leakage, and heat dissipation. This is leading to new multi-core architectures, where a multi-core processor is an integrated circuit (IC) to which many, sometimes in the hundreds, of processors have been attached for enhanced performance, reduced power consumption, and more efficient simultaneous processing of multiple tasks. A multiple core set-up is somewhat comparable to having multiple, separate processors in the same chip. Multi-core processing is a growing industry trend as single core processors rapidly reach the physical limits of possible complexity and speed.

The current means of connecting elements on a chip will prove insufficient as chips advance to include many independent processing elements (PEs). This motivates research into various forms of networks on chip (NoC) to connect the PEs. Another term often used is system on chip (SoC), which refers to the integration of an entire macroscopic device, such as general-purpose computer, on a single chip. In the short term, current lithography-based approaches will continue to evolve to fabricate chips and only the architecture of the chips will change. However, longer-term at the scale of 22 nanometers and less, current techniques simply cannot be used to produce large-scale integrated circuits. Here, the Nano-Net conference has provided a venue for novel ideas for fabricating computing devices, such as combining self-assembled DNA structures with processing and communication elements based on carbon nanotubes (CNTs).

A. Carbon Nanotube Networks

Current computer chips are fabricated with lithographic techniques operating at 65 nm with predictions for 45-nm scale chips in 2008 [1]. The industry roadmap predicts that in 2018 feature size will reach 16 nm; however, no currently known process can reliably produce this scale of interconnects in mass quantity [1]. Researchers are now looking towards carbon nanotubes to achieve this objective. Currently, the resulting population of carbon nanotubes (CNTs) is highly variable. This is a basis for considering long-term approaches based on self-assembly of DNA and integration with CNTs.

A carbon nanotube (CNT) is a sequence of carbon atoms (C60), which are arranged into a long thin cylinder with a diameter of approximately one nanometer [2]. The atomic structure of CNTs makes them mechanically strong and the atomic properties lead them to be conductors of electric current. Researchers have used CNTs to construct various electronic components, such as resistors, capacitors, inductors, diodes and transistors [2]. CNTs, which appear as rolled tubes of graphite (graphene) with walls constructed from hexagonal carbon rings, can be formed into large bundles (much as typical electronic wires can be bundled) [4]. CNTs come in two general forms: single-walled (SWNTs) and multi-walled (MWNTs). SWNTs have only a single tube, while MWNTs consist of concentric tubes [4].

B. Molecular Communication

Molecular communication aims to allow nanoscale machines to communicate using molecules as a carrier to

convey information. [6] “Molecular communication is inspired by the observation that in biological systems, communication is typically done through molecules. For instance, biological systems perform intra-cellular communication through vesicle transport, inter-cellular communication through neurotransmitters, and inter-organ communication through hormones. Current nano and biotechnology focus on observation and understanding of existing biological systems such as how communication is done within a cell or between cells. Molecular communication would work toward the actual design and control of a nano-scale communication system.” [6] The fundamental research issues include: (a) controlling propagation of carrier molecules, (b) encoding and decoding information onto molecules and (c) achieving transmission and reception of carrier and information molecules.

The aim is to achieve communication over 10’s of micrometers using carrier molecules, such as molecular motors, hormones or neurotransmitters. Information is encoded as proteins, ions or DNA molecules. The environment is taken to be the aqueous solution found within and between typical cells. [6] One can imagine a variety of new information assurance issues for this type of media.

C. Solid-State Quantum Devices

Another approach to nanoscale electronics is to exploit devices based on quantum effects. These include tunneling diodes, single-electron transistors and quantum dots [3]. It is well known that quantum devices are sensitive to noise and, if one assumes lithographic techniques for interconnection, would be highly sensitive to lithographic accuracy since quantum devices operate on the scale of one or a few electrons.

With regard to information assurance, quantum devices may enable the use of quantum cryptographic techniques to improve information assurance at the nanoscale level. The BB84 [39] quantum key distribution scheme developed by Charles Bennett and Gilles Brassard in 1984 is a well-known example. The protocol is provably secure, relying on the quantum property that information gain is only possible at the expense of disturbing the signal if the two states we are trying to distinguish are not orthogonal. Quantum approaches to information assurance are growing rapidly in both macroscale and nanoscale networks.

IV. NETWORKING ON A CHIP

Solutions from macroscale wide-area networking are being proposed for use in on-chip networks. The implementations for the routers vary widely using techniques of packet or circuit switching, dynamic or static scheduling, wormhole or virtual-cut through routing. The majority of the current router implementations for network-on-chip are based on packet-switched, synchronous networks.” [7]

Some research has proposed an NoC topology and architecture that injects data into the network using four sub-NICs (Network Interface Controllers), rather than one NIC, per node. This scheme achieves significant improvements in nano-network latency and energy consumption with only negligible area overhead and complexity over existing architectures. In fact, in the case of MESH network topologies, the proposed scheme provides substantial savings in area as well, because it requires fewer routers.

Another theme that drives research in on-chip networks is the likelihood that production of chips with massive numbers of processing elements and interconnections will increase uncertainty with respect to on-chip properties. Researchers following this theme begin to address issues that will also be of concern in the long-term for self-assembled systems. For example, some links might be so long that communications between PEs cannot occur in a single clock cycle [13]. In other cases, chip properties might lead to transient, intermittent or permanent communication errors [14]. Other research considers how to operate a chip when dimensions are so small as to preclude distribution of a reliable clock [15]. Such uncertainty leads researchers to propose various schemes for robust on-chip communications [16-18].

V. ACTIVE NETWORKING AT THE NANOSCALE

Active networks [37] [38] at the macroscale is a network paradigm in which intermediate network nodes—for example, switches, routers, hubs, bridges, gateways etc.—perform customized computation on packets flowing through them. The network is called “active” because new computations are injected into nodes dynamically, altering the behavior of the network. Packets in an active network can carry program code in addition to data. Customized computation is embedded within the packet’s code, which is executed on network nodes. By making network node computation application-specific, applications using the network can customize network behavior to suit their requirements.

A similar concept is seen in [36] where an active network architecture at the nanoscale is used to solve the problem of limited node size, which prevents the design of a single node that can perform all operations. Instead, DNA self-assembly designs different node types (e.g., add, memory, shift) based on node size constraints. A configuration phase at system startup determines defective nodes and links, organizes a memory system, and sets up routing in the network. When executed, an instruction searches for a node with the appropriate functionality (e.g., add), performs its operation, and passes its result to the next dependent instruction. In this active network execution model, the accumulator and all operands are stored within a packet, a

hallmark of macroscale active networks, rather than at specific nodes, thus reducing per-node resource demands. This enables the encoding of a series of dependent instructions within a single packet. Thus, the security techniques used to assure information in macroscale active networks might be called upon to help solve nanoscale active networks.

VI. SELF-ASSEMBLY AND INFORMATION ASSURANCE

Tags are used in DNA self-assembly to stimulate the construction of structures with specific properties. Once a DNA structure exists, other organic components can be attached to the structure and the attached components can be interconnected with communication links, perhaps composed of CNTs, to construct the functional equivalent of a computer chip, including large numbers of processing elements. For the short-term, DNA-based self-assembly is likely to be restricted to two layers. [5]

Alignment of Carbon nanotubes has been the topic of vigorous research. Cost and separation of impurities, namely metallic tubes, is still an unsolved problem. In the approach proposed by GE, lower-cost, randomly oriented tubes are directly utilized as a communication media. [23] Information flow through a CNT network may be controlled in spite of the random nature of tube alignment. The same technique used for sensing in CNT networks, namely, change in resistance of semiconducting material, may be used to effectively route information. The traditional networking protocol stack is inverted in this approach because, rather than the network layer being logically positioned above the physical and link layers, the CNT network and routing of information is an integral part of the physical layer. The potential benefits of better utilizing individual nanotubes within random carbon nanotube networks (CNT) to carry information is distinct from traditional, potentially less efficient and wasteful, approaches of using CNT networks to construct transistors which are then used to implement communication networks. [24]

Self-assembly is currently limited to producing small sized DNA lattices thus limiting circuit size. However, the parallel nature of self-assembly enables the construction of a large number (~109-1012) of nodes that may be linked together by self-assembled conducting nanowires." [26] This implies that control over the production process (for node placement, node orientation, and inter-node link creation) would be quite imprecise. Resulting devices produced by the same process could differ distinctly. Systems created using such techniques would need to discover the placement, orientation and connection among nodes and organize their run-time processes to take maximum advantage of the characteristics of the system. Different systems, created with the same processes, could yield devices with varying capabilities. The same technique that would enable systems to determine and utilize a "nano-network" might also be used to attack such a network.

Alternatively, self-assembled systems might be considered as stochastic systems whose performance envelops can be described only probabilistically. Ultimately, self-assembly at the nanoscale seems destined to create systems with intrinsic defects. Two types of defects have been noted: functional and positional. A functional defect corresponds to a component that does not perform its specified function and a positional defect corresponds to a potentially functionally correct component that is placed incorrectly. This implies that nanoscale systems must be designed with fault tolerance as a fundamental property.

Nanotechnology provides smaller, faster, and lower energy devices, which allow more powerful and compact circuitry; however, these benefits come with a cost—the nanoscale devices may be less reliable. Thermal- and shot-noise estimations alone suggest that the transient fault rate of an individual nanoscale device may be orders of magnitude higher than today's devices. As a result, one can expect combinational logic to be susceptible to transient faults, not just the storage and communication systems. Therefore, to build fault-tolerant nanoscale systems, one must protect both combinational logic and memory against transient faults. Based on these assumptions, researchers are investigating error-correcting codes that can work effectively under the higher error rates expected from nanoscale memories. [19]

VII. CONCLUSIONS

Nanoscale networking is still in its infancy, however, it may not be too early to begin outlining the potential information assurance challenges that such networks will have. This paper attempts to layout the current nanonetworking approaches and identify aspects of their security.

REFERENCES

[1] The Third International Conference on Nano-Networks (Nano-Nets 2008), Sept 15-17, Boston, MA, http://nanonets.org/cfp.shtml.

[2] Adamson, B., Bormann, C., Handley, M., Macker, J., Negative-acknowledgment (NACK)-Oriented Reliable Multicast (NORM) Protocol, IETF RFC 3940, November 2004.

[3] http://en.wikipedia.org/wiki/Semiconductor_fabrication

[4] http://www.webopedia.com/TERM/C/Carbon_Nanotube_Technology.html

[5] T. Raja, V. D. Agrawal, M. Bushnell, A Tutorial on Emerging Nanotechnology Devices, 17th International Conference on VLSI Design, Jan. 7, 2004.

[6] http://www.sigmaaldrich.com/Area_of_Interest/Chemistry/Materials_Science/Nanomaterials/Tutorial.html

[7] J. Patwardhan, ARCHITECTURES FOR NANOSCALE DEVICES, PhD Thesis, Department of Computer Science, Duke University, 2006.

[8] S. Hiyama, Y. Moritani, T. Suda, R. Egashira, A. Enomoto, M. Moore and T. Nakano, “Molecular Communication”, Proceedings of Nanotechnology 2005.
[9] P. Wolkotte, G. Smit, G. Rauwerda, L. Smit, “An Energy-Efficient Reconfigurable Circuit-Switched Network-on- Chip”, in Proceedings of the 19th IEEE Parallel and Distributed Processing Symposium, April 2005.
[10] P. Meloni, S. Murali, S. Carta, M. Camplani, L. Raffo, G. De Micheli, “ Routing Aware Switch Hardware Customization for Networks on Chips”, Proceedings of the 1st International Conference on Nano-Networks and Workshops, September 2006.
[11] D. Park, C. Nicopoulos, J. Kim, N. Vijaykrishnan, C. Da, “A Distributed Multi-Point Network Interface for Low- Latency, Deadlock-Free On-Chip Interconnects”, Proceedings of the 1st International Conference on Nano-Networks and Workshops, September 2006.
[12] I. O'Connor and F. Gaffiot, “ADVANCED RESEARCH IN ON-CHIP OPTICAL INTERCONNECTS”, report from a research conducted under an EU project: Photonic Interconnect Layer on CMOS by waferscale integration, circa 2005.
[13] A. Bartzas, N. Skalis, K. Siozios, D. Soudris, “Exploration of Alternative Topologies for Application-Specific 3D Networks-on-Chip”, Proceedings of the Workshop on Application -Specific Processors, 2007.
[14] K. Nomura, K. Abe, S. Fujita, A. Detion, “Novel Design of Three-Dimensional Crossbar for Future Network on Chip based on Post-Silicon Devices”, Proceedings of the 1st International Conference on Nano-Networks and Workshops, September 2006.
[15] M. Ghoneima, Y. Ismail, M. Khellah, V. De, “Variation-Tolerant and Low-Power Source-Synchronous Multicycle On-Chip Interconnection Scheme”, in Networks-on-Chip, special issue of VLSI Design, Hindawi Publishing Corporation, 2007.
[16] T. Lehtonen, P. Liljeberg, J. Plosila, “Online Reconfigurable Self-Time Links for Fault Tolerant NoC”, in Networks-on-Chip, special issue of VLSI Design, Hindawi Publishing Corporation, 2007.
[17] T. Bjerregaard, The MANGO Clockless Network-on-Chip: Concepts and Implementation, PhD Thesis, Technical University of Denmark, 2006.
[18] A. Hansson, K. Goossens, A. R˘adulescu, “Avoiding Message-Dependent Deadlock in Network-Based Systems on Chip”, in Networks-on-Chip, special issue of VLSI Design, Hindawi Publishing Corporation, 2007.
[19] S. Murali, D. Atienza, L. Benini, G. De Micheli, “A Method for Routing Packets Across Multiple Paths in NoCs with In-Order Delivery and Fault-Tolerance Guarantees”, in Networks-on-Chip, special issue of VLSI Design, Hindawi Publishing Corporation, 2007.
[20] P. Bogdan, T. Dumitras, R. Marculescu, “Stochastic Communication: A New Paradigm for Fault-Tolerance Networks-on-Chip”, in Networks-on-Chip, special issue of VLSI Design, Hindawi Publishing Corporation, 2007.
[21] H. Naeimi and A. DeHon, “Fault Tolerant Nano-Memory with Fault Secure Encoder and Decoder” ”, Proceedings of the 2nd International Conference on Nano-Networks and Workshops, September 2007.
[22] T. Mangir, “Integrity and Integration Issues for Nano -Tube Based Interconnect Systems”, Proceedings of the 2006 International Conference on Data Mining, June 2006.
[23] N. Srivastava and K. Banerjee, “Performance Analysis of Carbon Nanotube Interconnects for VLSI Applications”, Proceeings of the 2005 IEEE/ACM International Conference on Computer-aided Design, 2005.
[24] H. Colfen and S. Mann, “Higher-Order Organization by Mesoscale Self-Assembly and Transformation of Hybrid Nanostructures”, Angew. Chem. Int. Ed. 2003, 42, 2350 – 236.
[25] S. Bush and S. Goel, “Graph Spectra of Carbon Nanotube Networks”, Proceedings of the 1st International Conference on Nano-Networks and Workshops, September 2006.
[26] S. Bush and Y. Li, “Nano-Communications: A New Field? An Exploration into a Carbon Nanotube Communication Network, GE Technical Report 2006GRC066, February 2006.
[27] B. Agrawal, N. Srivastava, F. Chong, K. Banerjee, T. Sherwood, “Nano-enhanced Architectures: Using Carbon Nanotube Interconnects in Cache Design”, Proceedings of the 4th workshop on Non-Silicon Computing (NSC-4) held in conjunction with the 2007 International Symposium on Computer Architecture (ISCA'07 workshop), San Diego, California, June 2007.
[28] J. Patwardhan, C. Dwyer and A. Lebeck, “Self-Assembled Networks: Control vs. Complexity”, Proceedings of the 1st International Conference on Nano-Networks and Workshops, September 2006.
[29] Nathan A. Weir, Dannelle P. Sierra, and James F. Jones, “A Review of Research in the Field of Nanorobotics”, System Technologies, SAND2005-6808, October, 2005, Intelligent Systems and Robotics Center, Sandia National Laboratories.
[30] M. Sitti, “Micro- and nano-scale robotics,” in *Proc. American Control Conf.*, Boston, USA, June 2004, pp. 1–8.
[31] M. Sitti, "Microscale and nanoscale robotics systems [Grand Challenges of Robotics]," *Robotics & Automation Magazine, IEEE* , vol.14, no.1, pp.53-60, March 2007.
[32] G. Alfano; D. Miorandi, "On Information Transmission Among Nanomachines," *Nano-Networks and Workshops, 2006. NanoNet '06. 1st International Conference on*, vol., no., pp.1-5, Sept. 2006.
[33] “Electromagnetically coupled interconnect system,” United States Patent 6882239, 2005.
[34] M. Chang, V. Roychowdhury, L. Zhang, H. Shin, and Y Qian, "RF/Wireless interconnect for inter-and intra-chip communications," Proc. of the IEEE, vol. 89, no. 4, pp. 456-466, Apr. 2001.
[35] Nano-Net, Third International Conference on Nano-Networks, Boston, MA, Sept 15-17, 2008, http://nanonets.org/.
[36] J. P. Patwardhan, C. L. Dwyer, A. R. Lebeck, D. J. Sorin. “NANA: A Nanoscale Active Network Architecture”, ACM Journal on Emerging Technologies in Computing Systems) Vol. 2, No. 1, Pages 1-30, January 2006.
[37] S. F. Bush and A. Kulkarni, Active Networks and Active Network Management: A Proactive Management Framework, Kluwer Academic/Plenum Publishers, New York, Boston, Dordrecht, London, Moscow, 2001, 196 pp. Hardbound, ISBN 0-306-46560-4.
[38] S. F. Bush (2007), The Handbook of Computer Networks, John Wiley & Sons, chapter Active Networking, pp. 3008.
[39] C. H. Bennett & G. Brassard, (1984). Quantum cryptography: Public key distribution and coin tossing. In Proceedings of International Conference on Computers, Systems and Signal Processing, New York.

Manuscript received February 6, 2008 (date on which paper was submitted for review). Corresponding author: S. F. Bush (e-mail: bushsf@research.ge.com; phone: 518-387-6827; fax: 518-387-4042).