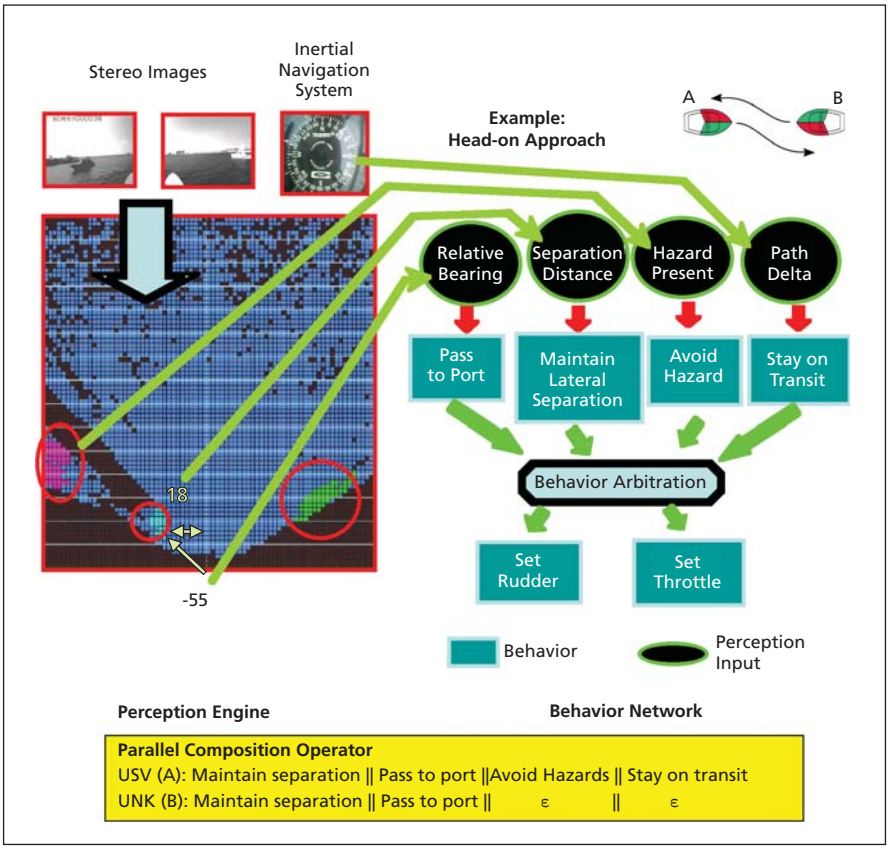



An example of the **Inference Mechanism** in a Rules-of-the-Road behavior shows two boats approaching each other head-on. The left side shows the sensory inputs that are needed by the behaviors that are competing with each other to control the actuators. The right side shows the behavior network with four behaviors fed into the Arbitration module to produce the settings for the rudder (heading) and throttle (speed) of the vehicle. Mapping of the behavior network to an equivalent cost-calculus expression is shown at the bottom.

action they choose and why. Robotic agents with enough self-awareness to dynamically adjust the information conveyed back to the Operations Center based on a detail level component analysis of requests could provide this description capability. One way to accomplish this is to map the behavior base of the robot into a formal mathematical framework called a cost-calculus. A cost-calculus uses composition operators to build up sequences of behaviors that can then be compared to what is observed using well-known inference mechanisms.

The explanation system is broken up into three subsystems that address the principal developments needed:

1. An inference mechanism for the mapping of observed behaviors into the cost-calculus: The observation equivalence of behaviors on a single autonomous agent and between two or more agents is done through bi-simulation relations. An example of the inference mechanism at work in a Rules-of-the-Road behavior is shown in the figure.
2. A learning mechanism for the cost-expression generation for observed behaviors outside of the cost-calculus tactical behavior base: Reinforcement learning of observed behavior patterns is used for the common grounding of behaviors sequences that were not previously observed, or that are in the command dictionary of the autonomous agent.
3. Explanation capabilities for the system: A dynamic decision tree decomposition of the observed behaviors is used to generate a set of rules for explanation. An adaptive level of detail is automatically built into this process in that all of the sensory information that led to a behavior is available, and can be conveyed to the operator if the human/machine interface (HMI) has a detail level of request capability.

*This work was done by Terrance L. Huntsberger of Caltech for NASA's Jet Propulsion Laboratory. Further information is contained in a TSP (see page 1).*

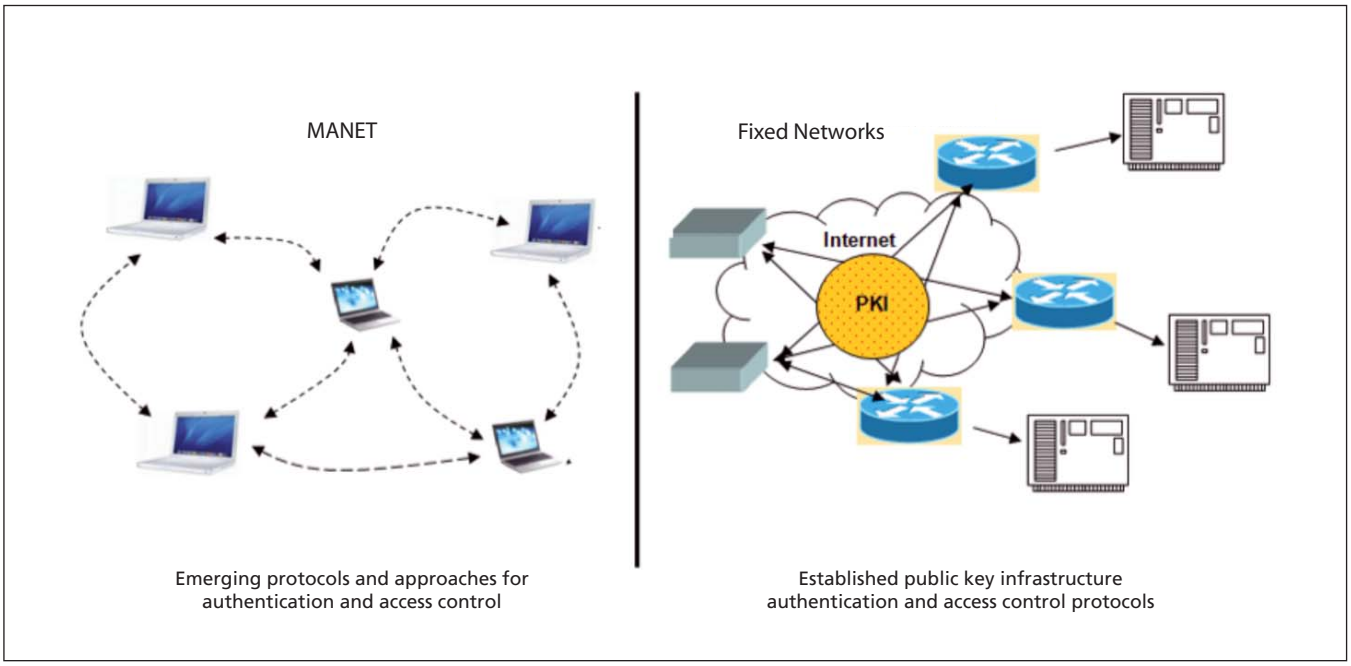
*The software used in this innovation is available for commercial licensing. Please contact Daniel Broderick of the California Institute of Technology at danielb@caltech.edu. Refer to NPO-46864.*

# A DNA-Inspired Encryption Methodology for Secure, Mobile *Ad Hoc* Networks

## An encryption mechanism uses the principles of DNA replication and steganography.

*Goddard Space Flight Center, Greenbelt, Maryland*

Users are pushing for greater physical mobility with their network and Internet access. Mobile *ad hoc* networks (MANET) can provide an efficient mobile network architecture, but security is a key concern. The figure summarizes differences in the state of network security for MANET and fixed networks. MANETs require the ability to distinguish trusted peers, and tolerate the ingress/egress of nodes on an unscheduled basis. Because the networks by their very nature are mobile and self-organizing, use of a Public Key Infrastructure (PKI), X.509 certificates, RSA, and nonce exchanges becomes problematic if the ideal of MANET is to be achieved. Molecular biology models such as DNA evolution can provide a basis for a proprietary security architecture that achieves high degrees of diffusion and confusion, and resistance to cryptanalysis. A proprietary encryption mechanism was developed that uses the principles of DNA replication and steganography (hidden word cryptography) for confidentiality and authentication. The foundation of the approach includes organization of coded words and messages using base pairs organized into genes,




**MANET** versus fixed network security.

an expandable genome consisting of DNA-based chromosome keys, and a DNA-based message encoding, replication, and evolution and fitness. In evolutionary biology, fitness is a characteristic that relates to the number of offspring produced from a given genome. From a population genetics point of view, the relative fitness of the mutant depends upon the number of descendants per wild-type descendant. In evolutionary computing, a fitness algorithm determines whether candidate solutions, in this case encrypted messages, are sufficiently encrypted to be transmitted.

The technology provides a mechanism for confidential electronic traffic over a MANET without a PKI for authenticating users. Users may enter and leave a network at will. Users may alternate between trusted, untrusted, unknown, and malicious behavior. Existing mobile networks rely on PKI-provided certificates and public encryption standards such as AES (Advanced Encryption Standard). These are public standards, subject to continuous scrutiny for methods of attacking the underlying basis of security.

The DNA-inspired approach uses a rapidly evolving genome to resist cryptographic analyses. It produces one-way (encryption only) and two-way (encryption/decryption) codes. Because of the dynamic, evolutionary nature of this approach, potential intruders must continually intercept decoding instructions between source and destination. Missing one generation of genome decryption information seriously corrupts the decryption process. Missing multiple generations eventually renders previous decryption analyses useless. Potential attackers are likely to be unable to continuously intercept all traffic. The genome becomes more fit relative to cryptographic analyses. Furthermore, DNA provides a convenient molecule to establish a new type of physical layer encryption through which encryption codes are instantiated through biochemical means and read back or modified by biochemical means. Such encryption models provide "Security by Obscurity."

Areas of interest include proprietary secure virtual private MANETs, military MANETs, mobile-commercial MANETs, covert surveillance and tracking of goods, and commercial surveillance and tracking of goods.

*This work was done by Harry Shaw of Goddard Space Flight Center. Further information is contained in a TSP (see page 1).* ***GSC-15374-1***