Secure algorithm defends wireless networks against malicious nodes

Chaorong Peng

An innovative routing protocol and security algorithm improve the performance of mobile ad hoc networks for military applications.

Network-centric warfare\(^1\) is a highly effective combination of strategies, emerging tactics, techniques, procedures, and organizations in the military. Ad hoc wireless networks are useful for stable operations and reliable communication when security is a concern. Bringing the two together is thus a logical step. The success of ad hoc wireless networks depends on their routing protocols. Current routing protocols offer excellent solutions for situations in which people need to communicate in small groups. In the military, however, the focus is on the capability to collect, process, and distribute relevant data to thousands of locations.\(^2\) Not coincidentally or surprisingly, some properties of ad hoc wireless networks pose difficulties in military operations. Our research focuses on the development of ad hoc wireless networks that are suitable for network-centric architectures. This necessitates the creation of multi-communication environments for development and deployment of network-centric applications that seamlessly use open and industry-accepted standards across a wide range of connectivity infrastructures.

A desirable scenario would allow collecting, processing, and disseminating an uninterrupted flow of information through a controlling path while soldiers communicate with commanders via multiple routing paths, leading to central commanders gaining information dominance regarding the locations of soldiers, which is essential to operational patterns. Our assignment router identifier protocol (ARIP)\(^3\) enables this. The protocol includes intelligent clusterhead agents (ICHAs) that provide routing algorithms that are suitable for particular applications.

Mobile ad hoc networks (MANETs) play an important role in network-centric networks. However, they are quite vulnerable to malicious attacks because MANETs rely on protocols that use IP addresses extensively. Malicious nodes in an untrusted network environment can easily compromise IP addresses. However, due to their highly dynamic topology, MANETs cannot use a centralized scheme to connect nodes through network address translation (NAT)\(^4\) or host identify protocol (HIP).\(^5\) Another problem in using the conventional central services scheme is that the session key is needed to encrypt the entire conversation to defend against most of the attacks. In addition, encryption devices are expensive, often slow, hard to administer, and uncommon in the civilian sector.

In our ARIP routing protocol, a new layer embedded in an architectural model hides real IP addresses without a cen-

Figure 1. Packet delivery fractions for simulations using the dynamic hybrid multi routing protocol (DHMPR), assignment router identifier protocol (ARIP), the ATTACK model, and the DEFATTACK model. In the ATTACK model, malicious nodes employ a variety of attacks against ARIP. In the DEFATTACK model, we use the improving the defense against malicious attacks (IDMA) routing protocol to defend against attacks to ARIP. Using IDMA increases the packet delivery ratio about 56% compared to the ATTACK model.

Continued on next page
tral service or encryption devices. The ARIP model defines a set of components and the modular relationships among them based on the dynamic hybrid multi routing protocol (DHMRP) algorithm.\(^6\)

Based on ARIP, we designed a secure algorithm called improving the defense against malicious attacks (IDMA)\(^7\) that defends against malicious nodes that disrupt route discovery by impersonating the destination, responding with corrupted routing information, or disseminating forged controlling traffic. The IDMA algorithm is also able to counterattack malicious nodes when they launch denial of service attacks by broadcasting a large number of route requests, creating target traffic congestion by delivering huge amounts of data, or spoofing IP addresses and sending forged packets with fake IDs to the same target. We implemented the IDMA algorithm using the GloMoSim\(^8\) simulator and demonstrated its performance under a variety of operating conditions, as shown in Figure 1. Using the IDMA algorithm improves the packet delivery ratio about 56% compared to ARIP alone. IDMA’s inherent capability to improve defense against malicious attacks will be of great use in network-centric warfare as well as other applications.

**Author Information**

Chaorong Peng  
Florida Institute of Technology  
Selma, NC

Chaorong Peng is currently a PhD candidate at the Florida Institute of Technology. She received a BS degree from the University of Electronic Science and Technology of China in 1986, and an MS degree from the New Jersey Institute of Technology in 2003, both in computer and electrical engineering.

**References**